PRAXEOLÓGIA
SÚKROMIA

PRAXEOLÓGIA SÚKROMIA

Ekonomická logika
v cypherpunkovej implementácii

Tretie vydanie

MAX HILLEBRAND

Praxeológia súkromia
Ekonomická logika v cypherpunkovej implementácii

Tretie vydanie

Max Hillebrand

Slovenský preklad, 2026

Toto dielo je vydané do **verejnej domény**.

Žiadne práva nie sú vyhradené. Môžete ho voľne kopírovať, upravovať, šíriť a predvádzať, aj na komerčné účely, bez toho, aby ste o to museli žiadať.

OHLASY

„Odporúčania kníh od Maxa Hillebranda ma priviedli k dvom z mojich najobľúbenejších kníh všetkých čias. Jeho vlastná kniha sa teraz pridáva do tohto zoznamu. Praxeológia súkromia *dokáže plynule uplatniť misesovskú logiku na internetový svet, v ktorom dnes žijeme. Upozorňuje na nebezpečenstvo utopených nákladov plošného sledovania a vysvetľuje, prečo budúcnosť stále vyzerá sľubne, a to vďaka všetkým inováciám v technológii „Freedom-go-Up“ (teda v technológii, pri ktorej sloboda rastie), ktorú sa Max celý život snaží pomôcť uviesť do skutočnosti.“*

— Knut Svanholm

„Max sa súkromiu venuje a presadzuje ho, odkedy ho poznám, a Praxeológia súkromia *je kniha, na ktorú som celý ten čas čakal. Kniha spája cypherpunkový étos a rakúsku ekonómiu a pomáha ľuďom z každej tradície pochopiť tú druhú. V čase štátneho sledovania a kontroly je* Praxeológia súkromia *praktickým sprievodcom, ako brániť svoje súkromie.“*

— Luke de Wolf

„Praxeológia súkromia *výborne začleňuje axiómu odporu do ucelenej praxeologickej analýzy súkromia ako selektívneho odhaľovania a strategickej obrany. Spája rakúske princípy konania, cypherpunkový étos a softvérové inžinierstvo a ponúka praktický plán na budovanie paralelných inštitúcií, ktoré zvyšujú náklady na sledovanie. Syntéza je súdržná aj aktuálna a ukazuje, prečo na odolných peniazoch, anonymnej komunikácii a decentralizovaných protokoloch záleží ďaleko za hranicami jednej technológie. Ústredná syntéza o konaní a odpore je silná a čitatelia získajú veľa z dôsledného spojenia teórie*

a implementácie, ktoré kniha ponúka. Vrelo odporúčame každému, kto to myslí vážne s budovaním slobodnejšej budúcnosti.“

— Eric Voskuil

„Kniha Praxeológia súkromia *od Maxa Hillebranda nadväzuje na myslenie Misesa, Rothbarda a Hoppeho, ale aj iných mysliteľov, medzi nimi aj mňa, a pokračuje v rozširovaní vedy o slobode na ďalšie oblasti a témy. Hillebrand odmieta predstavu nezávislého „práva na súkromie“, ktoré by nebolo ukotvené vo vlastníckych právach k hmotným zdrojom. Súkromie nie je samostatné vlastnícke právo, ale výsledok rešpektovania sebavlastníctva a vlastníckych práv. Napriek tomu je súkromie nesmierne dôležité: je to schopnosť selektívne sa odhaliť svetu, jeden z aspektov účelného správania. Hillebrand rozvíja aj to, čo nazýva axiómou odporu, vychádzajúcou z Voskuilovej knihy „Kryptoekonómia“ (angl.* Cryptoeconomics*), aby vysvetlil, prečo práva kontrolovať zdroje vyžadujú schopnosť odolať vonkajšej kontrole. Je to pútavé a ambiciózne dielo, ktoré poteší a vyprovokuje všetkých, čo hladujú po ďalšom skúmaní praxeológie a slobody.“*

— Stephan Kinsella, autor knihy „Proti ‚duševnému vlastníctvu‘ “ (angl. *Against Intellectual Property*)

ÚVODNÉ SLOVO

Paul Rosenberg

Praxeológia súkromia je mimoriadna kniha a hlavný dôvod, prečo to hovorím, je jednoduchý: dvadsať rokov som strávil v zákopoch súkromia a za ten čas som sa naučil veľa vecí, ktoré ma stáli veľa času a úsilia. Max Hillebrand však všetky tie lekcie, a ešte ďalšie, zhromaždil do knihy, ktorú dostanete za skromnú cenu a z ktorej sa dokážete hlboko vzdelať za pomerne málo hodín.

Za takto prístupné informácie by som pred rokmi zaplatil draho.

Podľa mňa má kniha tri hlavné prednosti. Prvá je jednoducho v tom, že Max nevysvetľuje len veci samotné, ale aj prečo sú pravdivé a prečo fungujú tak, ako fungujú. Ak ste aspoň trochu ako ja, práve táto zložka drží celý výklad pokope. Zoznamy faktov sú fajn, ale až pochopenie, ako a prečo fungujú, urobí z celku niečo zrozumiteľné, rozpoznateľné a zapamätateľné.

Druhý faktor poznám z rokov priateľstva s Maxom a som rád, že vám ho môžem odovzdať: Max to nielen pozoroval, on to žil. Žil cypherpunkovým životom. (Cypherpunkeri sú zástancovia súkromia a šifrovania.) Myšlienky z tejto knihy musel vyskúšať v skutočnom živote, a to už mnoho rokov. To nevyhnutne oddeľuje zrno od pliev a bez toho sa nezaobíde nijaké praktické pochopenie toho, čo funguje a čo nie. Skúška v skutočnom svete odstráni nepochopenie aj plytké chápanie ako máločo iné. Pekne znejúce myšlienky, ktoré by neprežili nepriateľský styk so svetom, teda odpadli ešte pred napísaním tejto knihy.

Tretí dôvod, prečo si knihu cením, by ste od názvu nečakali: kým skončíte, získate výborné vzdelanie z ekonómie. Hoci je to ďaleko od učebnice ekonómie, prienik medzi ľudskými motiváciami, stimulmi a nákladmi (peňažnými aj inými), ktoré sa s tým všetkým spájajú, sa azda najlepšie vysvetľuje ekonomickými pojmami. A tak vás tento najlepší spôsob výkladu mimochodom zoznámi s množstvom ekonómie, hoci si ani neuvedomíte, že sa ekonómiu učíte.

Dlhé roky nám takýto rozbor súkromia v ľudskom živote a ľudských záležitostiach chýbal. Teraz ho máme a vrelo odporúčam, aby ste si knihu zaobstarali. Na pochopenie informačnej ekonomiky 21. storočia potrebu-

jete buď túto knihu, alebo kariéru v oblasti súkromia. Verte mi, že tadiaľto je to ľahšie.

Paul Rosenberg máj 2026

PREDSLOV

Súkromie je predpokladom každého dobrovoľného dojednania, ktoré slobodný človek uzatvára, a z každodenného života ho systematicky vytláčajú. Táto kniha je o podmienkach, za akých prežije. Súkromie v pracovnom zmysle, aký tu rozvíjame, je selektívne odhaľovanie (selective disclosure): moc rozhodnúť, čo sa odhalí a komu. Selektívne odhaľovanie je silnejší pojem než skrývanie alebo tajnosť. Práve zámena týchto troch pojmov je hlavným dôvodom, prečo verejná debata o sledovaní uviazla na mŕtvom bode.

Téma sa stala naliehavou, lebo dve infraštruktúry dozreli naraz. Kryptografické schopnosti, ktoré stačia na ochranu bežnej komunikácie, platieb, identity aj výpočtov, sú už v ostrej prevádzke. Nasadzujú sa postkvantové podpisy, prahové systémy, dôkazy s nulovou znalosťou aj výpočty nad šifrovanými údajmi, a ľudia ich používajú. Rovnako dozrel pozorovací stack (vrstvený súbor technológií), ktorý sa medzitým zostavil na druhej strane. Komerčný špionážny softvér (spyware) sa cez telefóny vo vreckách dostane k novinárom, právnikom aj politikom z opozície.[1] Dátoví brokeri (obchodníci s osobnými údajmi) predávajú zhromaždené záznamy úradom, ktoré ich kedysi museli získavať priamo. Návrhy vo veľkých jurisdikciách by nariadili skenovanie vnútri šifrovaných aplikácií, a tým by odstránili ochranu, ktorú poskytuje end-to-end šifrovanie.[2] Programovateľné peniaze s obmedzeniami výdavkov, ktoré určuje emitent, prechádzajú z výskumu do pilotných projektov.[3] O postavenie predvolenej voľby súperia dve architektúry. Ktorá z nich sa stane bežnou infraštruktúrou, tú bude v rámci obvyklého politického kalendára ťažké nahradiť.

Tlak sa netýka jednej skupiny ľudí. Novinár chrániaci zdroj, majiteľ malej firmy, ktorému platobný procesor bez vysvetlenia zmrazil účet, lekár, ktorého záznamy o pacientoch ležia na serveri dodávateľa, rodič, ktorého dieťaťu škola vydáva povinné zariadenia so sledovaním, organizátor opozície v krajine s nepriateľskými úradmi, vývojár, ktorý chce vydať fungujúci systém bez výzvy od úradov: všetci pôsobia v tom istom prostredí pozorovania a všetci majú na svoju obranu k dispozícii tie isté kryptogra-

fické primitíva. Otázka, kto môže overovať, kto môže odmietnuť a kto môže budovať, už nie je záležitosťou špecialistov.

Kniha spája dve tradície, ktoré dospeli k rovnakým záverom z rôznych východísk. Rakúska ekonómia odvodzovala z faktu, že ľudia konajú. Dospela k tomu, že súkromie je štrukturálnou súčasťou uvažovania a výmeny, že zdravé peniaze sú nevyhnutné pre ekonomickú koordináciu, že štát je systematická agresia v takom rozsahu, aký mu dovoľuje jeho schopnosť vynucovať, a že problém socialistickej kalkulácie robí z centrálneho plánovania nezmysel.[14] Cypherpunková tradícia vychádzala z kryptografického inžinierstva, ktoré sa opiera o agoristické a voluntaryistické myslenie.[15] Ukázala, že súkromie sa dá brániť v ostrej prevádzke, že zdravé peniaze sa dajú naprogramovať, že systémy sa dajú postaviť tak, aby odolali kontrole za cenu, ktorú ich prevádzkovatelia unesú, a že infraštruktúra môže byť dosť otvorená, aby ju mohol overiť každý používateľ. Ich syntéza je účelom tejto knihy.

Medzi oboma tradíciami sa tiahne stará a praktická medzera. Rakúske spisy sa k otázke implementácie zaväzujú zriedka a mnohé sa zastavia pri diagnóze, lenže štát, ktorému hrozí softvér, nepresvedčí ďalšia esej. Cypherpunková prax sa často zaviaže k implementácii skôr, než si vyrieši otázku politickej ekonómie. Vytvorí fungujúcu kryptografiu, ktorá ako spoločenský systém môže aj tak zlyhať. Tvorcovia systémov centralizujú, čo malo zostať rozptýlené, robia kompromisy, ktoré zrádzajú účel systému, prehrávajú v súboji so stimulmi, ktoré nikdy nepreskúmali, a vydávajú produkty, ktoré obracajú naruby ochranu, akú ich technológia dáva. Teoretici zverejňujú vysvetlenia pasce a nástroje nechávajú iným. Každá tradícia potrebuje tú druhú a to, čo majú spoločné, stačí na to, aby sa znovu postavila obranná vrstva, ktorú éra sledovania zbúrala.

Kniha je pojednanie: dôsledná argumentácia, ktorá postupuje cez definíciu, odvodenie, vymedzenie rozsahu a krížový odkaz. Každá kapitola uvedie, čo ustanovuje, odvodí záver z predchádzajúcich kapitol, vymedzí svoj rozsah, aby sa nepustila za hranice dôkazov, a ukáže dopredu, kde odvodenie pokračuje. Štrukturálnu prácu robia tri axiómy. Misesova axióma konania chápe súkromie ako podmienku účelného konania smerujúceho k zvoleným cieľom. Hoppeho axióma argumentácie ho chápe ako podmienku racionálneho diskurzu. Voskuilova axióma odporu ho chápe ako dôsledok zvyšovania nákladov na pozorovanie nad hranicu, ktorú je pozorovateľ ochotný zaplatiť. Kapitoly tieto axiómy uplatňujú na kryptografické primitíva, vďaka ktorým je takéto inžinierstvo možné.

Rakúska línia, ktorú kniha preberá, vedie od Misesa[4] (konanie) cez Rothbarda[5] (vlastníctvo), Hoppeho[6] (argumentácia) a Hayeka[7] (problém znalostí) po Oppenheimera[8] (pôvod štátu). Cypherpunkovú líniu tvoria May[9] a Hughes[10] s úvahami o politickom význame kryptografie, Finney[11] s fungujúcim kódom, Nakamoto[12] so zdravými digitálnymi peniazmi a Voskuil[13]

s axiómou odporu. Agoristické a voluntaryistické spisy, ktoré formovali sebapochopenie cypherpunkerov, sa objavujú tam, kde majú váhu. Tvrdenia o súkromí, ktoré kniha obhajuje, stoja na troch právach, ktoré sú spoločným základom libertariánsko-rakúskej tradície: na sebavlastníctve tela, na vlastníckych právach k fyzickým zdrojom a na zmluve. „Právo na súkromie“ ako samostatná kategória sa nepoužíva. Kapitola 6 rozvádza vlastnícko-teoretický rámec do podrobností a vyznačuje, kde ležia stále živé spory v rámci rakúskej školy o patenty a autorské právo.

Čitateľ z rakúskej tradície nájde teóriu uplatnenú v praxi. Kryptografické primitíva sa tu prekladajú cez ekonomické analógie a inžinierske argumenty sú formálne zlučiteľné s axiomatickou metódou. Čitateľ z cypherpunkovej tradície nájde ekonomický a praxeologický rámec, o ktorý sa veľká časť tejto tradície už nevysloveným spôsobom opiera: prečo na týchto systémoch záleží aj nad rámec ich technických prednosti, ktoré kompromisy zachovávajú ich účel a ktoré ho ničia, a ako sa projekty zdravých peňazí a kryptografie zbiehajú do jedného prevádzkového stacku. Čitateľ, ktorý nepatrí k žiadnej z tradícií, ale cíti, že sa niečo utiahlo, a chce pochopiť prečo, nájde argument prístupný od základných princípov. Jediným predpokladom je vážny záujem.

Súkromie patrí k podmienkam, v ktorých ľudia uvažujú, vymieňajú, šetria, koordinujú sa a žijú nepozorovaní, keď sa tak rozhodnú. Strategické tvrdenie, ktoré kapitoly rozvíjajú, je jednoduché. Štátne vykorisťovanie závisí od štátneho pozorovania. Keď sa pozorovanie zlacní, zlacní sa aj vykorisťovanie, a keď sa pozorovanie predraží, vykorisťovanie ustupuje. O inžinierstve, ktoré zvyšuje náklady na pozorovanie, je táto kniha.

Poznámky

[1] Citizen Lab pri Torontskej univerzite, `https://citizenlab.ca/`, je hlavným empirickým zdrojom dokumentujúcim infekcie komerčným spyware u novinárov, disidentov, právnikov a politikov v súvislosti s viac než tridsiatimi štátnymi zákazníkmi. Pegasus od firmy NSO Group, `https://www.nsogroup.com/`, je referenčný produkt. Vo veci *WhatsApp LLC v. NSO Group*, Case No. 4:19-cv-07123 (N.D. Cal. 2024), vznikol prvý významný občianskoprávny rozsudok o zodpovednosti voči dodávateľovi spyware.

[2] Nariadenie EÚ o sexuálnom zneužívaní detí („Chat Control“ / CSAR), návrh COM(2022) 209, `https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52022PC0209`; britský zákon o bezpečnosti online (Online Safety Act 2023), oddiel 122, `https://www.legislation.gov.uk/ukpga/2023/50/section/122`. Európsky súd pre ľudské práva vo veci *Podchasov v. Russia* (App. no. 33696/19) z 13. februára 2024, `https://hudoc.echr.coe.int/`, rozhodol, že zákonná povinnosť oslabiť end-to-end šifrovanie „sa nedá považovať za nevyhnutnú v demokratickej spoločnosti“ (angl. „cannot be regarded as necessary in a democratic society“).

[3] Atlantic Council, „Central Bank Digital Currency Tracker“, `https://www.atlanticcouncil.org/cbdctracker/`, sleduje viac než sto

jurisdikcií vo fáze výskumu, pilotných projektov aj ostrej prevádzky. Human Rights Foundation, „CBDC Tracker“, https://cbdctracker.hrf.org/, sa zameriava na dôsledky pre občianske slobody.

[4] Ludwig von Mises, *Human Action: A Treatise on Economics*, 4. rev. vyd. (Irvington-on-Hudson, NY: Foundation for Economic Education, 1996; pôvodne 1949), https://mises.org/library/book/human-action. Základný text praxeológie: ekonómia odvodená prísnou dedukciou z axiómy konania, teda z faktu, že ľudia konajú účelne, aby odstránili pociťovaný nepokoj (Prvá časť, najmä s. 11–29). Konajúci, ktorého plány sledujú protivníci, je v schopnosti dosahovať zvolené ciele oslabený. Tento dôsledok axiómy konania je praxeologickým základom, na ktorom stojí výklad súkromia v tejto knihe. Misesov samostatný argument, že peňažná kalkulácia vyžaduje súkromné vlastníctvo a skutočné ceny (s. 200–231), podporuje tézu o socialistickej kalkulácii citovanú v poznámke 14. Mises Institute poskytuje celý text zadarmo.

[5] Murray N. Rothbard, *Man, Economy, and State: A Treatise on Economic Principles*, 2. vyd. Scholar's Edition (Auburn, AL: Ludwig von Mises Institute, 2004; pôvodne 1962), https://mises.org/library/book/man-economy-and-state-power-and-market; a Rothbard, *The Ethics of Liberty* (New York: New York University Press, 1998; pôvodne 1982), https://mises.org/library/book/ethics-liberty. *Man, Economy, and State* rozširuje Misesovu praxeológiu na teóriu cien, kapitálu a štruktúry výroby a všetku výmenu zakladá na dobrovoľnom súhlase. *The Ethics of Liberty* zakladá individuálne práva na sebavlastníctve a princípe neagresie a ustanovuje vlastnícky rámec, ktorý argument knihy o súkromí preberá v celom rozsahu.

[6] Hans-Hermann Hoppe, *The Economics and Ethics of Private Property: Studies in Political Economy and Philosophy*, 2. vyd. (Auburn, AL: Ludwig von Mises Institute, 2006), https://mises.org/library/book/economics-and-ethics-private-property. Hoppeho etika argumentácie (argumentation ethics) odvodzuje vlastnícke práva z performatívnych predpokladov racionálneho diskurzu: kto argumentuje, ten už predpokladá sebavlastníctvo a kontrolu nad prostriedkami, ktorými argumentuje, pretože popierať túto kontrolu znamená protirečiť sám sebe. Kapitola 4 rozvíja tento rámec ako normatívny základ pre chápanie súkromia ako podmienky racionálneho diskurzu.

[7] Friedrich A. Hayek, „The Use of Knowledge in Society“, *American Economic Review* 35, č. 4 (1945): 519–530, https://www.econlib.org/library/Essays/hykKnw.html. Kanonické vyjadrenie problému znalostí: ceny koordinujú rozptýlené miestne znalosti, ktoré nijaká ústredná autorita nemôže zhromaždiť ani spracovať, a každý systém, ktorý potláča cenový mechanizmus, potláča aj informáciu, ktorú ceny nesú. Hayek, *The Constitution of Liberty* (Chicago: University of Chicago Press, 1960), Druhá časť, rozvíja súvisiaci argument, že sloboda je sčasti vymedzená priestorom, v ktorom sa plány človeka nemusia odhaliť úradom.

[8] Franz Oppenheimer, *The State: Its History and Development Viewed Sociologically*, prel. John M. Gitterman (New York: B. W. Huebsch, 1914; pôvodne *Der Staat*, 1908), https://mises.org/library/book/state. Oppenheimerovo ústredné rozlíšenie medzi „ekonomickými prostriedkami“ (dobrovoľná výroba a výmena) a „politickými prostriedkami“ (donucovacie vyvlastňovanie) dáva analytický základ pre chápanie štátu ako vykorisťovateľského už svojím pôvodom. Albert Jay Nock, *Our Enemy, the State* (Caldwell, ID: Caxton Printers, 1935), uplatňuje tento rámec na americké dejiny. Obe diela stoja za výkladom štátneho sledovania ako vykorisťovania v kapitole 4.

[9] Timothy C. May, „The Crypto Anarchist Manifesto“ (1988), https://www.activism.net/cypherpunk/crypto-anarchy.html; a Timothy C. May, „Crypto Anarchy and Virtual Communities“ (1994), https://nakamotoinstitute.org/library/virtual-communities/. May predpovedal, že kryptografia s verejným kľúčom prinesie nezvratné zmeny v rozsahu

vládnej regulácie, v schopnosti zdaňovať a kontrolovať ekonomické interakcie a v tom, ako fungujú dôvera a reputácia. Politický program sformuloval skôr, než existovala infraštruktúra, ktorá by ho mohla vykonať.

[10] Eric Hughes, „A Cypherpunk's Manifesto“ (9. marca 1993), `https://www.activism.net/cypherpunk/manifesto.html`. Prevádzkový doplnok k Mayovmu manifestu: kým May pomenúva, o čo ide politicky, Hughes určuje inžinierske požiadavky. Súkromie sa musí brániť anonymnými transakčnými systémami a otvoreným kryptografickým kódom, nie dôverou v inštitúcie. Hughesova definícia súkromia ako „moci selektívne sa odhaliť svetu“ je definícia, ktorú táto kniha prijíma.

[11] Hal Finney, „RPOW: Reusable Proofs of Work“ (15. augusta 2004), `https://nakamotoinstitute.org/rpow/`; a Finney, „Bitcoin and me“, BitcoinTalk (19. marca 2013), `https://bitcointalk.org/index.php?topic=155054.0`. Finneyho systém RPOW bol priamym technickým predchodcom ťažobného mechanizmu Bitcoinu a prvou fungujúcou implementáciou prenosného digitálneho tokenu krytého výpočtovou prácou. Finney bol tiež príjemcom prvej bitcoinovej transakcie (od Nakamota, 12. januára 2009) a jeho rozprávanie o vlastnej rannej účasti opisuje Bitcoin ako vyvrcholenie cypherpunkového projektu.

[12] Satoshi Nakamoto, „Bitcoin: A Peer-to-Peer Electronic Cash System“ (31. októbra 2008), `https://bitcoin.org/bitcoin.pdf`. Deväťstranový whitepaper, ktorý uvádza Bitcoin: decentralizovaný elektronický hotovostný systém, ktorý na dosiahnutie konsenzu bez dôveryhodnej tretej strany používa reťazec dôkazov práce (proof-of-work chain). Model súkromia v oddiele 10 stojí na pseudonymite a oddelení kľúčov. Whitepaper je zakladajúci dokument oblasti kryptomien a prvý fungujúci dôkaz, že zdravé digitálne peniaze sa dajú vybudovať bez ústredného emitenta.

[13] Eric Voskuil, *Cryptoeconomics: Fundamental Principles of Bitcoin* (Libbitcoin Institute, 2020), `https://github.com/libbitcoin/libbitcoin-system/wiki/Cryptoeconomics`. Voskuilova axióma odporu tvrdí, že bezpečnostný model Bitcoinu predpokladá ľudí ochotných vzdorovať štátnemu nátlaku na vlastné osobné náklady. Bez tohto predpokladu sa Bitcoin zmení na databázu s povolením. Axióma je tretím štrukturálnym predpokladom, ktorý kniha používa popri Misesovej axióme konania a Hoppeho axióme argumentácie.

[14] Ludwig von Mises, „Economic Calculation in the Socialist Commonwealth“, prel. S. Adler, in *Collectivist Economic Planning*, ed. F. A. Hayek (London: Routledge, 1935; pôvodne *Die Wirtschaftsrechnung im sozialistischen Gemeinwesen*, 1920), `https://mises.org/library/essay/economic-calculation-socialist-commonwealth`. Práca, ktorá odštartovala debatu o socialistickej kalkulácii: racionálna ekonomická kalkulácia vyžaduje súkromné vlastníctvo výrobných prostriedkov a skutočné trhové ceny a nijaký socialistický plánovač nedokáže ani jedno z toho napodobniť. Problém kalkulácie a problém znalostí (poznámka 7) sa dopĺňajú: spolu ustanovujú, že centrálne plánovanie je v princípe nezmyselné.

[15] Samuel Edward Konkin III, *New Libertarian Manifesto* (Koman Publishing, 1980; 2. vyd. 1983), `https://agorism.info/NewLibertarianManifesto.pdf`. Zakladajúci dokument agorizmu: cesta k slobodnej spoločnosti vedie cez kontraekonómiu, teda mierovú dobrovoľnú výmenu mimo oficiálnej ekonomiky, nie cez volebnú politiku. Konkin vytvoril termíny „agorizmus“ a „kontraekonómia“ (counter-economics). Voluntaryistická tradícia, spájaná s Carlom Watnerom a časopisom *The Voluntaryist* (`https://voluntaryist.com/`), dospieva k podobným záverom cez zásadové nezúčastňovanie sa. Oba prúdy sformovali presvedčenie cypherpunkerov, že na budovaní fungujúcich systémov záleží viac než na vyhrávaní politických sporov.

Obsah

Ohlasy v
Úvodné slovo vii
Predslov ix
Obsah xv

I Úvod **1**

1 Podstata súkromia 3
1.1 Súkromie ako kontrola nad odhaľovaním 3
1.2 Tri príbuzné pojmy 4
1.3 Súkromie ako strategická obrana 5
1.4 Argument knihy v skratke 5
2 Dve tradície, jeden záver 11
2.1 Rakúsky prístup: odvodzovanie z konania 11
2.2 Cypherpunkový prístup: budovanie toho, čo teória vyžaduje 14
2.3 Nezávislá konvergencia: prečo obe dospeli na to isté miesto 17

II Filozofické základy **23**

3 Axióma konania: súkromie ako štrukturálna vlastnosť 25
3.1 Axióma konania 26
3.2 Vnútorné premýšľanie a subjektívne hodnotenie 27
3.3 Informačná asymetria a kontrola 28
4 Axióma argumentácie a sebavlastníctvo 33
4.1 Argument: performatívny rozpor 34
4.2 Námietky a odpovede 35
4.3 Otázka is--ought 39
4.4 Dôsledky: vlastníctvo a neagresia 41
4.5 Axióma argumentácie a súkromie 42
5 Axióma odporu 49
5.1 Čo axióma tvrdí 50
5.2 Prečo je axióma dobre podložená 51
5.3 Vzťah k ostatným základom 53

III Ekonomické základy **57**

6 Informácia, vzácnosť a vlastníctvo . . . 59
6.1 Vzácnosť ako základ vlastníctva . . . 60
6.2 „Duševné vlastníctvo`` ako agresia . . . 61
6.3 Obsah a nosič: rozhodujúci rozdiel . . . 63
6.4 Ako sa chráni súkromie . . . 64
6.5 Dôsledky pre analýzu súkromia . . . 66

7 Teória výmeny a súkromie . . . 75
7.1 Logika výmeny . . . 75
7.2 Ako súkromie zlepšuje výmenu . . . 76
7.3 Ako sledovanie skresľuje výmenu . . . 78
7.4 Výmena môže prebiehať aj pod sledovaním . . . 80
7.5 Konkrétne výmenné prostredia . . . 81

8 Teória kapitálu a podnikanie . . . 87
8.1 Infraštruktúra súkromia ako kapitálové statky . . . 88
8.2 Časová preferencia a kompromis medzi súkromím a pohodlím . . . 89
8.3 Podnikateľské objavovanie v oblasti súkromia . . . 90
8.4 Heterogenita kapitálu a špecializácia v súkromí . . . 92
8.5 Tvorba kapitálu a rozvoj súkromia . . . 92

9 Teória peňazí a zdravé peniaze . . . 97
9.1 Trhový pôvod peňazí . . . 98
9.2 Regresná teoréma . . . 98
9.3 Vlastnosti zdravých peňazí . . . 100
9.4 Fiat peniaze a ich problémy . . . 101
9.5 Slobodné a centrálne bankovníctvo . . . 102
9.6 Peniaze v pravom zmysle a peňažné náhrady . . . 103
9.7 Požiadavky na digitálne peniaze . . . 104
9.8 Most k Bitcoinu . . . 105

IV Protivník **111**

10 Finančné sledovanie a štátna kontrola . . . 113
10.1 Teória intervencií: autistická, binárna, trojuholníková . . . 113
10.2 Autistická intervencia a súkromie . . . 114
10.3 Binárna intervencia a súkromie . . . 115
10.4 Trojuholníková intervencia a súkromie . . . 116
10.5 Digitálne meny centrálnych bánk ako totálna intervencia . . . 119
10.6 Rozhodovací cyklus protivníka . . . 125

11 Firemné sledovanie a vyťažovanie údajov . . . 133
11.1 Obchodný model vyťažovania údajov . . . 133
11.2 Prepojenie firiem a štátu . . . 135
11.3 Je to zlyhanie trhu? . . . 136
11.4 Problém nezvratnosti . . . 139

11.5 Reakcie trhu a konkurencia v súkromí 141
12 Analytický stack 151
12.1 Deľba práce v sledovaní 151
12.2 Strojové videnie vo veľkom 152
12.3 Model ako analytik 153
12.4 Kanál dátových brokerov 154
12.5 Infraštruktúra vo fyzickom svete 156
12.6 Komerčný špionážny softvér 157
12.7 Stlačenie slučky OODA 159
12.8 Prečo úrady stále nakupujú 160
12.9 Prečo stack existuje práve teraz 161
13 Kryptovojny 167
13.1 História: od exportných kontrol po čip Clipper 167
13.2 Ekonomická logika kontroly nad kryptografiou 169
13.3 Prečo kontrola zlyháva (a kde nie) 171
13.4 Súťaž jurisdikcií a arbitráž 172
13.5 Vojna pokračuje 173

V Technická implementácia 183

14 Kryptografické základy 185
14.1 Symetrická a asymetrická kryptografia 186
14.2 Hašovacie funkcie a digitálne podpisy 188
14.3 Dôvera: matematická a inštitucionálna 189
14.4 Obmedzenia a zraniteľnosti 191
15 Dôkazy s nulovou znalosťou 199
15.1 Dilema overovania 199
15.2 Princíp ZK: dokázať bez odhalenia 200
15.3 Druhy: SNARK, STARK, Bulletproofs 201
15.4 Aplikácie: Zcash, rollupy, identita 203
15.5 Ekonomické dôsledky: overovanie ako služba 208
15.6 Obmedzenia 208
16 Výpočty nad tajomstvami 215
16.1 Rozdiel medzi overením a vykonaním 216
16.2 Homomorfné šifrovanie: aritmetika nad šifrovým textom 216
16.3 Bezpečný výpočet viacerých strán 218
16.4 Dôveryhodné prostredia na vykonávanie kódu 220
16.5 Súkromné získavanie informácií 224
16.6 Diferenciálne súkromie a vrstva agregácie 225
16.7 Návrhový priestor a doplnky 228
16.8 Axióma odporu použitá na výpočty 229
17 Anonymné komunikačné siete 237
17.1 Problém: ako internet prezrádza súkromie 237

17.2 Požiadavky na anonymnú komunikáciu . . . 239
17.3 VPN: jednoduché, ale obmedzené riešenie . . . 241
17.4 Cibuľové smerovanie: Tor a I2P . . . 242
17.5 Mixnety: najsilnejšia ochrana . . . 246
17.6 Prečo nestačí jediná architektúra anonymity . . . 248
17.7 Keď internet nie je sieť . . . 248
17.8 Šifrovaná komunikácia: aplikačná vrstva . . . 251
18 Bitcoin a prelom v digitálnych peniazoch . . . 265
18.1 Dva problémy digitálnych peňazí . . . 265
18.2 Predchodcovia a ich zlyhania . . . 266
18.3 Nakamotov konsenzus . . . 268
19 Bitcoin ako zdravé a odolné peniaze . . . 279
19.1 Vlastnosti zdravých peňazí ako Schellingove body . . . 279
19.2 Vlastnosti odolnosti: prečo Bitcoin prežíva . . . 284
20 Súkromie na Bitcoine a menové vrstvy . . . 293
20.1 Ako zlyháva súkromie na základnej vrstve . . . 293
20.2 Programovateľné peniaze: skriptové primitíva . . . 300
20.3 Riešenia súkromia: spoločné transakcie a výmeny . . . 302
20.4 Platby mimo reťazca bez úschovy u tretej strany . . . 307
20.5 Vrstvy súkromia s úschovou u tretej strany . . . 311
20.6 Chránená validácia na strane klienta . . . 315
20.7 Porovnávacie kryptomeny so súkromím . . . 317
20.8 Kvantový horizont pre Bitcoin . . . 326
21 Decentralizovaná sociálna infraštruktúra . . . 341
21.1 Problém centralizovaných platforiem . . . 341
21.2 Nostr: riešenie na úrovni protokolu . . . 344
21.3 Kľúče ako identita: kryptografická suverenita . . . 346
21.4 Architektúra relayov a trhová dynamika . . . 348
21.5 Reputácia bez ústrednej autority . . . 349
21.6 Moderovanie ako trhová služba . . . 352
21.7 Nielen sociálne siete: jeden protokol, mnoho druhov obsahu . . . 353
21.8 Obmedzenia súkromia . . . 354
21.9 Prečo alternatívy nestačia . . . 359

VI Prax 369

22 Operačná bezpečnosť . . . 371
22.1 Modelovanie hrozieb: kto je váš protivník? . . . 371
22.2 Najslabší článok: ľudský faktor . . . 374
22.3 Technické základy bezpečnosti . . . 376
22.4 Kompartmentalizácia a oddelenie identít . . . 380
22.5 Organizačná bezpečnosť a problém infiltrácie . . . 382
22.6 Bezpečnosť miesta stretnutí a fyzické uzly . . . 384

22.7 Odhaľovanie sledovania . . . 385
22.8 Bežné spôsoby zlyhania (prípadové štúdie) . . . 386
22.9 Hranice OPSEC . . . 388
23 Stratégia zavádzania . . . 399
23.1 Začíname tam, kde sa nachádzate . . . 399
23.2 Skôr než začnete: použite model hrozieb . . . 400
23.3 Postupné kroky: od jednoduchých k pokročilým . . . 401
23.4 Hľadanie komunity . . . 407
23.5 Od individuálnej praxe k spoločnej praxi . . . 409
23.6 Čo nerobiť . . . 410
24 Dôvera a spory v paralelnej ekonomike . . . 423
24.1 Prečo samotné nástroje trh nevytvoria . . . 424
24.2 Reputácia pri pseudonymite . . . 424
24.3 Poverenia a selektívne odhaľovanie . . . 426
24.4 Escrow a jednoduché riešenie sporov . . . 428
24.5 Arbitráž a sporné fakty . . . 429
24.6 Objavovanie obchodníkov a vznik inštitúcií . . . 430
24.7 Súčasné limity a čestné hranice . . . 432
25 Budovanie paralelnej ekonomiky . . . 437
25.1 Zbiehanie základov . . . 437
25.2 Syntéza . . . 438
25.3 Prerušenie slučky pozorovania . . . 438
25.4 Čo sa podarilo . . . 439
25.5 Hranice a otvorené otázky . . . 443
25.6 Odpoveď na „nemám čo skrývať`` . . . 447
25.7 Záver . . . 448

ČASŤ I

ÚVOD

1
PODSTATA SÚKROMIA

„Súkromie je nevyhnutné pre otvorenú spoločnosť v elektronickom veku.“

Eric Hughes, *A Cypherpunk's Manifesto* (1993)[1]

Úvod

„Ak nemáte čo skrývať, nemáte sa čoho báť.“

Túto vetu počuť všade, kde sa hovorí o súkromí, a zaberá preto, že ešte pred začiatkom sporu podsunie nesprávnu definíciu.[2] Súkromie vyhlási za skrývanie. Keď sa to podarí, odpor proti sledovaniu vyzerá podozrivo od prvej chvíle.

Správna odpoveď nie je rozpačitosť ani slabé tvrdenie, že každý má nejakú súkromnú hanbu, ktorú nechce vystavovať na obdiv. Správna odpoveď je definičná: súkromie nie je ukrývanie viny, ale kontrola nad odhaľovaním. Keď sa tento bod ustáli, celý spor sa zmení.

Úplná odpoveď na argument „nemám čo skrývať“ príde na konci knihy, v kapitole 25. Zatiaľ ide o to, aby boli pojmy dosť jasné a argument nemohol podvádzať.

1.1 Súkromie ako kontrola nad odhaľovaním

Spory o súkromí sa zvyčajne rozpadnú preto, že sa slovu dovolí plávať. Jeden rečník myslí tajnosť, druhý anonymitu a tretí zákonnú ochranu pred prehliadkou. Výsledkom nie je ani tak nesúhlas, ako zrážka pojmov.

Eric Hughes sformuloval čistú definíciu, ktorú táto kniha preberá: súkromie je moc selektívne sa odhaliť svetu. Nosné slovo je *selektívne*.

Súkromie znamená riadiť odhaľovanie voči tým, ktorí majú na informáciu oprávnený nárok, a na účely, ktoré ju vyžadujú. Pacient, ktorý sa le-

károvi otvorene zdôverí, využíva súkromie. Rovnako obchodník, ktorý pred konkurenciou drží podmienky svojich dodávateľov. Nejde o absolútne skrývanie. Ide o kontrolu nad tým, kto čo vie, a tá kontrola je aktívna. Súkromie je schopnosť rozhodnúť, ktoré informácie pôjdu von a ktoré zostanú na mieste. Ak táto schopnosť zmizne, zmizne aj súkromie, hoci zatiaľ nikto odhalené údaje nezneužil. Náklad vzniká už stratou kontroly: každé ďalšie rozhodnutie konajúceho čelí širšiemu spektru možných reakcií protivníka.

Definícia zároveň vymedzuje predmet. Súkromie sa týka informácií o osobách: plánov, preferencií, korešpondencie, zdravia, financií, vzťahov, politického presvedčenia, polohy a tisícok ďalších podrobností, vďaka ktorým je život čitateľný pre tých, čo by ho chceli využiť. Kniha neskôr tvrdí, že informácia nemôže byť vlastníctvom v striktnom zmysle. Z toho však neplynie, že osobné informácie si môže vziať každý.

Táto úvaha berie argumentu „nemám čo skrývať" jeho lacnú silu. Každý riadi odhaľovanie a rôznym ľuďom odhaľuje rôzne fakty. Kto sa s účtovníkom rozpráva inak než na verejnosti, nekoná podozrivo, len ako človek.

1.2 Tri príbuzné pojmy

Ďalší zmätok vzniká tým, že sa tri rôzne myšlienky pokladajú za zameniteľné. Súkromie sa týka kontrolovaného odhaľovania, tajnosť skrývania a anonymita pripísania. Čiastočne sa prekrývajú, ale nesplývajú.[3]

Súkromie je z nich najširšie. Zahŕňa bežné nakladanie s informáciami vo vzťahoch, v ktorých sa ľudia poznajú. Človek môže byť pred lekárom úplne známy a súkromie mu zostane, ak záznamy o ňom ostanú pod náležitou kontrolou. Môže byť známy aj obchodnému partnerovi a súkromie si zachová, ak sa zdieľajú len podmienky potrebné na obchod.

Tajnosť je užšia a tvrdšia než súkromie. Tajomstvo je skryté pred všetkými okrem niekoľkých, ktorí o ňom majú vedieť, alebo pred všetkými bez výnimky. Na tajnosti stoja obchodné tajomstvá, ochrana zdrojov, spravodajské metódy aj súkromné kľúče. Niektoré súkromné veci sú tajné, ale mnohé nie.

Anonymita sa týka väzby medzi činom a konajúcim. Anonymný dar alebo neprepojená platba pozorovateľovi nepovie, kto čin vykonal; pseudonymná esej to povie len pod zvolenou identitou. Človek si môže zachovať anonymitu v jednej oblasti a byť v inej plne identifikovaný. Otázka nie je, čo sa o osobe vie vo všeobecnosti, ale či sa tento konkrétny čin dá pripísať tejto osobe.

Sledovanie ťaží z toho, že sa tieto pojmy pletú.

Ak sa súkromie zmieša s tajnosťou, obranca musí vysvetľovať, prečo niečo skrýva.

Ak sa anonymita zmieša s kriminálnym úhybom, obranca musí vysvetliť, prečo strpieť akékoľvek konanie bez pripísaného autora.

Ak sa tajnosť pokladá za celé súkromie, bežná kontrola nad osobnými informáciami začne vyzerať extrémne.

Lepší pohľad je priamy.

Súkromie je bežné a stále.

Tajnosť je užší prípad, ktorý vyžadujú niektoré činnosti.

Anonymita je nástroj, ktorý sa stane nevyhnutným, keď už samotné pripísanie vytvára nebezpečenstvo.

Mnohé skutočné situácie používajú viacero týchto nástrojov naraz. Novinár, ktorý chráni zdroj, môže potrebovať súkromie komunikácie aj tajnosť totožnosti zdroja. Kupujúci, ktorý používa platobný systém chrániaci súkromie, nemusí chcieť úplnú tajnosť. Môže mu stačiť, aby obchodníci a banky nemohli sledovať celú históriu jeho transakcií.

Argument proti súkromiu podvádza vtedy, keď sa tieto tri slová zlievajú.

1.3 Súkromie ako strategická obrana

Súkromie je mravné dobro aj strategická obrana.

Dôvod najjednoduchšie ukazuje slučka OODA Johna Boyda (pozoruj – zorientuj sa – rozhodni – konaj).[4] Protivník, ktorý chce kontrolovať, zhabať, potrestať, cenzurovať alebo predbehnúť, musí najprv pozorovať. Bez pozorovania sa zvyšok sledu zasekne. Štát, ktorý nevidí prostriedky, ich nemôže na príkaz zmraziť. Platforma, ktorá nevidí do správ, ich nemôže zoraďovať ani potláčať s rovnakou presnosťou. A regulátor, ktorý nevie zmapovať sieť, nenájde mäkké miesta, kde bude tlak bolieť najviac.

Pozorovanie je dôvod, prečo sa boj o súkromie začína tak skoro v reťazci. Vyzerá pasívne, ale nie je. Práve pozorovanie umožňuje, aby bol každý ďalší zásah cielený a lacný.

Výhoda obrancu leží presne tu. Sledovanie vyžaduje infraštruktúru, úložisko, indexovanie, právne oprávnenie, softvér, analytikov a čas. Protiopatrenie je často oveľa lacnejšie: kľúčový pár stojí takmer nič a end-to-end šifrovanie môže bežať na zariadeniach, ktoré ľudia už vlastnia. Komunikačný nástroj chrániaci súkromie dokáže znemožniť ľahký zber údajov za zlomok nákladov útočníka.[5]

Táto asymetria má väčšiu váhu než heslo, že súkromie je právo. Reč o právach je dôležitá, no o politickej realite stále z veľkej časti rozhodujú náklady. Štát si udrží kontrolu, kým je pozorovanie lacné. Zápasí, keď sa pozorovanie stane drahým a nespoľahlivým.

Táto kniha sa k tej asymetrii vráti mnohokrát. Tá asymetria je jedným z dôvodov, prečo nástroje súkromia vyvolávajú takú nevraživosť v inštitúciách postavených na sledovaní. Neskrývajú informácie. Zvyšujú cenu nadvlády.[6]

1.4 Argument knihy v skratke

Táto kniha rozvíja jeden argument vo viacerých vrstvách. Súkromie patrí k samotnej štruktúre konania. Podporuje aj ekonomickú koordináciu, lebo chráni uvažovanie a vyjednávanie spolu so signálmi, na ktorých trhy stoja. Sledovanie preto nie je neutrálne administratívne zjednodušenie. Je to spôsob kontroly, ktorý štáty a spriaznené inštitúcie používajú na zdaňovanie, presmerovanie alebo potláčanie. Odpoveď je praktická, nielen teoretická: súkromie sa dá brániť kryptografiou, anonymnou komunikáciou, odolnými peniazmi, selektívnym odhaľovaním a decentralizovanými protokolmi. Tieto nástroje umožňujú rast paralelnej ekonomiky, ktorá čoraz menej závisí od systémov postavených na pozorovaní.[7]

Poradie knihy sleduje túto logiku. Časť II rozvíja axiómy, časť III uplatňuje ekonomické uvažovanie, časť IV skúma protivníka a časti V a VI sa obracajú k nástrojom, implementácii, inštitúciám a samotnej paralelnej ekonomike.

Kniha tiež uvádza svoje hranice.

Netvrdí, že súkromie odstráni každé nebezpečenstvo, ani že technológia robí politiku bezvýznamnou. Netvrdí ani, že paralelné inštitúcie nahradia oficiálny poriadok cez noc. Tvrdí niečo užšie a silnejšie. Súkromie je obhájiteľné v teórii. V praxi je možné. A ekonomicky účinným sa stáva, len čo ho dosť ľudí vie používať.

Kniha vymedzuje ešte jednu hranicu. Súkromie nie je samostatné vlastnícke právo popri vlastníctve vlastného tela a vlastníctve vzácnych vonkajších zdrojov. To, čomu bežná reč hovorí „súkromie“, vzniká vtedy, keď sa rešpektuje sebavlastníctvo tela, vlastnícke práva k fyzickým zariadeniam a priestorom a zmluvná dôvernosť. Tieto tri práva sú spoločným základom libertariánsko-rakúskej tradície. Locke a Rothbard ich zakladajú na sebavlastníctve a prvotnom privlastnení;[8] Hoppe na predpokladoch argumentácie;[9] Kinsella ich spresňuje kritériom vzácnosti.[10] Argument knihy o súkromí stojí na tom, v čom sa tieto pozície zhodujú. Kapitola 6 rámec rozpracúva podrobne. Drží sa neskoršieho Kinsellovho spracovania, lebo je presnejšie v tom, čo zmluva dokáže a čo nie, a zároveň ukazuje, v čom sa od neho líši Rothbardovo staršie spracovanie a ako ďaleko tie rozdiely siahajú. Kapitoly medzi nimi budujú argument za ochranu základných práv a za inžinierstvo, ktoré ich v praxi bráni.

Zhrnutie kapitoly

Súkromie je kontrola nad odhaľovaním, nie skrývanie; je to moc selektívne sa odhaliť. Táto definícia oddeľuje súkromie od dvoch susedných pojmov. Tajnosť je užšia a anonymita sa týka pripísania. Argument „nemám čo skrývať“ funguje len vtedy, keď tieto tri pojmy zlieva do jedného; keď sa udržia oddelene, stráca silu.

Súkromie je aj strategické. Pozorovanie je prvým krokom každého cieleného zásahu a zvýšenie jeho ceny naruší celý sled. Sledovanie vyžaduje infraštruktúru, analytikov a čas, kým kľúčový pár nestojí takmer nič. Práve táto asymetria, viac než akýkoľvek odkaz na práva, vysvetľuje, prečo nástroje súkromia vyvolávajú takú nevraživosť v inštitúciách postavených na sledovaní.

Zostáva základ, na ktorom tieto tvrdenia stoja. Súkromie ako štrukturálna črta konania čaká na kapitolu 3. Normatívny argument, že sledovanie je nespravodlivé, patrí do etiky argumentácie v kapitole 4 a ekonomické dôsledky pozorovanej výmeny do kapitol 7 a 9. Táto kapitola ustaľuje slovník, ktorý tieto argumenty predpokladajú.

Poznámky

[1] Eric Hughes, „A Cypherpunk's Manifesto“ (9. marca 1993), `https://www.activism.net/cypherpunk/manifesto.html`. Úvodné vyhlásenie cypherpunkového hnutia, napísané ako krátky manifest a šírené v e-mailovej konferencii cypherpunks. Hughesova pracovná definícia súkromia ako „moci selektívne sa odhaliť svetu“ dáva operačnú definíciu, ktorú táto kapitola preberá. Veta v epigrafe pomenúva štrukturálne tvrdenie: súkromie je predpokladom otvorenej spoločnosti v elektronickom veku, a nie samostatné právo, ktoré stojí proti iným spoločenským dobrám. Základné akademické spracovanie súkromia ako kontroly nad informáciami zo stredu dvadsiateho storočia pozri Alan F. Westin, *Privacy and Freedom* (New York: Atheneum, 1967). Westin ustálil štandardnú taxonómiu štyroch funkcií (samota, intimita, anonymita, zdržanlivosť) a jeho kniha je základným odkazom pre právnu a akademickú tradíciu výskumu súkromia.

[2] Základné odborné spracovanie argumentu „nemám čo skrývať“ je Daniel J. Solove, „‚I've Got Nothing to Hide' and Other Misunderstandings of Privacy,“ *San Diego Law Review* 44 (2007): 745, dostupné na `https://papers.ssrn.com/abstract=998565`. Solove zoraďuje rétorické ťahy, vďaka ktorým heslo uspieva (stotožnenie súkromia so skrývaním, stavanie súkromia ako individuálneho práva proti bezpečnosti ako kolektívnemu dobru, požadovanie konkrétnych škôd skôr, než sa súkromiu prizná postavenie), a ukazuje, prečo každý z nich zlyháva. Knižné rozpracovanie je v Solove, *Nothing to Hide: The False Tradeoff between Privacy and Security* (Yale University Press, 2011); kniha prechádza argumenty sledovacieho štátu, ktoré sa po roku 2001 stali dominantnými, a vysvetľuje, prečo odpoveď „nemám čo skrývať“ prijíma celý rámec protistrany. Vyvrátenie zo životnej skúsenosti ponúka Aleksandr Solzhenitsyn, *The Gulag Archipelago*, prel. Thomas P. Whitney (New York: Harper & Row, 1974), ktorý dokumentuje sovietsku skúsenosť, že pri dostatočne dôkladnom skúmaní zo strany štátu sa u každého jednotlivca dá nájsť niečo, čo by chcel zatajiť. Solženicynovo pozorovanie je, že obrana „nemám čo skrývať“ predpokladá dobromyseľný štát, ktorého správanie pod tlakom nie je historicky doložené.

[3] K pojmovej taxonómii súkromia pozri Westin (cit. v pozn. 1 vyššie), ktorého taxonómia štyroch funkcií a definícia založená na kontrole sú moderným východiskom. Daniel J. Solove, *Understanding Privacy* (Harvard University Press, 2008), Westinovu prácu rozširuje a analyzuje súkromie cez taxonómiu šestnástich odlišných ujmov vrátane sledovania, agregácie, identifikácie a odhalenia; je to štandardné moderné odborné spracovanie. Helen Nissenbaum, *Privacy in Context: Technology, Policy, and the Integrity of Social Life* (Stanford University Press, 2010), rozvíja rámec kontextovej integrity, ktorý vysvetľuje, prečo sa odhalenie vhodné v jednom kontexte (zdravotné informácie lekárovi) stáva porušením

v inom (tie isté informácie zamestnávateľovi). Anita L. Allen, *Unpopular Privacy: What Must We Hide?* (Oxford University Press, 2011), skúma práva na súkromie z právnofilozofického uhla a obhajuje, že niektoré nároky na súkromie patria každému bez ohľadu na preferencie toho, kto ich uplatňuje. Julie E. Cohen, „What Privacy Is For," *Harvard Law Review* 126 (2013): 1904–1933, dopĺňa, že súkromie chráni vznikajúcu subjektivitu jednotlivca pred snahou obchodných a vládnych aktérov urobiť ju pevnou, priehľadnou a predvídateľnou. K ústavnoprávnemu pôvodu americkej tradície práv na súkromie pozri nesúhlasné stanovisko Louisa D. Brandeisa vo veci *Olmstead v. United States*, 277 U.S. 438, 478 (1928), ktoré ustálilo ako štandardnú formuláciu „právo byť ponechaný o samote, najvšeobecnejšie z práv a právo, ktoré si civilizovaní ľudia cenia najviac" („the right to be let alone, the most comprehensive of rights and the right most valued by civilized men"); a Samuel D. Warren a Louis D. Brandeis, „The Right to Privacy," *Harvard Law Review* 4 (1890): 193–220, zakladajúci článok americkej judikatúry o súkromí.

[4] John Boyd rozvinul slučku OODA v sérii vojenských brífingov, najmä „Patterns of Conflict" a „The Strategic Game of ? and ?"; jeho snímky sú archivované v projekte Defense and the National Interest (`https://www.projectwhitehorse.com/pdfs/boyd/patterns%20of%20conflict.pdf`). Knižné spracovanie pozri Frans P. B. Osinga, *Science, Strategy and War: The Strategic Theory of John Boyd* (Routledge, 2007), čo je štandardná akademická štúdia Boydovho diela, ktorá sleduje slučku OODA od taktiky stíhacích pilotov až po veľkú stratégiu. Chet Richards, *Certain to Win: The Strategy of John Boyd, Applied to Business* (Xlibris, 2004), je najlepšie nevojenské uplatnenie. K pôvodnému cyklu brífingov, zostavenému a vydanému, pozri Grant T. Hammond, *The Mind of War: John Boyd and American Security* (Smithsonian, 2001).

[5] Ekonomickú asymetriu medzi lacným šifrovaním a drahým útokom rozoberá Bruce Schneier, *Applied Cryptography*, 20. výročné vyd. (Wiley, 2015), a Niels Ferguson, Bruce Schneier a Tadayoshi Kohno, *Cryptography Engineering: Design Principles and Practical Applications* (Wiley, 2010). K dôsledkom pre politiku pozri Whitfield Diffie a Susan Landau, *Privacy on the Line: The Politics of Wiretapping and Encryption*, aktualizované vyd. (MIT Press, 2007), a Susan Landau, *Listening In: Cybersecurity in an Insecure Age* (Yale University Press, 2017). Základná práca o kryptografii s verejným kľúčom je Whitfield Diffie a Martin Hellman, „New Directions in Cryptography," *IEEE Transactions on Information Theory* IT-22, č. 6 (1976): 644–654, ktorá tvrdila, že asymetrická kryptografia mení ekonomiku bezpečnej komunikácie tým, že odstraňuje úzke hrdlo distribúcie kľúčov.

[6] Politickú ekonómiu štátneho a firemného sledovania rozoberá v knižnej podobe Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (PublicAffairs, 2019), ktorá chápe sledovanie ako obchodný model, ktorý ako hlavnú komoditu ťaží údaje o správaní. Carissa Véliz, *Privacy Is Power: Why and How You Should Take Back Control of Your Data* (Bantam Press, 2020), predkladá kratší populárny argument. Bruce Schneier, *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World* (Norton, 2015), mapuje technickú a politickú infraštruktúru. K historickému rámcu, na ktorom stojí výklad knihy o tom, prečo štáty hľadajú čitateľnosť, pozri James C. Scott, *Seeing Like a State: How Certain Schemes to Improve the Human Condition Have Failed* (Yale University Press, 1998), ktorý dokumentuje, že čitateľnosť je sama predpokladom štátneho zásahu a že odolné populácie využívali nepreniknuteľnosť ako politickú stratégiu. K sledovaciemu priemyslu špecifickému pre kryptomeny pozri Andy Greenberg, *Tracers in the Dark: The Global Hunt for the Crime Lords of Cryptocurrency* (Doubleday, 2022), definitívne novinárske rozprávanie o forenznej analýze blockchainu, ako ju vykonávajú firmy, ktorými sa zaoberá kapitola 20 tejto knihy.

[7] Ďalšie čítanie o súkromí ako odbore: Julia Angwin, *Dragnet Nation: A Quest for Privacy, Security, and Freedom in a World of Relentless Surveillance* (Times Books, 2014), dokumentuje praktický pokus jednej reportérky vymaniť sa zo sledovacej infraštruktúry a je užitočným doplnkom ku kapitole 23. Finn Brunton a Helen Nissenbaum, *Obfuscation: A User's Guide for Privacy and Protest* (MIT Press, 2015), zostavuje techniky pridávania šumu do signálov,

ktoré protivník chce mať čisté, a ich etiku. Glenn Greenwald, *No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State* (Metropolitan Books, 2014), zostáva najlepším rozprávaním o odhaleniach o NSA z roku 2013. Simon Singh, *The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography* (Anchor, 2000), je najprístupnejším všeobecným úvodom do dejín kryptografie. Andy Greenberg, *This Machine Kills Secrets: How WikiLeakers, Cypherpunks, and Hacktivists Aim to Free the World's Information* (Dutton, 2012), sleduje cypherpunkovú líniu, ktorú rozvíja kapitola 2.

[8] John Locke, *Two Treatises of Government*, ed. Peter Laslett (Cambridge: Cambridge University Press, 1988; pôvodne 1689), Second Treatise, kap. V–IX, `https://www.gutenberg.org/ebooks/7370`. Locke zakladá vlastnícke práva na sebavlastníctve: každý človek vlastní svoje telo, a preto vlastní aj prácu svojho tela, a zmiešaním tejto práce s nikomu nepatriacimi zdrojmi nadobúda oprávnený titul. Murray N. Rothbard tento rámec rozširuje a radikalizuje v *The Ethics of Liberty* (New York: New York University Press, 1998; pôvodne 1982), `https://mises.org/library/book/ethics-liberty`, kde tvrdí, že všetky práva sa redukujú na sebavlastníctvo a prvotné privlastnenie, že štát porušuje obe a že zmluvná dôvernosť je priamym uplatnením vlastníckych práv k vlastnej osobe a informáciám.

[9] Hans-Hermann Hoppe, *The Economics and Ethics of Private Property: Studies in Political Economy and Philosophy*, 2. vyd. (Auburn, AL: Ludwig von Mises Institute, 2006), `https://mises.org/library/book/economics-and-ethics-private-property`, najmä „The Ultimate Justification of the Private Property Ethic." Hoppeho etika argumentácie tvrdí, že samotný akt argumentovania predpokladá výlučnú kontrolu nad vlastným telom a nad zdrojmi, ktoré človek na argumentovanie používa. Každý pokus poprieť vlastnícke práva sa preto v diskurze sám vyvracia. Kapitola 4 tejto knihy tento rámec uplatňuje priamo na súkromie: schopnosť racionálneho diskurzu predpokladá schopnosť kontrolovať, čo sa partnerom v rozhovore odhaľuje.

[10] Stephan Kinsella, *Against Intellectual Property* (Auburn, AL: Ludwig von Mises Institute, 2008), `https://mises.org/library/book/against-intellectual-property`; a Kinsella, „How We Come to Own Ourselves," *Mises Daily* (7. septembra 2006), `https://mises.org/mises-daily/how-we-come-own-ourselves`. Kinsellov prínos je v tom, že zakladá vlastnícke práva výlučne na vzácnosti fyzických zdrojov: len vzácne statky môžu vyvolať skutočný spor o užívanie, a preto len vzácne statky môžu byť predmetom vlastníckych práv. Toto kritérium vzácnosti vylučuje informáciu z kategórie vlastníctva v striktnom zmysle (záver, ktorý kniha prijíma), pričom zachováva plné vlastnícke práva k fyzickým nosičom a zariadeniam, ktoré informáciu uchovávajú alebo prenášajú, čo je presne to, čo argument o súkromí vyžaduje.

2
DVE TRADÍCIE, JEDEN ZÁVER

„V kryptoanarchii nie je vláda dočasne zničená, ale natrvalo zakázaná a natrvalo zbytočná.“

Wei Dai, „b-money“ (1998)[1]

Úvod

Táto kniha spája dve tradície, ktoré sa vyvíjali nezávisle od seba, a predsa dospeli na to isté miesto.

Rakúska tradícia pristúpila k súkromiu cez logiku. Vyšla zo skutočnosti ľudského konania a došla k záverom o vlastníctve, výmene, kalkulácii a donucovaní. Cypherpunková tradícia pristúpila k súkromiu cez inžinierstvo. Vyšla z technickej možnosti bezpečnej komunikácie a postavila nástroje, vďaka ktorým môžu ľudia konať bez toho, aby žiadali o povolenie. Jedna tradícia vysvetlila, prečo na súkromí záleží; druhá ukázala, ako sa dá v praxi brániť.

Ich zhoda nie je náhodná. Obe sa museli popasovať s tým istým problémom: ako sa ľudia koordinujú, keď konajú podľa vlastných plánov a keď sa iní pokúšajú tie plány prerušiť, zdaniť, sledovať alebo riadiť. Rakúski ekonómovia sa s ním vyrovnali cez praxeológiu, cypherpunkeri cez kód. Dospeli k rovnakej odpovedi, lebo skúmali tú istú realitu z rôznych strán.

Kapitoly 3 až 5 rozvíjajú axiomatické jadro. Táto kapitola ukazuje, prečo obe tradície patria do jednej knihy a prečo ich syntéza dáva niečo silnejšie než každá línia zvlášť.

2.1 Rakúsky prístup: odvodzovanie z konania

Carl Menger a metodologický individualizmus

Rakúska škola začína konajúcim jednotlivcom. „Základy ekonómie“ (angl. *Principles of Economics*) Carla Mengera sa rozišli s historickou školou tým, že odmietli pokladať kolektívne abstrakcie za prvotné.[2] Konajú len jednotlivci. Trhy, spoločnosti a štáty sú vzory, ktoré z ich konania vznikajú.

Tento záväzok je metodologický, nie rečnícky. Ak spoločenské javy vznikajú z rozhodnutí jednotlivcov, analýza musí začať u nich. Ceny, inštitúcie aj menové usporiadania vyplývajú z konania a nech nadobudnú akúkoľvek stabilitu a rozsah, zostávajú súhrnným výsledkom mnohých samostatných rozhodnutí.

Rovnaká metodika platí pre súkromie. Ak konanie začína v osobe, začína tam aj poznanie dôležité pre konanie. Plány sa tvoria v mysliach skôr, než sa objavia v reči alebo v obchode, a preferencie nie sú verejné fakty, ktoré čakajú na zber, ale vnútorné úsudky, ktoré konajúci odhaľuje len za podmienok, ktoré si zvolí.

Menger zároveň rozpoznal spontánny poriadok. Peniaze, jazyk a trhová koordinácia nepotrebujú návrhára, ktorý by stál nad procesom. Vznikajú opakovanou interakciou a tento bod bude dôležitý neskôr, keď sa kniha dostane k paralelnej ekonomike. Ak môže poriadok vzniknúť bez centrálneho architekta, môže bez štátneho dozoru vzniknúť aj poriadok, ktorý chráni súkromie.

Ludwig von Mises a praxeológia

Mises z týchto poznatkov vytvoril metódu. Praxeológia vychádza z jednoduchého faktu, že ľudia konajú účelne. Toto tvrdenie nie je štatistické, ale je zabudované do samotného pokusu poprieť ho: kto argumentuje, že konanie nie je účelné, na obhajobu svojho tvrdenia stále používa účelné správanie.

Z tohto východiska Mises odvodil ucelené ekonomické uvažovanie bez čakania na prieskumy či laboratórne potvrdenie. Konanie znamená voľbu, preferenciu a náklady obetovanej príležitosti. Výmena znamená očakávaný zisk a kalkulácia vyžaduje zmysluplné signály. Celá stavba sa rozvíja z vnútornej logiky samotného konania.

Táto stavba má priame dôsledky pre súkromie. Uvažovanie je vnútorné skôr, než sa stane vonkajším, preferencie sú subjektívne skôr, než ich niekto pozoruje, a plány existujú skôr, než sa odhalia. Svet, v ktorom by bola každá voľba viditeľná ešte pred jej urobením, by nebol svetom slobodného konania. Bol by svetom, v ktorom môže každý plán zmariť alebo využiť ktokoľvek dosť silný na to, aby ho pozoroval.

Kapitola 3 tento argument rozvíja naplno. Tu stačí jednoduchší bod: rakúska metóda pokladá súkromie za súčasť podmienok konania, nie za voliteľný cit alebo buržoázny vkus.

Vlastníctvo a argument

Rothbard rozšíril praxeológiu do politickej teórie tým, že spojil konanie so sebavlastníctvom a vlastníctvom[16] a potom s agresiou.[3] Hoppe neskôr ukázal, že niektoré z tých istých záverov sú predpokladom už samotnej argumentácie.[17] Ich cesty sa líšia, ale cieľ sa prekrýva.

Pre túto knihu je kľúčové, že sledovanie nie je neutrálne pozorovanie. Keď štát núti k odhaleniu, prehľadáva dom, monitoruje korešpondenciu alebo zostavuje dosje zo stôp bežného života, vstupuje do oblastí, ktoré konajúci neponúkol na verejné použitie. Súkromný úsudok tak mení na predmet privlastnenia.

Rothbard to zdôvodňoval prirodzenými právami, Hoppe predpokladmi diskurzu. Kapitola 4 ide hoppeovskou cestou, lebo sa tesnejšie hodí k metóde knihy. Hoppeov argument vychádza z toho, čo človek už musí predpokladať, keď vstupuje do argumentácie a kladie nároky na iných, a nie z morálnej intuície.

Inštitucionálny dôsledok je už viditeľný. Spoločnosť postavená na konaní a výmene, ktorá je ochotná o pravidlách argumentovať, sa zle znáša so všeobecným pozorovaním. Režim, ktorý každú transakciu a každú správu, vrátane väzieb, ktoré odhaľujú, pokladá predvolene za prístupné kontrole, sa vzďaľuje od poriadku založeného na súhlase a smeruje k nadvláde.

Konkin a kontraekonómia

Samuel Edward Konkin tretí previedol rakúsku analýzu do strategickej praxe. Položil otázku, ktorej sa mnohí teoretici vyhýbajú: ak je štát parazit, čo majú robiť slobodní ľudia, kým nezmizne?

Jeho odpoveďou bola kontraekonómia[18]: budovať mimo kanálov, ktoré štát ľahko vidí a zdaňuje, obchodovať tam, kde je sledovanie slabé, používať formy peňazí, ktoré štát nemôže podľa ľubovôle zmraziť, a presúvať výrobu a výmenu do priestorov, kde sa dobrovoľný poriadok môže osvedčiť v praxi.[4]

Týmto krokom priblížil rakúsku teóriu k okraju cypherpunkovej stratégie, hoci Konkin písal v čase, keď neexistoval Bitcoin, Nostr ani moderné anonymné siete. Logika je v jeho argumente už prítomná. Ak sa štát živí viditeľnosťou, nepozorovaná výmena ho oslabuje. Ak regulácia závisí od kontrolných bodov, systémy, ktoré ich obchádzajú, uvoľňujú jeho zovretie. A ak trhy dokážu riešiť koordinačné problémy samy, slobodní ľudia nepotrebujú povolenie, aby začali budovať alternatívu.

Konkinov význam pre túto knihu spočíva práve tu. Mení rakúsku kritiku na teóriu prechodu. Posúva ju od logickej analýzy k paralelnej praxi.

Čo dodáva rakúska tradícia

Rakúska línia dodáva tri veci, ktoré zvyšok knihy rozvinie do hĺbky.

Dáva deskriptívne tvrdenie: súkromie patrí k štruktúre konania.

Dáva základ pre normatívne tvrdenie, ktoré sa rozvinie neskôr: donucovacie vniknutie do súkromných oblastí nie je mravne nevinné.

Dáva strategické tvrdenie: slobodný poriadok môže vzniknúť dobrovoľnou koordináciou bez centrálneho riadenia.

Rakúsky príspevok stačí na to, aby určil miesto súkromia v konaní, vlastníctve a výmene. Nestačí však na obranu súkromia v skutočnom svete. Na to je potrebná druhá tradícia.[5]

2.2 Cypherpunkový prístup: budovanie toho, čo teória vyžaduje

David Chaum a súkromie už v návrhu

David Chaum videl problém skôr, než väčšina sveta pochopila, o čo ide.[6] Prvé sieťové systémy už vytvárali podmienky na úplné zaznamenávanie. Chaumova odpoveď bola architektonická: nástroje, ktoré by predpoklad sledovania urobili neúčinným, bez čakania na zákonodarcov alebo súdy.

Slepé podpisy ukázali, že overiteľná digitálna platba nevyžaduje, aby vydavateľ vedel, kto token minul. Ten poznatok je väčší než samotný stavebný prvok. Zmenil podmienky debaty. Otázka už nebola, či sa dá veriť, že sa inštitúcie po zhromaždení údajov budú správať slušne. Otázka znela, či sa systém dá navrhnúť tak, aby údaje vôbec nezbieral.

To je jadro cypherpunkového postupu. Neprosme moc, aby sa sama obmedzila. Odstráňme ju.

Rovnaká logika sa v tejto knihe vráti znova a znova. Nádej je slabým základom súkromia, a preto platí vždy rovnaká disciplína: odstrániť schopnosť, ktorá by si nádej vyžadovala. Nespoliehame sa na to, že banka zostane poctivá pri histórii našich transakcií, ale používame peniaze, ktoré banka nemôže ovládať. Nedúfame, že platforma odolá cenzúre, keď príde tlak, ale používame protokoly, ktoré nevlastní žiadna platforma. Nespoliehame sa na to, že databáza zostane bezpečná po každom prelomení či súdnom príkaze na vydanie dokumentov (subpoena), ale odmietame dosje vôbec zostavovať. V každom prípade je cypherpunkový inštinkt odstrániť schopnosť pri zdroji a nespoliehať sa, že ju inštitúcia odmietne použiť.

Slobodný softvér a overiteľnosť

Cypherpunkové riešenie vyžadovalo ešte jednu podmienku: používatelia musia mať možnosť skontrolovať nástroje, ktorým dôverujú.

Význam Richarda Stallmana je tu monumentálny.[7] Softvéru, ktorý sa nedá študovať, sa v silnom zmysle nedá dôverovať. Uzavretý binárny súbor môže sľubovať súkromie a pritom tajne odosielať kľúče, zapisovať metadáta alebo zabudovať závislosti, ktoré používateľ nikdy neschválil. Otvorený kód nezaručuje bezpečnosť, ale uzavretý kód bráni nezávislému overeniu už od začiatku.

Cypherpunkové systémy žiadajú od používateľov, aby dôverovali matematike a verejnej kontrole viac než dobrej vôli inštitúcií. Táto dôvera sa zrúti, ak sa kód nedá preskúmať a udržiavať mimo kontroly jedného dodávateľa, s možnosťou vytvoriť vlastnú vetvu (fork), ak je to potrebné. Na tomto predpoklade stojí každý významný systém súkromia v modernom stacku (vrstvenom súbore technológií), vrátane Toru, Bitcoinu, Signalu a klientov protokolu Nostr.[8]

Spojenie s rakúskou analýzou je tesné. Informácia nie je vzácna a dobrovoľný poriadok vyžaduje slobodu skontrolovať to, na čom človek stojí. Skrytá kontrola v uzavretom softvéri znovu vytvára závislosť pod technickým povrchom.

Timothy May a politika anonymného obchodu

Timothy May vyslovil politické dôsledky s nezvyčajnou jasnosťou. Ak kryptografia umožní ľuďom komunikovať a prenášať hodnotu bez preukázania zákonnej identity, bežné nástroje štátu na zdaňovanie a kontrolu strácajú veľkú časť sily.[9]

May videl aj ďalší problém. Anonymný obchod dôveru neruší, mení len spôsob, akým sa musí budovať, lebo reputácia sa stáva ústrednou, keď zákonná identita prestane robiť svoju obvyklú prácu.[10] Toto pozorovanie je jedným z najdôležitejších mostov celej knihy: cypherpunkový projekt nikdy nebol len o tajnosti správ, ale aj o podmienkach ekonomickej koordinácie, keď sa identita a platby presunú mimo predvolených kanálov štátu.

Táto kniha ide za Mayom až k tej inštitucionálnej otázke. Kapitola 24 je jednou z odpovedí na problém, ktorý videl.

Eric Hughes a selektívne odhaľovanie

Eric Hughes dal hnutiu jeho najčistejšie etické zhrnutie.[11] Súkromie znamená selektívne odhaľovanie. Každá strana transakcie má vedieť len to, čo je pre túto transakciu priamo nevyhnutné. Cypherpunková línia je tu viditeľná v plnej podobe.

Disciplína spočíva v otázke, čo výmena vyžaduje, a nie v zbieraní širokých údajov o identite so sľubom, že sa neskôr zachová zdržanlivosť. Ak transakcia potrebuje dôkaz platby, treba dokázať platbu. Ak potrebuje dôkaz veku, treba dokázať vek. Ak potrebuje dôkaz kontinuity so známym kľúčom, treba dokázať túto kontinuitu. Všetko, čo presahuje skutoč-

nú informačnú potrebu, je vyťažovanie nadbytku, ktoré by mal protokol odmietnuť už v zárodku.

Hughes dodal hnutiu aj jeho riadiacu metódu: cypherpunkeri píšu kód. Argumenty sa ťažšie zvracajú, keď sú stelesnené vo fungujúcich systémoch. Súdny rozsudok možno zrušiť. Legislatívny úspech možno odvolať. Protokol so skutočnou používateľskou základňou a rozptýlenou množinou prevádzkovateľov je fakt iného druhu.

Od nezávislosti kyberpriestoru k paralelným inštitúciám

Vyhlásenie Johna Perryho Barlowa zachytilo skorý optimizmus internetu bez hraníc.[12] Neskoršie texty boli tvrdšie a disciplinovanejšie. Keď optimizmus vyhorel, zostal trvalý strategický poznatok: slobodu možno praktizovať paralelne, cez oddelené kanály komunikácie, platieb a združovania, bez čakania na konečný politický zlom.

Tu sa cypherpunková línia stretáva s Konkinovou kontraekonómiou. Anonymné správy, digitálna hotovosť, otvorené protokoly a kryptografické dôkazy fungujú ako infraštruktúra oddelenia, a nie iba ako technické novinky, ktorými sa zdajú. Umožňujú ľuďom začať budovať trhy a komunity, ktoré nekladú každú otázku cez štátne kategórie.

Smuggler a XYZ preniesli túto líniu do strategickej praxe. Kniha „Druhá ríša“ (angl. *The Second Realm*) chápe cypherpunkové nástroje ako pracovnú infraštruktúru paralelných inštitúcií: chránené digitálne kanály a opakované fyzické miesta stretnutí, k tomu sprostredkujúcich obchodníkov (proxy merchants), vďaka ktorým môže obchod prechádzať cez hranicu s menším rizikom odhalenia. V tomto zmysle je to moderná cypherpunková stratégia uplatnená na bežný život.[13]

Zrelá podoba tejto stratégie mieri na niečo ťažšie než digitálny eskapizmus a nepredstavuje si čistý presun do oddelenej kyberdomény. Mieri na fungujúce inštitúcie, ktoré existujú popri oficiálnom poriadku a čoraz menej od neho závisia.

Predchodcovia digitálnej hotovosti a cypherpunkový postup

Bezpečné a súkromné digitálne peniaze boli snom cypherpunkerov od začiatku. Pred Bitcoinom riešili časti hádanky jednu po druhej. Hashcash ukázal, ako môže výpočet uvaliť náklady.[19] B-money opísal digitálne peniaze vytvárané účastníkmi a Bit Gold posunul digitálnu vzácnosť bližšie k použiteľnému návrhu.[20] Opakovane použiteľný dôkaz práce (proof-of--work, PoW)[21] a príbuzné pokusy dopĺňali ďalšie časti mapy.[14]

Aj systémy, ktoré zlyhali, ukazujú cypherpunkový postup: postaviť, zverejniť, otestovať na realite a ponechať to, čo prežije.

Cypherpunkový postup sa od praxeológie líši, no nie je s ňou v rozpore. Cypherpunkeri odpovedajú na praktické otázky, ktoré samotná teória nerozhodne: ktoré kryptografické predpoklady vydržia útok, ktoré návrhy

sietí odolajú cenzúre v nepriateľských podmienkach a ktoré menové systémy prežijú tlak protivníka aj skutočné chyby používateľov. Takéto otázky vyžadujú kód, nielen dedukciu.

Čo dodáva cypherpunková tradícia

Cypherpunková línia dodáva tri veci.

Ukazuje, že súkromie sa dá do systémov vstavať ako vlastnosť architektúry.

Ukazuje, že overovanie sa nemôže opierať o dôveru v nepreniknuteľné inštitúcie, a preto musia byť nástroje otvorené a preskúmateľné.

Ukazuje, že cesta k slobode vedie cez nasadené systémy, nie cez samotné vyhlásenia.

Cypherpunkový príspevok stačí na vysvetlenie, ako sa dá súkromie brániť. Nestačí však na vysvetlenie, prečo súkromie patrí k štruktúre ľudskej koordinácie. Na to je naďalej potrebná rakúska línia.[15]

2.3 Nezávislá konvergencia: prečo obe dospeli na to isté miesto

Rozdielne metódy, rovnaké obmedzenia

Rakúska a cypherpunková tradícia používali rozdielne metódy, lebo čelili rôznym častiam toho istého problému.

Rakúski ekonómovia sa pýtali, čo musí platiť, ak sú konanie a výmena skutočné v podmienkach kalkulácie. Cypherpunkeri sa pýtali, čo treba postaviť, aby súkromie, zdravé peniaze a slobodná komunikácia prežili v nepriateľských podmienkach. Jedna línia išla cez dedukciu, druhá cez implementáciu.

Konvergencia je napriek tomu pozoruhodná.

Obe tradície vychádzajú z osoby, nie z kolektívnej abstrakcie. Odmietajú predstavu, že centrálny dohľad ako taký zlepšuje koordináciu. A zisťujú, že donucovanie skresľuje signály, od ktorých poriadok závisí. Obe nakoniec bránia decentralizáciu a dobrovoľnú výmenu proti neobmedzenému pozorovaniu.

Táto zhoda nevyžaduje, aby jedna tradícia prevzala závery od druhej. Silnejšie vysvetlenie je, že obe sa museli vyrovnať s tými istými obmedzeniami konania a kontroly.

Spoločné závery

Spoločné závery sa dajú povedať jednoducho.

Ľudia konajú podľa súkromných úsudkov skôr, než sa tieto úsudky stanú verejnými.

Výmena funguje lepšie, keď si strany môžu vybrať, čo odhalia.

Slobodný poriadok môže vzniknúť bez hlavného plánu.

Sledovanie a donucovanie poškodzujú proces, o ktorom tvrdia, že ho zlepšujú.

Tradícia, ktorá vychádza z konania, dospeje k súkromiu. Dospeje k nemu aj tradícia, ktorá sa snaží brániť slobodu v kóde.

Čo dodáva syntéza

Každá tradícia osamote necháva niečo nekryté.

Rakúska teória vie odvodiť súkromie z konania a ukázať, prečo zásah zhoršuje koordináciu. Sama o sebe však nevie určiť, ktoré nástroje odolávajú sledovaniu v dnešnom svete.

Cypherpunkové inžinierstvo vie postaviť komunikačné a platobné systémy, ktoré fungujú v nepriateľských podmienkach, a k nim aj identitné systémy. Samo o sebe sa však môže ekonomicky stratiť: projekty sa centralizujú, stimuly sa vychyľujú a systémy, ktoré v kóde vyzerajú elegantne, zlyhávajú, lebo ignorujú ľudskú koordináciu alebo štruktúru kapitálu.

Syntéza zapĺňa obe medzery.

Rakúska analýza zasadzuje súkromie do ľudského konania a určuje stimuly, ktoré musia systémy chrániace súkromie rešpektovať. Cypherpunková prax ukazuje, ako sa tieto systémy dajú postaviť a brániť proti skutočným protivníkom.

Táto kombinácia dáva knihe jej tvar. Kapitoly pred nami postupujú od axiómy k ekonómii, potom cez protivníka a súbor nástrojov (tool stack) až k praxi. Obe tradície sa nezhodujú len v abstraktnej rovine. Dopĺňajú sa postupne.

Zhrnutie kapitoly

Dve tradície dospeli k rovnakému záveru o súkromí z odlišných východísk. Rakúska línia začína konajúcim jednotlivcom: od Mengera cez Misesa, Rothbarda a Hoppeho po Konkina ukazuje, že konanie začína v súkromnom úsudku, že dobrovoľný poriadok môže vzniknúť bez centrálneho návrhu a že donucovacie vniknutie poškodzuje podmienky výmeny. Cypherpunková línia začína technickou možnosťou: od Chauma cez Hughesa a Maya, potom k predchodcom digitálnej hotovosti, ukazuje, že súkromie sa dá vstavať do systémov, že otvorený kód je dôležitý pre overovanie a že fungujúce nástroje môžu presunúť moc od inštitúcií postavených na pozorovaní.

Ich konvergencia je dôkazom. Používali rozdielne metódy, lebo čelili rôznym stranám tej istej reality, a každá dopĺňa to, čo druhej chýba. Rakúska analýza zakladá súkromie v konaní a pomenúva dobrovoľný poriadok, ktorý ho umožňuje. Cypherpunkové inžinierstvo ukazuje, ako sa dajú odolné systémy postaviť a udržať proti skutočným protivníkom. Kon-

kinova kontraekonómia je most: rakúska kritika premenená na program prechodu, ktorý cypherpunkeri urobili použiteľným v praxi.

Táto kapitola sleduje intelektuálny pôvod. Úplné axiomatické odvodenie sa začína v kapitole 3, normatívny argument v kapitolách 4 a 5 a posúdenie Bitcoinu, Toru, Nostru a ostatných nástrojov v častiach V a VI.

Poznámky

[1] Wei Dai, „b-money“ (November 1998), `http://www.weidai.com/bmoney.txt`. Dvojstranový návrh anonymnej digitálnej meny, ktorý Satoshi Nakamoto citoval ako odkaz [1] vo whitepaperi Bitcoinu. Daiov úvodný odsek, citovaný v epigrafe tejto kapitoly, pomenúva spojenie kryptografie s ekonomickým myslením, ktoré kapitola sleduje: infraštruktúra súkromia navrhnutá nie ako reforma politiky, ale ako trvalá architektúra výmeny. Sprievodný rétorický text, ktorý hnutie pomenoval, pozri Eric Hughes, „A Cypherpunk's Manifesto“ (1993), `https://www.activism.net/cypherpunk/manifesto.html`; z neho pochádza slogan „cypherpunkeri píšu kód“ a cituje sa z neho v celej kapitole.

[2] K Mengerovej metóde a rozchodu rakúskej školy s historickou školou pozri Carl Menger, *Principles of Economics* (1871), a Ludwig von Mises, *Human Action* (1949), najmä metodologické kapitoly.

[3] Murray N. Rothbard, *The Ethics of Liberty* (Humanities Press, 1982), rozvíja odvodenie sebavlastníctva a vlastníctva z konania a pojem agresie ako prekročenia hranice.

[4] K Hoppeho etike argumentácie pozri Hans-Hermann Hoppe, *A Theory of Socialism and Capitalism* (1989), kap. 7. K Konkinovi a kontraekonómii pozri Samuel Edward Konkin III, *New Libertarian Manifesto* (1980).

[5] Čitatelia, ktorí chcú rakúsku tradíciu preštudovať do hĺbky, by mali začať s Ludwig von Mises, *Human Action* (1949), stále najúplnejším výkladom praxeológie. Murray Rothbard, *Man, Economy, and State* (1962), Misesa rozširuje a systematizuje. Pre kratší vstup sú výborné Peter Boettke, *Living Economics* (2012), a Jesús Huerta de Soto, *The Austrian School* (2008). Carl Menger, *Principles of Economics* (1871) a *Investigations into the Method of the Social Sciences* (1883) sú pôvodné pramene. K vzťahu medzi rakúskou metódou a kryptografickými systémami konkrétne pozri Eric Voskuil, *Cryptoeconomics* (online), ktorý uplatňuje praxeológiu priamo na Bitcoin.

[6] David Chaum, „Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms,“ *Communications of the ACM* 24, č. 2 (1981): 84–88, `https://nakamotoinstitute.org/library/untraceable-electronic-mail/`, zaviedol zmiešavacie siete (mix networks); Chaum, „Blind Signatures for Untraceable Payments,“ in *Advances in Cryptology: Proceedings of Crypto '82* (Plenum, 1983), 199–203, zaviedol stavebný prvok slepého podpisu, o ktorom je v tomto oddiele reč; Chaum, „Security Without Identification: Card Computers to Make Big Brother Obsolete,“ *Communications of the ACM* 28, č. 10 (1985): 1030–1044, `https://nakamotoinstitute.org/library/security-without-identification/`, zovšeobecnil filozofiu návrhu.

[7] Richard Stallman, „The GNU Manifesto“ (1985), `https://www.gnu.org/gnu/manifesto.html`, a Free Software Foundation, `https://www.fsf.org/`. Štyri slobody sú uvedené na `https://www.gnu.org/philosophy/free-sw.html`.

[8] Hlavné stránky projektov systémov, ktoré sa v tomto odseku spomínajú a ktorým sa kniha ďalej podrobne venuje: Tor (`https://www.torproject.org`), sieť anonymného smerovania vyvinutá z Chaumovho návrhu zmiešavacej siete z roku 1981 a nasadená od roku 2004, rozoberaná v kapitole 20. Bitcoin (`https://bitcoin.org`;

whitepaper na https://bitcoin.org/bitcoin.pdf), peer-to-peer systém elektronickej hotovosti, ktorý Satoshi Nakamoto predstavil v októbri 2008 a spustil v januári 2009, rozoberaný v kapitole 18 a kapitole 19. Signal (https://signal.org), end-to-end šifrovaný komunikátor, ktorého protokol Double Ratchet je referenčným návrhom moderného zabezpečeného posielania správ, rozoberaný v kapitole 17; špecifikácia protokolu je na https://signal.org/docs/. Nostr (https://nostr.com; špecifikácie protokolu v repozitári NIP na https://github.com/nostr-protocol/nips), decentralizovaný sociálny protokol založený na verejných kľúčoch, ktorý predstavil fiatjaf v novembri 2020, rozoberaný v kapitole 21.

[9] Timothy C. May, „The Crypto Anarchist Manifesto“ (1988), https://nakamotoinstitute.org/library/crypto-anarchist-manifesto/. Podrobnejšie spracovanie trvalých digitálnych pseudonymov, anonymného obchodu a reputácie vo virtuálnych komunitách pozri May, „Crypto Anarchy and Virtual Communities“ (1994), https://nakamotoinstitute.org/library/virtual-communities/.

[10] K libertariánskemu vlastníckemu výkladu reputácie, na ktorom Mayovo pozorovanie stojí: reputácia nie je zdrojom vo vlastníckoteoretickom zmysle, lebo spočíva v tom, čo si o osobe myslia iní ľudia, a nie v nejakom zdroji, ktorý osoba vlastní. Cypherpunkové systémy reputácie (rozvinuté v kapitole 21) reputáciu nepokladajú za vlastniteľnú; podpísané osvedčenia a dôsledné správanie v čase robia empirickými signálmi, na ktorých si protistrany vytvárajú vlastné posudky. K rámcu pozri Stephan Kinsella, „Defamation as a Type of Intellectual Property,“ in Jörg Guido Hülsmann and Stephan Kinsella, eds., *A Life in Liberty: Liber Amicorum in Honor of Hans-Hermann Hoppe* (Mises Institute, 2024), a spracovanie v kapitole 6, oddiel 6.5 tejto knihy.

[11] Eric Hughes, „A Cypherpunk's Manifesto“ (March 9, 1993); úplnú citáciu a URL pozri pozn. 1 vyššie.

[12] John Perry Barlow, „A Declaration of the Independence of Cyberspace“ (February 8, 1996), https://www.eff.org/cyberspace-independence. Vyhlásenie, napísané na Svetovom ekonomickom fóre v Davose dva dni po tom, čo prezident Clinton podpísal Telecommunications Reform Act, tvrdí, že kyberpriestor tvorí samostatný spoločenský priestor mimo štátnej suverenity: „Vlády priemyselného sveta, vy unavení obri z mäsa a ocele, prichádzam z kyberpriestoru, nového domova Mysle. V mene budúcnosti žiadam vás, ktorí patríte minulosti, aby ste nás nechali na pokoji.“ Optimizmus vyhlásenia o dobrovoľnej samospráve a jeho odmietnutie územnej jurisdikcie sa ako predpovede nepotvrdili; ako výraz raného sebapochopenia hnutia a jeho ašpirácií nemá text páru.

[13] K neskoršiemu strategickému textu, ktorý vedie cypherpunkovú líniu za anonymné správy a digitálnu hotovosť až k opakovaným paralelným inštitúciám, pozri Smuggler and XYZ, *The Second Realm: Book on Strategy* (Liberty Under Attack Publications, 2018). K staršiemu jazyku autonómie, ktorý čiastočne preberá, pozri Hakim Bey, *T.A.Z.: The Temporary Autonomous Zone, Ontological Anarchy, Poetic Terrorism* (Autonomedia, 1991). Hodnota týchto prác pre túto kapitolu je genealogická a strategická, nie axiomatická.

[14] K ceste od Hashcashu a B-money k Bit Gold a Bitcoinu pozri Adam Back, „Hashcash: A Denial of Service Counter-Measure“ (2002); Wei Dai, „B-money“ (1998); Hal Finney, „RPOW – Reusable Proofs of Work“ (2004); a Nick Szabo, „Bit Gold“ (2005).

[15] Štandardným dejepisným rozprávaním o cypherpunkovej tradícii je Steven Levy, *Crypto: How the Code Rebels Beat the Government, Saving Privacy in the Digital Age* (2001). Neskoršie fázy pokrývajú Andy Greenberg, *This Machine Kills Secrets* (2012) a *Tracers in the Dark* (2022). Simon Singh, *The Code Book* (1999), približuje predigitálny kontext. Primárne pramene zahŕňajú Mayov „Crypto Anarchist Manifesto“ (1988); Hughesov „A Cypherpunk's Manifesto“ (1993); Hal Finney, „Protecting Privacy with Electronic Cash“ (1993), https://nakamotoinstitute.org/library/protecting-priva

cy-with-electronic-cash/; Phil Zimmermann, „Why I Wrote PGP“ (1991); a archívy e-mailovej konferencie Cypherpunks.

[16] Murray N. Rothbard, *Man, Economy, and State: A Treatise on Economic Principles*, Scholar's Edition (Auburn, AL: Ludwig von Mises Institute, 2009 [1962]). Rothbardovo najsystematickejšie dielo, odvodzujúce teóriu cien, teóriu kapitálu a teóriu výroby z axiómy konania. Kým *The Ethics of Liberty* zakladá vlastnícke práva na sebavlastníctve a prirodzenom práve, *Man, Economy, and State* ich zakladá na logike konania a výmeny, a tak je hlavným ekonomickým doplnkom politickej teórie citovanej v pozn. 3.

[17] Hans-Hermann Hoppe, *The Economics and Ethics of Private Property: Studies in Political Economy and Philosophy*, 2. vyd. (Auburn, AL: Ludwig von Mises Institute, 2006), https://mises.org/library/economics-and-ethics-private-property. Smerodajná zbierka Hoppeho odvodenia vlastníckych práv z etiky argumentácie a jeho uplatnení. Hoppe ukazuje, že každý, kto argumentuje proti sebavlastníctvu, už predpokladá kontrolu nad vlastným telom a schopnosťou uvažovať, aby mohol argumentovať, čo je performatívny rozpor (rozpor medzi tým, čo sa hovorí, a tým, čo sa pri hovorení robí), ktorý zakladá vlastnícke práva bez odvolávania sa na morálnu intuíciu. Kapitola o etike argumentácie (pôvodne publikovaná 1988) je tu dotlačená spolu s uplatneniami na peniaze, bankovníctvo a teóriu štátu.

[18] Samuel Edward Konkin III, *An Agorist Primer* (KoPubCo, 2008), https://kopubco.com/pdf/An_Agorist_Primer_by_SEK3.pdf. Konkinov kratší a prístupnejší úvod do kontraekonómie a agorizmu, napísaný ako sprievodca k *New Libertarian Manifesto.* Kým Manifesto predkladá strategický a filozofický argument, *An Agorist Primer* vysvetľuje ekonomickú logiku sivých a čiernych trhov ako praktického terénu, na ktorom sa dobrovoľný poriadok rozširuje na úkor štátu.

[19] Adam Back, „Hashcash – A Denial of Service Counter-Measure,“ technická správa (August 2002), http://www.hashcash.org/papers/hashcash.pdf. Backov systém dôkazu práce bol pôvodne navrhnutý na boj proti e-mailovému spamu tým, že od odosielateľov vyžadoval vynaložiť čas procesora. Satoshi Nakamoto ho citoval ako odkaz [6] vo whitepaperi Bitcoinu a nákladová funkcia Hashcashu založená na SHA-1 priamo ovplyvnila mechanizmus ťažby Bitcoinu. Back sa neskôr stal výkonným riaditeľom firmy Blockstream, spoločnosti zaoberajúcej sa infraštruktúrou Bitcoinu (https://blockstream.com).

[20] Nick Szabo, „Bit Gold“ (2005), https://nakamotoinstitute.org/library/bit-gold/. Szabov návrh decentralizovaného systému digitálnej vzácnosti využívajúceho reťazce dôkazov práce a verejné účtovné knihy predvídal architektúru Bitcoinu v niekoľkých ohľadoch, vrátane reťazenia dôkazov práce a potreby distribuovaného registra vlastníctva. Szabo vypracoval aj pojem inteligentných zmlúv; pozri „Smart Contracts“ (1994), https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html, a „The Idea of Smart Contracts“ (1997), https://nakamotoinstitute.org/library/the-idea-of-smart-contracts/.

[21] Hal Finney, „RPOW – Reusable Proofs of Work“ (August 2004), https://nakamotoinstitute.org/library/rpow/. Finneyho systém umožňoval vymeniť token hashcash za podpísaný token rovnakej hodnoty a riešil problém dvojitého míňania pre tokeny dôkazu práce cez dôveryhodný server, ktorého kód bol otvorený pre vzdialenú atestáciu. Finney bol prvou osobou po Satoshim Nakamotovi, ktorá spustila softvér Bitcoin, a prijal prvú transakciu v Bitcoine (10 BTC v bloku 170, 12. januára 2009). Bol tiež vedúcim vývojárom PGP 2.0 v PGP Corporation a jedným z technicky najschopnejších prispievateľov do e-mailovej konferencie cypherpunkerov.

ČASŤ II

FILOZOFICKÉ ZÁKLADY

3

AXIÓMA KONANIA: SÚKROMIE AKO ŠTRUKTURÁLNA VLASTNOSŤ

„Ľudské konanie je účelné správanie."

Ludwig von Mises, *Human Action: A Treatise on Economics* (1949)[1]

Úvod

Axióma konania, ktorú sformuloval Ludwig von Mises, hovorí, že ľudské konanie je účelné správanie. Mises ju nazýva samozrejmou a a priori. Čitateľ, ktorý je zvyknutý žiadať empirický test pre každé tvrdenie, sa pri týchto slovách právom zarazí a jeho pochybnosť si zaslúži odpoveď.

Niektoré tvrdenia sú zabudované už v pojmoch, z ktorých sa skladajú. „Ak je A vyšší ako B a B je vyšší ako C, potom je A vyšší ako C." Platí to, len čo pochopíme, čo znamená „vyšší ako", a nijaké terénne údaje na overenie netreba. Axióma konania robí takéto tvrdenie o účelnom správaní. Každý pokus namietať proti nej musí byť sám účelným správaním, ktorým chce niekoho presvedčiť, a tak poprenie robí presne to, čo sa snaží vyvrátiť. Nie je to rétorický trik. Podobné formulácie sa objavujú v nezávislých tradíciách: poľská prakseológia Tadeusza Kotarbińského (od neho Mises prevzal termín), konfuciánska etika účelného sebazdokonaľovania a logika performatívneho rozporu z 20. storočia smerujú k tvrdeniu rovnakého tvaru.[2] Ak sa viaceré tradície dostanú k tomu istému základu rôznymi cestami, je pravdepodobnejšie, že tento základ zachytáva niečo skutočné o konaní, než že opakuje dogmu jedinej školy.

Z axiómy odvodíme, že súkromie je štrukturálnou vlastnosťou ľudského konania. Premýšľanie prebieha vo vnútri človeka, preferencie sú sub-

jektívne a informačná asymetria medzi konajúcim a pozorovateľom patrí k samotnej štruktúre účelného správania.[8] To všetko sú opisné fakty o tom, ako konanie funguje. Či sa má súkromie chrániť, je normatívna otázka a rieši ju kapitola 4.

Tvrdenie tejto kapitoly je opisné: súkromie patrí k štruktúre konania, pretože ľudia pred odhalením navonok uvažujú a vyberajú. Nasledujúca kapitola kladie samostatnú normatívnu otázku: ak je súkromie zabudované v konaní, čo s ním smú iní ľudia spravodlivo robiť?

3.1 Axióma konania

Samozrejmé východisko

Ludwig von Mises určil základ celej ekonomickej analýzy: ľudské konanie je účelné správanie.[3] Konať znamená používať prostriedky na dosiahnutie cieľov podľa predstáv o príčinných vzťahoch. Konanie nie je holý pohyb, ale usmernené úsilie zmeniť okolnosti z menej uspokojivého stavu na uspokojivejší.

Toto tvrdenie je samozrejmé v presnom zmysle: jeho poprenie vyvracia samo seba. Kto tvrdí, že konanie nie je účelné, musí účelne zostaviť argument, účelne vybrať dôkazy a účelne nasmerovať duševné úsilie na presviedčanie. Pokus poprieť účelné správanie je sám účelným správaním, takže potvrdzuje to, čo chce poprieť. Nie je to rétorická šikovnosť, ale logická nevyhnutnosť: poprenie sa performatívne vyvracia.

Axióma konania je preto a priori, teda známa pred akoukoľvek konkrétnou skúsenosťou a nezávisle od nej. Nezískavame ju pozorovaním, ale uvedomujeme si ju úvahou o tom, čo konanie obnáša. Každá skúsenosť, ktorú môžeme mať, je sama konaním, a preto predpokladá to, čo axióma hovorí.

Čo axióma tvrdí

Axióma konania tvrdí naraz viacero vecí. Konanie smeruje k cieľom: konajúci si predstavuje želaný budúci stav a svoje správanie usmerňuje k jeho dosiahnutiu. Konanie bez účelu nie je konanie, ale reflex alebo náhoda. Konanie tiež používa prostriedky na dosiahnutie cieľov: konajúci vidí viaceré cesty k želanému výsledku a vyberá si medzi nimi. Výber predpokladá hodnotenie, teda posúdenie, ktoré prostriedky sa k ktorým cieľom hodia.

Konanie je voľba medzi alternatívami. Konať znamená vzdať sa niektorých možností v prospech iných, pretože zvolená cesta vylučuje tú nezvolenú. A napokon, konanie je vedomé správanie: konajúci si uvedomuje, čo robí a prečo. Nevedomé správanie, nech je akokoľvek zložité, nie je konaním v praxeologickom zmysle.

Čo axióma netvrdí

Rovnako dôležité je, čo axióma konania netvrdí. Netvrdí, že konanie je racionálne v nejakom vecnom zmysle. Hovorí, že konanie je účelné, nie že ciele sú múdre alebo prostriedky účinné. Konajúci môže sledovať pošetilé ciele nevhodnými metódami a stále ide o konanie. Axióma tiež netvrdí, že konajúci majú úplné informácie. Konajú v neistote a s neúplnými znalosťami. Axióma opisuje štruktúru konania, nie jeho úspech.

Axióma netvrdí ani to, že konanie možno morálne hodnotiť. Je opisná a nehovorí nič o tom, ktoré konkrétne činy sú dobré, správne alebo prípustné. Etické hodnotenie potrebuje ďalšie premisy. Napokon axióma netvrdí, že konanie by malo byť ušetrené zásahov, lebo to by bolo normatívne tvrdenie. Opisuje, ako konanie funguje, a nepredpisuje, ako sa s ním má zaobchádzať.[4]

3.2 Vnútorné premýšľanie a subjektívne hodnotenie

Premýšľanie prebieha v mysli

Konanie vyžaduje voľbu medzi alternatívami. Voľba vyžaduje premýšľanie: vážiť možnosti, uvažovať o následkoch, posudzovať kompromisy. Kde toto premýšľanie prebieha?

Prebieha v mysli konajúceho.[8] Nejde o nahodilý fakt o tom, ako sú ľudia zariadení, ale o niečo, čo patrí k samotnému významu premýšľania. Premýšľať znamená uskutočňovať vnútorné duševné procesy: predstavovať si alternatívy, odhadovať výsledky, porovnávať hodnotenia. Tieto procesy sú svojou podstatou vnútorné a odohrávajú sa v premýšľajúcom subjekte.

Vonkajší pozorovateľ sa k premýšľaniu iného priamo nedostane.[9] Môže pozorovať správanie, zaznamenávať výroky a merať telesné reakcie. Samotný duševný proces, vážanie a hodnotenie, z ktorého premýšľanie pozostáva, však zostáva vnútri premýšľajúceho. Premýšľanie je už svojou podstatou vnútorné.

Toto tvrdenie o vlastnej neprístupnosti si zaslúži preskúmanie. Možno namietnuť, že dnešná neprístupnosť je len dôsledkom dnešnej techniky a nepatrí k podstate premýšľania. Budúca neurovedná metóda by mohla čítať procesy premýšľania priamo zo stavov mozgu.[11] Súkromie premýšľania by potom bolo empiricky podmienené, a nie štrukturálne zaručené.

Prechod od fenomenologického pozorovania (premýšľanie nám zatiaľ pripadá ako vnútorné) k štrukturálnemu tvrdeniu (premýšľanie je vnútorné zo svojej podstaty) je sporný. To, čo prežívame ako súkromné premýšľanie, sa raz môže dať prečítať dostatočne pokročilým zobrazovaním mozgu. Samotnú axiómu konania by to nevyvrátilo, lebo tá sa týka účelného správania, nie jeho pozorovateľnosti. Oslabilo by to však tvrdenie,

že informačná asymetria je trvalo štrukturálna, a ukázalo by sa, že je podmienená technikou.

Pre naše účely je dôležité, že premýšľanie je v súčasnosti a v dohľadnej budúcnosti vnútorné a neprístupné. Dôsledky pre súkromie, ktoré rozvíja táto kapitola, platia pri skutočných ľudských schopnostiach. Či by to budúca technika mohla zmeniť, je empirická otázka a dnešnú analýzu sa netýka.

Subjektívne hodnotenie

Konanie smeruje k cieľom, ktoré konajúci hodnotí. Hodnota však nie je objektívna vlastnosť vecí, ale vzťah medzi hodnotiacim subjektom a hodnoteným predmetom. Ten istý predmet môžu rôzni konajúci hodnotiť odlišne, ba aj ten istý konajúci ho môže hodnotiť inak v rôznom čase. Hodnota existuje iba v samotnom akte hodnotenia.

Túto myšlienku objavil Menger a Mises ju neskôr rozvinul: hodnota je subjektívna.[5] Pochádza z hodnotiacej mysle, nie z hodnoteného predmetu. Nijaká „objektívna hodnota" nejestvuje nezávisle od niečieho hodnotenia. Ceny vznikajú zo vzájomného pôsobenia subjektívnych hodnotení a nemerajú nijaké vopred existujúce objektívne hodnoty.

Pre súkromie z toho plynú okamžité dôsledky. Hodnotenia konajúceho existujú v jeho mysli. Nijaký vonkajší pozorovateľ sa nedostane priamo k hodnotovému poradiu iného človeka. Preferencie môže odvodzovať z pozorovaných volieb, ale samotný subjektívny zážitok hodnotenia zostáva vnútorný a súkromný.

Ordinálne poradie preferencií

Preferencie sú ordinálne, nie kardinálne.[10] Konajúci zoraďujú alternatívy ako viac alebo menej preferované, nie ako veci s merateľným množstvom úžitku. Konajúci uprednostní A pred B a B pred C. Nemá „50 utilov z A, 30 z B a 20 z C".

Z ordinálnej štruktúry vyplýva, že preferencie sa nedajú sčítať medzi jednotlivcami. Neexistuje spôsob, ako poradie preferencií jedného človeka pripočítať k poradiu iného a dostať spoločné poradie. Štruktúra preferencií každého človeka je jeho vlastná a s ostatnými nesúmerateľná.

Pre súkromie z toho vyplýva priamy záver: poradie preferencií existuje iba v mysliach jednotlivcov. Nijaký vonkajší proces sa nemôže dostať k individuálnym preferenciám ani ich sčítať bez toho, aby stratil to, čím preferencie sú. Kolektívne rozhodnutia, ktoré sa vydávajú za vyjadrenie „spoločenských preferencií", sú v najlepšom prípade len metafora.

3.3 Informačná asymetria a kontrola

Štrukturálna informačná asymetria

Z predchádzajúcej analýzy vyplýva štrukturálny fakt: konajúci nevyhnutne majú informácie, ktoré pozorovatelia nemajú.[12]

Konajúci pozná svoje preferencie a plány aj hodnotenia, ktoré ich zoraďujú, kým pozorovateľ si ich môže iba odvodiť z vonkajších dôkazov. Konajúci premýšľanie prežíva priamo, pozorovatelia majú prístup len k tomu, čo sa z neho prejaví v správaní. Za bežných ľudských podmienok je táto asymetria štrukturálna: ciele a hodnotenia vznikajú vo vnútri človeka a pozorovatelia sa k nim dostávajú usudzovaním, odhalením alebo nátlakom.

Súkromie je v najzákladnejšom zmysle informačná asymetria medzi konajúcim a pozorovateľom, ktorá je zabudovaná do štruktúry konania. Súkromie existuje ako opisný fakt skôr, než sa vysloví akékoľvek normatívne tvrdenie o tom, či sa má chrániť, alebo porušovať.

Kontrola nad odhaľovaním

Konajúci, keďže má vnútorné stavy, stojí pred voľbami o odhaľovaní. Môže svoje preferencie odhaliť konaním či výrokom, môže plány zatajiť tým, že nebude komunikovať, a v príslušnom zmysle má kontrolu nad tým, ktoré informácie o jeho vnútorných stavoch sa dostanú k iným.

Táto kontrola nie je absolútna: iní môžu preferencie usudzovať z pozorovaného správania a nátlak môže odhalenie vynútiť. Základným stavom však je, že vnútorné stavy sú vnútorné: prístupné konajúcemu a neprístupné iným, okrem prípadu, keď ich konajúci odhalí alebo keď ich iní usúdia.

Selektívne odhaľovanie je to, čo mal na mysli Hughes: moc rozhodnúť, čo sa odhalí a komu.[6] Axióma konania ukazuje, že táto schopnosť je zabudovaná priamo do konania. Či sa má chrániť, alebo potlačiť, je samostatná otázka.

Sledovanie ako zvonka vnútená transparentnosť

Sledovanie sa snaží prekonať informačnú asymetriu tým, že vnútorné stavy konajúceho sprístupní pozorovateľom. Zaznamenávanie správania a monitorovanie komunikácie majú zmenšiť rozdiel medzi tým, čo konajúci vedia o sebe, a tým, čo o nich vedia pozorovatelia.

Axióma konania netvrdí, že sledovanie je zlé. Hovorí, že sledovanie sa pokúša prekonať štrukturálnu vlastnosť konania. Či sa takéto pokusy podaria, alebo či sa majú povoliť, sú empirické a normatívne otázky, ktoré presahujú samotnú axiómu.

Axióma ukazuje, že asymetria, ktorú sledovanie prekonáva, patrí k samotnému konaniu. Sledovanie sa pokúša prekonať vlastnosť, ktorá k účelnému správaniu patrí od základu.

Zhrnutie kapitoly

Ľudské konanie je účelné správanie a toto tvrdenie sa nedá dôsledne poprieť, pretože jeho poprenie je samo účelným správaním. Z axiómy vyplýva niekoľko opisných faktov. Premýšľanie je vnútorné a prebieha v mysli konajúceho skôr, než sa objaví akýkoľvek vonkajší prejav. Preferencie sú subjektívne a existujú iba v jednotlivých aktoch hodnotenia, ku ktorým sa vonkajší pozorovateľ nedostane priamo. Informačná asymetria medzi konajúcim a pozorovateľom je preto štrukturálna, nie náhodná. Súkromie je podľa tohto výkladu predovšetkým fakt o tom, ako konanie funguje.

Kapitola je opisná a tam aj končí. Netvrdí, že súkromie je nevyhnutné na to, aby konanie vôbec mohlo nastať (ľudia konajú pod sledovaním neustále), ani že jeho porušenie je zlé, ani že konajúci vlastnia svoje telá a myšlienky ako majetok. To sú normatívne tvrdenia a axióma konania ich sama uniesť nedokáže. Princíp neagresie, vlastnícke práva a morálny argument proti sledovaniu potrebujú argumentačný základ, ktorý kapitola 4 rozvíja z Hoppeho etiky argumentácie.[7]

Poznámky

[1] Ludwig von Mises, *Human Action: A Treatise on Economics*, Scholar's Edition (Auburn, AL: Ludwig von Mises Institute, 1998), 11.

[2] Tadeusz Kotarbiński rozvinul prakseológiu (angl. *praxiology*, písané s „i", na rozdiel od *praxeology*) nezávisle v Poľsku v dvadsiatych a tridsiatych rokoch 20. storočia; pozri jeho *Praxiology: An Introduction to the Sciences of Efficient Action*, trans. Olgierd Wojtasiewicz (Oxford: Pergamon Press, 1965). Mises uznal Kotarbińskeho za zdroj termínu, hoci Misesova praxeológia siaha hlbšie do štruktúry konania než Kotarbińskeho užšia teória účinného výkonu. Pokiaľ ide o konfuciánsku paralelu, *Daxue* (Veľké učenie) a *Zhongyong* (Učenie o strede) považujú účelné sebazdokonaľovanie za predpoklad ľudského správania a neokonfuciánska tradícia nadväzujúca na Zhu Xiho rozvinula „skúmanie vecí" (*gewu* □□) a „rozširovanie poznania" (*zhizhi* □□) ako štrukturálne účelné činnosti. K modernej logike performatívneho rozporu ako spôsobu argumentácie pozri Karl-Otto Apel, *Transformation der Philosophie* (Frankfurt: Suhrkamp, 1973) a literatúru o transcendentálnej pragmatike, ktorá z neho vychádza.

[3] Mises, *Human Action*, 11-29. Úvodné kapitoly rozvíjajú axiómu konania a jej bezprostredné dôsledky. Pozri tiež Murray N. Rothbard, *Man, Economy, and State*, Scholar's Edition (Auburn, AL: Ludwig von Mises Institute, 2009), 1-77, pre alternatívne podanie tých istých základov.

[4] K rozlíšeniu medzi opisnými a normatívnymi tvrdeniami v rakúskej ekonómii pozri Hans-Hermann Hoppe, *Economic Science and the Austrian Method* (Auburn, AL: Ludwig von Mises Institute, 1995), najmä diskusiu o praxeológii ako vede bez hodnotových súdov. Mises trval na tom, že ekonómia opisuje, čo je, nie čo by malo byť; etické hodnotenie vyžaduje ďalšie premisy.

[5] Carl Menger, *Principles of Economics*, trans. James Dingwall and Bert F. Hoselitz (Auburn, AL: Ludwig von Mises Institute, 2007 [1871]), 114-174. Mengerova subjektívna teória hodnoty spôsobila v ekonómii prevrat tým, že hodnotu umiestnila do hodnotiacej mysle, nie do objektívnych vlastností statkov.

[6] Eric Hughes, „A Cypherpunk's Manifesto" (March 9, 1993), https://www.activism.net/cypherpunk/manifesto.html. Formulácia „selektívne sa odhaliť" je pracovná definícia, ktorú táto kniha preberá; pozri kapitolu 1, poznámku 1, kde je úplnejší citačný kontext.

[7] Odvodenie sebavlastníctva a vlastníckych práv z etiky argumentácie je rozpracované v Hans-Hermann Hoppe, *A Theory of Socialism and Capitalism: Economics, Politics, and Ethics* (Boston: Kluwer Academic Publishers, 1989), kap. 7, a ďalej rozvinuté v Hoppe, *The Economics and Ethics of Private Property* (Auburn, AL: Ludwig von Mises Institute, 2006); kapitola 4 tejto knihy toto odvodenie uplatňuje na súkromie. K širšej praxeologickej literatúre sú hlavnými rakúskymi zdrojmi (v poradí rastúcej náročnosti) Ludwig von Mises, *Human Action: A Treatise on Economics*, Scholar's Edition (Mises Institute, 1998; pôvodne 1949), úplné spracovanie, pričom kapitoly I–VII sa venujú axióme a jej odvodeniam; Murray N. Rothbard, *Man, Economy, and State*, Scholar's Edition (Mises Institute, 2009; pôvodne 1962), časť 1, ktorá podáva systematickejšie odvodenie od axiómy až po úplnú ekonomickú teóriu; a Hans-Hermann Hoppe, *Economic Science and the Austrian Method* (Mises Institute, 1995), https://mises.org/library/economic-science-and-austrian-method, najstručnejšia dôsledná obrana epistemologického postavenia praxeológie proti empiristickým a popperovským kritikom. Kratšie vstupné body ponúkajú Peter Boettke, *Living Economics: Yesterday, Today, and Tomorrow* (Independent Institute, 2012) a Jesús Huerta de Soto, *The Austrian School: Market Order and Entrepreneurial Creativity* (Edward Elgar, 2008). K poznaniu a priori a jeho úlohe v teórii konania Barry Smith, „In Defense of Extreme (Fallibilistic) Apriorism," *Journal of Libertarian Studies* 12, no. 1 (1996): 179–192, vstupuje do polemiky s popperovskou námietkou. Nerakúske paralely, ktoré stojí za to čítať popri Misesovi, sú Ludwig Wittgenstein, *Philosophical Investigations* (1953), o účelnom správaní a dodržiavaní pravidiel, a G. E. M. Anscombe, *Intention* (Basil Blackwell, 1957), o filozofii konania. Z kritickej literatúry zhromaždili Walter Block, Frank Arbas a Jay Chang hlavné námietky a odpovede v *Journal of Libertarian Studies* a *Quarterly Journal of Austrian Economics* za niekoľko desaťročí; Jörg Guido Hülsmann, ed., *The Last Knight of Liberalism: An Intellectual Biography of Ludwig von Mises* (Mises Institute, 2007), zasadzuje axiomatickú metódu do historického kontextu.

[8] F. A. Hayek, „The Use of Knowledge in Society," *American Economic Review* 35, no. 4 (September 1945): 519–530, https://www.econlib.org/library/Essays/hykKnw.html. Hayekova najcitovanejšia esej tvrdí, že znalosti dôležité pre ekonomickú koordináciu sú rozptýlené medzi milióny jednotlivcov a žiadny centrálny plánovač ich nemôže zhromaždiť bez straty. Esej zakladá epistemický argument pre trhy ako procesy objavovania a opiera o ňu tvrdenie, že informačná asymetria medzi konajúcimi a pozorovateľmi nie je technický nedostatok, ale trvalá štrukturálna vlastnosť spoločenskej skutočnosti. Súvislosť s argumentom tejto kapitoly je priama: to, čo Hayek označuje ako problém znalostí na spoločenskej úrovni – žiadny pozorovateľ nemôže mať to, čo jednotliví konajúci vedia o vlastných preferenciách, plánoch a miestnych okolnostiach – je tá istá asymetria, ktorú axióma konania pomenúva na úrovni jednotlivca.

[9] Gilbert Ryle, *The Concept of Mind* (London: Hutchinson, 1949), najmä kapitola 2, „Knowing How and Knowing That." Rylovo rozlíšenie medzi výrokovým poznaním (vedieť, že) a praktickým poznaním (vedieť, ako) zodpovedá priepasti medzi premýšľaním a správaním: pozorovateľ môže vedieť, že konajúci vykonal čin, a pritom nevedieť nič o vnútornom procese premýšľania – o vážení cieľov a prostriedkov – ktorý z tohto činu urobil účelné konanie. Rylova kritika toho, čo nazval „duchom v stroji", sa týka aj

neurovednej námietky z oddielu 3.2: behaviorálne pozorovanie dosahuje výstupy, nie hodnotiacu štruktúru, ktorá ich vytvorila.

[10] Murray N. Rothbard, *Man, Economy, and State*, Scholar's Edition (Auburn, AL: Ludwig von Mises Institute, 2009 [1962]), 1–30. Rothbardova úvodná kapitola odvodzuje ordinálnu štruktúru poradia preferencií z axiómy konania s väčšou formálnou presnosťou než Misesovo pôvodné spracovanie. Kľúčový argument: keďže konanie spočíva vo voľbe medzi zoradenými alternatívami, preferencie sa odhaľujú voľbou, nie introspekciou či prieskumom; kardinálne miery úžitku („50 utilov") predpokladajú medziosobné porovnávanie, ktoré nemá základ v logike konania. Pozri tiež Murray N. Rothbard, „Toward a Reconstruction of Utility and Welfare Economics," in *On Freedom and Free Enterprise*, ed. Mary Sennholz (Van Nostrand, 1956), pre úplnú kritiku kardinálnej a blahobytovej ekonómie.

[11] Neurovedné dekódovanie duševných stavov je aktívna oblasť výskumu. Reprezentatívne práce o „čítaní mozgu" pomocou fMRI a o hraniciach usudzovania intencionálneho obsahu z neurónových signálov pozri John-Dylan Haynes, „A Primer on Pattern-Based Approaches to fMRI: Principles, Pitfalls, and Perspectives," *Neuron* 87, no. 2 (2015): 257–270; a Poldrack et al., „Inferring Mental States from Neuroimaging Data: From Reverse Inference to Large-Scale Decoding," *Neuron* 72, no. 5 (2011): 692–700. Filozofické hranice prechodu od neurónových korelátov k intencionálnemu obsahu – priepasť medzi stavmi mozgu a *významom* premýšľania – rozoberá Ned Block, „On a Confusion about a Function of Consciousness," *Behavioral and Brain Sciences* 18, no. 2 (1995): 227–247. Aj úplné neurónové čítanie by narazilo na problém rámca: určiť intencionálny predmet stavu premýšľania vyžaduje vykladať neurónové vzory na pozadí presvedčení a cieľov, ktoré samy nie sú priamo pozorovateľné.

[12] Israel M. Kirzner, *Competition and Entrepreneurship* (Chicago: University of Chicago Press, 1973), najmä kapitola 2. Kirznerova teória podnikania sa zameriava na ostražitosť, ktorá konajúcim umožňuje všimnúť si ziskové príležitosti, ktoré si iní zatiaľ nevšimli – ide o znalosť, ktorá je prediskurzívna, nedá sa vyjadriť ako súbor tvrdení, a preto je štrukturálne neprístupná každému vonkajšiemu pozorovateľovi, kým sa podľa nej nekoná. Dôsledok pre informačnú asymetriu: ekonomicky najdôležitejšie znalosti, ktoré konajúci majú, sú práve tie, ktoré nevedia úplne opísať, ani keby sa snažili, pretože spočívajú vo vnímaní toho, čo iní prehliadli. Pozri tiež Kirzner, *The Meaning of Market Process* (London: Routledge, 1992), o súvislosti medzi subjektívnym poznaním, podnikateľským objavovaním a hranicami centrálnej koordinácie.

4

AXIÓMA ARGUMENTÁCIE A SEBAVLASTNÍCTVO

> *„Každé tvrdenie musí mať navrhovateľa a jeho právo predložiť návrh sa musí predpokladať."*
>
> Hans-Hermann Hoppe, *A Theory of Socialism and Capitalism* (1988)[1]

Úvod

Táto kapitola je normatívna. Predkladá argument pre etické závery.

Kapitola 3 stanovila opisné fakty: súkromie je štrukturálnou vlastnosťou ľudského konania. Samotný opis však ešte nedáva predpis. Z toho, že konanie má určitú štruktúru, sa nedá usúdiť, čo s ním máme robiť.

Táto kapitola rozvíja normatívne zdôvodnenie. Hans-Hermann Hoppe tvrdí, že argumentovanie predpokladá určité podmienky a že ich popieranie počas argumentovania vytvára performatívny rozpor. Z toho Hoppe odvodzuje sebavlastníctvo, vlastnícke práva a princíp neagresie (non-aggression principle, NAP).[1717]

O tomto argumente sa diskutuje takmer štyri desaťročia. Filozofi vzniesli námietky a Hoppe so svojimi obhajcami na ne odpovedali. Kapitola predstavuje argument a skúma hlavné námietky, ktorým čelil. Problém *is–ought*, ktorý trápi filozofiu od čias scholastikov, dostáva prepracované riešenie: argument neodvodzuje má byť z je, ale ukazuje, že určité normatívne tvrdenia sa v racionálnom diskurze nedajú dôsledne poprieť.

Kapitola stojí na troch samostatných otázkach: čo argumentovanie predpokladá, kým prebieha, prečo popretie týchto predpokladov vyvracia samo seba a ako ďaleko táto logika siaha, keď sa argument presunie od kon-

troly nad telom a mysľou ku kontrole nad vonkajšími zdrojmi. Práve tretia otázka je miesto, kde väčšina čitateľov prvýkrát pocíti tlak argumentu.

4.1 Argument: performatívny rozpor

Pôvod v diskurzívnej etike

Hoppeho etika argumentácie čerpá z diela Jürgena Habermasa a Karla-Otta Apela, ktorí rozvinuli diskurzívnu etiku v tradícii transcendentálnej pragmatiky.[2] Obaja sa snažili určiť predpoklady racionálneho diskurzu, teda podmienky, ktoré musia byť splnené, aby zmysluplná argumentácia mohla prebehnúť.

Habermas s Apelom tvrdili, že určité normy sú obsiahnuté v samotnom akte argumentovania. Ak sú tieto normy pre argumentovanie nevyhnutné, ich popieranie počas argumentovania vytvára to, čo nazvali performatívnym rozporom: poprenie podkopáva samotný akt popierania.

Hoppe túto metodologickú cestu prijal, ale odmietol závery Habermasa a Apela o tom, ktoré normy diskurz predpokladá. Kým oni odvodili sociálnodemokratické politiky, Hoppe odvodil sebavlastníctvo, súkromné vlastníctvo a libertariánsku etiku. Metóda je spoločná, závery sa líšia.

Štruktúra argumentu

Hoppeho argument postupuje takto:

Premisa 1: Argumentujeme. Argument platí iba v tomto kontexte; ak neargumentujeme, neplatí.

Premisa 2: Argumentovanie je osobitná forma konania s osobitnými predpokladmi. Nie každé konanie je argumentovanie, ale každé argumentovanie je konanie.

Premisa 3: Kto argumentuje, musí mať výlučnú kontrolu nad svojím telom. Bez tela, ktorým človek vytvára zvuky, gestá alebo písmo, nemožno argumentovať. Ak by človek počas argumentovania nemal kontrolu nad vlastným telom, nemohol by formulovať, vyjadriť ani obhajovať svoje stanovisko.

Premisa 4: Kto argumentuje, musí mať výlučnú kontrolu nad svojou mysľou. Argumentovanie vyžaduje formulovať myšlienky a vážiť dôkazy voči konkurenčným tvrdeniam. Ak by duševné procesy človeka riadil niekto iný, nemohol by skutočne argumentovať.

Záver 1: Kto argumentuje, tým implicitne predpokladá výlučnú kontrolu nad telom a mysľou. Sebavlastníctvo znamená presne toto: výlučnú kontrolu nad vlastnou osobou.

Premisa 5: Poprieť sebavlastníctvo počas argumentovania je performatívny rozpor. Ten, kto ho popiera, musí na formulovanie a vyjadrenie poprenia využiť výlučnú kontrolu nad vlastným telom a mysľou. Akt popierania predpokladá to, čo poprenie odmieta.

Záver 2: Sebavlastníctvo sa v argumentácii nedá dôsledne poprieť. Každý pokus o jeho popretie ho potvrdzuje.

Rozšírenie na vlastnícke práva

Sebavlastníctvo pokrýva telo a myseľ počas samotného diskurzu. Ťažšia otázka je, či argumentovanie predpokladá aj pravidlá pre vzácne zdroje mimo tela, pretože diskurz sa niekde odohráva a niečo používa. Hoppe argument rozširuje zo sebavlastníctva na vonkajšie vlastníctvo:

Premisa 6: Argumentovanie sa odohráva v čase a priestore. Ľudia, ktorí argumentujú, zaberajú miesto a po celý čas diskurzu využívajú zdroje.

Premisa 7: Kto argumentuje, musí mať prístup k fyzickým zdrojom, minimálne k miestu, na ktorom stojí.

Premisa 8: Keby sa zdroje mohli argumentujúcim počas diskurzu odobrať, argumentovanie by sa nemohlo spoľahlivo odohrávať.

Premisa 9: Princíp, ktorý argumentovanie chráni najlepšie, je prvotné privlastnenie: prvý užívateľ ničej veci si vlastnícke práva založí tým, že s ňou zmieša svoju prácu.[16][16]

Záver 3: Vlastnícke práva sú predpokladom argumentovania. Poprieť vlastnícke práva a pritom z nich pri argumentovaní ťažiť je performatívny rozpor.

Princíp neagresie

Zo sebavlastníctva a vlastníckych práv vyplýva princíp neagresie[15]:

Ak jednotlivci vlastnia seba a svoj oprávnene nadobudnutý majetok, potom nevyžiadaný zásah do osoby alebo majetku porušuje vlastnícke práva. Takýto zásah je agresia. NAP hovorí, že začať takúto agresiu je nelegitímne; sila je opodstatnená iba ako odpoveď na predchádzajúcu agresiu.

NAP teda stojí na Hoppeho etike argumentácie, nie na samotnej axióme konania. Kapitola 3 nemohla NAP odvodiť, pretože bola čisto opisná. Normatívny základ prichádza až tu.

4.2 Námietky a odpovede

Hoppeho argument čelil značnej kritike. Najsilnejšie námietky a odpovede na ne preskúmame postupne.

Medzera medzi užívaním a vlastníctvom (Murphy a Callahan)

Robert Murphy a Gene Callahan vzniesli námietku, ktorú mnohí pokladajú za najvážnejšiu: Hoppeho argument preukazuje najviac to, že ľudia, ktorí argumentujú, môžu počas diskurzu užívať svoje telo, nie že ho vlastnia.[3]

Námietka znie: „Niekto môže poprieť libertariánsku etiku a pritom svojim protivníkom priznať užívanie ich tiel na debatu. Nie je na tom nič rozporné.“

Socialista môže napríklad povedať: „Pripúšťam, že na túto debatu môžete užívať svoje telo. Po jej skončení však budú majetkové usporiadania určené kolektívne.“ Toto stanovisko priznáva dočasné užívanie bez toho, aby uznalo trvalé vlastníctvo.

Murphy a Callahan ďalej tvrdia, že aj keby sa sebavlastníctvo preukázalo, Hoppeho argument platí len pre tie časti tela, ktoré sa pri argumentovaní používajú: „Hoppe v najlepšom prípade dokázal, že by bolo rozporné tvrdiť, že niekto právom nevlastní svoje ústa, uši, oči, srdce, mozog a všetky ostatné časti tela podstatné pre účasť na debate.“

Na túto námietku odpovedalo viacero autorov.[4] Walter Block tvrdí, že rozlišovanie medzi užívaním a vlastníctvom je v tomto kontexte umelé: kto má výlučné užívanie dostatočné na argumentovanie, má podstatný obsah vlastníctva. Socialista, ktorý povie „pripúšťam, že na túto debatu môžete užívať svoje telo, ale potom budú majetkové usporiadania určené kolektívne“, sa rozporu nezbavil. Samotný návrh totiž predpokladá, že jeho telo a myseľ sú jeho, aby ich pri návrhu použil, že jeho slová sú jeho a že jeho miesto v argumente je jeho, aby ho obhajoval. Rámec „dočasného dovolenia“ prepašúva vlastníctvo dovnútra pod iným názvom.

Frank van Dun vysvetľuje, čo sa stane, keď niekto odmietne tieto predpoklady uznať: postaví sa mimo spoločenstva racionálneho diskurzu.[5] Takýto človek etiku argumentácie „nevyvrátil“, ale odmietol argumentovať vôbec. Stáva sa tým, čo van Dun nazýva „vyhnancom“ v pôvodnom zmysle slova, teda tým, kto sa postavil mimo rámca, ktorý umožňuje rozumné riešenie sporov. Argument netvrdí, že takíchto ľudí niet. Ukazuje, že nemôžu dôsledne žiadať ochranu, ktorú upierajú iným.

Hatim Kheir ponúka ďalšie preformulovanie, ktoré argument posilňuje.[6] Keď sa strany rozhodnú riešiť spor arbitrážou, implicitne prijmú rámec, ktorý presahuje bezprostrednú držbu. Arbitráž vyžaduje, aby rozhodca rozhodoval podľa objektívnych skutočností a objektívnych zásad, nie podľa osobného záujmu. Samotné predloženie sporu neutrálnej tretej strane predpokladá, že nároky sa dajú zdôvodniť intersubjektívne overiteľnými meradlami. Kheir tvrdí, že tieto meradlá nevyhnutne zahŕňajú nadobudnutie prvým užívateľom a trvalé vlastníctvo: keby nároky na majetok zanikli vždy, keď sa držba preruší, arbitráž väčšiny reálnych sporov by bola nemožná. Štruktúra arbitráže teda predpokladá vlastníctvo, nielen užívanie.

Kheirov argument nijako „neposúva základy“. Ukazuje skôr odolnosť etiky argumentácie: či sa začne argumentovaním vo všeobecnosti, alebo konkrétne arbitrážou, vyplývajú rovnaké závery. Logika racionálneho diskurzu v ktorejkoľvek jeho podobe predpokladá majetkové normy, ktoré taký diskurz umožňujú.

Námietka čiastočného uplatnenia

S predchádzajúcim súvisí aj toto: aj keby Hoppeho argument preukázal určité sebavlastníctvo, platí len počas argumentovania. Čo keď ľudia neargumentujú?

Totalitár môže povedať: „Počas tejto debaty máte sebavlastníctvo. Keď debatu skončíme, platia iné pravidlá." Hoppeho argument, ktorý sa týka argumentovania, akoby nemal čo povedať o kontextoch, v ktorých sa neargumentuje.

Odpoveď je, že zásady, ktoré sa odhalia argumentovaním, musia byť univerzalizovateľné, aby vôbec fungovali ako zásady.[7] Argumentovanie je činnosť, pri ktorej sa uvádzajú dôvody na tvrdenia a hľadá sa vzájomné porozumenie racionálnou výmenou. Keď niekto navrhne inej osobe normu ako záväznú pre oboch, musí byť univerzalizovateľná, aby bola prijateľná. Partikularistická norma („smiem ti urobiť X, ale ty mne nesmieš") nedáva druhej strane nijaký dôvod, ktorý by mohla prijať.

Požiadavka univerzalizovateľnosti nie je ľubovoľný predpoklad, ale konštitutívna črta argumentovania. Kto predkladá iba partikularistické nároky, neargumentuje, ale len prejavuje moc. Povedať „sebavlastníctvo platí počas argumentovania, ale potom už nie" znamená navrhnúť partikularistickú normu: hovoriaci si dáva právo pozastaviť cudzie sebavlastníctvo, keď sa mu to hodí, a vlastné si pravdepodobne ponecháva. Druhej strane to nedáva nijaký dôvod, ktorý by mohla prijať, a preto to nemožno považovať za argumentovanie.

Rozdiel medzi argumentovaním a holým tvrdením je to, čo racionálny diskurz umožňuje. Ak sa niekto univerzalizovateľnosti vzdá, môže vyhlásiť akúkoľvek normu tým, že vymyslí partikularistickú výnimku. Bez univerzalizovateľnosti sa rozumný diskurz o normách rozpadne na tvrdenie a protitvrdenie, čo je presne to, čo argumentovanie existuje na prekonanie. Totalitár, ktorý hovorí „po debate platia iné pravidlá", nepredložil argument, ale vyhlásenie o zamýšľanom násilí.

Zamieňanie kontroly a vlastníctva

Iná námietka: Hoppe prechádza od opisného faktu, že ľudia, ktorí argumentujú, ovládajú svoje telá, k normatívnemu tvrdeniu, že majú mať výlučnú kontrolu. Tým zamieňa je a má byť.

Námietka znie: „To, že niekto dokáže ovládať seba, ešte nevysvetľuje, prečo by sa mal niekto iný zdržať fyzického zasahovania do tejto kontroly."

Táto námietka nechápe štruktúru argumentu. Hoppe netvrdí: „Svoje telo ovládate, a preto ho vlastníte." Tvrdí: „Pri argumentovaní nemôžete dôsledne poprieť sebavlastníctvo, pretože poprenie predpokladá to, čo popiera." Má byť nevstupuje odvodením z je, ale cez požiadavky bezrozpornej racionálnej výmeny.

Predstavme si, že niekto argumentuje: „Nemáte právo ovládať svoje telo.“ Musí na tento argument použiť vlastné telo. Musí predpokladať, že má právo formulovať myšlienky, hýbať hlasivkami, gestikulovať alebo písať. Predpokladá, že jeho argument je jeho, aby ho predniesol. Performatívny rozpor nespočíva v tom, že kontrola existuje, ale v tom, že ten, kto popiera, musí vykonávať práva, ktoré popiera, aby ich mohol popierať.

Stephan Kinsella ponúka doplňujúcu obranu cez princíp estoppelu (zákaz protirečiť vlastnému konaniu).[8] Agresor, ktorý namieta proti obrannej sile, musí tvrdiť, že sila je neprípustná. Lenže tým, že spáchal agresiu, svojím konaním ukázal, že sila je prípustná. Je preto zbavený práva namietať: aby namietal, musel by protirečiť zásade obsiahnutej vo vlastnom konaní. Nejde o odvodzovanie má byť z je, ale o ukázanie, že určité stanoviská sa nedajú dôsledne zastávať.

Námietka o poradí odvodzovania

Samostatná a vážna námietka hovorí, že hoppeovský argument má poradie odvodzovania opačné. Tradícia Locka a Rothbarda začína vlastníctvom: sebavlastníctvo je prvý fakt, prvotné privlastnenie ho rozširuje na vonkajšie zdroje a princíp neagresie je dôsledok, že agresia proti majetku je neprípustná. V tomto poradí je vlastníctvo základné a prvotné; NAP závisí od definície vlastníctva, ktorá sa stanoví najprv. Hoppeho argument akoby to obracal: základom je argumentovanie, sebavlastníctvo sa odvodzuje z toho, čo argumentovanie predpokladá, a z neho sa potom odvodzuje vlastníctvo vonkajších zdrojov. Námietka znie, že definovať vlastníctvo odkazom na predpoklady argumentovania je ten istý kruh v inom šate: NAP stále nakoniec závisí od vlastníctva, ale vlastníctvo teraz závisí od argumentovania, ktoré je samo formou konania predpokladajúcou vlastníctvo vlastného tela. Reťaz musí niekde začať a začať ju pri argumentovaní nie je o nič menej ľubovoľné než začať ju priamo pri vlastníctve.

Odpoveď je, že obe poradia odvodzovania dospejú k rovnakým záverom rôznymi cestami. Poradie Locka a Rothbarda berie sebavlastníctvo ako východiskový mravný fakt a uvažuje smerom von. Hoppeovské poradie berie argumentovanie ako metodologicky privilegovaný kontext (pretože sa v ňom odohráva každý spor o normách) a usudzuje, že predpoklady argumentovania sa v ňom dôsledne poprieť nedajú. Ani jedno poradie nie je logicky vynútené; obe sú metodologickou voľbou, odkiaľ začať.

Hoppeovské poradie má jednu výhodu a jedno obmedzenie. Výhodou je, že priamo odpovedá na Humeovu výzvu is–ought: neodvodzuje má byť z je, ukazuje, že určité normatívne tvrdenia sa v argumentovaní nedajú dôsledne tvrdiť, čo je iný ťah a poradie Locka a Rothbarda ho neurobí tak čisto. Obmedzením je, že voči partnerovi, ktorý argumentovať odmietne, nemá čím zaúčinkovať. Poradie Locka a Rothbarda má opačný profil: voči

mlčiacemu agresorovi niečo zmôže (porušil vlastníctvo, bodka), ale na Huma priamo neodpovedá.

Táto kniha sa drží hoppeovského poradia, pretože argument o súkromí z neho ťaží. Kognitívne súkromie a kontrola nad vlastným vyjadrovaním sú predpoklady argumentovania a zakladať ich ochranu na tom, čo argumentovanie vyžaduje, je priamejšie než zakladať ju na vlastníctve odvodenom z osobitnej axiómy sebavlastníctva. Obe poradia dávajú rovnaké praktické závery: sebavlastníctvo tela a mysle, prvotné privlastnenie vonkajších zdrojov, NAP a ochranu pred vynúteným odhalením, ktorú kniha obhajuje. Čitateľ, ktorý uprednostňuje poradie Locka a Rothbarda, príde na to isté miesto inou cestou a ďalšie kapitoly nevyžadujú, aby si vyberal.

Námietky proti rozšíreniu na vlastníctvo

Aj ak prijmeme sebavlastníctvo, rozšírenie na vonkajšie vlastníctvo je samostatne sporné. Prečo musia ľudia, ktorí argumentujú, mať súkromné vlastníctvo vonkajších zdrojov? Prečo nie spoločné vlastníctvo s pravidlami prístupu?

Hoppe tvrdí, že režimy spoločného vlastníctva sa nedajú univerzalizovať bez rozporu. Ak má každý rovnaký prístup ku všetkým zdrojom, spory o užívanie sú nevyhnutné. Dvaja ľudia nemôžu zaberať rovnaké miesto ani naraz používať ten istý nástroj. Je potrebný nejaký mechanizmus riešenia.

Otázka teda znie, aký mechanizmus riešenia sa dá zdôvodniť argumentovaním. Každý navrhnutý mechanizmus musí byť vyjadriteľný ako univerzalizovateľná zásada. „Prvé privlastnenie zakladá práva“ je takou zásadou: platí pre všetkých rovnako, dáva jasné riešenie sporov a nepredpokladá žiadne predchádzajúce nároky na majetok. „Rozhoduje kolektív“ ňou nie je: predpokladá, že niekto má právo hovoriť za „kolektív“, že hranice kolektívu sú vymedzené a že existuje mechanizmus kolektívneho rozhodovania. Každý z týchto predpokladov na svoje vyriešenie potrebuje predchádzajúce majetkové normy.

Kto argumentuje za spoločné vlastníctvo, musí zaujímať miesto, z ktorého argumentuje. Musí mať prístup k zdrojom (miesto, kde stojí, vzduch na dýchanie, prostriedok komunikácie), ktoré iní nemôžu súčasne využívať rovnakým spôsobom. Zástanca spoločného vlastníctva si už privlastnil zdroje potrebné na jeho argument. Ak potom popiera, že privlastnenie zakladá práva, popiera legitimitu aktu, ktorým popiera.

Ľavicovo-libertariánske alternatívy, ktoré prijímajú sebavlastníctvo, ale odmietajú silné vlastnícke práva, narážajú na ďalšiu ťažkosť: musia vysvetliť, ako sa dá sebavlastníctvo uplatňovať bez vlastníctva vonkajších zdrojov. Konať znamená používať priestor a materiály. Ak podliehajú kolektívnemu vetu, sebavlastníctvo je len formálne, nie skutočné.

4.3 Otázka is--ought

Problém

David Hume si všimol, že mnohé argumenty neoprávnene prechádzajú od výrokov o tom, čo je, k záverom o tom, čo má byť.[9] Opisné premisy samy osebe nemôžu priniesť normatívne závery: je to priepasť is–ought.

Preklenuje Hoppeho argument túto priepasť, alebo sa dopúšťa Humeovho omylu?

Hoppeho riešenie

Hoppeho argument neodvodzuje má byť z je tak, ako to Hume kritizoval. Jeho štruktúra je:[10]

1. Argumentovanie predpokladá vlastníctvo vlastného tela a prvotné privlastnenie (homesteading). (Opisné tvrdenie o predpokladoch)
2. Preto sa žiadna odchýlka od tejto etiky nedá argumentačne obhájiť. (Záver o tom, čo sa dá obhájiť)

Argument nehovorí: „Veci sú takéto, a preto majú takéto byť.“ Hovorí: „Kto vstúpi do oblasti rozumného diskurzu, tým aktom už predpokladal normy, ktoré diskurz umožňujú.“ Má byť nevzniká z je, ale z požiadaviek bezrozporného racionálneho dorozumievania.

Murray Rothbard rozpoznal význam tohto ťahu, keď o Hoppem napísal, že „prekonal slávnu dichotómiu is/ought, fakt/hodnota“.[11]

Zvyšné námietky

Kritici tvrdia, že aj keď sa určité tvrdenia nedajú poprieť bez rozporu, preukazuje to len obmedzenie toho, čo sa dá argumentovať, nie to, čo je pravda. To, že nemôžem dôsledne poprieť X, kým argumentujem, nedokazuje, že X je pravda, len že ho nemôžem dôsledne poprieť.

Táto námietka nechápe oblasť etických tvrdení. Etika sa týka toho, ako sa majú racionálne bytosti správať jedna k druhej. Ak sa navrhnutá etická norma nedá vysloviť bez rozporu, je to dôkaz, že norma ako norma zlyháva, a nie nepríjemnosť len pre navrhovateľa. „Norma“, ktorú sa nedá dôsledne obhajovať, nie je normou, ktorú by niekto mohol nasledovať alebo odporúčať. Kritérium bezrozporného vyslovenia nie je ľubovoľné, ale patrí k podstate toho, čo znamená normu vôbec navrhnúť.

Námietka, že etika by mohla byť „celkom o niečom inom“ (o následkoch, cnostiach, božích príkazoch), tejto analýze neujde. Každý alternatívny etický rámec sa musí dať argumentovať. Konzekvencionalista, ktorý hovorí „maximalizujte úžitok“, musí na svoj argument predpokladať sebavlastníctvo; etik cnosti, ktorý hovorí „pestujte dokonalosť“, musí predpokladať právo pestovať; teoretik božích príkazov, ktorý hovorí „poslúchajte

Boha“, musí predpokladať právo hovoriť a obhajovať. Nech je obsah etickej teórie akýkoľvek, už samotné jej navrhnutie predpokladá hoppeovský rámec.

Rozsah argumentu

Možná námietka sa pýta, ako sa etika argumentácie vzťahuje na tých, ktorí argumentovať nemôžu: na dojčatá, ťažko kognitívne postihnutých, dočasne v bezvedomí. Ak práva vyplývajú z predpokladov argumentovania, majú práva aj tí, ktorí neargumentujú?

Odpoveď je, že každý, kto argumentuje, bol kedysi takým človekom.[12] Kto argumentuje, musí si vážiť podmienky, ktoré umožnili jeho súčasnú schopnosť, vrátane toho, že ho nezabili v čase, keď argumentačnú schopnosť ešte nemal, ale mal potenciál ju rozvinúť. Tvrdiť, že potenciálni argumentujúci nemajú práva, by znamenalo protirečiť podmienkam vlastnej existencie ako argumentujúceho. Stav pred argumentovaním nie je mimo rozsahu argumentu, ale je ním predpokladaný.

Táto kniha preberá Hoppeho argument ako normatívny základ súkromia. Argument obstál v takmer štyroch desaťročiach kritického skúmania. Kto ho chce odmietnuť, nesie dôkazné bremeno, aby ukázal, ako to môže urobiť bez performatívneho rozporu.

4.4 Dôsledky: vlastníctvo a neagresia

Ak Hoppeho argument obstojí, vyplýva z neho stručná etická štruktúra.

Prvým dôsledkom je sebavlastníctvo. Jednotlivci majú výlučné práva nad vlastným telom a mysľou. Iní nesmú bez súhlasu používať cudzie telo ani zasahovať do duševných procesov. Telesná integrita (sloboda od napadnutia, ublíženia a zadržiavania), duševná integrita (sloboda od manipulácie, nátlaku a psychickej invázie) a kontrola nad vlastným vyjadrovaním (sloboda komunikovať alebo mlčať) vyplývajú z jedného základného tvrdenia: výlučného práva usmerňovať vlastné konanie.

Vlastnícke práva k vonkajším zdrojom nasledujú ďalej. Konanie vyžaduje prostriedky a prostriedky sa musia nejako prideliť; jediné pravidlo prideľovania, ktoré nie je samo agresiou, je prvotné privlastnenie dosiaľ nevlastnených zdrojov a následný dobrovoľný prevod. Vlastnícke práva v tomto výklade zahŕňajú výlučné užívanie (vlastník rozhoduje, ako sa zdroj používa), prevod (vlastník môže zdroj darovať alebo predať) a vylúčenie (vlastník môže iným zabrániť, aby zdroj používali). Nie sú to tri osobitné práva, ale tri stránky jedného práva, ktoré zodpovedajú trom spôsobom, akými sa môže niekto iný pokúsiť zasiahnuť.

Princíp neagresie je etický rámec, ktorý obe veci spája. Začať násilie voči osobám alebo majetku je nelegitímne; sila je opodstatnená len na obranu proti predchádzajúcej agresii. Vziať majetok bez súhlasu je agresia. Ublížiť osobám bez súhlasu je agresia. Použiť klam na získanie majetku

alebo súhlasu je agresia. Nútiť niekoho, aby o sebe prezradil informácie, porušuje sebavlastníctvo, a je preto tiež agresiou.

Pre súkromie z toho vyplývajú konkrétne dôsledky. Duševné súkromie je chránené, pretože myšlienky a preferencie spadajú pod sebavlastníctvo. Súkromie komunikácie je chránené, pretože rozhodovať, čo odhaliť a komu, je výkon sebavlastníctva nad vlastným vyjadrovaním. Súkromie údajov je chránené, pretože informácie o sebe, uložené na vlastných nosičoch alebo zdieľané za podmienok, ktoré si človek stanovil, spadajú pod vlastnícke práva k nosičom a pod sebavlastníctvo nad pôvodom informácií. A nútené sledovanie, či už ide o vynútené odhalenie, alebo monitorovanie bez súhlasu, porušuje sebavlastníctvo v koreni, bez ohľadu na to, čo sa zistí.

4.5 Axióma argumentácie a súkromie

Oddiel 4.4 vyložil dôsledky Hoppeho argumentu pre vlastníctvo a neagresiu vo všeobecnosti. Jeden dôsledok si zaslúži osobitný výklad: čo argument znamená konkrétne pre súkromie.

Kognitívne súkromie ako predpoklad argumentu

Hoppeho argument vychádza z pozorovania, že ľudia, ktorí argumentujú, musia mať výlučnú kontrolu nad telom aj mysľou, aby mohli formulovať a vyjadriť svoje stanoviská. Tá časť tvrdenia, ktorá sa týka mysle, siaha ďalej, než sa na prvý pohľad zdá.

Argumentovať znamená uvažovať pred rečou. Stanovisko vzniká vnútorným procesom: hodnotením dôkazov, vážením konkurenčných tvrdení, výberom slov, rozhodovaním o tom, čo tvrdiť a čo zadržať. Tento proces nie je samotným argumentom, ale podmienkou, za ktorej sa argument stáva možným. Ak by uvažovanie niekoho, kto argumentuje, mohla pred vyjadrením skúmať a ovplyvňovať iná strana, neuvažoval by slobodne. Závery, ku ktorým by za takých podmienok dospel, by neboli skutočne jeho. Boli by artefaktmi pozorovateľovho prístupu.

Nútené odhalenie nevyjadrenej myšlienky a sledovanie duševného procesu, ktorý predchádza reči, preto porušuje predpoklady argumentovania rovnako ako fyzický nátlak na telo. Jedno odoberá kontrolu nad tým, čo človek hovorí, druhé nad tým, čo si myslí predtým, než to povie. Obe ničia podmienku, ktorú argument vyžaduje.

Kognitívne súkromie pomenúva túto podmienku: výlučné právo na proces uvažovania, ktorý predchádza vyjadreniu. Neodvodzuje sa z všeobecného práva na tajnosť, ale z toho, čo argumentovanie samo predpokladá.

Kontrola nad vlastným vyjadrovaním ako selektívne odhaľovanie

Axióma argumentácie zahŕňa aj kontrolu nad vlastným vyjadrovaním: právo rozhodnúť, čo sa odhalí a komu, a zadržať to, čo človek odhaliť nezvolil.

Kto nemá právo mlčať alebo kto môže byť nútený odhaliť viac, než argument vyžaduje, nemá skutočnú kontrolu nad tým, čo vyjadruje. Vynútené odhalenie nie je podmienka, za ktorej môže argument voľne prebiehať. Kto môže byť povinný vydať všetko vnútorné uvažovanie, predchádzajúcu komunikáciu, korešpondenciu a združenia, nie je slobodný argumentovať: podlieha nátlaku, ktorý predchádza ten fyzický.

Formulácia Erica Hughesa v „Cypherpunkovom manifeste“[14] sa na túto štruktúru presne vzťahuje. Súkromie je selektívne odhaľovanie: každá strana transakcie odhalí to, čo transakcia vyžaduje, a nič navyše. Hughes k tomu dospel inžinierskym inštinktom; Hoppeho etika argumentácie mu dáva normatívny základ. Právo na selektívne odhaľovanie nie je preferencia, ale predpoklad racionálneho diskurzu. Systém, ktorý ho odstráni, odstráni podmienku samotného argumentovania.

Sledovanie ako performatívny rozpor

Štát, ktorý vynucuje úplnú transparentnosť, teda žiada od občanov komunikáciu, odhalenie združení, prezradenie finančných transakcií a podrobenie sa nepretržitému pozorovaniu, sa dopúšťa performatívneho rozporu osobitného druhu.

Štát musí svoju autoritu zdôvodňovať argumentom. Prijíma zákony, vydáva rozsudky, uplatňuje nároky voči občanom a pripúšťa spochybnenie na súdoch. Každá z týchto činností je formou argumentovania a každá predpokladá rámec, ktorý určil Hoppe: účastníci musia mať výlučnú kontrolu nad vlastným uvažovaním a vyjadrovaním, aby sa mohli zúčastniť skutočného diskurzu o normách, ktoré ich spravujú.

Štát, ktorý svojim poddaným odníma kognitívne súkromie a kontrolu nad vyjadrovaním, zničil podmienky, za ktorých by sa títo poddaní mohli zúčastniť ako skutoční účastníci akéhokoľvek normatívneho diskurzu. Vytvoril obyvateľstvo, ktoré nemôže odpovedať argumentom, pretože predpoklady argumentovania sú mu odňaté. Sledovací režim nie je len agresiou voči právam jednotlivca, ale útokom na inštitucionálne podmienky samotného diskurzu.

Od normy k architektúre

Axióma argumentácie ustanovuje normu, nie mechanizmus. Hovorí, že kognitívne súkromie a kontrola nad vlastným vyjadrovaním sú predpoklady racionálneho diskurzu a že ich porušenie je agresia v plnom hoppeovskom zmysle. Nehovorí, ako sa tieto predpoklady dajú chrániť pred sledovacím aparátom, ktorému je jedno, či mu poddaní vedia odpovedať.

Tu cypherpunková tradícia preberá štafetu od normatívnej. Kapitola 5 predstavuje axiómu odporu, ktorá normu prekladá do štruktúry nákladov. Ďalšie kapitoly ukazujú, ktoré kryptografické a ekonomické nástroje zvyšujú náklady na pozorovanie natoľko, aby sa norma dala v praxi presadiť.

Zhrnutie kapitoly

Hoppeho etika argumentácie ukazuje, že účasť v diskurze predpokladá sebavlastníctvo: kto popiera sebavlastníctvo, musí na formuláciu a vyjadrenie poprenia vykonávať výlučnú kontrolu nad telom a mysľou, čo je performatívny rozpor. Vlastnícke práva vyplývajú zo sebavlastníctva cez prvotné privlastnenie, jediné univerzalizovateľné pravidlo na riešenie sporov o vzácne zdroje. Z toho zasa vyplýva princíp neagresie: nevyžiadaný zásah do osoby alebo majetku je agresia a sila je opodstatnená len na obranu proti nej. Nútené sledovanie porušuje sebavlastníctvo, a podľa toho istého rámca je preto agresiou.

Argument čelil námietkam štyri desaťročia a odpovedal na ne. Murphy s Callahanom sa pýtali, či Hoppe preukazuje vlastníctvo, alebo len užívanie; rozdiel pri skúmaní zaniká a odmietnuť uznať vlastníctvo znamená postaviť sa úplne mimo racionálneho diskurzu. Humeova otázka is–ought sa pýta, či argument preklenuje opis a predpis; neodvodzuje má byť z je, ale ukazuje, že určité normatívne tvrdenia sa nedajú dôsledne poprieť. Námietka čiastočného uplatnenia sa pýta, prečo zásady ustanovené v argumentovaní platia aj mimo neho; univerzalizovateľnosť je pre argumentovanie konštitutívna. Kinsellov argument estoppelu, obrana potenciálne argumentujúcich vychádzajúca zo stavu pred argumentovaním a van Dunovo vysvetlenie, že odmietnutie predpokladov argumentu stavia človeka mimo spoločenstva diskurzu, posilňujú ten istý rámec.

Axióma argumentácie siaha do súkromia ďalej než samotná všeobecná analýza agresie. Argumentovanie predpokladá kognitívne súkromie: proces uvažovania, ktorý predchádza vyjadreniu, musí výlučne ovládať ten, kto argumentuje, inak závery, ku ktorým dospeje, nie sú jeho. Predpokladá aj kontrolu nad vlastným vyjadrovaním: právo rozhodnúť, čo sa odhalí, a zadržať to, čo človek neponúkol. Neodvodzujú sa zo všeobecného práva na tajnosť, ale z toho, čo diskurz vyžaduje. Štát, ktorý odníma kognitívne súkromie a vynucuje úplné odhalenie, zničil podmienky, za ktorých by sa jeho poddaní mohli zúčastniť ako skutoční účastníci akéhokoľvek normatívneho argumentu o pravidlách, ktoré ich spravujú. Sledovací režim je performatívny rozpor na inštitucionálnej úrovni: tvrdí, že vládne prostredníctvom zákona a argumentu, a pritom odstraňuje predpoklady, ktoré zákon a argument umožňujú.

Dostávame tým kritérium, nie úplný zákonník. Súhlas, verejné pozorovanie a usudzovanie z dostupných informácií si vyžadujú uplatňova-

nie zásady od prípadu k prípadu. Rámec tiež nepreukazuje, že súkromie sa dá v praxi vynútiť. Kapitola 5 sa zaoberá axiómou odporu; technické a ekonomické kapitoly, ktoré nasledujú, menia normu na niečo, čo svet dokáže udržať.[13]

Poznámky

[1] Hans-Hermann Hoppe, "Argumentation Ethics," in *The Economics and Ethics of Private Property*, 2. vyd. (Auburn, AL: Ludwig von Mises Institute, 2006), 380.

[2] K diskurzívnej etike pozri Jürgen Habermas, *Moral Consciousness and Communicative Action*, prel. Christian Lenhardt a Shierry Weber Nicholsen (Cambridge, MA: MIT Press, 1990); Karl-Otto Apel, "The Problem of Philosophical Foundations in Light of a Transcendental Pragmatics of Language," in *After Philosophy: End or Transformation?*, ed. Kenneth Baynes a kol. (Cambridge, MA: MIT Press, 1987). K Hoppeho úprave diskurzívnej etiky na etiku argumentácie pozri kapitolu 3, poznámku 7.

[3] Robert P. Murphy and Gene Callahan, "Hans-Hermann Hoppe's Argumentation Ethic: A Critique," *Journal of Libertarian Studies* 20, no. 2 (2006): 53-64. Dostupné na https://cdn.mises.org/20_2_3.pdf.

[4] K odpovediam Murphymu a Callahanovi pozri Walter Block, "Rejoinder to Murphy and Callahan on Hoppe's Argumentation Ethics," *Journal of Libertarian Studies* 22 (2010): 631-639; Marian Eabrasu, "A Reply to the Current Critiques Formulated Against Hoppe's Argumentation Ethics," *Libertarian Papers* 1, no. 20 (2009).

[5] Frank van Dun, "Argumentation Ethics and the Philosophy of Freedom," *Libertarian Papers* 1, no. 20 (2009). Van Dunova analýza objasňuje, že kto odmieta uznať predpoklady argumentovania, argument nevyvrátil, ale postavil sa mimo spoločenstva racionálneho diskurzu.

[6] Hatim Kheir, "Bridging the Use-Ownership Gap: A Reformulation of Hoppe's Argumentation Ethics on Praxeological Grounds," *Journal of Libertarian Studies* 27, no. 1 (2023): 115-134. Dostupné na https://jls.mises.org/article/84874.

[7] K univerzalizovateľnosti pozri Hoppe, "Argumentation Ethics," 383-384; Stephan Kinsella, "Explaining Argumentation Ethics and Universalizability Concisely," (2019), dostupné na https://stephankinsella.com/2019/03/explaining-argumentation-ethics-and-universalizability-concisely-to-a-facebook-friend/. Argument, že partikularistické normy sa v racionálnom diskurze vyvracajú samy, pochádza z kantovskej tradície, ale v Hoppeho rámci dostáva výrazne libertariánske uplatnenie.

[8] K estoppelu ako doplňujúcemu zdôvodneniu práv pozri Stephan Kinsella, "Estoppel: A New Justification for Individual Rights," *Reason Papers* 17 (1992): 61-74. Kinsella tvrdí, že agresori sú zbavení práva namietať proti obrannej sile, pretože ich vlastné konanie ukazuje, že prijímajú zásadu, že sila je prípustná.

[9] David Hume, *A Treatise of Human Nature* (1739-40), book III, part I, §1. Rozlíšenie is–ought sa objavuje v Humeovom pozorovaní, že autori nebadane prechádzajú od „je" a „nie je" k „má byť" a „nemá byť"; na logickú medzeru upozornil, ale nevyriešil ju.

[10] Pozri Kinsellov výklad Hoppeho štruktúry: Stephan Kinsella, "Argumentation Ethics and Liberty: A Concise Guide," Mises Institute (2011). Dostupné na https://mises.org/mises-daily/argumentation-ethics-and-liberty-concise-guide.

[11] Murray N. Rothbard, "Beyond Is and Ought," *Liberty* 2, no. 2 (1988): 44-45. Rothbard uviedol, že sa Hoppemu „podarilo prekonať slávnu dichotómiu is/ought, fakt/hodnota, ktorá trápi filozofiu od čias scholastikov".

[12] K rozšíreniu etiky argumentácie na potenciálne argumentujúcich pozri Patrick Tinsley, "Preargumentation Ethics and the Issue of Abortion," *Journal of Libertarian Studies* (2020). Argument hovorí, že súčasní argumentujúci si musia vážiť podmienky, ktoré umožnili ich vlastnú argumentačnú schopnosť, vrátane ochrany v čase, keď mali potenciál, ale nie skutočnú argumentačnú schopnosť.

[13] Ďalšie čítanie o libertariánskej etike a etike argumentácie. K základným Hoppeho textom (*A Theory of Socialism and Capitalism*, kap. 7, a *The Economics and Ethics of Private Property*) pozri kapitolu 3, poznámku 7. K rothbardovskej tradícii prirodzených práv, ktorú Hoppe rozširuje, je kanonickým zdrojom Murray N. Rothbard, *The Ethics of Liberty* (NYU Press, 1998; pôvodne 1982). Ako kratší vstup: Stephan Kinsella vo svojich priebežných textoch na `https://stephankinsella.com` systematicky rozoberá Hoppeho argumenty a odpovedá kritikom; jeho *Legal Foundations of a Free Society* (Papinian Press, 2023) zbiera jeho výklady. K širšej tradícii libertarianizmu prirodzených práv pozri Robert Nozick, *Anarchy, State, and Utopia* (Basic Books, 1974), a Eric Mack, *Libertarianism* (Polity, 2018). K analytickému filozofickému spracovaniu problému is–ought, ktorým sa etika argumentácie zaoberá, pozri J. L. Mackie, *Ethics: Inventing Right and Wrong* (Penguin, 1977), a heslo *Stanford Encyclopedia of Philosophy* „Moral Anti-Realism" na `https://plato.stanford.edu/entries/moral-anti-realism/`. K habermasovskej „diskurzívnej etike", s ktorou je Hoppeho etika argumentácie čiastočne paralelná (a ktorú kritizuje), pozri Jürgen Habermas, *Moral Consciousness and Communicative Action*, prel. Christian Lenhardt a Shierry Weber Nicholsen (MIT Press, 1990), a Karl-Otto Apel, *Understanding and Explanation: A Transcendental-Pragmatic Perspective*, prel. Georgia Warnke (MIT Press, 1984). K kritickým posúdeniam Hoppeho argumentu osobitne: Robert P. Murphy and Gene Callahan, "Hans-Hermann Hoppe's Argumentation Ethic: A Critique," *Journal of Libertarian Studies* 20, no. 2 (2006): 53–64; hlavné námietky katalogizujú aj odpovede v nasledujúcich číslach toho istého časopisu. K argumentu pre sebavlastníctvo nezávislému od Hoppeho: Michael Huemer, *The Problem of Political Authority* (Palgrave Macmillan, 2013), zakladá silné vlastnícke práva v morálnych intuíciách zdravého rozumu.

[14] Eric Hughes, "A Cypherpunk's Manifesto" (1993), dostupné na `https://www.activism.net/cypherpunk/manifesto.html`. Hughes definuje súkromie ako selektívne odhaľovanie: „Súkromie je moc selektívne sa odhaliť svetu." Jeho manifest je zakladajúci dokument cypherpunkového hnutia a priamy zdroj formulácie selektívneho odhaľovania, ktorá sa cituje v oddiele 4.5. Hoppeho etika argumentácie dáva Hughesovej inžinierskej intuícii normatívny základ: právo na selektívne odhaľovanie je predpoklad racionálneho diskurzu, nie preferencia.

[15] Murray N. Rothbard, *The Ethics of Liberty* (New York: NYU Press, 1998; pôvodne Humanities Press, 1982). Dostupné na `https://mises.org/library/ethics-liberty`. Kanonické libertariánske vyjadrenie princípu neagresie, založené na sebavlastníctve: „Nikto ani žiadna skupina ľudí nesmie páchať agresiu voči osobe alebo majetku niekoho iného." Hoppeho etika argumentácie je navrhnutá tak, aby tomuto rothbardovskému NAP dala pevnejší, nekruhový základ než Rothbardovo vlastné odvodenie z prirodzených práv.

[16] John Locke, *Two Treatises of Government* (1689), Second Treatise, kap. V, §27: „Whatsoever then he removes out of the state that nature hath provided, and left it in, he hath mixed his labour with, and joined to it something that is his own, and thereby makes it his property." Lockova teória miešania práce je historickým pôvodom prvotného privlastnenia ako aktu, ktorý zakladá vlastníctvo; Hoppeho princíp homesteadingu túto štruktúru preberá, ale zakladá ju na predpokladoch argumentovania, nie na prirodzenej teológii.

[17] Hans-Hermann Hoppe, *A Theory of Socialism and Capitalism: Economics, Politics, and Ethics* (Boston: Kluwer Academic Publishers, 1989; dotlač Auburn, AL: Ludwig von Mises Institute, 2010). Dostupné na https://mises.org/library/theory-socialism-and-capitalism. Kapitola 7 obsahuje úplné pôvodné vyjadrenie etiky argumentácie, z ktorého vychádza analýza v tejto kapitole; ďalšie kapitoly uplatňujú argument na odvodenie noriem súkromného vlastníctva a systematickú kritiku socialistických a intervencionistických usporiadaní.

5
AXIÓMA ODPORU

„Kto neprijíma axiómu odporu, uvažuje o úplne inom systéme než Bitcoin."

Eric Voskuil, *Cryptoeconomics* (2019)[1]

Kniha používa slovo „axióma" trikrát: axióma konania v kapitole 3, axióma argumentácie v kapitole 4 a axióma odporu v tejto kapitole. Nie sú to axiómy v tom istom zmysle a ten rozdiel treba vyznačiť skôr, než kapitola pokročí.

Axióma konania je samozrejmá v striktnom praxeologickom zmysle. Podľa Misesa nemožno poprieť vetu „ľudia konajú účelne" bez toho, aby sa popierač dopustil práve toho účelného správania, ktoré chce poprieť. Je pravdivá a priori a zakladá deskriptívnu vedu o konaní.

Axióma argumentácie je performatívne nepopierateľná v Hoppeho zmysle. Kto vstúpi do argumentácie, ten už predpokladá sebavlastníctvo, právo používať vlastné telo na vyjadrovanie tvrdení a normy, ktoré robia diskurz možným. Zakladá normatívnu stránku celého rámca.

Axióma odporu je metodologická. Je to pracovný predpoklad o technických možnostiach, ktorý vychádza z kryptografickej teórie a zo skúseností s nasadenými systémami a vymedzuje predmet každej analýzy technológie slobody. Eric Voskuil zaviedol tento pojem v knihe „Kryptoekonómia" (angl. *Cryptoeconomics*), aby oddelil systémy, ktoré dokážu klásť odpor vonkajšej kontrole (Bitcoin, Tor, end-to-end šifrovanie), od systémov, ktoré to nedokážu

(PayPal, peniaze centrálnych bánk, identita sprostredkovaná platformou). Kto tento predpoklad odmieta, nedopúšťa sa logickej chyby. Odmietnutie len presúva predmet skúmania na systémy, ktoré odpor nekladú.

Tri axiómy plnia rôzne úlohy. Konanie vysvetľuje ekonómiu dobrovoľného poriadku. Argumentácia dodáva etiku, ktorá zakazuje agresiu. Odpor dodáva stratégiu, bez ktorej sa prvé dve nedajú v praxi ubrániť. Dokonalé vlastníctvo statkov je prázdna norma, ak ich vlastník vydá v okamihu, keď sa objaví agresor. Spolu tvoria chrbticu každej dôkladnej analýzy technológie slobody. Zvyšok kapitoly skúma, čo tvrdí tretí predpoklad a prečo je dobre podložený.

Úvod

Táto kapitola predstavuje tretí základ: axiómu odporu. Na rozdiel od predchádzajúcich dvoch axióm nejde o samozrejmé ani o normatívne tvrdenie, ale o predpoklad. Eric Voskuil v rozbore bezpečnostného modelu Bitcoinu píše, že axióma nie je „prijatá ako fakt, ale pokladaná za rozumný predpoklad vzhľadom na správanie podobných systémov“.[2]

Predpoklad znie takto: systémy možno navrhnúť tak, aby kládli odpor vonkajšej kontrole. Kryptografické nástroje môžu sledovanie technicky sťažiť. Matematické vlastnosti dokážu chrániť súkromie tam, kde politické sľuby nestačia. Tento predpoklad možno bez rozporu poprieť. Systémy typu PayPal, ktoré sa opierajú o centrálnu autoritu, sú úplne koherentným predmetom analýzy. Odmietnutie axiómy odporu nie je logická chyba. Len presúva predmet skúmania k návrhu systémov, ktoré odpor nekladú.

Predpoklad je však dobre podložený. Opiera sa o matematické základy a empirické dôkazy a posilňuje ho metodologická nevyhnutnosť. Kapitola najprv skúma, čo axióma tvrdí a prečo je dobre podložená, a potom vyznačí, kde sa jej hranice začínajú.

5.1 Čo axióma tvrdí

Jadro tvrdenia

Axióma odporu tvrdí, že systémy odolné voči vonkajšej kontrole sa dajú navrhnúť, a opiera sa o niekoľko konkrétnych schopností. Kryptografické systémy môžu chrániť informácie pred neoprávneným prístupom. Decentralizované siete môžu fungovať bez jediného bodu kontroly. Matematické vlastnosti môžu dať silnejšie záruky než právna alebo politická ochrana. Odpor nie je zaručený, ale je technicky dosiahnuteľný.

Čo znamená „odpor``

Odpor je schopnosť klásť náklady protivníkom, ktorí sa snažia o kontrolu. Systém kladie odpor v tej miere, v akej si obchádzanie jeho ochrany vyžaduje viac zdrojov, než sú protivníci ochotní alebo schopní vynaložiť. Odpor nie je binárny, ale existuje na škále. Systém môže odolať bežným útočníkom, no nie národným štátom, alebo odolať všetkým známym útokom a zostať zraniteľný voči pokroku v matematike či vo výpočtovej technike.

Odpor pôsobí vo viacerých rozmeroch. Výpočtový: kryptografické systémy vyžadujú zdroje, ktoré sú prakticky nedosiahnuteľné, lebo 256-bitový kľúč by si vyžiadal viac operácií hrubou silou, než dovoľuje vek vesmíru. Ekonomický: náklady na útok presahujú hodnotu úspechu, takže aj prelomiteľný systém kladie odpor, ak jeho prelomenie stojí viac, než sú informácie hodné. Štrukturálny: decentralizované systémy nemajú jediné miesto, na ktoré by sa dalo zaútočiť, pretože zhodenie jedného uzla nechá fungovať ostatné a kompromitovanie jedného účastníka nekompromituje sieť. Jurisdikčný: systémy rozložené cez právne hranice kladú odpor, lebo žiadna jediná autorita nedokáže vynútiť poslušnosť od všetkých súčastí.

Odpor nie je nezraniteľnosť. Žiadny systém nie je dokonale bezpečný. Axióma tvrdí, že odpor je možný: systémy sa dajú navrhnúť tak, aby ich prekonanie vyžadovalo viac zdrojov, než sú útočníci ochotní vynaložiť. Odpor je tiež asymetrický. Obranca dosiahne ochranu lacnejšie, než útočník dosiahne prielom: šifrovanie je lacné, prelomenie silného šifrovania je drahé. Táto asymetria mení rovnováhu síl. Bez kryptografickej ochrany je sledovanie ľahké a súkromie ťažké. S kryptografickou ochranou je súkromie dosiahnuteľné a sledovanie nákladné.

Čo axióma netvrdí

Axióma netvrdí, že odpor je zaručený. Systémy môžu zlyhať, implementácie môžu mať chyby a používatelia robia omyly, takže axióma predpokladá, že odpor je možný, nie že vždy uspeje. Netvrdí ani, že odpor je absolútny. Štáty majú zdroje, ktoré jednotlivci nemajú, a keď sú dostatočne rozhodnuté, vedia odpor niekedy prekonať právnym nátlakom, fyzickým donútením alebo obrovským vynaložením prostriedkov. Netvrdí ani, že odpor vyrieši všetky problémy, pretože fyzické donútenie, sociálne inžinierstvo a ľudské omyly ovplyvňujú náklady aj výsledky. A napokon, na rozdiel od axiómy konania nevzniká popretím odporu logický rozpor. Axióma sa predpokladá, nedokazuje, a práve tým sa jej logický status líši od samozrejmých základov z predchádzajúcich kapitol.

5.2 Prečo je axióma dobre podložená

Axióma odporu je predpoklad, nie dôkaz, no stojí na solídnych základoch.

Matematický základ

Moderná kryptografia stojí na predpokladoch o výpočtovej náročnosti.[3] Niektoré matematické problémy sa zdajú byť ťažko riešiteľné. Jedným z nich je rozklad veľkých čísel: dve veľké prvočísla sa dajú ľahko vynásobiť, ale z ich súčinu je pri súčasnej technike výpočtovo neuskutočniteľné zistiť pôvodné prvočísla. Podobné vlastnosti má problém diskrétneho logaritmu: v istých matematických štruktúrach je hodnotu ľahké vypočítať, ale opačný výpočet je neuskutočniteľný.[13] Ďalším základom je odolnosť hašovacích funkcií voči nájdeniu vzoru: ak poznáme výstup kryptografického haša, nájsť vstup, ktorý ho vytvorí, je výpočtovo neuskutočniteľné. Na týchto predpokladoch o náročnosti stojí RSA,[14] kryptografia na eliptických krivkách[15] aj hašovacie funkcie, ktoré používa Bitcoin a ďalšie systémy. Ak predpoklady platia, kryptografická ochrana je skutočná.

Predpoklady nie sú dokázané. Keby P bolo rovné NP, čo je stále otvorená otázka, väčšina súčasných kryptografických predpokladov by sa zrútila. Celá stavba kryptografie s verejným kľúčom stojí na domnienkach, ktoré sú síce podložené desaťročiami neúspešných útokov, ale nemajú matematický dôkaz správnosti.

Algoritmický pokrok neustáva. Všeobecné číselné sito (General Number Field Sieve)[16] zvýšilo efektívnosť rozkladu na prvočinitele oproti skorším metódam, útoky založené na mriežkach oslabili niektoré implementácie eliptických kriviek a kvantové výpočty, o ktorých pojednáva kapitola 14, hrozia úplne prelomiť väčšinu súčasnej kryptografie s verejným kľúčom.[4] Bezpečnostné rezervy, ktoré sa dnes zdajú pohodlné, sa môžu zmenšiť, ako matematika a výpočtová technika pokročia.

Desaťročia výskumu nepreukázali, že tieto problémy sú dokázateľne ťažké. Preukázali len to, že zatiaľ nikto nenašiel efektívne riešenia. Predpoklady sú empiricky dobre podložené, nie matematicky dokázané. Kryptografická bezpečnosť teda závisí od toho, že výskum útokov bude naďalej neúspešný, nie od nemožnosti, ktorá by bola už dokázaná. Tieto výpočtové základy podrobne skúma kapitola 14.[5]

Empirický záznam

Systémy navrhnuté na kladenie odporu sa v praxi ukázali ako odolné. Sieť Tor funguje od roku 2002 a napriek protivníkom na úrovni štátov poskytuje anonymnú komunikáciu vo významnom rozsahu. Jej hranice sú reálne: obavy zostávajú pri časových útokoch, kompromitovaných výstupných uzloch[17] aj pri chybách používateľov. Napriek tomu Tor funguje ďalej a patrí medzi najtrvanlivejšie verejné systémy anonymity, aké boli kedy nasadené. Bitcoin funguje od roku 2009, spracúva transakcie a udržiava konsenzus bez centrálnej autority. Štáty obmedzili burzy, ťažiarov a prístupové body, ale sieť nevypli. PGP a jeho nasledovníci chránia komunikáciu desaťročia silným šifrovaním.[6] Ak kľúče nie sú k dispozícii, ani

trestné stíhanie nedá úradom dešifrovanie na príkaz. Signal a ďalšie aplikácie s end-to-end šifrovaním chránia súkromnú komunikáciu vo veľkom rozsahu.[7]

Tento empirický záznam nedokazuje, že odpor vždy uspeje. Ukazuje však, že odpor uspel v praxi, počas dlhých období a proti protivníkom s veľkými zdrojmi.

Metodologická nevyhnutnosť

Voskuil zdôrazňuje, že prijatie axiómy odporu určuje, čo analyzujeme. „Kto neprijíma axiómu odporu, uvažuje o úplne inom systéme než Bitcoin."

Ak predpokladáme, že odpor je nemožný, analyzujeme systémy s povolením: PayPal, bankové účty, regulované finančné inštitúcie. Tieto systémy fungujú z milosti úradov a dajú sa kedykoľvek vypnúť alebo sledovať.

Ak predpokladáme, že odpor je možný, analyzujeme systémy bez povolenia: Bitcoin, Tor, end-to-end šifrovanie. Tieto systémy fungujú nezávisle od úradov a už svojím návrhom kladú odpor kontrole.

Oba druhy systémov existujú a oba stoja za štúdium. Sú však rozdielne a analýza vhodná pre jeden nemusí platiť pre druhý. Axióma je metodologická voľba, ktorá vymedzuje predmet skúmania.

Epistemický problém popierania

Popieranie axiómy odporu má epistemickú zvláštnosť.

Ak je odpor nemožný, ak štáty ovládajú všetky toky informácií a dokážu prekonať každú kryptografickú ochranu, ako by sme to vôbec vedeli? Naše zdroje informácií by boli pod kontrolou. Možnosť objaviť spôsoby odporu by bola obmedzená. A presvedčenie, že odpor je nemožný, by mohlo byť len výsledkom kontroly, ktorú pokladáme za úplnú.

Toto pozorovanie nie je dôkaz, že odpor je možný. Naznačuje však, že sebaisté popieranie čelí vlastným epistemickým ťažkostiam. Popierač len ťažko overí svoje popieranie bez prístupu k informáciám, ktorým by nemohol dôverovať, ak je jeho popieranie správne.

5.3 Vzťah k ostatným základom

Axióma konania (kapitola 3)

Axióma konania zakladá, že súkromie je zabudované do štruktúry konania. Úvaha prebieha vo vnútri, preferencie sú subjektívne a informačná asymetria je neodmysliteľná.

Axióma odporu sa pýta: dá sa táto vlastnosť chrániť? Dá sa súkromie, ktoré existuje ako fakt ľudského konania, zachovať pred pokusmi o jeho odstránenie?

Axióma odporu odpovedá, že áno. Technická ochrana je možná. Štrukturálne súkromie konania sa dá udržať kryptografickými prostriedkami.

Axióma argumentácie (kapitola 4)

Axióma argumentácie ukazuje, že súkromie sa v diskurze nedá koherentne poprieť. Sebavlastníctvo zahŕňa kontrolu nad vlastnými duševnými procesmi a komunikáciou.

Tento normatívny záver je však bez uskutočnenia v praxi prázdny. Tvrdenie, že súkromie by malo byť chránené, ho ešte nechráni.

Axióma odporu premosťuje priepasť medzi normatívnym a praktickým. Ak je odpor možný, súkromie, ktoré by malo byť chránené (podľa kapitoly 4), sa dá chrániť (podľa kapitoly 5).

Tri základy spolu

Tri základy do seba zapadajú. Kapitoly 3 a 4 stanovili, čo je súkromie, a vysvetlili, čo je v hre z mravného a ekonomického hľadiska. Táto kapitola pridáva praktický predpoklad: dá sa chrániť.

Zhrnutie kapitoly

Axióma odporu je tretí základ: systémy možno navrhnúť tak, aby kládli odpor vonkajšej kontrole, nie ako dokázaný fakt, ale ako dobre podložený predpoklad. Opiera sa o výpočtovú náročnosť v kryptografii, o empirický záznam Toru,[8] Bitcoinu[9] a end-to-end šifrovania, ktoré už roky odolávajú nátlaku, a o metodologickú úvahu, že prijatie axiómy vymedzuje predmet zvyšku knihy. Epistemická zvláštnosť jej popierania spočíva v tom, že kto by nikdy nemohol overiť odpor, nemôže spoľahlivo uzavrieť ani to, že je nemožný. Axiómu to nedokazuje, ale zužuje to, čo môže sebaisté odmietnutie koherentne tvrdiť.

Axióma tvrdí možnosť, nie nevyhnutnosť. Odpor často zlyháva pri fyzickom donútení („útok kľúčom za päť dolárov“, angl. *wrench attack*),[10] pri chybe v implementácii,[11] pri omyloch používateľov alebo pri nedostatočnej veľkosti siete. Nie je ani bezplatný. Kryptografia robí digitálnu obranu lacnou a digitálny útok drahým, no fyzické donútenie asymetriu obracia a návrh systému môže náklady presúvať, ale neodstráni ich. Dnešná bezpečnosť môže byť zajtrajšou zraniteľnosťou, ako sa hrozby vyvíjajú a štáty získavajú zdroje, ktoré jednotlivci nemajú: právnu autoritu, vynútenú spoluprácu, prístup do dodávateľského reťazca. Predpoklad zostáva predpokladom a rozumní ľudia ho môžu odmietnuť a analyzovať iné systémy. Umožňuje zvyšok knihy, ktorý postupuje podľa prvej z týchto dvoch možností.[12]

Poznámky

[1] Eric Voskuil, ”Axiom of Resistance,” *Cryptoeconomics: Fundamental Principles of Bitcoin*, dostupné na `https://github.com/libbitcoin/libbitcoin-system/wiki/Axiom-of-Resistance`.

[2] Voskuil, ”Axiom of Resistance.” Celý citát: „Axióma sa neprijíma ako fakt, ale pokladá sa za rozumný predpoklad vzhľadom na správanie podobných systémov.“ (angl. ”The axiom is not accepted as a fact but deemed to be a reasonable assumption, due to the behavior of similar systems.”)

[3] O výpočtovej náročnosti a kryptografických predpokladoch pozri Jonathan Katz a Yehuda Lindell, *Introduction to Modern Cryptography*, 3. vyd. (Boca Raton: CRC Press, 2020), najmä kapitoly o výpočtovej bezpečnosti a predpokladoch o náročnosti.

[4] O postkvantovej kryptografii pozri NIST Post-Quantum Cryptography Standardization project, `https://csrc.nist.gov/projects/post-quantum-cryptography`. NIST vydal prvé finálne postkvantové šifrovacie štandardy v auguste 2024.

[5] O probléme P vs NP a jeho dôsledkoch pre kryptografiu pozri Scott Aaronson, *Quantum Computing Since Democritus* (Cambridge: Cambridge University Press, 2013), a Michael Sipser, *Introduction to the Theory of Computation*, 3. vyd. (Boston: Cengage Learning, 2012).

[6] Phil Zimmermann vydal PGP (Pretty Good Privacy) v roku 1991; k textu ”Why I Wrote PGP” (1991) a k spracovaniu dejín cypherpunkerov pozri kapitolu 2, poznámku 15. Protokol je štandardizovaný ako OpenPGP, v súčasnosti RFC 9580 (júl 2024), pričom historickým východiskom je RFC 4880 (2007); hlavná stránka projektu je `https://www.openpgp.org/`.

[7] Signal Foundation, `https://signal.org/`, so špecifikáciami protokolu na `https://signal.org/docs/`. Protokol Double Ratchet, na ktorom Signal stojí, je referenčným návrhom modernej end-to-end šifrovanej komunikácie; k širšiemu spracovaniu skupiny systémov pozri kapitolu 2, poznámku 8. Obšírnejšie sa Signalu venuje kapitola 17.

[8] O bezpečnostnom modeli Toru a jeho obmedzeniach pozri Roger Dingledine, Nick Mathewson a Paul Syverson, ”Tor: The Second-Generation Onion Router,” USENIX Security Symposium (2004). Priebežné analýzy pozri na `https://blog.torproject.org/`.

[9] O bezpečnostnom modeli Bitcoinu pozri Voskuil, *Cryptoeconomics* (citované v poznámke 1 vyššie), najmä oddiely o bezpečnostných modeloch a ekonomických predpokladoch. K širšiemu rakúsko-praxeologickému spracovaniu *Cryptoeconomics* pozri kapitolu 2, poznámku 5.

[10] Randall Munroe, ”Security,” *xkcd* #538, `https://xkcd.com/538/`. Komiks zobrazuje útočníka, ktorý obíde silné šifrovanie fyzickým donútením („mlátiť ho týmto kľúčom za päť dolárov, kým nepovie heslo“; angl. ”hit him with this $5 wrench until he tells us the password”). Je to kanonická ilustrácia toho, že kryptografický odpor sa nevzťahuje na model hrozieb s fyzickou silou. Starším synonymom v kryptografickej literatúre je výraz ”rubber-hose cryptanalysis” (kryptoanalýza gumovou hadicou).

[11] O zlyhaniach implementácií a ich poučeniach pozri Ross Anderson, *Security Engineering*, 3. vyd. (Indianapolis: Wiley, 2020), najmä kapitoly o zlyhaniach pri implementácii kryptografie.

[13] O probléme diskrétneho logaritmu ako kryptografickom predpoklade o náročnosti pozri Whitfield Diffie a Martin E. Hellman, ”New Directions in Cryptography,” *IEEE Transactions on Information Theory* 22, č. 6 (1976): 644–654. Táto zakladajúca práca zaviedla kryptografiu s verejným kľúčom využitím asymetrie medzi výpočtom diskrétnych logaritmov a ich obrátením a položila výpočtový základ, ktorý neskôr rozšírili systémy RSA a eliptických kriviek.

[14] R. L. Rivest, A. Shamir a L. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," *Communications of the ACM* 21, č. 2 (1978): 120–126. Pôvodná práca o RSA; bezpečnosť systému stojí na predpoklade o náročnosti rozkladu celých čísel, ktorý opisuje okolitý odsek.

[15] Victor S. Miller, "Use of Elliptic Curves in Cryptography," in *Advances in Cryptology - CRYPTO '85*, Lecture Notes in Computer Science 218 (Berlin: Springer, 1986), 417–426; Neal Koblitz, "Elliptic Curve Cryptosystems," *Mathematics of Computation* 48, č. 177 (1987): 203–209. Tieto dve nezávislé práce zaviedli kryptografiu na eliptických krivkách; ECC dosahuje rovnakú bezpečnosť ako RSA s kratšími kľúčmi, a preto je dominantným primitívom s verejným kľúčom v moderných nasadeniach vrátane krivky secp256k1, ktorú používa Bitcoin.

[16] A. K. Lenstra, H. W. Lenstra Jr., M. S. Manasse a J. M. Pollard, "The Number Field Sieve," in *Proceedings of the 22nd Annual ACM Symposium on Theory of Computing* (1990), 564–572. Všeobecné číselné sito je najúčinnejší známy klasický algoritmus na rozklad veľkých celých čísel, beží v subexponenciálnom čase; jeho vývoj si vyžiadal výrazné zvýšenie odporúčaných dĺžok kľúčov RSA a ukazuje, ako môže algoritmický pokrok narúšať predpokladané bezpečnostné rezervy.

[17] O známej útočnej ploche Toru pozri Steven J. Murdoch a George Danezis, "Low-Cost Traffic Analysis of Tor," *Proceedings of the 2005 IEEE Symposium on Security and Privacy* (2005), 183–195; a Aaron Johnson et al., "Users Get Routed: Traffic Correlation on Tor by Realistic Adversaries," *Proceedings of the 2013 ACM SIGSAC Conference on Computer and Communications Security* (2013), 337–348. Tieto práce dokumentujú útoky časovou koreláciou a útoky cez výstupné uzly, ktoré zostávajú hlavnými praktickými obmedzeniami modelu anonymity Toru proti protivníkom s veľkými zdrojmi.

[12] Ďalšie čítanie o odpore, bezpečnosti a rozhraní medzi kryptografiou a politikou. O teoretických základoch výpočtovej bezpečnosti je štandardom na postgraduálnej úrovni Katz a Lindell, *Introduction to Modern Cryptography* (citované v poznámke 3 vyššie). Pre praktický úvod (Ferguson, Schneier a Kohno) a kanonické spracovanie kryptografie a schopností štátu (Diffie a Landau, *Privacy on the Line*; Landau, *Listening In*) pozri kapitolu 1, poznámku 5. K myšlienkovému zdôvodneniu, že kryptografia mení politickú ekonómiu, je primárnym zdrojom, rozsiahlym cypherpunkovým vymedzením, už citovaný *Cyphernomicon* Timothyho C. Maya. Pre verziu špecifickú pre kryptomeny pozri Voskuil, *Cryptoeconomics* (citované v poznámke 1 vyššie), a širšie rakúsko-praxeologické spracovanie v kapitole 2, poznámke 5. O odpore ako o širšom jave mimo kryptografie je štandardom korpus Jamesa C. Scotta: k *Seeing Like a State* (Yale University Press, 1998) pozri kapitolu 1, poznámku 6; širší korpus siaha cez *Weapons of the Weak: Everyday Forms of Peasant Resistance* (Yale University Press, 1985) a *The Art of Not Being Governed: An Anarchist History of Upland Southeast Asia* (Yale University Press, 2009). K rakúsko-libertariánskej politickej teórii odporu sú kanonickými textami Murray N. Rothbard, *For a New Liberty: The Libertarian Manifesto* (Macmillan, 1973), a *The Ethics of Liberty* (citované v kapitole 2, poznámke 3), a Hans-Hermann Hoppe, *Democracy: The God That Failed: The Economics and Politics of Monarchy, Democracy, and Natural Order* (Transaction, 2001). K analytickej obrane filozofického anarchizmu spoza rakúskej tradície pozri Michael Huemer, *The Problem of Political Authority* (citované v kapitole 4, poznámke 13). O postkvantovom prechode a jeho strategických dôsledkoch Michele Mosca, "Cybersecurity in an Era with Quantum Computers: Will We Be Ready?" *IEEE Security & Privacy* 16, č. 5 (2018): 38–41, `https://arxiv.org/abs/1512.04202`, zavádza rámec „Moscovej nerovnosti"; prebiehajúci proces NIST na `https://csrc.nist.gov/projects/post-quantum-cryptography` sleduje štandardizáciu.

ČASŤ III

EKONOMICKÉ ZÁKLADY

6

INFORMÁCIA, VZÁCNOSŤ A VLASTNÍCTVO

„Ak príroda urobila niečo menej spôsobilým na výlučné vlastníctvo než čokoľvek iné, je to dej myslenia, ktorému hovoríme idea. Jednotlivec ju môže vlastniť výlučne, kým si ju necháva pre seba. Hneď ako sa však prezradí, vtlačí sa do vlastníctva každého a ten, kto ju prijal, sa jej už nemôže zbaviť.“

Thomas Jefferson, list Isaacovi McPhersonovi (1813)[1]

Úvod

Aký je vzťah medzi informáciou a vlastníctvom? Odpoveď určuje, ako sa dá chrániť súkromie. Ak môže byť informačný obsah vlastníctvom, súkromie by sa mohlo chrániť vlastníckymi právami k samotnej informácii. Ak informačný obsah vlastníctvom byť nemôže, súkromie treba chrániť inými prostriedkami.

Rámec poskytuje analýza Stephana Kinsellu.[2] Vlastnícke práva sa vzťahujú len na vzácne zdroje, teda také, pri ktorých užívanie jednou stranou vylučuje užívanie druhou. Informačný obsah, ktorý je raz známy, môže neobmedzený počet strán používať súčasne a bez vyčerpania. Je nevzácny, a preto nemôže byť vlastníctvom.

Táto kapitola nasleduje Kinsellov rámec, lebo je priamou aplikáciou teórie vlastníctva založenej na vzácnosti, ktorú rakúska ekonómia rozvíjala od Rothbarda. Nie je to jediný rakúsko-libertariánsky postoj k „duševnému vlastníctvu“ a kapitola to otvorene hovorí. Murray Rothbard v knihe *Človek, ekonomika a štát* (angl. *Man, Economy, and State*) posudzoval patent a autorské právo osobitne. Patent udeľuje monopol, ktorý potláča nezá-

vislých vynálezcov, a je nelegitímny. Autorské právo v podobe zmluvnej výhrady autora voči kupujúcim (pôvodný význam pred moderným zákonným režimom) je v zásade legitímne ako zmluva, hoci nezaväzuje tretie strany, ktoré s ním nikdy nesúhlasili. Kinsellov neskorší rozvoj Rothbardovu analýzu spresňuje. Ukazuje, že zmluvná cesta v skutočnosti nedosiahne to, čo autorský zákon dosahuje v praxi: zaväzovanie tých, ktorí nie sú stranou zmluvy, kontrolu fyzických nosičov v ďalšom obehu a pretrvávanie aj po tom, čo sa dielo stane voľným (public domain). Rovnakú logiku založenú na vzácnosti zároveň rozširuje na všetky druhy informačných monopolov udelených štátom. Oba postoje sa zhodujú v tom, čo je pre súkromie podstatné: sebavlastníctvo pokrýva telo a myseľ, fyzické vlastníctvo pokrýva zariadenia a priestory a zmluva vytvára vymáhateľnú dôvernosť medzi stranami, ktoré s ňou súhlasia.[3] Kapitola rozvíja Kinsellovu verziu, lebo je presnejšia v tom, čo zmluva dokáže a čo nie. Argument o súkromí, ktorý kniha obhajuje, však obstojí v oboch podobách.[4]

Súkromie tým nezostáva bez ochrany. Chráni ho sebavlastníctvo (kontrola nad vlastným telom a mysľou), fyzické vlastníctvo (zariadenia, písomnosti, domov) a zmluva (dohody o dôvernosti). Tieto mechanizmy chránia súkromie bez toho, aby považovali informačný obsah za vlastníctvo. Pochopiť tento rozdiel je nevyhnutné pre jasnú analýzu ekonómie súkromia.

6.1 Vzácnosť ako základ vlastníctva

Prečo existujú vlastnícke práva

Vlastnícke práva existujú, aby riešili konflikty o vzácne zdroje. Vzácny zdroj je taký, ktorý nemôže, keď ho používa jedna strana, súčasne rovnakým spôsobom používať iná. Pôda, jedlo, nástroje a telá sú vzácne: moje užívanie tohto jablka vylučuje, aby to isté jablko súčasne užíval niekto iný.

Vzácnosť vytvára možnosť konfliktu. Ak viacero strán chce rovnaký zdroj používať nezlučiteľnými spôsobmi, musia sa buď o neho biť, alebo sa dohodnúť na pravidlách prideľovania. Vlastnícke práva sú pravidlá prideľovania, ktoré určitým stranám prisudzujú kontrolu nad zdrojmi. Ekonómovia nazývajú túto vlastnosť fyzických statkov rivalita: užívanie jednou stranou vylučuje užívanie druhou. Informácia je nerivalitná. Keď sa niekto dozvie to, čo viem ja, moje poznanie sa tým nezmenší, a preto sa na ňu rovnaká logika vlastníctva nevzťahuje.

Bez vzácnosti vlastnícke práva nemajú zmysel. Ak môže zdroj súčasne používať každý bez konfliktu, pravidlá prideľovania netreba.[5]

Rámec spresňuje ešte jeden rozdiel. Držba je vec faktu: kto zdroj práve ovláda. Vlastníctvo je vec normy: kto má právo ho ovládať. Rímske právo aj anglo-americké zvykové právo (common law) tento rozdiel poznajú a Kinsella ho robí základným.[6] Vlastnícke práva poskytujú držbe norma-

tívnu oporu a odpovedajú na otázku, kto má v spore lepší nárok. Držba je deskriptívna, vlastníctvo je preskriptívne. Pravidlá nadobúdania, o ktorých je reč nižšie, prideľujú vlastníctvo. Nepopisujú, kto práve vec drží.

Fyzická vzácnosť a umelá vzácnosť

Fyzická vzácnosť je vlastná samotnému zdroju. Pôda je vzácna, lebo obsadenie jedného miesta vylučuje, aby ho súčasne obsadil niekto iný. Jablká sú vzácne, lebo keď niekto zje jablko, nikto iný už to isté nezje.

Umelú vzácnosť vnucuje vonkajšia sila zdrojom, ktoré nie sú vzácne od prírody. Ak napíšem báseň a niekto iný si ju zapamätá, môže ju recitovať bez toho, aby tým zmenšil moju schopnosť recitovať ju. Báseň ako vzor slov je nevzácna. Ak mi však štát udelí „autorské právo“ vynucované násilím, umelo obmedzí užívanie nevzácneho zdroja inými.

Vlastnícke práva k fyzicky vzácnym zdrojom riešia skutočné konflikty. „Vlastnícke práva“ k umelo vzácnym zdrojom vytvárajú konflikty, ktoré by inak nevznikli. Jednej strane dávajú kontrolu nad tým, ako smú iní používať svoje vlastné, legitímne nadobudnuté fyzické zdroje.

6.2 „Duševné vlastníctvo`` ako agresia

Oddiel 6.1 ukázal, že vlastnícke práva existujú na riešenie konfliktov o vzácne zdroje a že informačný obsah je nevzácny. Z toho vyplýva, že „duševné vlastníctvo“ vytvára umelú vzácnosť štátnym násilím a porušuje skutočné vlastnícke práva k fyzickým zdrojom.

Zoberme jednoduchý prípad. Alice vymyslí nový návrh pasce na myši. Bob nezávisle vyvinie ten istý návrh alebo sa o ňom dozvie a zrealizuje ho z vlastných materiálov.

Ak má Alice k návrhu „duševné vlastníctvo“, môže použiť štátne násilie, aby Bobovi zabránila používať vlastné materiály (drevo, pružiny, drôt) v určitých konfiguráciách. Štát potrestá Boba za to, že usporiadal svoj majetok spôsobom, ktorý sa Alice nepáči.

Takýto nárok je agresia. Bob neurobil nič Alice ani jej majetku. Použil vlastný majetok. Nárok „duševného vlastníctva“ je nárok, že Alice môže ovládať, ako Bob používa Bobov majetok, a štátne násilie ho podopiera.

Príklad patentu

Patenty udeľujú monopoly na myšlienky. Držiteľ patentu môže zabrániť komukoľvek inému v realizácii patentovanej myšlienky, aj keď na ňu prišiel nezávisle.

Držiteľ patentu ovláda, ako môžu iní používať svoj vlastný fyzický majetok. Nezávislí vynálezcovia sa nemajú ako brániť, lebo vyhráva ten, kto podal prihlášku skôr. Konkurenciu obmedzuje právne privilégium, nie lepšia služba. Inovácia sa zdaňuje, pretože každý, kto patentované myšlienky zlepšuje, musí platiť tribút.

Patenty sú monopolné privilégiá udelené štátom a vynucované agresiou voči skutočnému majetku iných.[7]

Príklad autorského práva

Autorské právo dáva kontrolu nad kopírovaním vzorov. Jeho držiteľ môže iným zabrániť, aby usporiadali svoj vlastný fyzický majetok (papier, atrament, pevné disky) v určitých konfiguráciách.

Na vlastný papier nemožno vytlačiť určité vzory, na vlastný pevný disk uložiť určité bitové vzory ani v obchodnom prostredí vysloviť určité postupnosti slov. Fyzický majetok človeka ovládajú cudzie nároky na vzory.

Autorské právo funguje ako cenzúra podopretá štátnym násilím: obmedzuje, čo smie človek robiť so svojím fyzickým majetkom, na základe podobnosti s tým, čo si niekto iný nárokuje ako svoj vzor.

„Duševné vlastníctvo`` ako nedobrovoľné negatívne vecné bremeno

Právny názov toho, čo štát dáva držiteľovi „duševného vlastníctva", robí rámec presným. Negatívne vecné bremeno (negative servitude, alebo easement) je majetkový záujem, ktorý dovoľuje jednej strane zabrániť vlastníkovi iného zdroja v jeho používaní určitými spôsobmi. Dobrovoľné negatívne vecné bremená sú bežné a bezproblémové: reštriktívna zmluva v obytnej štvrti, ktorá zakazuje komerčné využitie, je negatívne vecné bremeno, ktoré prijíma každý kupujúci pri kúpe. Patent a autorské právo však vytvárajú *nedobrovoľné* negatívne vecné bremeno, ktoré štát udelí bez súhlasu vlastníka, ktorého užívanie obmedzuje. Nezávislý vynálezca nikdy nesúhlasil, že sa zdrží usporiadania vlastných materiálov v patentovanej konfigurácii. Čitateľ, ktorý si kúpi knihu, nikdy nesúhlasil, že sa zdrží usporiadania bitov na vlastnom pevnom disku podľa chráneného vzoru. Držiteľ „duševného vlastníctva" štátnym udelením získava moc spoluvlastníka nad majetkom, ktorý nikdy nevlastnil ani nekúpil.[8]

Tvorba je zdrojom bohatstva, nie vlastníctva

Chyba, ktorá sa pod tým všetkým stále vracia, je lockeovská intuícia, že tvorba je zdrojom vlastníckych práv, teda myšlienka, že zmiešaním svojej práce s niečím človek získava vlastníctvo k tomu. Tvorba je zdrojom *bohatstva*, nie zdrojom *vlastníctva*. Každý akt tvorby premieňa materiály, ktoré už niekto vlastní, na hodnotnejšiu výslednú konfiguráciu. Vlastník vstupov je vlastníkom výstupov preto, že vlastnil vstupy, nie preto, že výstupy vytvoril. Zamestnanci v továrni vytvárajú výrobky a nevlastnia ich. Prvotné privlastnenie, zmluvný prevod a náprava sú tri zdroje vlastníckych práv k vzácnym vonkajším zdrojom. Sebavlastníctvo tela zakladá práva k vlastnej osobe. Tvorba nie je štvrtým zdrojom. Intuícia, že tvorcovia by mali vlastniť svoje výtvory, je duch, ktorý oživuje obhajobu „duševného vlastníctva", a treba ju výslovne odmietnuť. Užitočné myšlienky, pôvod-

né vyjadrenia a rozpoznateľné značky sú produkty tvorby, ktoré zvyšujú bohatstvo vo svete, a nijaké z nich nie je vlastníctvom.[9]

6.3 Obsah a nosič: rozhodujúci rozdiel

Informácia existuje na fyzických nosičoch

Informácia je vždy zapísaná na fyzickom nosiči: kniha je papier a atrament usporiadané do vzorov, pevný disk obsahuje magnetické domény v určitých konfiguráciách a mozog obsahuje neurónové vzory, ktoré kódujú spomienky a vedomosti.

Nosiče (papier, pevný disk, mozog) sú vzácne fyzické predmety. Obsah (vzory, informácie, myšlienky) je nevzácny.

Vlastnícke práva sa vzťahujú na nosič, nie na obsah

Papier, ktorý človek vlastní, môže použiť na čokoľvek: popísať ho, spáliť, poskladať z neho klobúk. Vlastnícke práva sú úplné.

Pevný disk, ktorý človek vlastní, môže uložiť akékoľvek bitové vzory. Vlastnícke práva zahŕňajú aj rozhodovanie o tom, v akej konfigurácii sa jeho majetok nachádza.

Keď však človek obsah oznámi inému, nemôže ovládať, čo ten robí so svojimi nosičmi. Ak mi niekto prezradí tajomstvo a ja si ho zapíšem do zápisníka, nemá k môjmu zápisníku nijaký vlastnícky nárok. Obsah, ktorý je teraz v mojej mysli a v mojom zápisníku, nie je jeho majetok.

Čo by znamenalo „vlastniť informáciu``

Keby bol informačný obsah vlastníctvom, vyučovanie by bolo prevodom majetku (strácajú učitelia vedomosti, keď sa učia žiaci?), učenie by bolo nadobúdaním majetku (od koho? s akým súhlasom?), pamäť by bola uložením cudzieho majetku (môžu si majitelia vyžiadať jeho vymazanie?) a rozhovor by bol výmenou majetku (sledovať, komu patrí ktorá prediskutovaná myšlienka?).

Tieto absurdity ukazujú, že informácia ako vlastníctvo je nekoherentná. Poznanie nie je vec, ktorú možno vlastniť, stratiť, ukradnúť alebo previesť tak, ako sa to dá s fyzickými predmetmi.

Zámena s „krádežou``

Keď niekto skopíruje cudzí súbor bez dovolenia, „ukradol“ ho? Nie. Majiteľovi súbor zostáva, nič mu nebolo odňaté a jeho majetok je nedotknutý.

Stalo sa to, že kopírujúci vytvoril nové vzory na vlastných nosičoch, vzory podobné vzorom na nosičoch majiteľa. To môže porušiť zmluvu, ak mali strany dohodu. Môže to byť zlé aj z iných dôvodov. Krádež to však nie je, lebo sa nič nevzalo.

Reči o „kradnutí“ myšlienok mätú, lebo prenášajú pojmy vlastníctva tam, kde sa nehodia.

6.4 Ako sa chráni súkromie

Ak informačný obsah nemôže byť vlastníctvom, ako sa chráni súkromie? Tromi mechanizmami, ktoré nepotrebujú tvrdenia o informácii ako vlastníctve.

Sebavlastníctvo

Kapitola 4 ukázala, že sebavlastníctvo vyplýva z etiky argumentácie. Sebavlastníctvo zakladá nároky na duševné súkromie a telesnú integritu aj na kontrolu nad tým, čo človek vyjadruje. Myšlienky patria tomu, kto ich myslí, a ich vyťahovanie bez súhlasu je s týmto nárokom v napätí. To isté platí pre telo: aj neželané prehliadanie či sledovanie je s týmto nárokom v napätí. Čo oznámiť, určuje človek sám a mlčanie zostáva v jeho moci.

Sebavlastníctvo chráni súkromie pri zdroji. Kým sa informácia neoznámi, existuje len v mysli a tele, ktoré patria človeku.

Fyzické vlastníctvo

Zariadenia a písomnosti, dom a pevné disky patria ich majiteľovi. Vlastnícke práva k týmto veciam zahŕňajú rozhodovanie o tom, kto môže vstúpiť, a právo odmietnuť prehliadku bez súhlasu. Majiteľ určuje, ako je jeho majetok nakonfigurovaný, vrátane toho, aké údaje zariadenia ukladajú.

Fyzické vlastnícke práva chránia informáciu tým, že chránia nosiče, na ktorých existuje. Zašifrovaný pevný disk je majetok svojho majiteľa. Iní nemajú automatické právo na prístup k nemu a každý nárok na vynútené dešifrovanie by potreboval samostatné zdôvodnenie mimo samotného vlastníckeho nároku.

Zmluva

Dobrovoľné dohody môžu vytvárať vymáhateľné záväzky.[10] Dohody o mlčanlivosti (NDA) zaväzujú strany, aby určité informácie neodhaľovali. Pracovné alebo servisné zmluvy môžu obsahovať doložky o dôvernosti. Advokáti, lekári a duchovní pracujú podľa tradičného profesijného tajomstva, ktoré vyžaduje dôvernosť.

Zmluva chráni súkromie dobrovoľným záväzkom. Kto sa dohodne, že informácie zachová v dôvernosti, je touto dohodou viazaný.

Porušenie dohody o dôvernosti je viac než „porušenie sľubu“. Ak sa platí s podmienkou utajenia, prezradenie tajomstva môže znamenať prijatie platby pod falošnou zámienkou. Peniaze sa previedli podmienene a prijať platbu, pričom sa podmienka poruší, je prinajmenšom podvod, v niektorých prípadoch sa to dá posúdiť ako krádež podmieneného prevodu, nie ako obyčajné porušenie abstraktného záväzku. Porušenia zmlúv majú zu-

by, lebo sa týkajú prevodov vzácnych zdrojov uskutočnených za určitých podmienok.

Zmluva viaže strany, ktoré s ňou súhlasili. Tretie strany, ktoré nikdy nesúhlasili, neviaže. Zamestnanec viazaný dohodou o mlčanlivosti je ňou viazaný, ale cudzí človek, ktorý nájde dokument na chodníku, podľa nej žiaden záväzok nemá. Držiteľ licencie, ktorý prijme podmienky používania, je nimi viazaný, no priateľ, ktorý si jeho kópiu požičia, je viazaný len tou samostatnou dohodou, ak nejakú uzavrel. Dosah zmluvy je dosah súhlasu a súhlas sa na ľudí, ktorí zmluvu nepodpísali, nešíri. Práve tým sa zmluvná cesta líši od vlastníckeho nároku na samotnú informáciu: vlastnícky nárok by dosiahol na každého, aj na nezávislých objaviteľov a na ďalších, ktorí nie sú stranou zmluvy, zatiaľ čo zmluva dosahuje len na tých, ktorí s ňou súhlasili. Kniha pokladá toto obmedzenie za vlastnosť rámca, za čestné vyúčtovanie toho, čo dobrovoľná dohoda dokáže a čo nie.

Obchodné tajomstvá

Obchodné tajomstvo je najčistejší prípad na ukážku toho, čo rámec chráni a čo nie, pretože oddeľuje otázku od sporov o patenty a autorské právo.

Predstavme si výrobcu nápojov s receptom, ktorý by jeho konkurenti radi mali. Recept chráni kombinácia opatrení: samotný dokument je fyzicky zabezpečený, zamestnanci s prístupom podpísali dohody o mlčanlivosti, firma veľa investovala do stavby trezorov a preverovania personálu a živí sa značkou a výrobnou kapacitou, ktorú okolo tajomstva vybudovala. Ani jedno z týchto opatrení nie je vlastnícky nárok na samotný vzor receptu. Sú to vlastnícke nároky na vzácne fyzické zdroje (dokument, trezor, výrobný závod) a zmluvné nároky voči stranám, ktoré s dôvernosťou súhlasili. Kombinácia stačí na to, aby sa tajomstvo v praxi udržalo dlhodobo.

Predpovede rámca pre okrajové prípady sú jasné. Zlodej, ktorý sa vlámal do trezora, sa dopustil agresie voči fyzickému majetku a zodpovedá z toho dôvodu. Zamestnanec, ktorý recept prezradil v rozpore s dohodou o mlčanlivosti, prijal platbu podmienene a dopustil sa podvodu alebo porušenia zmluvy. Chemik, ktorý kúpi fľašu z police a spätným inžinierstvom zistí zloženie, sa agresie nedopúšťa: použil vlastné vybavenie a vlastnú myseľ a dospel k vzoru, ktorý sa náhodou zhoduje s firemným. Firme nič nedlhuje. Nezávislý vynálezca, ktorý dospeje k rovnakému receptu bez toho, aby sa kedy stretol s produktom firmy, sa z rovnakého dôvodu agresie nedopúšťa. Tieto predpovede zodpovedajú rozumnej libertariánskej intuícii a zodpovedajú Rothbardovmu postoju k patentu v knihe *Človek, ekonomika a štát*: nezávislý objav nie je krádež a spätné inžinierstvo legitímne nadobudnutého fyzického majetku nie je krádež tiež.

Postavenie držiteľa obchodného tajomstva je teda silné aj bez vlastníctva vzoru. Ochranu mu dáva fyzické zabezpečenie nosičov, zmluvné záväzky ľudí s prístupom a práca a kapitál vynaložené na to, aby tajomstvo

zostalo v úzkom kruhu. Držiteľ nemá nárok voči celému svetu. Táto absencia je celý obsah sporu s patentovým právom. Práve v tomto postoji sa Rothbard a Kinsella zbiehajú a rovnaký postoj rozvíja aj rámec, ktorý kniha nasleduje.

Medzi týmito tromi mechanizmami nie sú vlastnícke práva k samotnému informačnému obsahu, nároky voči ľuďom, ktorí nezávisle objavia tú istú informáciu, právo brániť iným v určitom využívaní ich vlastného majetku ani kontrola nad informáciou po dobrovoľnom a bezpodmienečnom odhalení. Ak niekto prezradí tajomstvo cudziemu človeku bez dohody o dôvernosti, nemá vlastnícky nárok, ktorým by mu mohol zabrániť v ďalšom šírení. Odhaľovanie mal pod kontrolou (sebavlastníctvo) a mohol mlčať. Keď sa rozhodol prehovoriť, nemôže si nárokovať vlastnícke práva k vzorom, ktoré sú teraz v cudzej mysli.

6.5 Dôsledky pre analýzu súkromia

Čo znamená „porušenie súkromia``

Podľa tohto rámca nie je porušením súkromia to, že niekto vie niečo, o čom si neželáme, aby to vedel. To môže byť nešťastné, ale nie je to porušenie. V štandardnom prípade je porušením súkromia to, že niekto získa informáciu agresiou voči osobe alebo majetku.

Príklady porušenia: násilné vymáhanie informácií mučením alebo vynúteným svedectvom, vniknutie za účelom získania informácií vlámaním do domu alebo zariadenia, porušenie zmluvy o dôvernosti, ktoré je krádežou podmienenej platby, a podvod, pri ktorom sa informácie získavajú vydávaním sa za niekoho iného alebo klamaním.

Príklady, ktoré porušením nie sú: pozorovanie niekoho na verejnosti, prijatie informácií, ktoré niekto zdieľal dobrovoľne, nezávislé objavenie informácií a zistenie informácií od niekoho, komu boli povedané bez dohody o dôvernosti.

Povesť nie je vlastníctvo

Súvisiaci prípad, ktorý rámec vylučuje, je povesť: povesť nie je vlastníctvo. Povesť je to, čo si o človeku myslia iní. Existuje v ich mysliach a na ich nosičoch, nie v nijakom zdroji, ktorý by človek, o ktorom sa hovorí, vlastnil. Právo proti ohováraniu, podobne ako právo ochranných známok a autorské právo, si nárokuje záujem podobný vlastníctvu na niečom nevzácnom, tu na tom, čomu iní veria a čomu publikum venuje pozornosť. Rámec zaobchádza s nepravdivou rečou rovnako ako s pravdivou: legitímnou odpoveďou je protirečenie, odopretie priazne a spoločenské odmietnutie. Tam, kde reč zohráva príčinnú úlohu v skutočnej agresii (svedok, ktorý pred súdom luže, aby poslal obžalovaného do väzenia, rozkaz na útok, podnecovanie davu k lynčovaniu), zodpovedá rečník za agresiu, ktorú je-

ho reč spôsobí, nie za poškodenie povesti obete ako takej. Platí rovnaký záver, ku ktorému dospela táto kapitola pri patentoch a autorských právach: štátne vynucovanie práv na povesť proti pokojnej reči je agresia, nie ochrana.[11]

Úloha technológie

Technológia mení, čo je možné, nie čo je legitímne.

Šifrovanie chráni fyzický majetok (zariadenia) pred prehliadkou. Je to výkon vlastníckych práv, nie nové právo vytvorené technológiou.

Anonymné siete chránia sebavlastníctvo tým, že umožňujú komunikáciu bez odhalenia identity. Rozširujú prirodzené súkromie osobných hotovostných transakcií na digitálne prostredie.

Technológia súkromia uskutočňuje existujúce práva. Nevytvára nové práva ani nové kategórie vlastníctva.

Slobodný softvér s otvoreným zdrojovým kódom ako pracovný príklad

Slobodný softvér s otvoreným zdrojovým kódom (FOSS)[14] je trvalým dôkazom, že rámec nevzácnosti opisuje fungujúcu ekonomiku. Zdrojový kód je vzor. Keď sa uvoľní pod permisívnou licenciou alebo licenciou copyleft, môže ho kopírovať, upravovať a ďalej šíriť ktokoľvek, kto má fyzický nosič, na ktorý ho uloží. Nikto sa nedovoláva vynucovania umelej vzácnosti a softvér sa napriek tomu píše, udržiava a zlepšuje v rozsahu, v akom dnes beží väčšina serverov, vstavaných zariadení a kryptografickej infraštruktúry na svete. Linux,[15] OpenSSH, OpenSSL, GnuPG, Bitcoin Core, Tor,[16] Signal[17] a kompilačné nástroje, ktoré ich zostavujú, sú všetko príklady hodnotného softvéru vzniknutého bez predpokladov o patentoch a autorskom práve, ktoré hlavný prúd ekonómie pokladá za nevyhnutné podmienky tvorby softvéru.

Príjmové modely, ktoré túto prácu podporujú, sú s rámcom v súlade. Vývojári sú platení za vzácne vstupy: svoj čas, pozornosť, odbornosť a povesť, že dodávajú fungujúci kód. Firmy platia za zmluvy o podpore, vývoj na mieru, hostované inštancie a hardvér, na ktorom softvér beží. Nadácie vyberajú dobrovoľné príspevky od používateľov, ktorým práca prospieva a ktorí chcú, aby pokračovala. Nijaké z týchto usporiadaní nevyžaduje vlastnícke nároky na samotné vzory. Vyžadujú bežné zmluvy o vzácnej práci a službách, ktoré vzory vytvárajú a udržiavajú. Licencia pripojená ku kódu je vzdanie sa určitých privilégií udelených štátom, nie tvrdenie o vlastníctve obsahu.

Rovnakej logike zodpovedajú aj rozšírené licencie. Permisívne licencie (MIT, BSD, Apache) povoľujú akékoľvek ďalšie použitie a opierajú sa o základný fakt, že obsah nie je vlastníctvo. Autorskoprávne privilégium udelené štátom sa úplne vzdávajú. Licencie copyleft (GPL, AGPL)[18] používajú autorskoprávne privilégium nástrojovo: podmienené udelenie vyža-

duje, aby ďalší distribútori rozšírili tie isté slobody na svojich používateľov, takže umelú vzácnosť nemožno neskôr v dodávateľskom reťazci opäť uzavrieť. Obe stratégie pokladajú autorské právo za privilégium, ktoré treba neutralizovať, a obe vytvárajú softvér s dlhšou životnosťou, širšou možnosťou auditu a väčšou odolnosťou voči ovládnutiu zo strany dodávateľa než uzavreté alternatívy, o ktorých kritici rámca predpovedali, že ich prekonajú.

Praktický dôsledok pre súkromie je priamy. Každý základný prvok dôležitý pre súkromie, na ktorom sa kniha opiera, vrátane kryptografických knižníc v kapitole 14, anonymných sietí v kapitole 17, implementácií Bitcoinu v kapitolách 18 až 20, nástrojov na dôkazy s nulovou znalosťou v kapitole 15 a prostredí pre bezpečný výpočet v kapitole 16, je slobodný softvér. Ich auditovateľnosť je to, čo robí tvrdenia o odpore z kapitoly 5 vôbec dôveryhodnými. Nástroj na ochranu súkromia so zatvoreným zdrojovým kódom je nástroj, ktorého model protivníka zahŕňa jeho vlastného autora. Slobodný softvér je prevádzkové prostredie, v ktorom technické argumenty knihy platia, a jeho existencia je ekonomickým potvrdením rámca nevzácnosti rozvinutého v tejto kapitole.

„Sledovací kapitalizmus`` a ekonómia informácií[19]

Či firmy, ktoré zbierajú údaje o používateľoch, porušujú súkromie, závisí od podmienok. Ak používatelia so zberom údajov súhlasia (hoci nerozumne) výmenou za služby, k porušeniu nedochádza: je to dobrovoľná výmena. Výmena môže byť pošetilá a podmienky môžu byť pochované v hustých zmluvách, ale súhlas bol daný.

Ak firmy zbierajú údaje bez súhlasu alebo klamaním, ktoré presahuje rozsah dohôd, môže ísť o porušenie zmluvy alebo o podvod.

Zozbierané údaje sú však v držbe firmy a sú uložené na jej nosičoch. Servery vlastní firma. Informačné vzory na týchto serveroch nie sú „majetkom používateľa“, ktorý by si mohol nárokovať späť. Nápravou nadmerného zberu údajov nie sú vlastnícke nároky, ale lepšie zmluvy a konkurencia, ktorá chráni súkromie.[12]

Zhrnutie kapitoly

Vlastnícke práva sa vzťahujú na vzácne zdroje a vzácnosť vytvára konflikty, ktoré majú vlastnícke práva riešiť. Informačný obsah je nevzácny: neobmedzený počet strán môže mať tú istú myšlienku bez konfliktu. Nemôže byť vlastníctvom a mechanizmy, ktorými patenty a autorské práva predstierajú opak, vytvárajú umelú vzácnosť štátnym násilím a dávajú niektorým stranám kontrolu nad tým, ako smú iní usporiadať svoje vlastné fyzické nosiče. To je obmedzenie vynucované agresiou, nie ochrana práv.

Súkromie nepotrebuje informáciu ako vlastníctvo, aby sa dalo obhájiť. Sebavlastníctvo chráni myseľ a telo, fyzické vlastníctvo chráni zariadenia,

písomnosti aj domovy a zmluva vytvára vymáhateľné záväzky dôvernosti dobrovoľnou dohodou. Tieto tri mechanizmy pokrývajú osobu a jej veci, nie abstraktné vzory informácií. Nedosahujú na nezávislých objaviteľov, na ďalšie používanie cudzieho majetku ani na informácie dobrovoľne a bezpodmienečne odhalené, a ani nemajú: rámec odmieta nároky na vlastníctvo vzorov a vlastníctvo obmedzuje na vzácne veci. Slobodný softvér s otvoreným zdrojovým kódom je trvalým empirickým potvrdením rámca. Zdrojový kód je nevzácny vzor vydaný pod licenciami, ktoré sa vzdávajú autorskoprávneho privilégia alebo ho neutralizujú, výsledný softvér beží na väčšine kryptografickej a komunikačnej infraštruktúry sveta a vývojári sú odmeňovaní za vzácne vstupy (čas, pozornosť, odbornosť) bežnými zmluvami o práci, podpore a službách.

Táto kapitola stanovuje kritérium, nie jeho úplné použitie. Úplná teória obchodných praktík s údajmi potrebuje spracovanie klamlivého zberu údajov v kapitole 11 a technické prostriedky vynucovania súkromia, keď zmluva sama nestačí, patria do neskorších kapitol o kryptografii, anonymných sieťach a súkromných peňažných vrstvách. Nástroje súkromia, o ktoré sa kniha opiera, uskutočňujú existujúce práva a nasledujúce tri kapitoly prenášajú rámec do výmeny, teórie kapitálu a menovej analýzy.[13]

Poznámky

[1] Thomas Jefferson, letter to Isaac McPherson, August 13, 1813, in *The Writings of Thomas Jefferson*, ed. Andrew A. Lipscomb and Albert E. Bergh (Washington, DC: Thomas Jefferson Memorial Association, 1905), 13:326–338, dostupné v Library of Congress na `https://founders.archives.gov/documents/Jefferson/03-06-02-0322`. List je kanonickým vyjadrením postoja proti „duševnému vlastníctvu" od jedného z predstaviteľov, ktorí ako minister zahraničných vecí a neskôr prezident spravovali americký patentový systém. Moderným prepracovaním Jeffersonovho argumentu je Stephan Kinsella, *Against Intellectual Property* (Auburn, AL: Ludwig von Mises Institute, 2008), 15, ktoré táto kapitola podrobne rozvíja a ktoré poskytuje súčasný teoretický rámec.

[2] Kinsellovo najúplnejšie vyjadrenie je *Against Intellectual Property*, pôvodne vydané ako "Against Intellectual Property," *Journal of Libertarian Studies* 15, č. 2 (2001): 1–53. Pozri tiež jeho blog na `https://stephankinsella.com`, kde nájdete priebežné rozvíjanie a odpovede kritikom.

[3] Rothbardovo spracovanie v *Man, Economy, and State* (citované v kapitole 3, poznámke 3), kapitola 10 §7, rozlišuje patent (monopol udelený štátom, ktorý potláča nezávislých vynálezcov, a preto je nelegitímny) od autorského práva preformulovaného ako zmluvné obmedzenie, ktoré kupujúci slobodne prijímajú (čo je podľa Rothbarda v zásade legitímne ako súkromná dohoda, hoci uznáva, že nezaväzuje tretie strany, ktoré s ním nikdy nesúhlasili). Tento rozdiel bol skutočným intelektuálnym príspevkom a je verziou libertariánsko-rakúskeho postoja, ktorá sa najčastejšie cituje v staršom okruhu okolo Mises Institute. Libbitcoinov "Patent Resistance Principle" Erica Voskuila (`https://github.com/libbitcoin/libbitcoin-system/wiki/Patent-Resistance-Principle`) pracuje v tom istom rothbardovskom registri na úrovni návrhu protokolu: patenty považuje za monopol udelený štátom, ktorý má neutralizovať prístup Bitcoinu založený na otvorených licenciách a predchádzajúcom stave techniky (prior art).

[4] Kinsellov vývoj od *Against Intellectual Property* (2001) spresňuje argument o zmluvnej ceste tým, že ukazuje, čo dodáva a čo nie. Zmluva viaže svoje strany; tretie strany neviaže; ďalší čitatelia knihy nikdy nesúhlasili s podmienkami vydavateľa; preto „autorské právo ako zmluva" nemôže dosiahnuť to, čo v praxi dosahuje zákonné autorské právo (viazanie všetkých tretích strán vrátane tých, ktoré dielo nadobudli bez upozornenia). Kinsellova teória zmluvy ako prevodu titulu, rozvinutá v *The Title-Transfer Theory of Contract* (Papinian Press Working Paper No. 1, 2024), vysvetľuje, prečo záväzky prechádzajú so súhlasom a inak nie. Nezhoda medzi Rothbardovým staršim spracovaním a Kinsellovým neskorším je užšia, než sa zdá: obaja odmietajú patent, obaja pripúšťajú, že zmluva viaže svojich signatárov za podmienok, na ktorých sa dohodli, a obaja popierajú, že zmluvná cesta dáva nárok voči tretím stranám. Argument knihy o súkromí závisí od bodov, ktoré majú oba postoje spoločné, nie od bodov, v ktorých sa rozchádzajú.

[5] O vzácnosti ako základe vlastníctva pozri Murray N. Rothbard, *The Ethics of Liberty* (citované v kapitole 2, poznámke 3), kapitoly 6–8, a Hans-Hermann Hoppe, *A Theory of Socialism and Capitalism* (citované v kapitole 3, poznámke 7), kapitola 2. O ekonómii nerivalitných statkov a empirickom prípade proti intelektuálnemu monopolu pozri Michele Boldrin a David K. Levine, *Against Intellectual Monopoly* (Cambridge: Cambridge University Press, 2008), `https://levine.sscnet.ucla.edu/general/intellectual/against.htm`.

[6] O rozdiele medzi držbou a vlastníctvom pozri Stephan Kinsella, "Another Way to Explain the Problem with IP: Resources v. Knowledge, Ownership v. Possession," *Center for the Study of Innovative Freedom* (February 2017), `https://c4sif.org/2017/02/another-way-to-explain-the-problem-with-ip-resources-v-knowledge-ownership-v-possession/`. Pramene rímskeho práva sú zhrnuté v J. A. C. Thomas, *Textbook of Roman Law* (North-Holland, 1976), §§13–14. O modernom vyjadrení toho istého rozdielu v rámci Kinsellovho rámca pozri *Legal Foundations of a Free Society* (Papinian Press, 2023), Appendix I, o držbe, vlastníctve a práve držať.

[7] O rozdiele medzi vlastníctvom a privilégiom pozri Rothbard, *The Ethics of Liberty* (citované v kapitole 2, poznámke 3), kapitola 10, a Lysander Spooner, "The Law of Intellectual Property" (1855), ktorý obhajoval duševné vlastníctvo, ale osvetľuje sporné otázky.

[8] O „duševnom vlastníctve" ako nedobrovoľnom negatívnom vecnom bremene pozri Stephan Kinsella, "Intellectual Property Rights as Negative Servitudes," *Center for the Study of Innovative Freedom* (June 2011), `https://c4sif.org/2011/06/intellectual-property-rights-as-negative-servitudes/`. Toto zarámovanie je zopakované v Kinsella, *The Problem with Intellectual Property* (Papinian Press Working Paper No. 2, 2025), §III.A.2. O rozdiele medzi dobrovoľnými a nedobrovoľnými vecnými bremenami v majetkovom práve pozri A. N. Yiannopoulos, *Louisiana Civil Law Treatise: Predial Servitudes*, 4. vyd. (West, 2013), a spracovanie v rímskom práve v Justinian, *Digest*, Book 8.

[9] Lockeovská intuícia, že zmiešaním svojej práce so zdrojom človek nadobúda jeho vlastníctvo, je vyložená v John Locke, *Second Treatise of Government* (1689), §27 („Čokoľvek teda vyberie zo stavu, ktorý príroda poskytla a v ktorom to zanechala, s tým zmiešal svoju prácu a pripojil k tomu niečo, čo je jeho vlastné, a tým to robí svojím vlastníctvom"; angl. "Whatsoever then he removes out of the State that Nature hath provided, and left it in, he hath mixed his Labour with, and joyned to it something that is his own, and thereby makes it his Property"); kanonické online vydanie je na `https://www.gutenberg.org/ebooks/7370`. O odmietnutí tvorby ako zdroja vlastníckych práv pozri Stephan Kinsella, "Libertarian Lockean Creationism," *Center for the Study of Innovative Freedom* (May 2025), `https://c4sif.org/2025/05/libertarian-lockean-creationism/`, a Kinsella, *The Problem with Intellectual Property* (Papinian Press, 2025), §III.A.1. Rovnaká

myšlienka je podrobne rozvedená v Kinsella, "Locke on IP; Mises, Rothbard, and Rand on Creation, Production, and 'Rearranging,'" Center for the Study of Innovative Freedom (2010). K širšiemu prípadu, že „duševné vlastníctvo" nie je vlastníctvom vôbec, pozri Kinsella, "IP Is Not (Not) Property" (April 2025), https://c4sif.org/2025/04/ip-is-not-not-property/. Roderick T. Long, "Owning Ideas Means Owning People," *Cato Unbound* (November 19, 2008), http://www.cato-unbound.org/2008/11/19/roderick-long/owning-ideas-means-owning-people, a Longovo skoršie "The Libertarian Case Against Intellectual Property Rights," *Formulations* 3, č. 1 (Autumn 1995), http://freenation.org/a/f3l1.html, rozvíjajú dôsledok, že nároky „duševného vlastníctva" sa dajú vystopovať k nárokom nad inými osobami.

[10] O zmluve ako základe dôvernosti pozri Randy Barnett, "A Consent Theory of Contract," *Columbia Law Review* 86 (1986): 269–321, a Kinsellove rozbory obchodných tajomstiev v *Against Intellectual Property* (citované v poznámke 2 vyššie).

[11] O povesti ako nevlastníctve a nezlučiteľnosti práva proti ohováraniu s rámcom pozri Stephan Kinsella, "Defamation as a Type of Intellectual Property" (citované v kapitole 2, poznámke 10), a skorší príspevok na https://c4sif.org/2024/07/defamation-type-of-ip/. Rámec považuje povesť za obsah presvedčení iných ľudí, ktorý je nevzácny, a teda nevlastniteľný; rovnaká úvaha založená na vzácnosti, ktorá vylučuje patenty a autorské práva, vylučuje aj práva na povesť. Klasické vyjadrenie Murraya N. Rothbarda je "Knowledge, True and False," v *The Ethics of Liberty* (citované v kapitole 2, poznámke 3), kapitola 16, kde Rothbard tvrdí, že žaloby za ohováranie sú nelegitímne, pretože nikto nevlastní obsah myslí iných. Walter Block, "The Slanderer and Libeler," v *Defending the Undefendable* (Fleet Press, 1976), dospieva k rovnakému záveru inou cestou. O prípadoch príčinného podnecovania, ktoré sa niekedy zamieňajú s ohováraním, pozri Kinsella, "Causation and Aggression," v *Legal Foundations of a Free Society* (Papinian Press, 2023), kapitola 8.

[12] O údajoch a súkromí v digitálnom veku z hľadiska vlastníckych práv pozri priebežné písanie Stephana Kinsellu na https://stephankinsella.com (najmä jeho eseje označené "intellectual property" a "Against IP Reader") a Center for the Study of Innovative Freedom na https://c4sif.org. Pozri tiež Kinsella, *You Can't Own Ideas: Essays on Intellectual Property* (Papinian Press, 2023), ktoré zhromažďuje jeho najnovšie spracovania. K rámcu „vlastníctva údajov" osobitne pozri Jaron Lanier, *Who Owns the Future?* (Simon & Schuster, 2013), ktorý z nelibertariánskeho stanoviska obhajuje údaje ako vlastníctvo; Kinsellova odpoveď je v jeho blogovom príspevku "Data Ownership Misses the Point."

[13] Ďalšie čítanie o duševnom vlastníctve z viacerých hľadísk.

[14] Richard Stallman, "What is Free Software?", GNU Project, https://www.gnu.org/philosophy/free-sw.html. Kanonická definícia slobodného softvéru: softvér, ktorý používateľom dáva slobodu spúšťať ho, študovať ho, upravovať ho a ďalej šíriť. Free Software Foundation, ktorú Stallman založil v roku 1985, poskytuje ideovú a právnu infraštruktúru (vrátane GPL) za príkladmi, ktoré tento oddiel uvádza. K širšiemu hnutiu pozri Sam Williams, *Free as in Freedom: Richard Stallman's Crusade for Free Software* (O'Reilly Media, 2002), https://www.oreilly.com/openbook/freedom/. Pojem "open-source" vytvorila v roku 1998 Christine Peterson a formalizovala ho Open Source Initiative; pozri https://opensource.org/history.

[15] Linus Torvalds oznámil jadro Linuxu v príspevku na Usenete z roku 1991 do comp.os.minix: „Robím (slobodný) operačný systém (len ako hobby, nebude veľký a profesionálny ako gnu) pre klony AT s procesormi 386(486)." (angl. "I'm doing a (free) operating system (just a hobby, won't be big and professional like gnu) for 386(486) AT clones.") Zdrojový kód jadra je na https://kernel.org. Linux je paradigmatický

prípad rozsiahlej tvorby softvéru bez vynucovania duševného vlastníctva; o politickej ekonómii jeho vývojového modelu pozri Steven Weber, *The Success of Open Source* (Harvard University Press, 2004).

[16] The Tor Project, `https://www.torproject.org`. Tor (The Onion Router) je slobodná anonymná sieť s otvoreným zdrojovým kódom, ktorá smeruje prevádzku cez rad uzlov (relays) prevádzkovaných dobrovoľníkmi a šifruje každú vrstvu tak, aby žiaden jednotlivý uzol nepoznal zdroj aj cieľ zároveň. Pôvodne ju vyvinulo U.S. Naval Research Laboratory; pozri Roger Dingledine, Nick Mathewson a Paul Syverson, "Tor: The Second-Generation Onion Router," *Proceedings of the 13th USENIX Security Symposium* (2004), `https://svn.torproject.org/svn/projects/design-paper/tor-design.pdf`. Tor je hlavný primitív anonymnej siete, o ktorý sa kapitola 17 tejto knihy opiera.

[17] Signal, `https://signal.org`. Signal je slobodná aplikácia na šifrovanú komunikáciu s otvoreným zdrojovým kódom, ktorú vyvíja Signal Foundation (predtým Open Whisper Systems). Jeho kryptografický protokol – protokol Signal, ktorý spája algoritmus Double Ratchet a dohodu o kľúčoch X3DH – je základom end-to-end šifrovania vo WhatsApp, Google Messages a v niekoľkých ďalších bežných aplikáciách. Pozri Moxie Marlinspike a Trevor Perrin, "The Double Ratchet Algorithm" (2016), `https://signal.org/docs/specifications/doubleratchet/`. Signal sa v tejto knihe uvádza ako príklad infraštruktúry dôležitej pre súkromie, vytvorenej pod licenciami s otvoreným zdrojovým kódom.

[18] Richard Stallman, *GNU General Public License*, verzia 2 (1991) a verzia 3 (2007), `https://www.gnu.org/licenses/gpl-3.0.html`. GPL je zakladajúci nástroj copyleftu: dáva všetky slobody slobodného softvéru a zároveň vyžaduje, aby každé šírené odvodené dielo nieslo rovnakú licenciu, čím bráni ďalším stranám kód uzavrieť. Affero GPL (AGPL) to rozširuje na softvér nasadený v sieti. Právna mechanika je rozobraná v Eben Moglen, "Enforcing the GNU GPL," *Columbia Law School* (2001), `https://moglen.law.columbia.edu/publications/lu-12.html`. Stratégia opísaná v texte – nástrojové používanie autorskoprávneho privilégia udeleného štátom na zabránenie opätovnému uzavretiu – je Stallmanov vynález a je najjasnejším príkladom rámca z oddielu 6.2: použitie existujúceho právneho mechanizmu proti pôvodnému účelu.

[19] Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (PublicAffairs, 2019). Zuboff tvrdí, že platformové firmy vyťažujú „behaviorálny prebytok" (angl. "behavioral surplus") – údaje nad rámec toho, čo je potrebné na poskytovanie služby – a využívajú ho na budovanie predikčných produktov predávaných inzerentom. Nadpis oddielu používa jej pojem; analýza sa líši: kým Zuboff obhajuje nové vlastnícke právo k behaviorálnym údajom, rámec tejto knihy popiera, že vzory údajov môžu byť vlastníctvom, a nápravu hľadá v zmluve a konkurencii, nie v nárokoch na vlastníctvo údajov. Nezhoda je zásadná a je presným bodom, v ktorom sa rakúsky rámec vlastníckych práv a progresívny rámec práv k údajom rozchádzajú. Najnovšie Kinsellove preformulovania rámca: *The Problem with Intellectual Property* (Papinian Press Working Paper No. 2, 2025), `https://stephankinsella.com/wp-content/uploads/publications/kinsella-problem-intellectual-property-v1.1-2025.pdf`, je súčasným spracovaním na úrovni kapitoly knihy, s *The Title-Transfer Theory of Contract* (Papinian Press Working Paper No. 1, 2024) ako sprievodnou prácou o zmluve. Libertariánsko-rakúsky prípad v rozsahu knihy: Stephan Kinsella, *Against Intellectual Property* (Mises Institute, 2008), `http://www.stephankinsella.com/wp-content/uploads/publications/kinsella-against-IP-book.pdf`; jeho *You Can't Own Ideas: Essays on Intellectual Property* (Papinian Press, 2023) zhromažďuje novšie eseje. Kratšie práce priamo relevantné pre zarámovanie tejto kapitoly: Kinsella, "Intellectual Property Rights as Negative Servitudes" (citované v poznámke 8 vyššie),

rozvíja zarámovanie cez negatívne vecné bremeno, o ktoré sa táto kapitola opiera; Kinsella, "Another Way to Explain the Problem with IP" (citované v poznámke 6 vyššie), rozvíja rozdiel medzi držbou a vlastníctvom; Kinsella, "Libertarian Lockean Creationism" (citované v poznámke 9 vyššie), pomenúva opakujúcu sa chybu, ktorú táto kapitola odmieta. Roderick T. Long, "Owning Ideas Means Owning People" (citované v poznámke 9 vyššie), vystopuje nárok „duševného vlastníctva" k dôsledku, že držiteľ vlastní časť iných osôb. O kritike intelektuálneho monopolu z hľadiska hlavného prúdu ekonómie je Michele Boldrin a David K. Levine, *Against Intellectual Monopoly* (citované v poznámke 5 vyššie), empirickým spracovaním. Fritz Machlup, *An Economic Review of the Patent System*, Study No. 15 (U.S. Senate Subcommittee on Patents, 1958), je klasická inštitucionálno-ekonomická štúdia, ktorá dospela k záveru, že patentový systém sa na základe dostupných dôkazov nedá ospravedlniť. Pre historický kontext je štandardnou históriou Adrian Johns, *Piracy: The Intellectual Property Wars from Gutenberg to Gates* (University of Chicago Press, 2009). K autorskému právu osobitne je Lawrence Lessig, *Free Culture: How Big Media Uses Technology and the Law to Lock Down Culture and Control Creativity* (Penguin, 2004), kanonickou kritikou z hlavného progresívneho prúdu; Tom W. Bell, *Intellectual Privilege: Copyright, Common Law, and the Common Good* (Mercatus Center, 2014), je libertariánskejšou verziou. Opačný názor, pre úplnosť: William M. Landes a Richard A. Posner, *The Economic Structure of Intellectual Property Law* (Harvard University Press, 2003), je štandardnou obhajobou existujúceho systému z hľadiska práva a ekonómie.

7
TEÓRIA VÝMENY A SÚKROMIE

„Výmena nie je cieľom sama osebe. Je to prostriedok, ktorým ľudia zlepšujú svoj blahobyt."

Carl Menger, *Principles of Economics* (1871)[1]

Úvod

Výmena je základom spoločenskej spolupráce.[2] Keď ľudia obchodujú, dávajú najavo svoje hodnotenia, koordinujú výrobu a vytvárajú bohatstvo, ktoré by osamotené konanie nikdy nedosiahlo. Cenové signály, ktoré z výmeny vznikajú,[13] umožňujú ekonomickú kalkuláciu, vďaka ktorej môžu fungovať zložité spoločnosti.

Ľudia si vymieňajú tovar pod neustálym sledovaním a trhy fungujú, hoci nedokonale, aj v sledovanom prostredí. Tvrdenie tejto kapitoly je užšie: súkromie výmenu zlepšuje. Sledovanie narúša trhové procesy zistiteľnými spôsobmi. Ochrana súkromia zlepšuje mnohé výmeny a zachováva niektoré hraničné výmeny, ktoré by sledovanie odradilo.

7.1 Logika výmeny

Výmena ako vzájomný prospech

K výmene dochádza, keď strany očakávajú prospech. Alice si váži to, čo má Bob, viac než to, čo ponúka ona. Bob si zasa váži to, čo ponúka Alice, viac než to, čo má on. Obaja očakávajú, že po obchode na tom budú lepšie ako predtým.

Tu priamo pôsobí subjektívna hodnota. Neexistuje objektívna miera, podľa ktorej by bola výmena „spravodlivá" alebo „rovnocenná". Každá

strana hodnotí zo svojho pohľadu, podľa vlastných preferencií a okolností. Ak obe uprednostnia obchod, obe získavajú.

Výmena je teda hra s kladným súčtom. Pri krádeži alebo prerozdeľovaní je zisk jedného stratou druhého. Dobrovoľná výmena naopak vytvára hodnotu pre všetkých zúčastnených. Celkové bohatstvo spoločnosti obchodom rastie.

Výmena si vyžaduje informácie

Aby k výmene došlo, strany potrebujú informácie. Musia poznať príležitosť: vedieť, že výmena je možná, nájsť sa, dorozumieť sa a vymedziť možné obchody. Musia poznať podmienky: rozumieť tomu, čo sa ponúka a čo sa žiada, lebo nepochopenie podmienok vedie k ľútosti namiesto vzájomného prospechu. Nakoniec musia vedieť dosť na to, aby mohli posúdiť, či im výmena vyhovuje.

Výmena však nevyžaduje úplné informácie. Strany bežne obchodujú s nedokonalou znalosťou kvality tovaru a spoľahlivosti protistrany, a to v neistých budúcich podmienkach. Neistota patrí ku konaniu. Výmena prebieha v neistote, nie tak, že by ju odstránila.

Výmena si vyžaduje zvažovanie

Pred súhlasom s obchodom každá strana zvažuje. Berie do úvahy, čoho sa vzdáva a čo dostáva, či je tento obchod lepší než iné možnosti, aké sú riziká a čo sa môže pokaziť, a či obchod slúži jej cieľom.

Toto zvažovanie je, ako ukázala kapitola 3, vnútorné.[3] Odohráva sa v mysli konajúceho. Závery, teda konečné hodnotenia a rozhodnutia, závisia od subjektívnych činiteľov, ktoré vonkajším pozorovateľom unikajú.[4]

7.2 Ako súkromie zlepšuje výmenu

Chránené zvažovanie

Zvažovanie najlepšie funguje, keď ho nikto zvonka neruší.

Ak Alice vie, že jej myslenie niekto sleduje, môže sa jej zvažovanie zmeniť.[5] Môže uvažovať o tom, ako jej myšlienky vyznejú, vyhýbať sa záverom, ktoré by mohli vyvolať kritiku, prispôsobovať úvahy pozorovateľom alebo pochybovať o sebe podľa očakávaných reakcií.

Takéto myslenie je predstavenie formované pozorovaním, nie zvažovanie v prospech Alice. „Voľby“, ktoré zo sledovaného zvažovania vzídu, nemusia zodpovedať jej skutočným preferenciám.

Súkromie zvažovanie chráni tým, že vytvára priestor pre úprimné hodnotenie. Keď je Alicino myslenie súkromné, posudzuje možnosti podľa vlastných meradiel a nemusí myslieť na reakcie pozorovateľov. Jej závery pravdepodobnejšie vyjadrujú jej skutočné záujmy.

Pre výmenu z toho vyplýva: súkromné zvažovanie vedie k lepšie informovaným obchodným rozhodnutiam. Ako ukázala kapitola 3, zvažovanie je z podstaty vnútorné. Vonkajšie pozorovanie sa k subjektívnemu procesu hodnotenia nedostane, ale môže ho skresliť. Strany, ktoré môžu myslieť slobodne, posudzujú príležitosti presnejšie než strany obmedzované pozorovaním.

Vyjednávanie bez odhalenia

Vyjednávanie je strategická interakcia.[14] Každá strana sa snaží dosiahnuť výhodné podmienky a zároveň sa dohodnúť.

Účinné vyjednávanie vyžaduje kontrolované odhaľovanie, pretože každá informácia, ktorú strana odhalí, posúva podmienky dohody.[6] Kto prezradí, koľko je maximálne ochotný zaplatiť, oslabí svoju vyjednávaciu pozíciu. Kto ukáže naliehavosť, vyzve na zneužitie. Kto ukáže alternatívy, prezradí hranicu, pri ktorej obchod nepodpíše. A kto odhalí budúce plány, umožní protistrane zaujať strategicky výhodnú pozíciu.

Keby boli všetky informácie vo vyjednávaní transparentné, vyjednávanie by sa výrazne prikláňalo k strane, ktorá má viac trpezlivosti a lepšie alternatívy alebo menej naliehavú potrebu. Strategická interakcia vyžaduje strategickú kontrolu informácií.

Súkromie vyjednávanie umožňuje tým, že chráni informácie, ktoré strany potrebujú ovládať. Každá strana môže odhaliť to, čo jej slúži, a zatajiť to, čo by jej pozíciu oslabilo. Takéto asymetrické odhaľovanie nie je nepoctivosť, ale primerané spravovanie hraníc: strategická interakcia predpokladá, že strany spravujú, čo odhaľujú, a účinné vyjednávanie závisí od schopnosti to robiť.

Dôverné podmienky

Mnohým výmenám prospievajú dôverné podmienky. Cenová dôvernosť umožňuje predávajúcim ponúkať rôznym kupujúcim rôzne ceny podľa okolností. Keby boli všetky ceny verejné, táto pružnosť by zanikla a mohla by zabrániť obchodom, z ktorých majú prospech obe strany. Zákazkové dohody umožňujú prispôsobiť podmienky konkrétnej situácii, zatiaľ čo verejné odhalenie by tlačilo strany k štandardným podmienkam aj tam, kde zákazkové riešenie vyhovuje obom. A odhalenie zmluvných podmienok môže poskytnúť informácie konkurentom, ktorí potom ponúknu nižšie ceny alebo skopírujú dohody, ktorých vývoj si vyžiadal investície.

Súkromie umožňuje stranám nastaviť výmeny podľa vlastných potrieb bez toho, aby dohody vystavili kopírovaniu konkurenciou alebo zásahom tretích strán.

Budovanie dôvery v čase

Dlhodobé výmenné vzťahy vyžadujú dôveru. Dôvera vzniká opakovanou interakciou a stálym plnením, potom sa prehlbuje postupným odhaľovaním a spoločnými investíciami do aktív viazaných na daný vzťah.

Súkromie podporuje budovanie dôvery tým, že umožňuje postupné odhaľovanie. Strany môžu odhaliť viac, keď dôvera rastie, bez toho, aby ich niekto nútil k predčasnej transparentnosti. Vzťah sa vyvíja vlastným tempom, ktoré mu nenarúša vonkajšie pozorovanie.

Sledovanie budovanie dôvery narúša, lebo odoberá kontrolu nad tempom odhaľovania. Ak sa pozorujú všetky interakcie, strany nemôžu riadiť postupné odkrývanie, ktoré prirodzený vývoj dôvery potrebuje.

7.3 Ako sledovanie skresľuje výmenu

Odrádzací účinok

Sledovanie výmenu odrádza tým, že k obchodu pridáva riziká, ktoré s ním samým nesúvisia.

Ak sa transakcie monitorujú, strany pravdepodobne zvažujú, ako bude výmena vnímaná, či by sa transakcia mohla neskôr použiť proti nim, aké závery z nej pozorovatelia vyvodia a či je výmena bezpečná vzhľadom na to, kto sa môže pozerať.

Tieto úvahy nemajú nič spoločné s tým, či výmena prospieva obom stranám. Sú to vonkajšie činitele, ktoré sledovanie vnáša a ktoré skresľujú rozhodovanie.

V hraničných prípadoch to znamená, že niektoré výmeny, ktoré by obom stranám prospeli, sa pre riziko sledovania neuskutočnia. Hodnota, ktorá mohla vzniknúť, nevznikne. Trhová koordinácia sa zhoršuje.

Zhoršenie cenových signálov

Ceny koordinujú hospodársku činnosť tým, že odovzdávajú informácie o relatívnej vzácnosti a hodnote. Presné ceny závisia od pravých výmen, ktoré odrážajú skutočné hodnotenia.

Sledovanie cenové signály zhoršuje. Odrádza od transakcií, ktoré by bez sledovania prebehli, tlačí transakcie k vzorcom prijateľným pre sledujúcich, vnáša strategické správanie, ktorého cieľom je spravovať záznamy o sledovaní, a znižuje účasť na trhu u ľudí, ktorí sledovanie odmietajú.[7]

Ceny vznikajúce na sledovaných trhoch odrážajú nielen ponuku a dopyt, ale aj vyhýbanie sa sledovaniu. Ako informačné signály sú systematicky skreslené.

Posun v strategickom správaní

Pod sledovaním strany prestávajú slúžiť vlastným záujmom a začínajú spravovať svoje záznamy.

Namiesto otázky „Aká výmena slúži mojim cieľom?“ sa môžu pýtať „Aká výmena vyzerá v očiach pozorovateľov vhodne?“. Rozhodovacie kritériá sa pravdepodobne posunú od skutočnej preferencie k riadeniu zdania.

Kde k tomuto posunu dôjde, je jeho účinok hospodársky ničivý. Zdroje netečú k svojmu najcennejšiemu využitiu, ale k využitiu, ktoré sledovanie najľahšie prijme. Pridelenie zdrojov skresľuje vonkajší súd a neriadia ho hodnotenia samotných účastníkov.

Zasahovanie tretích strán

Sledovanie umožňuje tretím stranám zasahovať do výmeny.

Ak sa transakcie monitorujú, strany s prístupom k údajom o monitorovaní môžu zasiahnuť do transakcií, ktoré neschvaľujú, zdaniť transakcie, ktoré vidia, regulovať výmeny podľa pozorovaných vzorcov a cieliť na účastníkov z politických alebo konkurenčných dôvodov.

Toto zasahovanie je možné len preto, že sledovanie dodáva informácie, ktoré ho umožňujú. Súkromie zasahovanie znemožňuje tým, že odopiera informácie, ktoré potrebuje.

Režimová neistota a odrádzanie od investícií

Robert Higgs v analýze Veľkej hospodárskej krízy a povojnového oživenia pomenoval stav, na ktorom stojí argument tejto kapitoly.[8] Režimová neistota je stav, v ktorom súkromné osoby nevedia predvídať, či štát zmení právne pravidlá upravujúce vlastníctvo, zmluvy, reguláciu a zdaňovanie. Pri režimovej neistote sa očakávaný výnos z dlhodobých investícií znižuje o pravdepodobnosť, že sa pravidlá, od ktorých návratnosť investície závisí, zmenia skôr, než sa návratnosť dostaví. Tvorba kapitálu sa presúva ku kratším časovým horizontom a projekty, ktorých hodnota závisí od stabilného právneho režimu, sa odkladajú alebo opúšťajú.

Sledovanie režimovú neistotu zosilňuje v konkrétnom smere. Transakcia zaznamenaná dnes je transakciou, ktorú možno kedykoľvek neskôr preinterpretovať a stíhať podľa pravidiel, ktoré budú vtedy platiť. Podnikateľ, ktorý vstúpi do odvetvia s nejasným právnym postavením, musí očakávaný výnos znížiť o pravdepodobnosť, že sa pravidlá sprísnia a záznamy z nejasného obdobia sa použijú na zostavenie prípadu. Čím menej súkromný je záznam, tým väčšia je zrážka.

Účinok sa násobí, keď sa hranice dovolenej činnosti posúvajú s politickým počasím. Prejav chránený za jednej administratívy sa za nasledujúcej stane predmetom vyšetrovania. Finančné toky povolené v jednej regulačnej ére sa v ďalšej stanú dôvodom na odopretie bankových služieb

(de-banking). Kto uvažuje o dlhodobom záväzku v činnosti, ktorej právne postavenie závisí od výkladu, dostal náklad čitateľnosti pre štát, ktorý musí investícia prekonať, než začne prinášať výnos. Súkromie v mieste transakcie zužuje rozptyl budúceho regulačného vystavenia na pravidlá, ktoré sú práve vyhlásené. A je to najbližšia náhrada stabilného práva, akú si súkromná osoba môže vybudovať bez spolupráce štátu.

7.4 Výmena môže prebiehať aj pod sledovaním

Netvrdíme, že sledovanie robí výmenu nemožnou. Výmena prebieha pod sledovaním neustále. Je však skreslená.

Existujúca sledovaná výmena

Väčšina dnešnej výmeny je do určitej miery sledovaná. Finančné transakcie sa monitorujú a hlásia. Online nákupy zanechávajú stopy v údajoch, komunikácia podlieha odpočúvaniu a fyzický pohyb sa sleduje rozličnými prostriedkami.

Trhy v tomto prostredí napriek tomu fungujú. Ceny vznikajú, tovar mení majiteľov a širšia hospodárska koordinácia stále prebieha.

Skreslenia sú skutočné, ale obmedzené

Opísané skreslenia sú skutočné. Ich rozsah však závisí od toho, aké rozsiahle je sledovanie, ako veľmi na tom stranám záleží, že ich niekto pozoruje, aká pravdepodobná je intervencia založená na sledovaní a aké alternatívy k sledovanej výmene existujú.

Keď je sledovanie mierne a následky nepravdepodobné, skreslenia môžu byť malé, najmä tam, kde nie sú reálne alternatívy. Strany potom prijímajú náklady sledovania ako súčasť podnikania.

Keď je sledovanie intenzívne a následky pravdepodobné, skreslenia sú väčšie, najmä tam, kde alternatívy existujú. Strany môžu prejsť na nesledované kanály, alebo sa výmeny celkom vzdať.

Hraničné prípady

Aj keď väčšina výmeny pod sledovaním pokračuje, výsledky stále formujú hraničné prípady:

Výmeny, ktoré neprebehnú, sú stratená hodnota. Obchody, ktoré by obom stranám prospeli, bráni riziko sledovania.

Výmeny, ktoré sú skreslené, zle prideľujú zdroje. Rozhodnutia formované riadením sledovania namiesto skutočnej preferencie vedú k horším výsledkom.

Výmeny, ktoré sa presunú k alternatívam, spôsobujú náklady na prispôsobenie. Zdroje vynaložené na vytvorenie a udržiavanie nástrojov na ochranu súkromia nie sú k dispozícii na iné účely.

Ochrana súkromia nerobí výmenu možnou v abstraktnom zmysle. Celkovo ju zlepšuje a zachováva niektoré výmeny, ktoré by sledovanie inak odradilo: viac transakcií v hraničných prípadoch, menej skreslenia, presnejšie ceny, účinnejšie pridelenie zdrojov.

7.5 Konkrétne výmenné prostredia

Zamestnanie

Zamestnanie je trvalá výmena: práca za odmenu. Vzťah zahŕňa opakované vyjednávanie a hodnotenie výkonu, ako aj vzájomné posudzovanie, ktoré sa odvíja mesiace a roky.

Súkromie ovplyvňuje zamestnanie v každej fáze. Uchádzača o prácu, ktorého súčasný zamestnávateľ zistí, že aktívne hľadá, môžu predčasne prepustiť alebo odstrihnúť od ďalšieho rozvoja. Pri vyjednávaní o plate treba utajiť minimálnu mzdu, ktorú by uchádzač prijal: kto prezradí, čo by akceptoval, ukotví ponuku na tejto spodnej hranici, hlboko pod tým, čo by pozícia inak priniesla. Počas trvajúceho zamestnania neustále sledovanie posúva zamestnancov od vecnej práce k predvádzaniu práce a vedie ich optimalizovať pozorovateľné ukazovatele namiesto skutočného prínosu. Metaanalýzy nenachádzajú významný vzťah medzi elektronickým monitorovaním a výkonom, nachádzajú však pozitívny vzťah so stresom a kontraproduktívnym správaním v práci.[9] Tvorivá práca, riešenie zložitých problémov aj dobrovoľné úsilie pod pozorovaním slabnú. Zamestnávateľ, ktorý monitoruje úplne, môže vidieť všetko, čo zamestnanec robí, a zároveň zaistiť, že to, čo zamestnanec robí, má nižšiu hodnotu.

Asymetria problém prehlbuje. Zamestnávatelia, ktorí môžu monitorovať, kým zamestnanci nevidia do zámerov zamestnávateľa, získavajú systematickú výhodu pri vyjednávaní platu, hodnotení výkonu a prepúšťaní. Zamestnanec, ktorý žiada zvýšenie, nemôže vedieť, či zamestnávateľ už nerozhodol o zrušení jeho miesta. Pracovník, ktorému pridávajú zodpovednosť, nevie, či ho čaká povýšenie, alebo vykorisťovanie. Zamestnanec, ktorý plánuje odísť, potrebuje dôvernosť, aby si udržal súčasné miesto, kým hľadá inde, lebo odhalenie zvyčajne urýchli výpoveď, pripraví ho o záverečné odmeny a otrávi referencie.

Odborné služby

Odborné služby závisia od dôvernosti a právne systémy to uznávajú doktrínou profesijného tajomstva. Advokáti nemôžu byť nútení prezradiť komunikáciu s klientmi. Lekári zachovávajú mlčanlivosť o pacientoch. Tieto povolania bez chráneného odhaľovania nemôžu fungovať.[10]

Štruktúra je vo všetkých chránených povolaniach rovnaká. Klient hľadajúci právnu radu musí opísať fakty, z ktorých vzniká zodpovednosť. Pacient musí opísať príznaky a správanie. Investor musí odhaliť svoju finanč-

nú pozíciu a toleranciu rizika. Bez ochrany klienti zadržiavajú relevantné informácie, odborníci radia na základe neúplného chápania a služba sa zrúti. Profesijné tajomstvo nikdy nebolo darom pre odborníkov. Je to inštitucionálne uznanie, že niektoré výmeny bez súkromia fungovať nemôžu.

Medzi podnikmi

Obchod medzi podnikmi zahŕňa interné informácie, ktoré sú zložitejšie než pri spotrebiteľských transakciách. Dodávatelia sa dozvedia prognózy dopytu zákazníkov, zákazníci poznajú nákladovú štruktúru dodávateľov a partneri strategické plány. Každé odhalenie vytvára konkurenčnú zraniteľnosť, ak sa informácia dostane ku konkurentom.

Podniky to zvládajú postupným odhaľovaním, ktoré zodpovedá hĺbke vzťahu. Prvé transakcie odhalia len to, čo je pre danú výmenu nevyhnutné. Keď vzťahy dozrievajú a dôvera rastie, strany zdieľajú viac strategických informácií, čo umožňuje užšiu koordináciu. Bez súkromia, ktoré stranám dovoľuje ovládať, čo odhalia, by tento postupný vzorec, podobný vývoju osobnej dôvery, nebol možný.

Vyjednávanie o cene ukazuje, čo je v hre. Dodávateľ, ktorý vie, že zákazník nemá alternatívy, môže presadiť vyššie ceny, a zákazník, ktorý vie, že dodávateľ zúfalo potrebuje tržby, môže žiadať ústupky. Obe strany preto tajia informácie o svojich alternatívach a naliehavosti, ako aj o obmedzeniach, ktorým čelia. Transparentné vyjednávanie by sa zvrhlo na vykorisťovanie slabšej strany.

Spoločné podniky a partnerstvá vyžadujú zdieľanie informácií, ktoré by sa dali zneužiť, ak partnerstvo zlyhá. Plány vývoja a zoznamy zákazníkov, rovnako ako technické schopnosti zdieľané s partnermi, sa stanú konkurenčnými zbraňami, ak sa partneri stanú rivalmi. Výmena informácií je sama predmetom obchodu. Bez súkromia, ktoré chráni zdieľané informácie pred tretími stranami a obmedzuje ich použitie po skončení partnerstva, by podniky odmietli zdieľať to, čo produktívna spolupráca vyžaduje.

Vzťahy v dodávateľskom reťazci ukazujú, ako súkromie umožňuje výmenu naprieč hranicami organizácií. Výrobca, ktorý zdieľa prognózy dopytu s dodávateľmi, im umožňuje optimalizovať výrobu, čo prospieva obom stranám. Tie prognózy však zároveň prezrádzajú očakávania výrobcu o vlastnom trhu. Súkromie dovoľuje funkčné odhalenie partnerom v dodávateľskom reťazci bez strategického odhalenia konkurentom.

Spotrebiteľské trhy

Spotrebiteľská výmena sa zdá jednoduchšia, no zahŕňa záujmy súkromia, ktoré sa kumulujú naprieč transakciami. Jediný nákup prezradí málo. Sú-

hrnné údaje o nákupoch prezrádzajú preferencie, okolnosti, zdravotné ťažkosti, politické názory, vzťahy aj zraniteľné miesta.

Pozrime sa, ako nákupné vzorce fungujú ako sledovanie. Nákupy liekov prezrádzajú zdravotné ťažkosti, nákupy kníh intelektuálne záujmy a politické sklony, nákupy potravín stravovacie obmedzenia, ktoré môžu naznačovať náboženskú prax alebo zdravotný stav. Vzorce polohy prezrádzajú pracovisko a bydlisko, ako aj širšie väzby. Finančné údaje prezrádzajú ekonomické postavenie a peňažný tok, ako aj platobnú spoľahlivosť. Nič z toho nie je pre samotnú transakciu potrebné. Každé z toho je prebytok zo sledovania, vyťažený z výmeny.

Nástroje súkromia, ktoré tradične chránili spotrebiteľskú výmenu, miznú. Hotovosť umožňuje nákup bez identifikácie, no jej prijímanie klesá, keď sa platobná infraštruktúra presúva do digitálnej podoby.[11] Anonymný nákup v obchode vyžaduje fyzickú prítomnosť, ale maloobchod sa presúva online, kde sa každá transakcia zaznamenáva. Súkromie spotrebiteľa kedysi nevyžadovalo žiadne aktívne kroky. Dnes vyžaduje vedomé prijatie nástrojov proti predvolenému sledovaniu.

Súhrnný rozmer odlišuje spotrebiteľské súkromie od ostatných prostredí. Zamestnávateľ, ktorý sleduje konkrétneho zamestnanca, má konkrétny cieľ. Podnikové sledovanie spotrebiteľov je úplné: história transakcií, stopy polohy aj záznamy o klikaní sa hromadia o všetkých spotrebiteľoch, aby umožnili cielenie, manipuláciu a predpovedanie.[15] Záujem spotrebiteľa na súkromí nespočíva v žiadnej jednotlivej transakcii, ale v odporovaní zhromažďovaniu, ktoré mení nevinné nákupy na úplné profily.

Tým vznikajú problémy kolektívneho konania, ktoré jednotlivé nástroje súkromia nevyriešia. Ak jeden spotrebiteľ platí hotovosťou, kým ostatní sledovanými platbami, hotovostný platiteľ si súkromie zachová, no nemôže zabrániť vytváraniu profilov, ktoré umožňujú súhrnné údaje. Súkromie spotrebiteľa si vyžaduje buď masové prijatie nástrojov súkromia, alebo štrukturálne zmeny, ktoré zhromažďovaniu zabránia. Obe cesty čelia koordinačným ťažkostiam, aké zamestnanecké či odborné súkromie nepozná.

Zhrnutie kapitoly

Výmena je vzájomný prospech prostredníctvom obchodu. Vyžaduje informácie, zvažovanie a dohodu a cez cenové signály koordinuje výrobu a spotrebu v celom hospodárstve. Súkromie zlepšuje výmenu na každej vrstve: chránené zvažovanie vedie k lepšie informovaným rozhodnutiam, kontrolované odhaľovanie umožňuje vyjednávanie bez zrútenia do vykorisťovania slabšej strany, dôverné podmienky dovoľujú stranám usporiadať dohody, ktoré konkurenti nemôžu skopírovať, a postupné odhaľovanie nechá dôveru vyvíjať sa vlastným tempom. Sledovanie skresľuje tie isté procesy. Monitorované zvažovanie posúva rozhodnutia k riadeniu

zdania, odradené transakcie neprebehnú a tretie strany zasahujú do výmen, ktoré vidia.[1216]

Tvrdenie je porovnávacie, nie absolútne. Výmena prebieha pod sledovaním neustále. Súkromie ju nerobí možnou, ale lepšou: zachováva hraničné transakcie a znižuje systematické skreslenie. Ekonomický argument stojí nezávisle od normatívneho. Aj bez etického argumentu z kapitoly 4 by koordinačné zisky, ktoré súkromie prináša, ospravedlňovali jeho ochranu. Axiomatický základ z kapitoly 3, etický zákaz z kapitoly 4 a implementácia na úrovni nástrojov v častiach V a VI dopĺňajú obraz, ktorý táto kapitola posudzuje výlučne z ekonomického hľadiska.

Poznámky

[1] Carl Menger, *Principles of Economics*, prel. James Dingwall a Bert F. Hoselitz (Auburn, AL: Ludwig von Mises Institute, 2007; nemecký originál 1871), kapitola 4 („The Theory of Exchange"), najmä s. 175–191. Zakladajúci text rakúskej školy, v ktorom Menger odvodzuje výmenný vzťah z hraničného úžitku bez odvolania na teóriu práce alebo rovnovážnu cenu. Mises rozvíja ten istý vzťah podrobnejšie v diele *Human Action* (cit. v kap. 3, pozn. 1), 195 a vo štvrtej časti vcelku, z ktorej táto kapitola vychádza.

[2] K výmene ako základu spoločenskej spolupráce pozri Mises, *Human Action* (cit. v kap. 3, pozn. 1), Part II, „Action Within the Framework of Society", a Murray N. Rothbard, *Man, Economy, and State* (cit. v kap. 3, pozn. 3), kapitoly 2–3.

[3] K zvažovaniu a konaniu pozri Mises, *Human Action* (cit. v kap. 3, pozn. 1), kapitola 1, „Acting Man", a rozbor v kapitole 3 tejto knihy.

[4] K teórii subjektívnej hodnoty a výmene pozri Carl Menger, *Principles of Economics* (cit. v kap. 3, pozn. 5), 175–225 (kapitola o výmene, odlišná od kapitoly o subjektívnej hodnote citovanej v kap. 3, pozn. 5).

[5] K účinkom sledovania na správanie pozri Michel Foucault, *Discipline and Punish: The Birth of the Prison*, prel. Alan Sheridan (New York: Vintage, 1995; francúzsky originál 1975). Analýza panoptikonu je štandardným odkazom na behaviorálny účinok vnímaného pozorovania. Ekonomická analýza tu je rakúska, nie foucaultovská.

[6] Friedrich A. Hayek, „The Use of Knowledge in Society," *American Economic Review* 35, č. 4 (1945): 519–530, `https://www.jstor.org/stable/1809376`. Kanonická štúdia o cenách ako decentralizovaných signáloch koordinujúcich znalosti. Argument o vyjednávaní tu rozvíja Hayekovu myšlienku, že relevantné informácie sú rozptýlené a vonkajší pozorovateľ ich nemôže zhromaždiť bez skreslenia dohody. Pozri tiež Israel M. Kirzner, *Market Theory and the Price System* (Indianapolis: Liberty Fund, 2011; pôvodne Van Nostrand, 1963), o podnikateľskej funkcii v trhovom procese koordinovanom cenami.

[7] K cenovým signálom a ekonomickej kalkulácii pozri Mises, *Human Action* (cit. v kap. 3, pozn. 1), Part III, „Economic Calculation", a Mises, *Socialism: An Economic and Sociological Analysis*, prel. J. Kahane (Indianapolis: Liberty Fund, 1981; nemecký originál 1922), Part II. Argument o kalkulácii pomenúva konkrétnu funkciu cien, ktorú skreslenie sledovaním poškodzuje.

[8] Robert Higgs, „Regime Uncertainty: Why the Great Depression Lasted So Long and Why Prosperity Resumed after the War," *The Independent Review* 1, č. 4 (Spring 1997): 561–590. Argument rozvíja Robert Higgs, *Depression, War, and Cold War: Studies in Political Economy* (New York: Oxford University Press, 2006), a „Regime Uncertainty: Pirrong Responds to Krugman," *The Independent Review* 16, č. 2 (Fall 2011): 243–246. Higgs nie je rakúsky v prísnom metodologickom zmysle, ale jeho pojem je s rakúskou školou zlučiteľný a od

svojho zavedenia sa ujal v rakúskych politicko-ekonomických textoch. Rozšírenie na neistotu vyvolanú sledovaním je prínosom tejto kapitoly.

[9] Daniel M. Ravid et al., „The Impact of Electronic Monitoring on Employees' Job Satisfaction, Stress, Performance, and Counterproductive Work Behavior: A Meta-Analysis," *Computers in Human Behavior Reports* 8 (2022). Pozri tiež Paul Glavin a Scott Schieman, s Alex Bierman, „Private Eyes, They See Your Every Move: Workplace Surveillance and Worker Well-Being," *Socius* 10 (2024).

[10] K advokátskemu tajomstvu je kanonickým moderným vyjadrením *Upjohn Co. v. United States*, 449 U.S. 383 (1981), a vedúcim spracovaním v odbornej literatúre John Henry Wigmore, *Evidence in Trials at Common Law*, ed. John T. McNaughton, zv. 8 (Boston: Little, Brown, 1961), §§2290–2329. K federálnemu tajomstvu vzťahu psychoterapeuta a pacienta *Jaffee v. Redmond*, 518 U.S. 1 (1996). K mlčanlivosti lekára voči pacientovi ako profesijnej etike je zakladajúcim vyjadrením Hippokratova prísaha a súčasnou americkou kodifikáciou *Code of Medical Ethics* Americkej lekárskej asociácie (AMA), stanovisko 3.2.1 („Confidentiality"). Ekonomicko-funkčný výklad podaný v tejto kapitole predznamenávajú Daniel J. Solove, *Understanding Privacy* (Harvard University Press, 2008), a rámec kontextovej integrity Helen Nissenbaum, *Privacy in Context: Technology, Policy, and the Integrity of Social Life* (Stanford University Press, 2010). Obe diela sú citované v kap. 1, pozn. 3.

[11] K empirickému poklesu používania hotovosti pozri Federal Reserve Bank of Atlanta a Federal Reserve Bank of San Francisco, *Diary of Consumer Payment Choice* (ročná séria, 2012 až súčasnosť), ktorý dokumentuje klesajúci podiel hotovosti na spotrebiteľských platbách podľa počtu aj hodnoty transakcií. Správa Federal Reserve Bank of San Francisco *2024 Findings from the Diary of Consumer Payment Choice* uvádza podiel hotovosti 16 % platieb podľa počtu, oproti 31 % v roku 2016. K medzinárodnému porovnaniu pozri Bank for International Settlements, *Committee on Payments and Market Infrastructures: Red Book Statistics* (ročne). K politickým a inštitucionálnym hnacím silám nahrádzania hotovosti digitálnymi platbami je najprístupnejším knižným spracovaním Brett Scott, *Cloudmoney: Cash, Cards, Crypto, and the War for Our Wallets* (Harper Business, 2022).

[12] K sledovaniu ako skresleniu trhových procesov pozri Shoshana Zuboff, *In the Age of the Smart Machine: The Future of Work and Power* (Basic Books, 1988), základnú štúdiu o tom, ako monitorovanie na pracovisku posúva správanie zamestnancov od vecného výkonu k predvádzaniu výkonu. Ten istý mechanizmus na úrovni spotrebiteľských trhov je predmetom neskoršej Zuboffovej knihy *The Age of Surveillance Capitalism* (cit. v pozn. 15 vyššie). K odrádzacím účinkom v ekonomickom správaní pri právnej neistote pozri Richard A. Posner, *Economic Analysis of Law*, 9. vyd. (Wolters Kluwer, 2014), §§1.1–1.2, o všeobecnom rámci odstrašovania, a Higgs, „Regime Uncertainty" (cit. v pozn. 8 vyššie), o skracovaní investičného horizontu, ktoré sledovanie transakcií spôsobuje.

[13] Israel M. Kirzner, *Competition and Entrepreneurship* (Chicago: University of Chicago Press, 1973). Kirznerovým ústredným prínosom je pojem podnikateľskej ostražitosti: ziskové príležitosti existujú na trhu, pretože ceny ešte nie sú vyrovnané, a podnikatelia, ktorí si tieto medzery všimnú, poháňajú proces cenovej koordinácie. Veta o „cenových signáloch vznikajúcich z výmeny" v úvode z toho vychádza: rozptýlené hodnotenia mení na užitočnú cenovú informáciu podnikateľská funkcia, nie mechanický vyrovnávací stroj. Pozri tiež Kirzner, *The Meaning of Market Process* (Routledge, 1992), pre úplnejšie vyjadrenie jeho teórie trhového procesu, a *Discovery and the Capitalist Process* (University of Chicago Press, 1985).

[14] Thomas C. Schelling, *The Strategy of Conflict* (Cambridge: Harvard University Press, 1960). Schellingova teoreticko-herná analýza vyjednávania, záväzkov a ohniskových bodov je štandardným odkazom na strategickú interakciu pri vyjednávaní. Jeho ústredné poznanie – že strany vo vyjednávaní často profitujú z obmedzenia vlastných možností, z odovzdávania vierohodných záväzkov a zo spravovania informačných asymetrií – tvorí

základ argumentu tohto oddielu, že súkromie umožňuje vyjednávanie tým, že každej strane dovoľuje ovládať, čo odhalí. Schelling dostal v roku 2005 Nobelovu pamätnú cenu za ekonómiu. K použitiu na informačnú asymetriu konkrétne pri vyjednávaní pozri tiež Roger B. Myerson a Mark A. Satterthwaite, „Efficient Mechanisms for Bilateral Trading," *Journal of Economic Theory* 29 (1983): 265–281.

[15] Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (New York: PublicAffairs, 2019). Zuboff dokumentuje, ako platformové firmy hromadia behaviorálne údaje zo všetkých spotrebiteľských interakcií, aby vytvorili predikčné profily predávané inzerentom a využívané na úpravu správania. Jej pojem „sledovací kapitalizmus" pomenúva obchodný model. Veta, ku ktorej sa táto poznámka viaže, opisuje jeho mechanizmus: zhromažďovanie jednotlivo nevinných transakcií do úplných behaviorálnych profilov. Rámec tejto kapitoly sa od Zuboff líši diagnózou aj nápravou: ona sa zasadzuje za nové vlastnícke práva k údajom, táto kapitola hľadá nápravu v presadzovaní zmlúv a v alternatívach zachovávajúcich súkromie. Jej empirický opis dynamiky zhromažďovania je však východiskovým bodom.

[16] Ďalšie čítanie o výmene, cenových signáloch a trhovom procese. Základným textom rakúskej cenovej teórie je Mises, *Human Action* (cit. v kap. 3, pozn. 1), časti III–IV, ktoré spracúvajú kalkuláciu, ceny a trh ako ucelený proces. Murray N. Rothbard, *Man, Economy, and State* (cit. v kap. 3, pozn. 3), kapitoly 2–7, predkladá ten istý materiál systematickejšie. Klasickoliberálnou paralelou z devätnásteho storočia je Frédéric Bastiat, *Economic Harmonies*, prel. W. Hayden Boyers (Foundation for Economic Education, 1964; francúzsky originál 1850), ktorý rozvíja argument, že výmena sama tvorí spoločnosť. Kratším sprievodným textom sú Bastiatove *Economic Sophisms* (1845). K funkcii cien ako koordinátora znalostí je kanonickou štúdiou Hayek, „The Use of Knowledge in Society" (cit. v pozn. 6 vyššie), a Hayekovo „Competition as a Discovery Procedure" v *New Studies in Philosophy, Politics, Economics, and the History of Ideas* (University of Chicago Press, 1978) argument rozširuje. Israel Kirzner, *Competition and Entrepreneurship* (University of Chicago Press, 1973), a *Discovery, Capitalism, and Distributive Justice* (Blackwell, 1989) rozvíjajú podnikateľskú stránku toho istého rámca. Pre hlavný prúd je neoklasickým odkazom Alfred Marshall, *Principles of Economics*, 8. vyd. (Macmillan, 1920), a východiskom hlavného prúdu pre ekonómiu informácií George Stigler, „The Economics of Information," *Journal of Political Economy* 69, č. 3 (1961): 213–225. Ako humanistickú protiváhu karikatúr trhovej teórie rozvíja nemeckú ordoliberálnu tradíciu Wilhelm Röpke, *A Humane Economy: The Social Framework of the Free Market* (Henry Regnery, 1960). K behaviorálnej literatúre spájajúcej sledovanie s konaním je skoršou štúdiou, spred *Surveillance Capitalism*, a zameranou výslovne na monitorovanie na pracovisku Shoshana Zuboff, *In the Age of the Smart Machine* (Basic Books, 1988). K súkromiu ako podmienke úprimného vyjadrovania preferencií je klasickou štúdiou z polovice dvadsiateho storočia Alan Westin, *Privacy and Freedom* (cit. v kap. 1, pozn. 1), a analýzu rozširuje práca Anity L. Allen, citovaná v kap. 1, pozn. 3.

8

TEÓRIA KAPITÁLU A PODNIKANIE

„Kapitál sú vyrobené výrobné prostriedky."

Eugen von Böhm-Bawerk, *The Positive Theory of Capital* (1889)[1]

„Podnikateľ je hnacou silou trhového hospodárstva."

Israel M. Kirzner, *Competition and Entrepreneurship* (1973)[2]

Úvod

Infraštruktúra súkromia je kapitál. Vyžaduje obetu dnes výmenou za schopnosť zajtra. Investície do šifrovaných komunikačných systémov a bezpečných vývojových prostredí, ako aj do anonymných sietí,[19] prinášajú formy koordinácie, ktoré priame prístupy nedosiahnu.

Táto kapitola uplatňuje rakúsku teóriu kapitálu a analýzu podnikania na súkromie. Böhm-Bawerkove poznatky o okľukovej výrobe vysvetľujú, prečo nepriame spôsoby dosiahnutia súkromia (budovanie infraštruktúry) prekonávajú priame (dôveru v inštitúcie). Kirznerova podnikateľská ostražitosť vysvetľuje, ako inovácie v oblasti súkromia vznikajú trhovým objavovaním.

Analýza zároveň osvetľuje praktický kompromis: súkromie často vyžaduje prijať nepohodlie teraz kvôli ochrane neskôr. Teória časovej preferencie vysvetľuje, prečo niektorí ľudia investujú do infraštruktúry súkromia a iní prijímajú sledovanie kvôli okamžitému pohodliu. Ani jedna voľba nie je iracionálna. Odrážajú rôzne preferencie medzi súčasným a budúcim uspokojením.

Predstavme si obchodníka, ktorý chce predávať bez toho, aby o zákazníkoch zostavoval trvalé dosje. Priama cesta vedie cez bežné bankovníctvo a štandardný internetový obchod a spolieha sa, že sprostredkovatelia

sa budú správať slušne. Okľuková cesta je pomalšia a obchodník sa musí naučiť Bitcoin,[3] presunúť komunikáciu na šifrované kanály a postaviť obchod na platobných kanáloch, ktoré nezávisia od sledovania platformami. Druhá cesta vyžaduje úsilie hneď. Vytvára však schopnosti do budúcnosti, aké prvá cesta poskytnúť nemôže.

8.1 Infraštruktúra súkromia ako kapitálové statky

Kapitálové statky a spotrebné statky

Praxeológia rozlišuje kapitálové a spotrebné statky podľa vzťahu k ľudským potrebám. Spotrebné statky uspokojujú potreby priamo, ako jedlo hlad. Kapitálové statky ich uspokojujú nepriamo tým, že zvyšujú budúcu výrobu, ako továreň vyrába tovar, ktorý potreby uspokojuje. Jediná šifrovaná správa alebo jednorazový anonymný nákup je spotrebný statok súkromia, ktorý uspokojuje potrebu priamo. Šifrované komunikačné systémy, bezpečné vývojové prostredia a infraštruktúra anonymných sietí sú kapitálové statky súkromia: umožňujú budúcu výrobu prínosov súkromia pri mnohých použitiach.

Statky vyššieho a nižšieho rádu

Menger triedil statky podľa vzdialenosti od konečnej spotreby:[4]

Statky prvého rádu (spotrebné statky) uspokojujú potreby priamo. Statky druhého rádu vyrábajú statky prvého rádu. Statky tretieho rádu vyrábajú statky druhého rádu a tak ďalej, pričom každý rád umožňuje výrobu na nasledujúcej nižšej úrovni.

Infraštruktúra súkromia má túto hierarchickú štruktúru. Kryptografický výskum a vývoj protokolov sú blízko vyššieho konca, používateľské aplikácie a služby súkromia na nižšom konci a vývojové rámce a komunikačné protokoly medzi nimi. Každý vyšší rád umožňuje výrobu na nasledujúcom nižšom.[14]

Investície do statkov vyššieho rádu prinášajú väčšie výnosy, no vyžadujú dlhšie časové horizonty a viac trpezlivosti. Kým kryptografický výskum vyústi do aplikácií pre používateľov, môžu uplynúť roky.[13]

Okľuková výroba

Böhm-Bawerk ukázal, že nepriame (okľukové) výrobné metódy často prinášajú lepšie výsledky.[5] Priamy prístup používa jednoduché nástroje na okamžitý výsledok. Okľukový prístup investuje čas do budovania lepších nástrojov: začína pomalšie, no prináša lepšiu schopnosť v dlhodobom horizonte.

Priame súkromie sa spolieha na sľuby inštitúcií a právne rámce opreté o dôveru. Dá sa zaviesť rýchlo, ale je zraniteľné voči zmenám postoja úradov a kompromitácii inštitúcií. Okľukové súkromie buduje kryptogra-

fickú infraštruktúru, ktorá umožňuje matematické overenie. Vývoj je pomalší, no ochrana je nezávislá od spolupráce inštitúcií. Okľukový prístup vyžaduje nižšiu časovú preferenciu a odmenou je súkromie, ktoré nezávisí od spolupráce druhých.

8.2 Časová preferencia a kompromis medzi súkromím a pohodlím

Kompromis

Súkromie často vyžaduje nepohodlie. Šifrovaná komunikácia vyžaduje správu kľúčov a anonymné transakcie ďalšie kroky. Bezpečné systémy vo všeobecnosti vyžadujú zaučenie, kým sa dajú používať.

Vzniká tak skutočný kompromis: prijať sledovanie kvôli okamžitému pohodliu, alebo prijať nepohodlie kvôli budúcej ochrane súkromia.

Pre spomínaného obchodníka je nepohodlie konkrétne: dodatočné nastavovanie a viac zručností, ktoré sa musí naučiť, než sa prvý súkromný predaj začne zdať bežný. Konkrétny je aj neskorší prínos: čistejšie vyrovnanie a menej kontrolných bodov, ktoré sledujú vzťah so zákazníkom.

Ani jedna voľba nie je sama osebe iracionálna. Odrážajú rôzne časové preferencie, hoci časová preferencia nie je jediným činiteľom. Záleží aj na znalostiach: používatelia, ktorí nerozumejú rizikám sledovania, ich nemôžu racionálne zvažovať. Pohodlné technológie často zakrývajú svoje náklady, takže súčasné prínosy sú nápadné, kým budúce riziká zostávajú skryté. Voľby ovplyvňujú aj spoločenské normy: ak všetci používajú sledované služby, alternatívam chrániacim súkromie môžu chýbať sieťové efekty. Technická zručnosť mení cenu súkromia: komu je šifrovanie ľahké, pre toho sa kompromis prikláňa k súkromiu, kto s ním zápasí, pre toho váži viac pohodlie. Časová preferencia zostáva ústredná, no pôsobí spolu s informáciami, zručnosťami a spoločenským kontextom.

Teória časovej preferencie

Časová preferencia je uprednostňovanie súčasného uspokojenia pred budúcim. Pri inak rovnakých podmienkach ľudia uprednostňujú statky teraz pred statkami neskôr. Dolár dnes má väčšiu hodnotu než dolár o rok.

Časová preferencia sa však medzi jednotlivcami líši:

Jednotlivci s vysokou časovou preferenciou silno uprednostňujú súčasné uspokojenie a sú ochotní prijať budúce náklady za súčasný prínos. Jednotlivci s nízkou časovou preferenciou uprednostňujú súčasné uspokojenie slabšie a sú ochotní prijať súčasné náklady za budúci prínos.

Použitie na súkromie

Jednotlivci s vysokou časovou preferenciou si môžu racionálne zvoliť služby, ktoré umožňujú sledovanie. Pohodlie je okamžité a isté, kým náklady

na súkromie sú budúce a neisté. Keďže budúce náklady silno diskontujú, obchod sa prikloní k pohodliu.

Jednotlivci s nízkou časovou preferenciou si môžu racionálne zvoliť infraštruktúru súkromia. Nepohodlie je dočasné, kým prebieha učenie, a prínosy pre súkromie sa v čase kumulujú. Keďže budúce prínosy vysoko oceňujú, obchod sa prikloní k súkromiu.

To vysvetľuje segmentáciu trhu v technológiách súkromia. Niektorí používatelia prijímajú nástroje súkromia napriek nepohodliu, iní uprednostňujú pohodlné sledované alternatívy. Obe skupiny reagujú racionálne na vlastné časové preferencie.

Investícia do infraštruktúry ako nízka časová preferencia

Budovanie infraštruktúry súkromia vyžaduje ešte nižšiu časovú preferenciu než používanie nástrojov súkromia. Vývojári investujú roky, kým sa dočkajú prijatia. Návrhári protokolov pracujú bez okamžitej odmeny. Prispievatelia do open source obetujú súčasný príjem kvôli budúcemu vplyvu.[15]

To vysvetľuje, prečo sa vývoj infraštruktúry súkromia sústreďuje medzi ľuďmi s mimoriadne nízkou časovou preferenciou, často s pevným ideovým presvedčením alebo mimoriadnou trpezlivosťou.

Trhová koordinácia časových preferencií

Trhy koordinujú rôzne časové preferencie:

Jednotlivci s nízkou časovou preferenciou budujú infraštruktúru. Prijímajú súčasnú obetu výmenou za budúcu schopnosť a investujú do nástrojov, protokolov a systémov.

Jednotlivci s vysokou časovou preferenciou infraštruktúru používajú. Ťažia z investícií druhých bez toho, aby niesli bremeno vývoja.

Toto rozdelenie vyzerá ako jazda zadarmo, no bližšie je k špecializácii. Vývojári sú odmenení neskorším prijatím a reputáciou, používatelia platia kúpnymi cenami alebo darmi a trhy koordinujú rôzne časové preferencie oboch strán dobrovoľnou výmenou.

8.3 Podnikateľské objavovanie v oblasti súkromia

Kirznerovská ostražitosť

Israel Kirzner vysvetlil podnikanie ako ostražitosť voči ziskovým príležitostiam, ktoré druhým unikajú:[6]

Podnikatelia nemajú lepšie znalosti o daných údajoch. Všímajú si príležitosti, ktoré v údajoch existujú, ale druhí ich prehliadajú. Vďaka tejto ostražitosti môžu využívať rozdiel medzi súčasnými trhovými podmienkami a nerozpoznanými možnosťami.

Technológia súkromia je príkladom kirznerovského objavovania. Podnikatelia si všímajú koordinačné problémy. Existujúce nástroje nechránia

niektoré komunikácie a účastníci trhu sa bez sledovania nemôžu koordinovať. Inštitucionálne riešenia nechávajú medzery, ktoré môže technológia vyplniť.

Potom vyvíjajú riešenia. Nové protokoly riešia nenaplnené potreby a aplikácie obsluhujú trhy, ktoré zavedení hráči ignorovali, lebo ich obchodným modelom bolo sledovanie.

Z tejto ostražitosti podnikatelia profitujú. Skoré prijatie prináša trhovú pozíciu a investície do infraštruktúry vytvárajú trvalé konkurenčné výhody.

Objavovanie potrieb súkromia

Potreby súkromia nie sú vždy zjavné. Mnohí ľudia si neuvedomia, že ich súkromie je narušené, kým nenastane škoda. Podnikatelia si tieto nerozpoznané potreby všímajú:

Niektoré potreby sú latentný dopyt: ľudia by si súkromie cenili, keby chápali, o čo prichádzajú, a podnikatelia pri službe aj vzdelávajú. Iné potreby sú nevyjadrené: ľudia zažijú krádež identity alebo trápne úniky, ako aj odrádzací účinok, bez toho, aby to spojili so súkromím, a podnikatelia toto spojenie vytvárajú. A ďalšie potreby smerujú do budúcnosti: schopnosti sledovania porastú a podnikatelia predvídajú problémy skôr, než sa stanú akútnymi.

Tento proces objavovania vysvetľuje, prečo technológia súkromia často predbieha dopyt používateľov, namiesto aby ho nasledovala. Podnikatelia vidia to, čo používatelia zatiaľ nerozpoznali.

Tvorivá deštrukcia

Schumpeter opísal inováciu ako tvorivú deštrukciu: nové riešenia vytláčajú staré, často ničia zavedené podniky a vytvárajú novú hodnotu.[7]

Technológia súkromia je príkladom tvorivej deštrukcie. Šifrované správy vytláčajú SMS,[16] ktoré sú menej bezpečné a viac sledované. Kryptomena vytláča niektoré platobné systémy postavené na sledovaní a kontrole.[17] Decentralizované platformy súťažia s centralizovanými, ktorých príjmy závisia od vyťažovania údajov.

Táto deštrukcia je tvorivá, pretože lepšie slúži používateľom. Vytlačené riešenia boli horšie a ich vytlačenie je pokrok. Je však deštruktívna pre zavedené záujmy, ktoré zo starých usporiadaní profitovali.

Podnikateľský úsudok v neistote

Peter Klein zdôrazňuje, že podnikanie zahŕňa úsudok v neistote:[8] rozhodnutia o prideľovaní zdrojov, keď sa výsledky nedajú vopred poznať.

Podnikatelia v oblasti súkromia čelia značnej neistote. Prijatie závisí od činiteľov, ktoré nemôžu ovplyvniť, a právne prostredie sa im môže počas vývoja pod rukami zmeniť. Konkurenti môžu vyvinúť lepšie riešenia, kým

oni budujú, a samotná implementácia môže odhaliť problémy, s ktorými žiadny návrh nepočítal.

Podnikateľský úsudok znamená nasadiť zdroje napriek tejto neistote. Úspešní podnikatelia nie sú tí, čo neistotu odstránia, ale tí, čo v nej dobre usudzujú.

8.4 Heterogenita kapitálu a špecializácia v súkromí

Hayek o heterogenite kapitálu

Hayek ukázal, že kapitálové statky sú heterogénne: rôzne nástroje slúžia rôznym účelom a nemožno ich ľubovoľne nahrádzať.[9] Ludwig Lachmann túto analýzu prehĺbil a ukázal, že kapitálové statky sú vo vzťahoch komplementarity a substituovateľnosti, ktoré môže posúdiť iba podnikateľský úsudok.[18]

Kladivo nie je zameniteľné s pílou a nákladné auto s lodou. Každý kapitálový statok má špecifické použitie a schopnosti.

Investičné rozhodnutia preto musia priradiť kapitál k účelu. Nesprávne pridelený kapitál sa nedá prerozdeliť a koordinácia vyžaduje priradiť konkrétny kapitál ku konkrétnym potrebám.

Špecializácia kapitálu súkromia

Infraštruktúra súkromia má vlastnosti heterogénneho kapitálu. Kryptografické knižnice nenahradia rámce používateľských rozhraní a smerovanie anonymných sietí nenahradí správu identít. Každý kapitálový statok má svoju funkciu a dobre vyvinutá knižnica nevynahradí slabú operačnú bezpečnosť.

Trhová koordinácia heterogénneho kapitálu

Trhy koordinujú heterogénny kapitál cez cenové signály a podnikateľské objavovanie:

Ziskové príležitosti signalizujú, kde je kapitál potrebný: vysoké výnosy v danom segmente priťahujú investície, kým nízke výnosy signalizujú nadbytok. Špecializácia umožňuje rozvoj odbornosti, keď sa vývojári sústredia na konkrétne súčasti, kde majú komparatívnu výhodu. Výmena umožňuje koordináciu medzi špecialistami, keďže tí s kryptografickou odbornosťou obchodujú s tými, čo ovládajú používateľské rozhrania.

Žiaden centrálny plánovač by tento heterogénny kapitál nedokázal koordinovať. Potrebné znalosti o konkrétnych schopnostiach, obmedzeniach kompatibility a trhových potrebách sú príliš rozptýlené. Účinne ho môžu koordinovať iba trhové procesy.

8.5 Tvorba kapitálu a rozvoj súkromia

Proces tvorby kapitálu

Tvorba kapitálu vyžaduje úspory, investície, čas a údržbu.[10] Tvorba kapitálu súkromia sleduje tento vzorec:

Vo fáze šetrenia sa vývojári vzdávajú súčasného príjmu, aby investovali do vývoja infraštruktúry, a používatelia sa vzdávajú pohodlných sledovaných služieb, aby investovali do učenia sa nástrojov súkromia. Vo fáze investovania tečú zdroje do vývoja protokolov, tvorby aplikácií a budovania sietí a čas a úsilie vytvárajú kapitálové statky. Časový rozmer je výrazný: vývoj a nasadenie infraštruktúry súkromia trvá roky a výnosy v podobe ochrany súkromia sa dostavujú postupne. Údržba prebiehajúcim vývojom potom zachováva bezpečnostné vlastnosti; revízie kódu a aktualizácie udržiavajú hodnotu kapitálu.

Open source ako tvorba kapitálu

Vývoj open source je osobitná forma tvorby kapitálu:[11]

Open source znamená kolektívnu investíciu: mnohí vývojári prispievajú bez priamej odmeny a vytvárajú spoločný kapitál. Výsledný kód je nerivalitný kapitál: na rozdiel od fyzického kapitálu môže otvorený kód používať neobmedzený počet strán bez vyčerpania. Súťažné zlepšovanie urýchľuje tvorbu kapitálu, keď viacerí vývojári vylepšujú tú istú kódovú základňu. Transparentnosť zvyšuje aj kvalitu kapitálu, pretože otvorený kód umožňuje bezpečnostné overenie.

Tento spôsob tvorby kapitálu umožňuje vývoj infraštruktúry súkromia, ktorému by sa uzavreté (proprietárne) prístupy nevyrovnali. Kapitál vzniká kolektívne a je voľne dostupný. Keďže je kód otvorený, ktokoľvek s potrebnou zručnosťou a motiváciou ho môže priebežne zlepšovať.

Akumulácia kapitálu a schopnosti súkromia

Kapitál sa hromadí úspešnou investíciou:

Individuálna akumulácia nastáva, keď vývojári, ktorí vybudujú úspešné nástroje, ich môžu použiť v ďalších projektoch; odbornosť sa násobí a vznikajú siete spolupracovníkov. Systémová akumulácia nastáva, keď úspešné protokoly umožňujú nové aplikácie, investície do infraštruktúry vytvárajú platformy pre budúci vývoj a každá vrstva umožňuje ďalšiu. Akumulácia znalostí nastáva, keď riešenia minulých problémov formujú budúci vývoj a získané skúsenosti sa vtelia do postupov a kódu.

Táto akumulácia vysvetľuje, prečo sa technológia súkromia za desaťročia výrazne zlepšila. Každá generácia stavia na úspechoch predchádzajúcej a na ďalší postup využíva nahromadený kapitál.

Zhrnutie kapitoly

Infraštruktúra súkromia je kapitál v rakúskom zmysle: vyrobené výrobné prostriedky, ktoré vyžadujú obetu dnes výmenou za schopnosť zajtra. Okľukové metódy dosiahnutia súkromia, ktoré budujú kryptografické nástroje a protokoly, prekonávajú priame metódy opreté o sľuby inštitúcií. Druhý prístup závisí od trvalej dobrej vôle inštitúcií, ktoré používateľ nemôže ovládať, kým prvý nie. Statky vyššieho rádu (kryptografické základy, protokoly) umožňujú statky nižšieho rádu (aplikácie, služby) a každá generácia vývoja stavia na nahromadenom kapitáli predchádzajúcej.

Teória časovej preferencie vysvetľuje, prečo sa používatelia v kompromise medzi súkromím a pohodlím delia, bez toho, aby bola ktorákoľvek strana iracionálna. Vysoká časová preferencia uprednostňuje okamžité pohodlie služieb umožňujúcich sledovanie. Nízka časová preferencia uprednostňuje investície do infraštruktúry súkromia, ktorej odmena sa hromadí v čase. Trhy tieto preferencie koordinujú špecializáciou: vývojári s nízkou časovou preferenciou budujú nástroje, ktoré môžu používatelia s vysokou časovou preferenciou neskôr prijať. Samotnú inováciu poháňa podnikateľské objavovanie: ostražití podnikatelia si všímajú nenaplnené potreby súkromia a vyvíjajú riešenia, ktoré vytláčajú horšie sledované systémy. Heterogenita kapitálu znamená, že rôzne nástroje slúžia rôznym účelom, a žiaden centrálny plánovač by nedokázal koordinovať rozptýlené znalosti, ktoré si ich pridelenie vyžaduje.

Kapitola poskytuje kapitálovoteoretický základ. Ktoré konkrétne nástroje prijať a ako fungujú v praxi, patrí do častí V a VI. Etický argument proti štátnym kanálom stojí na etike argumentácie z kapitoly 4 a na analýze nátlaku z kapitoly 5. Inštitucionálne formy, v ktorých sa kapitál súkromia nasadzuje vo veľkom, prídu v kapitolách 24 až 26 a táto kapitola dodáva základ, ktorý predpokladajú.[12]

Poznámky

[1] Eugen von Böhm-Bawerk, *Capital and Interest*, vol. 2: *Positive Theory of Capital*, prel. George D. Huncke a Hans F. Sennholz (South Holland, IL: Libertarian Press, 1959), 13-21.

[2] Israel M. Kirzner, *Competition and Entrepreneurship* (Chicago: University of Chicago Press, 1973), 35-42.

[3] Bitcoin Core, `https://bitcoincore.org/`, s pôvodným opisom protokolu v Satoshi Nakamoto, „Bitcoin: A Peer-to-Peer Electronic Cash System“ (2008), `https://bitcoin.org/bitcoin.pdf`. K spracovaniu Bitcoinu v skupine systémov v cypherpunkovej línii pozri kap. 2, pozn. 8; k spracovaniu bezpečnostného modelu pozri kap. 5, pozn. 9.

[4] Carl Menger, *Principles of Economics*, prel. James Dingwall a Bert F. Hoselitz (Auburn, AL: Ludwig von Mises Institute, 2007 [1871]), 55-67. Mengerova teória rádov statkov, rozvinutá v úvodných kapitolách diela *Principles*, tvorí základ rakúskej teórie kapitálu. Spracovanie subjektívnej hodnoty citované v kap. 3, pozn. 5 pokrýva neskoršie kapitoly toho istého zväzku.

[5] Böhm-Bawerk, *Capital and Interest*, vol. 2, kapitoly 1-4; pozri tiež „The Roundabout Process in the Interest Theory," *Quarterly Journal of Economics* 21, no. 4 (1907): 529-590.

[6] Kirzner, *Competition and Entrepreneurship*, 65-85. K ďalšiemu rozvoju pozri Kirzner, *Perception, Opportunity, and Profit: Studies in the Theory of Entrepreneurship* (Chicago: University of Chicago Press, 1979).

[7] Joseph A. Schumpeter, *Capitalism, Socialism and Democracy*, 3rd ed. (New York: Harper & Row, 1950), 82-85, kde formulácia „tvorivá deštrukcia" dostáva svoje kanonické vyjadrenie.

[8] Peter G. Klein, *The Capitalist and the Entrepreneur: Essays on Organizations and Markets* (Auburn, AL: Ludwig von Mises Institute, 2010), 1-35.

[9] Friedrich A. Hayek, *The Pure Theory of Capital* (Chicago: University of Chicago Press, 1941), kapitoly 15-18; pozri tiež Hayek, *Individualism and Economic Order* (Chicago: University of Chicago Press, 1948), kapitoly 4-6.

[10] Peter Lewin, *Capital in Disequilibrium: The Role of Capital in a Changing World* (London: Routledge, 1999), 85-112. Lewin ukazuje, ako tvorba kapitálu zahŕňa hromadenie znalostí.

[11] K open source ako ekonomickému javu pozri Eric S. Raymond, *The Cathedral and the Bazaar*, rev. ed. (Sebastopol, CA: O'Reilly Media, 2001); Yochai Benkler, *The Wealth of Networks: How Social Production Transforms Markets and Freedom* (New Haven: Yale University Press, 2006).

[12] Ďalšie čítanie o rakúskej teórii kapitálu. Klasickým rakúskym spracovaním je Eugen von Böhm-Bawerk, *Capital and Interest*, 3 vols. (cit. v pozn. 1 vyššie). Ludwig M. Lachmann, *Capital and Its Structure* (Sheed Andrews and McMeel, 1956; reprinted by Ludwig von Mises Institute, 1978), `https://mises.org/library/capital-and-its-structure`, rozvíja heterogenitu a komplementaritu kapitálových statkov. Friedrich A. Hayek, *The Pure Theory of Capital* (cit. v pozn. 9 vyššie), je najprísnejším rozšírením. Ku kirznerovskej syntéze kapitálu, času a podnikateľského objavovania pozri Israel M. Kirzner, *An Essay on Capital* (Augustus M. Kelley, 1966). *Competition and Entrepreneurship* (cit. v pozn. 2 vyššie) rámec rozširuje a Kirzner sa rozoberá aj v kap. 7, pozn. 6 a 12. K moderným rakúskym spracovaniam pozri Peter Lewin, *Capital in Disequilibrium* (cit. v pozn. 10 vyššie); Peter Lewin a Nicolás Cachanosky, *Austrian Capital Theory: A Modern Survey of the Essentials* (Cambridge University Press, 2019), je najlepším súčasným vstupom. K otázke časovej preferencie osobitne Hans-Hermann Hoppe, *Democracy: The God That Failed* (cit. v kap. 5, pozn. 12); Hoppe, *The Great Fiction* (Laissez Faire Books, 2012), rozvíja dôsledky pre politickú ekonómiu. K open source výrobe ako spôsobu tvorby kapitálu pozri Yochai Benkler, *The Wealth of Networks* (cit. v pozn. 11 vyššie); Steven Weber, *The Success of Open Source* (Harvard University Press, 2004), je štandardným sociologickým spracovaním. K ekonomike vývoja softvéru a protokolov pozri Glyn Moody, *Rebel Code: Linux and the Open Source Revolution* (Perseus, 2001); Eric Raymond, *The Cathedral and the Bazaar* (cit. v pozn. 11 vyššie), je rozprávacou históriou.

[13] K časovým rámcom kryptografického výskumu a odstupu medzi teoretickými základmi a nasadenými aplikáciami pozri Whitfield Diffie a Martin E. Hellman, „New Directions in Cryptography," *IEEE Transactions on Information Theory* 22, no. 6 (1976): 644-654, `https://ieeexplore.ieee.org/document/1055638`. Štúdia z roku 1976 založila kryptografiu s verejným kľúčom ako teoretickú možnosť; RSA nasledovalo v roku 1977; masové nasadenie v TLS trvalo do polovice deväťdesiatych rokov, teda takmer dve desaťročia, čo ilustruje tu opísanú štruktúru výroby vyššieho a nižšieho rádu.

[14] Vrstvená štruktúra zodpovedá zásobníku protokolov opísanému v Steven Levy, *Crypto: How the Code Rebels Beat the Government - Saving Privacy in the Digital Age* (New York: Viking, 2001). Levyho rozprávanie ukazuje, ako akademická kryptografia s verejným kľúčom (najvyšší rád) umožnila PGP (stredný rád), ktoré umožnilo aplikácie šifrovanej pošty (najnižší rád), pričom každá vrstva závisí od tej nad ňou a umožňuje tie pod ňou.

[15] Hans-Hermann Hoppe, *Democracy: The God That Failed: The Economics and Politics of Monarchy, Democracy, and Natural Order* (New Brunswick, NJ: Transaction Publishers, 2001), kapitoly 1-2. Hoppe odvodzuje dôsledky teórie časovej preferencie pre akumuláciu kapitálu a civilizáciu z Misesovho rámca. Jeho analýza vysvetľuje, prečo inštitucionálne prostredia s vysokou časovou preferenciou systematicky vytláčajú dlhodobé investície, ktoré infraštruktúra súkromia vyžaduje.

[16] K bezpečnostným slabinám SMS pozri vlastné uznanie zraniteľností protokolu SS7 zo strany GSM Association: Adrian Lison, „SS7 Vulnerabilities and the Threats They Pose to Mobile Network Security," *GSMA Intelligence* (2017); Karsten Nohl et al., „Roaming Off the Beaten Track: Cellular Traffic Interception," *31st Chaos Communication Congress* (2014). K vytláčaniu šifrovanými správami pozri Open Whisper Systems (now Signal Messenger), `https://signal.org`, a špecifikáciu protokolu Signal: Trevor Perrin a Moxie Marlinspike, „The Double Ratchet Algorithm" (2016), `https://signal.org/docs/specifications/doubleratchet/`.

[17] Friedrich A. Hayek, *Denationalisation of Money: The Argument Refined*, 2nd ed. (London: Institute of Economic Affairs, 1978). Hayek tvrdil, že vládny monopol na emisiu peňazí nie je ani ekonomicky nevyhnutný, ani prospešný a že súťažiace súkromné meny by spotrebiteľom slúžili lepšie. Poskytol tak teoretický základ na chápanie kryptomeny ako vytláčania platobných systémov závislých od sledovania z ekonomických dôvodov.

[18] Ludwig M. Lachmann, *Capital and Its Structure* (London: Bell & Sons, 1956; reprinted Auburn, AL: Ludwig von Mises Institute, 1978), `https://mises.org/library/capital-and-its-structure`, kapitoly 2-3. Lachmann ukázal, že kapitálové statky sú druhovo heterogénne a vstupujú do zložitých vzťahov komplementarity a substituovateľnosti, ktoré sa menia podľa výrobného plánu. Žiadna inžinierska špecifikácia nemôže nahradiť podnikateľský úsudok, ktorý určuje, ktoré kombinácie sú životaschopné.

[19] Roger Dingledine, Nick Mathewson a Paul Syverson, „Tor: The Second-Generation Onion Router," *Proceedings of the 13th USENIX Security Symposium* (2004), `https://svn.torproject.org/svn/projects/design-paper/tor-design.pdf`; Tor Project, `https://www.torproject.org`. Tor je kanonickým príkladom infraštruktúry anonymných sietí ako kapitálového statku: roky akademického výskumu a priebežný vývoj vytvárajú smerovaciu vrstvu, na ktorú sa aplikácie súkromia spoliehajú a ktorú nevyčerpá žiadne jednotlivé použitie.

9

TEÓRIA PEŇAZÍ A ZDRAVÉ PENIAZE

„Peniaze sa zvyčajne znehodnocujú, keď ich je priveľa."
Nicolaus Copernicus, *Monete Cudende Ratio* (1517)[1]

Úvod

Každá výmena má dve strany a peniaze sú jednou z nich. Teória súkromia v ekonomickom živote musí začať peniazmi, nie preto, že by boli najzaujímavejším prípadom, ale preto, že sa im nedá vyhnúť. Či peňažné médium sleduje, alebo chráni súkromie, či sa dá vysledovať, alebo je nepreniknuteľné, či vyžaduje povolenie, alebo nie, tieto vlastnosti sa premietajú do každej transakcie, ktorá sa v ňom uskutoční.

Kapitola rozvíja rakúsky teoretický rámec na hodnotenie peňažných systémov. Peniaze vznikajú trhovým procesom, nie vládnym nariadením. Menger ukázal, prečo, a jeho argument nikto nevyvrátil. Zdravé peniaze (sound money) majú konkrétne vlastnosti, ktoré vyplývajú z troch funkcií: prostriedku výmeny, uchovávateľa hodnoty a zúčtovacej jednotky. Fiat peniaze tieto vlastnosti systematicky podkopávajú a pridávajú k nim štvrtú funkciu, o ktorej ich tvorcovia mlčia: infraštruktúru sledovania. Digitálne peniaze otvárajú otázku, či sa stratené vlastnosti dajú obnoviť.

Kapitola prechádza teoretické základy v tomto poradí: trhový pôvod peňazí, regresná teoréma a jej sporné uplatnenie na nové digitálne aktíva, vlastnosti, ktoré zdravé peniaze potrebujú (vrátane súkromia transakcií, ktoré bežné výklady vynechávajú), systematické zlyhania fiat peňazí, alternatíva slobodného bankovníctva, rozdiel medzi peniazmi v pravom zmysle a peňažnými náhradami a nakoniec požiadavky na zdravé digitál-

ne peniaze. Kapitoly 18 až 19 uplatňujú tento rámec priamo na Bitcoin. Spor o regresnú teorému a obmedzenia súkromia na Bitcoine sa preto odkladajú do nich.[2]

9.1 Trhový pôvod peňazí

Mengerov objav

Carl Menger ukázal, že peniaze vznikajú spontánnym trhovým procesom.[3] Peniaze nevymyslela žiadna vláda. Nevznikli ani zo spoločenskej zmluvy. Vznikli z nezávislého konania jednotlivcov, ktorí chceli umožniť výmenu.

Problémom barteru je dvojitá zhoda potrieb.[14] Aby k priamej výmene došlo, musí každá strana chcieť presne to, čo ponúka druhá. Pekár, ktorý chce topánky, musí nájsť obuvníka, ktorý chce chlieb. Čím viac sa hospodárstvo rozvíja a špecializuje, tým ťažšie sa takéto zhody nachádzajú.

Riešením je nepriama výmena. Ľudia začnú prijímať tovar, ktorý sami nechcú, no vedia ho ďalej vymeniť. Pekár môže prijať látku nie preto, aby ju nosil, ale preto, že ju prijme obuvník. Vymení chlieb za látku a látku za topánky. Dvoma výmenami tak dosiahne to, čo priamy barter nedokázal.

Vznik peňazí

Niektoré statky sa na nepriamu výmenu hodia obzvlášť dobre. Menger si všimol vlastnosť, ktorú nazval speňažiteľnosť (salability): ako ľahko sa statok dá vymeniť za iné statky. Vysoko speňažiteľné statky sa stávajú preferovaným prostriedkom výmeny.

Speňažiteľnosť závisí od deliteľnosti (dá sa statok rozdeliť na malé transakcie?), trvanlivosti (zachová si statok hodnotu v čase?), prenosnosti (dá sa efektívne prepravovať?) a rozpoznateľnosti (dá sa ľahko identifikovať a overiť?).

Statky s vyššou speňažiteľnosťou, historicky drahé kovy, sa stávajú všeobecne prijímaným prostriedkom výmeny. Peniaze tak vznikajú trhovým výberom, nie nariadením.

Etapy vývoja peňazí

Menger opísal postup od priameho barteru (kde výmenu obmedzuje dvojitá zhoda potrieb) cez nepriamu výmenu (kde sa kvalitnejšie statky prijímajú na ďalší obchod) až po všeobecné prijatie (kde sa najspeňažiteľnejší statok stáva univerzálne prijímaným) a napokon po postavenie zúčtovacej jednotky (kde sa peniaze stávajú mierkou pri oceňovaní a kalkulácii). Tento postup prebieha prostredníctvom rozhodnutí jednotlivcov, nie kolektívneho uznesenia. Každý, kto hľadá ľahšiu výmenu, sa prikláňa k statkom, ktoré prijmú aj ostatní. Výsledkom je spontánna zhoda na peniazoch.

9.2 Regresná teoréma

Problém hodnoty peňazí

Ako peniaze získavajú hodnotu? Bežné statky sa oceňujú kvôli priamemu užívaniu, no peniaze kvôli svojej výmennej sile, a tá zasa závisí od hodnoty peňazí. Úvaha sa zdá byť kruhová.

Mises ju vyriešil regresnou teorémou:[4] súčasná hodnota peňazí závisí od očakávanej budúcej kúpnej sily, a tá od kúpnej sily včerajška. Reťazec sa vracia späť až k okamihu, keď sa komodita, ktorá sa stala peniazmi, oceňovala kvôli nepeňažnému využitiu.

Zlato sa cenilo kvôli šperkom a ozdobám skôr, než sa stalo peniazmi. Striebro malo priemyselné a dekoratívne využitie. Dobytok slúžil ako potrava a ťažná sila skôr, než slúžil ako peniaze. Každé úspešné peniaze začali ako komodita ocenená kvôli priamej užitočnosti a až potom získali dodatočný peňažný dopyt vďaka svojej speňažiteľnosti.

Uplatnenie na nové peniaze

Regresná teoréma vyvoláva otázky o nových peniazoch, ktoré nikdy nemali nepeňažné využitie. Ak sa peniaze musia dať vysledovať až k pôvodnej hodnote komodity, ako môžu vzniknúť peniaze celkom nové? Táto otázka rozdelila rakúskych ekonómov a spor nie je uzavretý.[5]

Niektorí autori tvrdia, že nové digitálne peniaze teorému nespĺňajú. Podľa nich musia peniaze vzniknúť z komodity s predchádzajúcou užitkovou hodnotou. Digitálne aktíva bez fyzického komoditného krytia sa nemôžu stať skutočnými peniazmi a fungujú len ako prostriedok výmeny postavený na existujúcich fiat peniazoch.

Opačný názor hovorí, že požiadavky teorémy spĺňa subjektívne hodnotenie akéhokoľvek druhu. Subjektívna teória hodnoty, základ rakúskej metodológie, tvrdí, že hodnota existuje len v mysliach ľudí, ktorí hodnotia. Teoréma ukazuje, že súčasná hodnota peňazí sa vracia k predchádzajúcemu hodnoteniu. Tie predchádzajúce hodnotenia však samy pochádzajú zo subjektívnych súdov jednotlivcov, nie z objektívnych vlastností komodity. Ak mali prví oceňovatelia akýkoľvek dôvod peniaze oceniť a táto hodnota sa prenášala trhovou výmenou, regresný reťazec sa môže rozbehnúť. Praxeológia nedáva žiadny základ na to, aby sa niektoré subjektívne hodnotenia vyhlásili za oprávnené a iné za neoprávnené.

Ešte jedna interpretačná poznámka oddeľuje vysvetľovaciu silu teorémy od metafyzickej nevyhnutnosti. Teoréma vysvetľuje, ako peniaze zvyčajne vznikajú trhovým procesom, a ukazuje, že peňažnú hodnotu nemusí určiť autorita. Nemusí však obmedzovať, ktoré statky sa môžu stať peniazmi, ak si ich účastníci trhu začnú ceniť.

Táto kniha sa prikláňa k výkladu založenému na subjektívnej hodnote. Otázka zostáva v rakúskej ekonómii sporná a uvážliví autori sa v nej

rozchádzajú. Základný poznatok teorémy, že peniaze vznikajú trhovým procesom a nie nariadením, nikto nespochybňuje. Otvorené je, či digitálne aktíva bez predchádzajúceho fyzického komoditného využitia môžu požiadavky teorémy splniť, alebo či ide o nový jav, ktorý teóriu peňazí rozširuje. Kapitola 19 uplatňuje tento rámec priamo na Bitcoin.

9.3 Vlastnosti zdravých peňazí

Zdravé peniaze majú vlastnosti, vďaka ktorým môžu slúžiť ekonomickej koordinácii. Vyplývajú z funkcií peňazí, nie zo svojvoľných preferencií.[6]

Tri klasické funkcie

Peniaze plnia tri funkcie a každá kladie na médium, ktoré ju vykonáva, určité požiadavky.

Ako **prostriedok výmeny** musia byť peniaze v obchode prijateľné. Obchodní partneri musia vedieť overiť pravosť bez špeciálneho vybavenia, čo vyžaduje rozpoznateľnosť a zvyšuje náklady falšovania. Médium sa musí dať deliť na transakcie ľubovoľnej veľkosti, lebo nedeliteľné peniaze výmenu obmedzujú. A vzhľadom na svoju hodnotu musí byť prenosné: vysoký pomer hodnoty k hmotnosti umožňuje väčšie obchody a siaha ďalej.

Ako **uchovávateľ hodnoty** musia peniaze zachovať kúpnu silu v čase. Fyzické peniaze musia odolávať opotrebovaniu a digitálne peniaze strate údajov, čo spolu dáva trvanlivosť. Ponuka musí byť predvídateľná, lebo svojvoľná inflácia ničí funkciu uchovávateľa hodnoty bez ohľadu na ostatné prednosti média. A držiteľ musí vedieť odolať konfiškácii, lebo peniaze, ktoré sa dajú ľubovoľne zhabať, sú slabým úložiskom, nech majú v abstraktnom zmysle akékoľvek peňažné vlastnosti.

Ako **zúčtovacia jednotka** musia peniaze umožňovať ekonomickú kalkuláciu. Hodnota musí byť dosť stabilná, aby ceny niesli informáciu. Prudké výkyvy kazia cenové signály, ktoré koordinujú výrobu a výmenu. Jednotky musia byť zameniteľné, lebo peniaze, ktorých hodnota závisí od ich histórie, komplikujú kalkuláciu na každom kroku a znemožňujú ju.

Súkromie ako vlastnosť zdravých peňazí

Súkromie transakcií je vlastnosť zdravých peňazí, ktorú bežné výklady často prehliadajú, hoci vyplýva z ostatných. Ako ukázala kapitola 7, výmena funguje najlepšie, keď strany majú kontrolu nad odhaľovaním. Peniaze, ktoré vystavujú všetky transakcie, deformujú dobrovoľnú koordináciu. Peniaze, ktoré umožňujú sledovanie treťou stranou, umožňujú aj jej zásahy. A peniaze, ktorých jednotky sa dajú rozlíšiť a diskriminovať, strácajú zameniteľnosť, ktorú kalkulácia potrebuje. Súkromie preto nie je ďalšia požiadavka prilepená k funkcii prostriedku výmeny. Je to podmienka, za ktorej ostatné tri funkcie ďalej fungujú.

Fyzická hotovosť má túto vlastnosť prirodzene: transakcie nezanechávajú automatický záznam. Chýbajúce záznamy nie sú chyba, ale prednosť, ktorá umožňuje dobrovoľnú výmenu bez sledovania. Digitálne peniaze, ktoré túto vlastnosť stratia, strácajú viac než súkromie. Strácajú aj časť peňažnej schopnosti, ktorú súkromie chránilo.

9.4 Fiat peniaze a ich problémy

Čo sú fiat peniaze

Fiat peniaze sú peniaze z príkazu vlády. Nemajú komoditné krytie. Ich hodnotu zakladajú zákony o zákonnom platidle, ktoré vyžadujú ich prijatie, a daňové povinnosti splatné len vo fiat mene.

Moderné fiat meny (dolár, euro, jen) sú toho príkladom: papier a digitálne zápisy majú hodnotu preto, že to vlády hovoria, a svoje slovo aj vynucujú.

Problém inflácie

Fiat peniaze umožňujú neobmedzené rozširovanie ponuky. Centrálne banky vytvárajú peniaze podľa vlastného uváženia, obmedzujú ich len politické ohľady. To spôsobuje systematické problémy.[7]

Nové peniaze vstupujú do hospodárstva určitými kanálmi, napríklad bankovými úvermi a vládnymi výdavkami. Prví príjemcovia míňajú za staré ceny, neskorší sa stretnú s cenami už zvýšenými. Tento mechanizmus presúva bohatstvo od neskorších príjemcov k skorším. Keď ceny rastú nepredvídateľne, podniky nedokážu rozlíšiť skutočné zmeny dopytu od peňažného skreslenia a zdroje plynú do odvetví, ktoré infláciu zvýhodňuje, namiesto využitia, ktoré uprednostňujú spotrebitelia. Tým sa kazí ekonomická kalkulácia. Inflácia trestá sporiteľov, ktorým klesá kúpna sila, a odmeňuje dlžníkov, ktorým záväzky reálne klesajú, a tak odrádza od tvorby kapitálu. Umelé rozširovanie úverov vytvára neudržateľné konjunktúry, po ktorých nasledujú nevyhnutné krízy. Chybné investície z čias expanzie sa musia v období poklesu zlikvidovať. Tak vzniká hospodársky cyklus.

Problém sledovania

Fiat peniaze v modernej podobe sú sledované peniaze. Digitálne fiat transakcie sa zaznamenávajú, hlásia, analyzujú a dajú sa ovládať. Banky vedú úplnú históriu ako súčasť bežnej prevádzky. Predpisy vyžadujú oznamovanie úradom pri čoraz nižších hraniciach. Z výsledných tokov sa analýzou vzorcov získavajú osobné informácie. A účty sa dajú zmraziť alebo transakcie zablokovať na pokyn úradov, ktoré si držiteľ nevybral.

Táto schopnosť sledovania sa dramaticky rozšírila s požiadavkami na povinné overenie totožnosti zákazníka (Know Your Customer, KYC),[15] s monitorovaním v rámci boja proti praniu špinavých peňazí (Anti-Money

Laundering, AML), s automatickou výmenou informácií medzi jurisdikciami[16] a s nižšími hranicami na hlásenie transakcií, ktoré zachytia čoraz viac platieb.

Výsledok je jednoduchý: používanie fiat peňazí vytvára úplné záznamy o sledovaní. Súkromie v ekonomickom živote vyžaduje alternatívy k sledovaným fiat systémom.

Problém kontroly

Fiat peniaze umožňujú ekonomickú kontrolu na viacerých úrovniach. Úrady môžu zmraziť účty a zabrániť ľuďom v prístupe k vlastným peniazom. Môžu blokovať konkrétne platby. Môžu odoprieť finančný prístup úplne, vyradením z platformy, a sankciami môžu vylúčiť z platobných sietí celé štáty. Každá z týchto schopností stojí na tom istom fakte: peniaze sú nárok voči sprostredkovateľovi, na ktorého štát dosiahne.

Túto kontrolu možno použiť proti zločincom, ale aj proti disidentom, novinárom, aktivistom a každému, kto sa nepáči tým, čo kontrolu držia. Fiat peniaze sú peniaze závislé od povolenia: transakciu možno uskutočniť, ak to úrady dovolia.

9.5 Slobodné a centrálne bankovníctvo

Alternatíva slobodného bankovníctva

Slobodné bankovníctvo (free banking) je konkurenčný systém peňazí a bankovníctva bez monopolu centrálnej banky.[8] Viacero bánk vydáva vlastné bankovky a súťaží o zákazníkov spoľahlivosťou a službami.

Historické príklady (Škótsko 1716–1845, Kanada pred rokom 1935) naznačujú, že systémy slobodného bankovníctva boli stabilnejšie než centrálne bankovníctvo, s menším počtom kríz a lepšími službami pre zákazníkov. Toto hodnotenie sa spája s Lawrencom Whiteom a Georgeom Selginom a v rakúskej tradícii je sporné. Murray Rothbard a ďalší uprednostňovali bankovníctvo so 100 % rezervami pred slobodným bankovníctvom s čiastočnými rezervami.[9] Trhová disciplína bránila nadmernému riskovaniu: banky, ktoré vydali priveľa bankoviek, prichádzali o zákazníkov v prospech opatrnejších konkurentov.

Slobodné bankovníctvo chráni súkromie prostredníctvom konkurencie. Banky slúžia zákazníkom a zákazníci, ktorým na súkromí záleží, si vyberú banky, ktoré ho rešpektujú. Žiadna jediná autorita nemôže vnútiť sledovanie celej finančnej činnosti.

Problémy centrálneho bankovníctva

Centrálne bankovníctvo nahrádza trhovú konkurenciu monopolom a z tejto výmeny vyplýva viacero problémov. Vzniká jediný bod zlyhania, lebo chyby jednej inštitúcie postihnú celé hospodárstvo naraz. Nasleduje poli-

tické zachytenie, lebo menová politika potom slúži politickým cieľom namiesto ekonomických. Rozvíja sa morálny hazard, keď banky podstupujú nadmerné riziko v istote, že ich centrálna banka zachráni. A jednotný regulačný rámec umožňuje štandardizované sledovanie a úplné monitorovanie.

Prechod od konkurenčného k centrálnemu bankovníctvu, ktorý sa vo väčšine krajín dokončil do polovice dvadsiateho storočia, nahradil peniaze trhu peniazmi pod politickou kontrolou, a tomu zodpovedala aj strata súkromia.

9.6 Peniaze v pravom zmysle a peňažné náhrady

Rakúska teória peňazí rozlišuje medzi peniazmi v pravom zmysle (money proper) a peňažnými náhradami (money substitutes).[10]

Peniaze v pravom zmysle sú základné peniaze (base money): konečný platobný prostriedok, ktorý už nevyžaduje žiadne ďalšie vyplatenie. Zlaté mince v ruke sú peniaze v pravom zmysle. Držiteľ má hodnotu priamo v ruke. Niet emitenta, ktorému by sa muselo veriť, žiadna protistrana, ktorá musí splniť záväzok, žiadny nárok, ktorý treba uspokojiť.

Peňažné náhrady sú nároky voči peniazom v pravom zmysle. Bankovka, ktorá sľubuje zlato na požiadanie, je peňažná náhrada. Zostatok na bankovom účte je peňažná náhrada. Držiteľ nemá peniaze samotné, ale sľub emitenta.

Peňažné náhrady nesú riziko protistrany. Držiteľ musí dôverovať, že emitent existuje, drží sľúbené rezervy, vyplatí na požiadanie a že mu v tom nik nezabráni. Keď emitenti zlyhajú, keď ich zatvoria alebo keď odmietnu vyplácať, peňažné náhrady sa stanú bezcennými, aj keď peniaze v pravom zmysle, na ktoré sa viazali, stále existujú.

Pri digitálnych peniazoch na tomto rozdiele záleží. Každá digitálna mena pred Bitcoinom bola peňažná náhrada: nárok voči emitentovi, ktorý vedie zostatky na účtoch. Účty e-gold boli nároky na zlato, ktoré držala firma. Zostatky Liberty Reserve boli nároky voči účtovníctvu tejto firmy a tokeny DigiCash boli nároky potvrdzované centrálnym serverom. Keď týchto emitentov zatvorili, používatelia prišli o všetko.[11] Toto zlyhanie bolo zabudované v samotnej podstate: peňažné náhrady potrebujú dôveryhodných emitentov a dôveryhodní emitenti sú zraniteľní.

Pre zdravé digitálne peniaze z toho vyplýva otázka: môže byť digitálne aktívum peniazmi v pravom zmysle, a nie peňažnou náhradou? Môže byť samotnou vecou, a nie nárokom na ňu?

Súčasná menová architektúra

Rozlíšenie medzi peniazmi v pravom zmysle a peňažnými náhradami vysvetľuje dnešnú štruktúru fiat peňazí.

Základné peniaze existujú v dvoch podobách. Fyzická hotovosť patrí k základným peniazom, ktoré môže priamo držať široká verejnosť. Rezervy centrálnej banky sú tiež základné peniaze, ale prístup k nim majú len obchodné banky a vlády. Bežní občania si nemôžu otvoriť účet vo Federálnom rezervnom systéme (Fed)[17] ani v Európskej centrálnej banke (ECB).[18]

To, čo občania držia na bankových účtoch, nie sú základné peniaze, ale peňažné náhrady: nároky voči obchodným bankám. Zostatok v banke je dlžobný úpis banky, nie samotné základné peniaze. Preto zlyhania bánk ničia vklady, hoci základné peniaze naďalej existujú.

Táto architektúra vytvára nárazník medzi štátom a občanom. Centrálna banka vydáva základné peniaze obchodným bankám a obchodné banky vydávajú peňažné náhrady občanom. Občania sa s menovou autoritou stretávajú len nepriamo, cez súkromné inštitúcie. Kapitola 10 skúma, ako by digitálne meny centrálnych bánk tento nárazník zrušili, keď by občanom dali priame zostatky základných peňazí v centrálnej banke, s priamymi dôsledkami pre sledovanie a kontrolu.

9.7 Požiadavky na digitálne peniaze

Čo by zdravé digitálne peniaze vyžadovali? Rakúska teória peňazí naznačuje niekoľko kritérií.[12]

Zdravé digitálne peniaze vyžadujú decentralizované overovanie: vyriešiť problém dvojitého míňania bez dôveryhodných tretích strán, bez jediného miesta, ktoré by sa dalo zachytiť, skorumpovať alebo prinútiť, a s overovaním rozloženým medzi účastníkov namiesto sústredenia v jednej autorite.

Digitálna vzácnosť prostredníctvom rivality je nevyhnutná na to, aby sa dali uplatniť vlastnícke práva, a práve tu sa digitálne peniaze líšia od bežných digitálnych informácií. Jednotky musia byť rivalitné, čo znamená, že držba jednej osoby vylučuje držbu inej. Fyzické statky sú prirodzene rivalitné, digitálne informácie nie. Vyriešenie dvojitého míňania rivalitu vytvára: ak sa ten istý token nedá minúť dvakrát, držba sa stáva výlučnou a až vtedy môžu vzniknúť vlastnícke práva. Bez rivality zostávajú digitálne tokeny informáciou, ktorú možno ľubovoľne kopírovať, a vlastníctvom byť nemôžu.

Od samotnej vzácnosti sa líši požiadavka na transparentnú a nemennú ponuku. Zdravé digitálne peniaze vyžadujú, aby celková ponuka a pravidlá emisie boli transparentné, overiteľné a aby ich žiadna tretia strana nemohla jednostranne meniť. To sa líši od fiat peňazí, kde sú rozhodnutia o ponuke nepriehľadné a zmeny politiky závisia od uváženia centrálnej banky. Transparentnosť umožňuje racionálnu ekonomickú kalkuláciu spôsobom, aký nepriehľadná menová politika nedovolí.

Pravidlá určené používateľmi obracajú tradičný model, v ktorom peňažné systémy vnucujú pravidlá zhora a používatelia sa prispôsobia alebo odídu. V zdravých digitálnych peniazoch každý účastník pravidlá, ktoré prijíma, sám určuje, overuje a presadzuje. Prevádzkovať plný uzol (full node) znamená overovať každú transakciu podľa pravidiel, ktoré si človek zvolil sám. Konsenzus vzniká tým, že účastníci nezávisle dospejú k zlučiteľným pravidlám, nie tým, že autorita vnúti jednotnosť. Pravidlá sú to, čo sieť presadzuje, nie to, čo vyhlási nejaká autorita. Zmeny vyžadujú presvedčiť používateľov, aby prijali nový softvér, a predvolený stav je status quo.

Zdravé digitálne peniaze musia byť tiež bez nutnosti povolenia, zachovávať súkromie, odolávať cenzúre a byť prijímané dobrovoľne. Prístup bez povolenia znamená, že použitie nekontroluje žiadny strážca. Súkromie transakcií znamená, že overenie je možné bez automatického sledovania a používatelia majú kontrolu nad tým, čo sa odhalí. Odolnosť voči cenzúre znamená, že sa transakcie vykonajú vždy, keď sú splnené pravidlá protokolu, a žiadna tretia strana ich nemôže povoliť ani zakázať. Dobrovoľné prijatie znamená, že systém vzniká trhovým procesom a svoju hodnotu potvrdzuje výmenou.

9.8 Most k Bitcoinu

Kapitoly 18 až 19 skúmajú Bitcoin ako uskutočnenie týchto požiadaviek. Tu uvedieme len základné črty tejto analýzy.

Bitcoin sa snaží splniť požiadavky teórie peňazí decentralizovaným overovaním cez konsenzus dôkazu práce (proof-of-work),[19] digitálnou vzácnosťou vďaka vyriešeniu dvojitého míňania, transparentnou a nemennou ponukou cez pravidlá protokolu, ktoré presadzuje každý uzol, a suverenitou používateľa, keď každý účastník nezávisle overuje pravidlá, ktoré prijíma. Bitcoin má v oblasti súkromia obmedzenia: základné bitcoinové transakcie sú pseudonymné, nie anonymné, analýza reťazca ich dokáže prepojiť s identitami[20] a súkromie vyžaduje ďalšie nástroje, o ktorých pojednáva kapitola 20.

Kapitola 19 rozvíja aj analýzu regresnej teorémy pre Bitcoin: skúma, ako sa rámec subjektívnej hodnoty uplatňuje na jeho vznik ako peňazí.

Zhrnutie kapitoly

Peniaze vznikajú trhovým procesom, nie vládnym nariadením. Menger ukázal, že jednotlivci, ktorí chcú prekonať dvojitú zhodu potrieb pri barteri, sa prirodzene ustália na statkoch s vyššou speňažiteľnosťou, a spontánny vznik vysvetľuje pôvod peňazí bez centrálneho plánovania. Zdravé peniaze majú vlastnosti vyplývajúce z troch funkcií, prostriedku výmeny, uchovávateľa hodnoty a zúčtovacej jednotky, a súkromie transakcií patrí

k nim. Peniaze, ktoré vystavujú všetky transakcie, deformujú dobrovoľnú koordináciu, ktorú majú ostatné vlastnosti podporovať.

Fiat peniaze vytvárajú systematické problémy, ktoré rakúska tradícia dokumentuje už sto rokov. Neobmedzené rozširovanie ponuky presúva bohatstvo od neskorších príjemcov k skorším, kazí kalkuláciu, od ktorej výroba závisí, ničí úspory a vyvoláva hospodársky cyklus. Moderné fiat peniaze sú aj sledovacie peniaze: vytvárajú záznamy o transakciách, ktoré umožňujú monitorovanie a kontrolu. Rozlíšenie medzi peniazmi v pravom zmysle a peňažnými náhradami osvetľuje súčasnú architektúru: fyzická hotovosť je jediná podoba základných peňazí, ktorú môžu občania držať priamo, kým zostatky na účtoch sú nároky voči obchodným bankám a dajú sa zmraziť, zhabať alebo odoprieť pod právnym tlakom, ktorému sa banka nemôže vzoprieť. Kapitola 10 skúma, čo sa stane, keď sa štát pokúsi tento nárazník odstrániť digitálnymi menami centrálnych bánk.

Digitálne peniaze môžu obnoviť vlastnosti, ktoré fiat peniaze stratili. Požiadavky, ktorými sú decentralizované overovanie, digitálna vzácnosť cez rivalitu, transparentná a nemenná ponuka, pravidlá určené používateľmi, prístup bez povolenia, súkromie transakcií a odolnosť voči cenzúre, sú to, čo kapitoly 18 až 20 posudzujú na príklade Bitcoinu, vrátane jeho skutočných obmedzení v oblasti súkromia. Uplatnenie regresnej teorémy na nové digitálne peniaze zostáva v rakúskej ekonómii sporné. Táto kniha sa prikláňa k výkladu založenému na subjektívnej hodnote, no samotnú otázku necháva otvorenú. Kapitola kritizuje systematické problémy fiat peňazí, no ich funkciu prostriedku výmeny uznáva.[13]

Poznámky

[1] Nicolaus Copernicus, *Monete Cudende Ratio* (*On the Minting of Money*, 1517; niekedy s názvom *Monetae Cudendae Ratio*). Anglický preklad v Nicholas Copernicus, *Minor Works*, prel. Edward Rosen a Erna Hilfstein (Baltimore: Johns Hopkins University Press, 1992; Warsaw: Polish Scientific Publishers, 1985). Napísané desaťročia predtým, než Sir Thomas Gresham sformuloval zásadu „zlé peniaze vytláčajú dobré", Copernicus rozpoznal princíp kvantitatívnej teórie peňazí, ktorý stojí za znehodnocovaním meny, aj to, čo sa neskôr nazvalo Greshamov zákon. Pre kanonické moderné rakúske spracovanie, o ktoré sa kapitola opiera, pozri Mises, *Human Action* (uvedené v kapitole 3, poznámka 1), 398 a časť IV.

[2] Prístupné knižné spracovania, ktoré pokrývajú oblúk od komoditných peňazí cez fiat peniaze k digitálnym: Saifedean Ammous, *The Bitcoin Standard* (Hoboken, NJ: John Wiley & Sons, 2018); Nik Bhatia, *Layered Money* (Self-published, 2021); Lyn Alden, *Broken Money: Why Our Financial System Is Failing Us and How We Can Make It Better* (Timestamp Press, 2023). Každý z nich pristupuje k rovnakému oblúku z iného uhla: Ammous z rakúskej teórie peňazí, Bhatia z vrstvenej štruktúry peňažných systémov, Alden z dejín peňazí a makroekonómie.

[3] Carl Menger, „On the Origin of Money," *Economic Journal* 2, č. 6 (1892): 239–255. Pozri tiež Menger, *Principles of Economics* (uvedené v kapitole 3, poznámka 5), kapitola 8.

[4] Ludwig von Mises, *The Theory of Money and Credit*, prel. H. E. Batson (Indianapolis: Liberty Fund, 1981 [1912]), 97–123. Pozri tiež Mises, *Human Action* (uvedené v kapitole 3, poznámka 1), 408–416.

[5] Pre skeptické názory na Bitcoin a regresnú teorému pozri Frank Shostak, „The Bitcoin Money Myth," *Mises Daily* (April 17, 2013), `https://mises.org/mises-daily/bitcoin-money-myth`. Pre obhajoby zlučiteľnosti Bitcoinu s teorému pozri Peter Šurda, „Economics of Bitcoin: Is Bitcoin an Alternative to Fiat Currencies and Gold?" (master's thesis, Vienna University of Economics and Business, 2012); Konrad Graf, „On the Origins of Bitcoin: Stages of Monetary Evolution" (2013), `https://konradsgraf.com`; Eric Voskuil, „Regression Fallacy," v *Cryptoeconomics* (uvedené v kapitole 5, poznámka 1), `https://github.com/libbitcoin/libbitcoin-system/wiki/Regression-Fallacy`. Pre nedávnu syntézu pozri Laura Davidson a Walter Block, „Bitcoin, the Regression Theorem, and the Emergence of a New Medium of Exchange," *Quarterly Journal of Austrian Economics* 18, č. 3 (2015): 311–338.

[6] O vlastnostiach zdravých peňazí pozri Mises, *The Theory of Money and Credit* (uvedené v poznámke 4 vyššie), časť I; Murray N. Rothbard, *What Has Government Done to Our Money?*, 5th ed. (Auburn, AL: Ludwig von Mises Institute, 2010), kapitoly 1–3.

[7] O problémoch fiat peňazí pozri Rothbard, *What Has Government Done to Our Money?* (uvedené v poznámke 6 vyššie); Jörg Guido Hülsmann, *The Ethics of Money Production* (Auburn, AL: Ludwig von Mises Institute, 2008); Hans-Hermann Hoppe, „How Is Fiat Money Possible? or, The Devolution of Money and Credit," *Review of Austrian Economics* 7, č. 2 (1994): 49–74.

[8] O slobodnom bankovníctve pozri Lawrence H. White, *Free Banking in Britain: Theory, Experience and Debate, 1800-1845*, 2nd ed. (London: Institute of Economic Affairs, 1995); George A. Selgin, *The Theory of Free Banking* (Lanham, MD: Rowman & Littlefield, 1988).

[9] Pre Rothbardovu kritiku slobodného bankovníctva s čiastočnými rezervami pozri Murray N. Rothbard, *The Mystery of Banking*, 2nd ed. (Auburn, AL: Ludwig von Mises Institute, 2008), a „The Case for a 100 Percent Gold Dollar," v *In Search of a Monetary Constitution*, ed. Leland Yeager (Cambridge, MA: Harvard University Press, 1962). Spor medzi zástancami 100 % rezerv (Rothbard, Jesús Huerta de Soto) a zástancami slobodného bankovníctva s čiastočnými rezervami (White, Selgin) zostáva v rakúskej tradícii nevyriešený.

[10] O peniazoch v pravom zmysle a peňažných náhradách (nazývaných aj fiduciárne médiá) pozri Mises, *The Theory of Money and Credit* (uvedené v poznámke 4 vyššie), časť II, kapitoly 1–3; tiež Mises, *Human Action* (uvedené v kapitole 3, poznámka 1), 432–444.

[11] E-gold fungovalo od roku 1996 do obžaloby v roku 2007 a zatvorenia v roku 2009 (*United States v. E-Gold, Ltd.*, D.D.C. 2008). Liberty Reserve fungovalo od roku 2006 do zhabania americkými úradmi v máji 2013 (*United States v. Liberty Reserve S.A.*, S.D.N.Y. 2013). DigiCash, ktorý v roku 1989 založil David Chaum, vyhlásil bankrot v roku 1998. O Chaumovej staršej práci o nevystopovateľných platbách pozri Chaum, „Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms" (uvedené v kapitole 2, poznámka 6).

[12] O uplatnení rakúskej teórie peňazí na digitálne peniaze pozri Ammous, *The Bitcoin Standard* (uvedené v poznámke 2 vyššie); Eric Voskuil, *Cryptoeconomics: Fundamental Principles of Bitcoin* (uvedené v kapitole 5, poznámka 1).

[13] Ďalšie čítanie o teórii peňazí pre čitateľa, ktorý sa k tejto kapitole dostáva spoza rakúskej tradície. Nenahraditeľným primárnym zdrojom je Mises, *The Theory of Money and Credit* (uvedené v poznámke 4 vyššie), základné rakúske spracovanie, ktoré ako prvé uplatnilo Mengerov marginalizmus na peniaze. Misesovo neskoršie dielo *Human Action* (uvedené v kapitole 3, poznámka 1), časti III–IV, spája teóriu peňazí s úplným praxeologickým rámcom. Rothbard, *What Has Government Done to Our Money?* (uvedené v poznámke 6 vyššie), je najkratší úvod. *The Mystery of Banking* (uvedené v poznámke 9 vyššie) je dlhšie

praktické spracovanie. Jesús Huerta de Soto, *Money, Bank Credit, and Economic Cycles*, 3rd ed. (Auburn, AL: Ludwig von Mises Institute, 2012), https://mises.org/library/money-bank-credit-and-economic-cycles, je najširšie súčasné rakúske spracovanie peňazí a bankovníctva. Pre stranu slobodného bankovníctva sú referenčnými dielami Lawrence H. White, *The Theory of Monetary Institutions* (Oxford: Blackwell, 1999), a Selgin, *The Theory of Free Banking* (uvedené v poznámke 8 vyššie). Pre dejiny podané rozprávaním: Murray N. Rothbard, *A History of Money and Banking in the United States* (Auburn, AL: Ludwig von Mises Institute, 2002), a Vera C. Smith, *The Rationale of Central Banking and the Free Banking Alternative* (Indianapolis: Liberty Fund, 1990 [1936]), pokrývajú inštitucionálny vývoj. K regresnej teoréme pozri Menger, „On the Origin of Money" (uvedené v poznámke 3 vyššie), a jeho uplatnenie na Bitcoin v Šurda, „Economics of Bitcoin" (uvedené v poznámke 5 vyššie), a Graf, „On the Origins of Bitcoin" (uvedené v poznámke 5 vyššie). Pre opačnú školu, ktorá si zaslúži vážnu diskusiu: Milton Friedman a Anna J. Schwartz, *A Monetary History of the United States, 1867-1960* (Princeton, NJ: Princeton University Press, 1963), je základné monetaristické empirické dielo. Milton Friedman, *A Program for Monetary Stability* (New York: Fordham University Press, 1960), je najkratšie vyjadrenie politiky. John Maynard Keynes, *A Tract on Monetary Reform* (London: Macmillan, 1923), podáva menovú analýzu opačnej tradície. Pre súčasné heterodoxné myslenie o peniazoch Perry Mehrling, *The New Lombard Street: How the Fed Became the Dealer of Last Resort* (Princeton, NJ: Princeton University Press, 2011), vysvetľuje moderné inštitucionálne usporiadanie, ktoré rakúska teória kritizuje.

[14] W. Stanley Jevons, *Money and the Mechanism of Exchange* (London: Kegan Paul, 1875), kapitola 1. Jevons razil výraz „double coincidence of wants" (dvojitá zhoda potrieb) a podal prvé systematické vysvetlenie, prečo barter pri väčšom rozsahu zlyháva. Mengerov nezávislý objav trhového pôvodu peňazí (uvedený v poznámke 3 vyššie) dopĺňa túto analýzu pohľadom zo strany ponuky.

[15] Bank Secrecy Act, Pub. L. 91-508, 84 Stat. 1114 (1970), kodifikované v 31 U.S.C. §§ 5311–5336. Zákon o bankovom tajomstve (Bank Secrecy Act) vytvoril základný americký rámec hlásenia v oblasti KYC a AML. Finančným inštitúciám ukladá viesť záznamy o transakciách a podávať hlásenia o hotovostných transakciách (Currency Transaction Reports, CTR) nad 10 000 dolárov a hlásenia o podozrivej činnosti (Suspicious Activity Reports, SAR) pri nezvyčajných vzorcoch. Aktuálne pokyny FinCEN k vykonávaniu pozri U.S. Department of the Treasury, Financial Crimes Enforcement Network, https://www.fincen.gov.

[16] Financial Action Task Force (FATF), *International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation* (Paris: FATF, 2012, updated 2023), https://www.fatf-gafi.org/en/topics/fatf-recommendations.html; OECD, *Standard for Automatic Exchange of Financial Account Information in Tax Matters*, 2nd ed. (Paris: OECD Publishing, 2017), https://doi.org/10.1787/9789264267992-en. Odporúčania FATF určujú globálny štandard KYC a AML, ktorý prijalo vyše 200 jurisdikcií. Spoločný štandard OECD pre podávanie správ (Common Reporting Standard, CRS) zavádza automatickú cezhraničnú výmenu údajov o finančných účtoch a dáva štátom úplný prehľad o zahraničných aktívach občanov.

[17] Federal Reserve Act, Pub. L. 63-43, 38 Stat. 251 (1913). Zákon o Federálnom rezervnom systéme (Federal Reserve Act) vytvoril americký systém centrálneho bankovníctva, Radu guvernérov Federálneho rezervného systému a dvanásť regionálnych federálnych rezervných bánk. Rezervné účty vo Federálnom rezervnom systéme sú prístupné len členským obchodným bankám a niektorým ďalším depozitným inštitúciám, nie širokej verejnosti. Aktuálnu politiku prístupu k účtom Fedu pozri Board of Governors of the Federal Reserve System, https://www.federalreserve.gov.

[18] Treaty on the Functioning of the European Union, art. 282 (2007); Protocol No. 4 on the Statute of the European System of Central Banks and of the European Central Bank. ECB bola zriadená Maastrichtskou zmluvou (1992) a svoju činnosť začala v roku 1998. Rovnako ako Federálny rezervný systém vedie rezervné účty pre úverové inštitúcie eurozóny, ale nie pre fyzické osoby ani nefinančné subjekty. European Central Bank, https://www.ecb.europa.eu.

[19] Satoshi Nakamoto, „Bitcoin: A Peer-to-Peer Electronic Cash System“ (2008), https://bitcoin.org/bitcoin.pdf. Oddiel 4 zavádza dôkaz práce ako mechanizmus na dosiahnutie distribuovaného konsenzu bez dôveryhodnej tretej strany. Reťazec kumulovanej práce nahrádza potrebu centrálnej autority, ktorá by usporadúvala transakcie, a tým rieši dvojité míňanie. Je to základný technický dokument pre všetky ďalšie analýzy Bitcoinu ako peňažného systému.

[20] Sarah Meiklejohn et al., „A Fistful of Bitcoins: Characterizing Payments Among Men with No Names,“ *Proceedings of the 2013 Internet Measurement Conference* (ACM, 2013), https://dl.acm.org/doi/10.1145/2504730.2504747. Meiklejohn a kol. ukázali, že verejný blockchain Bitcoinu umožňuje heuristické zhlukovanie adries podľa spoločného vlastníctva vstupov, čo cez analýzu grafu dovoľuje deanonymizovať významnú časť transakcií. Je to základný akademický výsledok, ktorý dokazuje, že pseudonymita sa podstatne líši od anonymity.

ČASŤ IV

PROTIVNÍK

10

FINANČNÉ SLEDOVANIE A ŠTÁTNA KONTROLA

„Štát je organizácia politických prostriedkov."
Franz Oppenheimer, *The State* (1907)[1]

Úvod

Rothbardova typológia intervencií odlišuje autistickú a binárnu intervenciu od trojuholníkovej, pri ktorej štát zasahuje do výmen medzi tretími stranami.[2] Tento rámec ukazuje, ako štáty sledujú a kontrolujú prostredníctvom financií. Vrcholom sú digitálne meny centrálnych bánk (CBDC), ktoré spájajú všetky tri druhy intervencie.

10.1 Teória intervencií: autistická, binárna, trojuholníková

Rothbardov rámec

Rothbard vypracoval v diele *Power and Market* systematickú typológiu vládnych intervencií.[2] Každá intervencia znamená použitie násilia alebo hrozbu ním, aby sa zmenilo správanie, ktoré by na nenarušenom trhu prebiehalo inak.

Autistická intervencia (autistic intervention) spočíva v príkazoch namierených na jednotlivcov, bez akejkoľvek výmeny. (Rothbard používa slovo „autistická" v technickom ekonomickom zmysle, odvodenom od Misesa: ide o uzavretú, nevýmennú činnosť, nie o psychologický pojem.) Štát nariaďuje: toto rob, toto nerob. K žiadnej transakcii nedochádza, jednotlivec dostane príkaz. Patrí sem brannosť a povinná školská dochádzka, ale aj zákazy spotreby.

Binárna intervencia znamená, že štát je stranou výmeny, ktorá je z pohľadu druhej strany spravidla nedobrovoľná. Klasickým prípadom je zdaňovanie: štát berie jednotlivcom bohatstvo a nedáva nič, čo by si jednotlivec dobrovoľne kúpil. Binárnou intervenciou je aj zhabanie majetku, vyvlastnenie a konfiškácia.

Trojuholníková intervencia znamená, že štát zasahuje do výmen medzi tretími stranami. Sám nie je stranou transakcie, ale diktuje jej podmienky. Trojuholníkovými intervenciami sú cenové regulácie, licenčné požiadavky a povinné zmluvné podmienky. Štát nariaďuje alebo zakazuje výmeny, na ktorých sa sám nezúčastňuje.

Uplatnenie na finančné súkromie

Tento rámec osvetľuje finančné sledovanie. Autistická intervencia zahŕňa príkazy o správaní v oblasti súkromia, napríklad zákazy šifrovania alebo anonymných transakcií. Binárna intervencia znamená, že štát získava informácie alebo majetok predvolaním a zhabaním, ako aj nútením k odhaleniu. Trojuholníková intervencia ukladá povinnosti súkromným transakciám. Príkladom sú požiadavky KYC, ktoré nútia banky zbierať informácie o zákazníkoch skôr, než im poskytnú službu.

Väčšina finančného sledovania sa deje trojuholníkovou intervenciou. Štát občanov nesleduje priamo, čo by si vyžadovalo zdroje a naráželo by na ústavné obmedzenia. Namiesto toho núti súkromné inštitúcie, aby sledovali v jeho mene. Náklady znášajú ony a údaje odovzdávajú štátu.

10.2 Autistická intervencia a súkromie

Priama kriminalizácia

Autistická intervencia v oblasti súkromia má podobu priamych zákazov nástrojov a správania. Americké exportné kontroly do roku 1996 zaradili kryptografický softvér medzi vojenský materiál, takže matematické algoritmy sa považovali za zbrane a na ich zdieľanie bolo treba povolenie vlády. Niektoré štáty dodnes obmedzujú silu šifrovania alebo vyžadujú úschovu kľúčov u štátu (key escrow).[15] Do tej istej kategórie patria návrhy zakázať privacy coiny, služby zmiešavania cez CoinJoin[16] či nástroje anonymnej komunikácie: jednotlivec dostane príkaz a k výmene so štátom nedôjde.

Ekonomická analýza

Autistická intervencia v oblasti súkromia má vlastné vnútorné obmedzenia. Štát len ťažko zistí, kto nástroje súkromia používa, bez sledovania, ktoré chce presadiť. Šifrovanie vyzerá ako náhodné údaje a jeho prítomnosť sa dá poprieť. Priamy zákaz vyžaduje odhaliť porušovateľov, a to si vyžaduje práve tú schopnosť sledovania, ktorú nástroje súkromia má-

ria. Intervencia sa tak podkopáva sama. Digitálne nástroje prekračujú hranice, takže zákaz v jednej jurisdikcii činnosť presunie, ale nezastaví.

Preto štáty pri finančnom sledovaní uprednostňujú trojuholníkovú intervenciu. Priamy zákaz je náročný na zdroje a proti technicky zdatným používateľom býva často neúčinný.

10.3 Binárna intervencia a súkromie

Štát ako strana, ktorá berie

Pri binárnej intervencii je štát stranou nedobrovoľnej výmeny. Berie jednotlivcom, namiesto toho aby zasahoval do transakcií tretích strán.

Občianskoprávne prepadnutie majetku (civil asset forfeiture) umožňuje zhabanie bez trestného odsúdenia. Majetok sa obviní zo spojenia so zločinom a vlastník musí dokázať svoju nevinu, ak ho chce získať späť. Táto binárna intervencia odoberá bohatstvo a zároveň vyvoláva odrádzací účinok na finančné súkromie.[17]

Ďalšou formou binárnej intervencie sú súdne príkazy, ktoré jednotlivcov nútia odhaliť heslá alebo šifrovacie kľúče, ale aj údaje o účtoch. Štát získava informácie priamo a na vynútenie poslušnosti používa sankcie za pohŕdanie súdom.

Binárnou intervenciou je aj požiadavka štátu na záznamy, ktoré držia jednotlivci (na rozdiel od povinností hlásenia treťou stranou). Jednotlivec musí informácie štátu vydať.

Samotné zdaňovanie je binárne (štát berie, jednotlivec nedostane nič), ale požiadavky na plnenie daňových povinností pridávajú ďalšie binárne bremená. Jednotlivci musia odhaliť finančné informácie, aby preukázali súlad, a tým vyjavia súkromnú činnosť bez ohľadu na to, či im vznikla daňová povinnosť.

Odpor a hranice

Binárna intervencia sa stretáva s cieľom priamo. Na rozdiel od trojuholníkovej intervencie, ktorá pôsobí cez sprostredkovateľov, musí štát pri binárnej identifikovať konkrétnych jednotlivcov, nájsť ich a donútiť.

V niektorých jurisdikciách naráža priame vymáhanie štátom na procesné požiadavky (príkazy, dôvodné podozrenie), ktoré trojuholníková intervencia obchádza. Štvrtý dodatok obmedzuje, čo môže štát žiadať priamo, ale nie to, čo zbierajú a hlásia tretie strany.[18]

Nútené odhalenie šifrovaných údajov naráža na praktický problém, že splnenie sa nedá overiť. Ak obžalovaný tvrdí, že zabudol heslo, dokázať opak by vyžadovalo poznatok, ktorý by, keby ho štát mal, urobil nátlak zbytočným.

Správne implementované šifrovanie odoláva binárnej intervencii úplne. Štát môže požadovať kľúče, no ak sa nikdy neuložili alebo sa zabudli, požiadavku nemožno splniť. Axióma odporu tu funguje v praxi.[3]

10.4 Trojuholníková intervencia a súkromie

Uprednostňovaný mechanizmus

Trojuholníková intervencia je hlavným mechanizmom finančného sledovania. Namiesto toho, aby štát jednotlivcom priamo prikazoval alebo od nich bral, zasahuje do súkromných transakcií a núti strany, aby svoje výmeny upravili.

Príkladom je Zákon o bankovom tajomstve z roku 1970 (Bank Secrecy Act, BSA). Napriek názvu bankové tajomstvo zničil, lebo finančným inštitúciám uložil viesť záznamy a hlásiť transakcie. Banky musia podávať hlásenia o hotovostných transakciách (Currency Transaction Reports, CTR) nad 10 000 dolárov a hlásenia o podozrivej činnosti (Suspicious Activity Reports, SAR), keď vedia, majú podozrenie alebo majú dôvod podozrievať, že transakcia spĺňa platný štandard podozrivej činnosti.[4] Je to trojuholníková intervencia: štát zasahuje do vzťahov medzi bankou a zákazníkom, ktorých nie je stranou. Banka musí zákazníkov sledovať a zákazníci sa musia sledovaniu podrobiť, ak chcú využívať bankové služby.

Požiadavky KYC nútia finančné inštitúcie zbierať a overovať totožnosť zákazníka skôr, než s ním nadviažu vzťah. Výmena medzi zákazníkom a bankou je podmienená odhalením informácií, ktoré vyžaduje štát. Rovnakú štruktúru majú zákony o hraniciach anonymných nákupov. Alice a Bob chcú uskutočniť transakciu v súkromí nad určitou sumou a Charlie (štát) im to zakáže. Štát nie je stranou výmeny, ale diktuje podmienky stranám, ktoré by sa inak dohodli odlišne. Hranica spúšťa povinnosť odhalenia, ktorá zaťažuje kupujúceho aj predávajúceho, nie príkaz namierený na jedného z nich osobitne. Pravidlá KYC a programu identifikácie zákazníkov (Customer Identification Program) vyžadujú určené identifikačné údaje o zákazníkoch a pri právnických osobách aj informácie o skutočných majiteľoch. Podľa rizikového profilu zákazníka môžu inštitúcie žiadať aj doklad o adrese či dokumentáciu o pôvode prostriedkov. Tieto informácie slúžia sledovaniu, nie obchodnému záujmu banky. Banky by preferovali jednoduchšie a lacnejšie vzťahy so zákazníkmi, KYC im vnucujú zvonka.

Povinnosti hlásenia treťou stranou nútia finančné inštitúcie podávať hlásenia vládnym úradom: CTR, SAR, hlásenia podľa FATCA o zahraničných účtoch, formuláre 1099 o príjmoch. Finančná činnosť jednotlivca sa hlási bez jeho súhlasu a často bez jeho vedomia.

Monopolné privilégiá ako trojuholníková intervencia

Monopol je v praxeologickom zmysle výlučné privilégium udelené štátom, nie dominantné postavenie na trhu dosiahnuté lepšími službami. Rothbard rozlišoval medzi trhovou dominanciou (keď jediný predávajúci vzniká dobrovoľnou výmenou) a monopolným privilégiom (keď štát zakazuje konkurenciu). Monopolom v pravom zmysle je len to druhé.

Finančné sledovanie sa o monopolné privilégiá opiera. Bankové licencie obmedzujú, kto smie prijímať vklady, a vytvárajú kartel, ktorý musí poslúchať príkazy na sledovanie, ak si chce svoje privilégium udržať. Predpisy o platobných sieťach obmedzujú, kto smie prevádzať peniaze, a zaisťujú, že všetky hlavné cesty sú sledované. Zákony o zákonnom platidle vyžadujú prijímanie štátnej meny a smerujú transakcie cez monitorované systémy. Každé monopolné privilégium vytvára kontrolný bod: štát ponúka výlučné privilégium a cenou je podriadenie sa sledovaniu.

Najzákladnejším monopolným privilégiom je výlučné právo vydávať samotnú menu. Federálny rezervný systém má jedinú zákonnú právomoc vytvárať základné peniaze denominované v amerických dolároch.[19] Rozmer sledovania je tu druhoradý, rozhodujúci je fiškálny. Cena každého tovaru vyrobeného v konkurenčných podmienkach sa približuje k hraničným nákladom výroby. Papierová mena stojí na vytlačenie zlomok centu za bankovku. Keby mohli konkurenti zákonne vydávať menu denominovanú v dolároch, konkurencia by znížila výmennú hodnotu tej meny na výrobné náklady. Zmizol by rozdiel medzi nominálnou hodnotou a nákladmi, ktorý štát zachytáva ako senioráž (seigniorage). Menový monopol je preto predpokladom toho, aby tlač peňazí mohla byť zdrojom príjmov. Otvorená konkurencia pri vydávaní meny by senioráž zlikvidovala rovnako isto, ako otvorená konkurencia v ktoromkoľvek inom odvetví zlikviduje výnosy nad úrovňou nákladov. Zákony o zákonnom platidle a zákazy falšovania tento rozdiel spoločne udržiavajú. Zaisťujú, že vytváranie základných peňazí zostáva štátnym fiškálnym nástrojom, chráneným pred konkurenčným tlakom.

Preto sa alternatívy chrániace súkromie stretávajú s právnymi útokmi. Bitcoin ohrozuje menový monopol,[5] neoprávnené poskytovanie platobných služieb ohrozuje platobný monopol a privacy coiny ohrozujú infraštruktúru sledovania postavenú na týchto monopoloch. Právna odpoveď je predvídateľná: rozšíriť monopolnú ochranu tak, aby vylúčila konkurenciu.

Prečo štáty uprednostňujú trojuholníkovú intervenciu

Trojuholníková intervencia má oproti autistickej a binárnej niekoľko výhod.

Náklady na sledovanie nesú banky. Infraštruktúru na dodržiavanie predpisov (ľudí, technológie, systémy hlásenia) financujú súkromné sub-

jekty, no slúži cieľom vlády. Veľké banky vydávajú na tento účel ročne miliardy a náklady nakoniec dopadnú na zákazníkov a akcionárov.

Informácie, ktoré súkromné strany zbierajú na obchodnom základe, majú slabšiu právnu ochranu než informácie, ktoré zbiera priamo vláda. Podľa doktríny tretej strany informácie zdieľané so súkromnými stranami strácajú ústavnú ochranu. Banky obsluhujú milióny zákazníkov, takže keď štát prinúti banky sledovať, dosiahne široké pokrytie, aké by priame vládne sledovanie nezvládlo.

Rothbard si všimol, že intervencie vytvárajú problémy, ktoré si vyžadujú ďalšie intervencie, a Mises analyzoval mechanizmus, ktorý za tým stojí.[6] Intervencionizmus je nestabilný, lebo každá intervencia vyvoláva následky, ktoré nezamýšľala, a tie lákajú k ďalšej intervencii. Štát pri každom kroku stojí pred voľbou: pôvodnú intervenciu zrušiť, alebo ju rozšíriť. Politická ekonómia správy vedie k rozšíreniu, lebo aparát vybudovaný pre prvý krok je už zaplatený a obsadený. Finančné sledovanie sa takto vyvíjalo päť desaťročí. Zákon o bankovom tajomstve z roku 1970 uložil povinnosti hlásenia, ktoré odhalili medzery. Zákon o kontrole prania špinavých peňazí z roku 1986[20] niektoré medzery zaplátal tak, že z podkladového konania urobil predikatívny trestný čin a k režimu hlásení o hotovostných transakciách pridal hlásenia o podozrivej činnosti. Zákon USA PATRIOT Act z roku 2001[21] rozšíril režim na nebankových poskytovateľov peňažných služieb, ktorých rast patril k odhaleným medzerám. Pravidlo o povinnej starostlivosti o zákazníka z roku 2016[22] prikázalo bankám zisťovať skutočných majiteľov za právnickými osobami a zatvorilo medzeru, ktorú otvorili schránkové firmy. Rozšírenie pravidla Travel Rule (pravidla o sprievodných údajoch pri prevodoch) Finančnou akčnou skupinou (FATF) v roku 2019 na poskytovateľov služieb s virtuálnymi aktívami a jeho globálne zavedenie do roku 2024 zatvorilo medzeru, ktorú otvorili prevody kryptomien bez úschovy u tretej strany. Každý krok bol logickou odpoveďou na medzeru, ktorú odhalil predchádzajúci, a každý zväčšil aparát sledovania, ktorý odhalí ďalšiu medzeru. Rovnováha nedrží na žiadnej strednej úrovni: ústup nemá v aparáte žiadnu politickú podporu, zatiaľ čo rozširovanie ju predvídateľne nachádza pri každom rozpočtovom cykle.

Ekonomické účinky

Trojuholníková intervencia deformuje transakcie, na ktoré cieli.

Zdroje vynaložené na sledovanie (ľudia, technológie, právnici, hlásenia) sa nedajú využiť na produktívnu činnosť. Je to mŕtva strata: sledovanie nevytvára hodnotu pre strany transakcie. Banky, ktoré čelia regulačnému riziku zo „podozrivých“ zákazníkov, odopierajú služby celým kategóriám: kryptomenovým firmám, konopným firmám, politicky nepohodlným skupinám, ba aj jednotlivým majiteľom účtov označeným ne-

priehľadnými algoritmami. Intervencia sa pretavuje do úplného vylúčenia z finančných služieb.

Vedomie sledovania mení správanie. Účastníci trhu sa vyhýbajú legitímnym transakciám, ktoré by mohli vyvolať hlásenie, a ekonomická koordinácia trpí, keď sa strany vyhýbajú označeným činnostiam. Finančné súkromie zaniká, keď sa vo vládnych databázach hromadia úplné záznamy o transakciách. „Finančný panoptikon" robí ekonomickú činnosť čitateľnou pre štátne pozorovanie.

10.5 Digitálne meny centrálnych bánk ako totálna intervencia

Od trojuholníkovej k priamej intervencii

Kapitola 9 ukázala, že dnešná menová architektúra vkladá medzi občanov a základné peniaze obchodné banky. Občania držia peňažné náhrady (nároky voči bankám), nie samotné základné peniaze. Nárazník núti štát pracovať cez sprostredkovateľov: banky zbierajú údaje pod regulačným nátlakom a štát k nim pristupuje právnou cestou. Finančné sledovanie dnes funguje prevažne ako trojuholníková intervencia.

V najsilnejších návrhoch maloobchodnej CBDC by sa toto sprostredkovanie výrazne zúžilo alebo zaniklo. Ako vysvetlila kapitola 9, niektoré modely CBDC dávajú občanom digitálne základné peniaze priamo v centrálnej banke a obchádzajú tak veľkú časť nárazníka obchodných bánk. Z pohľadu intervencie je tento posun rozhodujúci, lebo štát by potreboval menej tretích strán, ktoré treba prinútiť. Čím viac sa centrálna banka približuje k tomu, aby bola bankou, tým priamejší je vzťah k účtu.

To mení ekonomiku intervencie. V najsilnejších verziách pozorovanie nezávisí od súdnych príkazov, lebo štát číta vlastnú účtovnú knihu. Kontrola nezávisí od rovnakých regulačných príkazov, lebo štát spravuje vlastný systém. Náklady a trenie trojuholníkovej intervencie prudko klesajú. To, čo si kedysi vyžadovalo právny postup a súčinnosť inštitúcií, sa môže priblížiť k automatickej správe.

Totálna intervencia

CBDC môžu spojiť všetky tri druhy intervencie do jedného riadiaceho mechanizmu. Niektoré architektúry CBDC podporujú programovateľnosť a môžu rozšíriť sledovanie a kontrolu ďaleko nad to, čo dovoľuje hotovosť. Iné sa verejne prezentujú ako šetrnejšie k súkromiu alebo prísnejšie sprostredkované.[7] Programovateľnosť je návrhová voľba v rámci digitálnej meny a CBDC by sa dala navrhnúť tak, aby napodobnila viac vlastností hotovosti: anonymná alebo na doručiteľa a bez obmedzení míňania. Inštitucionálny stimul však ukazuje jedným smerom: väčšina verejných návrhov smeruje k väčšej vysledovateľnosti a kontrole, než dovoľuje fyzická hotovosť.

Pravidlá CBDC môžu transakcie zakazovať priamo, v podstate ako autistickú intervenciu zabudovanú do menovej infraštruktúry. Mena sama odmietne vykonať nežiaducu platbu. Zákazy anonymných transakcií, nákupov obmedzeného tovaru či platieb na čierne listiny sa stávajú automatickými. Netreba žiadne stíhanie: transakcia jednoducho zlyhá.

Tam, kde CBDC zriaďujú občanom priame účty v centrálnej banke, umožňujú binárnu intervenciu bez zberu údajov treťou stranou: štát získava údaje o transakciách priamo a ekonomická činnosť je pre menovú autoritu viditeľná v okamihu zúčtovania. Nie je žiadny súdny príkaz, ktorý by bolo treba vydať, ani banka, ktorú by bolo treba prinútiť. Pozorovanie je omnoho okamžitejšie, lebo štát je bližšie k tomu, aby bol protistranou každého zostatku.

Silno programovateľná CBDC môže tiež zasahovať do súkromných transakcií trojuholníkovou intervenciou, napríklad tlakom na obchodníkov, aby menu prijímali, overovali stav súladu zákazníka alebo presadzovali obmedzenia míňania. Štát potom cez samotné menové médium ovláda výmeny, na ktorých nie je stranou.

Programovateľná kontrola

Niektoré návrhy CBDC môžu podporovať zásahy, ktoré s fyzickou hotovosťou ani so súčasnými digitálnymi peniazmi nie sú možné. Peniaze sa dajú naprogramovať tak, aby vypršali, čo núti míňať a bráni sporeniu. Tak vzniknú záporné úrokové sadzby bez nulovej dolnej hranice. Dajú sa obmedziť na určité oblasti, takže sociálna dávka sa dá minúť len u schválených predajcov a regionálny stimul neopustí cieľovú oblasť. Môžu odmietnuť kategórie nákupov a na menovej úrovni blokovať platby za alkohol, tabak, strelné zbrane či politicky nežiaduci tovar. Transakcie môžu vyžadovať overenú totožnosť oboch strán, čím sa anonymná výmena znemožní a každá transakcia sa pripíše konkrétnej osobe. Niektoré návrhy by mohli viazať míňanie aj na širšie podmienky súladu.

Ilúzia dvojúrovňového modelu

Niektoré centrálne banky navrhujú „dvojúrovňové“ alebo sprostredkované návrhy CBDC, v ktorých obchodné banky zostávajú sprostredkovateľmi v kontakte so zákazníkom. Tvrdia, že tak sa zachová existujúca architektúra. Toto tvrdenie treba spresniť.

V dvojúrovňovej alebo sprostredkovanej CBDC zostávajú obchodné banky alebo poskytovatelia platobných služieb v kontakte so zákazníkom, kým centrálna banka si ponecháva emisiu a základné infraštruktúrne funkcie. Obchodná banka sa môže stať skôr používateľským rozhraním než nezávislým menovým sprostredkovateľom, hoci miera vyradenia sprostredkovateľov závisí od návrhu. Nárazník, na ktorý poukázala kapitola 9, kde občania držia nároky voči obchodným bankám a nie priame záväzky cen-

trálnej banky, sa môže výrazne zúžiť podľa toho, koľko kontroly nad zúčtovaním a pravidlami si centrálna banka ponechá.

Keďže peniaze sú jej záväzok, centrálna banka môže určovať alebo obmedzovať kľúčové pravidlá zúčtovania a prístupu. Podľa právnej a technickej architektúry môže získať aj široký prehľad o maloobchodných platbách alebo možnosť presadzovať obmedzenia cez sprostredkovateľov. Obchodné banky v dvojúrovňovej CBDC môžu zostať poskytovateľmi služieb v parametroch, ktoré vymedzí centrálna banka, namiesto úplne nezávislých inštitúcií vytvárajúcich peňažné náhrady. Schopnosti sledovania a kontroly môžu zostať veľké, aj keď sa používateľské rozhranie prenechá iným.

Mechanizmus prijatia

Praxeologická analýza ukazuje, prečo na prijatie CBDC netreba výslovný zákaz.

Autistická intervencia (zákaz hotovosti) je nákladná: vyžaduje presadzovanie, vyvoláva odpor a zároveň robí cieľ kontroly viditeľným. Štát má silný dôvod dosiahnuť rovnaký výsledok prostriedkami, ktoré vyvolávajú menší odpor. Ak občania prijmú CBDC dobrovoľne, náklady na presadzovanie zmiznú a politická opozícia sa nikdy nezmobilizuje.

Stimuly podporujú dobrovoľné prijatie, lebo CBDC môžu ponúkať skutočné výhody: okamžité zúčtovanie, prepojenie s vládnymi službami a prístup cez smartfón. Pre ľudí s vysokou časovou preferenciou je okamžité pohodlie silnejšie ako abstraktné budúce riziko. Odhalená preferencia pri prijímaní súčasných digitálnych platieb ukazuje, že väčšina ľudí volí pohodlie pred súkromím, keď je kompromis nenápadný. Štátu stačí zaistiť, aby bola CBDC pohodlnejšia než alternatívy.

Sieťové efekty vytvárajú závislosť od cesty, ktorú je po vzniku ťažké zvrátiť. S rastúcim prijatím CBDC sa infraštruktúra na spracovanie hotovosti stáva menej hospodárnou: banky nesú náklady na hotovostné služby pre klesajúce používanie a obchodníci nesú náklady na manipuláciu s fyzickou menou pre čoraz menej transakcií. Každý účastník, ktorý sleduje svoj záujem, racionálne znižuje hotovostnú infraštruktúru. Výsledkom je, že hotovosť je čoraz menej praktická bez ohľadu na svoj právny štatút.

Tento vývoj má historickú paralelu. Používanie hotovosti vo Švédsku sa v rokoch 2010 až 2019 prudko znížilo bez formálneho zákazu. S nástupom digitálnych platieb a zmenšovaním hotovostnej infraštruktúry kleslo zhruba na jeden nákup z desiatich.[8] Ekonomická logika funguje nezávisle od konkrétností CBDC.

Kam táto cesta vedie, je zrejmé, aj keď časový plán nie je: keď sa hotovostná infraštruktúra zmenší pod hranicu praktickej použiteľnosti, používanie CBDC sa môže stať povinným fakticky, hoci formálne zostane dobrovoľné. Sledovanie, ktoré si ľudia najprv zvolia pre pohodlie, sa mô-

že zmeniť na sledovanie, z ktorého sa dá uniknúť len za cenu odchodu z národnej meny.

Human Rights Foundation tento vývoj sleduje celosvetovo. K roku 2025 skúma CBDC viac ako 130 krajín a menových únií, hoci sa tieto aktivity značne líšia.[9] Výskum a štúdie sú rozšírené, ale plné nasadenie zostáva obmedzené. Väčšina jurisdikcií je vo fáze skúmania: spúšťa pilotné projekty s obmedzenou účasťou alebo študuje technickú uskutočniteľnosť. Skúmanie jurisdikciu nezaväzuje k nasadeniu a mnohé pilotné programy sa končia ešte pred tým, ako sa dostanú k verejnosti. Maloobchodné CBDC spustilo niekoľko autoritárskych režimov, najvýraznejším príkladom je digitálny juan v Číne, kým demokratické štáty postupujú vo všeobecnosti opatrnejšie. Nadácia tvrdí, že autokracie zostávajú špičkou skutočného nasadenia.

Záznam z nasadenia

Empirické výsledky z prvej vlny spustení maloobchodných CBDC ukazujú, čo teoretická analýza predpovedala a čo nie.

Nigérijská eNaira je najjasnejším negatívnym prípadom. Centrálna banka Nigérie ju spustila v októbri 2021 ako prvú maloobchodnú CBDC vo veľkej africkej ekonomike. Prijatie zostalo do roku 2024 pod jedným percentom dospelej populácie a koncom roka 2024 centrálna banka stiahla podstatnú časť obiehajúcich tokenov v rámci širšieho obratu v politike. Nigéria neukázala, že CBDC zlyhávajú. Ukázala, že opísaný mechanizmus prijatia závisí od toho, či je CBDC pohodlnejšia než dostupné alternatívy, a Nigérijčania mali k dispozícii služby mobilných peňazí, ktoré boli pohodlnejšie než eNaira už predtým. Keď je štátny produkt menej pohodlný než zavedený konkurent a autistická alternatíva zákazu hotovosti je politicky priveľmi nákladná, cesta dobrovoľného prijatia zlyhá.

Čínske e-CNY je najjasnejším pozitívnym prípadom v štáte, ktorý má regulačnú kapacitu aj ambíciu sledovať, aby prijatie vnútil. Ľudová banka Číny uvádza kumulatívny objem transakcií v biliónoch renminbi a nasadenie v každom veľkom meste. Hĺbka nasadenia kopíruje hĺbku regulácie. Prijatie je najvyššie v jurisdikciách, kde štátni zamestnávatelia, miestne daňové orgány a predpisy pre obchodníkov spoločne nasmerujú tok transakcií do systému. Čína potvrdzuje, čo tvrdil oddiel 10.5: maloobchodná CBDC dosiahne rozsah nasadenia, keď regulačná architektúra okolo nej smeruje platby do nej a preč od alternatív. Voľby v návrhu meny majú menší význam než inštitucionálny tlak, ktorý emitent uplatní.

Európska centrálna banka previedla digitálne euro z prípravnej fázy do ďalšej koncom októbra 2025. Podľa zverejneného harmonogramu sa pilotná fáza začne koncom roka 2026, ak sa prijme podporná legislatíva, a prvá emisia je možná v roku 2029. Otvorené zostávajú rozhodnutia o architektúre súkromia, o limite držby, o spracovaní online oproti offline a o roz-

sahu programovateľnosti povolenej na úrovni protokolu. Tieto otvorené otázky ukazujú, že politika nasadenia CBDC v demokratickej menovej únii sa točí okolo schopností meny. Verejná debata v členských štátoch sa sústredila na to, či offline režim môže v praxi dať súkromie podobné hotovosti a či sa programovateľnosť dá obmedziť zákonom.

Spojené štáty išli opačným smerom. Výkonný príkaz č. 14178, podpísaný v januári 2025, zakazuje federálnym úradom vyvíjať alebo vydávať maloobchodnú CBDC v USA. Príkaz ukončil výskumnú činnosť povolenú za predchádzajúcej administratívy. Ako výslovnú alternatívu uprednostňuje regulované stablecoiny kryté dolárom. Maloobchodná CBDC a regulovaný stablecoin krytý dolárom majú veľa rovnakých schopností sledovania, ak emitent stablecoinu podlieha povinnostiam KYC, AML a zmrazovania majetku. Rozdiel je v tom, že stablecoin necháva nátlak na sledovanie na súkromných emitentoch, čím zachováva mechanizmus trojuholníkovej intervencie, ktorý kapitola už rozobrala, kým maloobchodná CBDC by presunula tento nátlak priamo na centrálnu banku. Uprednostniť staršiu architektúru pred novšou neznamená zavrhnúť finančné sledovanie.[10]

Cezhraničné zúčtovanie a rozkol BRICS

Otázka maloobchodnej CBDC je jedna os. Veľkoobchodná cezhraničná otázka je osobitná os a jej politika sa vyvíjala tak rýchlo, že sa jej história dnes dá čisto rozdeliť.

Projekt mBridge Banky pre medzinárodné zúčtovanie (BIS) prepojil centrálne banky Číny, Hongkongu, Thajska a Spojených arabských emirátov. V polovici roka 2024 sa pripojila Saudská centrálna banka. Deklarovaným cieľom projektu bolo ukázať cezhraničné zúčtovanie viacerých CBDC bez korešpondenčného bankovníctva. Koncom roka 2024 sa BIS z projektu stiahla. Verejné vysvetlenie zdôrazňovalo, že mBridge dosiahol štádium minimálneho životaschopného produktu a BIS svoju úlohu splnila. Viaceré neskôr zverejnené analýzy poznamenali, že mBridge sa stal použiteľným ako alternatíva ku korešpondenčným kanálom vedeným cez americký dolár a SWIFT a že odchod sa časovo zhodoval s politickou citlivosťou toho, že BIS hostí takúto alternatívu v súvislosti so summitom BRICS v roku 2024. Nech sa týmto dôvodom pripíše akákoľvek váha, projekt pokračuje bez účasti BIS.

BIS spustila v apríli 2024 projekt Agora ako paralelné úsilie, ktoré spája Federálnu rezervnú banku v New Yorku, Európsku centrálnu banku, Anglickú banku, Francúzsku banku, Japonskú banku, Kórejskú banku, Mexickú banku, Švajčiarsku národnú banku a Centrálnu banku Brazílie. Projekt Agora je postavený na veľkoobchodnej CBDC a tokenizovaných vkladoch obchodných bánk a zoznam jeho účastníkov tvoria centrálne banky politicky spojené s finančným poriadkom, ktorý nasledoval po Bretton Woods. Cezhraničná menová architektúra sa rozdelila pozdĺž tých istých

línií ako architektúra sledovania. Jedna skupina centrálnych bánk buduje cezhraničné kanály, ktoré obchádzajú zúčtovanie v amerických dolároch a s ním spojený režim hlásenia. Druhá skupina buduje cezhraničné kanály, ktoré sa do neho zapájajú. Voľba kanálov určuje voľbu pozorovateľa.[11]

Pravidlo Travel Rule a vrstva analýzy reťazca

Finančné sledovanie sa nekončí na hranici banky. Odporúčanie 16 Finančnej akčnej skupiny (FATF), bežne nazývané pravidlo Travel Rule, vyžaduje, aby prevody nad stanovenú hranicu niesli údaje o odosielateľovi a príjemcovi celým platobným reťazcom. Pravidlo sa rozšírilo na poskytovateľov služieb s virtuálnymi aktívami v roku 2019 a do roku 2024 sa zaviedlo vo väčšine jurisdikcií, ktoré regulujú burzy kryptomien. Tým rozšírilo architektúru trojuholníkovej intervencie na trh s kryptoaktívami. Architektúra je rovnaká ako v bankovníctve: regulovaní sprostredkovatelia sú nútení sledovať v mene štátu a nátlak sa vzťahuje na každý prevod, ktorý prekročí hranicu sprostredkovateľa.

Firmy na analýzu blockchainu, medzi nimi Chainalysis, Elliptic a TRM Labs, predávajú doplnkovú schopnosť. Ich produkty spracúvajú verejný záznam blockchainu a zhlukujú adresy do subjektov heuristikami, ktoré firmy samy považujú za obchodné tajomstvo. Jediný kontakt s KYC kdekoľvek v histórii zhluku označí skutočného vlastníka zhluku a označenie sa šíri na všetky jeho nasledujúce transakcie. Odvetvie analýzy reťazca je spravodajská vrstva, ktorá mení transparentnosť blockchainu na identifikované ciele presadzovania. Konkrétne heuristiky a ich hranice skúma kapitola 20. Tu ide o to, že vrstva analýzy reťazca je infraštruktúra presadzovania, vďaka ktorej pravidlo Travel Rule funguje, a jej existencia ukazuje, prečo transparentnosť nie je v žiadnom regulovanom trhu so sprostredkovateľmi náhradou súkromia.[12]

Koncový bod sledovania

V najsilnejších podobách orientovaných na sledovanie sú CBDC vyvrcholením finančného sledovania. Každá platba komukoľvek a v akejkoľvek výške sa môže zaznamenať a pripísať. Úplná finančná história, o akej snívali skoršie programy sledovania, sa približuje k automatickému zberu. Na rozdiel od dodatočného hlásenia sú transakcie CBDC viditeľné okamžite, takže zásah môže prísť pred dokončením, nie až po odhalení. Ak sa CBDC stanú povinnými a hotovosť sa zruší, v systéme národnej meny zostane len málo nesledovanej ekonomickej činnosti alebo žiadna. Podzemné ekonomiky si musia vytvoriť úplne alternatívne meny.

Požiadavky na zdravé peniaze z kapitoly 9 preto zahŕňajú odolnosť voči cenzúre a súkromie. Peniaze, ktoré sa dajú sledovať a kontrolovať, zlyhávajú ako peniaze v mengerovskom zmysle a fungujú namiesto toho ako mechanizmus intervencie.

10.6 Rozhodovací cyklus protivníka

Štátne sledovanie sa riadi vzorcom OODA

Kapitola 1 predstavila slučku OODA Johna Boyda: pozorovanie, orientácia, rozhodnutie, konanie (Observe, Orient, Decide, Act).[13] Každá intervencia, ktorú táto kapitola skúma, sa riadi týmto vzorcom.

Infraštruktúra finančného sledovania existuje, aby umožnila pozorovanie: CTR hlásia hotovostné transakcie, SAR označujú podozrivú činnosť, požiadavky KYC zbierajú doklady totožnosti a hlásenia tretími stranami vytvárajú záznamy o transakciách. Zákon o bankovom tajomstve a jeho nástupcovia sú o pozorovaní. Bez pozorovania ďalšie fázy nemôžu prebiehať.

Pozorovanie živí orientáciu, v ktorej sa surové údaje menia na použiteľné spravodajské informácie koreláciou vzorcov a vyhodnocovaním podozrivých znakov, čo vedie k identifikácii cieľa. Údaje z KYC sú tu užitočné: prepojenie transakcií s identifikovanými jednotlivcami umožňuje orientáciu, ktorú by anonymné transakcie znemožnili. Orientácia vytvára ciele zoradené podľa priority pre rozhodnutie, v ktorom sa obmedzené zdroje prideľujú medzi možné vyšetrovania. A napokon konanie má podobu zhabania majetku, stíhania, regulačnej sankcie alebo zrušenia účtu, ale konať sa dá len proti identifikovaným cieľom, ktorých správanie bolo pozorované a vybrané. Celý aparát presadzovania závisí od predchádzajúcich fáz.

Prerušenie slučky pri pozorovaní

Technológia súkromia preruší tento cyklus v jeho najzraniteľnejšom bode. Ak štát nemôže pozorovať, nemôže sa orientovať podľa vzorcov, ktoré nevidí, nemôže rozhodnúť vyšetrovať transakcie, o ktorých nevie, že prebehli, a nemôže konať proti cieľom, ktoré nevie identifikovať.

Porovnajme tradičné bankovníctvo s starostlivo riadeným súkromím na Bitcoine. Tradičné bankovníctvo poskytuje úplné pozorovanie: každá transakcia sa zaznamená spolu s totožnosťou majiteľa účtu a nahlási úradom a slučka OODA štátu beží hladko od pozorovania až po konanie. Bitcoinové transakcie zostávajú verejné, no postupy ochrany súkromia, ktoré skúma kapitola 20, môžu sťažiť pripísanie a zhoršiť kvalitu štátneho pozorovania. Rozhodovací cyklus sa horšie rozbieha, ale nie je zázračne slepý.

Štáty preto vynakladajú veľké úsilie, aby pozorovanie obnovili. Požiadavky KYC na burzách sa pokúšajú prepojiť bitcoinové transakcie s identitami a obnoviť tak pozorovanie, ktoré pseudonymita Bitcoinu zhoršuje. Režimy pravidla Travel Rule sa pokúšajú rozšíriť povinnosti hlásenia na mnohé prevody, ktoré spracúvajú regulovaní kryptosprostredkovatelia. Firmy na analýzu blockchainu predávajú schopnosti orientácie, služby porovnávania vzorcov, ktoré sa pokúšajú transakcie deanonymizovať.

Každá z týchto snáh smeruje k obnove pozorovania, ktoré umožňuje ďalšie fázy.

Asymetria nákladov

Rámec OODA odhaľuje základnú asymetriu nákladov. Infraštruktúra pozorovania je drahá: vybudovanie a udržiavanie aparátu finančného sledovania si vyžaduje značné priebežné investície do systémov hlásenia, analytických schopností, ukladania údajov a ľudí. Každá fáza slučky spotrebúva zdroje.

Súkromie môže byť naopak lacné. Vygenerovať kryptografický kľúč nestojí nič a používanie CoinJoin[23] alebo siete Lightning[24] pridáva minimálne trenie. Vedenie transakcií cez infraštruktúru chrániacu súkromie ukladá používateľovi mierne náklady, no protivníkovi, ktorý sa snaží pozorovanie obnoviť, obrovské.

Táto asymetria vysvetľuje, prečo je súkromie strategické. Obranca, ktorý zabráni pozorovaniu, ukladá náklady, ktoré ďaleko presahujú jeho vlastný výdavok. Útočník, ktorý musí prekonať ochranu súkromia, čelí nákladom, ktoré môžu presiahnuť hodnotu získaných informácií. Keď sa pozorovanie stane dosť drahým, celý útočný cyklus sa stane neekonomickým.

CBDC ako infraštruktúra pozorovania

Digitálne meny centrálnych bánk útočia priamo na fázu pozorovania. Transakcie prechádzajúce štátom ovládanou infraštruktúrou sú viditeľné blízko okamihu zúčtovania, takže štát sa už nespolieha na nútené hlásenie tretími stranami ani na neúplné údaje. Maloobchodná CBDC by tým, že by prudko zúžila možnosť nepozorovaných transakcií, útočila na najúčinnejší bod, v ktorom súkromie preruší rozhodovací cyklus. Odpoveď, ktorú rozvíja časť V, je budovať peňažné systémy, kde je pozorovanie štrukturálne drahé. Cieľom nie je dokonalá nepozorovateľnosť, ale zvýšiť náklady pozorovania nad to, čo sú protivníci ochotní zaplatiť.[14]

Zhrnutie kapitoly

Finančné sledovanie funguje podľa Rothbardovej typológie intervencií. Autistická intervencia zakazuje nástroje súkromia priamo. Binárna intervencia získava informácie od jednotlivcov predvolaním, zhabaním a nútením k odhaleniu. Trojuholníková intervencia, dominantná forma, núti súkromné inštitúcie sledovať v mene štátu. Zákon o bankovom tajomstve a jeho nástupcovia zabudovali tretí mechanizmus do jadra finančného systému a misesovská logika intervencie vysvetľuje, prečo sa aparát rozširuje každé desaťročie. Digitálne meny centrálnych bánk v najsilnejších formách orientovaných na sledovanie zužujú alebo odstraňujú nárazník obchodných bánk medzi štátom a občanom a môžu spojiť všetky tri druhy intervencie do jedného programovateľného nástroja. Pravidlo Travel Rule

FATF a odvetvie analýzy reťazca rozširujú tú istú trojuholníkovú logiku na poskytovateľov služieb s virtuálnymi aktívami a menia transparentnosť blockchainu na identifikované ciele presadzovania tým, že zhluky adries ukotvia v kontaktoch s KYC.

Nigérijská eNaira zostala pod jedným percentom prijatia, lebo dobrovoľné prijatie vyžaduje, aby CBDC prekonala zavedených konkurentov, a mobilné peniaze boli pohodlnejšie už predtým. Čínske e-CNY sa dostalo do každého veľkého mesta vďaka regulačnému tlaku, ktorý smeroval tok transakcií do systému. Digitálne euro EÚ je v štádiu prípravy a rozpravy s možnou emisiou v roku 2029 a USA zmenili kurz výkonným príkazom č. 14178 (január 2025), ktorý zakazuje vývoj federálnej maloobchodnej CBDC a uprednostňuje regulované stablecoiny kryté dolárom. Cezhraničné zúčtovanie sa rozdelilo pozdĺž tých istých línií: BIS sa koncom roka 2024 z mBridge stiahla a projekt zostal ako alternatíva spojená s BRICS, kým projekt Agora, spustený v apríli 2024, nesie paralelu spojenú so Západom. Architektúra sa delí podľa politického spojenectva a voľba kanálov určuje voľbu pozorovateľa.

Súkromie preruší rozhodovací cyklus štátu pri pozorovaní. Boydova slučka OODA na ňom stojí a keď technológia súkromia pozorovanie zhorší, zhoršia sa za ním aj orientácia, rozhodnutie a konanie. Asymetria nákladov je v prospech obrancov: kryptografická obrana je lacná a útok drahý. Neznamená to, že každý návrh CBDC je rovnako orientovaný na sledovanie. Návrhy podobné hotovosti, na doručiteľa, stoja na jednom konci spektra a plne programovateľné systémy na druhom. Neznamená to ani, že štát je slepý. Konkrétne nástroje a ich obmedzenia skúma kapitola 20. Táto kapitola určila model hrozieb a časť V rozvíja technickú odpoveď.

Poznámky

[1] Franz Oppenheimer, *The State*, trans. John M. Gitterman (Indianapolis: Bobbs-Merrill, 1914), 15.

[2] Murray N. Rothbard, *Power and Market: Government and the Economy*, 4th ed. (Auburn, AL: Ludwig von Mises Institute, 2006), kapitoly 1–2.

[3] Axióma odporu je formulácia Erica Voskuila. Primárnu citáciu pozri v kapitole 5, poznámka 1.

[4] O vývoji požiadaviek hlásenia podľa BSA pozri U.S. Department of the Treasury, Financial Crimes Enforcement Network, „History of Anti-Money Laundering Laws," dostupné na `https://www.fincen.gov/history-anti-money-laundering-laws`.

[5] Satoshi Nakamoto, „Bitcoin: A Peer-to-Peer Electronic Cash System" (2008), `https://bitcoin.org/bitcoin.pdf`; referenčná implementácia v Bitcoin Core, `https://bitcoincore.org/`.

[6] Rothbard analyzuje účinky kaskády intervencií v *Power and Market*, kapitola 3; pozri tiež *Man, Economy, and State*, Scholar's Edition (Auburn, AL: Ludwig von Mises Institute, 2009), kapitola 13. Misesovo základné spracovanie je v *Human Action: A Treatise on Economics*, Scholar's Edition (Auburn, AL: Ludwig von Mises Institute, 1998 [1949]), Part Six, najmä

kapitola 30 („Interference with the Structure of Prices“); a v *Interventionism: An Economic Analysis*, ed. Bettina Bien Greaves (Indianapolis: Liberty Fund, 2011 [1940]). Tvrdenie, že každá intervencia vyvoláva ďalšiu a že politiky strednej cesty vedú buď k skĺznutiu do socializmu, alebo k ústupu k slobodnému trhu, je ústredným štrukturálnym tvrdením oboch Misesových diel.

[7] O ekonomickej analýze CBDC pozri Jörg Guido Hülsmann, *The Ethics of Money Production* (Auburn, AL: Ludwig von Mises Institute, 2008). O technickej analýze pozri Agustín Carstens (General Manager, BIS), „Digital Currencies and the Future of the Monetary System,“ prejav v Hoover Institution, január 2021.

[8] Sveriges Riksbank, *Payments Report 2023*, `https://www.riksbank.se/`, dokumentuje dlhodobý pokles hotovosti vo Švédsku od roku 2010 do začiatku dvadsiatych rokov. Podiel platieb v hotovosti na predajných miestach klesol z približne 39 percent v roku 2010 na približne 9 percent do konca desaťročia.

[9] Human Rights Foundation, „CBDC Tracker,“ dostupné na `https://cbdctracker.hrf.org`. Tracker sleduje vývoj CBDC vo svete so zvláštnym dôrazom na dôsledky pre občianske slobody. Spustený bol v roku 2023 a je prvým monitorovacím úsilím zameraným osobitne na vplyv digitálnych mien centrálnych bánk na ľudské práva. Nadácia konštatuje, že nasadenie CBDC vedú diktatúry a takmer polovica svetovej populácie žije v autokraciách, ktoré tieto systémy aktívne vyvíjajú.

[10] Záznam o nasadení maloobchodných CBDC v rokoch 2021–2025 sa delí na negatívny prípad (Nigéria), pozitívny prípad (Čína), prípad demokratickej rozpravy (EÚ) a prípad zvratu (výkonný príkaz USA č. 14178 z januára 2025, ktorý zakazuje vývoj federálnej maloobchodnej CBDC). Central Bank of Nigeria eNaira, `https://enaira.gov.ng/`. People's Bank of China digital yuan (e-CNY), prehľad na `http://www.pbc.gov.cn/en/3688006/3688253/4157443/index.html` a informácie o testovacej aplikácii na `https://money.163.com/special/ecny/`. European Central Bank Digital Euro project, `https://www.ecb.europa.eu/paym/digital_euro/html/index.en.html`. U.S. Executive Order 14178, „Strengthening American Leadership in Digital Financial Technology,“ 90 Fed. Reg. 8647 (January 23, 2025), `https://www.federalregister.gov/documents/2025/01/31/2025-02123/strengthening-american-leadership-in-digital-financial-technology`. Medzijurisdikčný tracker v Atlantic Council, „Central Bank Digital Currency Tracker,“ `https://www.atlanticcouncil.org/cbdctracker/`, a Human Rights Foundation, `https://cbdctracker.hrf.org/`.

[11] BIS sa z mBridge stiahla koncom roka 2024 a mBridge teraz funguje ako cezhraničná zúčtovacia alternatíva spojená s BRICS. Projekt Agora, spustený v apríli 2024, je paralelné úsilie BIS s centrálnymi bankami spojenými so Západom. Oba projekty rozdeľujú cezhraničné zúčtovacie kanály pozdĺž tých istých línií, pozdĺž ktorých sa rozdelila architektúra sledovania. BIS mBridge project page, `https://www.bis.org/about/bisih/topics/cbdc/mcbdc_bridge.htm`. Oznámenie BIS o stiahnutí, October 31, 2024, `https://www.bis.org/press/p241031.htm`. BIS Project Agora page, `https://www.bis.org/about/bisih/topics/fmis/agora.htm`, s oznámením o spustení z apríla 2024 na `https://www.bis.org/press/p240403.htm`. Nezávislú analýzu geopolitického kontextu pozri v komentároch Atlantic Council a CSIS, dostupných na `https://www.atlanticcouncil.org/` a `https://www.csis.org/`.

[12] Pravidlo Travel Rule FATF (Odporúčanie 16, rozšírené na poskytovateľov služieb s virtuálnymi aktívami v roku 2019) vyžaduje, aby regulovaní kryptosprostredkovatelia pri prevodoch odovzdávali údaje o odosielateľovi a príjemcovi. Chainalysis, Elliptic a TRM Labs sú firmy na analýzu blockchainu, ktoré menia transparentnosť blockchainu na

identifikované ciele presadzovania. FATF Recommendation 16 (Travel Rule), „Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers“ (October 2021), https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Guidance-rba-virtual-assets-2021.html. Chainalysis, https://www.chainalysis.com/. Elliptic, https://www.elliptic.co/. TRM Labs, https://www.trmlabs.com/. O implementácii pravidla Travel Rule v jednotlivých jurisdikciách pozri správy FATF o vzájomných hodnoteniach na https://www.fatf-gafi.org/en/publications/Mutualevaluations.html. Kritickú analýzu heuristík analýzy reťazca pozri v blogových príspevkoch Sergia Demiana Lernera a ďalších na https://bitslog.com/ a vo verejných analýzach Coinbase o metodike analýzy reťazca.

[13] Pre Boydovu primárnu formuláciu slučky OODA pozri kapitolu 1, poznámka 4.

[14] Ďalšie čítanie o CBDC a finančnom sledovaní: pozri poznámku 25 nižšie.

[15] Americké exportné kontroly kryptografického softvéru boli kodifikované v Export Administration Regulations (EAR) v rámci International Traffic in Arms Regulations (ITAR) a neskôr EAR Category 5, Part 2 (Information Security). Silné šifrovanie sa do roku 1996 pokladalo za vojenský materiál, ktorý vyžadoval exportnú licenciu ministerstva zahraničia. Uvoľnenie za Clintonovej administratívy nasledovalo po súdnom spore *Bernstein v. United States Department of Justice*, 922 F. Supp. 1426 (N.D. Cal. 1996), v ktorom sudkyňa Marilyn Patel rozhodla, že zdrojový kód je chránený prejav podľa Prvého dodatku. O čipe Clipper a návrhoch úschovy kľúčov (1993–1996) pozri Steven Levy, *Crypto: How the Code Rebels Beat the Government - Saving Privacy in the Digital Age* (New York: Viking, 2001), kapitoly 10–13. Medzi krajiny, ktoré si ponechali obmedzenia šifrovania alebo povinnú úschovu kľúčov, patrí Rusko (požiadavky registrácie FSB podľa SORM) a Čína (licencovanie komerčného šifrovania podľa zákona o kryptografii z roku 2020).

[16] Pojem „zmiešavanie cez CoinJoin“ (v origináli „coinjoining“) označuje protokol CoinJoin, techniku ochrany súkromia pri bitcoinových transakciách. Pôvodný technický návrh pozri Gregory Maxwell, „CoinJoin: Bitcoin Privacy for the Real World,“ príspevok vo fóre BitcoinTalk (August 22, 2013), https://bitcointalk.org/index.php?topic=279249.0. O regulačnom kontexte služieb zmiešavania cez CoinJoin pozri pokyny FinCEN o mixážnych službách a stíhanie vývojárov Tornado Cash a Samourai Wallet, o ktorých pojednáva kapitola 13.

[17] Občianskoprávne prepadnutie majetku podľa federálneho práva USA prebieha podľa 18 U.S.C. § 981 (civilné prepadnutie) a 21 U.S.C. § 881 (prepadnutie v súvislosti s drogami), s ekvivalentmi v právnych poriadkoch všetkých päťdesiatich štátov. Ústavný štandard vyžaduje len dôvodné podozrenie, že majetok súvisí so zločinom. Dôkazné bremeno, že vlastník je nevinný, nesie vlastník. Vedúce rozhodnutia: *United States v. $8,850 in United States Currency*, 461 U.S. 555 (1983), a *Bennis v. Michigan*, 516 U.S. 442 (1996). Pre systematickú dokumentáciu zneužívania pozri Institute for Justice, *Policing for Profit: The Abuse of Civil Asset Forfeiture*, 3rd ed. (2020), https://ij.org/report/policing-for-profit/. V roku 2019 Kongres vyžadoval, aby federálne úrady hlásili výnosy z prepadnutia na FinCEN, čím vznikla stopa údajov, ktorá zdokumentúva rozsah. Fiškálne údaje pozri U.S. Department of Justice, *Annual Asset Forfeiture Report*, https://www.justice.gov/afp/annual-reports.

[18] Doktrína tretej strany hovorí, že informácie, ktoré sa dobrovoľne zdieľajú s treťou stranou, strácajú ochranu podľa Štvrtého dodatku. Základné rozhodnutia sú *United States v. Miller*, 425 U.S. 435 (1976) (bankové záznamy) a *Smith v. Maryland*, 442 U.S. 735 (1979) (vytočené telefónne čísla). Najvyšší súd doktrínu čiastočne obmedzil v rozhodnutí *Carpenter v. United States*, 585 U.S. 296 (2018), podľa ktorého údaje o polohe z mobilných základňových staníc zbierané počas siedmich dní vyžadujú príkaz, no jadro doktríny zostáva pri finančných

záznamoch nedotknuté. O napätí medzi doktrínou a sledovaním v digitálnej ére pozri Paul Ohm, „The Fourth Amendment in a World Without Privacy," *Mississippi Law Journal* 81 (2012): 1309; a Orin S. Kerr, „The Case for the Third-Party Doctrine," *Michigan Law Review* 107 (2009): 561.

[19] O menovom monopole, senioráži a praxeologickej analýze výlučného privilégia vytvárať peniaze, ktoré má Federálny rezervný systém, pozri Murray N. Rothbard, *The Mystery of Banking*, 2nd ed. (Auburn, AL: Ludwig von Mises Institute, 2008 [1983]), `https://mises.org/library/mystery-banking`, najmä kapitoly 1–4 o peniazoch a bankovníctve a kapitoly 10–14 o centrálnom bankovníctve. O Misesovom spracovaní vzťahu medzi monopolným vydávaním meny a infláciou ako formou zdanenia pozri *Human Action*, Scholar's Edition (Auburn, AL: Ludwig von Mises Institute, 1998 [1949]), kapitola 17 („Indirect Exchange"), oddiely 8–12. O právnej štruktúre emisnej právomoci Federálneho rezervného systému pozri Federal Reserve Act of 1913, 12 U.S.C. § 411 (vydávanie bankoviek Federálneho rezervného systému ako zákonného platidla).

[20] Money Laundering Control Act of 1986, Pub. L. 99-570, 100 Stat. 3207 (1986), kodifikovaný v 18 U.S.C. §§ 1956–1957. Zákon vytvoril prvý federálny trestný čin prania špinavých peňazí ako samostatný trestný čin (nie len predikatívny čin obchodovania s drogami) a vyžadoval od finančných inštitúcií podávať hlásenia o podozrivej činnosti. Bolo to prvé významné legislatívne rozšírenie rámca Zákona o bankovom tajomstve.

[21] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA PATRIOT Act) of 2001, Pub. L. 107-56, 115 Stat. 272 (2001). Hlava III („International Money Laundering Abatement and Anti-Terrorist Financing Act") rozšírila povinnosti podľa BSA na poskytovateľov peňažných služieb, sprostredkovateľov obchodovania s cennými papiermi a ďalšie nebankové finančné inštitúcie a zatvorila regulačné medzery, ktoré umožňovali alternatívnym remitenčným kanálom fungovať mimo režimu hlásení. Vykonávacie predpisy FinCEN pozri 31 C.F.R. Part 1022 (money-service businesses).

[22] FinCEN Customer Due Diligence Requirements for Financial Institutions, 81 Fed. Reg. 29398 (May 11, 2016), kodifikované v 31 C.F.R. § 1010.230. Pravidlo pridalo piaty pilier k rámcu BSA/AML: dotknuté finančné inštitúcie musia identifikovať a overiť skutočných majiteľov právnických osôb (fyzické osoby vlastniace 25 % alebo viac kapitálu, plus jedna určená osoba s kontrolou) čím sa zatvorila medzera schránkových firiem, ktorú predchádzajúci režim nechal otvorenú. Zmenené zákonom Corporate Transparency Act of 2021, Pub. L. 117-54, ktorý presunul hlásenie skutočného vlastníctva do vlastného registra FinCEN namiesto spoliehania sa výlučne na zber údajov na úrovni bánk.

[23] CoinJoin je hlavná technika ochrany súkromia na Bitcoine, ktorá spája vstupy a výstupy viacerých používateľov do jednej transakcie, čím sťažuje vysledovanie jednotlivých platobných tokov. Pôvodný opis protokolu pozri Gregory Maxwell, „CoinJoin: Bitcoin Privacy for the Real World," BitcoinTalk (August 2013), `https://bitcointalk.org/index.php?topic=279249.0`. Hlavné implementácie zahŕňajú Wasabi Wallet (protokol WabiSabi, `https://wasabiwallet.io/`) a JoinMarket (`https://github.com/JoinMarket-Org/joinmarket-clientserver`). O zárukách súkromia pri CoinJoin a jeho obmedzeniach pozri Adam Ficsor (nopara73) et al., „WabiSabi: Centrally Coordinated CoinJoins with Variable Amounts," Financial Cryptography and Data Security 2022; a Malte Möser et al., „An Empirical Analysis of Traceability in the Monero Blockchain," *Proceedings on Privacy Enhancing Technologies* 3 (2018), ktorá CoinJoin zasadzuje do súvislostí porovnaním.

[24] Sieť Lightning je protokol platieb druhej vrstvy pre Bitcoin, ktorý umožňuje rýchle a lacné platby cez platobné kanály mimo reťazca, ktoré sa zúčtujú na základnej vrstve. Pôvodná špecifikácia je Joseph Poon and Thaddeus Dryja, „The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments" (January 14, 2016),

https://lightning.network/lightning-network-paper.pdf. Protokol je špecifikovaný v štandardoch BOLT (Basis of Lightning Technology) na https://github.com/lightning/bolts. O vlastnostiach súkromia a obmedzeniach pozri Rene Pickhardt and Mariusz Nowostawski, „Imbalance Measure and Risk-Minimization for Lightning Network Payment Channel Rebalancing," a George Kappos et al., „An Empirical Analysis of Privacy in the Lightning Network," *Financial Cryptography and Data Security* (2021), ktorá analyzuje útoky sondovaním a deanonymizáciu z grafu smerovania.

[25] Ďalšie čítanie o CBDC a finančnom sledovaní. K špecifickému návrhovému priestoru CBDC sú pracovné dokumenty Banky pre medzinárodné zúčtovanie najširším oficiálnym zdrojom: Raphael Auer, Giulio Cornelli, and Jon Frost, „Rise of the Central Bank Digital Currencies: Drivers, Approaches and Technologies," BIS Working Paper No. 880 (2020), https://www.bis.org/publ/work880.pdf; Codruta Boar and Andreas Wehrli, „Ready, Steady, Go? Results of the Third BIS Survey on Central Bank Digital Currency," BIS Papers No. 114 (2021); a každoročne aktualizované prieskumy CBDC citované v predslove. O politickej ekonómii je Eswar S. Prasad, *The Future of Money: How the Digital Revolution Is Transforming Currencies and Finance* (Harvard University Press, 2021), vyvážené akademické spracovanie; Christopher Leonard, *The Lords of Easy Money: How the Federal Reserve Broke the American Economy* (Simon & Schuster, 2022), dodáva inštitucionálny kontext. Pre občianskoslobodnú argumentáciu proti maloobchodným CBDC pozri Nicholas Anthony and Norbert Michel, „Central Bank Digital Currency: Assessing the Risks and Dispelling the Myths," Cato Institute Policy Analysis No. 941 (2023), https://www.cato.org/policy-analysis/central-bank-digital-currency; a Human Rights Foundation, „The Case Against Central Bank Digital Currencies," na https://hrf.org. O čínskom digitálnom juane (e-CNY) ako o najvýznamnejšom nasadenom príklade pozri opäť prácu Eswara Prasada; k trajektórii digitálneho eura pozri publikácie ECB na https://www.ecb.europa.eu/paym/digital_euro/html/index.en.html. K širšej literatúre o finančnom sledovaní: Nicholas Anthony, *The Infrastructure of Control: A Global Look at the Dangers of CBDCs* (Cato, 2024); Allen J. Dickerson and Lloyd M. Pierson, „Central Bank Digital Currencies: Privacy Implications," *Journal of Law and Liberty* (2022). K základnému problému čitateľnosti, ktorý štát rieši menovým sledovaním, je historickým rámcom James C. Scott, *Seeing Like a State* (Yale, 1998), už citovaný v kapitole 1; Rainer Böhme et al., „Bitcoin: Economics, Technology, and Governance," *Journal of Economic Perspectives* 29, č. 2 (2015): 213–238, je referenčné spracovanie vzťahu kryptomien a štátu. K regulačnému aparátu osobitne Todd Zywicki and Max Raskin, „CBDCs in the United States: A Constitutional Analysis" (2024), rieši obavy z rozdelenia právomocí, ktoré by nasadenie maloobchodnej CBDC v USA vyvolalo.

11

FIREMNÉ SLEDOVANIE A VYŤAŽOVANIE ÚDAJOV

„Keď sa technológia raz pripustí, rozohrá svoje karty; robí to, na čo bola navrhnutá.“

Neil Postman, *Technopoly* (1992)[1]

Úvod

Štáty nie sú jedinou hrozbou sledovania. Firmy, ktoré vyťažujú údaje, vybudovali monitorovaciu infraštruktúru, ktorá sa schopnostiam štátu vyrovná a často ich prekonáva. Jej obchodný model, prepojenie so štátnym sledovaním a vzťah k zlyhaniu trhu súvisia s tým, ako začínajú trhy reagovať na dopyt po súkromí.

11.1 Obchodný model vyťažovania údajov

Používateľ ako produkt

Shoshana Zuboff vytvorila pojem „sledovací kapitalizmus“ pre obchodný model, v ktorom sa ľudská skúsenosť pokladá za voľnú surovinu na premenu na behaviorálne údaje.[2] Z týchto údajov vznikajú predikčné produkty, s ktorými sa obchoduje na trhoch s behaviorálnymi futures.

Ekonomická logika je jednoduchá: služby sa zdajú bezplatné, lebo používatelia platia údajmi, nie peniazmi. Zákazníkom je inzerent a produktom používateľ. Presnejšie, produktom sú predpovede o správaní používateľov, kým používatelia dodávajú surovinu na ich výrobu.

To obracia tradičný trhový vzťah. V bežnej výmene firmy súťažia o to, kto lepšie poslúži zákazníkom. Pri vyťažovaní údajov súťažia o to, kto

získa viac používateľov. Slúžiť zákazníkom znamená uspokojovať ich preferencie. Získať používateľov znamená udržať ich pri obrazovke, či im to prospieva, alebo nie.

Zber pozornosti

Firmy, ktoré vyťažujú údaje, súťažia o pozornosť. Zapojenie používateľov vytvára údaje, väčšie zapojenie vytvára viac údajov a maximálne zapojenie dáva maximum suroviny pre predikčné produkty.

Z toho vznikajú podnety na manipuláciu. Ak zapojenie slúži záujmom používateľa, problém nevzniká. Keď však zapojenie záujmom používateľa odporuje (návykový dizajn, zosilňovanie rozhorčenia, králičie diery čoraz extrémnejšieho obsahu), obchodný model odmeňuje manipuláciu, nie službu.

Praxeológia zdôrazňuje odhalenú preferenciu: konanie ukazuje preferenciu v tom, čo ľudia volia. Výklad sa však komplikuje, keď je prostredie, v ktorom sa voľba robí, postavené tak, aby využívalo psychické slabiny. Používateľ, ktorý strávi hodiny listovaním, môže odhaľovať nejakú preferenciu, ale nie nutne záľubu v samotnom listovaní. Môže odhaľovať aj náchylnosť na premenlivé schémy odmeňovania.[17]

Behaviorálny prebytok

Zuboff rozlišuje medzi údajmi, ktoré treba na zlepšovanie služby, a „behaviorálnym prebytkom", ktorý sa vyťažuje pre predikčné produkty. Mapová aplikácia potrebuje na navigáciu polohu. Tá istá poloha, hromadená v čase a porovnávaná s ďalšími údajmi, sa stáva surovinou na predpovedanie budúceho správania a na predaj týchto predpovedí inzerentom.

Pojem prebytku ukazuje, že používatelia dostávajú službu v hodnote len zlomku údajov, ktoré poskytnú. Zvyšok, prebytok, sa vyťaží bez odmeny. Používatelia len ťažko posúdia, koľko prebytku sa vyťažilo, lebo nevidia, ako sa ich údaje používajú, spájajú alebo predávajú.

Informačná asymetria problém zhoršuje. Na bežných trhoch tlačí konkurencia ceny k hraničným nákladom. Na trhoch s vyťažovaním údajov sa podľa miery vyťažovania porovnávať nedá, lebo praktiky vyťažovania nie sú vidieť. Konkurencia preto prebieha v iných rozmeroch (funkcie, sieťové efekty), nie v ochrane súkromia.[3]

Cantillonova analógia pre údaje

Richard Cantillon v osemnástom storočí rozobral tok peňazí a všimol si, že nové peniaze vstupujú do ekonomiky v určitých bodoch a príjemcovia najbližšie k týmto bodom z nich profitujú skôr, než sa ceny prispôsobia rozšíreniu.[4] Rakúska tradícia tento pojem používa úzko, ako tvrdenie o distribučných účinkoch menovej expanzie, a v tomto vymedzení tvrdenie obstojí.

V ekonomike vyťažovania údajov sa dá viesť opatrná analógia, pričom netvrdíme, že je dôkazom. Behaviorálne záznamy vstupujú do obchodného systému v určených bodoch (prehliadač, telefón, inteligentné zariadenie, relácia v aplikácii) a firmy najbližšie k týmto bodom zberu ich môžu spájať a ďalej predávať, skôr než sa dotknutý človek môže spamätať. Ceny na trhu s pozornosťou sa nepretržite upravujú, ako sa zlepšuje presnosť predpovedí, a úprava prináša zisk firmám na začiatku reťazca. Podobnosť je štrukturálna, nie menová: výhoda prvého prístupu prináša neprimerané zisky bez ohľadu na to, či je podkladom mena, alebo správanie.

Cantillonov argument o peniazoch stojí na konkrétnej skutočnosti, že mena je vzácna a nová emisia zrieďuje kúpnu silu terajších držiteľov. Pri tokoch údajov nemá priamu obdobu. Analógia dokazuje len toľko, že ekonomická podoba vzorca (prví príjemcovia získavajú skôr, než sa zvyšok systému prispôsobí) sa opakuje na každom trhu, ktorého surovina tečie cez určené vstupné body.

Predikčné produkty

Firmy, ktoré vyťažujú údaje, predávajú predpovede. Inzerenti platia za používateľov, ktorí pravdepodobne kliknú, politické kampane za voličov, ktorých sa dá presvedčiť, poisťovne za zákazníkov, ktorí pravdepodobne uplatnia nárok. Hodnota je v presnosti predpovede, presnosť rastie s množstvom údajov a viac údajov vyžaduje rozsiahlejšie sledovanie.

Vzniká tak račňa vyťažovania. Každé zlepšenie presnosti robí údaje cennejšími, čo ospravedlňuje intenzívnejšie vyťažovanie, a to potom umožní presnejšie predpovede. Koncovým bodom, ktorému sa približuje asymptoticky, je čoraz širšie monitorovanie v prospech čoraz prepracovanejších predpovedí správania.

11.2 Prepojenie firiem a štátu

Zákonné povinnosti

Kapitola 10 rozobrala trojuholníkovú intervenciu, teda štátne príkazy nanútené súkromným transakciám, a firmy, ktoré vyťažujú údaje, takým príkazom čelia v niekoľkých podobách. Povinnosť uchovávať údaje núti firmy držať údaje, ktoré by inak zmazali. Povinnosť umožniť zákonné odpočúvanie núti poskytovateľov komunikácie budovať zadné vrátka na sledovanie. Oznamovacie povinnosti nútia platformy monitorovať určitý obsah.

Tieto požiadavky formujú firemnú prax s údajmi. Firma by z dôvodov bezpečnosti a zodpovednosti radšej zbierala čo najmenej údajov, ale zákon môže zber nariaďovať. Štát tak používa firemnú infraštruktúru ako násobič sily a dosahuje rozsah sledovania, ktorý by sa samotnou vládnou prevádzkou zostavoval omnoho ťažšie.

Dobrovoľná spolupráca

Popri zákonných povinnostiach mnohé firmy spolupracujú s vládou aj dobrovoľne. Program PRISM odhalil rozsiahly prístup vlády k údajom, ktoré držia veľké technologické firmy.[5] Národné bezpečnostné listy (National Security Letters) nútia k odhaleniu údajov a zároveň zakazujú adresátom priznať, že žiadosť dostali.[18]

Dobrovoľná spolupráca vytvára obchodné príležitosti. Vládne zákazky odmeňujú firmy so schopnosťami sledovania. Spravodajské služby sú dobre financovaní zákazníci predikčných produktov. Hranica medzi službou inzerentom a službou spravodajským službám sa stiera, keď obaja chcú rovnaké predpovede správania.

Partnerstvo verejného a súkromného sektora

Štátne a firemné sledovanie sa stali symbiotickými. Štáty ťažia z firemného zberu údajov, ktorý by priamo narazil na zákonné prekážky. Firmy ťažia zo zákonných rámcov, ktoré upevňujú ich obchodné modely a zaťažujú konkurentov.

Firmy zbierajú údaje v rozsahu, ktorý by vlády zákonne nariadiť nemohli, a vlády sa k nim potom dostávajú cez právne konanie, národné bezpečnostné listy alebo neformálnu spoluprácu. Komerčné analytické nástroje (strojové učenie, rozpoznávanie vzorov) slúžia rovnakým cieľom sledovania ako vládne programy. Firemné siete, zariadenia a platformy sa stávajú infraštruktúrou, na ktorej sa monitorovanie vezie. A veľké firmy zvládnu náklady na súlad so zložitými predpismi o súkromí, malí konkurenti nie, takže pravidlá, ktoré mali chrániť súkromie, namiesto toho vytvárajú priekopy chrániace zavedených hráčov.

Rozdiel je menej dôležitý, než sa zdá

Rozdiel medzi štátom a firmou je dôležitý z právneho hľadiska. Ústavné obmedzenia sa vzťahujú na konanie vlády, nie na súkromné konanie. Pre rozbor súkromia je tento rozdiel tenší.

Ak niekto sleduje vašu komunikáciu, základná strata súkromia môže byť rovnaká, či ide o NSA, alebo o Google. Ak sa vaše správanie predpovedá a usmerňuje, škoda nezmizne len preto, že manipulátorom je algoritmus sociálnej siete, a nie vládna propagandistická služba. Totožnosť sledujúceho má stále význam pre právo a pre následnú moc, ale strata súkromia nastáva ako prvá.

Z toho vyplýva, že ochrana súkromia musí riešiť štátne aj firemné sledovanie. Technické opatrenia účinné proti jednému môžu účinkovať proti obom. Právne opatrenia účinné proti vládnemu sledovaniu (ústavné obmedzenia, požiadavky na súdny príkaz) však firemné sledovanie priamo nepokrývajú.

11.3 Je to zlyhanie trhu?

Tvrdenie o zlyhaní trhu

Kritici tvrdia, že sledovací kapitalizmus je zlyhaním trhu.[6] Používatelia nechcú úplné sledovanie, no aj tak ho dostávajú. Firmy vyťažujú negatívne externality, napríklad náklady na súkromie, bez toho, aby ich niesli. Trhy nevytvárajú alternatívy, ktoré by súkromie rešpektovali.

Ak je to pravda, odôvodňovalo by to zásah na nápravu zlyhania. Mohli by byť oprávnené predpisy o súkromí, vlastnícke práva k údajom či rozbitie platforiem, aby sa obnovili fungujúce trhy.

Rakúska odpoveď

Rakúska ekonómia je voči tvrdeniam o zlyhaní trhu skeptická z viacerých dôvodov, ktoré platia súčasne. Problém znalostí robí centrálne posúdenie „správnej" úrovne súkromia nemožným: optimálne výsledky vznikajú trhovým procesom a vopred sa nedajú poznať, a čo vyzerá ako zlyhanie, môže byť trh, ktorý objavuje riešenia problémov, ktoré regulátori ešte nezaznamenali. Súčasná štruktúra trhu navyše odráža desaťročia intervencií, ktoré deformujú základ, voči ktorému sa zlyhanie diagnostikuje. Podstatná otázka je, či pozorované výsledky vyplývajú z trhov, alebo z intervencií, ktoré ich formujú. A statická analýza môže odhaliť zdanlivé neefektívnosti, ktoré dynamická analýza ukáže ako dočasné, takže trhy môžu problém práve napravovať, kým intervencia túto nápravu zastavuje.

Záznam intervencií v oblasti sledovania je rozsiahly a ľahko zdokumentovateľný. Autorské a patentové právo pomáha upevňovať zavedených hráčov, lebo zvyšuje náklady na kopírovanie protokolov a budovanie kompatibilného softvéru. GDPR[19] a podobné predpisy ukladajú náklady na súlad, ktoré veľké firmy zvládnu ľahšie než menší rivali, takže síce obmedzia niektoré zneužívajúce praktiky, ale zároveň spevnia výhodu zavedených hráčov. Veľké technologické firmy získavajú značné príjmy z vládnych zákaziek, čo vytvára priamy podnet budovať schopnosti sledovania, ktoré štáty chcú kupovať. Oddiel 230 a podobné ustanovenia znižujú právne riziká hostenia a rozsiahlej kurátorskej práce, čo uprednostňuje veľkosť platforiem.[7] Bankové predpisy vyžadujúce overenie zákazníka (know-your-customer) a boj proti praniu špinavých peňazí tlačia ekonomickú činnosť do sledovaných digitálnych kanálov a preč od súkromnej hotovosti, čím vzniká viac prúdov údajov, ktoré sledovacie firmy speňažujú. „Trh", na ktorom sledovací kapitalizmus pôsobí, má ďaleko od kontrafaktuálneho slobodného trhu. Jeho štruktúru formovala štátna politika na každej vrstve a výsledky, ktoré kritici pripisujú trhu, sčasti odrážajú tieto politické rozhodnutia.

Vytvoril by to slobodný trh?

Kontrafaktuálny stav sa posudzuje ťažko, no viaceré úvahy naznačujú, že súčasné výsledky nie sú nevyhnutným trhovým výsledkom. Bez ochrany „duševného vlastníctva", ktorá v softvéri vytvára umelú vzácnosť, by bola konkurencia ostrejšia; platformy by nemohli udržiavať sieťové efekty tým, že kompatibilným alternatívam hrozia patentovými žalobami. Keby používatelia mohli ľahko prechádzať medzi kompatibilnými platformami, vyťažovanie údajov by čelilo konkurenčnému tlaku a používatelia, ktorým záleží na súkromí, by mohli odísť k alternatívam rešpektujúcim súkromie bez straty sieťových kontaktov. Bez sledovania v menovom systéme, ktoré tlačí transakcie do sledovaných kanálov, by alternatívne platobné metódy zmenšili prúdy údajov, ktoré robia predpovedanie správania cenným.

Neznamená to, že slobodné trhy by vytvorili dokonalé súkromie. Sieťové efekty, problémy koordinácie a skutočné spotrebiteľské preferencie bezplatných služieb by pretrvali. Naznačuje to však, že súčasná intenzita sledovania odráža intervenciu rovnako ako trhový výsledok.

Sieťové efekty a uviaznutie

Aj keď pripustíme, že intervencia má svoj podiel, skutočná trhová dynamika k sústreďovaniu sledovania prispieva. Komunikačné platformy sú cennejšie s viac používateľmi, čo vytvára dynamiku, v ktorej víťaz berie všetko: niekoľko platforiem dominuje a odchod je pre používateľov drahý. Používatelia investovali do budovania kontaktov a tvorby obsahu na týchto platformách a prechod znamená tieto investície opustiť. Aj keď používatelia preferujú alternatívy rešpektujúce súkromie, môže presunu brániť zlyhanie koordinácie, keď každý čaká, že prejdú ostatní, a nikto nechce byť prvý na prázdnej platforme.

Ide o skutočné trhové javy, nie o účinky intervencie. Naznačujú, že aj bez intervencie by konkurencia v oblasti súkromia mohla naraziť na prekážky. Neodôvodňujú však ďalšiu intervenciu; naznačujú, že problém si vyžaduje technické a podnikateľské riešenia, nie regulačné.

To, čo je vidieť, a to, čo nie je vidieť

Esej Frédérica Bastiata z roku 1850 o tom, čo je vidieť a čo nie je vidieť, je správnym rámcom pre účtovanie nákladov, ktoré diskusie o „nemám čo skrývať" zvyčajne vynechávajú.[8] Dobrý ekonóm podľa Bastiata neberie do úvahy len bezprostredný účinok konania, ale aj účinky, ktoré vyvoláva v dlhšom čase a u iných skupín, než je tá, ktorá je priamo na očiach. Henry Hazlitt z rovnakého princípu urobil hlavnú lekciu knihy *Ekonómia v jednej lekcii* (angl. *Economics in One Lesson*, 1946) a princíp sa tu uplatní bez úprav.

Viditeľné účinky komerčného sledovania sa vymenúvajú ľahko: bezplatná služba, prispôsobený prúd príspevkov, pohodlné automatické vy-

plňanie, reklama, ktorá zasiahne cieľové publikum inzerenta. Neviditeľné účinky sú tie, ktoré si všimne len ekonóm s patričnou disciplínou. Myšlienka, ktorú autor nezdieľal, lebo rátal s tým, že príspevok si raz prečíta budúci zamestnávateľ. Podnikateľský pokus, ktorý sa neuskutočnil, lebo záznam o jeho neúspechu by bol trvalý a pripojený k zákonnému menu podnikateľa. Nákup, ktorý sa neuskutočnil, lebo transakcia by prezradila záujem kupujúceho o nepopulárnu tému. Konzultácia, na ktorú sa pacient neobjednal, lebo formulár pri príjme pýta otázky, o ktorých čaká, že sa mu raz obrátia proti. Každý z týchto prípadov je konkrétna dobrovoľná výmena, ktorú sledovanie zdanením vyhnalo z existencie, a súčet je ekonomika, ktorú sledovacia infraštruktúra potlačila.

To, čo nie je vidieť, je väčšie než to, čo vidieť je, lebo väčšina z toho, čo sledovanie potláča, sa nikdy nestane. Bezplatná služba je viditeľná na každej obrazovke. To, čo sa nestalo, nevytvára údaje a jeho cenu nemožno zvonku zmerať. Analýza ju však pomenovať môže a pomenovanie je disciplína, na ktorej Bastiat trval.

11.4 Problém nezvratnosti

Doterajšia analýza brala odhalené údaje ako jednu kategóriu. To je neúplné. Jeden druh údajov má vlastnosť, ktorú ostatné nemajú, a táto vlastnosť si vyžaduje osobitný obranný postoj. Biometrické a genetické údaje sa nedajú rotovať. Raz odhalené zostanú odhalené navždy.

Prečo je obvyklým liekom rotácia

Odhalenie prihlasovacích údajov má štandardný liek. Uniknuté heslo sa nahradí novým, kompromitovaný kľúč sa zruší a nahradí novým párom kľúčov, ukradnuté číslo kreditnej karty sa zablokuje a vydá nové, uniknutý token relácie vyprší sám podľa svojho harmonogramu. Liek funguje, lebo token je artefakt, ktorý sa dá vymeniť bez zmeny osoby, ktorú predstavuje. Rotácia prihlasovacích údajov je obranný postoj, z ktorého bezpečnostná literatúra vychádza vždy, keď opisuje „kompromitáciu“ ako stav s cestou späť.

Rovnaká logika platí, hoci nedokonale, pre väčšinu behaviorálnych a finančných údajov. Odhalené záznamy o transakciách sa nedajú vziať späť, ale znalosti protivníka o nich starnú: vzorec nákupov spred dvoch rokov opisuje človeka, ktorý sa mohol presťahovať, zmeniť prácu aj vkus. Informácia má pre firmu na analýzu blockchainu či dátového brokera stále hodnotu, no tá klesá. Rotácia starnutím je pomalšia než rotácia výmenou kľúča a závisí od toho, že dotknutý človek časom žije inak, no zachováva princíp, že odhalenie je stav s cestou späť.

Prečo sú biometrické a genetické údaje iné

Biometrické a genetické údaje sú určujúca kategória, pre ktorú nefunguje ani jeden z týchto mechanizmov rotácie. Odtlačok prsta z roku 2025 je ten istý ako v roku 2005 a bude taký aj v roku 2045. Tvár je tá istá tvár, dúhovka tá istá dúhovka a odtlačok hlasu sa s vekom mení len mierne. Genóm je rovnaký v každej bunke tela a stabilný počas všetkých rokov života. Identifikátorom je človek. Človeka vydať znova nemožno.

Praktický dôsledok je, že únik z databázy biometrických alebo genetických údajov nie je napraviteľný stav. Pri úniku databázy s prihlasovacími údajmi platí „rotujte všetko hneď"; pri úniku biometrickej databázy platí „protivník teraz navždy pozná identifikátor a každé ďalšie použitie tohto identifikátora treba považovať za pozorovateľné protivníkom". Odhalenie sa tiahne celým životom človeka.

Príznačná je analógia s poistením. Štandardné poistky proti kybernetickým rizikám oceňujú úniky prihlasovacích údajov vzorcami, ktoré predpokladajú, že náprava sa skončí rotáciou údajov. Vzorce použité na biometrické úniky podhodnocujú skutočné náklady o niekoľko rádov, lebo odhalenie sa nekončí. Niekoľko poisťovateľov si rozpor uvedomilo a upravilo ceny; úprava je trhovým uznaním, že biometrické a genetické údaje patria do inej kategórie aktív.

Prípady ilustrujú princíp

Dva prípady ukazujú princíp dosť konkrétne na to, aby ukotvili analýzu. Prvým je únik z veľkej spotrebiteľskej firmy na genetické testovanie koncom roka 2023, pri ktorom boli profily miliónov zákazníkov odhalené cez útoky typu credential stuffing (hromadné skúšanie uniknutých prihlasovacích údajov) a potom ponúkané na predaj na podzemných fórach, rozdelené podľa etnika. Firma neskôr vstúpila do konkurzu a genetická databáza sa stala hlavným majetkom v konaní a prešla na nástupnícku organizáciu. Zákazníci, ktorí svoje genómy poskytli, nemali pri tomto prevode žiadne slovo a žiadny opravný prostriedok ho nemohol vrátiť späť.[9]

Druhým je národný biometrický identifikačný program štátu s viac než miliardou zapísaných identít, v ktorom sú odtlačky prstov, skeny dúhovky a demografické údaje centrálne uložené už roky. Program prežil viaceré údajné úniky. Nezávisle od akéhokoľvek konkrétneho obvinenia takýto systém vytvára jediný bod, ktorého kompromitácia by navždy vyjmenovala biometrické identifikátory celej populácie, a jeho obranný postoj nemôže stáť na rotácii z rovnakého dôvodu ako v prvom prípade.[10]

Kapitola 12 podrobne rozoberá tretí vzorec: komerčné databázy rozpoznávania tváre postavené na obrázkoch stiahnutých z webu, kde dotknutí ľudia nikdy nesúhlasili a firmy regulačné pokuty pohltili ako bežný náklad podnikania. Štrukturálna vlastnosť je rovnaká.

Obranný postoj

Obranný postoj, ktorý z nezvratnosti vyplýva, sa líši od postoja pre prihlasovacie údaje. Obmedzte zápis do akejkoľvek biometrickej či genetickej zbierky, ktorej účel neospravedlňuje celoživotné odhalenie. Tam, kde sa zápisu nevyhnete (hraničná kontrola, štátny program identity, zdravotná nevyhnutnosť), uprednostnite systémy navrhnuté so zrušiteľnosťou biometrických šablón, v ktorých je uložená šablóna jednosmernou funkciou biometrického údaja a tajomstva, ktoré sa dá rotovať. Tam, kde je služba dobrovoľná (overenie telefónu podľa tváre, spotrebiteľská služba genetického testovania, biometrický systém členstva v posilňovni), porovnajte bežné pohodlie zápisu s jeho nezvratným odhalením. Pre väčšinu spotrebiteľov a väčšinu modelov hrozieb toto porovnanie zápis neospravedlní.

Právna reforma tu má úzku úlohu. Biometrické zákony o súkromí na úrovni štátov a federácie môžu zaviesť právo na žalobu, právo na vymazanie a občianskoprávne pokuty; zákony tohto druhu, ktoré od roku 2021 prijalo niekoľko amerických štátov, ukazujú, že právny systém vie biometrické odhalenie oceniť dodatočne. Nedokážu mu však zabrániť. Prevencia zostáva problémom inžinierstva a osobnej disciplíny a disciplína sa musí prispôsobiť nezvratnosti aktíva.[11]

Širší analytický záver je, že taxonómia sledovania musí nezvratné údaje považovať za osobitnú kategóriu. Skoršie kapitoly knihy analyzovali finančné sledovanie, firemné sledovanie a kryptovojny ako oddeliteľné kanály. Biometrické a genetické údaje pretínajú všetky tri kanály a ukladajú spoločné obmedzenie: nech obranca urobí čokoľvek, identifikátorom je človek a každá obranná architektúra postavená na rotácii identifikátora zlyháva už vo svojej konštrukcii. Táto kategória si vynucuje najprísnejšiu obrannú disciplínu a prevádzkové kapitoly knihy ju berú ako danosť.

11.5 Reakcie trhu a konkurencia v súkromí

Súkromie ako konkurenčná odlišnosť

Napriek prekážkam trhy začali na dopyt po súkromí reagovať. Niektoré zavedené firmy sa dnes odlišujú súkromím, noví hráči budujú obchodné modely s prednosťou súkromia a zmeny v infraštruktúre obmedzujú vyťažovanie údajov bez ohľadu na rozhodnutia jednotlivých firiem.

Najjasnejšiu ukážku vo veľkom meradle poskytuje Apple. V apríli 2021 zaviedol App Tracking Transparency (ATT), ktoré vyžaduje, aby aplikácie pred sledovaním používateľov v aplikáciách a na weboch iných firiem požiadali o povolenie. Výsledok bol dramatický: približne 80 % používateľov iOS sledovanie odmietlo, keď dostali jasnú voľbu.[12] Meta oznámila, že ATT zníži jej tržby za rok 2022 približne o 10 miliárd dolárov; odhady

z odvetvia uvádzali celkovú cenu pre Metu bližšie k 13 miliardám dolárov ročne.[13]

Táto jediná zmena politiky odhalila krehkosť obchodných modelov závislých od sledovania. Keď používatelia dostali jednoduchú voľbu, drvivá väčšina sa rozhodla nebyť sledovaná. Veľká skrytá preferencia pre súkromie tu už bola; ATT jej dalo jednoduchý spôsob vyjadrenia. Apple na jej odhalení zarobil, firmy závislé od sledovania utrpeli. Je to trhové objavovanie vo veľkom.

Podobnú dynamiku ukazujú alternatívy vyhľadávačov a prehliadačov. DuckDuckGo[20] vyrástol z okrajového vyhľadávača na službu spracúvajúcu ročne miliardy dopytov, a to napriek konkurencii najprepracovanejšej vyhľadávacej infraštruktúry v dejinách. Používatelia prijmú menej prepracované výsledky výmenou za súkromie; tento kompromis ukazuje skutočnú ochotu platiť. Prehliadač Brave[21] dosiahol desiatky miliónov používateľov spojením ochrany súkromia s reklamou založenou na pozornosti, ktorá používateľov odmeňuje namiesto toho, aby ich vyťažovala.

Vzostup šifrovanej komunikácie

End-to-end šifrovaná komunikácia sa presadila medzi širokou verejnosťou úplnejšie než ktorákoľvek iná technológia na ochranu súkromia.

Rast aplikácie Signal ukazuje proces trhového objavovania. V januári 2021, po oznámení WhatsAppu, že bude s Facebookom zdieľať viac údajov, sa servery Signalu zrútili pod náporom nových používateľov.[14] Epizóda ukázala, ako rýchlo používatelia prejdú, keď sa náklady na súkromie stanú citeľnými a existuje použiteľná alternatíva. Signal je navyše nezisková organizácia, čo ukazuje, že šifrovaná komunikácia nemusí závisieť od reklamy ani od vyťažovania údajov.

Aj WhatsApp, hoci patrí Mete, používa na end-to-end šifrovanie protokol Signal.[22] Rozhodnutie bolo obranné: bez šifrovania by WhatsApp stratil používateľov v prospech šifrovaných alternatív. Aj firmy závislé od sledovania často musia poskytovať nejaké funkcie súkromia, aby zostali konkurencieschopné. Je to tlak trhu pôsobiaci cez konkurenciu, nie cez reguláciu.

Spôsob, akým sa šifrovanie rozšírilo, čosi prezrádza o tom, ako trhy objavujú dopyt po súkromí. Šifrovanie bolo kedysi technológiou len pre odborníkov, ktorá vyžadovala ručnú výmenu kľúčov a starostlivé nastavenie. Signal ho urobil predvoleným a neviditeľným, takže používatelia z neho majú úžitok bez toho, aby technológii rozumeli. Poučenie: nástroje súkromia musia byť rovnako pohodlné ako sledovacie alternatívy, aby sa široko ujali. Úspech na trhu výrazne ovplyvňuje aj použiteľnosť, nielen bezpečnosť.

Platené a reklamou financované modely

Model „bezplatných“ služieb závisí od vyťažovania údajov. Platené modely ponúkajú alternatívu: používatelia platia peniazmi, nie údajmi. Keď sú používatelia zákazníkmi, a nie produktmi, podnety firmy sa zhodujú so záujmami používateľov namiesto toho, aby im odporovali.

Predplatné služby vyrástli vo všetkých kategóriách. Streamované video ponúka úrovne bez reklám; používatelia tým odhalili preferenciu platiť za to, aby sa vyhli reklamám, ktoré umožňujú sledovanie. Platený prístup k spravodajstvu odstraňuje reklamný podnet maximalizovať zapojenie bez ohľadu na kvalitu obsahu. Predplatné produktivitného softvéru vytlačilo nástroje financované reklamou a zmenilo štruktúru podnetov v celom softvérovom odvetví.

Nie každá predplatná služba súkromie rešpektuje; aj platené produkty môžu údaje vyťažovať. Platený model však odstraňuje štrukturálny podnet, ktorý robí z vyťažovania údajov jadro podnikania, nie vedľajšiu prax. Firma, ktorej tržby plynú z predplatného, nemá štrukturálny dôvod maximalizovať zber údajov; firma, ktorej tržby plynú z predikčných produktov, ho má vždy.

Vzorec prémiových úrovní, ktorý sa objavuje v produktoch aj službách, naznačuje rastúcu ochotu platiť za súkromie a menej sledovania. Používatelia, ktorí kedysi prijímali „bezplatné“ služby, dnes platia za alternatívy, ktoré lepšie zodpovedajú ich záujmom. Táto odhalená preferencia usmerňuje podnikateľské objavovanie ďalších produktov rešpektujúcich súkromie.

Infraštruktúra súkromia

Popri jednotlivých produktoch začínajú štrukturálne obmedzovať vyťažovanie údajov aj zmeny v infraštruktúre. DNS cez HTTPS (DNS-over-HTTPS)[23] bráni poskytovateľom internetu sledovať a speňažovať údaje o prehliadaní. Predvolené šifrovanie počas prenosu, dnes štandardné na celom webe, bráni náhodnému zachyteniu. Hardvérové bezpečnostné moduly v spotrebných zariadeniach robia niektoré druhy vyťažovania údajov podstatne ťažšími.

Tieto zmeny infraštruktúry sa od konkurencie produktov líšia v dôležitých veciach. Voľba produktu si vyžaduje aktívne rozhodnutie používateľa; zmeny infraštruktúry chránia aj tých, ktorí sa nerozhodnú vôbec. Súkromie ako predvolená voľba je silnejšie než súkromie na požiadanie, lebo chráni drvivú väčšinu ľudí, ktorí si nastavenia nikdy nemenia.

Posun k predvoleným nastaveniam chrániacim súkromie odráža trhové objavovanie na úrovni infraštruktúry. Firmy, ktoré infraštruktúru ovládajú (výrobcovia prehliadačov, dodávatelia operačných systémov, výrobcovia zariadení), zistili, že funkcie súkromia dávajú konkurenčnú výhodu. Google, ktorý zavádza funkcie súkromia do prehliadača Chrome napriek

reklamnému podnikaniu, ukazuje konkurenčný tlak: ak Chrome funkcie súkromia neposkytne, používatelia prejdú k prehliadačom, ktoré ich poskytujú.

Odhlásenie z registrov dátových brokerov ako záplata na režim

Dnes existuje predplatný trh so službami, ktoré sa pokúšajú odstrániť záznamy jednotlivca zo stoviek adresárov dátových brokerov, ktoré zhromažďujú verejné záznamy, údaje z katastra, zoznamy voličov a históriu nákupov. Optery, Incogni, DeleteMe, Kanary a Privacy Bee sú v čase písania hlavnými poskytovateľmi. Služby automatizujú žiadosti o odhlásenie voči každému brokerovi, vrátia snímky obrazovky ako dôkaz vymazania a proces opakujú podľa plánu, lebo brokeri záznamy dopĺňajú z primárnych zdrojov.[15]

Podstatný je samotný fakt, že takýto trh existuje. Predplatné, ktoré musí bežať, kým chce človek mať pred odvetvím dátových brokerov súkromie, je to, čo americké právo ponúka namiesto zákazu samotného zhromažďovania, a model predplatného existuje preto, že právo podkladové zhromažďovanie dovoľuje. Nástroje fungujú v rámci svojich hraníc a stojí za to ich mať. Rakúsky postreh je, že trh s týmito službami je záplatou na regulačný režim, a právny režim, ktorý by zhromažďovanie nepripúšťal, by záplatu nepotreboval.

Hranice reakcie trhu

Reakcie trhu sú skutočné, no čelia štrukturálnym prekážkam. Sieťové efekty uprednostňujú zavedené platformy; používatelia ľahko neprejdú inam, keď ich kontakty zostávajú na sledovacích platformách. Proces objavovania je pomalý; mnohí používatelia o alternatívach nevedia. Produkty na ochranu súkromia sú často ťažšie na používanie než sledovacie alternatívy, čo obmedzuje ich prijatie na tých, ktorí súkromie osobitne uprednostňujú.

Reakcia trhu navyše rieši len niektoré rozmery problému sledovania. Firmy môžu súťažiť v súkromí pri funkciách, kde existujú alternatívy rešpektujúce súkromie. Trhová konkurencia však nemôže priamo odstrániť vládne požiadavky na sledovanie, monitorovanie na úrovni infraštruktúry ani hromadenie údajov subjektmi, ktoré nečelia trhovému tlaku na ich mazanie.

Netvrdíme, že trhy vyriešia všetky problémy okamžite; naše tvrdenie je užšie. Trhy objavujú preferencie prostredníctvom podnikateľského experimentovania a konkurencia časom smeruje k uspokojovaniu týchto preferencií. Trh so súkromím je v ranom štádiu. Trajektória smeruje k väčšej konkurencii v súkromí, ale proces nie je dokončený.

Trhové objavovanie

Preferencie týkajúce sa súkromia boli skryté, kým ich podnikatelia nevytvorili produkty, ktoré ich odhalili. Apple nevedel, že 80 percent používateľov odmietne sledovanie, kým im ATT nedalo voľbu, a Signal nevedel, že milióny ľudí prijmú šifrovanú komunikáciu, kým použiteľnosť neumožnila jej prijatie. Proces objavovania nemá vopred určený koniec a súčasné nástroje súkromia sú v ranom štádiu. Každá generácia sa používa ľahšie a lepšie obstojí proti sledovacím alternatívam. Trhy problém súkromia nevyriešili; práve objavujú, ako ho vyriešiť.

Zhrnutie kapitoly

Firemné vyťažovanie údajov obracia tradičný trhový vzťah. Zákazníkom je inzerent, používateľ dodáva surovinu pre predikčné produkty a firma súťaží o získanie používateľov; slúžiť im je pre model len vedľajšie. Firemné a štátne sledovanie sa stali symbiotickými: zákonné povinnosti nútia zbierať údaje, dobrovoľná spolupráca dáva vláde prístup k údajom, ktoré by firmám nikto nemohol priamo zákonne nariadiť zbierať, a partnerstvo verejného a súkromného sektora dosahuje rozsah sledovania, aký by ani jedna strana sama nezvládla. Súčasné výsledky tiež odrážajú rozsiahlu štátnu intervenciu: „duševné vlastníctvo“ vytvára monopoly platforiem, predpisy o súlade budujú regulačné priekopy okolo zavedených hráčov a vládne zákazky podnecujú vývoj sledovania. Kontrafaktuálny slobodný trh by priniesol iné podnety.

Biometrické a genetické údaje tvoria osobitnú kategóriu. Nedajú sa rotovať, lebo odtlačok prsta, sken dúhovky, tvár, odtlačok hlasu alebo genóm je ten istý identifikátor počas všetkých rokov života človeka. Únik je pre jednotlivcov, ktorých záznamy obsahoval, trvalý a nenapraviteľný a právne prostriedky môžu odhalenie oceniť dodatočne, no nevrátia ho. Obranný postoj, ktorý si to vynucuje, stojí na prevencii a musí uspieť zakaždým, lebo jediný únik je trvalý.

Trhy reagujú na dopyt po súkromí, ktorý intervencia neuspokojila. App Tracking Transparency od Applu ukázalo, že zhruba 80 % používateľov sledovanie odmieta, keď dostanú jasnú voľbu, šifrovaná komunikácia sa presadila u širokej verejnosti a platené služby ponúkajú alternatívy k vyťažovaniu financovanému reklamou. Objavovanie nie je dokončené. Sieťové efekty, problémy koordinácie a vládne požiadavky na sledovanie vytvárajú prekážky, ktoré samotná trhová konkurencia možno neprekoná, a ďalšia regulácia hrozí upevnením existujúcej sledovacej infraštruktúry cez regulačné priekopy, ktoré uprednostňujú zavedených hráčov. Analýza trhy ani neodsudzuje, ani nezbavuje viny. Konštatuje, že súčasné podnety formuje intervencia rovnako ako spotrebiteľské preferencie, a že technic-

ké a podnikateľské riešenia môžu uspieť tam, kde by regulačné posilnili štruktúru, ktorú sa snažia obmedziť.[16]

Poznámky

[1] Neil Postman, *Technopoly: The Surrender of Culture to Technology* (New York: Alfred A. Knopf, 1992), 7. Postman to napísal o desaťročie skôr, než obchodný model sledovacieho kapitalizmu získal dominanciu, a jeho rámec predvídal vzorec, ktorý táto kapitola analyzuje: keď sa technológia zavedie na úzke komerčné účely, jej vnútorná logika prestavuje činnosti okolo nej. Internet financovaný reklamou nevynašiel sledovanie používateľov; zdedil logiku toho, čo Postman nazval technopoly, v ktorom sa meracie nástroje stávajú rámcom, cez ktorý sa chápe samotná skúsenosť. Pre populárnokultúrne zhrnutie toho istého argumentu pozri Andrew Lewis (používateľ „blue_beetle"), komentár na MetaFilter, 26. augusta 2010: „Ak za to neplatíte, nie ste zákazník; ste produkt, ktorý sa predáva" (If you are not paying for it, you're not the customer; you're the product being sold), formuláciu, ktorú analýza tejto kapitoly rozširuje a zakladá.

[2] Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (New York: PublicAffairs, 2019), 8-11. Zuboff podrobne dokumentuje vývoj a praktiky sledovacieho kapitalizmu, hoci jej analýza sa líši od rakúskej perspektívy použitej tu.

[3] O sieťových efektoch a ekonómii platforiem pozri David S. Evans a Richard Schmalensee, *Matchmakers: The New Economics of Multisided Platforms* (Boston: Harvard Business Review Press, 2016).

[4] Richard Cantillon, *Essai sur la Nature du Commerce en Général*, ed. Henry Higgs (London: Macmillan, 1931; francúzsky originál 1755), časť II, kapitoly 6–7. K rakúskemu spracovaniu pozri Ludwig von Mises, *The Theory of Money and Credit*, prel. H. E. Batson (New Haven: Yale University Press, 1953 [1912]), druhá časť, kapitola 8; a Rothbard, *Man, Economy, and State* (cit. v kap. 3, pozn. 3), kapitola 11. Obmedzenie Cantillonovho efektu na menovú expanziu je v rakúskej literatúre zámerné a analógia s tokmi údajov v hlavnom texte tvrdí len to, že štrukturálny vzorec sa opakuje, nie že sa menová analýza dá prenášať.

[5] Program PRISM vyšiel najavo vďaka dokumentom, ktoré v roku 2013 prezradil Edward Snowden. Pozri Glenn Greenwald, *No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State* (cit. v kap. 1, pozn. 7).

[6] K rakúskej kritike teórie zlyhania trhu pozri Israel M. Kirzner, „The Perils of Regulation: A Market-Process Approach," v *Discovery and the Capitalist Process* (Chicago: University of Chicago Press, 1985), a Rothbard, *Power and Market* (cit. v kap. 10, pozn. 2), kapitola 3.

[7] K oddielu 230 a imunite platforiem pozri Jeff Kosseff, *The Twenty-Six Words That Created the Internet* (Ithaca, NY: Cornell University Press, 2019).

[8] Frédéric Bastiat, „Ce qu'on voit et ce qu'on ne voit pas" (1850), preložené ako „That Which Is Seen, and That Which Is Not Seen," in *Selected Essays on Political Economy*, prel. Seymour Cain (Irvington-on-Hudson, NY: Foundation for Economic Education, 1995). Henry Hazlitt, *Economics in One Lesson* (New York: Harper, 1946), kapitola 1, formuluje princíp priamo: „The art of economics consists in looking not merely at the immediate but at the longer effects of any act or policy; it consists in tracing the consequences of that policy not merely for one group but for all groups." (Umenie ekonómie spočíva v tom, že sa človek nepozerá len na bezprostredné, ale aj na dlhodobejšie účinky každého činu alebo politiky; spočíva v sledovaní dôsledkov tejto politiky nielen pre jednu skupinu, ale pre všetky skupiny.)

[9] Útok typu credential stuffing na 23andMe v októbri 2023 odhalil približne sedem miliónov profilov zákazníkov; firma podala v marci 2025 návrh podľa Chapter 11 a jej genetická databáza bola v roku 2025 vydražená ako konkurzný majetok, čo potvrdzuje, že

genetické údaje sú trvalé, prenosné odhalenie, ktoré bežný spotrebiteľský súhlas neoceňuje. 23andMe, https://www.23andme.com/. 23andMe breach disclosure (December 2023), SEC filing, https://www.sec.gov/Archives/edgar/data/1804591/000110465923124825/tm2331489d1_8k.htm. Správy o urovnaní hromadnej žaloby v *Reuters* a *Bloomberg*, 2024. Konkurzné podanie podľa Chapter 11 v In re 23andMe Holding Co., Case No. 25-10625, U.S. Bankruptcy Court, Southern District of Texas (marec 2025). Genetic Information Nondiscrimination Act of 2008 (GINA), 42 U.S.C. § 2000ff. K hraniciam HIPAA a GINA pri spotrebiteľských genetických databázach pozri Natalie Ram, „Genetic Privacy After Carpenter," *Virginia Law Review* 105 (2019).

[10] Indický biometrický identifikačný program Aadhaar zapisuje viac než 1,3 miliardy obyvateľov s odtlačkami prstov, skenmi dúhovky a demografickými údajmi centrálne uloženými Unique Identification Authority of India; architektonické kritiky od roku 2017 označili centrálnu databázu za jediný bod, ktorého kompromitácia by navždy vyjmenovala biometrické identifikátory celej populácie. Aadhaar / UIDAI, https://uidai.gov.in/. K architektonickým kritikám pozri Reetika Khera et al., *Dissent on Aadhaar: Big Data Meets Big Brother* (Orient BlackSwan, 2019). K zrušiteľnosti biometrických šablón pozri Nalini Ratha, Jonathan Connell, and Ruud Bolle, „Enhancing Security and Privacy in Biometrics-Based Authentication Systems," *IBM Systems Journal* 40, no. 3 (2001): 614–634, a nadväzujúcu literatúru o ochrane biometrických šablón v zborníkoch IEEE International Joint Conference on Biometrics (IJCB). Porovnateľné programy sú pakistanská NADRA, https://www.nadra.gov.pk/, a navrhovaná Európska peňaženka digitálnej identity podľa eIDAS 2.0.

[11] Illinois BIPA (2008) je vzorovým štátnym zákonom o biometrickom súkromí so súkromným právom na žalobu; niekoľko amerických štátov (Texas, Washington, New York a ďalšie) prijalo od roku 2021 podobné zákony; právne prostriedky oceňujú biometrické odhalenie dodatočne, no samotnému odhaleniu zabrániť nevedia. Illinois Biometric Information Privacy Act (BIPA), 740 ILCS 14, https://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=3004&ChapterID=57. Texas Capture or Use of Biometric Identifier Act (CUBI), Tex. Bus. & Com. Code § 503.001. Washington State biometric privacy law, RCW 19.375. K sporom o BIPA pozri *Rosenbach v. Six Flags Entertainment Corp.*, 129 N.E.3d 1197 (Ill. 2019), a *Cothron v. White Castle System, Inc.*, 216 N.E.3d 918 (Ill. 2023). Porovnávaciu analýzu štátnych zákonov o biometrickom súkromí nájdete v správach Future of Privacy Forum, https://fpf.org/.

[12] V treťom štvrťroku 2021 približne 80 % používateľov iOS po zavedení ATT odmietlo sledovanie na veľkých platformách sociálnych sietí. Pozri Statista, „App Tracking Transparency: Opt-In Rate of iOS Users 2022," a Flurry Analytics, „App Tracking Transparency Opt-In Rate: Monthly Updates."

[13] Finančný riaditeľ Metu Dave Wehner uviedol odhadovaný vplyv na tržby 10 miliárd dolárov počas hovoru o výsledkoch za štvrtý štvrťrok 2021 vo februári 2022. Pozri „Facebook Says Apple iOS Privacy Change Will Result in $10 Billion Revenue Hit This Year," CNBC, February 2, 2022. Lotame odhadla celkový vplyv na 12,8 miliardy dolárov.

[14] Kanonický odkaz na Signal Foundation a špecifikácie protokolu pozri v kap. 5, pozn. 7. K neziskovej štruktúre a údajnému rastu Signalu pozri daňové priznania Signal Technology Foundation a Business of Apps, „Signal Revenue & Usage Statistics (2025)." Signal Foundation pôsobí ako nezisková organizácia 501(c)(3) financovaná predovšetkým z darov.

[15] Optery, Incogni, DeleteMe, Kanary a Privacy Bee sú hlavnými poskytovateľmi na trhu s predplatným za odhlasovanie z registrov dátových brokerov; existencia tohto trhu ukazuje, že americké právo oceňuje zhromažďovanie údajov dátovými brokermi dodatočným odhlásením namiesto zákazu. Optery, https://www.optery.com/. Incogni (Surfshark), https://incogni.com/. DeleteMe (Abine), https://joindeleteme.com/. Kanary, https://www.kanary.com/.

Privacy Bee, https://privacybee.com/. K základnému regulačnému dokumentu o odvetví dátových brokerov pozri Federal Trade Commission, *Data Brokers: A Call for Transparency and Accountability* (May 2014), už citované v pozn. 16. K vermontskému registračnému režimu dátových brokerov ako jednej odpovedi na úrovni štátu pozri 9 V.S.A. § 2446.

[17] Premenlivé schémy odmeňovania – vzorce prerušovaného posilňovania, ktoré maximalizujú zapojenie tým, že odmeny prichádzajú nepredvídateľne – prvýkrát opísal B.F. Skinner v *The Behavior of Organisms* (New York: Appleton-Century-Crofts, 1938). Ich uplatnenie v dizajne digitálnych produktov dokumentuje Natasha Dow Schüll, *Addiction by Design: Machine Gambling in Las Vegas* (Princeton, NJ: Princeton University Press, 2012), ktorá rozoberá, ako dizajnéri hracích automatov používajú schémy s premenlivým pomerom na maximalizáciu času stráveného pri zariadení; tá istá logika sa priamo preniesla do dizajnu prúdov príspevkov na sociálnych sieťach. Práca Tristana Harrisa v Center for Humane Technology, https://www.humanetech.com/, dokumentuje zámerné uplatňovanie týchto techník v aplikáciách pre smartfóny.

[18] National Security Letters sú administratívne predvolania, ktoré vydáva FBI podľa 18 U.S.C. § 2709 (elektronická komunikácia), 12 U.S.C. § 3414 (finančné záznamy) a súvisiacich predpisov a nútia k odhaleniu záznamov o zákazníkoch, pričom adresátom zakazujú priznať, že žiadosť dostali. Ustanovenie o zákaze hovoriť o žiadosti bolo napadnuté v *Doe v. Ashcroft*, 334 F. Supp. 2d 471 (S.D.N.Y. 2004), a následne v *Doe v. Mukasey*, 549 F.3d 861 (2d Cir. 2008), ktorý vyžadoval súdne preskúmanie takýchto zákazov. FBI vydávala začiatkom dvadsiatych rokov približne 16 000–17 000 žiadostí NSL ročne. K rozsahu používania pozri Electronic Frontier Foundation, „National Security Letters," https://www.eff.org/issues/national-security-letters, a výročné správy FBI pre Kongres o používaní NSL vyžadované podľa 18 U.S.C. § 2709(e).

[19] General Data Protection Regulation (GDPR), Regulation (EU) 2016/679, Official Journal of the European Union, L 119/1 (May 4, 2016), účinné od 25. mája 2018, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679. GDPR ukladá povinnosti minimalizácie údajov, súhlasu a zodpovednosti firmám, ktoré spracúvajú osobné údaje obyvateľov EÚ. K argumentu o asymetrii nákladov na súlad – že veľkí zavedení hráči zvládnu náklady na súlad, ktoré vylučujú menších rivalov – pozri Cristina Caffarra and Fiona Scott Morton, „The European Commission Digital Markets Act: A Translation," VoxEU, https://cepr.org/voxeu/ (2021); a Garrett Johnson, Scott Shriver, and Samuel Goldberg, „Privacy and Market Concentration: Intended and Unintended Consequences of the GDPR," *Marketing Science* 42, no. 3 (2023): 454–480.

[20] DuckDuckGo je vyhľadávač zachovávajúci súkromie, ktorý nesleduje používateľov ani nevytvára behaviorálne profily. DuckDuckGo, https://duckduckgo.com/. Založil ho Gabriel Weinberg v roku 2008; v januári 2021 DuckDuckGo oznámil prekročenie 100 miliárd dopytov za celé obdobie a do roku 2023 spracúval cez 3 miliardy dopytov mesačne. K údajom o návštevnosti pozri DuckDuckGo Traffic Statistics, https://duckduckgo.com/traffic. Vyhľadávač ukazuje odhalenú preferenciu pre alternatívy rešpektujúce súkromie, aj keď ponúkajú menej úplné výsledky než Google.

[21] Brave je prehliadač zameraný na súkromie, ktorý vyvinula firma Brave Software, Inc., založená Brendanom Eichom (spoluautorom JavaScriptu a bývalým generálnym riaditeľom Mozilly). Brave, https://brave.com/. Brave predvolene blokuje sledovače a reklamy a ponúka systém Basic Attention Token (BAT), ktorý odmeňuje používateľov za súhlas s reklamami rešpektujúcimi súkromie. Brave dosiahol 50 miliónov mesačne aktívnych používateľov do roku 2022 a viac než 60 miliónov do roku 2023. K štatistikám používania pozri správy o transparentnosti Brave na https://brave.com/transparency/. Model BAT opisuje Brendan Eich and Brian Bondy, „Basic Attention Token (BAT): Blockchain Based Digital Advertising" (white

paper, 2017), https://basicattentiontoken.org/static-assets/documents/BasicAttentionTokenWhitePaper-4.pdf.

[22] WhatsApp prijal protokol Signal na end-to-end šifrovanie v roku 2016 a v apríli 2016 dokončil zavedenie pre všetkých jednu miliardu používateľov. Integrácia vznikla v spolupráci s Open Whisper Systems. Pozri Moxie Marlinspike, „WhatsApp's Signal Protocol Integration Is Now Complete," Open Whisper Systems blog, April 5, 2016, https://signal.org/blog/whatsapp-complete/. Špecifikácia protokolu Signal je na https://signal.org/docs/. Prijatie zo strany WhatsAppu je najväčším nasadením end-to-end šifrovania v dejinách; že materská firma závislá od sledovania (Meta) považovala šifrovanie za konkurenčne nevyhnutné, ilustruje trhový tlak, ktorý táto kapitola analyzuje.

[23] DNS-over-HTTPS (DoH) šifruje dopyty DNS medzi klientom a prekladačom DNS a bráni poskytovateľom internetu sledovať vyhľadávanie doménových mien. Štandard definuje Paul Hoffman and Patrick McManus, „DNS Queries over HTTPS (DoH)," RFC 8484, Internet Engineering Task Force (October 2018), https://www.rfc-editor.org/rfc/rfc8484. Medzi hlavné nasadenia v prehliadačoch patria Firefox (predvolené DoH od roku 2020, https://blog.mozilla.org/en/products/firefox/firefox-continues-push-to-bring-dns-over-https-by-default-for-us-users/) a Chrome (bezpečné DNS od roku 2020). Odpor poskytovateľov internetu voči nasadeniu DoH je zdokumentovaný v dôkazoch pre britský parlament od Virgin Media, BT a Sky a v analýze Internet Society na https://www.internetsociety.org/resources/doc/2019/dns-over-https/.

[16] Ďalšie čítanie o sledovacom kapitalizme, adtech a dátových brokeroch. Ako kanonické kritické spracovanie pozri Zuboff, *The Age of Surveillance Capitalism*, pozn. 2 vyššie a kap. 1, pozn. 6; Carissa Véliz, *Privacy Is Power* (Bantam Press, 2020), je kratšia populárna verzia. K mechanizmu predikcie správania je prístupný Jaron Lanier, *Ten Arguments for Deleting Your Social Media Accounts Right Now* (Henry Holt, 2018); Yasha Levine, *Surveillance Valley: The Secret Military History of the Internet* (PublicAffairs, 2018), dokumentuje kontinuitu štátu a komerčného sektora. K odhaleniam o NSA z roku 2013, na ktorých stojí citácia PRISM v pozn. 5, je rozprávacím spracovaním Greenwald, *No Place to Hide* (cit. v kap. 1, pozn. 7). K dátovým brokerom osobitne zostáva základným regulačným dokumentom správa FTC *Data Brokers: A Call for Transparency and Accountability* (May 2014), https://www.ftc.gov/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014; priebežné reportáže Kashmir Hill v *The New York Times* sú najlepšou súčasnou žurnalistikou o konkrétnych praktikách dátových brokerov. K rakúskej kritike „zlyhania trhu" aplikovanej na platformy je teoretickým základom Kirzner, „The Perils of Regulation" (cit. v pozn. 6 vyššie); z empirických prác sa honbe za rentou na trhoch platforiem venujú Luigi Zingales, *A Capitalism for the People: Recapturing the Lost Genius of American Prosperity* (Basic Books, 2012), a priebežné pracovné dokumenty Stigler Center na https://stigler.capitalisnt.com. K mechanike sledovania je štandardnou empirickou štúdiou Timothy Libert, „Exposing the Hidden Web: An Analysis of Third-Party HTTP Requests on 1 Million Websites," *International Journal of Communication* 9 (2015): 3544–3561; práca OpenWPM, ktorú vedie Arvind Narayanan a kolegovia na Princetone, https://webtransparency.cs.princeton.edu, je technickým meracím východiskom. Ku kritike hedonického kompromisu pri „bezplatných službách" stojí za prečítanie popri kritikoch Hal Varian, „Beyond Big Data," *Business Economics* 49, no. 1 (2014): 27–31, ako pohľad obhajcu odvetvia.

12
ANALYTICKÝ STACK

„Záujem vládneho úradu o údaje sa nekončí pri tom, čo smie zákonne zbierať."

Anonym, pôvod neznámy

Úvod

Komerčné firmy bez zákonného poverenia vybudovali sledovacie schopnosti v rozsahu, ktorý by žiadny jednotlivý úrad nedokázal obhájiť, a štátne úrady ich výstupy nakupujú. Senzory zbierajú, brokeri zhromažďujú, modely analyzujú a úrady konajú. Čo ústava zakazuje akémukoľvek jednému aktérovi, to trh poskladá po etapách, aby si to štát mohol kúpiť. Sledovanie sa z priameho pozorovania štátom zmenilo na priemyselný proces, v ktorom má každý krok svoju cenu. Kapitola 13 ukáže, ako štát útočí na kryptografické nástroje. Táto kapitola ukazuje, ako štát kupuje pozorovaciu vrstvu, ktorá existuje pred zašifrovaním obsahu a po jeho dešifrovaní.

12.1 Deľba práce v sledovaní

Adam Smith si všimol, že deľba práce zvyšuje produktivitu, lebo umožňuje špecializáciu.[13] Ludwig von Mises to rozšíril: špecializácia závisí od trhovej výmeny, takže deľba práce a katalaktický poriadok sú jedno a to isté.[14] Analytický stack uplatňuje ten istý princíp na pozorovanie.

Jediný úrad nemôže zákonne vybudovať a udržiavať databázu rozpoznávania tváre so všetkými fotografiami z otvoreného webu. Nemá na to poverenie ani politické krytie. Súkromná firma takú databázu postaviť môže, lebo ju viažu oveľa slabšie obmedzenia komerčného prejavu. Potom predá prístup úradom, ktoré by ju priamo vytvoriť nemohli. Úrad

platí predplatné. Firma platí za inžinierstvo. Ani jedna strana nenesie plný reputačný či ústavný náklad, ktorý by priamy program priniesol.

Rovnaká logika platí v každej vrstve stacku. Zachytávanie evidenčných čísel vozidiel, sledovanie polohy, získavanie sociálnych grafov, predikcia správania, kompromitovanie koncových zariadení a analytická fúzia údajov: každú z týchto činností robia špecializované firmy a svoj výstup predávajú na konkurenčnom trhu. Štát je len jedným zo zákazníkov. Firma tak môže tvrdiť, že nie je dodávateľom vlády v regulačnom zmysle ani štátnym aktérom v zmysle ústavy, a štát môže platiť trhovú cenu za schopnosti, ktoré by zákonne nemohol vybudovať.[1]

Takéto usporiadanie je predvídateľným dôsledkom súhry dvoch doktrín. Prvou je doktrína tretej strany: informácie, ktoré niekto dobrovoľne zdieľa s treťou stranou, majú nižšiu ochranu podľa Štvrtého dodatku. Druhou je povolenie komerčného prejavu pri zbieraní údajov o ľuďoch, ktorí nie sú zákazníkmi zberateľa. Patrí sem automatizované sťahovanie webu (scraping), zbieranie dát z reklamných aukcií a fotografovanie evidenčných čísel na verejných cestách. Medzi nimi vzniká trh pre pozorovací apetít štátu: prvá doktrína nákup umožňuje a druhá vyrába ponuku. Lepšie pravidlá to nezalátajú, lebo tento stav pravidlá samy vyprodukovali.[2]

Koalícia, ktorú stack zostavuje

Každá štátna činnosť rozdeľuje obyvateľstvo na triedu, ktorá do aparátu platí viac, než dostáva, a triedu, ktorá dostáva viac, než platí. Rothbardovou novinkou bolo zaradiť do druhej triedy nielen štátnych zamestnancov, ale aj dodávateľov, predajcov a príjemcov monopolných privilégií, ktorých príjmy závisia od toho, že štát pokračuje v činnosti.[3] Firmy, z ktorých sa analytický stack skladá, patria do tejto triedy. Dátový broker, ktorý predáva ministerstvu vnútornej bezpečnosti, dodávateľ rozpoznávania tváre pre imigračný a colný úrad ICE, firma so spyware pre spojenecké ministerstvá vnútra a platforma prediktívnych policajných metód pre mestské policajné zbory: všetci majú príjmy viazané na to, že štát bude naďalej nakupovať.

Z tohto zosúladenia vyplýva odolnosť stacku voči politickému tlaku. Príjmy firiem závisia od toho, že štát bude kupovať ďalej, a nákupy štátu závisia od toho, že schopnosť, ktorú firmy vyrábajú, existuje. Verejný tlak proti jednej zákazke dopadne na koalíciu, ktorej členovia ho znášajú spoločne. Koalícia je trvácna, lebo každý člen má obchodný záujem udržať ostatných nad vodou.

12.2 Strojové videnie vo veľkom

Rozpoznávanie tváre mení vizuálny identifikátor, ktorý kedysi ohraničovala ľudská pamäť, na index do trvalej databázy. Matematika je pritom obyčajná: neurónová sieť priradí obrázku vektor vo viacrozmernom pries-

tore a dva snímky tej istej tváre dajú vektory, ktoré sú podľa zvolenej metriky blízko seba. Tento postup poznali dávno predtým, než sa stal politickou otázkou. Zmenila sa cena.

Získavanie snímok kleslo takmer na nulu vďaka všadeprítomným kamerám. Vyhodnotenie obrazu modelom kleslo na zlomky centu vďaka ekonomike spotrebiteľských GPU. Ukladanie vektorov vlastností kleslo na triviálnu cenu vďaka bežným databázam. Keď sa zrútili všetky tri náklady, porovnať fotografiu s korpusom miliardy obrázkov bolo lacnejšie než papierovanie, ktoré by si vyžiadalo, keby sa to nerobilo. Schopnosť, ktorá bola dovtedy len teoreticky dostupná, sa stala prevádzkovo univerzálnou.

Clearview AI je učebnicový prípad, lebo odstránila poslednú zostávajúcu prekážku: veľkosť korpusu. Sťahovaním obrázkov z otvoreného webu si firma vybudovala korpus s približne dvadsiatimi miliardami fotografií. Ten je väčší než akákoľvek databáza zostavená vládou a nepodlieha nijakému legislatívnemu dohľadu. Orgány činné v trestnom konaní, ktoré by taký korpus zákonne zostaviť nemohli, ho odoberajú ako službu. Európske úrady na ochranu údajov v niekoľkých členských štátoch uložili pokuty a zákazy, v Spojených štátoch to však nemalo žiadny prevádzkový účinok. Dohoda s organizáciou ACLU v prípade podľa zákona štátu Illinois o ochrane biometrických informácií (Biometric Information Privacy Act, BIPA) obmedzuje komerčný predaj Clearview v USA na vládne subjekty, a to je presne klientela, ktorú firma už obsluhovala.

Princíp nezávisí práve od Clearview. Každá firma, ktorá je ochotná ignorovať normy sťahovania webu, si môže vybudovať porovnateľný korpus. Nahraditeľnosť firmy robí schopnosť trvalou. Databáza HART (Homeland Advanced Recognition Technology) ministerstva vnútornej bezpečnosti je navrhnutá tak, aby obsahovala biometrické a demografické záznamy stoviek miliónov identít. Je prepojená s biometrickým systémom vstupu a výstupu colnej a pohraničnej správy (CBP) a s letiskovými kioskami na porovnávanie tvárí, ktoré prevádzkuje Správa bezpečnosti dopravy (TSA) a ktoré dnes stoja na desiatkach veľkých amerických letísk. Jediná kontrola totožnosti, ktorú nikto nikdy nezaviedol zákonom, tak beží naprieč komerčnými korpusmi, federálnymi indexmi, letiskovou infraštruktúrou aj hraničnými priechodmi.[4]

Ľudské rozpoznávanie malo prirodzený cenový strop, lebo pamäť je konečná a okoloidúci zabudne do niekoľkých minút. Strojové rozpoznávanie taký strop nemá. Schopnosť, ktorej používanie obmedzovala cena, už obmedzená nie je, keď cena padne, a nasadzuje sa takým tempom, aké dovolia ostatné obmedzenia. Zákon napísaný pre svet vzácnosti neopisuje svet hojnosti.

12.3 Model ako analytik

Pracné bolo v minulej spravodajskej práci čítanie. Dokumenty sa hromadili rýchlejšie, než ich analytici stíhali spracovať, a väčšina zozbieraného materiálu preto zostala mŕtvou váhou. Veľké jazykové modely menia kalkuláciu. Jediný analytik s dobre pripraveným modelom dnes vie vytvárať zhrnutia, extrakcie, preklady a korelácie nad objemami dokumentov, na ktoré bola predtým potrebná pozornosť celej organizácie. Úzke hrdlo sa presunulo od čítania k formulovaniu dopytu.

Viditeľným príkladom tohto posunu je Artificial Intelligence Platform firmy Palantir, uvedená v roku 2023 a predávaná spolu s existujúcimi produktmi Gotham a Foundry. Do roku 2025 prekročili jej tržby štyri miliardy dolárov, so zákazkami naprieč ministerstvom obrany, ministerstvom vnútornej bezpečnosti, imigračným a colným úradom ICE a námorníctvom. Hodnota zákaziek je menej dôležitá než to, čo sa za ne kupuje. Kupuje sa zlúčené dátové prostredie s dopytovým rozhraním riadeným modelom: analytik položí otázku v prirodzenom jazyku a dostane odpoveď zostavenú zo štruktúrovaných záznamov, neštruktúrovaných dokumentov, satelitných snímok a prúdov zo senzorov. Niekoľkodňová spolupráca špecialistov sa zmestí do jedinej konverzácie.[5]

Skorší argument tejto knihy hovoril, že obrana súkromia je lacnejšia než útok naň, lebo šifrovanie stojí centy, zatiaľ čo jeho prelomenie stojí miliardy. To platí pre každú jednotlivú komunikáciu. Analytický stack však neútočí na jednotlivé komunikácie, útočí na agregáciu. Milión zachytených záznamov nemá žiadnu cenu, ak ich nik nedokáže prečítať. Milión záznamov vložených do modelu má cenu obrovskú, lebo model z nich vytiahne vzorce za náklady na dopyt blížiace sa nule. Asymetria nákladov, ktorá dovtedy zvýhodňovala obranu, sa na vrstve agregácie sčasti vyrovnala.

Terč obrany sa preto presunul. Šifrovanie obsahu zostáva nevyhnutné, ale už nestačí. Treba chrániť aj metadáta, z ktorých model skladá vzorce, keď obsah nie je dostupný: načasovanie, sociálny graf, polohu, identifikátor zariadenia a frekvenciu. Model je predovšetkým analytik metadát a obsah analyzuje, až keď metadáta zlyhajú. Preto sú nevyhnutné obrany na úrovni prenosu, ktoré rozvádza kapitola 17.

12.4 Kanál dátových brokerov

Dátový broker (obchodník s osobnými údajmi) je firma, ktorá zhromažďuje záznamy o jednotlivcoch a ďalej ich predáva. Odvetvie je staršie než internet, s ním však narástlo a jeho ekonomická funkcia bola daná skôr, než sa niekto spýtal, či má vôbec existovať. Brokeri nakupujú od vydavateľov aplikácií, vernostných programov, úverových kancelárií, z verejných registrov a z prúdu dát z reklamných aukcií v reálnom čase (real-time bidding). Predávajú inzerentom, poisťovniam, zamestnávateľom, súkrom-

ným detektívom a prostredníctvom špecializovaných sprostredkovateľov aj vládnym úradom.

Zaujímavý je práve predaj vláde. Rozhodnutie Najvyššieho súdu z roku 2018 vo veci *Carpenter v. United States* určilo, že vláda potrebuje príkaz, ak chce od operátora vynútiť historické údaje o polohe mobilných vysielačov. Rozhodnutie bolo odôvodnené úzko. Súd zdôraznil nútené uchovávanie záznamov operátorom a podrobnosť historických záznamov o polohe. Rozhodnutie sa nijako nezaoberalo informáciami, ktoré vláda nevynucuje, ale kupuje od obchodného subjektu, ktorý ich získal zákonne. Táto medzera je medzera dátových brokerov (data-broker loophole).

Venntel, dcérska firma spoločnosti Gravy Analytics, ktorá pôsobí v reklamných technológiách, predávala federálnym úradom údaje o polohe z prúdu reklamných aukcií v reálnom čase koncom desiatych rokov tohto storočia. Generálny inšpektor ministerstva financií pre daňovú správu (TIGTA) v správe z roku 2023 potvrdil, že vyšetrovacia služba Internal Revenue Service (IRS Criminal Investigation) používala údaje z Venntelu bez príkazu v rokoch 2017 až 2018. Išlo o bežné vnútroštátne daňové veci, nie o výnimky z dôvodu národnej bezpečnosti. V roku 2024 prevzala schopnosti Venntelu firma Babel Street a premenovala ich na Locate X. Podobný produkt Fog Reveal zdokumentovali Electronic Frontier Foundation a agentúra Associated Press: používali ho desiatky miestnych, štátnych aj federálnych úradov na všetkých úrovniach amerického presadzovania práva.[6]

Štvrtý dodatok, napísaný proti priamemu získavaniu informácií štátom, či už prehliadkou, zhabaním alebo nátlakom, nemá slová pre prípad, keď štát nerobí nič z toho a len nakupuje. Informácie získané nákupom sú rovnako podrobné ako čokoľvek, čo by priniesol súdny príkaz. Právna teória, na ktorej to stojí, hovorí, že nikto nepotreboval príkaz na to, aby kúpil, čo trh už predával. Kongres opakovane zvažoval návrhy na uzavretie tejto medzery v podobe zákona „Štvrtý dodatok nie je na predaj“ (Fourth Amendment Is Not for Sale Act). Každý z nich zlyhal vo výbore alebo zanikol v legislatívnom procese, takže komerčný kanál funguje nepretržite.

Kapitola 10 analyzovala finančné sledovanie ako trojuholníkovú intervenciu v Rothbardovom zmysle: štát viaže bankovú licenciu na povinnosť banky hlásiť údaje o vkladateľoch a podmienky výmeny medzi bankou a vkladateľom sa nátlakom zmenia tak, aby zahŕňali štátne pozorovanie. Kanál dátových brokerov dosahuje rovnaký výsledok bez trojuholníkovej intervencie. Každá transakcia v reťazci je dobrovoľná. Dotknutý človek vstúpi do výmeny s vydavateľom aplikácie, vydavateľ údaje predá brokerovi a broker ich predá štátu. Štát žiadnu z týchto výmen nevynucuje, len kupuje ich výstupy. Prácu nerobí nátlak na výmenu, ale selektívna absencia ochrany okolo nej. Doktrína tretej strany odoberá človeku záujem chránený Štvrtým dodatkom v okamihu, keď údaje opustia jeho ruky,

a rámec komerčného prejavu dovoľuje ďalší predaj, ktorý táto doktrína urobila právne bezrizikovým. Informácie tečú rovnako ako pri nútenom odovzdaní, mechanizmus je iný a príkaz netreba. Štát, ktorý kedysi musel nútiť banky, zistil, že lacnejším nástrojom je právny režim, ktorý vytvára súkromný sledovací trh.

12.5 Infraštruktúra vo fyzickom svete

Stack sa neobmedzuje na internet. Rovnaké nákladové krivky, vďaka ktorým sa rozpoznávanie tváre vyplatilo, urobili ekonomickým každý druh snímania vo fyzickom svete.

Vzorovým prípadom je automatické rozpoznávanie evidenčných čísel vozidiel (ALPR), lebo evidenčné číslo je jediný identifikátor, ktorý musí zo zákona nosiť každý automobil, a jeho uchovávanie v práve sa zdôvodňuje ako minimálny nástroj na presadzovanie dopravných predpisov. Flock Safety, vedúci dodávateľ, prevádzkuje infraštruktúru ALPR vo viac než piatich tisícoch komunít takmer vo všetkých štátoch a zachytáva miliardy skenov vozidiel mesačne. Každý sken je obraz, odčítané číslo, miesto a časová pečiatka. Po zhromaždení za niekoľko mesiacov z nich vznikne záznam pohybu každého vozidla, ktoré prechádza pokrytými jurisdikciami. Obvodný súd v Norfolku vo Virgínii v roku 2024 rozhodol, že prístup k tomuto záznamu bez príkazu porušuje Štvrtý dodatok. O rozsudku sa bude roky súdne spierať na vyšších stupňoch a infraštruktúra medzitým skenuje ďalej.

Ten istý dodávateľ koncom roku 2024 kúpil výrobcu policajných dronov a buduje rad produktov Drone-as-First-Responder (dron ako prvý zasahujúci). Tento model, ktorý zaviedla polícia v Chula Viste v Kalifornii a dnes ho nasadzujú stovky amerických miest, vyšle dron na každý nahlásený incident skôr, než dorazí policajt. Dron počas letu nepretržite natáča a záznam sa dostáva do dôkazového systému, či už incident bol trestným činom, alebo nie. Americké platformy pre tento trh vyrábajú Skydio a BRINC. Čínsky pôvod vytlačil DJI z federálneho obstarávania. Schopnosť je voči dodávateľovi ľahostajná.

Ring, domáca kamera vo vlastníctve Amazonu, je príkladom čiastočného ústupu. Od roku 2018 do roku 2024 umožňovala aplikácia Neighbors polícii priamo žiadať majiteľov Ringu o zábery cez nástroj „Request for Assistance“ (žiadosť o pomoc). Verejný odpor voči dôsledkom pre sledovanie priviedol Amazon k tomu, že nástroj v januári 2024 odstránil. Infraštruktúra nezmizla. Polícia dnes získava zábery z Ringu cez príkazy doručené Amazonu alebo so súhlasom majiteľa, čo je starší postup s vyššími transakčnými nákladmi. Verejná pozornosť môže zvýšiť cenu sledovacieho kanála, nezatvorí ho však.

Simulátory mobilných základňových staníc, historicky známe pod značkou Stingray a dnes predávané pod rôznymi nástupníckymi názvami, uzat-

várajú fyzickú vrstvu. Simulátor sa vydáva za mobilnú vežu. Telefóny v okolí sa na ňu predvolene pripoja a vyzradia svoje medzinárodné identifikačné číslo účastníka (International Mobile Subscriber Identity). Simulátor vie zaznamenať prítomnosť a sledovať pohyb a v invazívnejších konfiguráciách vie priamo zachytávať metadáta. Výskum z rokov 2023 a 2024 zdokumentoval, že simulátory zostávajú prevádzkovo použiteľné proti sieťam 5G non-standalone aj proti niektorým konfiguráciám 5G standalone. Zmierňujúce opatrenia v štandardizačnej dráhe 3GPP existujú, nasadeniu však zaostávajú o roky, a dovtedy schopnosť pretrváva.[7]

Infraštruktúra vo fyzickom svete obracia naruby jeden z najstarších nevyslovených predpokladov o súkromí. Zvykové právo vychádzalo z toho, že človeka na verejnosti možno pozorovať, a tento predpoklad stál na cenovom strope ľudského pozorovania. Jeden policajt mohol sledovať jedného človeka. Mesto nemohlo sledovať všetkých. Kamery, čítačky a drony ten strop odstránili. Očakávanie, ktoré v zvykovom práve prežilo, nemá v novom režime žiadny ekonomický základ. Súkromie na verejnosti je dnes inžiniersky problém.

12.6 Komerčný špionážny softvér

Analytický stack predpokladá, že zariadenie cieľa je spoľahlivým zdrojom jeho údajov. Ten predpoklad padá, keď je zariadenie kompromitované. Komerčné spyware dozrelo na odvetvie s dodávateľskými stupňami, štandardnými katalógmi produktov, zverejnenými záznamami o nasadení a aktívnou súdnou praxou o zodpovednosti.

Referenčným produktom je Pegasus od firmy NSO Group. Nasadzuje sa cez zraniteľnosti bez kliknutia (zero-click exploit) v bežných komunikačných aplikáciách vrátane iMessage a WhatsAppu a cieľ nezistí, že došlo ku kompromitácii. Citizen Lab pri Torontskej univerzite zdokumentoval infekcie Pegasusom u novinárov, disidentov, právnikov a politikov najmenej v tridsiatich krajinách, vrátane prvej potvrdenej infekcie ruského novinára na území Európskej únie v roku 2023. Americké ministerstvo obchodu zaradilo NSO v novembri 2021 na zoznam Entity List, čo obmedzilo predaj amerických technológií firme, ale nezastavilo jej činnosť. Na konci roka 2024 rozhodol americký federálny súd, že NSO zodpovedá podľa zákona o počítačových podvodoch a zneužívaní (Computer Fraud and Abuse Act) za infikovanie približne 1 400 používateľov WhatsAppu. Bolo to prvé významné občianskoprávne rozhodnutie o zodpovednosti na trhu so spyware.

Intellexa, konzorcium za produktom Predator, dostala v marci 2024 sankcie amerického ministerstva financií, keď sa zistili jej zakladatelia a vystopovala sa jej schránková štruktúra. Paragon Solutions, ktorá predáva produkt Graphite, kúpila v decembri 2024 americká súkromná investičná spoločnosť AE Industrial Partners, takže vznikol dodávateľ spyware

v domácom vlastníctve. Candiru a niekoľko menších firiem pôsobí v susedných segmentoch trhu. Produkty sa líšia portfóliom zraniteľností, pokrytím cieľových platforiem a cenou, no schopnosť je zameniteľná a to, že odvetvie prežilo sankcie voči jednotlivým firmám, dokazuje, že obmedzovanie dodávateľov neobmedzuje schopnosť. Konkurenčná štruktúra opakuje vzorec Clearview: sankcionuj jedného dodávateľa a trh prevezme iný.

Paralelnú vrstvu širokého nasadenia zaberajú nástroje forenznej extrakcie. Cellebrite a Magnet Forensics (ktorá v roku 2023 kúpila Grayshift a jeho produkt GrayKey) predávajú zariadenia využívajúce slabiny reťazca zavádzania a zamknutej obrazovky na získanie údajov zo zhabaných telefónov. Zákazníkmi sú orgány činné v trestnom konaní na celom svete a je ich tisíce. Na rozdiel od Pegasusu tieto nástroje vyžadujú fyzickú držbu zariadenia, no ich cena je nastavená na bežné policajné použitie a fungujú v rozsahu obyčajných trestných vyšetrovaní. Každé ďalšie zatknutie dnes bežne prináša úplný výpis zariadenia.

GrapheneOS je verejnou výnimkou. Ide o spevnenú distribúciu Androidu pre hardvér Pixel. Po nastaviteľnej dobe nečinnosti sa automaticky reštartuje do stavu Before First Unlock (pred prvým odomknutím), za zamknutia obmedzuje periférie USB a podporuje vymazanie pod nátlakom. Uniknuté prehľady podpory od Cellebritu z roku 2024 uvádzali zariadenia s GrapheneOS ako ťažko alebo vôbec neprístupné v konfiguráciách, v ktorých sa dá preniknúť do štandardného Androidu aj iOS. Extrakcia zostáva možná pri dostatočne vyzbrojenom útoku, ale spodná hranica, ktorú si môže používateľ nastaviť, je dosť vysoká na to, aby bežná extrakcia zlyhala.

Výkonný príkaz č. 14093, ktorý podpísal prezident Biden v marci 2023 a ktorý pokračuje aj za nasledujúcich administratív, zakazuje americkej vláde operačné používanie komerčného spyware, ktoré ohrozuje kontrarozviedku alebo ľudské práva. Príkaz je vlastným priznaním štátu, že schopnosť je nebezpečná, keď ju niekto namieri na jeho úradníkov. Keď ju niekto namieri na hocikoho iného, nijaké obmedzenie ju nesprevádza. Štátni aktéri chcú spyware, keď sú cieľmi protivníci, a chcú ho obmedzovať, keď sú cieľmi oni sami.[8]

Kapitola 14 túto hranicu rozoberie v plnom rozsahu: kryptografia nevyrieši kompromitáciu koncového zariadenia, lebo kompromitované zariadenie číta otvorený text rovnako ako jeho používateľ. Analytický stack stojí na tejto hranici. Prelomenie moderného šifrovania stojí miliardy vo výpočtovom výkone alebo objav zraniteľnosti nultého dňa v implementácii. Kompromitácia koncového zariadenia stojí desaťtisíce až nízke milióny na cieľ pri vzdialenom spyware a desaťtisíce na kus pri fyzickej extrakcii a poskytne priamo otvorený text. Preteky sa presunuli do vrstvy, kde ceno-

vá štruktúra bola výhodnejšia útočníkovi, a zostali tam. Protiopatreniam sa venuje kapitola 22.

12.7 Stlačenie slučky OODA

Prvá kapitola tejto knihy predstavila Boydovu slučku pozoruj – zorientuj sa – rozhodni – konaj (OODA) ako štruktúru každého cieleného zásahu a tvrdila, že súkromie slučku preruší pri pozorovaní. Analytický stack sa oplatí skúmať ako odpoveď protivníka na toto tvrdenie, lebo stack stláča celú slučku do priemyselného procesu.[9]

Pozorovacou vrstvou je stack senzorov a získavania údajov: ALPR, kamery na zvončekoch, simulátory mobilných základňových staníc, stiahnuté obrázky z webu, prúdy polohy z aplikácií, hlásenia o bankových transakciách a komerčné spyware. Jej výstupom sú surové záznamy.

Orientačnou vrstvou je stack fúzie a analýzy: platformy triedy Palantir, dosje zostavené brokermi, služby biometrického porovnávania a veľké jazykové modely, ktoré sa dopytujú zlúčeného prostredia. Jej výstupom sú hypotézy a vzorce usporiadané podľa subjektu alebo udalosti.

Rozhodovacou vrstvou je stack správy prípadov a schvaľovania: žiadosti o príkazy, povolenia na zatknutie, výber na kontrolu, cestovné obmedzenia a administratívne sankcie. Jej výstupom sú príkazy na vynútenie namierené na jednotlivcov a zautomatizovala sa spolu s ostatnými. Hodnotenie rizika obvinených pred súdnym procesom pomocou Public Safety Assessment a COMPAS ovplyvňuje rozhodnutia o väzbe v stovkách amerických jurisdikcií. Výber daňových priznaní na kontrolu v IRS sa riadi štatistickými modelmi, ktoré určujú, ktoré priznania preverí človek. Hodnotiaci nástroj ICE na klasifikáciu rizika (Risk Classification Assessment) odporúčal v roku 2018 podľa dokumentácie väzbu v každom posudzovanom prípade, čo je spôsob zlyhania každej automatizácie rozhodovacej vrstvy, ktorú nikto empiricky nekontroluje. Austrálsky systém Robodebt vystavil automatizované oznámenia o sociálnych dlhoch stovkám tisícov poberateľov skôr, než súdy v roku 2019 zastavili jeho metodiku, a kráľovská komisia v roku 2023 uznala schému za nezákonnú a škodlivú. Vzorec je rovnaký: modely odporúčajú, ľudia podpisujú a okno na kontrolu sa so stúpajúcim výkonom zmenšuje na sekundy na prípad.[10]

Akčnou vrstvou je nasadenie vynucovania: policajné jednotky, daňové kontroly, zmrazenie majetku, zastavenie na hraniciach a regulačné zásahy. Jej výstupom je zásah do života cieľa.

Každá vrstva v tomto slede má špecializovaných dodávateľov a obchodné ceny a je optimalizovaná na priepustnosť. Stlačenie znamená, že policajt, ktorý by v roku 1990 potreboval týždne vyšetrovacej práce na zostavenie prípadu, má dnes dopytové rozhranie, ktoré mu ten istý balík vráti za minúty. Stlačenie sa týka sofistikovaných aj rutinných operácií. Prípa-

dy, ktoré sa predtým neoplatilo stíhať, sa dnes oplatí stíhať, a tým sa rozširuje skupina ľudí, ktorí prichádzajú do styku s vynucovaním.

Logika protiopatrení z toho priamo vyplýva. Ak stack slučku stláča, obrana musí zasiahnuť skôr. Len obrany na úrovni pozorovania prerušia celý reťazec, lebo zlúčená platforma nemôže zlúčiť to, čo sa nikdy nezozbieralo. Šifrovanie upiera pozorovacej vrstve obsah, zahmlievanie polohy jej upiera záznam pohybu, pseudonymita jej upiera identitu a hotovosť jej upiera transakciu. Každá z týchto obrán je dôležitejšia, čím sú lepšie nadväzujúce vrstvy, lebo práve tie sú násobiteľom, ktorý mení pozorovanie na konanie. Hodnota každého senzora, ktorý obranca odoprie, je jeho vlastná hodnota znásobená všetkými zlepšeniami v nadväzujúcich vrstvách.

Riziko nie je neistota

Rozlíšenie Franka Knighta z roku 1921 objasňuje, čo stlačená slučka dokáže a čo nie.[11] Riziko je podmienka, pri ktorej sú pravdepodobnosti výsledkov známe alebo empiricky odhadnuteľné. Pri neistote tieto pravdepodobnosti známe nie sú. Riziko vie riešiť poistenie, neistotu nevyrieši žiadny vzorec. Knightovo rozlíšenie, vypracované mimo rakúskej tradície a prevzaté neskoršími rakúskymi ekonómami vrátane Lachmanna a Shackleho, je správnym slovníkom na pomenovanie tejto hranice.

Vzorec, ktorý sa opakuje v historických údajoch, je riziko: čo sa stalo predtým, môže sa stať znova s približne rovnakou početnosťou, a zlúčená analytická platforma dokáže početnosť odhadnúť a nasmerovať zdroje na prípady s vyššou početnosťou. Nová udalosť druhu, ktorý údaje neobsahujú, je neistota: žiadna agregácia novosť nezmenší, lebo novosť je v samotnej kategórii, nie v niektorom parametri v rámci známej kategórie. Stlačená slučka OODA zlepšuje vynucovanie proti triede vzorcov, proti triede novosti ho nezlepšuje. Štátne modely hrozieb, ktoré závisia od triedy novosti, z agregácie nemajú nijaký prínos, hoci stojí veľa. Marketing obe triedy zamieňa, lebo politická klientela stacku ich nerozlišuje, kým epistemológia ich rozlišuje. Sledovacia infraštruktúra, ktorá sa platí ako odpoveď na Knightovu neistotu, sa platí ako odpoveď na problém, ktorého sa nemôže dotknúť.

12.8 Prečo úrady stále nakupujú

Mises analyzoval dynamiku byrokratického riadenia vo svojej štúdii z roku 1944.[12] Byrokratické riadenie je riadenie organizácií, ktorých výstup nemožno hodnotiť cez zisk a stratu, lebo nemá trhovú cenu. Úrad, ktorý na svojej činnosti tratí, nezmení kurz už len preto, a úrad, ktorý vyprodukuje viac spravodajských správ na jednotku rozpočtu, sa tým v ničom merateľnom nezlepšuje vo svojej funkcii. Bez testu ziskom rastie rozpočet a úspech sa určuje rastom rozpočtu.

Pri analytickom stacku tento argument pomenúva vnútornú dynamiku, ktorú samotná analýza nákladových kriviek nevysvetlí. Nákladové krivky vysvetľujú, prečo sa stack stal dostupným. Misesova analýza byrokracie vysvetľuje, prečo sa dostupná schopnosť kupuje a udržiava bez ohľadu na to, či prináša užitočný výstup. Riaditeľ, ktorý odmietne kúpiť komerčný prúd zo senzorov, ktorý kúpili porovnateľné úrady, nesie politickú cenu, ak nastane incident, ktorému sa mohlo zabrániť. Riaditeľ, ktorý prúd kúpi, nenesie zodpovedajúcu cenu za to, že prúd nedal nijakú použiteľnú informáciu, lebo vnútri úradu nič nemeria hraničný výnos z nákupu. Asymetria zvýhodňuje nákup aj udržanie a platí bez ohľadu na to, čo senzor dosiahne.

Byrokracie tiež rastú v tých smeroch, ktoré rozpočet dovoľuje. Úrad s nadbytkom rozpočtu získa schopnosť, úrad s novou schopnosťou získa personál na jej obsluhu a personál získa povýšenia a projekty, na ktoré treba, aby schopnosť zostala. Systém sa uzamkne na novej úrovni a ďalší rozpočtový cyklus začína od základne, ktorá už novú úroveň zahŕňa. Ekonomika stacku dala každému úradu s rozpočtovou právomocou dôvod nakupovať. Misesovská analýza vysvetľuje, prečo sa nákupy hromadia namiesto toho, aby sa orezávali.

12.9 Prečo stack existuje práve teraz

Stack nie je nový druhom. Pinkertonova agentúra zostavovala v devätnástom storočí sledovanie pre priemyselných aj štátnych klientov.[15] Stasi viedla spisy o tretine dospelých Východonemcov s technikou zo sedemdesiatych rokov.[16] Nová je cena na subjekt a celková dosiahnuteľná populácia a obe sa zmenili z dôvodov, ktoré vieme pomenovať.

Najprv sa zlomili náklady na senzory. Digitálne snímanie nahradilo film, bežný kremík nahradil hardvér na jeden účel, cloudové úložisko nahradilo lokálne a všadeprítomná bezdrôtová sieť nahradila nasadenie len na kábloch. Cena zachytenia jedného pozorovania klesla za štyridsať rokov približne o šesť rádov. Potom sa zlomili náklady na ukladanie. Dátové sklady a objektové úložisko spolu s Moorovým zákonom o hustote znížili cenu trvalého uchovávania jedného záznamu z ekonomicky neúnosnej na ekonomicky nepodstatnú. Naposledy sa zlomili náklady na analýzu. Ľudských analytikov nahradili systémy založené na pravidlách a tie nahradili veľké jazykové modely, pričom cena vyvodenia záveru z jedného záznamu klesla medzi rokmi 2010 a 2025 približne o tri rády.

Keď sa zrúti viac než jedna nákladová krivka naraz, schopnosť, ktorá bola dostupná len pre výnimočné prípady, sa stane dostupnou pre rutinné. Stack sa zostavil sám cez obyčajný konkurenčný tlak: každý úrad, ktorý ho odmietol, podával horšie výkony než úrady, ktoré ho prijali, a tie, čo zaostali, ho buď prijali, alebo prišli o rozpočet a právomoci v prospech tých, čo tak urobili. Rovnováha vznikla z miestnych rozhodnutí pod rov-

nakým tlakom stimulov, čo je znakom trhového poriadku, ktorý pôsobí proti používateľovi.

Pre obranu súkromia z toho ekonomicky vyplýva, že aj nákladová krivka obrancu sa musí ohnúť. Je to možné a deje sa to, no po väčšinu poslednej dekády sa to dialo pomalšie než rast útočníkovho stacku. Tor, Signal, Bitcoin a Nostr sú body na krivke obrancu, ktoré sa ohli najrýchlejšie.[17] Každý je štrukturálna inovácia, ktorá znižuje náklady obrancu o rády pri konkrétnom druhu pozorovania. Tempo týchto inovácií rozhoduje o tom, či analytický stack bude koniec príbehu, alebo len medzifáza predtým, než obrana dobehne.

Zhrnutie kapitoly

Analytický stack je integrovaný systém, v ktorom komerčné firmy zostavujú sledovacie schopnosti a štátne úrady ich nasadzujú. Skladá sa zo štyroch vrstiev: získavanie údajov senzormi, fúzia a analýza, rozhodovanie a schvaľovanie, vynucovanie. V každej vrstve sú špecializovaní dodávatelia, ktorí si konkurujú cenou. Sledovanie sa zindustrializovalo trhovou špecializáciou: schopnosť, ktorú by žiadny jednotlivý úrad zákonne nezostavil, zostavia firmy a predajú ju ako službu a štát platí trhovú cenu za schopnosti, ktoré by priamo získať nemohol. Komerčný kanál obchádza ústavné ochrany navrhnuté proti priamemu získavaniu údajov štátom. Štvrtý dodatok vznikol proti vynúteným záznamom. *Carpenter* úzko obmedzil získavanie údajov o polohe mobilných vysielačov bez príkazu, no bez toho, aby sa zaoberal širším komerčným trhom s rovnocennými informáciami, a v tejto medzere pôsobí odvetvie dátových brokerov.

Načasovanie vysvetľujú nákladové krivky. Cena senzorov, ukladania aj analýzy sa zrútila v prekrývajúcich sa fázach, a keď sa zlomili súčasne, stack sa stal ekonomicky povinným pre každý úrad, ktorého konkurenti ho prijali. Výsledkom je stlačenie Boydovej slučky OODA do priemyselného procesu: každá etapa od surového záznamu po vynútenie sa zefektívnila naraz. Obrana preto musí pôsobiť na vrstve pozorovania, lebo všetky nadväzujúce vrstvy sú optimalizované na priepustnosť. Šifrovanie, anonymné smerovanie, zahmlievanie polohy, pseudonymita aj hotovosť odopierajú stacku vždy jeden konkrétny druh pozorovania a okrajový zisk obrancu z ktorejkoľvek z nich násobí efektivita nadväzujúcich vrstiev.

Stack nie je nepremožiteľný. Aj nákladové krivky obrancu sa môžu ohýbať nadol a štrukturálne inovácie, ktoré rozvíja zvyšok knihy, teda silné šifrovanie, anonymné smerovanie, odolné peniaze a decentralizovaná sociálna infraštruktúra, majú za sebou doklady, že pri konkrétnych druhoch pozorovania zrušili útočníkovu nákladovú výhodu. Súčasti stacku sa líšia aj dosahom a cenou: čítačka evidenčných čísel vytvára záznam pohybu, zatiaľ čo komerčné spyware spôsobí úplnú kompromitáciu zariadenia, a kapitola 22 modeluje hrozby proti každej vrstve osobitne. Právna refor-

ma má svoje miesto, ale nie hlavné, lebo regulačný tlak na ktorúkoľvek jednu súčasť presunie schopnosť na susednú. Individuálne konanie nie je márne: stack je na úrovni celku ekonomicky povinný a na úrovni jednotlivca štrukturálne krehký a cieľ, ktorý odopiera pozorovanie v každej vrstve, je cieľ, ktorý nadväzujúci stroj nedokáže spracovať. Preteky sa presunuli z vrstvy jednotlivej komunikácie vyššie, do vrstvy agregácie, a zvyšok knihy pracuje vo výške, ktorú dnes zaujíma protivník.

Poznámky

[1] Kniha Byrona Taua z roku 2024 je súčasnou novinárskou mapou trhu so sledovaním od komerčných firiem k štátu, o prebiehajúcom spravodajstve sa starajú EFF Atlas of Surveillance a 404 Media. Byron Tau, *Means of Control: How the Hidden Alliance of Tech and Government is Creating a New American Surveillance State* (Crown, 2024). Electronic Frontier Foundation, *Atlas of Surveillance*, `https://atlasofsurveillance.org/`, sleduje konkrétne nasadenia podľa jurisdikcie. 404 Media, `https://www.404media.co/`, publikuje priebežné investigatívne spravodajstvo o tomto odvetví.

[2] Rozhodnutie *Carpenter* vyžaduje príkaz pre záznamy operátora získané nátlakom, ale neerieši komerčný nákup. Legislatívne pokusy uzavrieť túto medzeru zákonom „Fourth Amendment Is Not for Sale Act" neprešli. *Carpenter v. United States*, 585 U.S. 296 (2018). Odborné spracovanie: Orin S. Kerr, „The Case for the Third-Party Doctrine," *Michigan Law Review* 107 (2009): 561–601, a Paul Ohm, „The Fourth Amendment in a World Without Privacy," *Mississippi Law Journal* 81, č. 5 (2012): 1309–1355. Legislatívna reakcia v zákone „Fourth Amendment Is Not for Sale Act", sledovanom v niekoľkých funkčných obdobiach Kongresu na `https://www.congress.gov/`.

[3] Murray N. Rothbard, *Anatomy of the State* (Auburn, AL: Ludwig von Mises Institute, 2009; prvé vydanie 1974 v *Egalitarianism as a Revolt Against Nature and Other Essays*), v ktorom Rothbard obnovuje rozlíšenie Johna C. Calhouna medzi čistými platiteľmi daní a čistými príjemcami daní. Moderné vyjadrenie: každá štátna činnosť vytvára triedu, ktorá dostáva od štátu viac, než prispieva, a triedu, ktorá prispieva viac, než dostáva, a vládnucou triedou v Rothbardovom zmysle je koalícia tých prvých. Pozri tiež *Power and Market: Government and the Economy*, 4. vyd. (Auburn, AL: Ludwig von Mises Institute, 2006), kde sa tá istá analýza uplatňuje na konkrétne druhy intervencií, a John C. Calhoun, *A Disquisition on Government* (1851), pôvodné rozlíšenie, ktoré Rothbard rozšíril. Triedna analýza je tu štrukturálne odlišná od marxistickej, lebo hranica medzi triedami je daná štátnym privilégiom, nie vlastníctvom výrobných prostriedkov.

[4] Clearview AI vybudovala vzorový korpus na rozpoznávanie tváre z otvoreného webu (~dvadsať miliárd obrázkov), HART je paralelný federálny biometrický index a TSA a CBP nasadzujú porovnávanie tvári na fyzických kontrolných bodoch. Clearview AI, `https://www.clearview.ai/`. Kashmir Hill, *Your Face Belongs to Us: A Secretive Startup's Quest to End Privacy as We Know It* (Random House, 2023), je smerodajný novinársky opis. U.S. Department of Homeland Security, Office of Biometric Identity Management (HART), `https://www.dhs.gov/obim`. Porovnávanie tvári TSA na `https://www.tsa.gov/digital-id`. Biometrický systém vstupu a výstupu CBP na `https://www.cbp.gov/travel/biometrics`.

[5] Artificial Intelligence Platform firmy Palantir je komerčne viditeľným príkladom spravodajskej analýzy s pomocou veľkých jazykových modelov v štátnom meradle, Gotham a Foundry sú zlúčené dátové prostredia, nad ktorými beží. Palantir Artificial Intelligence Platform, `https://www.palantir.com/platforms/aip/`; Gotham, `https://www.palantir.com/platforms/gotham/`; Foundry,

https://www.palantir.com/platforms/foundry/. Hodnoty federálnych zákaziek sa dajú vyhľadať na https://www.usaspending.gov/. Kritické spravodajstvo: Caroline Haskins v *Business Insider* a Sam Biddle v *The Intercept* (https://theintercept.com/).

[6] Venntel a jeho nástupcovia (Locate X pod Babel Street) a Fog Data Science predávajú údaje o polohe z prúdu reklamných aukcií v reálnom čase federálnym, štátnym a miestnym úradom. Audit TIGTA z roku 2023 potvrdil, že IRS Criminal Investigation používala údaje z Venntelu bez príkazu. Venntel (dcéra Gravy Analytics), https://venntel.com/. Babel Street / Locate X, https://www.babelstreet.com/. Fog Data Science / Fog Reveal, https://fogdatascience.com/. Treasury Inspector General for Tax Administration, „The Criminal Investigation Division's Use of Commercial Databases Containing Personal Information Complied with Policy but Raised Privacy Concerns," Report No. 2023-IE-R003 (2023), https://www.tigta.gov/. Spravodajstvo Electronic Frontier Foundation o kanáli brokerov a o Fog Reveal na https://www.eff.org/issues/street-level-surveillance/fog-data-science.

[7] Flock Safety ovláda ALPR, Skydio, BRINC a DJI dodávajú trh policajných dronov, Amazon Ring tvorí vrstvu kamier na zvončekoch a simulátory mobilných základňových staníc uzatvárajú úroveň fyzických senzorov. Flock Safety, https://www.flocksafety.com/. Skydio, https://www.skydio.com/. BRINC, https://www.brinc.com/. DJI, https://www.dji.com/. Amazon Ring, https://ring.com/, a aplikácia Neighbors, https://shop.ring.com/pages/neighbors-app. Program Drone-as-First-Responder polície v Chula Viste, https://www.chulavistapd.org/police-services/drones-as-1st-responders. *Crowder v. Diamondback Investment Group, LLC*, Circuit Court of the City of Norfolk, Case No. CL24-000194 (2024), o prístupe k ALPR bez príkazu. O simulátoroch mobilných základňových staníc a 5G pozri priebežnú analýzu Citizen Lab na https://citizenlab.ca/.

[8] Pegasus (NSO), Predator (Intellexa), Graphite (Paragon) a produkty firmy Candiru tvoria trh so vzdialenou kompromitáciou, Cellebrite a Magnet Forensics (GrayKey) ovládajú trh fyzickej extrakcie, GrapheneOS je verejná obranná výnimka a výkonný príkaz č. 14093 obmedzuje operačné používanie americkou vládou, ale nie odvetvie. Citizen Lab, https://citizenlab.ca/, je hlavný empirický zdroj o nasadzovaní spyware. NSO Group, https://www.nsogroup.com/. *WhatsApp LLC v. NSO Group*, Case No. 4:19-cv-07123 (N.D. Cal. 2024). Intellexa / Predator: sankčné zaradenie amerického ministerstva financií (OFAC) z 5. marca 2024, https://ofac.treasury.gov/recent-actions/20240305. Paragon Solutions / Graphite (kúpila AE Industrial Partners, december 2024): verejné spravodajstvo v *TechCrunch* a *Haaretz*. Candiru: bez verejnej webovej stránky, zdokumentované správami Citizen Lab a Microsoft Threat Intelligence Center. Cellebrite, https://cellebrite.com/. Magnet Forensics, https://www.magnetforensics.com/. GrapheneOS, https://grapheneos.org/, dokumentácia funkcií na https://grapheneos.org/features. Executive Order 14093, „Prohibition on Use by the United States Government of Commercial Spyware That Poses Risks to National Security," 88 Fed. Reg. 18957 (March 27, 2023), https://www.federalregister.gov/documents/2023/03/30/2023-06730/prohibition-on-use-by-the-united-states-government-of-commercial-spyware-that-poses-risks-to.

[9] Boydova slučka OODA je štrukturálny rámec, ktorý kapitola používa na ukázanie, ako sa sledovanie integruje naprieč vrstvami. Primárnu citáciu Boydovho briefingu „Patterns of Conflict" pozri v kapitole 1, poznámka 4. Frans P. B. Osinga, *Science, Strategy and War: The Strategic Theory of John Boyd* (Routledge, 2006), je štandardné akademické

spracovanie. Grant T. Hammond, *The Mind of War: John Boyd and American Security* (Smithsonian, 2001), je biografické spracovanie.

[10] Rozhodovacia vrstva sa zautomatizovala spolu so senzorovou a orientačnou vrstvou. PSA a COMPAS riadia rozhodnutia o väzbe, Risk Classification Assessment úradu ICE odporúčalo väzbu takmer v každom prípade a austrálsky Robodebt vygeneroval stovky tisíc nezákonných automatizovaných oznámení o dlhu, kým ho kráľovská komisia v roku 2023 nezastavila. Public Safety Assessment (Arnold Ventures), `https://advancingpretrial.org/psa/about-the-psa/`. COMPAS / Equivant, `https://www.equivant.com/`. Kritická analýza hodnotenia rizika COMPAS: Julia Angwin, Jeff Larson, Surya Mattu, and Lauren Kirchner, „Machine Bias," *ProPublica* (May 23, 2016), `https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing`. K automatizovanému výberu priznaní na kontrolu v IRS pozri Internal Revenue Service, *Inflation Reduction Act Strategic Operating Plan* (2023), `https://www.irs.gov/pub/irs-pdf/p3744.pdf`. Risk Classification Assessment úradu ICE Enforcement and Removal Operations: Reade Levinson, Mica Rosenberg, and Kristina Cooke, „Special Report: How Trump Administration Altered ICE's Detention Tool," *Reuters* (June 26, 2018), `https://www.reuters.com/investigates/special-report/usa-immigration-detention/`. Robodebt: Commonwealth of Australia, *Report of the Royal Commission into the Robodebt Scheme* (July 2023), `https://web.archive.org/web/20230901000000/https://robodebt.royalcommission.gov.au/publications/report`.

[11] Frank H. Knight, *Risk, Uncertainty, and Profit* (Boston: Houghton Mifflin, 1921), najmä časť III. Knight je zakladateľ chicagskej školy, nie rakúsky ekonóm, a rozlíšenie, o ktoré sa argument knihy opiera, je Knightovo, nie Misesovo. Mises ponúka paralelné rozlíšenie medzi pravdepodobnosťou triedy a pravdepodobnosťou prípadu v *Human Action* (citované v kapitole 3, poznámka 1), kapitola 6 („Uncertainty"). K recepcii Knightovej neistoty v rakúskej škole pozri Ludwig M. Lachmann, *Capital, Expectations, and the Market Process* (Kansas City: Sheed Andrews and McMeel, 1977), a G. L. S. Shackle, *Epistemics and Economics* (Cambridge University Press, 1972).

[12] Ludwig von Mises, *Bureaucracy* (New Haven: Yale University Press, 1944; dotlač Indianapolis: Liberty Fund, 2007), najmä kapitoly „Profit Management" a „Bureaucratic Management". Misesov argument: byrokracie existujú tam, kde sa pre dané výstupy nemôžu vytvoriť trhové ceny, byrokratický personál preto nepodlieha disciplíne, ktorú ukladá účtovníctvo zisku a straty, a inštitucionálna forma má vnútorné expanzívne tlaky, ktoré nijaká administratívna reforma nezneškodní. William A. Niskanen, *Bureaucracy and Representative Government* (Chicago: Aldine-Atherton, 1971), rozvíja doplnkovú analýzu verejnej voľby z hľadiska mimo rakúskej školy.

[13] Adam Smith, *An Inquiry into the Nature and Causes of the Wealth of Nations* (London: W. Strahan and T. Cadell, 1776), kniha I, kapitoly 1–3, o deľbe práce, jej účinkoch na produktivitu a jej závislosti od veľkosti trhu. Kanonické moderné vydanie je Adam Smith, *The Wealth of Nations*, ed. R. H. Campbell, A. S. Skinner, and W. B. Todd, Glasgow Edition of the Works and Correspondence of Adam Smith, vols. 1–2 (Oxford: Oxford University Press, 1976; dotlač Indianapolis: Liberty Fund, 1981).

[14] Ludwig von Mises, *Human Action: A Treatise on Economics*, 4. vyd. (Irvington-on-Hudson, NY: Foundation for Economic Education, 1996; pôvodne vydané 1949), kapitola 8 („Human Society"), najmä oddiel 3 („The Division of Labor") a oddiel 5 („The Catallactic Problem of the Division of Labor"). Mises tvrdí, že deľba práce je tvorená trhovým poriadkom výmeny (ktorý nazýva katalaktickým poriadkom) a že je s ním totožná, a že zisky z produktivity, ktoré identifikoval Smith, sú samy výsledkom dobrovoľnej spolupráce v cenovom systéme. Argument o sledovacom stacku preberá tento rámec: špecializácia v pozorovaní je možná a ekonomicky racionálna, lebo trhové ceny koordinujú každú vrstvu.

[15] Pinkerton National Detective Agency, ktorú založil Allan Pinkerton v roku 1850, pôsobila počas celého devätnásteho storočia ako súkromná spravodajská a vynucovacia služba pre železnice, priemyselných zamestnávateľov a federálne úrady, vrátane potláčania štrajkov a infiltrácie odborových organizácií. Jej klientela ukazuje, že trh so sledovaním medzi komerčnou sférou a štátom je o viac než sto rokov starší než digitálna technológia. Frank Morn, *The Eye That Never Sleeps: A History of the Pinkerton National Detective Agency* (Bloomington: Indiana University Press, 1982), je štandardná história. Pozri tiež Robert P. Weiss, „Private Detective Agencies and Labour Discipline in the United States, 1855–1946," *Historical Journal* 29, č. 1 (1986): 87–107.

[16] Východonemecké ministerstvo štátnej bezpečnosti (Stasi) viedlo spisy o odhadovaných 5,6 milióna osôb (zhruba tretina dospelého obyvateľstva NDR) s približne 91 000 stálymi zamestnancami a 170 000 až 190 000 neformálnymi spolupracovníkmi na vrchole v osemdesiatych rokoch. Porovnanie s digitálnym analytickým stackom obracia nákladovú štruktúru: Stasi dosiahla vysoké pokrytie len obrovskými výdavkami ľudskej práce, zatiaľ čo komerčný stack dosahuje porovnateľné alebo väčšie pokrytie za takmer nulové hraničné náklady na subjekt. Gary Bruce, *The Firm: The Inside Story of the Stasi* (Oxford: Oxford University Press, 2010). Jens Gieseke, *The History of the Stasi: East Germany's Secret Police, 1945–1990*, prel. David Burnett (New York: Berghahn Books, 2014). Archívy úradu Stasi Records Agency (BStU) spravuje Federal Commissioner for the Records of the State Security Service of the Former German Democratic Republic, `https://www.bstu.de/`.

[17] Tor poskytuje anonymné smerovanie s nízkou latenciou cez cibuľové šifrovanie v sieti dobrovoľníckych uzlov, Signal poskytuje end-to-end šifrované správy na báze protokolu Signal, Bitcoin poskytuje pseudonymný platobný systém odolný voči finančnému sledovaniu na úrovni transakcií a Nostr je protokol na sociálny graf a posielanie správ, odolný voči cenzúre a postavený na kryptografii s verejným kľúčom. Každý z nich ruší nákladovú výhodu útočníka pri konkrétnom druhu pozorovania. Tor Project, `https://www.torproject.org/`; Roger Dingledine, Nick Mathewson, and Paul Syverson, „Tor: The Second-Generation Onion Router," *Proceedings of the 13th USENIX Security Symposium* (2004), `https://svn.torproject.org/svn/projects/design-paper/tor-design.pdf`. Špecifikácia protokolu Signal: Trevor Perrin and Moxie Marlinspike, „The Double Ratchet Algorithm" (2016), `https://signal.org/docs/specifications/doubleratchet/`; Signal Foundation, `https://signal.org/`. Bitcoin: Satoshi Nakamoto, „Bitcoin: A Peer-to-Peer Electronic Cash System" (2008), `https://bitcoin.org/bitcoin.pdf`. Špecifikácia protokolu Nostr, `https://github.com/nostr-protocol/nostr`.

13
KRYPTOVOJNY

„Ak sa súkromie postaví mimo zákon, súkromie budú mať len tí, čo stoja mimo zákona."

Phil Zimmermann, „Prečo som napísal PGP" (1991)[1]

Úvod

Kryptovojny sú trvalý konflikt medzi štátmi, ktoré chcú mať schopnosť sledovať, a jednotlivcami, ktorí vyvíjajú technológie na ochranu súkromia. Začal sa v chvíli, keď sa silná kryptografia dostala z utajeného vojenského výskumu k civilistom. Štáty, ktoré mali monopol na najúčinnejšiu praktickú kryptografiu, zrazu stáli pred občanmi s podobnou obrannou schopnosťou. Reakcia sa dala čakať: pokusy ovládnuť kryptografické technológie a tlačiť systémy k zadným vrátkam.[22]

Najväčšie pokusy o celkovú kontrolu sa vo veľkej miere nepodarili, a dôvody vysvetľuje ekonomická analýza. Neúspech však nebol úplný a konflikt pokračuje.

13.1 História: od exportných kontrol po čip Clipper

Kryptografia ako vojenský materiál

Až do konca roka 1996 sa mnohé americké exporty softvéru so silnou kryptografiou radili medzi vojenský materiál podľa amerických predpisov o medzinárodnom obchode so zbraňami (International Traffic in Arms Regulations, ITAR).[2] Koncom roka 1996 prešla väčšina komerčných šifrovacích produktov pod kontrolu ministerstva obchodu a v nasledujúcich rokoch sa pravidlá ďalej uvoľňovali. Kto prenášal softvér so silnou kryp-

tografiou cez hranice, riskoval exportné tresty také prísne, že odrádzali výskumníkov aj vývojárov.

Zaradenie vychádzalo z predstáv studenej vojny: kryptografia je vojenská technológia a kryptografická prevaha nad protivníkmi ospravedlňuje obmedzovanie prístupu civilistov. Že civilisti môžu mať oprávnené potreby súkromia aj nezávisle od vojenských záujmov, regulačný rámec vôbec nebral do úvahy.

Absurdnosť sa ukázala, keď sa výpočtová technika rozšírila. Matematické vzorce dostupné v univerzitných knižniciach mohli spôsobiť exportné problémy, len čo sa šírili ako softvér. Regulátori pripisovali právny význam formátu publikácie a spôsobu distribúcie, čo súdy neskôr označili za ústavne pochybné: tlačená publikácia a akademická diskusia požívali v praxi silnejšiu ochranu, zatiaľ čo zverejnenie zdrojového kódu online mohlo vyvolať konflikt s exportnými pravidlami.

Phil Zimmermann a PGP

Konflikt vykryštalizoval okolo programu Pretty Good Privacy (PGP) Phila Zimmermanna.[3] V roku 1991 Zimmermann vydal PGP ako slobodný softvér, ktorý dával obyčajným používateľom silnú kryptografiu s verejným kľúčom. PGP sa rýchlo šírilo cez raný internet a čoskoro ho používali aj ľudia mimo Spojených štátov.

Federálna vláda začala trestné vyšetrovanie. Tri roky hrozilo Zimmermannovi stíhanie za porušenie exportných pravidiel. Prípad sa stal známou kauzou (cause célèbre) vznikajúcej internetovej komunity. Zimmermann odpovedal v cypherpunkovom duchu: zdrojový kód PGP vydal ako tlačenú knihu, teda vo formáte, ktorý mal v praxi silnejšiu ochranu slobody prejavu než exportne regulované softvérové súbory.[4]

Prípad sa skončil bez obvinenia, ale určil vzor, podľa ktorého prebiehali neskoršie kryptovojny: vláda si nárokuje právomoc kontrolovať, technológovia obchádzajú obmedzenia, obmedzenia sa ukážu ako nevynútiteľné a formálna politika dobehne technickú realitu.

Čip Clipper

V roku 1993 oznámila Clintonova administratíva iniciatívu čip Clipper (Clipper Chip): kryptografický čipset navrhnutý NSA s povinnou úschovou kľúčov u štátu (key escrow).[5] Používatelia by mali šifrovanie, ale vládne úrady by držali duplikáty kľúčov, aby mohli komunikáciu dešifrovať, keď to zákon dovolí.

Návrh spájal šifrovanie so sledovaním. Zástancovia tvrdili, že to vyvažuje súkromie a potreby orgánov činných v trestnom konaní. Odporcovia poukázali na zásadné problémy.

Uschované kľúče vytvárajú jediný bod zlyhania: ak by sa databáza s kľúčmi kompromitovala, odhalila by sa naraz všetka chránená komunikácia.

Schéma tiež vyžadovala dôveru, že vládne úrady siahnu po kľúčoch len vtedy, keď to zákon dovolí, a po odhaleniach o sledovaní bez súdneho príkazu si takú dôveru nikto nezaslúžil. Výskumník Matt Blaze objavil v protokole Clippera chybu, vďaka ktorej mohli používatelia vypnúť úschovu kľúčov a šifrovanie si pritom ponechať.[6] Systém, ktorý mal zaručiť prístup štátu, sa dal obísť spôsobom, ktorý podkopával jeho hlavný sľub. Napokon si technologické firmy uvedomili, že produkty so zadnými vrátkami pre vládu stratia zahraničné trhy, lebo zákazníci, ktorým ide o skutočné súkromie, si vyberú produkty bez povinných zraniteľností.

Od Clippera sa prakticky upustilo, lebo ho trh odmietol a komerčne sa nedal udržať. Epizóda ukázala, že povinné zadné vrátka narážajú na technické aj ekonomické prekážky.

Koniec bojov z deväťdesiatych rokov

Koncom deväťdesiatych rokov prvé kryptovojny utíchali. Súdne spory a komerčný tlak sa spojili s praktickou nevynútiteľnosťou a posunuli politiku k liberalizácii. V roku 1996 výkonný príkaz č. 13026 začal presúvať kontrolu šifrovania z ministerstva zahraničia na ministerstvo obchodu. Spor *Bernstein* pomohol presadiť, že zdrojový kód je chránený prejav, a regulačný rámec ďalej oslabil.[7]

Exportné kontroly sa výrazne uvoľnili, hoci nezmizli. Silnú kryptografiu bolo odvtedy legálne šíriť a nasadzovať. Vďaka tomu vznikla infraštruktúra šifrovanej komunikácie, ktorú dnes berieme ako samozrejmosť.

13.2 Ekonomická logika kontroly nad kryptografiou

Prečo štáty chcú kontrolu

Štáty chcú kontrolovať kryptografiu, lebo šifrovanie ohrozuje ich schopnosť sledovať. Dôvody súvisia so základnými funkciami štátu.

Štáty získavajú zdroje zdaňovaním a úplné sledovanie financií umožňuje vymáhať dane. Šifrované finančné transakcie, ktoré úrady nevidia, vymáhanie podkopávajú. Ako ukázala kapitola 10, peňažné systémy štátu umožňujú kontrolu, kým šifrované platobné systémy túto kontrolu obchádzajú, lebo dovoľujú transakcie mimo monitorovaných kanálov. Štáty sledujú obyvateľstvo z rôznych dôvodov: odhaľujú nesúhlas, mapujú pohyb ľudí, zisťujú, aké sú medzi nimi sociálne väzby. Šifrovanie vytvára priestory, ktoré takéto sledovanie nevidí. Vyšetrovanie trestných činov si často vyžaduje prístup ku komunikácii a záznamom a šifrovanie môže prístup zablokovať, aj keď má úrad zákonné oprávnenie.

Z pohľadu štátu je šifrovanie problém schopností. Občania so silným šifrovaním môžu konať bez toho, aby ich štát videl. To obmedzuje štátne konanie, bez ohľadu na to, či ide o oprávnené presadzovanie práva, alebo o nelegitímnu represiu.

Informačná asymetria a štátna moc

Štátu vyhovuje informačná asymetria: o občanoch vie viac než občania o štáte. Táto asymetria umožňuje selektívne vynucovanie pravidiel. Odrádza ľudí od určitého správania a umožňuje zasiahnuť vopred. Keď úrady vidia všetky porušenia, ale stíhať môžu len niektoré, vynucovanie sa stáva vecou uváženia; každý je vinný z niečoho a stíhanie závisí od priazne úradov. Vedomie, že niekto sleduje, mení správanie: občania, ktorí vedia, že ich sledujú, upravia konanie tak, aby neupútali pozornosť, aj keď je zákonné. Včasné odhalenie organizovania alebo odporu umožňuje zasiahnuť skôr, než hnutia nabudnú silu.

Šifrovanie informačnú asymetriu zmenšuje. Štáty vidia menej a občania sa môžu koordinovať bez toho, aby ich niekto videl. Moc, ktorú asymetria poskytuje, slabne.

Ekonomické záujmy

Ekonomicky je v hre veľa na všetkých stranách. Pre štáty je sledovacia infraštruktúra obrovská investícia; celé úrady si vybudovali schopnosti postavené na prístupe a šifrovanie ohrozuje návratnosť tejto investície. Občanom súkromie umožňuje ekonomickú činnosť, ktorú by sledovanie znemožnilo; podzemné hospodárstvo, regulačná arbitráž, ochrana konkurenčných informácií aj obyčajná túžba nebyť pozorovaný majú hodnotu pre tých, ktorí o ne stoja. Podniky sú v napätí z oboch strán: vlády požadujú prístup, zákazníci súkromie a obchodná hodnota služieb pre zákazníkov, ktorým ide o súkromie, je v rozpore s požiadavkami regulácie.

Demokracia a račňa sledovania

Analýza demokratického a monarchického usporiadania, ktorú Hans-Hermann Hoppe vydal v roku 2001, pomenúva črtu demokratickej vlády, ktorá súvisí s dejinami sledovacej legislatívy.[8] Demokratickí vládcovia sú dočasní správcovia aparátu, nie majitelia jeho dlhodobej kapitálovej hodnoty. Tento štrukturálny rozdiel plodí vyššiu časovú preferenciu v demokratickom rozhodovaní než v dedičnom monarchickom.

Demokratická legislatíva o sledovaní dôsledne vymieňala súčasnú politickú istotu za budúce náklady na občianske slobody. Zákon USA PATRIOT Act prešiel Snemovňou reprezentantov v októbri 2001 so 357 hlasmi za, štyridsaťpäť dní po 11. septembri.[9] Každé rozšírenie právomocí na finančné sledovanie podľa nástupníckych zákonov k Zákonu o bankovom tajomstve (Bank Secrecy Act) prešlo drvivou väčšinou oboch strán, v prostredí, kde bola okamžitá politická cena za odpor viditeľná a dlhodobá cena za podporu rozptýlená. Rovnaký vzorec sledujú v Európe boje o Chat Control (plošné skenovanie súkromných správ), britský zákon o bezpečnosti online (Online Safety Act) a eIDAS 2.0. Odporcov podporujú špe-

cialisti, ktorým záleží na architektúre, a prijatie návrhu zasa podporuje každý, kto ho vie predstaviť ako odpoveď na konkrétnu aktuálnu obavu.

Podľa hoppeovského čítania demokratickí vládcovia budúce náklady na občianske slobody diskontujú, lebo ich už nebudú znášať vo funkcii. Cynickejšie čítanie hovorí, že ich nediskontujú vôbec, lebo čakajú, že náklady dopadnú na opozičné skupiny, do ktorých nebudú patriť. Obe čítania dávajú rovnaký vzorec a práve s týmto vzorcom sa zaoberá argument tejto knihy o asymetrii nákladov.

13.3 Prečo kontrola zlyháva (a kde nie)

Štrukturálne prekážky

Kryptografická bezpečnosť stojí na matematických vlastnostiach, ktoré právny zákaz nezmení. Ak je problém výpočtovo náročný, zostane náročný bez ohľadu na to, čo vyhlásia zákonodarcovia. Žiadny zákon nezjednoduší rozklad veľkých čísel na prvočinitele a žiadna politika neobráti vzťahy, na ktorých schémy fungujú. Kryptografické poznatky sa dajú objaviť nezávisle, takže ich potlačenie v jednej jurisdikcii nezabráni objavu inde; matematické vzťahy existujú, či ich niekto pozná, alebo nie. Zverejnený matematický poznatok sa nedá vziať späť; články, učebnice a internetové archívy uchovávajú kryptografické techniky trvalo a po celom svete. A keď sú algoritmy zverejnené, schopní programátori ich vedia implementovať priamo, takže potláčať implementácie znamená napokon potláčať samotné programovanie.

Problém zhoršujú takmer nulové hraničné náklady na informáciu. Kryptografický algoritmus, keď ho niekto objaví a zverejní, sa dá kopírovať donekonečna za zanedbateľné náklady. Jedna uniknutá kópia sa mení na neobmedzený počet kópií a šifrovací softvér sa šíri rýchlejšie, než ho stačí vynucovanie sledovať. Internet umožňuje celosvetovú distribúciu rýchlejšie, než dokáže odpovedať akýkoľvek národný vynucovací mechanizmus, a softvér zverejnený v jednej jurisdikcii je dostupný po celom svete do pár minút.

Aj keby sme nechali bokom, že poznatky sú rozptýlené, účinná kontrola by vyžadovala koordináciu štátov s rozdielnymi záujmami. Nie všetky štáty chcú šifrovanie obmedzovať; niektoré majú ekonomický prospech z toho, že sú útočiskom pre vývoj technológií na ochranu súkromia. Každý štát ovláda len vlastné územie, takže povinné zadné vrátka v jednej krajine sa nedotknú softvéru vyvíjaného inde. Aj koordinované medzinárodné dohody majú medzery vo vynucovaní a odhodlaní aktéri nájdu jurisdikcie, ktoré sa nezúčastňujú ani nevynucujú.

Kde kontrola uspieva

Napriek týmto prekážkam nie je kontrola nad kryptografiou celkom neúčinná. Uspieva nie proti matematike, ale okolo nej. Kryptografiu je ťažké implementovať správne a väčšina používateľov nevie posúdiť, či je daná implementácia bezpečná; kompromitované implementácie sa tak môžu šíriť pod neškodne znejúcimi názvami. Bezpečné systémy často obetujú použiteľnosť, takže keď je šifrovanie ťažké používať, ľudia ho používajú menej alebo nesprávne a v praxi tým oslabujú bezpečnosť, ktorá je v teórii v poriadku. Väčšina používateľov prijme predvolené nastavenia, a keď sa systém dodáva so slabým alebo žiadnym predvoleným šifrovaním, väčšina ľudí zostane bez ochrany, nech formálne existujú akokoľvek silné možnosti. Firmy pôsobiace v nejakej jurisdikcii musia dodržiavať miestne právo, inak im hrozí postih; veľké platformy často zavádzajú sledovacie schopnosti preto, že to vyžaduje súlad s reguláciou, nie preto, že by ich inžinieri preferovali nebezpečné riešenia. A šifrovanie chráni údaje, nie ľudí: fyzický nátlak môže vynútiť vydanie kľúča bez ohľadu na silu kryptografie a „útok kľúčom za päť dolárov“ (wrench attack) zostáva účinný proti neopatrnej obeti.

Kontrola teda zlyháva proti vyspelým a odhodlaným aktérom, ktorí pracujú s dobrými nástrojmi a dobrými postupmi. Často uspieva proti bežným používateľom, ktorým chýba odbornosť alebo motivácia zaviesť silnú ochranu súkromia. Výsledná dvojúrovňová situácia, v ktorej súkromie majú tí, čo ho uprednostňujú, a ostatní nie, je rovnováha, ktorú zvyšok knihy považuje za danú.

13.4 Súťaž jurisdikcií a arbitráž

Jurisdikcie medzi sebou súťažia o ekonomickú činnosť a vývoj technológií je súčasťou tejto súťaže. Jurisdikcie priaznivé súkromiu priťahujú vývojárov aj používateľov. Programátori radi pracujú tam, kde je ich práca legálna, a vývoj šifrovania sa sústredil v jurisdikciách s priaznivým zaobchádzaním. Podniky, ktoré slúžia zákazníkom dbajúcim na súkromie, sa usadzujú tam, kde to môžu robiť legálne; technologické firmy zamerané na súkromie prilákali napríklad Švajčiarsko a Estónsko. Zámožní používatelia, ktorí chcú súkromie, si poskytovateľov vyberajú čiastočne podľa jurisdikcie a dopyt po offshorových službách odráža tú istú arbitráž, len na strane spotreby.

Ekonóm Charles Tiebout analyzoval, ako súťaž jurisdikcií o obyvateľov tlačí k politikám, ktoré obyvatelia uprednostňujú.[10] Pri kryptografii táto analýza osvetľuje naraz niekoľko javov. Vývojári a firmy sa môžu presťahovať a dôveryhodná hrozba odchodu (exitu) obmedzuje, čo si môže ktorákoľvek jurisdikcia dovoliť uložiť. Jurisdikcie známe ochranou súkromia priťahujú aktivity, ktoré súkromie hľadajú, a výsledná povesť sa stáva aktí-

vom, ktoré sa oplatí udržiavať. Keď niektoré jurisdikcie ponúkajú priaznivé podmienky, ostatné čelia tlaku, aby ich dorovnali, inak o ekonomickú činnosť prídu.

Táto súťaž môže viesť k ochrane súkromia aj k sledovaniu, podľa toho, na aké tlaky vláda reaguje. Vlády, ktoré reagujú hlavne na tlak orgánov činných v trestnom konaní a spravodajských služieb, súťažia v ponuke väčších sledovacích schopností, teda v závode na dno. Vlády, ktoré reagujú hlavne na tlak ekonomického rozvoja, súťažia v ponuke väčšej ochrany súkromia, teda v závode na vrchol. Výsledok závisí od toho, ktoré podnety v ktorej jurisdikcii prevažujú, a dnešný obraz je zmiešaný: niektoré jurisdikcie súťažia v ochrane súkromia, iné rozširujú sledovanie, a tí istí aktéri sa pri prechode cez hranice niekedy ocitnú na opačných stranách tej istej čiary.

13.5 Vojna pokračuje

Posun od nástrojov k tvorcom

Kryptovojny sa neskončili liberalizáciou v deväťdesiatych rokoch. Zintenzívneli, no pozdĺž inej osi. Skoršie boje sa snažili zabrániť tomu, aby sa kryptografia vymkla z vojenskej kontroly; keď sa silné šifrovanie stalo bežným softvérom, tento front sa zrútil. Štáty sa potom prispôsobili. Ak sa matematika potlačiť nedá a softvér sa zadržať nedá, zostáva ako miesto nátlaku človek.

Protokol sa zatknúť nedá. Vývojára áno. Otvorený zdrojový kód je právne nepohodlné stíhať priamo; človek, ktorý ho napísal, nasadil, propagoval alebo prevádzkoval okolo neho postavenú infraštruktúru, je jasný právny cieľ. Sankčné režimy, zákony o poskytovaní platobných služieb, právo proti praniu špinavých peňazí a doktríny sprisahania zasahujú jednotlivcov bez ohľadu na to, čo protokol robí alebo nerobí. Druhá fáza kryptovojen je vojna proti tvorcom, lebo tvorcovia sú jediným zostávajúcim ľudským kontrolným bodom v systémoch navrhnutých tak, aby ľudské kontrolné body odstránili.

Mechanizmom je odrádzací účinok (chilling effect). Keď písanie kódu na ochranu súkromia môže pri agresívnom výklade sankčného práva alebo práva proti praniu špinavých peňazí znamenať riziko desiatich rokov väzenia, takýto kód píše menej ľudí. Keď sa prevádzkovanie infraštruktúry pre súkromný obchod dá stíhať ako zločinecká organizácia bez ohľadu na správanie používateľov, menej prevádzkovateľov niečo buduje. Stíhania nemusia uspieť pri každej právnej teórii, aby uspeli ako politika; stačí, že zvýšia osobné náklady budovania natoľko, aby odradili hraničného nováčika.

Tento vzorec ukotvujú dva prípady. Bernard von NotHaus vydával Liberty Dollar: súkromné strieborné a zlaté kusy a papierové certifikáty ur-

čené na použitie ako bežné platidlo popri bankovkách Federálneho rezervného systému, od roku 1998 do polovice prvého desaťročia tohto storočia. Federálne stíhanie pre falšovanie a sprisahanie túto činnosť ukončilo.[15] Téória nestála na tom, že by von NotHaus prevádzkoval neoprávnenú finančnú službu, ale na tom, že súkromne razené mince určené na obeh ako bežné platidlo útočia na samotnú peňažnú jednotku. Pokyn porote opisoval Liberty Dollar ako pokus podkopať dôveru verejnosti v americkú menu. Fyzická centralizovaná konkurencia voči štátnym peniazom v identifikovateľných rukách vyvoláva priamejšiu právnu odpoveď, než aká zvyčajne čaká digitálne systémy.

Tornado Cash ukázal digitálnu verziu rovnakého tlaku, ktorý pôsobí aj bez správcu, ktorého by bolo možné zabaviť. Zmluvy jeho hlavného fondu sa po nasadení v sieti Ethereum stali nemennými, takže ich nikto nemohol vypnúť. Dňa 8. augusta 2022 zaradil Úrad pre kontrolu zahraničných aktív (OFAC) na zoznam osôb pod sankciami (Specially Designated Nationals) samotný Tornado Cash. Cieľom sa stal kód inteligentných zmlúv a adresy v sieti Ethereum, na ktorých beží, nie osoba či firma; americkým osobám sa zakázalo s týmito adresami interagovať, nech bol účel akýkoľvek.[16] Zaradenie neobstálo. V novembri 2024 Piaty obvodný odvolací súd vo veci *Van Loon v. Department of the Treasury* rozhodol, že nemenné inteligentné zmluvy Tornado Cash nie sú „majetkom“ podľa zákona o mimoriadnych hospodárskych právomociach (International Emergency Economic Powers Act) a nemožno ich zaradiť na základe zákonných právomocí OFAC. Dňa 21. marca 2025 ministerstvo financií Tornado Cash zo sankčného zoznamu odstránilo. Trestné konania proti vývojárom, ktorí protokol napísali, medzi nimi proti Alexeymu Pertsevovi v Holandsku a Romanovi Stormovi v Spojených štátoch, pokračovali z iných právnych dôvodov a vyradenie zo zoznamu sa ich netýkalo.[17] Odolnosť protokolu a osobná bezpečnosť sú rozdielne problémy. Nemenný kód môže prežiť priame potlačenie a ľudia, ktorí ho napísali, na seba berú právny tlak, ktorý protokol odvracia. Kontrola sa presunula od kódu ku kóderovi, od systému k ľuďom, ktorí ho udržiavajú.

Komerčný špionážny softvér

Šifrovanie vyhralo na linke. Správa chránená moderným protokolom s račňou je počas prenosu nečitateľná, a tak si štát kupuje cestu späť na koncovom zariadení, kde je dešifrovaný obsah dostupný tou istou cestou, ktorou ho vidí používateľ. Komerčný špionážny softvér (spyware) je nástroj, po ktorom štát siahne, keď priama kontrola nad matematikou a stíhanie tvorcov k obsahu nedovedú. Kapitola 12 dokumentuje štruktúru tohto odvetvia aj jeho záznam o zodpovednosti dodávateľov; kryptovojnový pohľad je užší a vidí v spyware tretiu fázu, ktorá nastúpi, keď kryptografická kontrola a stíhanie tvorcov dospejú do konca.[11]

Šifrovanie obsahu, nech je matematicky akokoľvek bezpečné, nestačí, keď je koncové zariadenie kompromitované. Prevádzkovou odpoveďou sa zaoberá kapitola 22.

Súčasné právne boje

Návrhy „zodpovedného šifrovania" s „výnimočným prístupom" sa objavujú stále, s argumentmi blízkymi tým, ktoré ponúkal Clipper pred tromi desaťročiami, a technické problémy zostávajú. Od roku 2022 urobil súbor konkrétnych legislatívnych projektov súčasnú fázu konfliktu mimoriadne hmatateľnou.

Navrhované nariadenie Európskej únie o sexuálnom zneužívaní detí (CSAR), známe ako „Chat Control" (plošné skenovanie súkromných správ), by od poskytovateľov interpersonálnych komunikačných služieb vyžadovalo skenovať obsah používateľov kvôli materiálom zobrazujúcim sexuálne zneužívanie detí. Rozsah zahŕňa aj služby s end-to-end šifrovaním. Skenovanie obsahu s end-to-end šifrovaním vyžaduje buď šifrovanie prelomiť, alebo ešte pred zašifrovaním vložiť skener na koncové zariadenie; obe cesty znamenajú ten istý architektonický kompromis. Chat Control je trojuholníková intervencia uplatnená na komunikáciu: štát mení podmienky výmeny medzi poskytovateľom a používateľom tým, že núti poskytovateľa sledovať v mene štátu, tak ako kapitola 10 opísala nútenie bánk, aby sledovali vlastných vkladateľov. Nemecko, Rakúsko, Holandsko a ďalšie členské štáty v po sebe idúcich predsedníctvach Rady zablokovali kvalifikovanú väčšinu a Výbor Európskeho parlamentu LIBE odmietol povinné skenovanie vo vlastnej pozícii z novembra 2023. Text sa za štyri roky prepracoval a znovu predložil, no neprijal sa. To, že odpor vydržal tak dlho, ukazuje, že argumenty z čias Clippera o riziku zadných vrátok pôsobia presvedčivo, keď ich predkladáme ako tvrdenia o architektúre, nie ako politické preferencie.

Britský zákon o bezpečnosti online (Online Safety Act 2023) pokročil ďalej. Oddiel 122 zákona dáva regulátorovi komunikácií Ofcom právomoc vydávať oznámenia, ktoré vyžadujú, aby „akreditovaná technológia" skenovala komunikáciu s end-to-end šifrovaním kvôli materiálom zobrazujúcim sexuálne zneužívanie detí a obsahu súvisiacemu s terorizmom. Pri schvaľovaní zákona vydala vláda ministerské vyhlásenie, v ktorom pripustila, že právomoc sa nepoužije, kým nebude dostupné „technicky uskutočniteľné" skenovanie. Zákonná právomoc zostáva a jej použitie závisí od posúdenia regulátora, nie od ďalšej primárnej legislatívy. Každá z hlavných služieb s end-to-end šifrovaním pôsobiacich v Spojenom kráľovstve, vrátane Signalu, WhatsAppu a iMessage od Applu, oznámila, že sa z Británie stiahne skôr, než zavedie skenovanie na strane klienta. Európsky súd pre ľudské práva (ESĽP) v rozsudku *Podchasov v. Russia* vo februári 2024 rozhodol, že zákonná požiadavka oslabiť end-to-end šifrovanie

„nemôže byť považovaná za nevyhnutnú v demokratickej spoločnosti“; je to prvé rozhodnutie vysokého súdu týkajúce sa členského štátu Rady Európy, podľa ktorého architektonický kompromis neobstojí v teste proporcionality.

Nariadenie Európskej únie eIDAS 2.0 zavádza iný vektor útoku. Článok 45 nariadenia by v pôvodnom návrhu nútil webové prehliadače dôverovať kvalifikovaným certifikátom autentifikácie webových stránok vydaným poskytovateľmi určenými členskými štátmi, a to bez obvyklého oprávnenia prehliadačov certifikáty auditovať, odvolávať alebo odstraňovať, ak ich považujú za nebezpečné. Mechanizmus by každému určenému členskému štátu umožnil vydávať certifikáty, ktoré sú prehliadače povinné prijať, a to je architektonická definícia schopnosti útoku typu „muž uprostred“ (man-in-the-middle) proti TLS (Transport Layer Security). Proti návrhu podpísali otvorené listy výrobcovia prehliadačov vrátane Mozilly, organizácie na ochranu občianskych slobôd vrátane Electronic Frontier Foundation a viac než päťsto akademických kryptografov. Konečné znenie, prijaté v apríli 2024, obsahuje výnimku, ktorá prehliadačom dovoľuje prijať „preventívne opatrenia“, keď existujú „podložené obavy týkajúce sa narušenia bezpečnosti“; výrobcovia prehliadačov to vykladajú tak, že im zostáva oprávnenie viesť záznamy Certificate Transparency a odvolávať certifikáty. Základná povinnosť dôverovať kvalifikovaným certifikátom zostáva, a taký kompromis mala regulácia priniesť.[12]

Cypherpunkové čítanie týchto troch epizód nehovorí, že regulácia vždy prehrá, lebo právomoci Ofcomu podľa oddielu 122 sú skutočné a dajú sa použiť. Nehovorí ani to, že regulácia vždy vyhrá, lebo Chat Control sa štyri roky darí blokovať. Hovorí, že architektonické argumenty proti zadným vrátkam, ktoré vznikli ako odpoveď na Clipper, prežili tri desaťročia technologických zmien a dnes tvoria jedinú trvalú obranu proti súčasnej vlne. Keď sa vec podá ako „toto sú zadné vrátka“, politický odpor drží. Keď sa podá ako „toto je cielený mechanizmus proti závažnému trestnému činu“, politický odpor slabne. Obhajcovia musia udržať architektonický pohľad.

Stiahnutie systému NeuralHash

V auguste 2021 oznámil Apple systém NeuralHash, ktorý by na zariadeniach používateľov skenoval obrázky podľa súboru hašov známych materiálov zobrazujúcich sexuálne zneužívanie detí ešte pred nahraním do iCloudu. Systém sa predstavoval ako zachovávajúci súkromie: porovnanie hašov by prebehlo na zariadení a hlásili by sa len označené zhody. Do mesiaca zverejnili bezpečnostní výskumníci adverzárne kolízie funkcie NeuralHash a ukázali, že odhodlaný útočník vie vyrobiť obrázky, ktoré dajú falošne pozitívne zhody s ľubovoľnými cieľovými hašmi. Námietka akademických kryptografov, organizácií na ochranu občianskych slobôd aj App-

leho vlastnej inžinierskej komunity sa týkala architektúry; miera falošne pozitívnych výsledkov bola až druhoradá. Skener na každom zariadení, aj taký, ktorý v deň nasadenia hľadá jedinú triedu obsahu, je infraštruktúra, ktorej budúce použitie poskytovateľ nebude ovládať.

Apple systém stiahol v decembri 2022. Nástupca sa nenasadil. Firma presmerovala úsilie do funkcie Communication Safety, ktorá beží na zariadení, je dobrovoľná a nič nehlási mimo zariadenia. Stiahnutie ukázalo, že architektonická kritika môže zvrátiť komerčné nasadenie skôr, než sa infraštruktúra usadí. Rovnaká kritika platí pre každý ďalší návrh skenovania na strane klienta a rovnaké kryptografické námietky naďalej platia.[13]

Pokračujúce regulačné hrozby

Zodpovednosť platforiem za obsah používateľov vytvára stimuly sledovať používateľov a podkopávať end-to-end šifrovanie. Regulácia kryptomien rozširuje finančné sledovanie cez požiadavky KYC (povinné overenie totožnosti zákazníka), registráciu búrz kryptomien a pravidlo Travel Rule (pravidlo o sprievodných údajoch pri prevodoch).[25] Návrhy medzinárodných rámcov na reguláciu šifrovania sa snažia uzavrieť príležitosti jurisdikčnej arbitráže.

Debata o „going dark``

Orgány činné v trestnom konaní tvrdia, že sa im stráca prístup k obsahu komunikácie (tzv. „going dark“): nedostanú sa ku komunikácii, ktorú šifrovanie chráni, a FBI vedie kampaň za povinné prístupové schopnosti.[14] V skutočnosti sa prístup rozšíril, nie zúžil; napriek šifrovaniu majú orgány činné v trestnom konaní prístup k väčšiemu množstvu údajov než kedykoľvek predtým a metadáta, sledovanie polohy aj spolupráca platforiem im dávajú obrovské prúdy informácií. Každý bezpečnostný expert, ktorý sa touto otázkou zaoberal, dospel k záveru, že povinný prístup prináša zraniteľnosti, ktoré sa šíria za hranice policajného použitia a stávajú sa cieľmi útokov nepriateľských aktérov.[18]

Postkvantové obavy

Kvantové počítače ohrozujú dnešnú kryptografiu s verejným kľúčom. Dostatočne výkonný kvantový počítač by mohol prelomiť RSA a kryptografiu na eliptických krivkách, ktoré zabezpečujú väčšinu dnešnej internetovej prevádzky.[19][23]

To prináša hrozbu aj príležitosť. Šifrované údaje zachytené dnes sa dajú dešifrovať neskôr, keď kvantové počítače dozrejú, takže „zbieraj teraz, dešifruj neskôr“ je životaschopná stratégia pre trpezlivých protivníkov.[24] Zároveň sa postkvantová kryptografia posunula z výskumu k včasnej štandardizácii a plánovaniu nasadenia; NIST dokončil prvé základné štandardy v roku 2024, no prechod na algoritmy odolné voči kvantovým počíta-

čom zostáva veľkým infraštruktúrnym projektom.[20] Štáty sa môžu pokúsiť využiť tento prechod ako príležitosť presadiť zadné vrátka v nových kryptografických štandardoch.

Konflikt pokračuje

Kryptovojny pokračujú ako trvalá črta vzťahu medzi štátmi a občanmi, ktorí majú prístup k silnej kryptografii. Štáty chcú schopnosť sledovať; občania chcú súkromie; kryptografia môže poskytnúť súkromie, ktoré odoláva štátnemu sledovaniu; štáty preto kryptografiu chcú obmedziť. Žiadna strana nemôže natrvalo vyhrať. Vynález kryptografie nemožno vrátiť späť a štátnu moc nemožno zrušiť, a konflikt pretrváva, lebo obe strany majú trvalé záujmy.

Zhrnutie kapitoly

Kryptografická kontrola zlyháva proti vyspelým aktérom zo štrukturálnych dôvodov. Matematike je zákaz ľahostajný, replikácia informácie stojí takmer nič a celosvetová koordinácia jurisdikcií s rozdielnymi záujmami je prakticky nemožná. Kontrola napriek tomu uspieva proti bežným používateľom, a to cez ťažkú implementáciu a bariéry použiteľnosti: väčšina používateľov prijme predvolené nastavenia, nevie posúdiť kryptografickú bezpečnosť a žije v jurisdikciách, ktoré vynucujú súlad inštitúcií. Dvojúrovňová rovnováha, silná ochrana pre tých, čo ju uprednostňujú, a slabá pre všetkých ostatných, je empirickým výsledkom troch desaťročí konfliktu.

Súčasná fáza mieri na tvorcov. Sankcie, zákony o poskytovaní platobných služieb a doktríny sprisahania zasahujú jednotlivcov tak, ako sa protokoly zasiahnuť nedajú, a stíhania nemusia uspieť pri každej teórii, aby uspeli ako politika. Fázu nesie konkrétny súbor regulačných iniciatív: návrh Chat Control v Európskej únii, právomoci podľa oddielu 122 britského zákona o bezpečnosti online a povinná dôvera prehliadačov podľa eIDAS 2.0. Každá z nich čerpala z jazyka čias Clippera o „výnimočnom prístupe“ a každej sa kládol odpor z architektonických dôvodov. Stiahnutie návrhu NeuralHash (skenovania na strane klienta) Applom v decembri 2022 zasa ukázalo, že kritika môže zvrátiť komerčné nasadenie skôr, než sa usadí. Komerčný špionážny softvér je odpoveďou štátu na to, že šifrovanie obsahu vyhralo na linke, a odvetvie prežíva sankcie voči jednotlivým dodávateľom bežnou trhovou substitúciou. Kontrola sa presunula od kódu ku kóderovi a od prenosu ku koncovému zariadeniu; prevádzkovou odpoveďou sa zaoberá kapitola 22.

Konflikt je trvalý. Vynález kryptografie nemožno vrátiť späť a štátnu moc nemožno zrušiť; jurisdikčná arbitráž otvára príležitosti bez záruk a závod jurisdikcií sa môže uberať k sledovaniu rovnako ľahko ako k súkromiu, podľa toho, na aké tlaky vlády reagujú. Kapitola 14 rozvíja kryptografické

základy, ktoré táto kapitola predpokladá, a časť V skúma konkrétne implementácie, ktoré tunajšia politická a ekonomická analýza predpokladá.[21]

Poznámky

[1] Phil Zimmermann, „Why I Wrote PGP“, pôvodne vydané v *PGP User's Guide* (1991, aktualizované 1999), `https://web.archive.org/web/20240101000000/https://www.philzimmermann.com/EN/essays/WhyIWrotePGP.html`. Pozri tiež kap. 2, pozn. 15, kde je spracovaná história cypherpunkerov.

[2] Podrobnejšie dejiny amerických exportných kontrol kryptografie pozri Whitfield Diffie and Susan Landau, *Privacy on the Line: The Politics of Wiretapping and Encryption* (Cambridge, MA: MIT Press, 1998).

[3] Pozri Zimmermann, citovaný v pozn. 1 vyššie.

[4] Stratégia tlačeného zdrojového kódu využila v praxi právny rozdiel. Regulátori považovali softvér za exportne regulovaný, kým knihy mali silnejšiu a jasnejšiu ochranu slobody prejavu. Philip Zimmermann, *PGP: Source Code and Internals* (Cambridge, MA: MIT Press, 1995).

[5] K návrhu čipu Clipper a k polemike okolo neho pozri A. Michael Froomkin, „The Metaphor Is the Key: Cryptography, the Clipper Chip, and the Constitution“, *University of Pennsylvania Law Review* 143, č. 3 (1995): 709–897.

[6] Matt Blaze, „Protocol Failure in the Escrowed Encryption Standard“, *Proceedings of the 2nd ACM Conference on Computer and Communications Security* (1994): 59–67.

[7] Bernstein v. U.S. Department of State, 922 F. Supp. 1426 (N.D. Cal. 1996), a nasledujúce rozhodnutie senátu Deviateho obvodného odvolacieho súdu z 6. mája 1999, *Bernstein v. U.S. Department of Justice*, 176 F.3d 1132 (9th Cir. 1999), podľa ktorého je zdrojový kód softvéru prejavom chráneným Prvým dodatkom. Rozhodnutie bolo stiahnuté, keď sa prípad dostal pred súd v plnom zložení (en banc), no spor prispel k súbežnému uvoľneniu exportných kontrol podľa výkonného príkazu č. 13026 (15. novembra 1996) a k nasledujúcim revíziám pravidiel Bureau of Industry and Security.

[8] Hans-Hermann Hoppe, *Democracy: The God That Failed: The Economics and Politics of Monarchy, Democracy, and Natural Order* (New Brunswick, NJ: Transaction Publishers, 2001). Argument o časovej preferencii je najkoncentrovanejší v kapitole 1 („On Time Preference, Government, and the Process of Decivilization“) a v kapitole 2. Kritika z vnútra rakúskej školy zahŕňa Joseph T. Salerno, „Comment on Hoppe's ‚On Time Preference‘ “, *Review of Austrian Economics* 9, č. 1 (1996), a neskoršie výmeny názorov; Walter Block, „Is Monarchy a Libertarian Stance?“, *Reason Papers* 32 (2010), obhajuje Hoppeho proti niektorým námietkam. Rámec sa v hlavnom texte používa ako optika na sledovaciu legislatívu, nie ako všeobecná podpora Hoppeho porovnania monarchie a demokracie.

[9] Hlasovanie č. 398, Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act, H.R. 3162), 107. kongres, 24. októbra 2001: 357 za, 66 proti. Office of the Clerk of the U.S. House of Representatives, `https://clerk.house.gov/Votes/2001398`. Senát schválil návrh nasledujúci deň pomerom 98 : 1.

[10] Charles M. Tiebout, „A Pure Theory of Local Expenditures“, *Journal of Political Economy* 64, č. 5 (1956): 416–424.

[11] Odvetvie komerčného špionážneho softvéru je vyspelé, nasadené po celom svete a odolné voči sankciám na jednotlivých dodávateľov; úplný zoznam produktov a právny stack pozri kap. 12, pozn. 8 (NSO Pegasus, Intellexa Predator, Paragon Graphite, Candiru, Cellebrite, Magnet Forensics a americké rozhodnutie vo veci NSO). Citizen Lab,

https://citizenlab.ca/, je hlavným empirickým zdrojom, ktorý sleduje nasadenia u štátnych zákazníkov. *WhatsApp LLC v. NSO Group*, Case No. 4:19-cv-07123 (N.D. Cal. 2024), prvé významné občianskoprávne rozhodnutie o zodpovednosti dodávateľa špionážneho softvéru. NSO Group, https://www.nsogroup.com/. Zaradenie NSO Group na zoznam Entity List ministerstva obchodu USA (3. novembra 2021), 86 Fed. Reg. 60759 (4. novembra 2021).

[12] Chat Control (návrh nariadenia EÚ CSAR), oddiel 122 britského zákona o bezpečnosti online a článok 45 nariadenia eIDAS 2.0 tvoria súčasný súbor regulačného tlaku proti end-to-end šifrovaniu; Európsky súd pre ľudské práva rozhodol vo veci Podchasov v. Russia (február 2024), že oslabenie E2EE nie je nevyhnutné v demokratickej spoločnosti. EU Regulation on Child Sexual Abuse („Chat Control" / CSAR), proposal COM(2022) 209, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52022PC0209, pozícia Výboru LIBE Európskeho parlamentu je sledovaná na https://www.europarl.europa.eu/committees/en/libe/home. UK Online Safety Act 2023, Section 122, https://www.legislation.gov.uk/ukpga/2023/50/section/122. EU eIDAS 2.0 Regulation (EU) 2024/1183, https://eur-lex.europa.eu/eli/reg/2024/1183/oj. Otvorený list Mozilly, EFF a expertov na kybernetickú bezpečnosť o článku 45 nariadenia eIDAS 2.0 na https://blog.mozilla.org/en/mozilla/mozilla-eff-cybersecurity-experts-publish-letter-on-dangers-of-article-452-eidas-regulation/. European Court of Human Rights, *Podchasov v. Russia* (App. no. 33696/19), rozsudok z 13. februára 2024, https://hudoc.echr.coe.int/eng?i=001-230854. Signal Foundation, https://signal.org/, s verejnými vyhláseniami o odchode z jurisdikcií, ktoré nariaďujú skenovanie na strane klienta, archivovanými na https://signal.org/blog/; pozri tiež kap. 5, pozn. 7.

[13] Apple oznámil NeuralHash v auguste 2021 ako skener materiálov zobrazujúcich sexuálne zneužívanie detí (CSAM) priamo na zariadení, výskumníci zverejnili adverzárne kolízie do mesiaca a Apple systém stiahol v decembri 2022. Pôvodné oznámenie NeuralHash od Applu (5. augusta 2021), archivované na https://web.archive.org/web/20210805170250/https://www.apple.com/child-safety/. Demonštrácia adverzárnych kolízií: AsuharietYgvar et al., „AppleNeuralHash2ONNX", repozitár GitHub, https://github.com/AsuharietYgvar/AppleNeuralHash2ONNX. Odpoveď akademickej obce a organizácií na ochranu občianskych slobôd: Harold Abelson et al., „Bugs in our Pockets: The Risks of Client-Side Scanning", October 2021, https://arxiv.org/abs/2110.07450. Súčasná funkcia Communication Safety od Applu, ktorá beží na zariadení, je zdokumentovaná na https://support.apple.com/guide/iphone/communication-safety-iph00618be7a5/ios.

[14] James Comey, „Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course?", prejav v Brookings Institution, 16. októbra 2014, https://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course.

[15] Bernard von NotHaus založil Liberty Dollar v roku 1998 ako súkromný projekt meny z drahých kovov; federálne stíhanie sa sústredilo na teórie falšovania a sprisahania týkajúce sa súkromne razených mincí určených na použitie ako bežné platidlo. Odsúdenie bolo potvrdené v odvolacom konaní a činnosť Liberty Dollar sa potom skončila. Pozri *United States v. Bernard von NotHaus*, W.D.N.C. 5:09-cr-00027 (2011), a potvrdenie Štvrtým obvodným odvolacím súdom.

[16] U.S. Department of the Treasury, Office of Foreign Assets Control, zaradenie Tornado Cash, 8. augusta 2022, https://home.treasury.gov/news/press-releases/jy0916,

so zoznamom mnohých súvisiacich adries inteligentných zmlúv. Nasledovali trestné obvinenia vývojárov, medzi nimi Alexey Pertsev v Holandsku (odsúdený v máji 2024) a Roman Storm v Spojených štátoch.

[17] *Van Loon v. Department of the Treasury*, 122 F.4th 549 (5th Cir. 2024), rozhodol, že nemenné inteligentné zmluvy Tornado Cash nie sú „majetok" podľa zákona o mimoriadnych hospodárskych právomociach (International Emergency Economic Powers Act) a nemožno ich zaradiť na základe zákonných právomocí OFAC. Ministerstvo financií formálne odstránilo Tornado Cash zo zoznamu osôb pod sankciami (Specially Designated Nationals) 21. marca 2025 s odkazom na „novel legal and policy issues raised by use of financial sanctions against financial and commercial activity occurring within evolving technology and legal environments" („nové právne a politické otázky, ktoré vyvoláva uplatnenie finančných sankcií na finančnú a obchodnú činnosť v rámci vyvíjajúcich sa technologických a právnych prostredí"). Trestné konania proti vývojárom pokračovali z iných právnych dôvodov.

[18] Harold Abelson et al., „Keys Under Doormats: Mandating Insecurity by Requiring Government Access to All Data and Communications", *Journal of Cybersecurity* 1, č. 1 (2015): 69–79.

[19] Daniel J. Bernstein and Tanja Lange, „Post-Quantum Cryptography", *Nature* 549 (2017): 188–194.

[20] NIST finalizoval FIPS 203 (ML-KEM), FIPS 204 (ML-DSA) a FIPS 205 (SLH-DSA) 13. augusta 2024, `https://csrc.nist.gov/projects/post-quantum-cryptography`. Pozri tiež kap. 5, pozn. 4, kde je širší kontext štandardizácie postkvantovej kryptografie NIST.

[22] Cypherpunkové hnutie poskytlo intelektuálny a organizačný kontext, z ktorého sa kryptovojny viedli na civilnej strane. Kotvia ho dva zakladajúce dokumenty. Eric Hughes, „A Cypherpunk's Manifesto" (9. marca 1993), `https://www.activism.net/cypherpunk/manifesto.html`: „Súkromie je nevyhnutné pre otvorenú spoločnosť v elektronickom veku... My, cypherpunkeri, sme odhodlaní budovať anonymné systémy." (angl. „Privacy is necessary for an open society in the electronic age... We the Cypherpunks are dedicated to building anonymous systems.") Timothy C. May, „The Crypto Anarchist Manifesto" (1988, distribuovaný na konferencii Hackers Conference; uverejnený v e-mailovej konferencii Cypherpunks v roku 1992), `https://www.activism.net/cypherpunk/crypto-anarchy.html`, predpovedal, že kryptografia s verejným kľúčom úplne rozpustí štátnu kontrolu nad tokmi informácií. Cypherpunks mailing list, aktívny od roku 1992, je archivovaný na `https://mailing-list-archive.cryptoanarchy.wiki/`. Steven Levy, *Crypto: How the Code Rebels Beat the Government - Saving Privacy in the Digital Age* (Viking, 2001), je štandardné populárne spracovanie tohto obdobia.

[23] Matematické základy kryptografie s verejným kľúčom, o ktorých kapitola tvrdí, že sú voči zákazu ľahostajné, pochádzajú z dvoch prelomových článkov. Whitfield Diffie and Martin E. Hellman, „New Directions in Cryptography", *IEEE Transactions on Information Theory* 22, č. 6 (1976): 644–654, zaviedli výmenu kľúčov Diffie–Hellman a pojem asymetrickej kryptografie. Ronald L. Rivest, Adi Shamir, and Leonard Adleman, „A Method for Obtaining Digital Signatures and Public-Key Cryptosystems", *Communications of the ACM* 21, č. 2 (1978): 120–126, zaviedli RSA. Neal Koblitz, „Elliptic Curve Cryptosystems", *Mathematics of Computation* 48, č. 177 (1987): 203–209, a Victor S. Miller, „Use of Elliptic Curves in Cryptography", in *Advances in Cryptology - CRYPTO '85*, Lecture Notes in Computer Science 218 (Springer, 1986): 417–426, zaviedli kryptografiu na eliptických krivkách. Všetky štyri práce sú matematickými vzťahmi, o ktorých text tvrdí, že ich zákonodarný dekrét nemôže zvrátiť.

[24] Hrozba „zbieraj teraz, dešifruj neskôr“ opisuje programy protivníkov, ktoré zachytávajú a ukladajú dnes šifrovanú prevádzku do dňa, keď kryptoanalytická schopnosť umožní spätné dešifrovanie. Programy NSA MUSCULAR a BULLRUN, odhalené v dokumentoch Snowdena v roku 2013, ukázali, že hromadné zachytávanie šifrovanej prevádzky bolo už prevádzkovou politikou. Glenn Greenwald and Ewen MacAskill, „NSA Prism Program Taps into User Data of Apple, Google and Others“, *The Guardian* (6. júna 2013); James Ball, Julian Borger, and Glenn Greenwald, „Revealed: How US and UK Spy Agencies Defeat Internet Privacy and Security“, *The Guardian* (5. septembra 2013), o BULLRUN/EDGEHILL. Pokyny NIST k postkvantovej migrácii výslovne uvádzajú „zbieraj teraz, dešifruj neskôr“ ako hlavnú hrozbu, ktorá robí prechod naliehavým: NIST, *Migration to Post-Quantum Cryptography*, Special Publication 1800-38 (2023), `https://csrc.nist.gov/publications/detail/sp/1800-38/final`.

[25] Travel Rule Finančnej akčnej skupiny (FATF Recommendation 16) vyžaduje od poskytovateľov služieb s virtuálnymi aktívami, aby pri prevodoch nad určitou hranicou odovzdávali údaje o odosielateľovi a príjemcovi, čím rozširuje povinnosti typu KYC z bankového tajomstva na burzy kryptomien. FATF, *Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers* (October 2021), `https://www.fatf-gafi.org/publications/fatfrecommendations/documents/guidance-rba-virtual-assets-2021.html`. Vnútroštátna implementácia v Spojených štátoch prebieha cez FinCEN podľa Zákona o bankovom tajomstve (Bank Secrecy Act); navrhované pravidlo Travel Rule pre kryptomeny sa sleduje na `https://www.fincen.gov/`. Nariadenie EÚ o prevodoch finančných prostriedkov (Transfer of Funds Regulation) (EU) 2023/1113 rozšírilo pravidlo Travel Rule na poskytovateľov služieb s kryptoaktívami od 30. decembra 2024. Tieto požiadavky opakujú architektúru finančného sledovania, ktorú analyzovala kapitola 10: viazanie prístupu k službe na odhalenie údajov, uplatnené naprieč vrstvou kryptomien.

[21] Ďalšie čítanie o dejinách štátneho sledovania. Pre dejiny amerického plošného sledovania pred 11. septembrom je kanonickým textom trilógia Jamesa Bamforda: *The Puzzle Palace: A Report on America's Most Secret Agency* (Houghton Mifflin, 1982), *Body of Secrets* (Doubleday, 2001) a *The Shadow Factory: The Ultra-Secret NSA from 9/11 to the Eavesdropping on America* (Doubleday, 2008). K rozšíreniu sledovania po roku 2001 je štandardným investigatívnym spracovaním Dana Priest and William Arkin, *Top Secret America: The Rise of the New American Security State* (Little, Brown, 2011). K Snowdenovým odhaleniam konkrétne: Glenn Greenwald, *No Place to Hide* (Metropolitan Books, 2014), je opis udalostí z pohľadu novinára; Luke Harding, *The Snowden Files* (Vintage, 2014), pokrýva stranu *Guardianu*; Edward Snowden, *Permanent Record* (Metropolitan Books, 2019), sú Snowdenove memoáre. Nepublikované správy Church Committee, *Intelligence Activities and the Rights of Americans*, Senate Report No. 94-755 (1976), zostávajú najširším kongresovým vyšetrovaním amerického sledovania a sú dostupné na `https://www.intelligence.senate.gov/resources/intelligence-related-commissions`. K strane FBI sú dvoma štandardnými dejinami Athan Theoharis, *Spying on Americans: Political Surveillance from Hoover to the Huston Plan* (Temple University Press, 1978), a Tim Weiner, *Enemies: A History of the FBI* (Random House, 2012). K širšej technickej infraštruktúre: Whitfield Diffie and Susan Landau, *Privacy on the Line*, už citovaná, a Keith Devlin, *The Math Behind the Scenes* (Springer, 2022), pokrývajú dejiny kryptografickej politiky. K súčasnej praxi plošného sledovania mimo USA je Ronald Deibert, *Reset: Reclaiming the Internet for Civil Society* (House of Anansi, 2020), syntézou riaditeľa Citizen Lab; Cédric Biscay et al., správy *Privacy International's State of Privacy* na `https://privacyinternational.org`, sledujú konkrétne programy na medzinárodnej úrovni. K doktrinálnej a ústavnej stránke: Daniel J. Solove and Paul M. Schwartz, *Information Privacy Law*, 7th ed. (Aspen, 2020), je štandardná americká právnická učebnica; Orin S. Kerr, *The Digital Fourth Amendment* (Oxford University Press, 2024), je súčasná referenčná práca o doktríne Štvrtého dodatku v digitálnom kontexte.

ČASŤ V

TECHNICKÁ IMPLEMENTÁCIA

14
KRYPTOGRAFICKÉ ZÁKLADY

> *„Vesmír verí v šifrovanie. Informáciu je jednoduchšie zašifrovať než dešifrovať.“*
>
> Julian Assange, *Cypherpunks: Freedom and the Future of the Internet* (2012)[1]

Úvod

Cieľom tejto kapitoly je pochopiť princípy, nie absolvovať celý kurz kryptografie. Čitateľ musí vedieť, čo kryptografické nástroje dokážu a prečo fungujú, nie ako sa implementujú. Implementácia si vyžaduje odborné znalosti, no na používanie hotových implementácií stačí rozumieť ich vlastnostiam. Kto chce ísť hlbšie, môže siahnuť po knihe Davida Wonga *Real-World Cryptography* (Manning, 2021), ktorá je prístupným úvodom do praxe. Prísne formálne spracovanie ponúka kniha Jonathana Katza a Yehudu Lindella *Introduction to Modern Cryptography*, 3. vyd. (CRC Press, 2020). Dôkazové systémy rozoberá Justin Thaler, *Proofs, Arguments, and Zero-Knowledge* (2022, zadarmo online), a o tom, ako kryptografia zapadá do všetkého okolo, píše Ross Anderson, *Security Engineering*, 3. vyd. (Wiley, 2020).[2] Základné články tejto disciplíny, jej politické a etické vymedzenie aj dlhší historický príbeh sú zhromaždené v osobitnej poznámke s odporúčanou literatúrou na konci kapitoly.[3]

Kryptografia rieši problémy koordinácie matematikou, nie inštitúciami. Tradičné systémy vyžadujú dôveru v sprostredkovateľov, kryptografické systémy len dôveru v predpoklady o výpočtovej náročnosti. Tento posun od inštitucionálnej k matematickej dôvere je základom technológií, ktoré chránia súkromie.

Tri úlohy treba od začiatku držať oddelene. Jeden nástroj skrýva obsah, druhý dokazuje, kto správu schválil, a tretí umožňuje cudzím ľuďom overiť integritu bez dôvery v toho istého sprostredkovateľa. Kapitola prejde tieto úlohy v tomto poradí a potom sa spýta, čo matematika nahradiť dokáže a čo nie.

14.1 Symetrická a asymetrická kryptografia

Symetrická kryptografia

Symetrická kryptografia je najstaršou podobou prvej úlohy, teda skrývania obsahu. Jeden kľúč šifruje a ten istý kľúč dešifruje. Ak kľúč majú len Alice a Bob, správu prečítajú len oni.

Rýchlosť symetrických algoritmov z nich robí pracovného koňa ochrany obsahu. Moderné šifry (AES, ChaCha20) šifrujú údaje rýchlosťou gigabajtov za sekundu.[4] Samotná rýchlosť však problém dôvery nevyrieši.

Ako si Alice a Bob dohodnú spoločné tajomstvo, keď sa nemôžu stretnúť osobne? Ak kľúč pošlú po nezabezpečenom kanáli, odpočúvač ho zachytí. Ak potrebujú na výmenu kľúča zabezpečený kanál, už zabezpečenú komunikáciu majú a kľúč nepotrebujú. To je problém distribúcie kľúčov a tisícročia obmedzoval kryptografiu na strany, ktoré si tajomstvá mohli odovzdať fyzicky: diplomatov s kuriérmi, armády so zabezpečenými linkami, špiónov s odkladacími miestami. Aby sa šifrovanie rozšírilo medzi ľudí, bolo treba toto obmedzenie prelomiť.

Asymetrická kryptografia

Asymetrická kryptografia (kryptografia s verejným kľúčom), objavená v sedemdesiatych rokoch, prelomila úzke hrdlo distribúcie kľúčov.[5] Namiesto jedného spoločného kľúča si každá strana vygeneruje matematicky prepojený pár kľúčov: verejný kľúč, ktorý môže voľne zdieľať, a súkromný kľúč, ktorý si necháva pre seba.

Vzťah medzi oboma kľúčmi sa nedá obrátiť. Verejný kľúč sa zo súkromného vypočíta jednoducho, ale súkromný kľúč z verejného je výpočtovo neuskutočniteľné zistiť. Žiadny predchádzajúci vzťah netreba. Alice môže poslať Bobovi šifrovanú správu, hoci s ním nikdy nekomunikovala, stačí jej jeho verejne dostupný verejný kľúč. Otázka sa mení z „mám zabezpečený kanál k tomuto človeku?“ na „je tento verejný kľúč pravý?“. A na druhú otázku sa dá odpovedať aj bez inštitúcií.

Tým sa vyriešila tá časť distribúcie kľúčov, ktorá sa týka dôvernosti. Alice zverejní svoj verejný kľúč, ostatní jej šifrujú správy a dešifrovať ich vie len ona. Netreba zabezpečený kanál ani sprostredkovateľa. Pravosť verejného kľúča zostáva samostatným problémom, ktorému sa venujeme nižšie.

Hybridná realita

Symetrická kryptografia efektívne skrýva obsah, ak už strany zdieľajú tajomstvo. Asymetrická kryptografia odstraňuje potrebu tohto predchádzajúceho tajomstva. Samotná ani jedna nestačí.

V praxi sa používajú obe. Asymetrická kryptografia dohodne relačný kľúč a symetrická zašifruje samotné údaje. Vďaka hybridnému postupu stojí každé šifrované spojenie na internete na tom istom základe: na vrstve výmeny kľúčov nahrádza inštitucionálnu dôveru matematická a obsah potom chráni čistá rýchlosť.

Algoritmy

Asymetrickú kryptografiu umožňuje niekoľko základných algoritmov. Výmena kľúčov Diffie–Hellman, publikovaná v roku 1976, umožňuje dvom stranám dohodnúť spoločné tajomstvo cez verejný kanál.[6] Ani jedna strana neprezradí svoj súkromný kľúč, no obe odvodia to isté spoločné tajomstvo matematickými operáciami nad verejnými hodnotami. Diffie–Hellman rieši výmenu kľúčov, nie šifrovanie ako také. Spoločné tajomstvo, ktoré vznikne, sa zvyčajne stane kľúčom pre symetrické šifrovanie.

RSA, publikované v roku 1978, poskytuje šifrovanie aj digitálne podpisy a opiera sa o náročnosť rozkladu veľkých čísel na prvočinitele.[7] Bezpečnosť závisí od toho, že rozklad dostatočne veľkých čísel zostane výpočtovo neuskutočniteľný. RSA vie šifrovať správy priamo (do určitej veľkosti) a vytvárať podpisy. Jeho nevýhodou je veľkosť kľúča: bezpečné RSA potrebuje kľúče s dĺžkou 2048 bitov alebo viac, takže je pomalšie a náročnejšie na zdroje než alternatívy.

Kryptografia na eliptických krivkách (ECC), predstavená v polovici osemdesiatych rokov, dosahuje rovnakú bezpečnosť s menšími kľúčmi vďaka iným matematickým štruktúram.[8] Kľúč na eliptickej krivke s 256 bitmi poskytuje bezpečnosť porovnateľnú s kľúčom RSA s 3072 bitmi. Menšie kľúče robia ECC rýchlejšou a vhodnejšou pre zariadenia s obmedzeným výkonom. Bitcoin používa na podpisy eliptickú krivku secp256k1.[9] Väčšina moderných systémov uprednostňuje pri nových implementáciách ECC pred RSA.

V praxi tieto algoritmy plnia doplnkové úlohy. Diffie–Hellman (alebo jeho variant na eliptických krivkách, ECDH) dohodne spoločné tajomstvo, podpisy RSA alebo na eliptických krivkách overia pravosť strán a z výsledného tajomstva sa stane kľúč pre symetrické šifry, ako je AES, ktoré šifrujú hlavný objem údajov.

Úloha náhodnosti

Kryptografická bezpečnosť závisí od nepredvídateľnosti. Kľúče sa musia generovať náhodne. Ak útočník dokáže kľúč uhádnuť alebo predpovedať, ani najsilnejší algoritmus nijako nechráni.

Entropia meria nepredvídateľnosť. Kľúč so 256 bitmi má 256 bitov entropie len vtedy, ak je každý bit rovnako pravdepodobný ako 0, tak 1, nezávisle od všetkých ostatných bitov. Ak má generovanie kľúča skreslenie alebo pravidelnosti, skutočná entropia klesne pod hodnotu, ktorú naznačuje dĺžka kľúča, a kľúč je slabší, než vyzerá.

Náhodnosť v kryptografii musí byť kryptograficky bezpečná: nestačí, aby len „vyzerala náhodne“, musí byť nepredvídateľná pre každého protivníka. Generátor pseudonáhodných čísel (PRNG) je algoritmus, ktorý z malej východiskovej hodnoty, nazývanej seed, vytvorí dlhú postupnosť čísel, ktorá vyzerá náhodne, ale je deterministická. Aj PRNG, ktorých výstup je štatisticky náhodný, môžu byť predvídateľné, ak útočník pozná ich vnútorný stav alebo seed. Kryptograficky bezpečné generátory pseudonáhodných čísel (CSPRNG) sú navrhnuté tak, aby ani pozorovanie ich výstupu neprezradilo budúce hodnoty.

Zdrojmi entropie sú hardvérové generátory náhodných čísel, ktoré snímajú fyzikálne javy (tepelný šum, rádioaktívny rozpad, elektronický šum), a udalosti v systéme (načasovanie stlačení klávesov, pohyby myši, časy príchodu sieťových paketov). Ktorýkoľvek jednotlivý zdroj môže byť narušený alebo nedostatočný, a tak bezpečné systémy spájajú viacero nezávislých zdrojov entropie. Útočník, ktorý vie predpovedať jeden zdroj, stále nevie predpovedať spoločný výstup, ak ostatné zdroje zostávajú nepredvídateľné. Operačné systémy udržiavajú zásobníky entropie, ktoré zbierajú náhodnosť zo všetkých dostupných zdrojov a napájajú nimi CSPRNG, ktoré aplikácie využívajú na generovanie kľúčov.

Keď zlyhá náhodnosť, zlyhá kryptografia úplne. Algoritmy môžu byť v poriadku, ale predvídateľné kľúče sú kľúče, ktoré sa dajú uhádnuť.

14.2 Hašovacie funkcie a digitálne podpisy

Jednosmerné funkcie

Kryptografická hašovacia funkcia berie vstup ľubovoľnej veľkosti a vytvorí výstup pevnej veľkosti („haš“ alebo „odtlačok“). SHA-256, ktorá sa široko používa v Bitcoine aj inde, vytvára 256-bitový výstup bez ohľadu na veľkosť vstupu.[10]

Hašovacie funkcie majú niekoľko vlastností, ktoré ich spolu robia užitočnými. Ten istý vstup dáva vždy ten istý výstup. Z výstupu je výpočtovo neuskutočniteľné nájsť akýkoľvek vstup, ktorý ho vytvára, a rovnako neuskutočniteľné je nájsť dva rôzne vstupy s rovnakým výstupom. Funkcie majú aj lavínový efekt: malá zmena vstupu vyrobí radikálne odlišný výstup.

Hašovacie funkcie umožňujú efektívne overovať integritu. Namiesto porovnávania celých súborov sa porovnajú ich haše. Zhodné haše zname-

najú zhodné súbory s drvivou pravdepodobnosťou, odlišné haše ukazujú, že súbory sa líšia.

Digitálne podpisy

Digitálne podpisy využívajú asymetrickú kryptografiu na overenie pravosti a integrity.[11] Pri šifrovaní každý s verejným kľúčom zašifruje a dešifruje len držiteľ súkromného kľúča. Podpisy fungujú opačne: podpis vytvorí len držiteľ súkromného kľúča, ale overiť ho môže každý, kto má verejný kľúč.

Podpisovanie sa začína výpočtom haša dokumentu, čím vznikne odtlačok obsahu s pevnou veľkosťou. Podpisujúci potom použije podpisový algoritmus so svojím súkromným kľúčom a hašom a vznikne hodnota podpisu, ktorá dokument sprevádza.

Overenie tento proces obracia. Overovateľ nezávisle vypočíta haš dokumentu a potom použije overovací algoritmus s verejným kľúčom, podpisom a znova vypočítaným hašom. Algoritmus vydá výsledok „platný“ alebo „neplatný“.

Matematika sa líši podľa schémy. Podpisy RSA využívajú modulárne umocňovanie. ECDSA,[15] schéma používaná v Bitcoine, využíva násobenie bodov na eliptickej krivke a modulárnu aritmetiku. Schnorrove podpisy[16] sú postavené inak a majú užitočné algebraické vlastnosti. Spoločná je im základná asymetria: platný podpis vytvorí len súkromný kľúč, na overenie stačí verejný.

Podpisy dokazujú tri veci. Overenie pravosti: podpis mohol vytvoriť len ten, kto má súkromný kľúč, takže ak veríte, že verejný kľúč patrí Alice, podpis dokazuje, že podpísala Alice. Integrita: akákoľvek zmena dokumentu po podpísaní podpis zneplatní, lebo znova vypočítaný haš nebude sedieť. Nepopierateľnosť: Alice nemôže vierohodne poprieť, že podpísala, ak sa podpis zhoduje s jej verejným kľúčom.

Overenie bez dôvery

Čo znamená overovať bez dôvery v overovateľa? Podpis môže nezávisle potvrdiť ktokoľvek s verejným kľúčom, takže netreba pýtať súhlas žiadneho orgánu a žiadny sprostredkovateľ nemôže nepravdivo tvrdiť, že overenie prebehlo. Matematika sa presadzuje sama.

„Bez dôvery“ (angl. „trustless“) tu má úzky význam: samotný proces overenia dôveru nevyžaduje, lebo ho môže vykonať ktokoľvek. Otvorená zostáva otázka, či verejný kľúč patrí tomu, komu sa pripisuje, no to je iný problém, ktorému sa venujeme nižšie.

14.3 Dôvera: matematická a inštitucionálna

Tradičné modely dôvery

Pred kryptografiou si dôvera vyžadovala inštitúcie. Reputácia umožňovala stranám budovať si históriu časom, hoci noví účastníci čelili vysokým bariéram. Právne vynucovanie trestalo porušenie dohôd, ale jeho účinnosť závisela od jurisdikcie a zdrojov. Dôveryhodné tretie strany slúžili ako sprostredkovatelia, ktorí sa za neznáme strany zaručili, a tak sústreďovali dôveru v sebe. Fyzickú ochranu poskytovali trezory alebo stráže spolu s pečatenými dokumentmi.

Každý model má spôsoby zlyhania: reputáciu možno vyrobiť, vynucovanie vyžaduje prístup k právnym systémom, sprostredkovateľov možno skorumpovať alebo prinútiť a fyzickú ochranu možno prelomiť.

Digitálne systémy tento vzorec zdedili bez zmeny. Kto chcel poslať e-mail, zdieľať súbor alebo vstúpiť do chatovacej miestnosti, musel veriť správcovi servera, že jeho správy zostanú dôverné a že presadí, kto k nim má prístup. Riadenie prístupu bolo politikou na strane servera, zapísanou ako riadok v databáze, príznak oprávnenia alebo položka v konfigurácii, ktorá bežala na infraštruktúre, ktorú nikto nekontroloval a nemohol skúmať. Ak bol správca čestný, kompetentný a nikým nenútený, systém fungoval, ako sa tvrdilo. Ak bol zlomyseľný, dostal súdny príkaz alebo bol napadnutý, prístupové politiky nič neznamenali a údaje boli odkryté. Problém inštitucionálnej dôvery sa len preložil na problém správy systémov a nárok na dôveru tým nebol menší.

Matematická dôvera

Kryptografická dôvera sa opiera o predpoklady o výpočtovej náročnosti. Predpoklad faktorizácie hovorí, že rozložiť súčin dvoch veľkých prvočísel je výpočtovo neuskutočniteľné. Predpoklad diskrétneho logaritmu hovorí, že výpočet diskrétnych logaritmov v určitých grupách je výpočtovo neuskutočniteľný. Predpoklady o hašovacích funkciách hovoria, že nájsť kolízie alebo vzory pre správne navrhnuté hašovacie funkcie je výpočtovo neuskutočniteľné. Tieto predpoklady skúmajú desaťročia matematici a kryptografi na celom svete. Na rozdiel od inštitucionálnej dôvery nekolíšu so zmenou ľudí, politickým tlakom ani ekonomickými stimulmi. Matematika neberie úplatky.

End-to-end šifrovanie mení miesto, kde sa presadzujú pravidlá prístupu. O tom, kto smie správu čítať, už nerozhoduje server, rozhoduje kryptografia: dešifrovať môžu len držitelia správnych kľúčov a žiadna zmena konfigurácie na serveri to nedokáže prebiť. Riadenie prístupu sa presúva z politiky v infraštruktúre na vlastnosť samotných údajov. Správca, ktorý bol kedysi garantom, sa pre garanciu stáva nepodstatným. Infraštruktúra naďalej smeruje a ukladá šifrový text, no nevie ho čítať, a dôvera, ktorú

musí používateľ vložiť, sa zredukuje z dôvery v ľudí a inštitúcie na dôveru v matematiku a v správu kľúčov na koncových zariadeniach.

Prečo je matematika spoľahlivejšia

Prečo by mal niekto veriť matematickému dôkazu viac než ľudskej inštitúcii? Lebo matematická dôvera má vlastnosti, ktoré inštitucionálnej štrukturálne chýbajú. Ten istý dôkaz sa všade overuje rovnako, platný podpis v jednej krajine je platný vo všetkých. Algoritmy sú verejné, matematiku môže overiť ktokoľvek, bezpečnosť nezávisí od utajenia metódy. Overenie nepotrebuje tretiu stranu. Alice môže overiť Bobov podpis bez toho, aby sa kohokoľvek pýtala na povolenie a bez dôvery v akéhokoľvek sprostredkovateľa. A výpočtové overovanie sa škáluje spolu s hardvérom, ľudské overovanie nie.

Hranice matematickej dôvery

Matematická dôvera nie je neobmedzená. Matematika nepovie, či verejný kľúč patrí tomu, komu sa pripisuje. Na to treba vonkajšie overenie: osobné stretnutie, sieť dôvery, certifikačné autority alebo iné potvrdenie mimo daného kanála. Matematika môže byť v poriadku a implementácia chybná, softvérové chyby dokážu podkopať teoreticky dokonalú kryptografiu. Samotné výpočtové predpoklady by mohli zlyhať, ak by P = NP alebo ak by kvantové počítače dostatočne dozreli. Používateľov možno napokon oklamať, aby prezradili kľúče alebo uverili nesprávnym verejným kľúčom, a môžu sa spoliehať na kompromitovaný softvér.

Matematická dôvera nahrádza niektoré požiadavky na dôveru, nie všetky: závislosť sa presúva od inštitúcií k predpokladom, ktoré sa overujú v kóde a v matematike. Posun je cenný, ale nie absolútny.

14.4 Obmedzenia a zraniteľnosti

Chyby v implementácii oproti kryptografickým prelomom

Kryptografické algoritmy sa matematicky prelamujú zriedka, zlyháva implementácia.

Pretečenie vyrovnávacej pamäte umožňuje útočníkom prepísať pamäť a získať kľúče, zatiaľ čo časové útoky merajú, ako dlho operácie trvajú, a z časovania samotného odhaľujú informácie o kľúčoch. Zlyhania generátora náhodných čísel ohrozujú bezpečnosť, lebo kryptografia potrebuje nepredvídateľnú náhodnosť. K protokolovým chybám dochádza, keď sú jednotlivé algoritmy bezpečné, ale ich kombinácia nie. Väčšina reálnych kryptografických zlyhaní sú zlyhania implementácie. Matematika môže držať, aj keď kód zlyháva.

Útoky postranným kanálom

Útoky postranným kanálom získavajú informácie z fyzickej implementácie, nie z matematickej slabiny. Analýza príkonu meria spotrebu energie počas kryptografických operácií a odhaľuje bity kľúča, elektromagnetické žiarenie z výpočtovej techniky môže prezrádzať informácie prostredníctvom rádiových signálov. Útoky na časovanie vyrovnávacej pamäte sledujú správanie cache a odhaľujú vzory prístupu do pamäte súvisiace s kľúčmi. Akustické útoky analyzujú zvuk, ktorý počítače vydávajú, a z neho zisťujú kryptografické informácie. Tieto útoky si vyžadujú fyzickú blízkosť alebo sofistikované vybavenie, no ukazujú, že kryptografická bezpečnosť závisí nielen od sily algoritmu.

Ľudský faktor

Človek je najslabší článok. Sociálne inžinierstvo, ktoré presvedčí ľudí, aby prezradili kľúče alebo nainštalovali malvér, obchádza kryptografiu úplne. Šifrovanie chránené slabým heslom chráni slabo. Správa kľúčov prináša trvalé výzvy: stratené kľúče znamenajú stratené údaje a kompromitované kľúče znamenajú kompromitované údaje. Systémy, ktoré sa ťažko používajú správne, sa používajú nesprávne, a používatelia vypínajú bezpečnostné funkcie, ktoré im prekážajú pri práci.

Fyzický nátlak, „útok kľúčom za päť dolárov“ rozoberaný v kapitole 5, zostáva mimo oblasti kryptografie.[12] Kryptografia chráni údaje, nie ľudí.

Kvantový horizont

Kvantové počítače ohrozujú súčasnú kryptografiu s verejným kľúčom. Shorov algoritmus, ak by bežal na dostatočne výkonnom kvantovom počítači, by mohol prelomiť RSA aj kryptografiu na eliptických krivkách, lebo efektívne rieši matematické problémy, o ktoré sa opierajú.[13] Hrozba nie je hypotetická v akademickom zmysle, pretože algoritmy sú publikované a ich fungovanie dobre rozumieme. Hypotetická je v zmysle hardvéru, lebo stroje, ktoré by ich vykonali v potrebnom rozsahu, zatiaľ neexistujú. Odhady, v ktorom roku by taký stroj mohol vzniknúť, sa medzi štátnymi bezpečnostnými službami a priemyselnými výskumnými programami líšia, pričom hlavný publikovaný rozsah leží medzi rokmi 2030 a 2040. Plánovací horizont obrancu sa musí prispôsobiť najskoršiemu vierohodnému dátumu, nie mediánu.

Stav sa líši podľa druhu kryptografie. Asymetrická kryptografia vrátane RSA a ECC je voči kvantovému útoku zraniteľná prostredníctvom Shorovho algoritmu. Symetrická kryptografia je dotknutá menej: Groverov algoritmus[17] prináša len kvadratické zrýchlenie, takže zdvojnásobenie dĺžky kľúčov (napríklad AES-256 namiesto AES-128) bezpečnosť zachová. Hašovacie funkcie sú ovplyvnené podobne málo, kvantové počítače im dávajú len mierne zrýchlenie, ktoré ich neprelomí. Asymetrické primití-

va treba migrovať, symetrické potrebujú úpravu parametrov, nie výmenu architektúry.

Naliehavejšou hrozbou v blízkej budúcnosti nie je útok naživo, ale „zbieraj teraz, dešifruj neskôr“. Protivník, ktorý dnes zachytí šifrovanú komunikáciu a uchová ju, kým nebude kvantové dešifrovanie dostupné, ju prečíta, keď stroj príde. Vystavenie obrancu teda závisí od životnosti tajomstva, nie od aktuálneho stavu kvantového hardvéru. S komunikáciou, ktorá musí zostať dôverná desať rokov alebo dlhšie, treba počítať ako s vystavenou budúcemu kvantovému dešifrovaniu, aj keď ju niekto zachytí dnes.

Prichádzajú štandardy

NIST finalizoval v auguste 2024 tri hlavné štandardy: ML-KEM na výmenu kľúčov, ML-DSA na podpisy a SLH-DSA ako konzervatívnu zálohu založenú na hašoch. V marci 2025 pridal ako zálohu HQC, založený na kódoch.[14] Štandardizácia trvala osem rokov verejnej kryptoanalýzy.

Prechod od štandardizácie k nasadeniu bol rýchlejší než pri akomkoľvek predchádzajúcom kryptografickom prechode. Signal nasadil PQXDH (hybrid kombinujúci X25519 a Kyber) v septembri 2023, ešte pred finalizáciou štandardu NIST. Apple dodal iMessage PQ3 v iOS 17.4 a macOS 14.4 vo februári 2024. Google zapol v Chrome 124 v apríli 2024 predvolene hybridnú výmenu kľúčov založenú na Kyberi a neskôr v tom istom roku prešiel na štandardizovaný X25519MLKEM768. Cloudflare uviedol, že do polovice roka 2025 využívalo hybridnú postkvantovú výmenu kľúčov viac ako tridsať percent nadviazaní spojenia v protokole Transport Layer Security na jeho okrajových serveroch. Postup nasadzovania sa opakuje: nový primitív sa zmieša s overeným klasickým, aby prelomenie jedného z nich neohrozilo reláciu, a celý internet sa migruje skôr, než sa hrozba zhmotní.

Vlády uverejnili harmonogramy migrácie na rovnakom základe. Súprava CNSA 2.0 americkej Národnej bezpečnostnej agentúry vyžaduje ML-KEM a ML-DSA pre systémy národnej bezpečnosti do roku 2033, s možnosťou skoršieho nasadenia, kde sa dá. Britské Národné centrum kybernetickej bezpečnosti odporúča postkvantovú migráciu pre systémy s vysokou hodnotou do roku 2035. Oba harmonogramy predpokladajú, že kvantový počítač schopný prelomiť šifry sa môže objaviť pred rokom 2035, a oba berú roky 2033 až 2035 ako termín, do ktorého musí byť migrácia hotová, nie ako očakávaný dátum jeho príchodu. Zásada je v bezpečnostnom inžinierstve bežná: rozpočet na migráciu je medzera medzi termínom a hrozbou a termín musí hrozbe predchádzať s rezervou, ktorá počíta so zdržaním pri implementácii.

Kvantový horizont a axióma odporu

Axióma odporu hovorí, že bezpečnosť systému sa meria nákladmi potrebnými na jeho kompromitáciu. Postkvantová kryptografia je inžinierskou odpoveďou na predvídateľnú zmenu týchto nákladov. Matematické problémy, ktoré boli pre klasické počítače ťažké, sa pre kvantové počítače stávajú zvládnuteľnými a náklady na ich prelomenie sa zrútia. Axióma nevyžaduje, aby boli náklady nekonečné. Vyžaduje, aby náklady obrancu na udržiavanie zostali nižšie než náklady protivníka na kompromitáciu, a postkvantový prechod je to, čo túto nerovnosť udrží aj pri zmene hardvéru.

Konštrukcia založená na hašoch, ktorú ilustruje FIPS 205, závisí len od vlastností hašovacích funkcií, ktoré dobre poznáme a ktoré kvantové počítanie ovplyvňuje menej. Tento primitív je konzervatívny presne v tom zmysle, ktorý axióma žiada: čím menšia je množina predpokladov, tým menšia je plocha, na ktorej sa dá zlyhať. Štandardy ML-KEM a ML-DSA, založené na mriežkach, sa opierajú o predpoklady novšie a menej preskúmané než tie, na ktorých stojí RSA. To je cena prechodu. Obranca prijíma menej odskúšaný predpoklad výmenou za odolnosť voči kvantovým útokom a komunita okolo štandardov odpovedala zverejnením viacerých nezávislých rodín algoritmov, aby neočakávaný útok na jednu z nich nezrútil celý prechod.

Model hrozieb „zbieraj teraz, dešifruj neskôr“ núti aj prehodnotiť, čo je dlhodobé tajomstvo. Rozhovory, ktoré sa považovali za dočasné, lebo boli šifrované počas prenosu, sú dlhodobé, ak niekto zachytí šifrový text. Obranca, ktorý zašifroval správu v roku 2024 predkvantovými primitívmi, musí počítať s tým, že správa bude čitateľná v okamihu, keď stroj príde. Preto Signal, Apple a Chrome nasadili svoje hybridné konštrukcie skôr, než sa hrozba zhmotnila. Hodiny pre minulú komunikáciu sa vrátiť nedajú, no hodiny pre budúcu komunikáciu ešte bežia.

Prechod je veľký infraštruktúrny projekt. Je však aj technicky uskutočniteľný, čo nasadenia spomenuté vyššie dokazujú v meradle celého internetu. Premennou, od ktorej závisí, či hrozba „zbieraj teraz, dešifruj neskôr“ zasiahne, je to, či obranca dokončí prechod skôr, než protivník využije zachytenú komunikáciu spred prechodu.

Čo kryptografia nevyrieši

Kryptografia nevyrieši bezpečnosť koncového zariadenia. Ak je zariadenie kompromitované, kryptografia na ňom nič neznamená. Neskryje metadáta: šifrovanie skrýva obsah, nie fakt komunikácie, a bez dodatočnej ochrany zostáva viditeľné, kto s kým hovorí, aj načasovanie a frekvencia (pozri kapitolu 17). Fyzický nátlak môže stále vynútiť vydanie kľúčov. Kryptografia taktiež nevyrieši sociálne problémy ani z nikoho nespraví dôveryhodného človeka, len umožní odhaliť niektoré zrady. A nevie ani

zaručiť pravosť kľúča, lebo matematika nepovie, či verejný kľúč patrí tomu, komu sa pripisuje.

Kryptografia je nástroj. Rieši konkrétne problémy. Očakávať od nej, že vyrieši problémy mimo svojho rozsahu, vedie k falošnému pocitu istoty.

Zhrnutie kapitoly

Kryptografia presúva dôveru od inštitúcií k matematike. Tradičné systémy vyžadujú dôveru v sprostredkovateľov, kryptografické systémy len dôveru v predpoklady o výpočtovej náročnosti, teda v tú istú množinu predpokladov, ktorú desaťročia overovali neúspešné útoky. Symetrická kryptografia efektívne skrýva obsah, keď sa kľúče zdieľajú. Asymetrická kryptografia odstraňuje potrebu predchádzajúceho spoločného tajomstva tým, že dáva každej strane pár kľúčov, ktorého súkromnú polovicu nemožno odvodiť z verejnej. Hybridné systémy používajú obe: asymetrickú na dohodu o kľúči, symetrickú na šifrovanie hlavného objemu údajov. Hašovacie funkcie vytvárajú odtlačky s pevnou veľkosťou, ktoré umožňujú overovať integritu, a digitálne podpisy kombinujú hašovanie s asymetrickou kryptografiou, aby zaručili pravosť, integritu a nepopierateľnosť. Podpis môže nezávisle overiť každý, kto má verejný kľúč; nijaký orgán ho nemusí potvrdzovať a žiadny sprostredkovateľ nemôže výsledok sfalšovať.

Matematická dôvera nahrádza niektoré požiadavky na dôveru, nie všetky. Pravosť kľúča si stále vyžaduje vonkajšie overenie, osobné stretnutie, sieť dôvery, certifikačné autority alebo iný kanál mimo hlavného, pretože matematika nepovie, či verejný kľúč patrí tomu, komu sa pripisuje. Implementácie môžu byť chybné aj pri bezchybných algoritmoch a väčšina reálnych kryptografických zlyhaní pramení v kóde: zlé parametre, slabá náhodnosť, nedbalá práca s kľúčmi, postranné kanály. Útoky postranným kanálom získavajú informácie z fyzických veličín (spotreba energie, časovanie, elektromagnetické žiarenie), zatiaľ čo samotná matematika drží. Človek zostáva najslabším článkom: sociálne inžinierstvo obchádza matematiku úplne a fyzický nátlak vynúti vydanie bez ohľadu na silu kľúča. Kryptografia chráni údaje, nie ľudí.

Kvantový horizont sa presunul z výskumu do praxe. NIST finalizoval hlavné štandardy podpisov a výmeny kľúčov založené na mriežkach a hašoch (ML-KEM, ML-DSA, SLH-DSA) v auguste 2024 a v marci 2025 vybral HQC ako zálohu pre výmenu kľúčov, založenú na kódoch. Protokol Signalu PQXDH, iMessage PQ3 od Applu, hybridná výmena kľúčov v Chrome a okrajové servery Cloudflare dnes dodávajú postkvantovú kryptografiu v nasadených spotrebiteľských systémoch. Prechod je veľký infraštruktúrny projekt, ktorý musí skončiť skôr, než prídu kvantové počítače schopné prelomiť šifry, pretože „zbieraj teraz, dešifruj neskôr“ robí z dnešného šifrového textu zdroj pre zajtrajšie dešifrovanie. Kryptografia rieši dôvernosť, overenie pravosti a integritu, no nerieši kompromitáciu koncového

zariadenia, vystavenie metadát, fyzický nátlak ani pravosť kľúča, a zvyšok knihy sa venuje tomu, čo kryptografia sama nezvládne.

Poznámky

[1] Julian Assange, with Jacob Appelbaum, Andy Müller-Maguhn, and Jérémie Zimmermann, *Cypherpunks: Freedom and the Future of the Internet* (New York: OR Books, 2012). Citovaný úryvok z úvodu Assangea vyjadruje štrukturálne tvrdenie, ktoré kapitola rozvíja: že asymetria medzi nákladmi na zašifrovanie informácie a nákladmi na jej dešifrovanie je zákonom vesmíru, nie politickým rozhodnutím; silná kryptografia preto obmedzuje štátnu moc architektonicky, na úrovni fyziky a výpočtov, kam právo nedosiahne. Staršie vyjadrenie rovnakého cieľa v podobe manifestu pozri Eric Hughes, "A Cypherpunk's Manifesto" (1993), `https://www.activism.net/cypherpunk/manifesto.html`.

[2] Pre open source implementácie, ktoré môžu čitatelia skúmať a používať: GnuPG (gnupg.org) zostáva dominantnou implementáciou OpenPGP; age (age-encryption.org, Filippo Valsorda) je moderný minimalistický nástroj na šifrovanie súborov so silnými predvolenými nastaveniami; Signal (signal.org) je referenčné nasadenie protokolu Signal; OpenMLS (openmls.tech) je hlavná otvorená implementácia MLS. Ďalšie zdroje nad rámec základných textov vyššie: mailing list Cryptography Engineering (blog.cryptographyengineering.com, Matthew Green) a newsletter *Cryptogram* Bruca Schneiera zostávajú aktuálne a prístupné.

[3] Odporúčaná literatúra o kryptografii ako disciplíne a o jej politických dejinách. Základné články z dvadsiateho storočia: Claude E. Shannon, "Communication Theory of Secrecy Systems," *Bell System Technical Journal* 28, č. 4 (1949): 656–715, `https://www.iacr.org/museum/shannon/shannon45.pdf`, založil kryptografiu ako matematickú disciplínu a sformuloval zásadu „nepriateľ pozná systém" (Kerckhoffsov princíp, pôvodne uvedený v Auguste Kerckhoffs, "La cryptographie militaire," *Journal des sciences militaires* 9 [január–február 1883]: 5–38); Whitfield Diffie and Martin Hellman, "New Directions in Cryptography," *IEEE Transactions on Information Theory* IT-22, č. 6 (1976): 644–654, vynašli kryptografiu s verejným kľúčom; Ronald Rivest, Adi Shamir, and Leonard Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," *Communications of the ACM* 21, č. 2 (1978): 120–126, priniesli prvú praktickú schému s verejným kľúčom; David Chaum, "Security Without Identification: Transaction Systems to Make Big Brother Obsolete," *Communications of the ACM* 28, č. 10 (1985): 1030–1044, rozšíril disciplínu na transakcie, ktoré chránia súkromie. K politickému a etickému rámcu: Phillip Rogaway, "The Moral Character of Cryptographic Work," IACR Distinguished Lecture (2015), `http://web.cs.ucdavis.edu/~rogaway/papers/moral-fn.pdf`, tvrdí, že návrh kryptografie je aktom politického inžinierstva; Julian Assange, with Jacob Appelbaum, Andy Müller-Maguhn, and Jérémie Zimmermann, *Cypherpunks: Freedom and the Future of the Internet* (OR Books, 2012), zhromažďuje cypherpunkové politické čítanie tej istej disciplíny; často citovaná formulácia Jona Callasa, že „cryptography is the ultimate form of non-violent direct action" (kryptografia je najvyššou formou nenásilnej priamej akcie), vyjadruje rovnaký postoj z pohľadu praktika, ktorý sa podieľal na vydaní PGP, iMessage a Silent Circle. K dejinám a príbehu: David Kahn, *The Codebreakers: The Story of Secret Writing*, rev. vyd. (Scribner, 1996; orig. 1967), je smerodajné rozsiahle dielo o dejinách kryptografie do polovice dvadsiateho storočia; Simon Singh, *The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography* (Anchor, 2000), pokrýva podobnú látku prístupnejšie. Steven Levy, *Crypto: How the Code Rebels Beat the Government, Saving Privacy in the Digital Age* (Viking, 2001), je rozprávanie o dejinách kryptografie s verejným kľúčom a hnutia cypherpunkerov cez PGP a boj proti čipu Clipper.

[4] AES je špecifikovaný v NIST FIPS 197, *Advanced Encryption Standard* (*AES*) (2001), https://csrc.nist.gov/pubs/fips/197/final. ChaCha20 je špecifikovaný v RFC 8439, *ChaCha20 and Poly1305 for IETF Protocols* (2018), https://www.rfc-editor.org/rfc/rfc8439.

[5] Whitfield Diffie and Martin E. Hellman, "New Directions in Cryptography," *IEEE Transactions on Information Theory* 22, č. 6 (1976): 644-654.

[6] Diffie and Hellman, "New Directions in Cryptography."

[7] Ronald L. Rivest, Adi Shamir, and Leonard M. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," *Communications of the ACM* 21, č. 2 (1978): 120-126.

[8] Victor S. Miller, "Use of Elliptic Curves in Cryptography," *Advances in Cryptology: CRYPTO '85* (1985): 417-426; Neal Koblitz, "Elliptic Curve Cryptosystems," *Mathematics of Computation* 48, č. 177 (1987): 203-209.

[9] Parametre krivky secp256k1 definuje Standards for Efficient Cryptography Group, *SEC 2: Recommended Elliptic Curve Domain Parameters*, verzia 2.0 (2010), https://www.secg.org/sec2-v2.pdf. Referenčná open source implementácia, ktorú používa Bitcoin Core, je libsecp256k1, https://github.com/bitcoin-core/secp256k1.

[10] National Institute of Standards and Technology, *Secure Hash Standard* (*SHS*), FIPS PUB 180-4 (Gaithersburg, MD: NIST, 2015).

[11] K základom digitálnych podpisov pozri Shafi Goldwasser, Silvio Micali, and Ronald L. Rivest, "A Digital Signature Scheme Secure Against Adaptive Chosen-Message Attacks," *SIAM Journal on Computing* 17, č. 2 (1988): 281-308.

[12] „Útok kľúčom za päť dolárov" (angl. „$5 wrench attack") označuje postreh, že fyzický nátlak je často jednoduchší než kryptoanalýza. Pozri komiks XKCD 538, "Security."

[13] Peter W. Shor, "Algorithms for Quantum Computation: Discrete Logarithms and Factoring," *Proceedings 35th Annual Symposium on Foundations of Computer Science* (1994): 124-134.

[14] NIST finalizoval hlavné postkvantové štandardy v auguste 2024 (ML-KEM, ML-DSA, SLH-DSA) a v marci 2025 pridal HQC ako zálohu KEM založenú na kódoch; PQXDH od Signalu (sept. 2023), iMessage PQ3 od Applu (feb. 2024), X25519MLKEM768 v Google Chrome (nov. 2024) a okrajové servery Cloudflare (30 %+ PQ TLS do polovice 2025) sú najväčšie nasadené hybridné implementácie; NSA CNSA 2.0 a britské NCSC cielia na roky 2033–2035 pre migráciu systémov s vysokou hodnotou. NIST Post-Quantum Cryptography Standardization project, https://csrc.nist.gov/projects/post-quantum-cryptography. Finalizované štandardy: FIPS 203 (ML-KEM), https://csrc.nist.gov/pubs/fips/203/final; FIPS 204 (ML-DSA), https://csrc.nist.gov/pubs/fips/204/final; FIPS 205 (SLH-DSA), https://csrc.nist.gov/pubs/fips/205/final. Výber HQC: NIST IR 8547 (marec 2025), https://csrc.nist.gov/pubs/ir/8547/ipd. Špecifikácia Signal PQXDH na https://signal.org/docs/specifications/pqxdh/. Dokumentácia Apple iMessage PQ3 na https://security.apple.com/blog/imessage-pq3/. Oznámenie Google Chrome o postkvantovom TLS na https://blog.chromium.org/2024/05/advancing-our-amazing-bet-on-asymmetric.html a nasadenie X25519MLKEM768 na https://security.googleblog.com/. Telemetria Cloudflare k postkvantovému TLS na https://blog.cloudflare.com/pq-2024/. U.S. National Security Agency CNSA 2.0 suite, https://media.defense.gov/2022/Sep/07/2003071834/-1/-1/0/CSA_CNSA_2.0_ALGORITHMS_.PDF. Usmernenie U.K. National Cyber

Security Centre k postkvantovej migrácii na https://www.ncsc.gov.uk/guidance/pqc-migration-timeline.

[15] Don Johnson, Alfred Menezes, and Scott Vanstone, "The Elliptic Curve Digital Signature Algorithm (ECDSA)," *International Journal of Information Security* 1, č. 1 (2001): 36-63. ECDSA je podpisová schéma používaná v Bitcoine, Ethereu a mnohých implementáciách TLS; využíva násobenie bodov na eliptickej krivke a vytvára podpisy menšie a rýchlejšie než podpisy RSA pri rovnakej úrovni bezpečnosti. Pôvodný štandard je ANSI X9.62 (1998); verzia NIST je FIPS 186-5 (2023), https://csrc.nist.gov/pubs/fips/186-5/final.

[16] Claus-Peter Schnorr, "Efficient Signature Generation by Smart Cards," *Journal of Cryptology* 4, č. 3 (1991): 161-174. Schnorrove podpisy majú lineárnu algebraickú štruktúru, ktorú RSA a ECDSA nemajú: viaceré podpisy možno zlúčiť do jediného podpisu, ktorého veľkosť nezávisí od počtu podpisujúcich (MuSig, MuSig2), a schéma pripúšťa dokázateľne bezpečné konštrukcie v modeli náhodného orákula. Bitcoin pridal natívne Schnorrove podpisy cez BIP 340 (aktivovaný v aktualizácii Taproot, november 2021), https://github.com/bitcoin/bips/blob/master/bip-0340.mediawiki.

[17] Lov K. Grover, "A Fast Quantum Mechanical Algorithm for Database Search," *Proceedings of the 28th Annual ACM Symposium on Theory of Computing* (1996): 212-219. Groverov algoritmus prináša kvadratické zrýchlenie pri hľadaní v neštruktúrovaných problémoch: kvantový počítač prehľadá databázu s N položkami v $O(\sqrt{N})$ krokoch, oproti $O(N)$ pri klasickom počítači. Pri symetrickej kryptografii to znamená polovičnú efektívnu dĺžku kľúča: AES-128 pod Groverovým útokom má zhruba bezpečnosť 64-bitového klasického hľadania. Štandardnou odpoveďou je zdvojnásobiť dĺžky kľúčov (AES-256 namiesto AES-128), čo obnoví pôvodnú bezpečnostnú rezervu. Na rozdiel od Shorovho algoritmu, ktorý RSA a ECC prelamuje asymptoticky, Groverov útok symetrické primitíva a primitíva založené na hašoch nenaruší; vyžaduje väčšie parametre, nie výmenu architektúry.

15

DÔKAZY S NULOVOU ZNALOSŤOU

> *„V kryptografii je dôkaz s nulovou znalosťou metóda, ktorou môže jedna strana dokázať druhej, že dané tvrdenie je pravdivé, bez toho, aby poskytla akúkoľvek inú informáciu než fakt, že tvrdenie skutočne platí.“*
>
> Shafi Goldwasser, Silvio Micali, and Charles Rackoff, "The Knowledge Complexity of Interactive Proof Systems" (1985)[1]

Úvod

Dôkazy s nulovou znalosťou umožňujú jednej strane dokázať, že tvrdenie je pravdivé, bez odhalenia čohokoľvek okrem samotnej pravdivosti tvrdenia. Pre súkromie to mení, čo si overovanie vyžaduje. Tradičné overovanie žiada odhalenie. Overovanie s nulovou znalosťou túto požiadavku odstraňuje.

Kapitola ukazuje, ako dôkazy s nulovou znalosťou fungujú, čo umožňujú a aké majú obmedzenia. Technológia zostáva zložitá, ale jej dôsledky pre súkromie sú jednoduché: overovanie bez bežného sledovania sa môže stať možným.

Na prvé prečítanie stačia tri porovnávacie body: veľkosť dôkazu, dôveryhodné nastavenie a praktická cena vytvorenia a overenia dôkazu. Neskorší prehľad rozlišuje konštrukcie podľa toho, ako odpovedajú na tieto tri otázky.

15.1 Dilema overovania

Tradičné overovanie vyžaduje odhalenie

Zoberme bežné situácie, v ktorých sa niečo overuje. Pri overení totožnosti sa ukazujú identifikačné doklady, takže overovateľ vidí meno, adresu, fotografiu, čísla dokladov a viac údajov, než overenie potrebuje. Pri kontrole veku pri kúpe alkoholu sa odhalí presný dátum narodenia a meno, hoci predajca potrebuje len potvrdenie, že kupujúci je starší ako 21 rokov. Pri overení odbornej kvalifikácie sa odhalí vydávajúca inštitúcia, dátumy, známky a ďalšie údaje z toho istého dokladu. Pri overení bonity sa odhalia zdroje príjmu, vzory míňania, zostatky na účtoch a história transakcií.

V každom z týchto prípadov overenie prezradí viac informácií, než je logicky nutné na jeho účel.

Cena za súkromie

Toto nadmerné odhaľovanie má svoju cenu. Každé overenie rozširuje databázy a postupom času o ľuďoch vznikajú úplné profily zložené z jednotlivo drobných odhalení. Viac údajov znamená viac cieľov; úniky údajov odhalia informácie, ktoré by overovanie zachovávajúce súkromie nikdy nezozbieralo. Odhalené údaje umožňujú odvodzovanie: dátum narodenia a poštové smerovacie číslo často stačia na jednoznačnú identifikáciu človeka. Overovatelia informácie hromadia, ale jednotlivci nemôžu kontrolovať, ako sa používajú, a tým vzniká systematická nerovnováha moci.

Základná dilema

Overovanie vyžaduje informácie, no ich poskytnutím sa súkromie ničí. Tradičné systémy nútia vybrať si: buď sa zúčastniť činností, ktoré si overovanie vyžadujú, alebo zachovať súkromie.

Dôkazy s nulovou znalosťou túto dilemu riešia oddelením toho, čo sa dokazuje, od toho, čo sa odhaľuje.

15.2 Princíp ZK: dokázať bez odhalenia

Interaktívne dôkazy

Pôvodný koncept nulovej znalosti zahŕňa interaktívne protokoly.[1] Dokazovateľ chce presvedčiť overovateľa o pravdivosti tvrdenia, ale bez odhalenia podkladových informácií. Zapoja sa do protokolu, v ktorom overovateľ kladie výzvy a dokazovateľ odpovedá.

Princíp ilustruje analógia s tunelom. Predstavme si tunel v tvare podkovy, ktorého oba konce ústia na tú istú čistinu. Hlboko vnútri, tam, kde sa obe cesty stretávajú, sú dvere s číselným zámkom. Alice tvrdí, že pozná kombináciu. Bob stojí na čistine, odkiaľ vidí oba východy z tunela, ale

dovnútra nevidí. Alice vojde dnu, kým sa Bob pozerá inam. Bob potom zavolá „vyjdi ľavým východom“ alebo „vyjdi pravým východom“. Ak Alice pozná kombináciu, vždy vyhovie, v prípade potreby dvere odomkne. Ak ju nepozná, uviazla na tej strane, z ktorej vošla, a má len päťdesiatpercentnú šancu uhádnuť správne. Po dvadsiatich úspešných kolách je Bob presvedčený, že Alice kombináciu pozná, a pritom sa nikdy nedozvedel, aká je.

Z tejto výmeny sa Bob dozvie len to, že Alice tajomstvo pozná, nie samotné tajomstvo.

Neinteraktívne dôkazy

Moderné aplikácie zvyčajne používajú neinteraktívne dôkazy s nulovou znalosťou (NIZK). Namiesto komunikácie sem a tam vytvorí dokazovateľ jediný dôkaz, ktorý môže overiť ktokoľvek.

Neinteraktívnosť umožňuje praktické použitie: dôkazy možno pripojiť k transakciám alebo uložiť na blockchaine a viaceré strany ich môžu overiť bez účasti dokazovateľa.

Formálne vlastnosti

Systémy dôkazov s nulovou znalosťou majú tri vlastnosti.[2] Úplnosť znamená, že ak je tvrdenie pravdivé, čestný dokazovateľ presvedčí čestného overovateľa. Korektnosť znamená, že ak je tvrdenie nepravdivé, žiadny podvádzajúci dokazovateľ nepresvedčí čestného overovateľa, okrem zanedbateľnej pravdepodobnosti. Nulová znalosť znamená, že overovateľ sa nedozvie nič nad rámec pravdivosti tvrdenia; ani po videní dôkazu z neho nedokáže získať dodatočné informácie. Korektnosť a nulová znalosť sú v napätí: silná korektnosť vyžaduje, aby dôkaz niečo o tvrdení „obsahoval“, nulová znalosť vyžaduje, aby neodhalil nič. Kryptografické konštrukcie dosahujú obe vlastnosti matematickými technikami, ktoré pôsobia takmer ako mágia.

15.3 Druhy: SNARK, STARK, Bulletproofs

Rôzne systémy dôkazov s nulovou znalosťou robia rôzne kompromisy. Hlavné konštrukcie, ktoré sa dnes používajú, sú tieto:

SNARK

Stručné neinteraktívne argumenty znalosti (angl. Succinct Non-interactive Arguments of Knowledge, SNARK) sú dôkazové systémy, ktorých veľkosť dôkazu a náklady na overenie rastú podlineárne, zvyčajne polylogaritmicky, vzhľadom na veľkosť dokazovaného výpočtu.[3] SNARK môže potvrdiť výpočet s miliónmi krokov dôkazom veľkým pár stoviek bajtov, ktorý sa overí za milisekundy. Táto stručnosť umožňuje rollupy na blockchainoch a chránené transakcie: jediný dôkaz konštantnej veľkosti

môže zastúpiť ľubovoľne zložitý výpočet, takže práca overovateľa zostáva nepatrná bez ohľadu na to, aký veľký je dokazovaný výpočet. Praktické SNARK typu Groth16 vytvárajú dôkazy veľké asi 200 bajtov; novšie konštrukcie vymieňajú veľkosť dôkazu za iné vlastnosti vrátane transparentnosti a postkvantovej bezpečnosti.

Tradičné SNARK vyžadujú „dôveryhodné nastavenie“ (angl. trusted setup): počiatočné parametre sa vytvárajú v ceremónii, ktorej kompromitácia by umožnila vyrábať falošné dôkazy. Dnes existujú transparentné SNARK, ktoré túto požiadavku odstraňujú. Systémy ako Spartan[18] a Plonky2[19] dosahujú vlastnosti podobné SNARK bez dôveryhodného nastavenia a využívajú iné kryptografické techniky. Cenou sú zvyčajne o niečo väčšie dôkazy alebo pomalšie vytváranie dôkazov v porovnaní so SNARK s dôveryhodným nastavením.

Väčšina najrozšírenejších systémov SNARK sa opiera o kryptografické predpoklady, ktoré sú zraniteľné voči útokom kvantových počítačov. Zcash používa SNARK pre chránené transakcie (angl. shielded).[4]

STARK

Škálovateľné transparentné argumenty znalosti (angl. Scalable Transparent Arguments of Knowledge, STARK) odstraňujú potrebu dôveryhodného nastavenia.[5] STARK sú transparentné (bez dôveryhodného nastavenia), opierajú sa o minimálne kryptografické predpoklady (hašovacie funkcie), vo všeobecnosti sa považujú za postkvantové a dobre sa škálujú na veľké výpočty. Kompromisom sú väčšie dôkazy (desiatky až stovky kilobajtov) a zložitejšie overovanie.

StarkWare používa STARK pre riešenia škálovania Ethereu.

Bulletproofs

Bulletproofs sú navrhnuté pre dôkazy rozsahu a podobné účely.[6] Nevyžadujú dôveryhodné nastavenie a vytvárajú dôkazy strednej veľkosti, vďaka čomu sú efektívne pre dôkazy rozsahu (dokázanie, že hodnota leží v istom rozsahu, bez jej odhalenia). Overovanie je pomalšie než pri SNARK a ich použitie je užšie než pri SNARK či STARK.

Monero používa Bulletproofs, dnes už Bulletproofs+, predovšetkým na dôkazy rozsahu v rámci dôverných transakcií.

Výber medzi konštrukciami

Konštrukcie sa líšia v niekoľkých rozmeroch. Tradičné SNARK vytvárajú drobné dôkazy (okolo 300 bajtov) s rýchlym overovaním, ale vyžadujú dôveryhodné nastavenie a nie sú odolné voči kvantovým útokom; transparentné SNARK dôveryhodné nastavenie odstraňujú za cenu väčších dôkazov alebo dlhšieho vytvárania dôkazov. STARK sa dôveryhodnému nastaveniu vyhýbajú a vo všeobecnosti sa považujú za postkvantové, no

vytvárajú oveľa väčšie dôkazy (okolo 100 kilobajtov) pri strednej rýchlosti overovania. Bulletproofs stoja uprostred: majú stredne veľké dôkazy (okolo 2 kilobajtov) a bez dôveryhodného nastavenia, hoci overovanie je pomalšie a chýba im odolnosť voči kvantovým útokom.

Správna voľba závisí od požiadaviek aplikácie. Základné vrstvy blockchainov zvyčajne uprednostňujú malé dôkazy, ako sú SNARK, aplikácie vyžadujúce postkvantovú bezpečnosť smerujú k STARK a dôkazy rozsahu v dôverných transakciách často používajú Bulletproofs.

15.4 Aplikácie: Zcash, rollupy, identita

Súkromná kryptomena: Zcash

Zcash implementuje chránené transakcie pomocou SNARK.[7] Používatelia môžu uskutočniť transakciu tak, že obe protistrany aj suma zostanú skryté. Blockchain zaznamená, že prebehla platná transakcia, bez odhalenia jej podrobností.

Dôkaz ukazuje, že vstupné mince existujú a sú nevyčerpané, že odosielateľ má kľúče na míňanie a že hodnoty vstupov a výstupov sú vyrovnané bez dvojitého míňania. Robí to bez odhalenia, ktoré mince sa míňajú alebo kto prijíma prostriedky, a bez odhalenia prevádzanej sumy.

Zcash ukazuje dôkazy s nulovou znalosťou nasadené vo veľkom meradle v nepriateľských podmienkach. Využívanie chránených transakcií zostáva čiastočné a transparentné či selektívne transparentné použitie v praxi stále obmedzuje súkromie.[4] Mnohé burzy vyžadujú pre vklady a výbery transparentné adresy, čo prínosy súkromia podkopáva. Technológia chránenia funguje, ale sieťové efekty a regulačný tlak jej používanie obmedzujú.

Zcash ukazuje aj riziká zložitej kryptografie a potrebu priebežnej údržby. V roku 2019 sa objavila zraniteľnosť v pôvodnom dôkazovom systéme Sprout, ktorá mohla umožniť nezistiteľnú infláciu. Chyba existovala od spustenia; nezistilo sa žiadne zneužitie a aktualizácia Sapling (nasadená v roku 2018) ju opravila ešte pred verejným zverejnením zraniteľnosti. Prax tímu Zcash nasadzovať kryptografické aktualizácie umožnila, aby oprava prišla skôr, než sa o chybe dozvedela verejnosť. Objav ukázal, že aj starostlivo navrhnuté systémy môžu skrývať kritické chyby, a preto je aktívny vývoj protokolu nevyhnutný. Zcash sa dodnes aktualizuje; protokol sa aktívne udržiava a zlepšuje.

Škálovanie blockchainu: validity rollupy

Dôkazy s nulovou znalosťou umožňujú „rollupy“, ktoré zvyšujú priepustnosť blockchainu.[8] Rollup vykoná veľa transakcií mimo reťazca a potom na hlavný reťazec zverejní dôkaz, že všetky vykonania boli platné.

Hlavný reťazec overuje len dôkaz, nie jednotlivé transakcie. Veľa transakcií sa tak stlačí do jedného dôkazu, pričom hlavný reťazec môže overiť správnosť a zachovať dostupnosť údajov, takže sa transakcie dajú znovu zostaviť.

Systémy ako StarkNet a zkSync používajú tento prístup na škálovanie Ethereu.

Identita a poverenia

Dôkazy s nulovou znalosťou umožňujú overovanie identity, ktoré chráni súkromie. Základná myšlienka je, že väčšina situácií vyžaduje dokázať vlastnosť, nie odhaliť podkladové údaje: bar potrebuje vedieť, že ste starší ako 21 rokov, nie váš presný dátum narodenia, a veriteľ potrebuje vedieť, že splácať dokážete, nie celú vašu finančnú históriu. Služba potrebuje vedieť, že ste licencovaný odborník, nie vašu domácu adresu.

Tradičné overovanie spája potrebný dôkaz so zbytočným odhalením. Ukázať vodičský preukaz ako dôkaz veku prezradí meno, adresu, dátum narodenia, číslo preukazu a fotografiu. Každý z týchto údajov vytvára riziko: krádež identity, cielené obťažovanie a vystavenie v prípade úniku z databázy. Overenie splnilo svoj účel, odhalenie ho presiahlo.

Poverenia s nulovou znalosťou tento vzťah obracajú. Pri overení veku možno dokázať, že vek prekračuje prah, bez odhalenia dátumu narodenia; dôkaz ukazuje „dátum narodenia $<$ (dnes $-$ 21 rokov)“ a dátum narodenia samotný nezverejňuje. V dobre navrhnutom systéme sa overovateľ dozvie, čo potrebuje (potvrdený zákonný vek), a nie okolité osobné údaje. Overenie poverenia umožňuje dokázať vlastníctvo platného poverenia (titul, licencia, členstvo) bez odhalenia identifikačných údajov; overovateľ sa dozvie, že poverenie je platné, ale nie to, kto ho drží. Zamestnávateľ môže overiť odbornú licenciu bez toho, aby sa dozvedel domácu adresu kandidáta alebo dátum, kedy licenciu získal. Selektívne odhaľovanie umožňuje dokázať len určité vlastnosti z poverenia s mnohými atribútmi; z vodičského preukazu možno dokázať napríklad len „štát bydliska“ bez odhalenia osobných identifikačných údajov.

Tieto myšlienky realizuje niekoľko projektov. Polygon ID (dnes Privado ID) umožňuje vydávať a overovať poverenia, pri ktorých držitelia môžu vytvárať dôkazy s nulovou znalosťou o vlastnostiach poverenia.[9] Držiteľ poverenia môže dokázať členstvo v skupine alebo splnenie vekovej podmienky a môže tiež ukázať, že má platnú licenciu, bez odhalenia samotného poverenia alebo svojej identity. Systém oddeľuje poverenie, ktoré obsahuje podrobné údaje, od dôkazu, ktorý odhalí len to, čo overovateľ potrebuje.

zkPass volí iný prístup a umožňuje dôkazy s nulovou znalosťou z existujúcich dokumentov Web2.[10] Používatelia môžu dokázať vlastnosti z vodičských preukazov, účtov za energie a finančných záznamov bez toho,

aby tieto dokumenty nahrávali tretej strane. Dôkaz sa vytvára na zariadení používateľa; overovateľ dostane len dôkaz, nie podkladový dokument. Tým sa premosťuje priepasť medzi existujúcou infraštruktúrou identity a overovaním s nulovou znalosťou.

Súčasné požiadavky na „poznaj svojho zákazníka“ (KYC) nútia používateľov odovzdať úplné identifikačné doklady každej službe, ktorá vyžaduje overenie. Každé odhalenie vytvorí databázu, z ktorej môžu údaje uniknúť alebo na ktorú možno vydať súdny príkaz, a potom sa dajú zneužiť. KYC s nulovou znalosťou (ZK-KYC) ponúka alternatívu: dokázať súlad bez opakovaného odhaľovania následným stranám. Používateľ by mohol dokázať „totožnosť overila licencovaná inštitúcia“ bez odhalenia samotnej totožnosti následným službám. Regulačná požiadavka sa splní bez toho, aby sa v každej službe znovu vytvárali úplné databázy identít.

Ako nasadená regulácia to zostáva z veľkej časti špekulatívne. Regulátori zvyknutí na úplné odhalenie sa môžu brániť metódam overovania, ktoré nemôžu skontrolovať. Technická schopnosť však existuje: dá sa splniť regulačný účel a pritom minimalizovať zásah do súkromia. Či regulátori ZK-KYC prijmú, závisí od politických rozhodnutí, nie od technických obmedzení.

Dôsledky pre súkromie presahujú jednotlivé transakcie. Overovanie identity dnes vytvára úplné profily ako vedľajší produkt. Každá kontrola veku a každé predloženie poverenia spolu s overením adresy dopĺňajú dosjé, ktoré ľudí sprevádzajú naprieč kontextmi. Overovanie s nulovou znalosťou toto hromadenie výrazne obmedzuje. Každý dôkaz odhalí len to, čo si dané overenie vyžaduje, a tak zostáva oveľa menej údajov, ktoré by sa dali zhromažďovať naprieč kontextmi.

Nie všetky projekty v tejto oblasti kladú súkromie rovnako vysoko. Worldcoin, dnes World,[11] používa dôkazy s nulovou znalosťou na overenie statusu „jedinečného človeka“, no stále závisí od biometrickej registrácie. Aktuálne materiály projektu tvrdia, že spracovanie biometrických údajov je navrhnuté tak, aby sa vyhol centralizovanej biometrickej databáze, ale systém stále závisí od dôvery v okolitý hardvér, operátorov a návrh registrácie. Technológia súkromie umožňuje; či ho implementácie skutočne poskytujú, závisí od návrhu celého systému.

ZK nad vládnymi dokladmi

Najväčšie nasadenie osvedčovania identity s nulovou znalosťou v roku 2025 beží nad existujúcimi cestovnými dokladmi vydanými štátom. Štandard biometrických pasov ICAO 9303 vkladá podpísaný čip NFC do približne 1,8 miliardy pasov na svete. Čip obsahuje meno držiteľa, dátum narodenia, štátnu príslušnosť a číslo dokladu, všetko podpísané certifikačnou autoritou vydávajúcej krajiny. Podpis bežne overuje zariadenie hraničnej kontroly. Obvod s nulovou znalosťou nad tým istým podpisom

umožňuje mobilnému zariadeniu dokázať konkrétne atribúty z čipu bez odhalenia celého obsahu čipu alebo identity držiteľa.

Self (self.xyz, predtým Proof of Passport) je vlajkovým produkčným nasadením. Používa skenovanie NFC priamo na zariadení a obvod ZK nad objektom Document Security Object a vytvára dôkazy veku, štátnej príslušnosti alebo toho, že osoba nie je na sankčnom zozname. Projekt uvádza viac ako sto miliónov overení naprieč nasadeniami vrátane integrácií s Googlom a s blockchainovými aplikáciami, ktoré osvedčenie prijímajú ako primitív odolnosti voči útokom typu Sybil. Porovnateľné konštrukcie bežia na Aztec L2 (zkPassport), v infraštruktúre protiputinovského referenda v Rusku (Freedom Tool od Rarimo) a nad záznamami indického systému Aadhaar (Anon Aadhaar).[12]

Tento prístup využíva existujúcu identifikačnú infraštruktúru štátu proti jej sledovacím použitiam. Vláda doklad podpísala, aby pri hraničnej kontrole overila držiteľa; obvod ZK nad podpisom využije overenie pravosti bez identifikácie, a to je presne to oddelenie, o ktorom kapitola tvrdí, že ho nulová znalosť umožňuje. Protiťahom štátu je zmeniť vydávanie dokladov: zmeniť podpisové schémy, skrátiť životnosť certifikátov alebo pridať požiadavky na osvedčenie, ktoré obvod nevie splniť bez toho, aby odhalil viac než dnes. Prístup funguje dnes preto, že v obehu sú už stovky miliónov dokladov s podpismi, ktoré obvody vedia overiť, a túto nainštalovanú základňu nemožno rýchlo odvolať.

Privacy Pass a anonymné poverenia vo veľkom

Privacy Pass je protokol anonymných poverení štandardizovaný IETF (RFC 9576 a 9577), ktorý sa dodáva v iOS 16 a novších ako Apple Private Access Tokens.[13] Konštrukcia je slepý podpis nad osvedčením: poskytovateľ identity (Apple) osvedčí, že zariadenie je skutočný používateľ a nie bot, a overovateľ (Cloudflare alebo Fastly) osvedčenie prijme bez toho, aby sa dozvedel, ktorého zariadenia sa týka. Slepý podpis bráni overovateľovi prepájať jednotlivé požiadavky. Osvedčenie sa týka integrity zariadenia v jednom okamihu, nie identity používateľa, jeho správania ani trvalej aktivity.

Apple Private Access Tokens sú aktívne na stovkách miliónov zariadení Apple a Cloudflare ich prijíma namiesto CAPTCHA na významnej časti webu. Žiadne predchádzajúce nasadenie anonymných poverení sa tomuto rozsahu nepriblížilo. Neprepojiteľnosť, ktorú slepý podpis voči overovateľovi poskytuje, je skutočná, no osvedčenie, na ktorom systém stojí, vydáva jediná korporácia, ktorej účasť umožňuje takýto rozsah. Masové nasadenie anonymných poverení sa uskutočnilo cez centralizovaného osvedčovateľa, nie okolo neho.

Chránené fondy ZK na reťazcoch s inteligentnými zmluvami

Chránené fondy (angl. shielded pools) na reťazcoch s inteligentnými zmluvami sa od roku 2023 presunuli z výskumu do produkcie. Railgun beží na Ethereu, BSC, Polygone a Arbitrume ako fond na ochranu súkromia, do ktorého sa vstupuje dobrovoľne, a používa SNARK Groth16.[14] Aztec Network funguje ako L2 so súkromím ako predvolenou voľbou, kde samotné vykonávacie prostredie súkromie zachováva a selektívne odhaľovanie si riadi každý používateľ. Privacy Pools, ktoré v roku 2023 navrhol Buterin so spoluautormi, rozširujú architektúru zmiešavača vkladov Tornado Cash o asociačné množiny: používateľ dokáže členstvo v podmnožine vkladov fondu, ktorá neobsahuje vklady, ktoré chce používateľ z dôvodov súladu s reguláciou vylúčiť, a dôkaz neprezradí nič o tom, ktorý vklad schválenej podmnožiny je používateľov.[15] Produkčným vzorom je nasadenie 0xbow.io.

Tri návrhy sa líšia v tom, koľko súkromia poskytujú predvolene a v tom, ako sa súkromie spája s tlakom na súlad s reguláciou. Railgun je fond s dobrovoľným vstupom, kde sa musia používatelia sami rozhodnúť svoje prostriedky chrániť. Aztec je chránený predvolene. Privacy Pools sú návrh, ktorý najpriamejšie reaguje na kritiku Tornado Cash: súkromie bez nepreniknuteľnosti voči konkrétnemu zoznamu vylúčených vkladov, pričom zoznam vylúčení si volí používateľ, nie nijaký jediný orgán. Konštrukcia ukazuje, že primitív s nulovou znalosťou možno použiť na rozlíšenie trestného použitia od oprávneného bez toho, aby rozlišovanie vykonával centrálny orgán, čo je vlastnosť, ktorú si staršie návrhy fondov na ochranu súkromia nenárokovali.

Nasadené a špekulatívne aplikácie

Medzi aktuálne nasadené a fungujúce aplikácie patria chránené transakcie Zcash a škálovanie Ethereu a podobných platforiem pomocou rollupov. Nástroje na identitu a osvedčovanie založené na nulovej znalosti sa za posledné dva roky presunuli z ukážok do produkcie pre niekoľko konkrétnych vzorov. Osvedčovanie členstva v skupine, ktoré účastníkovi umožňuje dokázať členstvo v registrovanej skupine bez odhalenia, ktorý z členov je, sa nasadilo na podujatiach konferenčného rozsahu pri vstupenkách, hlasovaní a riadení prístupu; Semaphore a Zupass sú nasadené príklady tohto vzoru. Vytváranie peňaženiek na základe OAuth sa nasadilo na aspoň jednom produkčnom blockchaine cez zkLogin, ktorý používateľovi umožňuje odvodiť peňaženku z existujúceho prihlásenia do účtu Google alebo Apple bez toho, aby poskytovateľ účtu zistil, ktorá peňaženka sa odvodila. Selektívne odhaľovanie s nulovou znalosťou nad štandardnými overiteľnými povereniami bolo implementované v úzkych nasadeniach vrátane osvedčení veku a overenia odborných licencií.[16]

Univerzálne overiteľné výpočty a hlasovanie s nulovou znalosťou vo veľkom rozsahu spolu s úplnými systémami súladu s reguláciou, ktoré chránia súkromie, zostávajú špekulatívne v zmysle tejto knihy: ich praktické obmedzenia stále vylučujú široké nasadenie. Do produkcie sa vo všetkých prípadoch dostal vzor úzky, kde sa konkrétne tvrdenie osvedčuje pri konkrétnom modeli dôvery a konkrétnom výkone. Výskumom zostáva vzor všeobecný. Pre rámec tejto knihy je dôležitý smer pohybu: kategória produkčných nasadení sa rozširuje, výkonnostný rozsah rastie a primitíva, ktoré výskumná komunita vyvinula pred desiatimi rokmi, dnes nesú skutočnú záťaž.

Technológia je skutočná a nasadená v dôležitých aplikáciách, ale zrelosť sa podľa prípadu použitia výrazne líši. Čitateľ, ktorý uvažuje, či sa na konkrétny systém s nulovou znalosťou spoľahnúť pre konkrétny účel, by mal posudzovať zrelosť práve toho systému, nie zrelosť celého odboru.

15.5 Ekonomické dôsledky: overovanie ako služba

Keď sa dôkaz dá oddeliť od odhalenia, overovanie samo sa stane osobitnou službou. Vytvorenie zložitých dôkazov si vyžaduje veľa výpočtov, hoci overenie je rýchle, a to otvára priestor pre špecializovanú infraštruktúru na dokazovanie. Kompromis pre súkromie je, že dokazovateľ, ktorý vidí svedka (angl. witness), môže znovu zaviesť problém dôvery, ktorý mal dôkaz zúžiť; trhy s overovaním zapadajú do rámca tejto knihy len vtedy, keď spracovanie svedka zostáva lokálne, je rozdelené medzi viac strán alebo je chránené hardvérom, ktorý dokazovateľovi bráni získať podkladové údaje. Tam, kde tieto podmienky platia, môžu systémy s nulovou znalosťou znížiť náklady na overovanie v celom hospodárstve: súlad s reguláciou bez vystavenia obchodných podrobností, overiteľné poverenia bez réžie pri kontrole podvodov, súhrnné štatistiky bez rutinného zostavovania dosjé. Prínosy sú dnes úzke a v čase smerujú k rastu; overovanie nemusí vždy znamenať sledovanie.

15.6 Obmedzenia

Požiadavky na dôveryhodné nastavenie

Mnohé konštrukcie SNARK vyžadujú „dôveryhodné nastavenie“: úvodnú ceremóniu, ktorá vygeneruje parametre, ktoré potom používajú všetky budúce dôkazy a overenia. Ak je ceremónia kompromitovaná (ak si niekto ponechá „toxický odpad“ použitý na vytvorenie parametrov), ten môže vytvárať falošné dôkazy, ktoré sa overia ako správne.

Dôveryhodné nastavenia existujú v niekoľkých variantoch s rôznymi kompromismi. Nastavenia pre jednotlivé obvody, aké používal pôvodný systém Zcash Sprout, vyžadujú novú ceremóniu pre každú aplikáciu ale-

bo zmenu obvodu; akákoľvek úprava dokazovaného výpočtu znamená zahodiť staré parametre a spustiť nové dôveryhodné nastavenie. Univerzálne nastavenia, ako v systémoch PLONK[20] a Marlin,[21] generujú parametre, ktoré fungujú pre ľubovoľný obvod do určitej veľkosti; jedna ceremónia môže slúžiť mnohým aplikáciám, hoci samotná ceremónia zostáva predpokladom dôvery. Transparentné nastavenia požiadavku odstraňujú úplne: STARK a niektoré novšie SNARK, napríklad Spartan,[18] odvodzujú svoje parametre z verejnej náhodnosti, nepotrebujú ceremóniu a nezanechávajú toxický odpad, ktorý by si niekto mohol ponechať.

Medzi zmierňujúce opatrenia pre systémy vyžadujúce dôveryhodné nastavenie patria ceremónie s bezpečným výpočtom viacerých strán, v ktorých stačí, aby bol čestný jediný účastník, a ceremónie Powers of Tau s tisíckami účastníkov. Aplikácie s prísnymi požiadavkami na dôveru však môžu uprednostniť transparentné konštrukcie napriek ich väčším dôkazom.

Dôveryhodné nastavenie je skutočné obmedzenie, ktoré zodpovedné implementácie berú vážne.

Výpočtová náročnosť

Vytváranie dôkazov je výpočtovo drahé. Jednoduché dôkazy trvajú sekundy, zložité môžu trvať minúty alebo hodiny. To obmedzuje aplikácie, kde záleží na latencii.

Overovanie je rýchle (často milisekundy), no úzkym hrdlom je vytváranie dôkazu. Hardvérová akcelerácia (GPU, FPGA, ASIC) môže pomôcť, ale základnú výpočtovú cenu neodstráni.

Zložitosť implementácie

Systémy dôkazov s nulovou znalosťou sú matematicky sofistikované a chyby v implementácii môžu zničiť bezpečnostné vlastnosti, ktoré má matematika zaručovať. Zlyhanie korektnosti dovolí, aby sa neplatné dôkazy overili, takže sfalšované tvrdenia prejdú ako pravdivé; zlyhanie nulovej znalosti prezradí informácie samotným dôkazom, čím sa zničí súkromie, ktoré systém má poskytovať. Nenápadné chyby v implementácii oboch druhov postihli nasadené systémy a často zostali roky nezistené, kým sa na ne neprišlo.

Aj audit je preto ťažký. Len málo inžinierov dokáže kompetentne posúdiť implementácie ZK na úrovni potrebnej na zachytenie takýchto chýb a nedostatok kvalifikovaných recenzentov sústreďuje dôveru do malej komunity, ktorej čas je sám úzkym hrdlom pre počet systémov, ktoré možno zmysluplne preskúmať.

Čo dôkazy ZK nevyriešia

Kapitola 14 rozoberala, čo kryptografia vo všeobecnosti nevyrieši: bezpečnosť koncového zariadenia, vystavenie metadát, fyzický nátlak a pravosť kľúča. Dôkazy s nulovou znalosťou tieto obmedzenia zdedia a pridávajú ďalšie, špecifické pre ZK.

Najvýznamnejší je problém „smeti dnu, smeti von“, často nazývaný problém orákula. Dôkaz s nulovou znalosťou overuje, že výpočet bol správne vykonaný nad danými vstupmi. Nehovorí nič o tom, či tieto vstupy boli pravdivé. Aplikácia, ktorá tvrdí „tento úver je zabezpečený kolaterálom“ a opiera sa pritom o dôkaz ZK, dokázala len to, že výpočet bol správne vykonaný nad cenovými údajmi, ktoré dostala; ak boli tieto údaje zastarané, zmanipulované alebo nepravdivé, dôkaz je bezcenný. Žiadna kryptografická sofistikovanosť nepremostí priepasť medzi „správne vypočítané“ a „pravdivé“. Dokázať, že orákulové údaje boli spracované správne, nedokazuje, že orákulum poskytlo presné údaje. Toto obmedzenie je zásadné: dôkazy ZK overujú výpočet, nie realitu.

Nulová znalosť pridáva zložitosť, ktorá môže byť zbytočná. Ak problém overovania nevyžaduje skrývanie informácií, stačia jednoduchšie kryptografické nástroje. Pridanie mechanizmov ZK tam, kde nie sú potrebné, zväčšuje útočnú plochu a sťažuje implementáciu bez zodpovedajúceho prínosu.

Zhrnutie kapitoly

Dôkazy s nulovou znalosťou oddeľujú overovanie od odhalenia. Úplnosť, korektnosť a nulová znalosť spolu zaručujú, že pravdivé tvrdenia možno dokázať, nepravdivé nie a dôkaz neodhalí nič nad rámec pravdivosti tvrdenia; overovateľ sa dozvie, čo potrebuje, bez prístupu k podkladovým údajom. Primitív rieši dilemu overovania, ktorá by inak nútila voliť medzi účasťou a súkromím. Rôzne konštrukcie robia rôzne kompromisy. SNARK vytvárajú drobné dôkazy s rýchlym overovaním, ale tradične vyžadujú dôveryhodné nastavenie a sú zraniteľné voči kvantovému útoku; transparentné SNARK nastavenie odstraňujú za cenu väčších dôkazov alebo dlhšieho vytvárania dôkazov. STARK sa tiež vyhýbajú dôveryhodnému nastaveniu a poskytujú odolnosť voči kvantovým útokom, no vytvárajú oveľa väčšie dôkazy. Bulletproofs stoja uprostred a hodia sa na dôkazy rozsahu. Vhodnú voľbu určujú požiadavky aplikácie.

Do produkcie sa dostali konkrétne vzory. Chránené transakcie Zcash a validity rollupy na škálovanie blockchainu fungujú. Osvedčovanie členstva v skupine cez Semaphore a Zupass beží na podujatiach konferenčného rozsahu, zkLogin od Sui odvodzuje peňaženky z prihlásení OAuth bez toho, aby poskytovateľ vedel o odvodení, a overiteľné poverenia W3C podporujú selektívne odhaľovanie v úzkych nasadeniach pri kontrole ve-

ku a odborných licencií. Obvody s nulovou znalosťou nad podpismi pasov ICAO 9303 cez Self a príbuzné projekty zvládajú stovky miliónov overení nad identitnou infraštruktúrou, ktorú vydal sám štát. Privacy Pass sa dodáva ako Apple Private Access Tokens na stovkách miliónov zariadení so systémom iOS. Railgun, Aztec a Privacy Pools nesú chránené transakcie na reťazcoch s inteligentnými zmluvami, pričom konštrukcie s asociačnými množinami riešia obavy zo súladu s reguláciou, ktoré staršie návrhy fondov neriešili.

Univerzálne overiteľné výpočty a ZK-KYC v širokom hospodárskom meradle zostávajú špekulatívne. Problém orákula obmedzuje každú aplikáciu, ktorá závisí od vonkajších údajov: dôkaz ZK overuje, že výpočet bol vykonaný správne nad danými vstupmi, nie že vstupy boli pravdivé. Kategória produkčných nasadení sa rozširuje, výkonnostný rozsah rastie a primitíva vyvinuté vo výskume pred desiatimi rokmi dnes nesú skutočnú záťaž, no zrelosť sa podľa prípadu použitia výrazne líši a čitateľ, ktorý posudzuje konkrétny systém, by mal posudzovať práve ten systém, nie celý odbor. Súkromie na komunikačnej a peňažnej vrstve, ktoré dôkazy ZK dopĺňajú, patrí do kapitol 17 a 20.[17]

Poznámky

[1] Shafi Goldwasser, Silvio Micali, and Charles Rackoff, "The Knowledge Complexity of Interactive Proof Systems," *SIAM Journal on Computing* 18, č. 1 (1989): 186-208.

[2] Prístupný úvod k dôkazom s nulovou znalosťou pozri Matthew Green, "Zero Knowledge Proofs: An Illustrated Primer," *A Few Thoughts on Cryptographic Engineering* (2014).

[3] Jens Groth, "On the Size of Pairing-Based Non-interactive Arguments," *Advances in Cryptology: EUROCRYPT 2016* (2016): 305-326.

[4] Zcash, `https://z.cash`, je kryptomena zachovávajúca súkromie, spustená v októbri 2016 a odvodená z protokolu Zerocash opísaného v Eli Ben-Sasson et al., "Zerocash: Decentralized Anonymous Payments from Bitcoin," *IEEE Symposium on Security and Privacy* (2014), `https://eprint.iacr.org/2014/349`. Chránené transakcie Zcash používajú zk-SNARK (pôvodne BCTV14, neskôr Groth16, od aktualizácie NU5 v roku 2022 Halo 2, ktorá odstránila dôveryhodné nastavenie) na dôkaz platnosti transakcie bez odhalenia odosielateľa, príjemcu ani sumy. Protokol vyvíja Electric Coin Company (`https://z.cash`) so Zcash Foundation (`https://zfnd.org`) ako nezávislým protipólom vo verejnom záujme. K širšiemu priestoru návrhov kryptomien zachovávajúcich súkromie: Monero (`https://www.getmonero.org`) volí odlišný prístup, jeho záruky anonymity zabezpečujú kruhové podpisy a skryté adresy; pozri Shen Noether et al., "Ring Confidential Transactions," *Ledger* 1 (2016), `https://ledgerjournal.org/ojs/ledger/article/view/34`. Mimblewimble (implementovaný v Grin a Beam) a prístupy založené na CoinJoin na Bitcoine (Wasabi, JoinMarket) sú ďalšie hlavné rodiny.

[5] Eli Ben-Sasson et al., "Scalable, Transparent, and Post-Quantum Secure Computational Integrity," *CRYPTO 2018* (2018).

[6] Benedikt Bünz et al., "Bulletproofs: Short Proofs for Confidential Transactions and More," *IEEE Symposium on Security and Privacy* (2018): 315-334.

[7] Protokol Zerocash: úplnú citáciu a podrobnosti o nasadení Zcash pozri poznámku 4 vyššie.

[8] K návrhom rollupov pozri Vitalik Buterin, "An Incomplete Guide to Rollups," *Ethereum Blog* (2021). Dve najväčšie nasadenia ZK-rollupov na Ethereu sú StarkNet (`https://www.starknet.io/`, vyvíja ho StarkWare) a zkSync (`https://zksync.io/`, vyvíja ho Matter Labs); obe používajú dôkazy platnosti na stlačenie veľkých dávok transakcií do jediného dôkazu v reťazci. Dokumentácia StarkNet na `https://www.starknet.io/`; dokumentácia zkSync na `https://zksync.io/`. Obe používajú dôkazy platnosti na stlačenie veľkého počtu transakcií do jediného dôkazu v reťazci.

[9] Dokumentácia Polygon ID (premenovaný na Privado ID) na `https://docs.privado.id/`. Pozri tiež "Introducing Polygon ID, Zero-Knowledge Identity for Web3," Polygon Technology Blog (2022), a Identity Foundation, "Guest Blog: Polygon ID: Verifiable Credentials Meet Web3."

[10] Dokumentácia zkPass na `https://docs.zkpass.org/`. zkPass používa Three-Party TLS (3P-TLS) a bezpečný výpočet viacerých strán (MPC), aby umožnil dôkazy s nulovou znalosťou z údajov webových stránok cez HTTPS bez odhalenia pôvodných dokumentov.

[11] Worldcoin (premenovaný na World, `https://world.org/`) používa biometrickú registráciu skenom dúhovky na vydanie World ID, dôkazu s nulovou znalosťou o statuse jedinečného človeka. Projekt založil Sam Altman; prevádzkovateľom je Tools for Humanity. Model súkromia závisí od dôvery v hardvér Orb a v operátora registrácie; technická architektúra na `https://whitepaper.worldcoin.org/`. Kritickú analýzu pozri vyšetrovania ochrany údajov španielskych (AEPD) a keňských regulátorov v rokoch 2023-2024.

[12] Self (predtým Proof of Passport), zkPassport, Rarimo a Anon Aadhaar používajú obvody s nulovou znalosťou nad podpismi NFC pasov ICAO 9303 a podpismi RSA systému Aadhaar na vytváranie osvedčení identity so selektívnym odhaľovaním z poverení vydaných štátom; Freedom Tool od Rarimo v roku 2024 prevádzkoval produkčné nasadenie pre referendum ruskej opozície. Self Protocol (predtým Proof of Passport), `https://self.xyz/`, so zdrojovým kódom na `https://github.com/selfxyz`. zkPassport, `https://zkpassport.id/`. Rarimo a Freedom Tool, `https://rarimo.com/` a `https://freedomtool.org/`. Anon Aadhaar, projekt Privacy and Scaling Explorations, `https://pse.dev/projects/anon-aadhaar`, so zdrojovým kódom na `https://github.com/anon-aadhaar`. Špecifikácia ICAO Doc 9303 Machine Readable Travel Documents, `https://www.icao.int/publications/Documents/9303_p11_cons_en.pdf`. K širšej kategórii osvedčovania ZK nad existujúcimi podpismi pozri akademickú líniu od Jens Groth, Rafail Ostrovsky, and Amit Sahai, "Perfect Non-Interactive Zero Knowledge for NP," *EUROCRYPT 2006*, pokračujúcu cez Noir, Circom a vývojárske súpravy nástrojov dôkazových systémov uvedené v poznámke 16.

[13] Privacy Pass (IETF RFC 9576 a 9577) je štandard anonymných poverení a Apple Private Access Tokens sú jeho najväčším jednotlivým produkčným nasadením; rozsah architektúry závisí od toho, že Apple pôsobí ako centralizovaný osvedčovateľ. RFC 9576 (Privacy Pass Architectural Framework), Alex Davidson, Jana Iyengar, Christopher A. Wood, `https://datatracker.ietf.org/doc/rfc9576/`. RFC 9577 (Privacy Pass Issuance Protocols), Steven Valdez, `https://datatracker.ietf.org/doc/rfc9577/`. Dokumentácia Apple Private Access Tokens na `https://developer.apple.com/documentation/authenticationservices/privacy_access_tokens`, s integráciou Cloudflare zdokumentovanou na `https://blog.cloudflare.com/eliminat`

ing-captchas-on-iphones-and-macs-using-new-standard/. Staršie výskumné práce Cloudflare o Privacy Pass na https://blog.cloudflare.com/privacy-pass-v3/ a Alex Davidson, Ian Goldberg, Nick Sullivan, George Tankersley, and Filippo Valsorda, "Privacy Pass: Bypassing Internet Challenges Anonymously," *PoPETs* 2018, č. 3 (2018).

[14] Dokumentácia Railgun na https://railgun.org/, so špecifikáciou protokolu na https://docs.railgun.org/. Dokumentácia Aztec Network na https://aztec.network/, s programovacím jazykom Noir zameraným na súkromie na https://noir-lang.org/. K porovnaniu s architektúrou chráneného fondu Zcash rozoberanou v poznámke 4 pozri dokumentáciu Aztec "Private Execution Environment" na https://docs.aztec.network/aztec/concepts/.

[15] Vitalik Buterin, Ameen Soleimani, Jacob Illum, Matthias Nadler, Fabian Schär, and Ameen Soleimani, "Blockchain Privacy and Regulatory Compliance: Towards a Practical Equilibrium" (2023), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4563364, predstavuje konštrukciu asociačnej množiny. Nasadenie 0xbow je na https://0xbow.io/, so zdrojovým kódom na https://github.com/0xbow-io. K predchodcovi Tornado Cash, na ktorého Privacy Pools reagujú, pozri *Van Loon v. Department of the Treasury*, 122 F.4th 549 (5th Cir. 2024), a kapitolu 13 pre analýzu právnych fáz, s ktorou sa konštrukcia prekrýva.

[16] Semaphore (dôkazy členstva v skupine) a Zupass (vstupenky a poverenia v rozsahu podujatí) sú nasadené príklady osvedčovania skupín na báze ZK; zkLogin od Sui umožňuje používateľom odvodiť peňaženky z prihlásenia OAuth bez toho, aby poskytovateľ OAuth vedel o odvodení; selektívne odhaľovanie overiteľných poverení je v úzkej produkcii pre kontrolu veku a odborné licencie. Semaphore, https://semaphore.pse.dev/, so zdrojovým kódom na https://github.com/semaphore-protocol/semaphore. Zupass (rámec PCD), https://pcd.dev/ a https://zupass.org/. Dokumentácia Mina PCD / Proof-Carrying Data na https://pcd.dev/docs. zkLogin na Sui, https://docs.sui.io/concepts/cryptography/zklogin, so špecifikáciou na https://sui.io/zklogin. World Wide Web Consortium Verifiable Credentials Data Model, https://www.w3.org/TR/vc-data-model/. Štandard mobilného vodičského preukazu ISO/IEC 18013-5, https://www.iso.org/standard/69084.html. K nasadeniam osvedčovania veku a odborných licencií pozri Privado ID, https://docs.privado.id/, a referenčnú implementáciu európskej digitálnej peňaženky identity eIDAS 2.0 na https://github.com/eu-digital-identity-wallet.

[18] Srinath Setty, "Spartan: Efficient and General-Purpose zkSNARKs without Trusted Setup," *Advances in Cryptology: CRYPTO 2020* (2020): 704-737, https://eprint.iacr.org/2019/550. Spartan využíva protokol sum-check nad multilineárnymi rozšíreniami, aby dosiahol transparentné SNARK bez dôveryhodného nastavenia a bez toxického odpadu; bezpečnosť sa opiera o predpoklad diskrétneho logaritmu v grupe prvočíselného rádu. Zložitosť dokazovania je O(n log n) pre aritmetické obvody veľkosti n. Spartan je základom dokazovateľa Nova (schéma skladania) od Microsoftu (https://github.com/microsoft/Nova) a ovplyvnil neskoršie návrhy transparentných SNARK.

[19] Polygon Zero Team, "Plonky2: Fast Recursive Arguments with PLONK and FRI" (2022), https://github.com/0xPolygonZero/plonky2/blob/main/plonky2/plonky2.pdf. Plonky2 spája aritmetizáciu PLONK s univerzálnym nastavením a FRI (Fast Reed-Solomon Interactive Oracle Proofs of Proximity) ako schému polynomiálnych záväzkov, čím odstraňuje párovania na eliptických krivkách, ktoré bežné SNARK vyžadujú. Výsledkom je transparentný SNARK s časmi rekurzívnej kompozície dôkazov pod 170 milisekúnd na spotrebiteľskom hardvéri; Polygon ho používa ako dokazovací backend pre

svoje zkEVM a ďalšiu infraštruktúru škálovania. Predpoklady FRI založené len na hašovacích funkciách robia Plonky2 pravdepodobne postkvantovým, hoci formálne dôkazy postkvantovej bezpečnosti pre celú konštrukciu zostávajú otvorenou výskumnou otázkou.

[20] Ariel Gabizon, Zachary J. Williamson, and Oana Ciobanu, "PLONK: Permutations over Lagrange-Bases for Oecumenical Noninteractive Arguments of Knowledge," *IACR ePrint* 2019/953 (2019), `https://eprint.iacr.org/2019/953`. PLONK zaviedol univerzálny a aktualizovateľný štruktúrovaný referenčný reťazec: jedna ceremónia dôveryhodného nastavenia vytvorí parametre použiteľné pre ľubovoľný aritmetický obvod do danej veľkosti a parametre môžu aktualizovať ďalší účastníci bez opakovania ceremónie od začiatku. Vďaka tomu sa SNARK s univerzálnym nastavením stali praktickými pre ekosystémy ako Ethereum, kde veľa nezávislých aplikácií zdieľa dokazovaciu infraštruktúru; aritmetizácia PLONK je dnes základom Halo 2, UltraPLONK a mnohých backendov zkEVM.

[21] Alothman Zac, Mary Maller, and Pratyush Mishra, "Marlin: Preprocessing zkSNARKs with Universal and Updatable SRS," *Advances in Cryptology: EUROCRYPT 2020* (2020): 738-768, `https://eprint.iacr.org/2019/1047`. Marlin zovšeobecňuje prístup univerzálneho nastavenia z PLONK pomocou odlišnej aritmetizácie (R1CS nad univerzálnym SRS založeným na polynomiálnych záväzkoch) a poskytuje prvý formálny dôkaz knowledge-soundness pre univerzálny zkSNARK s predspracovaním. Konštrukcia je základom jazyka Leo blockchainu Aleo a vykonávacieho prostredia snarkVM, ktoré používajú Marlin ako dokazovací backend pre všeobecný súkromný výpočet.

[17] Odporúčaná literatúra o dôkazoch s nulovou znalosťou. Základné články sú Shafi Goldwasser, Silvio Micali, and Charles Rackoff, "The Knowledge Complexity of Interactive Proof-Systems," *SIAM Journal on Computing* 18, č. 1 (1989): 186–208 (pôvodne STOC 1985), `https://people.csail.mit.edu/silvio/Selected%20Scientific%20Papers/Proof%20Systems/The_Knowledge_Complexity_Of_Interactive_Proof_Systems.pdf`; a Oded Goldreich, Silvio Micali, and Avi Wigderson, "Proofs That Yield Nothing But Their Validity" (1991), ktorý rozšíril ZK na všetky problémy triedy NP. K učebnicovému spracovaniu: Oded Goldreich, *Foundations of Cryptography: Volume 1, Basic Tools* (Cambridge University Press, 2001), kapitola 4, a *Volume 2, Basic Applications* (2004), kapitola 4, sú kanonické referencie. Jonathan Katz and Yehuda Lindell, *Introduction to Modern Cryptography*, 3. vyd. (CRC Press, 2020), pokrýva ZK na úrovni postgraduálneho kurzu. Z praktickej stránky je Justin Thaler, *Proofs, Arguments, and Zero-Knowledge* (Now Publishers, 2023), `https://people.cs.georgetown.edu/jthaler/ProofsArgsAndZK.pdf`, moderným odkazom na konštrukciu SNARK/STARK. Matthew Green, "Zero Knowledge Proofs: An Illustrated Primer" na `https://blog.cryptographyengineering.com/2014/11/27/zero-knowledge-proofs-illustrated-primer/` je najlepším prístupným vysvetlením. K SNARK konkrétne je séria zkSNARK od Vitalika Buterina na `https://vitalik.eth.limo/general/2016/12/10/qap.html` priateľská k praktikom. Kurikulum 0xPARC na `https://0xparc.org` je komunitný zdroj na praktické učenie programovania ZK. Z praktických nástrojov sú Circom (`https://docs.circom.io`), Halo 2 (`https://zcash.github.io/halo2/`), arkworks-rs (`https://github.com/arkworks-rs`) a Nova (`https://github.com/microsoft/Nova`) referenčnými implementáciami pre vývoj SNARK; pre STARK je hlavnou verejnou súpravou nástrojov Cairo od StarkWare (`https://www.cairo-lang.org`). Na strane identity a poverení definujú W3C Verifiable Credentials Data Model (`https://www.w3.org/TR/vc-data-model/`) a Hyperledger AnonCreds (`https://github.com/hyperledger/anoncreds-spec`) štandardy, na ktoré sa zameriava veľká časť práce o identite s ZK.

16
VÝPOČTY NAD TAJOMSTVAMI

„Problém súkromia nespočíva v tom, ako skryť údaje, ale v tom, ako údaje využívať bez ich odhalenia.“

Andrew C. Yao, „Protocols for Secure Computations“ (1982)[1]

Úvod

Predchádzajúca kapitola sa venovala dôkazom s nulovou znalosťou. Jedna strana nimi dokáže, že tvrdenie je pravdivé, a neprezradí, prečo. Táto kapitola sa zaoberá príbuznou a doplnkovou schopnosťou: vykonať výpočet nad tajnými vstupmi tak, aby sa o nich nikto z účastníkov nič nedozvedel.

Dôkaz s nulovou znalosťou pracuje s výsledkom, ktorý už existuje. Výpočet, ktorého správnosť sa dokazuje, niekto niekde vykonal nad vstupmi, ktoré boli niekde dostupné. Dôkaz potvrdzuje, čo sa vypočítalo, nie to, kto videl vstupy. Nulová znalosť je overovací primitív (základný stavebný prvok).

Výpočty nad tajomstvami sú vykonávací primitív. Odpovedajú na inú otázku: dá sa výpočet vykonať, keď nikto nesmie vidieť vstupy? Dá, a to v troch architektonických rodinách, ktoré sa v poslednom desaťročí dostali do praktického nasadenia. Úplne homomorfné šifrovanie počíta priamo nad šifrovým textom. Bezpečný výpočet viacerých strán rozdelí výpočet medzi účastníkov tak, že nikto nevidí celý vstup. Dôveryhodné prostredia na vykonávanie kódu spúšťajú výpočet v hardvérovej enkláve, ktorej obsah je nepreniknuteľný pre operačný systém aj pre vlastníka hardvéru.

Tieto rodiny dôkazy s nulovou znalosťou dopĺňajú, nekonkurujú im. Systém, ktorý chráni súkromie od začiatku do konca, zvyčajne používa výpočty nad tajomstvami na prácu so súkromnými údajmi a nulovú znalosť

na dôkaz, že výsledok vznikol poctivo. Kapitola 15 sa venovala dokazovacej polovici tohto reťazca. Táto kapitola sa venuje vykonávacej polovici.

16.1 Rozdiel medzi overením a vykonaním

Predstavme si hlasovací systém, v ktorom musí zostať voľba každého voliča súkromná a spočítaný výsledok musí byť verejne overiteľný. Vstupy (jednotlivé hlasovacie lístky) musia ostať tajné. Výstup (súčet hlasov) sa musí dať vypočítať aj overiť.

Obyčajné šifrovanie chráni tajnosť vstupov v pokoji, ale nie ich použitie. Ak sú lístky zašifrované a poslané sčítacej službe, služba ich musí na sčítanie dešifrovať. K jednotlivým lístkom tak má prístup aspoň jedna strana. Architektúra problém nevyriešila, iba ho presunula z prenosu do konkrétneho spracovateľského uzla.

Dôkazy s nulovou znalosťou zaručujú overiteľnosť výstupu, no súkromie vstupov priamo neriešia. Dôkaz môže potvrdiť, že súčet bol z nejakej množiny lístkov vypočítaný správne. Nezaručí však, že lístky ostali počas sčítania súkromné. Zaručí len to, že súčet im zodpovedá. Ak sčítacia služba lístky na sčítanie dešifrovala, dôkaz sa s takou architektúrou dobre znáša. Súkromie vstupov je samostatná požiadavka.

Výpočty nad tajomstvami riešia súkromie vstupov priamo. Vďaka homomorfnému sčítaniu môže sčítacia služba spočítať lístky v zašifrovanej podobe, bez toho, aby dešifrovala čo i len jediný. Zašifrovaný súčet potom raz dešifruje distribuovaný prah držiteľov kľúčov. Bezpečný výpočet viacerých strán rozdelí sčítanie medzi uzly tak, že žiaden uzol nevidí voľbu žiadneho voliča, a výstup sa zloží až zo spoločného výsledku. Dôveryhodné prostredie na vykonávanie kódu vedie sčítanie v enkláve, ktorá svoju pamäť nikomu zvonka neodhalí. Zároveň poskytuje atestáciu (potvrdenie), že na očakávaných lístkoch bežal predpísaný sčítací softvér.

Úplný systém tieto dve rodiny spája. Lístky ostávajú súkromné vďaka výpočtom nad tajomstvami a súčet je verejne overiteľný vďaka nulovej znalosti. Problém nevyrieši ani jedna rodina sama, vyrieši ho až ich kombinácia.

16.2 Homomorfné šifrovanie: aritmetika nad šifrovým textom

Homomorfné šifrovanie dovoľuje operácie nad šifrovými textami, ktorým zodpovedajú operácie nad pôvodnými otvorenými textami. Nech $\mathrm{Enc}(a)$ je zašifrovaná hodnota a a $\mathrm{Enc}(b)$ zašifrovaná hodnota b. Homomorfné sčítanie vytvorí šifrový text, ktorého dešifrovaním dostaneme $a + b$, a nikto sa pritom nedozvie ani jednu z hodnôt v otvorenom tvare. Povedané jednoducho, znie to takmer ako zázrak. Dosiahnuteľné je to pri splnení určitých matematických predpokladov.

Od čiastočného k úplnému

Najstaršie homomorfné schémy podporovali iba jednu operáciu. RSA, ako je známe, podporuje homomorfné násobenie. Jeho autori to neinzerovali, výskumníci si to však rýchlo všimli a vďaka tomu vznikol širší výskumný smer. Kryptosystém Paillier podporuje homomorfné sčítanie. Čiastočne homomorfné schémy sa v praxi používajú desaťročia, na úzke účely, napríklad v systémoch elektronického hlasovania a pri súkromnom získavaní informácií (private information retrieval).[2]

Craig Gentry vo svojej dizertácii z roku 2009 prvýkrát zostrojil úplne homomorfnú schému. Zvládala sčítanie aj násobenie na ľubovoľných obvodoch.[3] Pôvodná konštrukcia bola zhruba miliardkrát pomalšia než rovnaký výpočet nad otvoreným textom, takže na vážne použitie nebola vhodná. Prelom spočíval v tom, že takáto schéma vôbec existuje. Inžiniersky program, ktorý nasledoval, znížil réžiu za pätnásť rokov zhruba o štyri rády. Úzke aplikácie sa tak dostali do dosahu, no všeobecné výpočty ostávajú mimo neho.

Súčasné nasadenie

Konštrukcie, ktoré praktici dnes používajú, patria do troch rodín. Schémy Brakerski-Gentry-Vaikuntanathan (BGV) a Brakerski-Fan-Vercauteren (BFV) podporujú celočíselnú aritmetiku a hodia sa na výpočty, ktoré sa dajú zapísať ako polynómy nad konečnými poľami.[10] Schéma Cheon-Kim-Kim-Song (CKKS) podporuje približnú aritmetiku nad reálnymi číslami. Hodí sa na inferenciu strojového učenia, kde malé číselné chyby nevadia. Rodina Torus FHE (TFHE) rýchlo vyhodnocuje ľubovoľné booleovské obvody technikou nazvanou programovateľný bootstrapping. Hodí sa na výpočty plné logiky. Open-source knižnice OpenFHE, Microsoft SEAL a TFHE-rs od firmy Zama tieto schémy implementujú v kvalite vhodnej na produkčné použitie.[4]

Praktické nasadenia spája jedno: úzka použiteľnosť vyhráva nad všeobecnou pomalosťou. Zašifrovaná inferencia strojového učenia umožňuje klientovi poslať službe zašifrovaný vstup a dostať zašifrovaný výstup, pričom služba vstup nevidí. Obvykle sa používa CKKS, napríklad na zašifrovanú lekársku diagnostiku alebo zašifrované hodnotenie finančného rizika. Súkromné získavanie informácií umožňuje klientovi dopytovať databázu bez toho, aby prezradil, ktorý záznam chce. Na homomorfných technikách stoja nasadenia tohto druhu v e-mailových a vyhľadávacích produktoch zameraných na súkromie. Zašifrované databázy dovoľujú službe hosťovať zašifrované údaje zákazníkov a odpovedať na dopyty bez dešifrovania. Obvykle sa na ne používa BGV a BFV.

Homomorfné šifrovanie zatiaľ neumožňuje úplne všeobecné výpočty prijateľnou rýchlosťou. Réžia ostáva taká veľká, že aplikácie sa vyberajú podľa toho, ako znášajú oneskorenie a aká jednoduchá je ich výpočtová

zložitosť. Hranica sa posúva k širšiemu využitiu, pomohla k tomu aj lepšia hardvérová akcelerácia. Zatiaľ to však nie je predvolený spôsob, ako spúšťať ľubovoľné programy nad súkromnými údajmi.

Štrukturálny sľub

Pod každou konkrétnou aplikáciou leží jednoduchšie tvrdenie. Homomorfné šifrovanie rúca predpoklad, že služba, ktorá výpočet vykonáva, musí vidieť údaje, nad ktorými ho vykonáva. Dvadsať rokov sa tento predpoklad pokladal za zákon cloudovej architektúry. Homomorfné šifrovanie ho popiera. Služba a používateľ sa stávajú stranami výmeny: služba vykoná funkciu a používateľ si ponechá vlastníctvo nad znalosťou vstupov. Zmluvná štruktúra, ktorá bola predtým neuskutočniteľná, je dnes neuskutočniteľná už len pri určitých veľkostiach úloh. Úlohy, pri ktorých ju možno použiť, sa každý rok rozširujú.

16.3 Bezpečný výpočet viacerých strán

Bezpečný výpočet viacerých strán (secure multi-party computation, MPC) rieši iný problém inou architektúrou. Viacero strán drží súkromné vstupy. Chcú spoločne vypočítať funkciu týchto vstupov a dozvedieť sa len výstup. Žiadna strana sa nedozvie vstup inej strany nad rámec toho, čo prezrádza samotný výstup.

Základné primitívy

Klasické konštrukcie sa opierajú o malú skupinu kryptografických primitívov. Zdieľanie tajomstva, ktoré v sedemdesiatych rokoch skúmal Shamir, rozdelí tajomstvo na podiely. Ľubovoľný prahový počet podielov tajomstvo zrekonštruuje, každá menšia podmnožina neprezradí nič. Funkciu, ktorá sa má počítať nad tajnými vstupmi, možno zapísať ako aritmetický obvod. Operácie obvodu sa potom dajú vykonať nad podielmi: každý účastník počíta lokálne nad svojím podielom a spoločne sa odhalí iba konečný výstup. Zašifrované obvody (garbled circuits), ktoré zaviedol Yao, umožňujú dvom stranám vyhodnotiť booleovský obvod. Jedna strana obvod zašifruje a druhá ho vyhodnotí. Správanie každého hradla je správne, ale jeho medzihodnoty ostávajú skryté. Nevedomý prenos (oblivious transfer) dovoľuje strane dostať jednu z dvoch hodnôt, ktorú si vybrala iná strana, pričom odosielateľ nezistí, ktorá z nich to bola. Je to základný primitív, na ktorom stojí mnoho protokolov MPC.

Praktické konštrukcie tieto primitívy skladajú spôsobmi, ktoré sedia na konkrétne aplikácie. Rodiny protokolov GMW, BGW a SPDZ sa líšia v kompromisoch medzi efektívnosťou, odolnosťou voči aktívne zlomyseľným protivníkom a prahom poctivých účastníkov, ktorý potrebujú. Produkčné nasadenie MPC musí zvoliť protokol, ktorého model hrozieb zod-

povedá skutočnému modelu hrozieb nasadenia. Voľba určuje, koľko účastníkov sa môže spolčiť, aby výpočet neohrozili.

Prahové podpisovanie v produkcii

Zatiaľ najúspešnejším nasadením MPC je prahové podpisovanie a dosiahlo inštitucionálnu mierku. Schéma prahového podpisu rozdelí súkromný kľúč medzi viaceré strany. Podpis vyžaduje spoluprácu určitého prahu strán a žiadna podmnožina pod prahom nedokáže vytvoriť platný podpis. Celý súkromný kľúč nemá nikdy žiadna strana, takže prienik do ktorejkoľvek jednej strany systém neohrozí. Firma Fireblocks, najväčší inštitucionálny poskytovateľ úschovy, prevádzkuje peňaženky s prahovým podpisom pre zhruba dvetisíc zákazníkov vrátane veľkých bánk a platobných spoločností. Práve vďaka tejto architektúre niektoré z týchto inštitúcií vôbec začali poskytovať úvery v sfére kryptoaktív, pretože alternatíva, správca úschovy ako jedna strana, by si vyžadovala úroveň dôvery v protistranu, ktorú neboli ochotné poskytnúť.

Dve konštrukcie založené na Schnorrovi umožnili prahové podpisovanie priamo na Bitcoine. MuSig2, špecifikovaný v BIP 327, zlúči ľubovoľný počet podpisovateľov do jediného verejného kľúča a jediného podpisu, ktorý sa nedá odlíšiť od bežného Schnorrovho podpisu jednej strany. FROST (Flexible Round-Optimized Schnorr Threshold signatures) rozširuje ten istý prístup na prahové podpisovanie t z n. Na podpis stačí ľubovoľných t z n držiteľov podielov kľúča. Protokol znesie, že až n−t podielov vypadne alebo sa stane nepriateľskými, a nestratí pritom schopnosť pokračovať. Oba sa dali použiť na Bitcoine od aktivácie Taprootu v novembri 2021. MuSig2 aj FROST vytvárajú platné Schnorrove podpisy podľa BIP 340 a výsledné transakcie v reťazci sa nedajú odlíšiť od míňania jedným podpisovateľom. Analýza reťazca nerozlíši transakciu MuSig2 desať z desiatich od transakcie s jedným kľúčom, ani míňanie FROST tri z piatich od ktorejkoľvek z nich. Táto architektúra spája záruku distribuovanej dôvery z MPC so súkromím na základnej vrstve Bitcoinu v jedinej konštrukcii. Práve ku takejto kombinácii má podľa rámca tejto knihy smerovať každý primitív zachovávajúci súkromie.

Prahové podpisovanie je tiež základom viacerých spotrebiteľských produktov peňaženiek. Ponúkajú používateľovi silnejšie bezpečnostné vlastnosti než úschova jedným kľúčom, a to bez ťažkopádnosti multisig nastavení na úrovni základného protokolu. Protokoly, na ktorých tieto produkty stoja, využívajú tie isté primitívy MPC ako inštitucionálne produkty. Sú len prispôsobené osobitným obmedzeniam mobilných zariadení a registrácie bežných používateľov.[5]

Štrukturálny sľub

MPC rozdeľuje dôveru medzi strany, ktoré si navzájom neveria. Rozdelená dôvera dáva kryptografickú záruku, ktorú nemôže porušiť žiadna jediná strana. Je to iná záruka než tá, ktorú dáva homomorfné šifrovanie. Pri homomorfnom šifrovaní vykoná jedna strana výpočet nad súkromným vstupom inej strany. Pri MPC vykonáva výpočet nad vlastnými súkromnými vstupmi viacero strán a žiadna sa nedozvie vstup inej. Oba primitívy riešia doplnkové problémy a mnohé skutočné systémy ich kombinujú.

Strany so súkromnými informáciami môžu dnes spolupracovať na spoločných úlohách, ktoré z tých informácií ťažia, bez toho, aby ich zhromaždili v centrálnom úložisku alebo sa spoliehali na spoločného sprostredkovateľa. Kryptografická záruka nahrádza koordinačný náklad, ktorý bol predtým započítaný do každej takejto spolupráce: náklad na vybudovanie dostatočnej dôvery, aby sa vstupy mohli zdieľať. Keď tento náklad klesne, spolupráca sa rozšíri aj na prípady, ktoré sa predtým nevyplatili.

16.4 Dôveryhodné prostredia na vykonávanie kódu

Dôveryhodné prostredia na vykonávanie kódu (trusted execution environments, TEE) idú inou architektonickou cestou. Kryptografické prostriedky bránia vypočítavajúcej strane vidieť vstupy. TEE jej v tom bráni hardvérovou izoláciou. Časť pamäte vnútri procesora je označená ako enkláva. Kód bežiaci v enkláve môže dešifrovať vstupy, spracovať ich a vytvoriť výstupy. Kód mimo enklávy (vrátane operačného systému, hypervízora a každého iného procesu na stroji) pamäť enklávy pozorovať nemôže. Mechanizmus atestácie dovoľuje vzdialenej strane overiť, že konkrétny softvér beží v pravej enkláve na pravom procesore. Vzdialená strana tak získa istotu, že výpočet prebehol tak, ako sa tvrdí.

Platformy

Intel Software Guard Extensions (SGX) bolo prvé masové TEE a v serverových aplikáciách je dodnes najrozšírenejšie. Na spotrebiteľských procesoroch Intel SGX vyradil od jedenástej generácie produktov Core, pretože séria útokov postranným kanálom spravila klientske SGX nepoužiteľným. Serverový variant, dnes nazývaný Scalable SGX, ostáva dostupný na procesoroch Xeon a naďalej podporuje aplikácie v cloudovej mierke. Nástupcom je architektúra Intel Trust Domain Extensions (TDX), ktorá má zraniteľnosti postranných kanálov riešiť kombináciou zmien v hardvéri a softvéri. AMD ponúka Secure Encrypted Virtualization s Secure Nested Paging (SEV-SNP), ktoré poskytuje vlastnosti podobné enklávam na hranici virtuálneho stroja. ARM TrustZone je viac než desať rokov hlavným TEE v mobilných zariadeniach a stojí za ukladaním biometrie a platobných poverení na stovkách miliónov zariadení. Secure Enclave od Applu

je spevnený variant ARM TrustZone, ktorý navyše zvláda kryptografické operácie lokálne v zariadení.[6]

Nasadenie v spotrebiteľskej mierke

Architektúra TEE sa v spotrebiteľskej mierke používa dvoma spôsobmi. Prvým je enkláva priamo v zariadení. ARM TrustZone v telefónoch s Androidom, Secure Enclave od Applu v zariadeniach s iOS a špecifikácia TPM 2.0 v moderných počítačoch spolu umiestňujú spevnené vykonávacie prostredie do stoviek miliónov spotrebiteľských zariadení. Drží v ňom biometrické šablóny, kľúče platobných poverení, kľúče k šifrovaniu disku a podklady na atestáciu. Enkláva v zariadení je najstarší a najrozšírenejší spotrebiteľský vzor TEE a vzbudzuje najmenej sporov, pretože používateľ a enkláva sú v tom istom fyzickom zariadení a majú jedného vlastníka.

Druhým vzorom je vzdialená atestovaná enkláva. Spotrebiteľské zariadenie pošle požiadavku cloudovému serveru, ktorého hardvér a softvér sa dajú kryptograficky atestovať a ktorého kód je zverejnený na kontrolu. Softvér každého servera sa kryptograficky zmeria, meranie sa zverejní a zariadenie odmietne poslať požiadavku serveru, ktorého meranie nezodpovedá zverejnenému obrazu. Servery sú postavené tak, aby po skončení požiadavky neuchovávali nijaký trvalý stav. Preto ani úplné napadnutie servera neskôr neprezradí vstupy skorších požiadaviek. Podniková cloudová úroveň ponúka túto architektúru už niekoľko rokov prostredníctvom služieb Google Cloud Confidential Computing, Microsoft Azure Confidential Computing a AWS Nitro Enclaves. Tie sprístupňujú podnikovým úlohám primitívy atestovaných enkláv na hardvéri AMD SEV-SNP, Intel TDX a podobnom. Služba Private Contact Discovery v aplikácii Signal používa enklávu na báze SGX. Klienti Signalu si v nej môžu vyhľadať, ktorí z ich telefónnych kontaktov Signal používajú, a server Signalu sa o dopyte nedozvie. Apple Private Cloud Compute, predstavený v júni 2024 na obsluhu úloh Apple Intelligence, ktoré presahujú výkon zariadenia, je zatiaľ najviditeľnejším príkladom pre spotrebiteľov. Jeho architektúra je tiež zverejnená najpodrobnejšie. Kategória sa u rôznych výrobcov zbližuje už niekoľko rokov. Apple ju spravil zrozumiteľnou pre masového spotrebiteľa.

Architektúru stojí za to opísať podrobne, pretože ukazuje sľub aj hranice súkromia založeného na TEE. Sľub je, že rozsiahlu cloudovú službu možno prevádzkovať tak, aby sama nemohla pozorovať vstupy používateľov. Je to ten istý štrukturálny sľub ako pri homomorfnom šifrovaní, dosiahnutý inými prostriedkami. Návrh Applu cielene rieši prípad, keď je protivníkom samotný Apple. Záznam, do ktorého sa len pridáva (append-only transparency log), obsahuje kryptografické meranie každého produkčného obrazu servera. Zariadenie používateľa odmietne šifrovať požiadavky pre ktorýkoľvek uzol, ktorého atestácia nezodpovedá zazna-

menanému meraniu. Podpísané binárne súbory sú zverejnené, aby ich nezávislí výskumníci mohli reprodukovať. Zvyšková dôvera je úzka, ale skutočná. Týka sa koreňových kľúčov atestácie od výrobcu kremíka, dodávateľského reťazca, ktorý ich do čipov inštaluje, a nezávislých monitorov, ktoré sledujú záznam a hľadajú rozdelené pohľady alebo potlačené záznamy. Útoky postranným kanálom na hardvérovú izoláciu enklávy ostávajú osobitnou triedou rizika. Dôvera sa znižuje, nezaniká. Používateľ vymenil dôveru v prevádzkové postupy poskytovateľa za dôveru v jeho hardvérový koreň a v audítorov, ktorí sledujú jeho záznam.

Atestovaná inferencia: špičkové modely bez odhalenia

Vzor vzdialenej atestovanej enklávy našiel druhé použitie, kde je v stávke viac súkromia než pri väčšine jeho prvých nasadení. Veľké jazykové modely sa sústredili v rukách niekoľkých prevádzkovateľov, pretože inferencia v špičkovej mierke vyžaduje výpočtový výkon, ktorý jednotliví používatelia nemajú. Výzva poslaná hosťovanému modelu je odhalená preferencia odovzdaná prevádzkovateľovi v otvorenom tvare. Predvolená cloudová architektúra dáva prevádzkovateľovi úplný prehľad o každej požiadavke každého zákazníka. Dôsledky pre sledovanie sa naprieč profesiami (lekárske dopyty, právne návrhy, novinárska práca s chránenými zdrojmi, stratégia vyjednávania, osobná korešpondencia) kumulujú spôsobom, aký sledovanie komunikácie na základnej vrstve nepozná, pretože výzva modelu je často zhustené vyjadrenie toho, nad čím autor práve premýšľa.

Dve architektúry posunuli atestovanú inferenciu z návrhu do produkcie. Nvidia predstavila podporu dôverných výpočtov na GPU H100 v roku 2023, všeobecná dostupnosť prišla v apríli 2024 a v apríli 2025 sa schopnosť rozšírila na H200 a Blackwell B200 s viac-GPU Protected PCIe.[7] GPU vytvorí hardvérový koreň dôvery s kľúčom jedinečným pre zariadenie, vypáleným pri výrobe. Zavedie zmeraný obraz firmvéru a vedie atestovanú reláciu SPDM s TEE na CPU (AMD SEV-SNP alebo Intel TDX), ktoré do GPU prenáša zašifrované údaje a z GPU ich vynáša. Spoliehajúca sa strana overí reťazec atestácie cez vzdialenú atestačnú službu Nvidie a posiela výzvy, ktorých otvorený text vidí len GPU. Azure to sprístupnil zákazníkom vo všeobecnej dostupnosti v septembri 2024 ako dôverné virtuálne stroje NCC H100 v5. Google Cloud nasadil ekvivalent na inštanciách A3 Confidential. Na tomto hardvéri prevádzkuje služby inferencie pre spotrebiteľov a vývojárov niekoľko externých prevádzkovateľov. Tinfoil zverejňuje atestácie zariadení pri každej požiadavke a viaže identitu modelu na atestáciu. Privatemode od Edgeless Systems ponúka dôvernú inferenciu hostovanú v EÚ na tom istom základe Azure. nilAI od Nillion nasadzuje modely s otvorenými váhami (Llama 3, DeepSeek, Gemma, GPT-OSS) v atestovaných GPU. Špička modelov s otvorenými váhami (Llama 3.3

70B, DeepSeek R1, Kimi K2, GPT-OSS 120B) dnes beží celá v atestovaných enklávach v produkčnej mierke.

Nasadenie, ktoré ide najďalej, spája dôvernosť s anonymitou. Apple Private Cloud Compute kombinuje opísanú architektúru atestovaných enkláv s dvoma nezávislými primitívmi prevzatými z výskumu anonymnej komunikácie. Každá produkčná požiadavka ide cez relay OHTTP (RFC 9458), ktorý prevádzkuje tretia strana. Relay odstráni IP adresu klienta skôr, než požiadavka dorazí do infraštruktúry Applu, takže cloudová strana nikdy nevidí sieťový pôvod požiadavky. Oprávnenie sa overuje slepými podpismi RSA (RFC 9474). Ide o jednorazové poverenie, ktoré dokazuje, že požiadavka pochádza z legitímneho zariadenia Apple, a neodhalí, z ktorého. Cloudová strana teda nevidí ani identitu používateľa. Výsledok: produkčná strana Applu nevie prečítať výzvu (dôvernosť, vďaka TEE), nevie prepojiť dve výzvy s tým istým používateľom (neprepojiteľnosť, vďaka novému slepému povereniu pre každú požiadavku) a nevie používateľa vôbec identifikovať (anonymita, vďaka odstráneniu IP cez OHTTP). Smerovanie s rozptylom cieľov bráni tomu, aby záťažový balancér nasmeroval prevádzku konkrétneho používateľa na napadnutý uzol, pretože nemá žiaden identifikátor používateľa, podľa ktorého by sa mohol riadiť. Úroveň suverénneho hostiteľa, ktorú rozoberá kapitola 23, poskytuje tie isté tri záruky tým, že výpočet vôbec neopustí hardvér používateľa. PCC ich poskytuje na úrovni cloudu pre úlohy, ktoré hardvér suverénneho hostiteľa nezvládne.

Medzera je na uzavretej špičke. OpenAI, Anthropic a Google ponúkajú zmluvné úrovne s nulovým uchovávaním a izolované nasadenia pre jednotlivých zákazníkov, nie hardvérovo atestovanú inferenciu. Zverejnená spolupráca Microsoftu s OpenAI na dôvernej inferencii Whisper (september 2024) je overovacie cvičenie, nie produkt vo všeobecnej dostupnosti pre vlajkové modely. Štrukturálny dôvod je, že uzavreté váhy modelu sa stanú stráženým majetkom, len čo sa dostanú na hranicu TEE obrátenú k zákazníkovi, a prevádzkovatelia zatiaľ uprednostnili zmluvné záruky pred architektonickými. Používatelia, ktorí potrebujú architektonickú záruku už dnes, majú dve možnosti. Môžu spustiť inferenciu s otvorenými váhami v atestovanej enkláve (Tinfoil, Privatemode alebo tie isté cloudové primitívy). Alebo môžu prijať menej schopnú alternatívu a spustiť model lokálne na vlastnom hardvéri. Uzavretá špička sa buď presunie k atestovanej inferencii, keď porastie dopyt zákazníkov, alebo prenechá tento segment trhu stacku s otvorenými váhami, ktorý ho už má.

Súkromie založené na TEE je dnes primitív, ktorý sa dá najľahšie škálovať. Homomorfné šifrovanie ostáva pri všeobecných výpočtoch drahé. Bezpečný výpočet viacerých strán potrebuje aspoň dve strany, ktoré sa nespolčujú, a ich zorganizovanie je rovnako sociálny problém ako technický. TEE bežia na všeobecných úlohách rýchlosťou otvoreného textu a kryp-

tografická réžia sa obmedzuje na atestáciu a izolačnú hranicu. Primitív sa takmer presne hodí na obchodný model cloudových služieb.

Má to však háčik: zníženie dôvery nie je jej odstránením. Každá architektúra TEE závisí od integrity hardvéru, od mechanizmu atestácie a od softvérového obrazu, voči ktorému sa atestácia overuje. História útokov postranným kanálom na SGX ukazuje, že integrita hardvéru je sporná, nie daná. Nedávne príklady Spectre, Meltdown a ich variantov ukazujú, že sporná hranica siaha cez celý návrh procesora.[11] Používateľ, ktorý posudzuje tvrdenie o súkromí založenom na TEE, musí posúdiť skúsenosti konkrétneho výrobcu hardvéru, návrh konkrétnej architektúry atestácie a konkrétny softvérový obraz zverejnený na overenie. Žiadne z týchto posúdení nie je triviálne a žiadne sa nedá zredukovať na jedinú binárnu odpoveď. TEE sú užitočné tam, kde je alternatívou žiadna záruka súkromia. Sú horšie tam, kde je alternatívou kryptografický primitív, ktorý nevyžaduje dôveru v hardvér.

16.5 Súkromné získavanie informácií

Súkromné získavanie informácií (private information retrieval, PIR) dovoľuje klientovi získať položku z databázy servera bez toho, aby server zistil, ktorú položku klient získal. Súkromným vstupom je index dopytu, výstupom je položka. Server vykoná výpočet nad celou svojou databázou. Výpočet kryptograficky závisí od dopytu, no nenecháva pozorovateľnú stopu o tom, ktorý prvok dopyt vybral.

Primitív má dve rodiny. Informačne teoretické PIR replikuje databázu na viacerých servroch, ktoré sa nespolčujú. Klient rozdelí dopyt na podiely a každý server odpovedá na svoj podiel, bez toho, aby poznal celý dopyt. Informačne teoretické súkromie platí, kým ostane čestný aspoň jeden server. Výpočtové PIR pracuje s jedným serverom a opiera sa o kryptografické predpoklady, obvykle o aditívne homomorfné alebo úplne homomorfné šifrovanie. Klient pošle zašifrovaný vektor dopytu, server počíta nad svojou databázou v šifrovom texte a odpoveď sa dešifruje na požadovanú položku. Server nezistí, ktorý index ju vytvoril. Daň je, že každý dopyt sa musí dotknúť každého záznamu v databáze. Preto trvalo výpočtovému PIR dve desaťročia inžinierskej práce, kým sa stalo praktickým.

Praktické nasadenia prišli za posledných päť rokov. SealPIR z Microsoft Research a Stanfordu z roku 2018 ukázal výpočtové PIR nad databázami v rádoch gigabajtov pri latencii jedného dopytu v stovkách milisekúnd. SimplePIR a DoublePIR, predstavené v roku 2022, znížili náklady na dopyt o rád vďaka predbežnému spracovaniu mimo hlavnej prevádzky. Dosiahli priepustnosť v desiatkach gigabitov za sekundu a PIR sa stalo použiteľným pre služby s veľkým objemom. V susedstve návrhového priestoru sú Spiral, OnionPIR a FrodoPIR. Súkromné vyhľadávanie kontaktov v Signale spája dopyty v štýle PIR s dôveryhodným prostredím na

vykonávanie kódu, takže server má kryptografickú istotu, že nevidí, ktoré telefónne čísla klient hľadá.

Pre rámec tejto knihy sú dôležité aplikácie, v ktorých je samotný dopyt informáciou. Kanonickým prípadom je preklad doménových mien. Každé vyhľadanie DNS prezradí resolveru, na ktoré služby sa používateľ chystá pripojiť, a z toho sa zloží vyčerpávajúci záznam online činnosti. Oblivious DNS over HTTPS (ODoH) to zmierňuje rozdelením dopytu medzi HTTP proxy a DNS resolver, ale úplný resolver na báze PIR by dopyt skryl pred oboma. Najpriamejšie sa argumentu knihy dotýkajú ľahkí klienti Bitcoinu. Bloomove filtre z BIP 37 prezrádzajú, ktoré adresy peňaženku zaujímajú. Kompaktné blokové filtre z BIP 158 prezrádzajú menej, ale sú náročnejšie na šírku pásma a výpočty. Ľahký klient na báze PIR by peňaženke dovolil získať údaje o transakciách bez toho, aby poskytujúci uzol zistil, ktoré adresy, UTXO alebo transakcie sleduje. Toky ľahkých klientov Lightningu vedú k poskytovateľom služieb Lightning, ktorí vidia každú platobnú činnosť klienta. Smerovacie dopyty s podporou PIR by toto vystavenie podstatne znížili. Kontroly zrušenia certifikátov cez OCSP prezrádzajú, aké TLS spojenia prehliadač zamýšľa nadviazať. OCSP stapling to čiastočne zakrýva, ale neodstráni. Služba na kontrolu zrušenia certifikátov na báze PIR by medzeru uzavrela.

Štrukturálny sľub je užší než pri homomorfnom šifrovaní alebo MPC, ale ostro zameraný. PIR nepočíta, získava. Do stacku tejto knihy pridáva schopnosť komunikovať so vzdialenými databázami tak, aby dopyt neunikal. Každá služba, od ktorej architektúra súkromia závisí, je aj miestom vyhľadávania, a každé miesto vyhľadávania je pozorovací kanál, pokiaľ nie sú chránené aj samotné dopyty. PIR je primitív, ktorý tento dopytový kanál uzatvára.[8]

16.6 Diferenciálne súkromie a vrstva agregácie

Diferenciálne súkromie je štatistická záruka o zverejňovaní agregovaných údajov. Na rozdiel od predchádzajúcich primitívov nechráni jednotlivé záznamy počas výpočtu. Chráni súkromie jednotlivcov, ktorých záznamy prispievajú do zverejneného agregátu.

Zlyhanie, z ktorého sa vychádza

Naivný postup pri zdieľaní súboru údajov je odstrániť zjavné identifikátory (mená, adresy, telefónne čísla) a zverejniť zvyšok. Tento postup opakovane zlyhal. V roku 1997 Latanya Sweeney opätovne identifikovala zdravotný záznam guvernéra Massachusetts v „deidentifikovanom“ súbore údajov o zamestnancoch štátu. Skrížila PSČ, dátum narodenia a pohlavie s verejne dostupnými zoznamami voličov. V roku 2008 Arvind Narayanan a Vitaly Shmatikov opätovne identifikovali podstatný podiel používateľov v súbore údajov Netflix Prize so 100 miliónmi hodnotení filmov,

skrížením s verejnými recenziami z IMDb. Všeobecný vzorec je útok prepájaním údajov (linkage attack). Zverejnený súbor sa skombinuje s akoukoľvek pomocnou informáciou, ktorú má útočník k dispozícii, a spojená informácia často stačí na opätovnú identifikáciu jednotlivcov. Žiadne vyradenie stĺpcov tomu nezabráni. Samotné údaje obsahujú dosť štruktúry na to, aby sa jedinečnosť objavila aj z hrubých atribútov.[9]

Diferenciálne súkromie je štatistická odpoveď na útok prepájaním. Nesnaží sa odstrániť identifikačné informácie zo záznamov, ale mení to, od čoho závisí samotné zverejnenie. Ak by zverejnený agregát vyzeral rovnako, či už je záznam konkrétneho jednotlivca zahrnutý, alebo nie, nemožno z neho zistiť nič špecifické o tomto jednotlivcovi. Záruka je výrok o mechanizme, ktorý výstup vytvára, nie o samotnom výstupe.

Intuícia náhodnostnej odpovede

Náhodnostnú odpoveď (randomized response) zaviedol Stanley Warner v roku 1965 pre prieskumný výskum. Je to najjednoduchší prípad a mechanizmus robí konkrétnym. Predpokladajme, že výskumník chce zistiť, aký podiel respondentov sa venoval citlivej činnosti, ktorú nikto neprizná otvorene. Každého respondenta požiada, aby si súkromne hodil mincou. Ak padne hlava, respondent odpovie na citlivú otázku pravdivo. Ak padne znak, hodí ešte raz: pri hlave odpovie „áno“ bez ohľadu na pravdu, pri znaku odpovie „nie“ bez ohľadu na pravdu. Každá odpoveď dá výskumníkovi nejakú informáciu, ale nič definitívne. „Áno“ mohlo prísť z pravdivej vetvy, alebo z náhodnej, a vie to len respondent. Vierohodná popierateľnosť je zabudovaná v protokole.

V súhrne však výskumník skutočnú mieru zistiť dokáže. Ak je skutočný podiel odpovedí „áno“ rovný p, očakávaný podiel pozorovaných „áno“ je $(1/2)p + 1/4$. Na pravdivej polovici prejde skutočná miera, na náhodnej polovici hod mincou dá „áno“ v polovici prípadov. Riešením pre p dostaneme $p = 2(\text{pozorovaný podiel} - 1/4)$. Šum sa v očakávaní vyruší a popierateľnosť jednotlivca ostáva.

Náhodnostná odpoveď je prototyp každého diferenciálne súkromného mechanizmu. Náhodnosť na úrovni jednotlivca dáva popierateľnosť, štruktúra na úrovni populácie zachováva užitočnosť. Skutočné nasadenia tento kompromis zovšeobecňujú na ľubovoľné dopyty cez jediný rozpočet súkromia. Rozpočet obmedzuje, ako veľmi môže jediný záznam pohnúť zverejneným výstupom, a pri dopytoch sa sčítava, takže každé zverejnenie spotrebuje časť rozpočtu.

Centrálne a lokálne diferenciálne súkromie

Existujú dve architektúry podľa toho, kde sa šum pridáva. Pri centrálnom diferenciálnom súkromí posielajú účastníci surové záznamy dôveryhodnému agregátorovi. Ten vypočíta skutočnú odpoveď a pred zverejnením

pridá šum. Používateľ verí agregátorovi, že so surovými údajmi naloží správne. Zverejnený agregát je diferenciálne súkromný voči vonkajším pozorovateľom. Algoritmus TopDown Úradu pre sčítanie ľudu USA je nasadenie centrálneho DP. Úrad dostane surové záznamy zo sčítania, vypočíta tabuľky a zverejní tabuľky so šumom. Pri tom uplatní celkový rozpočet súkromia rozdelený medzi mnohé tabuľky, z ktorých sa desaťročné zverejnenie skladá.

Pri lokálnom diferenciálnom súkromí pridávajú účastníci šum k vlastným záznamom, ešte než ich niekam pošlú. Dôveryhodný agregátor netreba. Daň je, že šumu treba pridať oveľa viac. Šum každého záznamu je jediný šum, ktorý ho chráni, a musí byť taký veľký, aby jediný záznam prezrádzal takmer nič, hoci sa šum v agregáte vyruší. Telemetria Applu používa lokálne DP: zariadenia s iOS zašumia jednotlivé záznamy o používaní priamo na zariadení, pred odoslaním. Apple potom zašumené záznamy agreguje a surové nikdy nevidí. Kompromis je ostrý. Lokálne DP dáva silnejšie súkromie (netreba dôveryhodného agregátora) za cenu podstatnej straty presnosti. Centrálne DP dáva lepšiu presnosť za cenu potreby dôveryhodného agregátora.

Čo diferenciálne súkromie chráni a čo nie

DP chráni pred dvoma širokými kategóriami útoku. Prvou je odvodzovanie členstva (membership inference): protivník sa snaží zistiť, či je konkrétny jednotlivec v súbore údajov. Pri správne nastavenom rozpočte súkromia je výhoda protivníka oproti hádaniu obmedzená a so zúžením rozpočtu sa zmenšuje. Druhou je odvodzovanie atribútov o akomkoľvek menovanom jednotlivcovi: dozvedieť sa o jednej osobe čokoľvek konkrétne, čo protivník predtým nevedel. Aj tu ten istý rozpočet obmedzuje, koľko sa protivník môže dozvedieť.

DP nechráni pred odvodeniami na úrovni populácie, ktoré od žiadneho jednotlivca nezávisia. Ak z údajov vyplýva, že každý v určitej demografickej skupine kupuje konkrétny produkt, štatistiky zverejnené s DP tento vzorec aj tak prezradia. Každý jednotlivec, o ktorom je známe, že do tej skupiny patrí, bude odvodením na úrovni populácie dotknutý. Je to obmedzenie „tajnosti vzorky“ (secrecy of the sample): DP chráni príspevok každého jednotlivca k odvodeniu, nie samotné odvodenie. DP nechráni ani surové údaje v pokoji. Ak je surový súbor údajov niekde uložený v čitateľnej podobe, prienik do tohto úložiska nezmierni ani to, že zverejnená tabuľka je chránená pomocou DP.

Nasadenia

Úrad pre sčítanie ľudu USA použil centrálne diferenciálne súkromie na zverejnenie prerozdeľovacích údajov zo sčítania 2020 cez algoritmus TopDown. Celkový rozpočet ε rozdelil medzi tabuľky a zverejnil tabuľky

so šumom spolu s dokumentáciou algoritmu, aby štatistici mohli šum modelovať. Apple používa lokálne diferenciálne súkromie od iOS 10 na agregovanú telemetriu (používanie emoji, predikcie QuickType, správy o pádoch Safari) so zverejnenými rozpočtami ε pre jednotlivé typy. Google používa diferenciálne súkromie na štatistiky používania prehliadača Chrome, na správy Community Mobility Reports o COVID-19[13] a na meranie publika v reklamných produktoch. Podľa produktu nasadzuje centrálne, lokálne aj hybridné varianty.

Kde zapadá

Diferenciálne súkromie patrí do rámca tejto knihy ako ochrana, ktorá platí vtedy, keď predmetom analýzy je populácia ako celok a záznam každého jednotlivca prispieva len ako dátový bod. Dopĺňa primitívy z prvej časti kapitoly, pretože nechráni samotný výpočet nad citlivým vstupom. Mnohé skutočné systémy potrebujú obe záruky naraz: aby jednotlivé výpočty neprezradili svoje vstupy a aby zverejnené agregáty nedeanonymizovali jednotlivcov, ktorí za nimi stoja. Kombinácia je architektúrou analytického systému, ktorý zachováva súkromie, a analytický systém je kategória, v ktorej sa musí usadiť každé zrelé nasadenie týchto primitívov.

16.7 Návrhový priestor a doplnky

Každý primitív sedí v inej oblasti návrhového priestoru. Homomorfné šifrovanie sa hodí vtedy, keď jedna strana spúšťa úlohu nad súkromnými vstupmi inej a réžia je znesiteľná. Bezpečný výpočet viacerých strán sa hodí vtedy, keď viacero strán drží súkromné vstupy a dá sa zorganizovať okolo stanoveného modelu spolčovania. Dôveryhodné prostredie na vykonávanie kódu sa hodí na všeobecnú úlohu, kde je kryptografická réžia neprijateľná a hardvérový model dôvery prijateľný. Súkromné získavanie informácií sa hodí na prístup k vzdialenej databáze, kde je súkromným vstupom samotný index dopytu. Diferenciálne súkromie je záruka, ktorá platí pri analýze na úrovni populácie. Príspevok jediného záznamu ostáva matematicky ohraničený.

Kombinácie sú rovnako dôležité ako jednotlivé primitívy. Homomorfné šifrovanie vnútri dôveryhodného prostredia dáva hardvér ako druhú obranu pre prípad, že sa schéma preruší. Bezpečný výpočet viacerých strán s účastníkmi, ktorí bežia vo vlastných TEE, zužuje plochu spolčovania na hardvér. PIR nad databázou hostovanou v TEE spája súkromie dopytu s integritou na strane servera. Práve túto architektúru využíva súkromné vyhľadávanie kontaktov v Signale. Dôkazy s nulovou znalosťou pripojené k ľubovoľnému z týchto primitívov potvrdzujú správnosť bez pridania ďalšej vykonávacej kópie. Hranicou je práca na skladaní, ktorá tieto primitívy spája pre konkrétne aplikácie.

16.8 Axióma odporu použitá na výpočty

Axióma odporu v tejto knihe tvrdí, že bezpečnosť systému sa meria nákladmi potrebnými na jeho prelomenie. Výpočty nad tajomstvami toto meranie rozširujú na výpočtovú vrstvu stacku.

Povrch odporu homomorfného šifrovania tvorí množina kryptografických predpokladov, na ktorých stojí konkrétna použitá schéma. Pri schémach založených na mriežkach je to problém učenia s chybami (learning with errors).[12] Pri schémach založených na kódoch je to náročnosť dekódovania náhodných lineárnych kódov. Pri iných konštrukciách platia iné predpoklady. Táto množina predpokladov je v modernej kryptografii štandardná a je to tá istá množina, na ktorej stoja postkvantové štandardy z kapitoly 14. Prelomenie konkrétnej schémy by zasiahlo nasadené aplikácie, ktoré ju používajú, ale rodinu by neprelomilo, lebo existujú alternatívne schémy založené na iných predpokladoch.

Povrchom odporu bezpečného výpočtu viacerých strán je model prahu. Záruka platí vtedy a len vtedy, keď sa nespolčí menej než prahový počet účastníkov. Prah sa musí zvoliť dosť vysoký, aby spolčenie bolo neuskutočniteľné, a účastníci musia mať rôznorodé záujmy. Záruka je funkciou sociálnej štruktúry množiny účastníkov, nielen kryptografickej konštrukcie.

Dôveryhodné prostredia na vykonávanie kódu majú najväčší povrch odporu. Integrita výrobcu hardvéru, správnosť mechanizmu atestácie, odolnosť voči postranným kanálom a overovanie softvérového obrazu sú samostatné predpoklady a výsledná záruka je ich konjunkcia. Prelomenie ktoréhokoľvek jediného predpokladu ohrozí celok. Empirická história TEE obsahuje viacero zdokumentovaných útokov postranným kanálom. Architektonickou odpoveďou bolo prestavať hardvér tam, kde softvérové záplaty nestačili. História ukazuje, že primitív je spochybniteľný, aj že toto spochybňovanie prebieha aktívne.

Povrch odporu diferenciálneho súkromia tvorí rozpočet súkromia a skladanie viacerých zverejnení v čase. Každé zverejnenie spotrebuje časť rozpočtu a dostatok zverejnení populáciu deanonymizuje, bez ohľadu na to, ako prísne bolo nastavené ktorékoľvek jedno. Praktické nasadenia kumulatívny rozpočet sledujú a obmedzujú, čo si vyžaduje prevádzkovú disciplínu nad rámec pôvodnej algoritmickej voľby.

Logika axiómy platí pre každú rodinu osobitne aj pre kompozície. Útočník musí prelomiť každý primitív v kompozícii a náklady na prelomenie narastajú. Architektonická voľba obrancu je výber primitívov, ktorých kompozície zvýšia náklady na prelomenie nad to, čo je protivník ochotný zaplatiť. Výpočty nad tajomstvami nesľubujú nezraniteľnosť. Sľubujú, že krivka nákladov na pozorovanie sa na vykonávacej vrstve teraz ohýba nahor. Je to vrstva, o ktorej protivník dovtedy predpokladal, že je zadarmo.

Zhrnutie kapitoly

Výpočty nad tajomstvami sú vykonávacím doplnkom k overovaniu s nulovou znalosťou. Nulová znalosť dokazuje správnosť výpočtu, ktorého vstupy sú súkromné. Výpočty nad tajomstvami vykonávajú výpočet nad vstupmi, ktoré vykonávajúca strana nevidí. Tieto dva primitívy riešia doplnkové problémy a skutočné systémy zachovávajúce súkromie ich kombinujú. Praktický návrhový priestor pokrývajú tri architektonické rodiny. Úplne homomorfné šifrovanie vykonáva aritmetiku nad šifrovými textami a ruší predpoklad, že služba, ktorá výpočet vykonáva, musí vidieť údaje, nad ktorými beží. Jeho réžia od Gentryho prelomu z roku 2009 klesla o štyri rády a naďalej klesá, hoci všeobecný výpočet ostáva mimo dosahu. Bezpečný výpočet viacerých strán rozdeľuje výpočet medzi účastníkov tak, že nikto nevidí celý vstup. Najrozšírenejším produkčným prípadom je prahové podpisovanie. MuSig2 a FROST vytvárajú na Bitcoine Schnorrove podpisy nerozoznateľné od míňania jedným podpisom a inštitucionálna úschova typu Fireblocks prevádzkuje prahové podpisovanie v mierke, ktorá by inak vyžadovala dôveru v protistranu, akú regulované inštitúcie neboli ochotné poskytnúť. Dôveryhodné prostredia na vykonávanie kódu spúšťajú výpočet v hardvérových enklávach, ktorých obsah je nepreniknuteľný pre vlastníka hardvéru. ARM TrustZone a Apple Secure Enclave sú na stovkách miliónov spotrebiteľských zariadení a cloudové služby v mierke nesú Apple Private Cloud Compute, Azure Confidential Computing, AWS Nitro Enclaves a Google Cloud Confidential Computing.

Súkromné získavanie informácií pokrýva prístup k vzdialeným databázam: každé miesto vyhľadávania je pozorovací kanál, pokiaľ nie sú chránené aj samotné dopyty, a PIR je primitív, ktorý ho uzatvára. Produkčné nasadenie v Signale a jednoserverové implementácie triedy SealPIR a SimplePIR spravili z PIR praktický nástroj tam, kde je samotný dopyt informáciou. Diferenciálne súkromie pokrýva vrstvu agregácie. Cez jediný rozpočet súkromia obmedzuje, koľko sa protivník môže o jednotlivcovi dozvedieť zo zverejnenej štatistiky. Náhodnostná odpoveď dáva intuíciu, kalibrovaný šum nasadenú konštrukciu a najväčšími nasadenými prípadmi sú algoritmus TopDown Úradu pre sčítanie ľudu USA a lokálna DP telemetria Applu.

Žiaden z týchto primitívov neponúka absolútne záruky. Homomorfné šifrovanie sa opiera o kryptografické predpoklady, ktoré môžu zlyhať. Bezpečný výpočet viacerých strán sa opiera o prahové predpoklady o spolčovaní. Dôveryhodné prostredia na vykonávanie kódu sa opierajú o výrobcov hardvéru, ktorých integrita je spochybnená. Diferenciálne súkromie sa opiera o disciplínu rozpočtu, ktorú možno prekročiť. Zrelosť sa podľa prípadu použitia ostro líši: réžia homomorfného šifrovania vylučuje všeobecné výpočty, organizačné nároky bezpečného výpočtu via-

cerých strán obmedzujú jeho nasadenie a dôveryhodné prostredia majú históriu zraniteľností postranných kanálov, ktorá zužuje okruh modelov hrozieb, pre ktoré sa hodia. Axióma odporu sa rozširuje aj na túto vrstvu. Každý primitív má osobitný povrch odporu a kompozície zvyšujú náklady na prelomenie. Výpočty nad tajomstvami nesľubujú nezraniteľnosť. Ohýbajú krivku nákladov na pozorovanie nahor na vykonávacej vrstve a toto ohnutie je architektonickým základom, na ktorom sa budú stavať aplikácie zachovávajúce súkromie v nasledujúcom desaťročí. Implementácia si vyžaduje odbornosť v konkrétnej schéme, protokole alebo platforme, na čo odkazujú odporúčania na čítanie.

Poznámky

[1] Yaov článok z roku 1982 založil oblasť bezpečného výpočtu. Motto parafrázuje jeho vodiacu zásadu, nie presné znenie. Andrew Chi-Chih Yao, "Protocols for Secure Computations," *Proceedings of the 23rd Annual Symposium on Foundations of Computer Science* (1982): 160–164.

[2] Vlastnosť homomorfného násobenia v RSA je implicitne obsiahnutá už v pôvodnom článku: R. L. Rivest, A. Shamir, and L. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," *Communications of the ACM* 21, no. 2 (1978): 120–126. Aditívnemu homomorfizmu kryptosystému Paillier sa venuje Pascal Paillier, "Public-Key Cryptosystems Based on Composite Degree Residuosity Classes," *EUROCRYPT 1999*, Lecture Notes in Computer Science vol. 1592, pp. 223–238.

[3] Gentryho dizertácia z roku 2009 dokázala, že úplne homomorfné šifrovanie je možné. Pätnásť rokov inžinierskej práce znížilo jeho réžiu o štyri rády a zníženie pokračuje. Craig Gentry, "Fully Homomorphic Encryption Using Ideal Lattices," *Proceedings of the 41st Annual ACM Symposium on Theory of Computing* (2009): 169–178. Dlhšie spracovanie je Gentryho dizertácia zo Stanfordu (2009). Širší prehľad súčasného stavu oblasti pozri Craig Gentry, "Computing Arbitrary Functions of Encrypted Data," *Communications of the ACM* 53, no. 3 (2010): 97–105, a Zvika Brakerski, "Fundamentals of Fully Homomorphic Encryption," in *Providing Sound Foundations for Cryptography* (ACM Books, 2019), ktorý ostáva najlepším prístupným prehľadom.

[4] BGV, BFV, CKKS a TFHE sú štyri rodiny schém nasadené v praxi. OpenFHE, Microsoft SEAL a Zama sú open-source implementácie v produkčnej kvalite. OpenFHE, `https://www.openfhe.org/`. Microsoft SEAL, `https://github.com/microsoft/SEAL`. Zama (TFHE-rs, Concrete), `https://www.zama.ai/`, so zdrojovým kódom na `https://github.com/zama-ai`. K schéme CKKS: pôvodným článkom je Jung Hee Cheon, Andrey Kim, Miran Kim, and Yongsoo Song, "Homomorphic Encryption for Arithmetic of Approximate Numbers," *ASIACRYPT 2017*. K TFHE a programovateľnému bootstrappingu: Ilaria Chillotti, Nicolas Gama, Mariya Georgieva, and Malika Izabachène, "TFHE: Fast Fully Homomorphic Encryption over the Torus," *Journal of Cryptology* 33, no. 1 (2020): 34–91.

[5] Zdieľanie tajomstva (Shamir 1979) a zašifrované obvody (Yao 1986) sú základné primitívy MPC. Fireblocks prevádzkuje prahové podpisovanie MPC pre zhruba dvetisíc zákazníkov inštitucionálnej úschovy. Na Bitcoine MuSig2 (BIP 327) zlučuje podpisovateľov n z n pri Schnorrovom podpise do jedného podpisu a FROST rozširuje tú istú konštrukciu na t z n. Oba vytvárajú podpisy v reťazci nerozoznateľné od míňania jednou stranou. Adi Shamir, "How to Share a Secret," *Communications of the ACM* 22, no. 11 (1979): 612–613, k zdieľaniu tajomstva. Andrew C. Yao, "How to Generate and Exchange Secrets,"

Proceedings of the 27th Annual Symposium on Foundations of Computer Science (1986): 162–167, k zašifrovaným obvodom. Oded Goldreich, *Foundations of Cryptography*, Volume 2 (Cambridge, 2004), je autoritatívne teoretické spracovanie a David Evans, Vladimir Kolesnikov, and Mike Rosulek, *A Pragmatic Introduction to Secure Multi-Party Computation* (NOW Publishers, 2018), je najprístupnejšia príručka pre praktikov. Fireblocks, `https://www.fireblocks.com/`. K prahovým podpisom pre Bitcoin a Ethereum pozri Rosario Gennaro and Steven Goldfeder, "Fast Multiparty Threshold ECDSA with Fast Trustless Setup," *ACM CCS 2018*, na ktorom stojí veľká časť produkčných nástrojov. MuSig2: Jonas Nick, Tim Ruffing, and Yannick Seurin, "MuSig2: Simple Two-Round Schnorr Multi-Signatures," *CRYPTO 2021*, `https://eprint.iacr.org/2020/1261`. Špecifikácia v BIP 327, `https://github.com/bitcoin/bips/blob/master/bip-0327.mediawiki`. Referenčná implementácia v libsecp256k1, `https://github.com/bitcoin-core/secp256k1`. FROST: Chelsea Komlo and Ian Goldberg, "FROST: Flexible Round-Optimized Schnorr Threshold Signatures," *SAC 2020*, `https://eprint.iacr.org/2020/852`. Návrh špecifikácie IETF na `https://datatracker.ietf.org/doc/draft-irtf-cfrg-frost/`. Produkčné implementácie na `https://github.com/ZcashFoundation/frost` (Zcash Foundation) a `https://github.com/coinbase/kryptology` (Coinbase). Taproot a Schnorr, na ktorých aktivácia stojí: BIP 340, "Schnorr Signatures for secp256k1," `https://github.com/bitcoin/bips/blob/master/bip-0340.mediawiki`, a BIP 341 Taproot, `https://github.com/bitcoin/bips/blob/master/bip-0341.mediawiki`.

[6] Intel SGX a TDX, AMD SEV-SNP, ARM TrustZone a Secure Enclave od Applu sú nasadené platformy TEE. Apple Private Cloud Compute (jún 2024) je najjasnejšia podrobne zverejnená architektúra TEE v spotrebiteľskej mierke. Victor Costan and Srinivas Devadas, "Intel SGX Explained," IACR ePrint Archive 2016/086, je kanonický technický odkaz k SGX. Dokumentácia Intel TDX na `https://www.intel.com/content/www/us/en/developer/tools/trust-domain-extensions/overview.html`. Biela kniha AMD SEV-SNP, David Kaplan, Jeremy Powell, and Tom Woller, "AMD Memory Encryption" (2021), `https://www.amd.com/system/files/TechDocs/SEV-SNP-strengthening-vm-isolation-with-integrity-protection-and-more.pdf`. Prehľad ARM TrustZone na `https://www.arm.com/technologies/trustzone-for-cortex-a`. Dokumentácia Secure Enclave od Applu na `https://support.apple.com/guide/security/secure-enclave-sec59b0b31ff/web`. Architektúra Apple Private Cloud Compute na `https://security.apple.com/blog/private-cloud-compute/`. Confidential Computing Consortium, `https://confidentialcomputing.io/`.

[7] Dôverné výpočty Nvidie na GPU Hopper a Blackwell pre atestovanú inferenciu LLM. Gavin Uberti and Steven Hecht, "Confidential Computing on NVIDIA H100 GPUs for Secure and Trustworthy AI," Nvidia Developer Blog (August 3, 2023), `https://developer.nvidia.com/blog/confidential-computing-on-h100-gpus-for-secure-and-trustworthy-ai/`, je technický úvod. Všeobecná dostupnosť na H100 bola oznámená v "Announcing Confidential Computing General Access on NVIDIA H100 GPUs" (April 25, 2024), `https://developer.nvidia.com/blog/announcing-confidential-computing-general-access-on-nvidia-h100-tensor-core-gpus/`. Všeobecná dostupnosť viac-GPU Protected PCIe bola oznámená v "Announcing NVIDIA Secure AI General Availability" (April 23, 2025), `https://developer.nvidia.com/blog/announcing-nvidia-secure-ai-general-availability/`, pre konfigurácie s ôsmimi GPU HGX H100 a H200, ktoré sú potrebné pre úlohy v špičkovej

mierke. Dôverné virtuálne stroje Azure NCC H100 v5 dosiahli všeobecnú dostupnosť v septembri 2024. Pozri Microsoft Azure Confidential Computing blog, "General Availability: Azure Confidential VMs with NVIDIA H100 Tensor Core GPUs" (September 24, 2024), https://techcommunity.microsoft.com/blog/azureconfidentialcomputingblog/general-availability-azure-confidential-vms-with-nvidia-h100-tensor-core-gpus/4242644. Platformy atestovanej inferencie tretích strán zahŕňajú Tinfoil (https://tinfoil.sh, s technickou dokumentáciou na https://tinfoil.sh/technology), Edgeless Systems Privatemode (https://www.privatemode.ai, postavený na frameworku Continuum AI na https://www.edgeless.systems/products/continuum) a Nillion nilAI (https://nillion.com). Každá zverejňuje správy o atestácii a obsluhuje modely s otvorenými váhami na infraštruktúre Nvidia CC. K mechanizmom anonymity v Apple Private Cloud Compute, na ktoré odkazuje text, sú relevantné dva RFC: Eric Kinnear et al., "Oblivious HTTP," RFC 9458 (January 2024), https://www.rfc-editor.org/rfc/rfc9458.html, a Frank Denis, Jonathan Hoyland, David Schinazi, and Christopher A. Wood, "RSA Blind Signatures," RFC 9474 (October 2023), https://www.rfc-editor.org/rfc/rfc9474.html. Apple ich spája v "Private Cloud Compute: A New Frontier for AI Privacy in the Cloud" (June 10, 2024), https://security.apple.com/blog/private-cloud-compute/. K pretrvávajúcej medzere pri uzavretých špičkových modeloch pozri septembrové oznámenie Microsoftu z roku 2024 o dôvernej inferencii Whisper s OpenAI na vyššie uvedenom blogu Azure a dokumentáciu OpenAI k podnikovému Zero Data Retention na https://platform.openai.com/docs/guides/your-data. Na začiatku roku 2026 žiaden vlajkový uzavretý špičkový model (GPT-5, Claude 4.x, Gemini Ultra) neponúka zákazníkom verejne oznámený, všeobecne dostupný produkt hardvérovo atestovanej dôvernej inferencie.

[8] Súkromné získavanie informácií dovoľuje klientovi získať položku z databázy servera bez toho, aby server zistil, ktorú. Informačne teoretické PIR potrebuje viacero servrov, ktoré sa nespolčujú, výpočtové PIR beží na jednom serveri za cenu kryptografických predpokladov. SealPIR (2018), SimplePIR a DoublePIR (2022) a súkromné vyhľadávanie kontaktov v Signale sú referenčné praktické systémy. Základné články o PIR: Benny Chor, Oded Goldreich, Eyal Kushilevitz, and Madhu Sudan, "Private Information Retrieval," *Journal of the ACM* 45, no. 6 (1998): 965–981, k informačne teoretickému PIR. Eyal Kushilevitz and Rafail Ostrovsky, "Replication Is Not Needed: Single Database, Computationally-Private Information Retrieval," *FOCS 1997*, k výpočtovému PIR. SealPIR: Sebastian Angel, Hao Chen, Kim Laine, and Srinath Setty, "PIR with Compressed Queries and Amortized Query Processing," *IEEE Symposium on Security and Privacy 2018*, https://eprint.iacr.org/2017/1142, s implementáciou na https://github.com/microsoft/SealPIR. SimplePIR a DoublePIR: Alexandra Henzinger, Matthew M. Hong, Henry Corrigan-Gibbs, Sarah Meiklejohn, and Vinod Vaikuntanathan, "One Server for the Price of Two: Simple and Fast Single-Server Private Information Retrieval," *USENIX Security 2023*, https://eprint.iacr.org/2022/949. Spiral: Samir Jordan Menon and David J. Wu, "Spiral: Fast, High-Rate Single-Server PIR via FHE Composition," *IEEE Symposium on Security and Privacy 2022*. Súkromné vyhľadávanie kontaktov v Signale: blog Signalu, "Technology preview: Private contact discovery for Signal," https://signal.org/blog/private-contact-discovery/, a následná architektúra s SGX a nevedomými operáciami opísaná na https://signal.org/blog/signal-private-group-system/. K Oblivious DNS over HTTPS (ODoH) ako slabšiemu zmierneniu než PIR pozri IETF RFC 9230, https://www.rfc-editor.org/rfc/rfc9230.html. K súkromiu dopytov ľahkých klientov Bitcoinu: analýza súkromia Bloomových filtrov BIP 37 v Arthur Gervais et al., "On the Privacy Provisions of Bloom Filters in Lightweight Bitcoin Clients," *ACSAC 2014*. Špecifikácia kompaktných blokových filtrov BIP 158 na https:

//github.com/bitcoin/bips/blob/master/bip-0158.mediawiki. Priebežná analýza súkromia na https://bitcoinops.org/. K ľahkým klientom na báze PIR ako výskumnému smeru pozri diskusie o sieti Portal Network pre Ethereum a vlákno "Vitalik on Ethereum light client privacy" na https://ethresear.ch/.

[10] Pôvodný článok k schéme BGV, ktorý vytvoril rámec pre stupňované úplne homomorfné šifrovanie nad celými číslami s využitím okruhového problému učenia s chybami: Zvika Brakerski, Craig Gentry, and Vinod Vaikuntanathan, "Fully Homomorphic Encryption without Bootstrapping," *ITCS 2012*, https://eprint.iacr.org/2011/277. Variant BFV, ktorý v praxi optimalizuje celočíselnú aritmetiku: Junfeng Fan and Frederik Vercauteren, "Somewhat Practical Fully Homomorphic Encryption," *IACR ePrint* 2012/144, https://eprint.iacr.org/2012/144. Tieto dva články sú teoretickým základom implementácií knižníc BGV/BFV, citovaných v poznámke 4. Knižnice (Microsoft SEAL, OpenFHE) tieto schémy implementujú, ale pôvodné články definujú bezpečnostné redukcie a voľbu parametrov, ktoré určujú praktické úrovne bezpečnosti.

[11] Spectre a Meltdown sú prelomové zraniteľnosti špekulatívneho vykonávania v CPU z roku 2018, ktoré odhalili spornú povahu izolačných hraníc na úrovni procesora. Pre bezpečnosť TEE sú relevantné tým, že tie isté hardvérové prvky (predikcia vetvenia, vykonávanie mimo poradia, hierarchia cache), ktoré tieto útoky umožňujú, sú prítomné aj vnútri hranice TEE a dajú sa zneužiť zvonku. Paul Kocher et al., "Spectre Attacks: Exploiting Speculative Execution," *IEEE Symposium on Security and Privacy* (2019), https://spectreattack.com/spectre.pdf. Moritz Lipp et al., "Meltdown: Reading Kernel Memory from User Space," *USENIX Security Symposium* (2018), https://meltdownattack.com/meltdown.pdf. Literatúra venovaná útokom postranným kanálom na SGX je rozsiahla. Reprezentatívne články sú Jo Van Bulck et al., "Foreshadow: Extracting the Keys to the Intel SGX Kingdom with Transient Out-of-Order Execution," *USENIX Security* (2018), https://foreshadowattack.eu/, a Daniel Moghimi et al., "Downfall: Exploiting Speculative Data Gathering," *USENIX Security* (2023), https://downfall.page/. Vyradenie klientskeho SGX Intelom a architektonický obrat k TDX je zdokumentovaný v oznámeniach Intelu o zmenách produktov od procesorov Core 11. generácie.

[12] Problém učenia s chybami (learning with errors, LWE), ktorý v roku 2005 zaviedol Oded Regev, je predpoklad náročnosti, na ktorom stoja BGV, BFV, CKKS a štandardy NIST pre postkvantovú výmenu kľúčov a digitálne podpisy. Jeho okruhový variant (RLWE) je predpoklad, na ktorom stojí väčšina nasadeného FHE. Oded Regev, "On Lattices, Learning with Errors, Random Linear Codes, and Cryptography," *STOC 2005*, https://cims.nyu.edu/~regev/papers/qcrypto.pdf. Časopisecká verzia v *Journal of the ACM* 56, no. 6 (2009). Vadim Lyubashevsky, Chris Peikert, and Oded Regev, "On Ideal Lattices and Learning with Errors over Rings," *EUROCRYPT 2010*, https://eprint.iacr.org/2012/230, zaviedli okruhový variant, ktorý používajú všetky praktické schémy FHE. Proces postkvantovej štandardizácie NIST zvolil ako primárne štandardy schémy založené na LWE (CRYSTALS-Kyber, CRYSTALS-Dilithium). Pozri NIST IR 8413 (2022), https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8413.pdf.

[13] Správy Google Community Mobility Reports o COVID-19 používali agregované, diferenciálne súkromné údaje o polohe od používateľov Google Maps. Vytvárali z nich anonymizované súhrny mobility na úrovni populácie počas pandémie. Metodický dokument opisuje použité parametre DP. Google LLC, "COVID-19 Community Mobility Reports: Understand the Data," metodická dokumentácia dostupná na https://support.google.com/covid19-mobility/answer/9825414. Archivované údaje správ na https://www.google.com/covid19/mobility/. K širšej infraštruktúre diferenciálneho súkromia Googlu pozri Miguel Guevara, "Helping public health officials combat COVID-19," Google Blog (April 3, 2020), a open-source

knižnicu DP na https://github.com/google/differential-privacy, ktorá implementuje mechanizmy používané v Chrome, Mobility Reports a reklamných meracích produktoch.

[9] Diferenciálne súkromie zaručuje, že z agregovaných zverejnení sa v rámci rozpočtu ε nedajú deanonymizovať jednotlivé záznamy. Warnerova náhodnostná odpoveď z roku 1965 je intuícia, Dworkovej formalizácia z polovice 2000. rokov matematický rámec a sčítanie USA 2020, telemetria Applu (od iOS 10) a štatistiky používania Googlu sú najväčšie nasadené prípady. Základná formalizácia: Cynthia Dwork, Frank McSherry, Kobbi Nissim, and Adam Smith, "Calibrating Noise to Sensitivity in Private Data Analysis," *TCC 2006*, https://iacr.org/archive/tcc2006/38760266/38760266.pdf. Autoritatívny zdroj: Cynthia Dwork and Aaron Roth, *The Algorithmic Foundations of Differential Privacy*, *Foundations and Trends in Theoretical Computer Science* 9, nos. 3–4 (2014): 211–407, https://www.cis.upenn.edu/~aaroth/Papers/privacybook.pdf. Pôvod náhodnostnej odpovede: Stanley L. Warner, "Randomized Response: A Survey Technique for Eliminating Evasive Answer Bias," *Journal of the American Statistical Association* 60, no. 309 (1965): 63–69. K motivujúcim zlyhaniam: Latanya Sweeney, "Simple Demographics Often Identify People Uniquely," Carnegie Mellon University, Data Privacy Working Paper 3 (2000), https://dataprivacylab.org/projects/identifiability/, a Arvind Narayanan and Vitaly Shmatikov, "Robust De-anonymization of Large Sparse Datasets," *IEEE Symposium on Security and Privacy 2008*, https://www.cs.utexas.edu/~shmat/shmat_oak08netflix.pdf, článok o deanonymizácii Netflix Prize. Dokumentácia algoritmu TopDown Úradu pre sčítanie ľudu USA na https://www.census.gov/programs-surveys/decennial-census/decade/2020/planning-management/process/disclosure-avoidance.html. Nasadenie Applu je zdokumentované v Differential Privacy Team, "Learning with Privacy at Scale," *Apple Machine Learning Journal* 1, no. 8 (2017), https://machinelearning.apple.com/research/learning-with-privacy-at-scale. Knižnica OpenDP od Googlu na https://github.com/google/differential-privacy. K teoretickým kompromisom: Salil Vadhan, "The Complexity of Differential Privacy," in *Tutorials on the Foundations of Cryptography* (Springer, 2017). K obmedzeniu „tajnosť vzorky" a rozdielu medzi odvodením na úrovni jednotlivca a na úrovni populácie je štandardným zdrojom Cynthia Dwork, "Differential Privacy: A Survey of Results," *TAMC 2008*.

17

ANONYMNÉ KOMUNIKAČNÉ SIETE

„Zabíjame ľudí na základe metadát.“

Michael Hayden, panelová diskusia, Johns Hopkins University (2014)[1]

Úvod

Kapitola 14 položila kryptografické základy. Šifrovanie chráni obsah komunikácie. Samo o sebe to však na súkromie nestačí.

Problémom sú metadáta, teda informácie o komunikácii, nie jej obsah. Kto s kým komunikuje, kedy, ako často a ako dlho, to všetko odhaľuje vzorce, ktoré môže sledovanie využiť. Aj pri dokonale zašifrovanom obsahu umožňujú metadáta úplne monitorovať sociálne siete, politické väzby i osobné vzťahy.

Táto kapitola skúma architektonické riešenia problému metadát na dvoch vrstvách. Na transportnej vrstve ponúkajú VPN, Tor a I2P a mixnety (zmiešavacie siete) každý iný bod v kompromise medzi latenciou a anonymitou. Na aplikačnej vrstve rad protokolov šifrovanej komunikácie, od PGP cez Signal až po MLS, postupne rozširoval to, čo end-to-end šifrovanie chráni, a zužoval to, čo stále prezrádza. Ani jedna vrstva problém nevyrieši sama, no navzájom sa dopĺňajú.

17.1 Problém: ako internet prezrádza súkromie

IP adresy: zabudované identifikátory

Internetový protokol vznikol pre spoľahlivosť, nie pre súkromie. Každý paket nesie IP adresu odosielateľa v otvorenom texte a vidí ju každý smerovač na ceste. Nie je to chyba, ale zásadné konštrukčné rozhodnutie: sieť aj vzdialený koncový bod potrebujú údaj o zdroji, aby sa odpoveď dostala späť.

IP adresa je identifikátor. Zodpovedá približnej fyzickej polohe a poskytovateľovi internetu, ktorý ju cez záznamy o odberateľoch spája s právnou identitou. Každý web, ktorý navštívite, a každá služba, ku ktorej sa pripojíte, dostane vašu IP adresu. Vie, odkiaľ sa pripájate, a ak má ďalšie záznamy alebo prepojenie na účet, môže odvodiť aj to, kto ste.

Aj keď je obsah zašifrovaný, hlavička IP nie je. HTTPS ukryje, čo na webe čítate, ale neukryje, že ste sa pripojili. Váš poskytovateľ internetu spoľahlivo vidí, že komunikujete, a vidí aj IP adresy alebo sieťových poskytovateľov, s ktorými ste v spojení. Často vidí aj cieľovú doménu cez DNS alebo metadáta TLS, hoci šifrované DNS a ECH tento prehľad môžu zúžiť. Sieťoví pozorovatelia na trase vidia zdrojovú aj cieľovú IP adresu na každom pakete.

Metadáta: celý obraz

Metadáta sú údaje o údajoch. Pri komunikácii patria medzi ne: kto (identifikátory odosielateľa a príjemcu, napríklad e-mailové adresy, telefónne čísla a IP adresy), kedy (časové značky komunikácie), ako dlho (trvanie hovorov, veľkosť správ), ako často (frekvencia komunikácie medzi stranami) a kde (údaje o polohe zo zariadení). Šifrovanie obsahu ukryje, čo bolo povedané. Metadáta prezradia všetko ostatné.

Haydenov výrok „zabíjame ľudí na základe metadát“ nie je prehnaný.[1] Samotné vzorce komunikácie odhaľujú sociálnu štruktúru (kto sú vodcovia a sprostredkovatelia), zmeny správania (náhly nárast alebo ticho, ktoré signalizuje plánovanie či samotnú operáciu), fyzický pohyb cez metadáta zariadení a spojenie so známymi cieľmi. Spravodajské služby sa priznali, že tieto informácie používajú pri rozhodovaní o cieľoch.

Prečo šifrovanie obsahu nestačí

Predstavme si šifrovanú komunikáciu medzi dvoma stranami. Pozorovateľ, ktorý správy nevie prečítať, aj tak vidí, že Alice a Bob komunikujú, ako často, kedy (v ktorých hodinách a dňoch v týždni), ako sa ich vzorce komunikácie menia v čase a s kým ďalším každý z nich komunikuje.

V mnohých situáciách takéto informácie na sledovanie stačia. Vedieť, že novinár často komunikuje s istým vládnym úradníkom, je cenná informácia bez ohľadu na obsah správ.

Analýza prevádzky

Analýza prevádzky je systematické zneužívanie metadát. Časová korelácia si všíma, že ak Alice pošle správu o 2:03:47 a Bob jednu dostane o 2:03:48, pravdepodobne spolu komunikujú, aj keď je obsah zašifrovaný a trasa nepriama. Korelácia objemu porovnáva veľkosti správ na jednotlivých skokoch siete, aby prepojila odosielateľa s príjemcom. Analýza vzorcov odhaľuje pravidelnú komunikáciu (každý utorok o 15:00), ktorá prezradí vzťahy aj bez obsahu. Analýza sieťových tokov sleduje prevádzku cez sieťovú infraštruktúru a odhalí koncové body, aj keď sú jednotlivé skoky šifrované. Analýza prevádzky funguje preto, že komunikácia musí prejsť fyzickou infraštruktúrou, ktorú možno pozorovať.

17.2 Požiadavky na anonymnú komunikáciu

Formálne vlastnosti

Systémy anonymnej komunikácie majú poskytovať niekoľko vlastností, z ktorých každá rieši iný aspekt problému metadát.

Anonymita odosielateľa znamená, že pozorovatelia nevedia určiť, kto správu poslal, takže pôvodca zostane skrytý, aj keď je obsah známy. Táto vlastnosť chráni oznamovateľov nekalých praktík a každého, kto by za svoje slová mohol čeliť odvete. Anonymita príjemcu znamená, že pozorovatelia nevedia určiť, kto správu dostal. Zamýšľané publikum zostáva skryté, a príjemcovia tak nie sú spájaní s odosielateľmi, ktorí môžu byť terčom.

Neprepojiteľnosť znamená, že pozorovatelia nevedia určiť, že konkrétny odosielateľ a konkrétny príjemca spolu komunikujú. Aj keď je známe, že obaja systém používajú, prepojenie ich aktivity maria sledovanie, ktoré stojí na mapovaní vzťahov. Nepozorovateľnosť znamená, že pozorovatelia nevedia určiť, či komunikácia vôbec prebieha. Komunikácia je ukrytá medzi inou prevádzkou alebo krycou aktivitou. Je to najsilnejšia vlastnosť, lebo skrýva samotný fakt komunikácie.

Tieto vlastnosti majú rôznu silu podľa modelu protivníka. Proti lokálnemu pozorovateľovi (ktorý vidí len časť siete) môže stačiť slabšia ochrana. Proti globálnemu protivníkovi (ktorý vidí všetku sieťovú prevádzku) je potrebná silnejšia. Návrh odráža očakávané hrozby: novinári v autoritárskych režimoch čelia iným protivníkom ako používatelia, ktorí chcú súkromie pred inzerentmi.

Modely protivníka

Sila anonymizačného systému závisí od predpokladov o protivníkovi, proti ktorému je navrhnutý. Pasívny protivník prevádzku pozoruje bez toho, aby ju menil: zbiera údaje a snaží sa o identifikáciu koreláciou vzorcov. Aktívny protivník môže správy vkladať, oneskorovať, zahadzovať alebo

meniť. Môže prevádzkovať vlastné uzly v sieti alebo robiť časové útoky, pri ktorých zámerným oneskorovaním núti používateľov k rozpoznateľnému správaniu.

Lokálny protivník vidí len časť siete: pripojenie používateľa k poskytovateľovi internetu alebo prevádzku cez jediný relay. Globálny protivník vidí všetku sieťovú prevádzku naraz. Je to najsilnejší model, lebo umožňuje end-to-end časovú koreláciu, ktorej žiadne šifrovanie nezabráni bez ďalších protiopatrení.

Realistické modelovanie hrozieb začína otázkou, kto je pravdepodobný protivník. Väčšina používateľov nečelí protivníkom na úrovni štátov. Systémy navrhnuté len proti slabým protivníkom však katastrofálne zlyhajú, keď sa objavia silnejší. Cypherpunkový prístup buduje systémy, ktoré odolajú najsilnejším pravdepodobným protivníkom, lebo schopnosti s časom rastú.

Množina anonymity

Anonymita je relatívna voči množine anonymity: skupine možných odosielateľov alebo príjemcov, medzi ktorými sa skutočná strana nedá rozlíšiť. Je to základná miera sily anonymity.

Ak má množina anonymity len troch ľudí, protivník trafí správnu osobu s pravdepodobnosťou 1 ku 3. Ak ich má milióny, šance sa úmerne zhoršia. Matematika je jednoduchá: anonymita závisí od toho, kto ešte systém používa.

Množiny anonymity závisia od toho, kto systém používa v tom istom čase. Vzniká tak dynamika kolektívneho konania: čím viac používateľov, tým silnejšia anonymita každého z nich. Systém s malým počtom používateľov poskytuje slabú anonymitu bez ohľadu na silu kryptografie. Systém s mnohými používateľmi môže poskytnúť silnú anonymitu aj s jednoduchšou kryptografiou.

Preto má rozšírenie rovnakú váhu ako samotná technológia. Nástroje na ochranu súkromia profitujú zo širokého používania. Prví používatelia obetujú časť anonymity, aby systém rozbehli, a neskorší ťažia z množiny anonymity, ktorú prvopočiatoční vytvorili. Problém kolektívneho konania však vytvára aj zraniteľnosť: ak protivníci dokážu znížiť rozšírenie (právnym tlakom alebo stigmatizáciou), oslabia anonymitu zvyšným používateľom.

Krycia prevádzka a fiktívne správy

Niektoré systémy zavádzajú krycú prevádzku, teda falošné správy nerozoznateľné od skutočných. Plní naraz niekoľko účelov: udržiava rovnaký objem prevádzky bez ohľadu na skutočné používanie, čím maria analýzu objemu, a vytvára aktivitu aj vtedy, keď používatelia nič nerobia, čo sťažu-

je časovú analýzu. Rozširuje aj účinnú množinu anonymity, lebo fiktívne správy sa miešajú medzi možné „skutočné“.

Krycia prevádzka má svoju cenu. Rastie spotreba šírky pásma, lebo fiktívne správy spotrebúvajú rovnaké zdroje ako skutočné. Latencia sa môže zvýšiť, ak systémy čakajú na zoskupenie skutočných a fiktívnych správ. Rastie aj zložitosť, pretože odlíšiť krycie správy od skutočných musí byť nemožné pre pozorovateľov, no možné pre príjemcov.

Voľba závisí od modelu hrozieb. Proti pasívnym lokálnym protivníkom môže byť krycia prevádzka zbytočná réžia. Proti aktívnym globálnym protivníkom môže byť pre účinnú ochranu nevyhnutná.

17.3 VPN: jednoduché, ale obmedzené riešenie

Čo VPN poskytuje

VPN (virtuálna súkromná sieť) je najjednoduchší spôsob, ako skryť IP adresu. Šifruje prevádzku medzi používateľom a serverom poskytovateľa VPN, ktorý ju potom preposiela na cieľ. Lokálny úsek siete je chránený pred pozorovateľmi, ako sú prevádzkovatelia wifi v kaviarni, poskytovateľ internetu nevidí konečné ciele, hoci samotné spojenie s VPN vidí, a cieľové servery vidia IP adresu servera VPN namiesto adresy používateľa. Pre mnohých používateľov to stačí. Ak ide o to, že poskytovateľ internetu zaznamenáva históriu prehliadania alebo že prevádzkovateľ siete odpočúva prevádzku, VPN rieši bezprostredný problém.

Sústredenie dôvery a jeho dôsledky

VPN sledovanie neodstraňuje, len ho premiestňuje. Poskytovateľ VPN pozná skutočnú IP adresu používateľa a vidí všetky ciele prevádzky. Sledovanie sa presunulo od poskytovateľa internetu k poskytovateľovi VPN. Ak poskytovateľ prevádzku zaznamenáva alebo spolupracuje s úradmi, používateľ nemá žiadnu ochranu. Weby aj tak vidia cookies a behaviorálne odtlačky, ktoré používateľov identifikujú bez ohľadu na IP adresu, ktorú pakety nesú. Na rozdiel od viacskokových systémov VPN sústreďujú dôveru do jedného komerčného subjektu a jeho kompromitácia kompromituje všetko, čo cezeň prešlo.

Model dôvery je navyše štrukturálne nepriehľadný. Poskytovatelia VPN tvrdia niečo o svojich pravidlách zaznamenávania, čo používatelia nemôžu overiť. Tvrdenia „bez záznamov“ boli vyvrátené, keď poskytovatelia vydali údaje úradom, a používatelia nemajú ako postupy poskytovateľa nezávisle auditovať. Aj poskytovateľa s dobrými úmyslami môže právny proces prinútiť začať zaznamenávať, môže ho odkúpiť firma menej naklonená súkromiu alebo ho môže niekto nabúrať. Používateľ musí dôverovať nielen terajšiemu postoju poskytovateľa, ale aj jeho budúcemu správaniu pod tlakom, ktorému ešte nečelil.

Niektorí poskytovatelia ponúkajú viacskokové konfigurácie, ktoré smerujú prevádzku cez dva alebo viac serverov, a používatelia môžu VPN reťaziť aj ručne: pripoja sa k poskytovateľovi A a cez toto spojenie k poskytovateľovi B. Poskytovateľ A vidí skutočnú IP adresu, ale nie cieľ; poskytovateľ B vidí cieľ, ale len IP adresu poskytovateľa A. Viacskokové VPN zostávajú slabšie než Tor. Poskytovateľov je málo v porovnaní s tisíckami relayov siete Tor. Sú to komerčné subjekty so známou identitou, na ktoré sa tlačí ľahšie než na pseudonymných prevádzkovateľov relayov. Jeden poskytovateľ často ovláda viac skokov vo vlastnej „viacskokovej" ponuke. A konfigurácie VPN bývajú statické, kým okruhy Toru sa striedajú. Jednoskoková VPN trasu zlepšuje, no účelovo budovaná anonymizačná sieť rozkladá dôveru medzi väčšiu a menej koncentrovanú množinu relayov.

Kde model dôvery drží

Model dôvery VPN drží, keď je hrozba lokálna a poskytovateľ stojí mimo modelu hrozieb. Ochrana pred zaznamenávaním u poskytovateľa internetu alebo pred odpočúvaním na verejnej wifi sa do tejto hranice zmestí a pri takých hrozbách VPN odvádza skutočnú prácu s malým trením.

Model sa láme, keď sa protivník dostane k poskytovateľovi. Anonymita voči štátu, ktorý môže poskytovateľa predvolať, ochrana pred samotným poskytovateľom a akákoľvek činnosť, pri ktorej je sústredenie dôvery v jednom komerčnom subjekte neprijateľné, to všetko presahuje možnosti VPN. Hranicu určuje architektúra a nijaký výber poskytovateľa ju nezmení.

17.4 Cibuľové smerovanie: Tor a I2P

Základný poznatok: rozložiť dôveru

Zásadnou slabinou VPN je, že jeden subjekt vidí všetko. Cibuľové smerovanie to rieši rozložením dôvery medzi viac relayov. Žiadny jednotlivý relay nevie naraz, kto ste a k čomu pristupujete.

Tor: architektúra a fungovanie

Tor (The Onion Router) je najrozšírenejší systém anonymnej komunikácie.[2] Používa vrstvené šifrovanie, kde každú vrstvu dešifruje postupne ďalší relay.

Klient Toru zostaví okruh cez tri relaye: vstupný uzol (guard), stredný uzol a výstupný uzol. Klient pozná všetky tri; každý relay pozná len svojich susedov. Správa je zašifrovaná trikrát, raz pre každý uzol: vstupný uzol dešifruje vonkajšiu vrstvu a posiela ju strednému, stredný dešifruje a posiela výstupnému, výstupný dešifruje a posiela cieľu. Žiadny jednotlivý uzol nepozná zároveň pôvod aj cieľ: vstupný pozná používateľa, ale nie cieľ, výstupný pozná cieľ, ale nie používateľa, a stredný nepozná ani jedno. Vďaka tejto architektúre jeden kompromitovaný relay protivníkovi auto-

maticky nedá úplný pohľad od jedného konca k druhému, hoci škodlivé uzly sa stále dozvedia metadáta špecifické pre svoju pozíciu. Na prepojenie používateľa s cieľom protivník spravidla potrebuje viac pozorovacích bodov alebo pomocné útoky.

Ekonomika siete Tor

Tor funguje vďaka dobrovoľným prevádzkovateľom relayov, ktorí darujú šírku pásma a výpočtové zdroje, a motivácia stojí na vlastnom záujme spojenom s ideovým presvedčením. Niektorí prevádzkovatelia Tor sami potrebujú a prispievajú do siete, ktorú používajú; iní prevádzkujú relaye z princípu, aby podporili slobodu komunikácie. Niektoré relaye prevádzkujú organizácie, napríklad univerzity a skupiny na obranu súkromia, ako súčasť svojho poslania. Dobrovoľnícky model však prináša problémy s udržateľnosťou. Výstupné uzly nesú zvláštne bremená: sťažnosti na zneužitie a právne vystavenie. Sieť dlhodobo trpí nedostatkom výstupnej kapacity.

Obmedzenia siete Tor

Tor má dobre zdokumentované obmedzenia a útoky v praxi tieto zraniteľnosti ukázali.[3]

Časové útoky umožňujú globálnemu protivníkovi, ktorý pozoruje oba konce okruhu, skorelovať časovanie a prepojiť odosielateľa s príjemcom; Tor nechráni pred protivníkmi, ktorí dokážu monitorovať prevádzku na vstupe aj výstupe. Analýza prevádzky môže odhaliť informácie zo vzorcov používania okruhu aj bez prelomenia šifrovania. Útoky rozpoznávaním webov podľa prevádzky (website fingerprinting) analyzujú veľkosť a časovanie šifrovanej prevádzky, aby zistili, ktoré weby používateľ navštevuje; výskum dosiahol v kontrolovaných podmienkach presnosť vyše 95 %, ak sledoval malú množinu populárnych webov, hoci účinnosť v reálnom svete je predmetom sporu.[4]

Zraniteľnosti výstupných uzlov existujú preto, že výstupné uzly vidia nešifrovanú prevádzku smerom k cieľom, ak cieľ nepoužíva HTTPS, a zlomyseľní prevádzkovatelia výstupných uzlov tak môžu nešifrovanú prevádzku pozorovať a meniť. Kompromitácia vstupného uzla je obzvlášť závažná, lebo používatelia Toru si ponechávajú rovnaké vstupné uzly dlhý čas; protivník, ktorý ovláda používateľov vstupný uzol, vidí všetku ich prevádzku Toru vstupujúcu do siete a v spojení s pozorovaním výstupu alebo s website fingerprintingom môže kompromitácia vstupného uzla podstatne zvýšiť riziko deanonymizácie.

Zdokumentované deanonymizačné útoky na používateľov Toru uspeli, hoci priebežná údržba projektu Tor mnohé konkrétne zraniteľnosti odstránila. V operácii Torpedo (2012) FBI nasadila malvér cez napadnuté služby onion, aby odhalila používateľov zneužitím zraniteľností prehliadača.[5]

Útok na Freedom Hosting v roku 2013 použil podobné techniky.[30] Oba útoky zneužili zásuvné moduly prehliadača (najmä Flash), ktoré Tor Browser teraz predvolene vypína; konkrétne zraniteľnosti boli opravené. V roku 2014 vedci (údajne z CMU/CERT) prevádzkovali vyše 100 škodlivých relayov, ktoré tvorili 6,4 % kapacity vstupných uzlov, a použili útok potvrdzovania prevádzky cez „relay early" na deanonymizáciu používateľov služieb onion; projekt Tor útok objavil, v júli 2014 zraniteľnosť „relay early" opravil a škodlivé relaye vylúčil.[6]

Tieto historické útoky ukazujú dôležitý vzorec: Tor prechádza nepretržitým bezpečnostným preskúmavaním a zlepšovaním. Konkrétne implementačné zraniteľnosti sa po objavení spravidla rýchlo opravia. Útoky, ktoré uspeli, zneužili chyby, ktoré už neexistujú. Zostávajú štrukturálne obmedzenia vlastné nízkolatenčnému návrhu Toru: časovú koreláciu globálnymi protivníkmi, analýzu prevádzky a website fingerprinting nemožno úplne odstrániť bez inej architektúry. Používatelia by mali rozlišovať medzi historickými zneužitiami (z veľkej časti opravenými) a štrukturálnymi obmedzeniami (vlastnými samotnému návrhu).

Štáty tiež preukázali sofistikované schopnosti odhaľovať a blokovať mosty Toru, neuvedené vstupné body určené na obchádzanie cenzúry. Čína, Irán a Rusko zaviedli blokovanie mostov s rôznym úspechom. Útoky typu Sybil, pri ktorých protivník vytvorí množstvo pseudonymných identít, aby získal neprimeraný vplyv v sieti, umožňujú protivníkom s mnohými relayami zvýšiť šancu, že ich vyberú do okruhov, a tým zlepšiť svoje útočné schopnosti.

Výkon trpí, lebo viacskokové smerovanie zvyšuje latenciu; Tor je pomalší než priame pripojenie, niekedy podstatne. Použiteľnosť ostáva náročná; Tor sa používa ťažšie než bežné prehliadanie a používatelia robia chyby, ktoré anonymitu ohrozujú.

Systém adresárových autorít Toru je bod centralizácie.[31] Desať adresárových autorít pravidelne hlasuje o dokumente sieťového konsenzu, ktorý uvádza všetky relaye a ich dôveryhodnosť. Klienti si tento konsenzus sťahujú, aby mohli budovať okruhy. Samotné adresárové autority sú známe subjekty so stálou identitou, ktoré prevádzkujú dôveryhodní členovia komunity a organizácie. Hoci kompromitácia jedinej autority má vďaka hlasovaciemu mechanizmu obmedzený dosah, celý systém závisí od toho, že táto malá skupina zostane čestná a nenapadnutá. Je to pragmatické rozhodnutie: plne decentralizovaný konsenzus je pri objavovaní relayov ťažký a model adresárových autorít sa celkom osvedčil. Líši sa však od modelov, ktoré dôveru nevyžadujú vôbec a o ktoré sa niektoré systémy usilujú.

Tor poskytuje silnú ochranu pred mnohými protivníkmi, no štáty s dostatkom zdrojov môžu stále narušiť prístup, blokovať mosty a zlepšiť svoju

útočnú pozíciu prevádzkovaním infraštruktúry alebo koreláciou prevádzky.

Služby onion: publikovanie odolné voči cenzúre

Najznámejšie využitie Toru je anonymizácia odchádzajúcich spojení: používatelia pristupujú k bežným webom bez toho, aby odhalili svoju identitu. Tor však umožňuje aj opak: publikovať služby bez odhalenia polohy servera a bez akejkoľvek registrácie u doménových autorít.

Služba onion vygeneruje pár kľúčov. Pri moderných službách onion verzie 3 sa adresa `.onion` odvodzuje z materiálu identitného kľúča ed25519 a v base32 kóduje verejný kľúč, kontrolný súčet a verziu. Služba sa pripojí k sieti Tor a vytvorí úvodné body (introduction points). Klienti sa cez sieť Tor pripoja k týmto úvodným bodom a potom vytvoria okruh na stretnutie (rendezvous circuit). Ani klient, ani server neodhalí svoju IP adresu druhej strane ani žiadnemu relayu.

Služby onion nevyžadujú registráciu domény. Tradičné weby potrebujú doménové mená kúpené u registrátorov, ktorí vynucujú požiadavky na identitu a môžu domény pod právnym tlakom odobrať. Adresy onion sa odvodzujú z kryptografických kľúčov. Neexistuje registrátor, na ktorého by sa dalo tlačiť, a DNS sa zhabať nedá. Adresa sa overuje sama: ak sa k službe dostanete, dostali ste sa ku správnej službe, čo potvrdzuje kryptografia, nie certifikačné autority.

Poloha servera zostáva skrytá: jeho IP adresa sa nikdy neobjaví v žiadnom spojení, takže protivníci nevedia určiť, ktorý server prepadnúť ani zákony ktorej jurisdikcie sa uplatnia. Web možno publikovať odkiaľkoľvek a zostane dostupný, kým existuje aspoň jedna cesta cez sieť Tor.

SecureDrop[29] umožňuje zdrojom odovzdávať dokumenty spravodajskej organizácii bez prezradenia svojej polohy. Cenzurované publikácie si udržia prítomnosť napriek príkazom na stiahnutie obsahu. Fóra a trhy fungujú bez jurisdikčného vystavenia, ktoré zničilo ich centralizovaných predchodcov. A bežné služby ako Facebook a BBC prevádzkujú verzie na `.onion`, aby oslovili používateľov v krajinách s cenzúrou. Obmedzenia pretrvávajú: služby onion sú pomalšie pre množstvo skokov, dlhé náhodné adresy sa ťažko odovzdávajú a zlyhania operačnej bezpečnosti môžu prevádzkovateľov odhaliť aj inými cestami.

I2P: iná architektúra pre interné služby

I2P (Invisible Internet Project) používa podobné princípy ako Tor, ale s inými cieľmi návrhu a inými architektonickými voľbami.[7]

Cesnakové smerovanie (garlic routing) sa od cibuľového líši v podstatnej veci: dokáže zbaliť viac prvkov správy (nazývaných „strúčiky“, angl. cloves) do šifrovaných paketov namiesto toho, aby sa každá časť posielala osobitne. V súčasnej praxi I2P to často znamená jednu hlavnú správu

a k nej riadiace strúčiky. Aj tak formát sťažuje analýzu prevádzky, lebo pozorovateľ nevie ľahko rozlíšiť, ktorý prvok patrí ku ktorému komunikačnému toku.

I2P tiež používa jednosmerné tunely namiesto obojsmerných okruhov Toru. Každá komunikácia potrebuje štyri tunely: odchádzajúci a prichádzajúci pre každú stranu. Údaje poslané cez I2P idú k cieľu jednou cestou a odpovede inou. Toto architektonické rozhodnutie sťažuje pozorovanie, lebo protivník nemôže predpokladať, že spiatočná cesta zrkadlí odchádzajúcu.

I2P je uzavretá sieť, ktorá hostí skryté služby (nazývané „eepsites“) dostupné len v rámci siete; používatelia komunikujú predovšetkým s inými používateľmi I2P, namiesto anonymizácie spojení s externými webmi. Keďže prevádzka zostáva vnútri I2P, neexistujú výstupné uzly so svojimi zraniteľnosťami a problémami so zneužitím. Architektúra je distribuovaná: každý používateľ I2P smeruje prevádzku aj pre ostatných, vďaka čomu je sieť symetrickejšia než v Tore, ktorý rozlišuje klientov a relaye.

I2P má vlastné bezpečnostné problémy. Sieť sa opiera o distribuovanú databázu („netDB“), ktorú udržiavajú smerovače floodfill. Výskum z roku 2013 ukázal, že útoky typu Sybil na smerovače floodfill môžu sieť kompromitovať; útočníci, ktorí ovládali dostatok uzlov floodfill, mohli databázu zmanipulovať tak, aby umožnila deanonymizáciu.[8] Projekt I2P reagoval zavedením zmierňujúcich opatrení, vrátane rozdelenia netDB na viac podriadených databáz a zlepšenia algoritmov výberu uzlov. Podobne ako Tor sa I2P nepretržite vyvíja; objavené zraniteľnosti sa riešia aktualizáciami softvéru. Menšia sieť v porovnaní s Torom znamená menej zdrojov na bezpečnostný výskum, ale projekt sa aktívne vyvíja a na nahlásené problémy reaguje.

Kompromisy I2P sú iné než u Toru. Menej používateľov znamená menšie množiny anonymity. Tor si získal oveľa väčšiu pozornosť akademického sveta, takže bezpečnostné vlastnosti I2P sú analyzované menej dôkladne. Zameranie na interné služby robí prístup k bežnému internetu menej pohodlným než pri Tore. I2P je vhodný pre používateľov, ktorým ide najmä o komunikáciu s inými používateľmi I2P, nie o anonymný prístup do všeobecného internetu.

17.5 Mixnety: najsilnejšia ochrana

Prečo cibuľové smerovanie nestačí

Tor a I2P chránia pred protivníkmi, ktorí nevidia celú sieť. Globálny protivník však, teda taký, ktorý dokáže naraz monitorovať prevádzku vstupujúcu do siete aj vystupujúcu z nej, môže robiť časovú koreláciu. Ak správa vstúpi do Toru o 2:03:47,123 a vystúpi o 2:03:47,456, časovanie ju spája bez ohľadu na vrstvy šifrovania medzi tým.

Mixnety riešia toto obmedzenie na úrovni architektúry.

Chaumova pôvodná vízia

David Chaum navrhol mixnety v roku 1981, ešte pred vznikom Toru.[9] Myšlienka: zmiešavacie uzly správy zhromažďujú, zoskupujú do dávok, preusporiadavajú a preposielajú. Zoskupovanie a preusporiadavanie maria časovú analýzu tým, že narúšajú vzťah medzi časovaním vstupu a výstupu.

Ako miešanie maria analýzu prevádzky

Zmiešavací uzol zhromažďuje správy počas istého časového úseku. Keď ich príde dosť, zoberie ich do dávky, z každej odstráni vonkajšiu vrstvu šifrovania, dávku náhodne premieša a všetky správy odošle naraz.

Pozorovateľ, ktorý vidí správy vstupovať do zmiešavacieho uzla a vystupovať z neho, nevie spojiť vstupy s výstupmi. Časová korelácia zlyháva, lebo všetky výstupy odchádzajú spolu. Korelácia poradia zlyháva, lebo poradie je premiešané. Ani globálny protivník, ktorý vidí všetko, nevie určiť, ktorý vstup zodpovedá ktorému výstupu.

Vysoká latencia ako nevyhnutný kompromis

Silné miešanie spravidla prináša latenciu a réžiu. Správy často čakajú, kým sa nazbierajú dávky alebo kým uplynú pravdepodobnostné oneskorenia. Klasické dávkové mixnety sa zle hodia na interaktívnu komunikáciu (okamžité správy, prehliadanie webu), no hodia sa na asynchrónnu (e-mail, prenos súborov, transakcie v kryptomenách).

Kompromis je zásadný: nižšia latencia zvyčajne znamená slabšie záruky anonymity, kým vyššia latencia umožňuje väčšie účinné množiny anonymity a silnejšiu odolnosť voči analýze prevádzky. Moderné nízkolatenčné mixnety sa snažia obnoviť použiteľnosť krycou prevádzkou a inými modelmi oneskorenia, ale kompromis len zvládajú, neodstraňujú ho.

Moderné implementácie

Medzi moderné projekty mixnetov patrí Nym, ktorý používa formát paketov Sphinx[10] a ekonomické stimuly pre prevádzkovateľov zmiešavacích uzlov.[11] Nym zavádza krycú prevádzku (falošné správy), aby ešte viac sťažil analýzu prevádzky, a namiesto dobrovoľníckej prevádzky využíva stimuly založené na kryptomene. Loopix je návrh mixnetu, ktorý poskytuje neprepojiteľnosť odosielateľa a príjemcu s odolnosťou voči aktívnym útokom.

Tieto projekty sa usilujú urobiť mixnety praktickými pre moderné použitie a zachovať ich silné vlastnosti anonymity. Zásadné obmedzenie však trvá: nasadené univerzálne mixnety majú stále oveľa menej používateľov než Tor alebo bežné ekosystémy VPN. Vysokolatenčné mixnety pre e-mail

(ako historické systémy Mixmaster a Mixminion[28]) zanikli. Moderné mixnety ako Nym sú v ranom nasadení s obmedzeným rozšírením. Teoretická sila miešania je skutočná, no anonymita závisí od toho, kto ešte systém používa; mixnet s malým počtom používateľov poskytuje v praxi slabšiu anonymitu bez ohľadu na kryptografickú sofistikovanosť. Pre aplikácie, kde je latencia prijateľná a rozšírenie dostatočné, poskytujú mixnety najsilnejšiu dostupnú ochranu proti pasívnej analýze prevádzky.

17.6 Prečo nestačí jediná architektúra anonymity

Kompromis medzi latenciou a silou anonymity je štrukturálny, nie chyba návrhu. Nízkolatenčné systémy zachovávajú informácie o časovaní, ktoré môžu globálni protivníci zneužiť; vysokolatenčné systémy informácie o časovaní ničia, no neumožňujú interaktívne použitie. VPN sústreďujú dôveru u jediného poskytovateľa kvôli rýchlosti. Tor rozkladá dôveru medzi tri relaye a obetuje latenciu, aby žiadny jednotlivý bod kompromitácie neodhalil oba koncové body. Mixnety ničia časovú koreláciu zoskupovaním a preusporiadavaním za cenu interaktivity. I2P optimalizuje interné sieťové služby a akceptuje nižšiu užitočnosť navonok.

Každá architektúra odpovedá na iného protivníka. Lokálneho pozorovateľa porazí VPN, pozorovateľa časti cesty viacskokové rozloženie Toru a globálneho pasívneho pozorovateľa jedine miešanie. Univerzálne optimálny nástroj neexistuje. Praktická anonymita znamená priradiť známe obmedzenia nástroja ku skutočnej hrozbe. Protokoly aplikačnej vrstvy, ktoré preskúmame ďalej, fungujú nad akýmkoľvek transportom, ktorý používateľ zvolí; šifrovanie obsahu nenahrádza anonymitu na transportnej vrstve a anonymita na transportnej vrstve nenahrádza end-to-end šifrovanie obsahu.

17.7 Keď internet nie je sieť

Každý transport, ktorý kapitola doteraz skúmala, predpokladá fungujúci internet. Architektúra súkromia, ktorá drží len za tohto predpokladu, zlyhá proti protivníkovi, ktorý internet ovláda alebo odstaví. Odstavenia internetu na Ukrajine, v Gaze, v Mjanmarsku a v Iráne za posledné desaťročie sú bežné prevádzkové podmienky, v ktorých na súkromí záleží najviac. Mesh a offline-first transporty prenášajú informácie, keď internet nie je dostupný alebo je sám protivníkom.

Meshtastic: LoRa na okraji spektra

Meshtastic je open source protokol pre mesh siete (siete typu mesh), ktorý beží na lacných rádiách LoRa. LoRa vymieňa dátovú rýchlosť za dosah: za priaznivých podmienok dosahuje stovky bitov za sekundu na vzdialenosť niekoľkých kilometrov a ručné zariadenia stoja ako jedlo v reštaurá-

cii. Uzly si navzájom preposielajú správy bez centrálnej koordinácie, obsah je šifrovaný end-to-end a sieť nemá autoritatívny adresár ani administratívnu hranicu. Šírka pásma je taká úzka, že prakticky možno posielať len krátke textové správy, a dosah obmedzuje fyzika priamej viditeľnosti bez ohľadu na protokol. Protivník, ktorý vypne internet, nevypne rádiové spektrum, a záložné riešenie obrancu vyžaduje len to, aby dostatok účastníkov už mal potrebný hardvér.[12]

Reticulum a kryptograficky samosmerujúci stack

Reticulum Network Stack (RNS) je kryptografický sieťový stack, ktorý môže bežať nad akýmkoľvek transportom, vrátane LoRa, paketového rádia, sériových liniek a bežného TCP/IP. Adresou každého uzla je jeho verejný kľúč a neexistuje centrálna smerovacia autorita. Architektúra súkromia, ktorá využíva bežný internet, keď je dostupný, a rádioamatérske vysielanie, keď nie, bez zmeny bezpečnostného modelu, je odolnejšia než architektúra viazaná na konkrétny transport. Protivník, ktorý chce používateľovi odoprieť konektivitu, musí potom odoprieť všetky dostupné transporty naraz.[13]

Briar, BitChat a mesh v rozsahu Bluetooth

Briar synchronizuje správy cez Bluetooth, wifi a Tor bez centrálneho servera a zameriava sa na aktivistov a novinárov v kompromitovaných alebo chýbajúcich sieťach. BitChat, ktorý vydal Jack Dorsey v júli 2025, beží na mesh sieti Bluetooth Low Energy v iOS aj Androide bez telefónneho čísla a bez účtu. Využíva princíp „ulož a pošli ďalej“ (store-and-forward), takže správa dorazí k cieľu, len čo odosielateľa a príjemcu spája akákoľvek cesta sprostredkujúcich telefónov. Po spustení sa rýchlo ujal a kategória sa rozšírila, keď používatelia a novinári začali tieto nástroje nosiť do prostredí (protesty, katastrofy, odstavenia), kde sa bežnej sieti nedá dôverovať. Mesh sieť cez Bluetooth je lacný protipól k mesh sieti LoRa, s krátkym dosahom; stack obrancu môže zahŕňať obe za obmedzenú cenu.[14]

FIPS: sieťová vrstva pod vlastnou kontrolou

Free Internetworking Peering System je overlay sieť nezávislá od transportu, v ktorej si každý uzol generuje vlastnú kryptografickú identitu a smeruje bez registrácie, DHCP, DNS či akejkoľvek certifikačnej autority.[15] Smerovacia adresa uzla FIPS sa odvodzuje z páru kľúčov secp256k1, ktorý prevádzkovateľ vygeneruje offline. Sieťové kľúče pre jednotlivé zariadenia, rotovateľné nezávisle od akejkoľvek inej identity prevádzkovateľa, bránia tomu, aby sa graf spojení zlial s ďalšími doménami dôvery používateľa.

FIPS prináša do transportného stacku adresovanie pod vlastnou kontrolou spojené s nezávislosťou od transportu. Tá istá mesh sieť môže naraz zahŕňať UDP, TCP, Ethernet, Tor aj Bluetooth Low Energy a jeden paket

môže prejsť ktorýmkoľvek z nich. Spojenia medzi susednými uzlami používajú šifrovanie Noise IK, takže každé spojenie medzi uzlami je overené a dôverné, a relácie medzi koncovými bodmi používajú Noise XK s pravidelným obnovovaním kľúčov, takže sprostredkujúce smerovače poznajú len 16-bajtové skrátené adresy uzlov, nie obsah ani identity koncových bodov. Konštrukcia kostrového stromu toleruje rozdelenie siete: lokálny segment, ktorého spojenie so širšou sieťou sa preruší, funguje ďalej sám a po obnovení spojenia sa automaticky znova zlúči. Voliteľná adaptačná vrstva IPv6 mapuje adresy uzlov do rozsahu `fd00::/8`, takže nezmenené aplikácie môžu oslovovať ľubovoľný koncový bod FIPS menom hostiteľa. Kým Tor poskytuje nízkolatenčnú anonymitu nad existujúcim internetom, FIPS poskytuje adresovanie a smerovanie, ktoré existujúci internet nepotrebuje vôbec.

Rádioamatérske vysielanie a licencované spektrum

Licencované rádioamatérske vysielanie je najstaršia mesh sieť. Operátori prenášajú správy protokolmi ako Winlink, FT8, JS8Call a APRS a dosiahnu všade, kam možno namieriť anténu a získať licenciu. Predpis FCC Part 97 v USA (s obdobnými predpismi inde) zakazuje zahmlievať význam správ, čo sa vykladá ako zákaz šifrovania. Rádioamatérske vysielanie preto vo väčšine jurisdikcií môže niesť overenú, ale nie dôvernú prevádzku. Podpísaná udalosť Nostr vysielaná na rádioamatérskom pásme zostáva kryptograficky pravá, hoci jej obsah je čitateľný, a v podmienkach štátom vynúteného odstavenia obranca využije to, čo mu režim regulácie dovoľuje.[16]

Satelity a otázka suverenity

Konštelácie na nízkej obežnej dráhe (Starlink, Iridium a konkurenti) poskytujú pripojenie, ktoré nezávisí od pozemnej siete žiadneho konkrétneho štátu. Starlink bol pod politickým tlakom predmetom zdokumentovaného geofencingu; staršie siete ako Iridium majú menšiu šírku pásma a menej politickej pozornosti, a preto sa ukázali ako stabilnejšie. Satelitné spoje patria do stacku súkromia, lebo sú ortogonálne k pozemnému internetu; ktorého operátora obranca zvolí, závisí od konkrétnych politických rizík.[17]

Spoločná nit

Každý transport v tejto časti odpovedá na tú istú otázku: čo prenesie správu, keď bežná sieť nie je dostupná alebo je nepriateľská? Odpovede sa líšia dosahom, šírkou pásma, regulačným štatútom a politickým vystavením. Spoločné majú to, že každý je lacný na nasadenie v uzle, drahý na potlačenie v sieti a škálovateľný do hustoty, keď rastie úroveň hrozby. Šifrovanie

chráni to, čo sa hovorí; mesh a offline-first transporty chránia to, či sa to vôbec dá povedať.

17.8 Šifrovaná komunikácia: aplikačná vrstva

Nástroje transportnej vrstvy z predchádzajúcich častí skrývajú fakt komunikácie. Protokoly šifrovanej komunikácie skrývajú jej obsah. Obe sedia na rôznych vrstvách stacku a riešia rôzne problémy, ale ich dejiny sú prepletené: každá generácia protokolov sa snažila ochrániť viac z toho, čo predchádzajúca nechala odkryté, a zvyšné úniky motivujú práve tie nástroje transportnej vrstvy, ktoré táto kapitola už preskúmala.

PGP: šifrovanie obsahu a jeho hranice

Pretty Good Privacy, ktorý vydal Phil Zimmermann v roku 1991 a ktorý bol štandardizovaný ako OpenPGP v RFC 4880, bol prvý široko dostupný nástroj, ktorý obyčajným ľuďom umožnil šifrovať a podpisovať e-maily.[18] Jeho príchod mal politický význam: Zimmermanna tri roky vyšetrovali podľa amerických predpisov o vývoze zbraní s odôvodnením, že jeho softvér je vojenský materiál.[23] Vyšetrovanie sa zastavilo, no ukázalo, že civilný prístup k silnej kryptografii bude predmetom sporu. Kapitola o hnutí cypherpunkerov sa k tejto epizóde vracia; protokol, ktorý z nej vzišiel, ovplyvnil ďalšiu generáciu šifrovania správ.

Kryptograficky je PGP hybridná schéma. Používateľa identifikuje dlhodobý primárny kľúč, ktorý sa zvyčajne delí na podpisový primárny kľúč a jeden či viac podkľúčov na šifrovanie a overovanie. Pri odosielaní správy odosielateľ vygeneruje nový symetrický kľúč relácie, ním zašifruje obsah symetrickou šifrou a potom tento kľúč relácie osobitne zašifruje na verejný šifrovací podkľúč každého príjemcu. Podpisy nad otvoreným textom alebo šifrovým textom vytvára odosielateľov podpisový primárny kľúč alebo podpisový podkľúč. Podkľúče umožňujú rotovať prevádzkové kľúče bez opustenia dlhodobej identity, ktorá už nazbierala podpisy dôvery, no v praxi väčšina používateľov nerotuje vôbec.

Model dôvery je sieť dôvery (web of trust). Neexistuje certifikačná autorita. Používatelia si navzájom podpisujú verejné kľúče po osobnom overení a dôvera sa prenáša tranzitívne pozdĺž podpísaných reťazcov. Verejné kľúče sa zverejňujú na serveroch kľúčov a overenie sa má diať iným kanálom, často na stretnutiach na podpisovanie kľúčov (key signing parties) na konferenciách, kde účastníci kontrolujú úradné doklady a vymieňajú si odtlačky kľúčov. Model je intelektuálne elegantný a prevádzkovo nepriateľský voči každému mimo malej technickej komunity.

To, čo PGP robí dobre, je zároveň to, čo ho obmedzuje. Dlhodobé kľúče sú užitočné na podpisovanie vydaní softvéru, commitov v Gite, balíčkových repozitárov a iných artefaktov, ktorých autorstvo má byť dokázateľné roky; preto PGP prežíva v úlohe zabezpečenia integrity dodávateľské-

ho reťazca aj tam, kde sa pre komunikáciu opustilo. Rovnaká dlhá životnosť je záťaž pri živej korešpondencii. PGP neposkytuje dopredné utajenie (forward secrecy): kto kompromituje dlhodobý súkromný kľúč, či už zhabaním zariadenia, malvérom, súdnym príkazom na vydanie kľúča alebo tichým pokrokom v dešifrovaní, môže dešifrovať každú minulú správu, ktorá bola na tento kľúč zašifrovaná. Podpisy sú z návrhu nepopierateľné, čo je žiaduca vlastnosť pri vydaniach softvéru a nesprávna vlastnosť pri osobnom rozhovore; ledabolá poznámka poslaná jednému človeku sa stane trvalým kryptografickým dôkazom autorstva, ktorý odosielateľ už nemôže poprieť.

Aj infraštruktúra dôvery v praxi zlyhala. Väčšina používateľov sa nikdy nezúčastnila podpisovania kľúčov a stiahnuté kľúče nevedela zmysluplne overiť. Zoskupenie serverov kľúčov SKS, ktoré roky slúžilo ako de facto systém distribúcie kľúčov, nemalo ochranu proti zneužitiu. V roku 2019 útočník zistil, že zahltenie kľúča státisícmi bezvýznamných podpisov vytvorí súbor kľúča taký veľký, že GnuPG pri pokuse o import zamrzne alebo spadne, a kľúče významných správcov projektov boli otrávené rýchlejšie, než ich stihli rotovať. Sieť serverov kľúčov sa už nezotavila. Existujú novšie mechanizmy distribúcie, vrátane štandardu Web Key Directory, ktorý doméne umožňuje zverejniť kľúče na známej URL pod vlastnou autoritou, servera kľúčov Hagrid, ktorý prevádzkuje projekt Sequoia podľa prísnejších pravidiel overovania, a oportunistickej výmeny kľúčov Autocrypt zabudovanej do klientov ako Thunderbird a K-9 Mail. Žiadny z nich však nevytvoril jedinú fungujúcu náhradu za to, čo mal robiť SKS, a moderný svet OpenPGP je roztrieštený medzi súperiace implementácie ako GnuPG, Sequoia, RNP a OpenPGP.js, pričom fork LibrePGP sa v roku 2024 oddelil od RFC 9580.

Použiteľnosť je známy problém odvtedy, čo PGP existuje. Štúdia z roku 1999 „Prečo Johnny nevie šifrovať“ (angl. „Why Johnny Can't Encrypt“) testovala PGP 5.0 na vzdelaných používateľoch a zistila, že väčšina nevedela spoľahlivo šifrovať ani dešifrovať poštu bez chýb, ktoré ochranu zmarili. Neskoršia práca z roku 2015 zistila rovnaké nedostatky nevyriešené v modernom Mailvelope a podobných nástrojoch. Model rozhrania nikdy nezodpovedal pojmovému modelu a pojmový model nikdy nezodpovedal tomu, čo používatelia potrebovali.

PGP navyše šifruje len obsah. Hlavičky e-mailu, predmety správ, adresy príjemcov, časové značky a identifikátory kľúčov v šifrovaných paketoch správ putujú v otvorenej podobe, takže pasívny pozorovateľ dokáže zrekonštruovať celý sociálny graf a časový vzorec údajne súkromnej korešpondencie. Pre bezpečnú komunikáciu PGP vyrieši jeden problém a mnoho ďalších nechá viditeľných. Protokoly, ktoré prišli po ňom, brali každú z týchto odkrytých plôch ako problém, ktorý treba riešiť výslovne.

OTR: dopredné utajenie a popierateľnosť pre živý chat

Off-the-Record Messaging, ktorý v roku 2004 predstavili Nikita Borisov, Ian Goldberg a Eric Brewer, bol zámernou odpoveďou na model PGP.[19] Ich štúdia o svojom cieli hovorí priamo: kryptografia v štýle PGP spôsobuje, že živý rozhovor nevyzerá ako živý rozhovor. Bežná reč je overená v okamihu, keď odznie, ale potom nezanecháva trvalý dôkaz, a hovoriaci môžu neskôr poprieť, čo povedali, bez toho, aby proti nim stál nejaký kryptografický nástroj. OTR sa spýtal, ako by vyzerala kryptografia, ktorá sa správa rovnako, a odpoveď postavil nad existujúcimi nosičmi okamžitých správ, najmä XMPP, AIM, ICQ a IRC.

Protokol poskytuje štyri vlastnosti: šifrovanie, overenie, dokonalé dopredné utajenie a popierateľnosť. Overenie beží na výmene Diffie-Hellman pre každú reláciu, ktorú pri nadviazaní relácie raz podpíšu dlhodobé identitné kľúče, takže strany preukážu, kto sú, na začiatku rozhovoru a nemusia podpisovať každú správu. Integrita správ stojí na autentifikačných kódoch správ (MAC) namiesto digitálnych podpisov, pretože kľúče MAC sú symetrické a zdieľané oboma účastníkmi; ktorákoľvek strana mohla vytvoriť ľubovoľný MAC, takže žiadny MAC sám osebe nie je dôkazom proti druhej strane. Keď už kľúč MAC nie je potrebný na overenie, OTR ho zverejní v prenose, čím zo záznamov rozhovorov spätne urobí falzifikáty, ktoré môže vytvoriť ktokoľvek, kto ich neskôr získa. Páry kľúčov Diffie-Hellman sa počas relácie posúvajú vpred ako račňa, keď sa vymieňa nový kľúčový materiál, takže kompromitácia jediného dočasného kľúča kompromituje len malé okno správ.

Ďalším problémom popierateľnosti, ktorý OTR riešil, je samotné overenie identity. Spýtať sa cez nedôveryhodný kanál „je toto Alice?“ je ťažké, ak odpoveď musí byť pre sieťového útočníka nepadelateľná, no kanál je jediný dostupný. OTR to vyriešil protokolom socialistického milionára (Socialist Millionaire Protocol),[24] interaktívnou konštrukciou s nulovou znalosťou, ktorá dvom stranám umožňuje potvrdiť, že poznajú rovnakú tajnú odpoveď na dohodnutú otázku, bez toho, aby odpoveď prezradili komukoľvek, vrátane druhej strany, ak odpovedala nesprávne. V praxi to dvom ľuďom, ktorí spolu už poznajú niečo súkromné (spoločnú minulosť, frázu dohodnutú osobne), umožňuje overiť si navzájom identitu bez výmeny dlhých odtlačkov kľúčov a bez vytvorenia podpisu, ktorý by mohol ktokoľvek zopakovať.

Prínos OTR bol pojmový: ukázal, že dopredné utajenie a popierateľné overenie sa dajú dosiahnuť súčasne pre interaktívne použitie a že súbor vlastností, ktorý má bežný rozhovor, sa dá kryptograficky reprodukovať. Protokol sa spočiatku šíril ako zásuvný modul libpurple pre Pidgin a Adium[25] a neskôr ho začlenili klienti ako Jitsi, ChatSecure, CryptoCat a Tor Messenger. OTR verzie 3, vydaný v roku 2012, pridal podporu viacerých inštancií, aby mohol používateľ spúšťať OTR z viac než jedného kli-

enta naraz. OTRv4, ktorý od roku 2017 navrhoval tím OTR Development Team, nahradil pôvodnú výmenu kľúčov popierateľnou autentifikovanou výmenou kľúčov a pridal konštrukciu s dvojitou račňou inšpirovanú prácou, z ktorej vznikol Signal.[26]

Úpadok mal prevádzkový dôvod. OTR predpokladal, že obe strany sú online naraz, aby mohla prebehnúť interaktívna výmena kľúčov, a predpokladal jednu dlhodobú reláciu na dvojicu zariadení. Éra smartfónov rozbila oba predpoklady. Mobilní klienti sa odpájali vždy, keď sa zamkla obrazovka alebo vypadlo pripojenie, a používatelia získali viac zariadení, ktoré mali zdieľať jeden rozhovor. OTR nikdy nezískal natívnu asynchrónnu podporu ani podporu viacerých zariadení na úrovni, akú mobilní používatelia očakávali od iMessage a WhatsAppu, a samotné siete XMPP, ktoré hostili väčšinu rozhovorov OTR, sa zmenšovali, keď používatelia prešli na integrované platformy. Nástupnícky protokol prevzal myšlienku račne z OTR do architektúry navrhnutej pre nové obmedzenia.

Signal: asynchrónne dopredné utajenie v rozsahu smartfónov

Protokol Signal, ktorý vyvinuli Trevor Perrin a Moxie Marlinspike v Open Whisper Systems, je motorom samotného Signalu aj end-to-end šifrovania, ktoré nasadili WhatsApp, Google Messages, Meta Messenger a väčšina ostatných hlavných komunikačných aplikácií, ktoré sa hlásia k E2EE.[2027] Sú to dva samostatné protokoly, ktoré pracujú po sebe.

X3DH dokončí dohodu o kľúčoch, aj keď je druhá strana offline, kombináciou vopred zverejnených kľúčov. Potom Double Ratchet mení kľúče po každej správe a poskytuje dopredné utajenie (minulé správy zostanú chránené, ak sa kompromituje aktuálny stav) aj bezpečnosť po kompromitácii (budúce správy sú opäť chránené, keď je útočník po jednom kole výmeny vylúčený). Doručenie v inom poradí sa rieši ukladaním kľúčov preskočených správ v ohraničených oknách.

Signal je nasadený v mimoriadnom rozsahu a v roku 2023 priniesol postkvantovú dohodu o kľúčoch (PQXDH). Čo natívne nerieši, je skupinová komunikácia. Skupiny v Signali sú implementované cez „sender keys“: každý účastník rozosiela ostatným symetrickú račňu cez ich párové kanály Double Ratchet. Pridanie alebo odobratie člena či rotácia kľúčov po kompromitácii stojí O(N) párových operácií, čo obmedzuje praktickú veľkosť skupín a robí bezpečnosť po kompromitácii pri väčšom rozsahu drahou. Signal tiež neskrýva, kto s kým hovorí; zapečatený odosielateľ (sealed sender) a súkromné vyhľadávanie kontaktov sú doplnky aplikačnej vrstvy nad protokolom, ktorý na doručovanie správ stále potrebuje centrálny server. Server Signalu je jediný cieľ na vypnutie.

Noise: rámec pre zabezpečené kanály

Signal a MLS riešia problém komunikačných aplikácií. Noise Protocol Framework, ktorý v roku 2016 zverejnil Trevor Perrin, rieši vrstvu pod nimi: ako vôbec zostaviť overený a dôverný kanál medzi dvoma stranami bez hierarchie certifikátov, z ktorej vychádza TLS. Noise nie je protokol, ale stavebnica. Návrhár vyberie vzor nadviazania spojenia (handshake pattern; IK, XK, XX a ďalšie sa pomenúvajú podľa tvaru overenia), krivku Diffie-Hellman (25519 alebo 448), šifru (ChaCha20-Poly1305 alebo AES-GCM) a haš (SHA-256, SHA-512 alebo BLAKE2) a rámec z toho odvodí konkrétny protokol, ktorého vlastnosti určuje zvolený vzor. Dopredné utajenie, vzájomné overenie a voliteľné skrývanie identity sú záruky na úrovni vzoru, nie podrobnosti implementácie.

Vzory nesú svoje vlastnosti v názve. IK znamená, že iniciátor vopred pozná statický kľúč respondenta, a môže ho teda overiť už pri prvej správe. XK je rovnaký vzor, kde je identita iniciátora skrytá, kým sa respondent nepreukáže, čo sa hodí, keď chce iniciátor zostať anonymný pred pasívnymi pozorovateľmi. XX je vzájomné overenie bez toho, aby jedna strana vopred poznala statický kľúč druhej, čo je vzor, ktorému sa približuje TLS 1.3. Bezpečnostné vlastnosti každého vzoru sú formálne analyzované a nadviazanie spojenia postavené na pomenovanom vzore tieto vlastnosti dedí z konštrukcie.

WireGuard používa Noise_IK_25519_ChaChaPoly_BLAKE2s na nadviazanie spojenia VPN, a preto partner WireGuardu vytvorí šifrovaný tunel jedným kolom výmeny a formát nadviazania je dosť malý, aby sa zmestil do paketu UDP. Z Noise vychádza aj X3DH v Signali a transport NTCP2 v I2P. Šifrovanie transportu BOLT #8 v Lightningu používa Noise_XK na komunikáciu medzi uzlami, takže každé vytvorenie kanála zahŕňa vzájomne overené nadviazanie spojenia so súkromím identity respondenta. FIPS používa Noise_IK na spojenia medzi susednými uzlami a Noise_XK na šifrovanie na úrovni relácie, a preberá tak stručnosť nadviazania aj formálnu analýzu pomenovaných vzorov. Rámec sa stal predvolenou konštrukciou pre nové návrhy zabezpečených kanálov, lebo návrhárska práca je už urobená: autor protokolu vyberie vzor, ktorého vlastnosti zodpovedajú modelu protivníka, a získa dokázanú konštrukciu bez toho, aby písal novú.

MLS: skupinová komunikácia ako štandard

Messaging Layer Security, štandardizovaný ako RFC 9420 v IETF v roku 2023, je prvou odpoveďou na úrovni štandardov na problém škálovania skupín, ktorý návrh Signalu nevedel efektívne vyriešiť.[21] MLS je protokol priebežnej skupinovej dohody o kľúčoch: overená výmena kľúčov navrhnutá od začiatku pre skupiny, nie pre dvojice, ktorá škáluje od dvoch členov až po desaťtisíce, ktoré RFC uvádza ako pracovný rozsah.

MLS používa strom račne (ratchet tree), ktorý znižuje náklady na pridanie, odobratie alebo aktualizácie člena na O(log N) operácií oproti párovým „sender keys“ Signalu s O(N). Životnosť skupiny postupuje cez výslovné prechody epoch, ktoré vnášajú novú entropiu, a noví členovia dostávajú stav skupiny asynchrónne cez KeyPackages v štýle prekľúčov (prekey).

Bezpečnostné vlastnosti, ktoré MLS z tejto štruktúry zdedí, sú presne to, čo Signal poskytuje po dvojiciach, povýšené na skupiny: dopredné utajenie rotáciou epoch a bezpečnosť po kompromitácii, pretože každý commit od kompromitovaného člena alebo o ňom vnesie entropiu, ktorú útočník neovláda. Ochranu metadát MLS ponecháva okolitému systému. RFC výslovne uvádza, že doručovacia služba vidí identifikátory skupín, frekvenciu správ a počty členov. Skrývať sociálny graf okolo správ nie je úlohou MLS. Cisco Webex, Wire, RingCentral a Matrix nasadili MLS do produkcie a Universal Profile 3.0 združenia GSMA určuje MLS pre end-to-end šifrovanie v RCS interoperabilné medzi operátormi,[33] pričom podobné plány oznámili aj pre iMessage. Pracovná skupina IETF MIMI stavia na MLS, aby splnila európske požiadavky na interoperabilitu.[34]

Osobitná línia nasadenia skladá MLS s decentralizovanou vrstvou relayov, ktorú skúma kapitola 21. Protokol Marmot používa kľúče Nostr ako autentifikačnú službu MLS a relaye Nostr ako doručovaciu službu MLS, takže časti identity a transportu, ktoré MLS zámerne nechalo abstraktné, dopĺňa infraštruktúra, ktorú nekontroluje žiadny jediný subjekt. Marmot rieši aj medzeru v metadátach, ktorú RFC pripúšťa. Každá skupinová správa sa publikuje pod novým dočasným párom kľúčov na vrstve relayov namiesto identitného kľúča používateľa a verejný identifikátor skupiny je rotovateľné pseudo-ID namiesto skutočného ID skupiny MLS. Uvítacie správy sú zabalené do obálok gift-wrap v štýle cibule, ktoré skrývajú odosielateľa aj príjemcu pred relayami, ktoré ich prenášajú. White Noise, vlajkový klient protokolu Marmot, je k dispozícii na zariadeniach s Androidom a iOS a začiatkom roka 2026 sa dokončil audit špecifikácie od firmy Least Authority.[32] Kapitola 21 túto kompozíciu rozoberá podrobne; tu ide o to, že práve zámerné oddelenie kryptografického jadra od overovania a doručovania v MLS takúto kompozíciu vôbec umožňuje.

Čo ukazuje tento vývoj

Každá generácia vyriešila základný problém, ktorý predchádzajúca nechala otvorený, a odhalila ďalší. PGP chránil obsah a vystavil všetko ostatné. OTR chránil živý rozhovor, no predpokladal synchrónne použitie na jednom zariadení. Signal urobil silné E2EE asynchrónnym a všadeprítomným pre dvojice, ale slabo škáloval na skupiny a závisel od centrálneho servera. MLS štandardizoval efektívne skupinové šifrovanie, no problém metadát pri doručovacej službe nechal na okolitý systém. Ten okolitý sys-

tém je presne to, čo sa snažia riešiť nástroje transportnej vrstvy z častí 17.3 až 17.5: aj najsilnejšie šifrovanie aplikačnej vrstvy necháva doručovacej infraštruktúre schopnosť pozorovať vzorce komunikácie, takže obe vrstvy sa skladajú, len keď sú prítomné obe. Kapitola 21 ukazuje, ako možno decentralizovanú vrstvu relayov skombinovať s MLS, aby sa táto medzera zatvorila viac.[22]

Zhrnutie kapitoly

Odhalenie metadát je štrukturálny problém, ktorý šifrovanie obsahu nevyrieši. Návrh internetu vkladá identifikátory odosielateľa a príjemcu do každého paketu a zašifrovanie obsahu necháva vzorce komunikácie, časovanie, frekvenciu a objem viditeľné pre každého pozorovateľa na trase. Anonymné komunikačné architektúry tvoria spektrum vymedzené kompromisom medzi latenciou a anonymitou. VPN premiestňujú dôveru k jedinému poskytovateľovi výmenou za rýchlosť; cibuľové smerovanie rozkladá dôveru medzi viac relayov, takže žiadny uzol sa nedozvie oba koncové body; mixnety ničia časovú koreláciu zoskupovaním a preusporiadavaním za cenu latencie, ktorá vylučuje interaktívne použitie. Vhodný nástroj určuje model protivníka. Lokálneho pozorovateľa porazí VPN, pozorovateľa časti cesty viacskokové rozloženie Toru a globálneho pasívneho pozorovateľa jedine miešanie. Keď je protivníkom samotný bežný internet, mesh a offline-first transporty (Meshtastic, Reticulum, Briar, BitChat, FIPS, rádioamatérske vysielanie, satelity) prenášajú správy po infraštruktúre, ktorú nekontroluje žiadny jediný štát. Architektúra súkromia profituje z toho, že skladá niekoľko týchto transportov, aby protivník, ktorý chce odoprieť konektivitu, musel odoprieť všetky dostupné kanály naraz.

Protokoly aplikačnej vrstvy postupne rozširovali to, čo šifrovanie chráni. PGP šifroval obsah a všetko ostatné nechal odkryté. OTR pridal doprednú utajenie a popierateľnosť pre živý chat. Signal urobil asynchrónnu komunikáciu s doprednym utajením praktickou v rozsahu smartfónov. Noise sa stal predvolenou konštrukciou pre nové zabezpečené kanály. MLS poskytuje rovnaké bezpečnostné záruky v štýle Signalu pre skupiny pri O(log N) operáciách a vyšiel ako štandard IETF v roku 2023. Každá generácia vyriešila to, čo predchádzajúca nechala otvorené, a problém metadát pri doručovacej službe prenechala vrstvám pod sebou. Žiadny jediný nástroj neposkytuje úplnú anonymitu a každá architektúra má štrukturálne obmedzenia dané jej kompromismi. Kapitola 22 sa venuje praktikám operačnej bezpečnosti, ktoré architektonickú ochranu dopĺňajú, a kapitola 20 skúma osobitné problémy metadát, ktoré pre peňažné súkromie vytvára transparentnosť Bitcoinu v reťazci a graf kanálov Lightningu.

Poznámky

[1] Citát sa všeobecne pripisuje Michaelovi Haydenovi z debaty na Johns Hopkins University v roku 2014. Pozri David Cole, "We Kill People Based on Metadata," *New York Review of Books*, May 10, 2014. Staršie štrukturálne vyjadrenie rovnakého problému dosjé v transakčných systémoch pozri David Chaum, "Security Without Identification: Card Computers to Make Big Brother Obsolete," *Communications of the ACM* 28, no. 10 (1985): 1030-1044, archivované na `https://nakamotoinstitute.org/library/security-without-identification/`.

[2] Roger Dingledine, Nick Mathewson, and Paul Syverson, "Tor: The Second-Generation Onion Router," *Proceedings of the 13th USENIX Security Symposium* (2004): 303-320. The Tor Project, `https://www.torproject.org/`.

[3] Úplný prehľad útokov na Tor pozri v repozitári „Attacks on Tor", ktorý spravujú bezpečnostní výskumníci, dostupnom na `https://github.com/Attacks-on-Tor/Attacks-on-Tor`.

[4] K rozpoznávaniu webov podľa prevádzky pozri Giovanni Cherubin et al., "Online Website Fingerprinting: Evaluating Website Fingerprinting Attacks on Tor in the Real World," *USENIX Security Symposium* (2022). Štúdia zistila, že presnosť rýchlo klesá, keď sa v realistických podmienkach sleduje väčšia množina webov.

[5] K operácii Torpedo pozri Kevin Poulsen, "FBI Used Drive-By-Downloads to Expose Tor Pedophiles," *Infosecurity Magazine*, August 2014. NIT (Network Investigative Technique) zneužila zraniteľnosť Flashu na odhalenie skutočných IP adries.

[6] The Tor Project, "Tor Security Advisory: 'Relay Early' Traffic Confirmation Attack," July 30, 2014, dostupné na `https://blog.torproject.org/tor-security-advisory-relay-early-traffic-confirmation-attack/`. Pozri tiež Philipp Winter et al., "Identifying and Characterizing Sybils in the Tor Network," *USENIX Security Symposium* (2016).

[7] K technickej dokumentácii I2P pozri `https://geti2p.net/en/docs`. Konkrétne k cesnakovému smerovaniu pozri `https://geti2p.net/en/docs/how/garlic-routing`.

[8] Christoph Egger et al., "Practical Attacks Against the I2P Network," *RAID Symposium* (2013). Výskumníci predviedli úspešné útoky s použitím len 20 škodlivých uzlov floodfill. K modelu hrozieb a zmierňujúcim opatreniam I2P pozri `https://geti2p.net/en/docs/how/threat-model`.

[9] David Chaum, "Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms," *Communications of the ACM* 24, no. 2 (1981): 84-90.

[10] K formátu paketov Sphinx, ktorý používajú moderné mixnety, pozri George Danezis and Ian Goldberg, "Sphinx: A Compact and Provably Secure Mix Format," *IEEE Symposium on Security and Privacy* (2009), `https://cypherpunks.ca/~iang/pubs/Sphinx_Oakland09.pdf`. K návrhu Loopix, z ktorého Nym čiastočne vychádza, pozri Ania M. Piotrowska et al., "The Loopix Anonymity System," *USENIX Security Symposium* (2017).

[11] Claudia Diaz, Harry Halpin, and Aggelos Kiayias, "The Nym Network," dostupné na `https://nym.com/`.

[12] Meshtastic je dominantný open source protokol pre mesh siete LoRa; Heltec, LILYGO a RAK Wireless sú tri hlavní výrobcovia hardvéru, na ktorých zariadeniach beží. Meshtastic project, `https://meshtastic.org/`, so zdrojovým kódom na `https://github.com/meshtastic`. Špecifikáciu modulácie LoRa spravuje LoRa Alliance na `https://lora-alliance.org/`. Hardvér: Heltec Automation, `https://heltec.org/`; LILYGO, `https://www.lilygo.cc/`; RAK Wireless, `https://www.rakwireless.com/`. Správy o nasadeniach v rozsahu podujatí

v komunitnom spravodajstve z bezpečnostných konferencií, ako je DEF CON, a podobných stretnutí od roku 2022.

[13] Reticulum je kryptografický sieťový stack nezávislý od transportu, v ktorom je adresou každého uzla jeho verejný kľúč; NomadNet a LXMF sú komunikačné aplikácie postavené nad ním. Reticulum Network Stack, `https://reticulum.network/`, dokumentácia na `https://markqvist.github.io/Reticulum/manual/`. NomadNet, `https://github.com/markqvist/NomadNet`. LXMF (Lightweight Extensible Message Format), `https://github.com/markqvist/LXMF`.

[14] Briar a BitChat sú dve referenčné komunikačné aplikácie s mesh sieťou cez Bluetooth; Briar je nástroj pre aktivistov a novinárov so synchronizáciou cez Tor a desaťročnou históriou recenzovania odborníkmi, BitChat (spustený v júli 2025 projektom spájaným s Jackom Dorseym) je vstup na masový trh s registráciou bez účtu a distribúciou pre iOS a Android. Briar, `https://briarproject.org/`, so zdrojovým kódom na `https://code.briarproject.org/briar/briar`. K návrhu a modelu hrozieb Briaru pozri Michael Rogers and Eleanor Saitta, "Briar: Private Messaging, Local Networks, and Censorship Resistance" (2018), `https://briarproject.org/publications/`. BitChat, `https://bitchat.free/`, so zdrojovým kódom na `https://github.com/permissionlesstech/bitchat`. K bezpečnostnému výskumnému odporu voči neauditovaným návrhom mesh sietí cez Bluetooth pozri Matthew Green a správy o audite od Trail of Bits na `https://blog.cryptographyengineering.com/`.

[15] FIPS (Free Internetworking Peering System) je samoorganizujúca sa overlay sieť nezávislá od transportu, v ktorej si každý uzol generuje vlastný pár kľúčov secp256k1 ako smerovaciu identitu, nezávislú od akéhokoľvek poskytovateľa internetu, regionálneho internetového registra či certifikačnej autority. FIPS, `https://github.com/jmcorgan/fips`, s dokumentáciou návrhu protokolu na `https://github.com/jmcorgan/fips/tree/master/docs/design`. Vydané pod licenciou MIT; v čase písania vo verzii v0.2.0. Rámec protokolov Noise, `https://noiseprotocol.org/`, je základom šifrovania medzi susednými uzlami (Noise IK) aj na úrovni relácie (Noise XK). Voliteľná adaptačná vrstva IPv6 mapuje adresy uzlov do rozsahu `fd00::/8`, takže nezmenené aplikácie môžu oslovovať ľubovoľný koncový bod FIPS.

[16] Americký predpis FCC Part 97 a obdobné predpisy vo väčšine jurisdikcií zakazujú šifrovanie na rádioamatérskych pásmach; Winlink, FT8, JS8Call a APRS sú nasadené dátové režimy; rádioamatérske vysielanie pri týchto režimoch nesie overenú, ale nie dôvernú prevádzku. Pravidlá FCC Part 97 na `https://www.ecfr.gov/current/title-47/chapter-I/subchapter-D/part-97`. Winlink, `https://www.winlink.org/`. FT8 (súčasť softvérovej sady WSJT-X), `https://wsjt.sourceforge.io/`. JS8Call, `http://js8call.com/`. APRS (Automatic Packet Reporting System), `http://www.aprs.org/`. K podpísaným udalostiam Nostr prenášaným po overených, ale nešifrovaných amatérskych pásmach pozri komunitné správy z priesečníka HamRadio + Nostr na `https://github.com/search?q=nostr+ham+radio`.

[17] Starlink, Iridium, OneWeb a Globalstar prevádzkujú konštelácie na nízkej obežnej dráhe, ktoré prenášajú prevádzku nezávisle od pozemnej infraštruktúry akéhokoľvek štátu; geofencing a výpadky Starlinku v bojových zónach dokazujú, že žiadnemu jedinému operátorovi sa politicky nedá dôverovať a že ortogonálny transport v obrannom stacku je lepší než spoliehanie sa na ktorýkoľvek jeden satelitný spoj. Starlink, `https://www.starlink.com/`. Iridium, `https://www.iridium.com/`. OneWeb (prevádzkuje Eutelsat Group), `https://oneweb.net/`. Globalstar, `https://www.globalstar.com/`. K zdokumentovaným výpadkom Starlinku na Ukrajine pozri správy v *Financial Times*, *Reuters* a verejné vyjadrenia Elona Muska na

X/Twitteri archivované na `https://web.archive.org/`. K incidentom s geofencingom pozri vyjadrenia ukrajinského ministerstva obrany v rokoch 2023–2024.

[18] J. Callas et al., "OpenPGP Message Format," RFC 4880 (November 2007); aktualizované RFC 9580 (July 2024) a rozštiepené špecifikáciou LibrePGP. K použiteľnosti a architektonickým limitom PGP pozri Alma Whitten and J. D. Tygar, "Why Johnny Can't Encrypt," *USENIX Security Symposium* (1999); Scott Ruoti et al., "Why Johnny Still, Still Can't Encrypt: Evaluating the Usability of a Modern PGP Client," *arXiv:1510.08555* (2015); a Matthew Green, "What's the Matter with PGP?" (2014), dostupné na `https://blog.cryptographyengineering.com`. K otráveniu serverov kľúčov SKS v roku 2019 pozri Daniel Kahn Gillmor, "OpenPGP Certificate Flooding," a Robert J. Hansen, "SKS Keyserver Network Under Attack" (June 2019), druhé na `https://gist.github.com/rjhansen/67ab921ffb4084c865b3618d6955275f`. K štandardu Web Key Directory pozri návrh IETF na `https://datatracker.ietf.org/doc/draft-koch-openpgp-webkey-service/`. K Autocrypt pozri `https://autocrypt.org`.

[19] Nikita Borisov, Ian Goldberg, and Eric Brewer, "Off-the-Record Communication, or, Why Not To Use PGP," *Workshop on Privacy in the Electronic Society* (2004). Špecifikácia na `https://otr.cypherpunks.ca/`.

[20] K špecifikáciám protokolu Signal pozri Moxie Marlinspike and Trevor Perrin, "The X3DH Key Agreement Protocol" (2016) a "The Double Ratchet Algorithm" (2016), obe na `https://signal.org/docs/`. K formálnej analýze pozri Katriel Cohn-Gordon et al., "A Formal Security Analysis of the Signal Messaging Protocol," *IEEE European Symposium on Security and Privacy* (2017). Postkvantové rozšírenie: "The PQXDH Key Agreement Protocol," 2023. Špecifikácia Noise Protocol Framework, Trevor Perrin, "The Noise Protocol Framework," revision 34 (2018), `https://noiseprotocol.org/noise.html`, je referenciou pre taxonómiu vzorov nadviazania spojenia. Nasadenia odvodené z Noise zahŕňajú WireGuard (Jason Donenfeld, "WireGuard: Next Generation Kernel Network Tunnel," *NDSS* 2017), šifrovanie transportu BOLT #8 v Lightningu, transport NTCP2 v I2P a šifrovanie medzi susednými uzlami a na úrovni relácie vo FIPS.

[21] R. Barnes et al., "The Messaging Layer Security (MLS) Protocol," RFC 9420 (July 2023); R. Barnes et al., "The Messaging Layer Security (MLS) Architecture," RFC 9750 (2024). Základný návrh stromu račne pochádza z práce Katriel Cohn-Gordon et al., "On Ends-to-Ends Encryption: Asynchronous Group Messaging with Strong Security Guarantees," *ACM CCS* (2018).

[23] Vyšetrovanie Phila Zimmermanna americkou vládou kvôli vývozu zbraní podľa predpisov International Traffic in Arms Regulations (ITAR) trvalo od roku 1993 do roku 1996 a ukázalo, že civilný prístup k silnej kryptografii bude právne sporný. Prípad sa zastavil bez obvinenia, no jeho odrádzací účinok na vývoz kryptografie formoval naliehavosť cypherpunkového hnutia. Philip R. Zimmermann, *The Official PGP User's Guide* (MIT Press, 1995), dokumentuje návrh PGP a politický kontext. Prípad ITAR je zdokumentovaný v Simson Garfinkel, *PGP: Pretty Good Privacy* (O'Reilly, 1994), s. 81–102, a v Steven Levy, *Crypto: How the Code Rebels Beat the Government Saving Privacy in the Digital Age* (Viking, 2001), s. 199–230. Vlastný opis Phila Zimmermanna je na `https://web.archive.org/web/20240101000000/https://philzimmermann.com/EN/background/index.html`.

[24] Protokol socialistického milionára (SMP) je test rovnosti s nulovou znalosťou, ktorý OTR používa na vzájomné overenie identity bez výmeny dlhých odtlačkov kľúčov. Odvodzuje sa z práce Fabrice Boudot, Berry Schoenmakers, and Jacques Traoré, "A Fair and Efficient Solution to the Socialist Millionaires' Problem," *Discrete Applied Mathematics* 111, no. 1–2 (2001): 23–36. Úprava SMP v OTR je určená v protokole OTR verzie 2 a v neskorších špecifikáciách na `https://otr.cypherpunks.ca/Protocol-v3-4.1.1.html`; konkrétna

implementácia ako interaktívneho dôkazu s nulovou znalosťou, že dve strany zdieľajú spoločné tajomstvo bez jeho odhalenia, je v oddiele 2.6 tohto dokumentu.

[25] Pidgin je multiprotokolový klient okamžitých správ, ktorého architektúra zásuvných modulov libpurple umožnila počiatočnú distribúciu OTR; Adium je jeho ekvivalent pre macOS. Pôvodný zásuvný modul OTR pre libpurple na `https://otr.cypherpunks.ca/`. Projekt Pidgin na `https://www.pidgin.im/`. Projekt Adium na `https://adium.im/`. Knižnica libpurple, zdieľaná medzi Pidginom a Finchom, poskytla API zásuvných modulov, ktoré umožnilo dodatočne pridať OTR do AIM, ICQ, XMPP a iných protokolov bez úpravy samotných klientov.

[26] OTRv4 nahrádza pôvodnú výmenu kľúčov Diffie-Hellman popierateľnou autentifikovanou výmenou kľúčov (DAKE) vychádzajúcou z práce Yehudu Lindella a pridáva mechanizmus dvojitej račne, ktorý poskytuje dopredné utajenie na úrovni správ v rámci relácie. Špecifikácia: Nik Unger, Sofía Celi, Jurre van Bergen, and the OTR Development Team, "OTRv4," draft specification (2019–present), `https://github.com/otrv4/otrv4/blob/master/otrv4.md`. K konštrukcii popierateľnej autentifikovanej výmeny kľúčov pozri Mario Di Raimondo, Rosario Gennaro, and Hugo Krawczyk, "Deniable Authentication and Key Exchange," *ACM CCS* (2006), `https://eprint.iacr.org/2006/280`.

[27] Nasadenie protokolu Signal vo WhatsAppe v roku 2016 pre vtedajšiu 1 miliardu používateľov bolo najväčším jednorazovým zavedením end-to-end šifrovania v histórii. Moxie Marlinspike and Trevor Perrin, "WhatsApp's Signal Protocol Integration Is Now Complete," Open Whisper Systems Blog (April 5, 2016), `https://signal.org/blog/whatsapp-complete/`. Technický whitepaper je WhatsApp Inc., "WhatsApp Encryption Overview: Technical White Paper" (2016, updated 2017), `https://www.whatsapp.com/security/WhatsApp-Security-Whitepaper.pdf`. End-to-end šifrovanie RCS v Google Messages pomocou protokolu Signal je zdokumentované na `https://support.google.com/messages/answer/10262381`. Zavedenie v Meta Messengeri opisuje Jon Millican, "Messenger End-to-End Encryption Overview," Meta Engineering Blog (2023), `https://engineering.fb.com/2023/12/06/security/messenger-end-to-end-encryption-default/`.

[28] Mixmaster a Mixminion boli dve nasadené vysokolatenčné siete anonymných remailerov pre e-mail; obe už zanikli. Mixmaster bol sieť remailerov typu II; Lance Cottrell, "Mixmaster and Remailer Attacks," in *Proceedings of the Workshop on Privacy Enhancing Technologies* (1994). Mixminion bol nástupca typu III: George Danezis, Roger Dingledine, and Nick Mathewson, "Mixminion: Design of a Type III Anonymous Remailer Protocol," *IEEE Symposium on Security and Privacy* (2003), `https://mixminion.net/minion-design.pdf`. Obe siete zanikli pre nedostatočné rozšírenie, nie pre kryptografické zlyhanie, čo ilustruje dynamiku kolektívneho konania, ktorú kapitola opisuje. Archív zdrojového kódu Mixminion zostáva na `https://mixminion.net/`.

[29] SecureDrop je open source systém na odovzdávanie podkladov oznamovateľmi, ktorý vyvinula Freedom of the Press Foundation, postavený na službách onion siete Tor; nasadilo ho vyše 75 spravodajských organizácií. Freedom of the Press Foundation, `https://freedom.press/`. Projekt SecureDrop na `https://securedrop.org/`, so zdrojovým kódom na `https://github.com/freedomofpress/securedrop`. Pôvodný návrh vytvorili Aaron Swartz a Kevin Poulsen pod názvom DeadDrop; Freedom of the Press Foundation prevzala správu v roku 2013. K modelu hrozieb a architektúre SecureDropu pozri oficiálnu dokumentáciu na `https://docs.securedrop.org/en/stable/threat_model/threat_model.html`.

[30] Operácia Freedom Hosting z roku 2013 bola akcia FBI, ktorá nasadila malvér (Network Investigative Technique) cez exploit v JavaScripte proti Firefoxu 17 ESR, aby odhalila používateľov skrytých služieb Toru hostovaných na infraštruktúre Freedom Hosting. Kevin Poulsen, "FBI Allegedly Ran Tor Hidden Services, Seized Them to Unmask Child Porn Viewers," *Wired*, August 5, 2013. Následná analýza Vlada Tsyrklevicha, "Tor Browser Bundle Exploit Analysis" (August 2013), zdokumentovala mechanizmus nákladu. Exploit mieril na zraniteľnosť use-after-free vo Firefoxe (CVE-2013-1690), ktorá bola opravená v novších verziách Firefoxu, ale zostala prítomná vo vtedajšom Tor Browser Bundle; útok sa zmiernil aktualizáciou Tor Browseru a vypnutím JavaScriptu.

[31] Systém adresárových autorít Toru a jeho konsenzuálny mechanizmus sú zdokumentované v návrhovom dokumente Toru a v dir-spec. Roger Dingledine and Nick Mathewson, "Tor Protocol Specification," na `https://spec.torproject.org/`; samotný protokol adresárových autorít v "Tor directory protocol, version 3," `https://spec.torproject.org/dir-spec`. Deväť v súčasnosti uznávaných adresárových autorít a ich prevádzkovatelia sú uvedení na `https://metrics.torproject.org/rs.html#search/flag:Authority`. K bezpečnostným vlastnostiam a známym slabinám systému adresárových autorít pozri Aaron Johnson et al., "Users Get Routed: Traffic Correlation on Tor by Realistic Adversaries," *ACM CCS* (2013), `https://www.ohmygodel.com/publications/usersrouted-ccs13.pdf`.

[32] Špecifikácia protokolu Marmot a klient White Noise sú hlavnou open source implementáciou MLS nad infraštruktúrou Nostr. Špecifikácia protokolu Marmot na `https://github.com/marmot-protocol/marmot`. Klient White Noise (Android a iOS) na `https://whitenoise.chat/`. Bezpečnostný audit špecifikácie Marmot od firmy Least Authority, dokončený začiatkom roka 2026, je dostupný od Least Authority na `https://leastauthority.com/`. K obálke gift-wrap podľa NIP-17, ktorú Marmot používa na doručovanie správ so skrytými metadátami, pozri `https://github.com/nostr-protocol/nips/blob/master/17.md`.

[33] RCS Universal Profile 2.4 združenia GSMA (Rich Communication Services) zaviedol end-to-end šifrovanie a Universal Profile 3.0 určuje MLS ako protokol skupinovej dohody o kľúčoch, čo umožňuje E2EE interoperabilné medzi operátormi v správach doručovaných operátormi. GSMA, "RCS Universal Profile Service Definition Document," version 3.0 (2024), dostupné členom GSMA na `https://www.gsma.com/solutions-and-impact/technologies/networks/rcs/`. Oznámenie spoločnosti Apple o podpore RCS s end-to-end šifrovaním pre interoperabilitu iMessage: Apple Inc., "Apple Announces RCS Support" (2024), s technickými podrobnosťami v relácii WWDC 2024 "What's new in Messages for Business." Implementácia E2EE RCS v Google Messages je zdokumentovaná na `https://support.google.com/messages/answer/10262381`.

[34] Pracovná skupina IETF More Instant Messaging Interoperability (MIMI) vyvíja štandardy, ktoré umožnia end-to-end šifrovanú komunikáciu medzi rôznymi poskytovateľmi, predovšetkým na splnenie požiadaviek Európskej únie na interoperabilitu podľa nariadenia Digital Markets Act. Charta a dokumenty pracovnej skupiny IETF MIMI na `https://datatracker.ietf.org/wg/mimi/about/`. Kľúčovými dokumentmi sú formát obsahu MIMI (draft-ietf-mimi-content) a protokol MIMI (draft-ietf-mimi-protocol), oba stavajúce na MLS (RFC 9420) ako vrstve skupinovej dohody o kľúčoch. K povinnosti interoperability podľa Digital Markets Act, ktorá túto prácu motivuje, pozri Regulation (EU) 2022/1925 of the European Parliament and of the Council, Article 7, `https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R1925`.

[22] Pre čitateľov, ktorí chcú nástroje z tejto kapitoly používať: Tor Browser (torproject.org) je referenčný anonymizačný klient; Mullvad (mullvad.net) a IVPN (ivpn.net) sú poskytovatelia VPN zameraní na súkromie s najsilnejšou verejnou históriou; Signal

(signal.org) a Session (getsession.org) sú hlavné šifrované komunikačné aplikácie; Element (element.io) je referenčný klient Matrix a Wire (wire.com) nasadzuje MLS v produkcii; Nym (nym.com) je najrozvinutejší nasadený mixnet. Ako pozadie stoja za pozornosť texty Matta Blazea z okruhu *Tangled Web*, priebežné výskumné poznámky projektu Tor a príručka EFF Surveillance Self-Defense (ssd.eff.org); Moxie Marlinspike, "The Ecosystem Is Moving" (2016), `https://signal.org/blog/the-ecosystem-is-moving/`, je kanonické moderné vyjadrenie toho, prečo majú federované protokoly problém proti integrovaným platformám s end-to-end šifrovaním a prečo sa priepasť medzi nasadenou a akademickou kryptografiou stále prehlbuje. Širší politický kontext okolo tej istej infraštruktúry rozoberajú Bruce Schneier, *Data and Goliath* (2015) a Carissa Véliz, *Privacy Is Power* (2020).

18

BITCOIN A PRELOM V DIGITÁLNYCH PENIAZOCH

> *„Čisto peer-to-peer verzia elektronickej hotovosti by umožnila posielať online platby priamo od jednej strany k druhej bez sprostredkovania finančnou inštitúciou.“*
>
> Satoshi Nakamoto, „Bitcoin: A Peer-to-Peer Electronic Cash System“ (2008)[1]

Úvod

Digitálne peniaze narážali na dva základné problémy, ktoré cypherpunkový výskum nedokázal za desaťročia vyriešiť naraz. Problém dvojitého míňania akoby vyžadoval centrálnu autoritu. Problém základných peňazí zasa znamenal, že väčšina digitálnych mien bola len pohľadávkou voči emitentovi, nie peniazmi samotnými.

Nakamotov prelom vyriešil oba. Kapitola sleduje tieto dva problémy a neúspešných predchodcov, ktorí priniesli čiastkové odpovede. Končí architektúrou konsenzu, vďaka ktorej sa decentralizované digitálne peniaze konečne stali možnými.

18.1 Dva problémy digitálnych peňazí

Problém dvojitého míňania

Fyzickú hotovosť nemožno minúť dvakrát. Keď Alice podá Bobovi zlatú mincu, už ju nemá. Fyzické odovzdanie je samotná transakcia. Fyzické predmety sú prirodzene vzácne: ak ich drží jeden človek, nedrží ich iný.

Digitálna informácia túto vlastnosť nemá. Ako ukázala kapitola 6, informácia je nerivalitná: skopírovaním súboru originál nezmizne. Keby digitálna hotovosť bola súbor, ktorý kóduje hodnotu, Alice by mohla poslať Bobovi kópiu, originál si nechať a tú istú „hotovosť" poslať Carol. Problém dvojitého míňania je problém vzácnosti: ako urobiť digitálne jednotky rivalitnými, keď sa digitálna informácia dá prirodzene kopírovať?

Aby sa dvojité míňanie zabránilo, treba určiť, ktoré transakcie boli prvé, a tým aj to, kto ktorú jednotku vlastní. Zaznamenať sa to dá v databáze, ale kto ju ovláda? Kto ovláda databázu, môže cenzurovať transakcie alebo zhabať prostriedky a úrady môžu prevádzkovateľa prinútiť, aby urobil jedno či druhé. Problém akoby vyžadoval centralizáciu.

Problém základných peňazí

Aj keby sa dvojité míňanie dalo vyriešiť, zostával druhý problém: čo sa vlastne prenáša?

Dovtedajšie digitálne meny boli peňažné náhrady: pohľadávky voči emitentom, nie peniaze v pravom zmysle. Používatelia držali zostatky na účtoch, ktoré firmy sľúbili splniť, a nie samotný peňažný statok. Zostatky v DigiCash boli pohľadávkami voči DigiCash Inc. a zostatky v E-gold pohľadávkami voči e-gold Ltd. Tieto systémy vytvárali digitálne dlžobné úpisy, nie digitálne peniaze.

Peňažné náhrady vyžadujú dôveru v emitenta. Emitenti môžu zlyhať, môžu byť zatvorení, môžu odmietnuť výplatu, alebo ich môžu úrady prinútiť zmraziť účty. Peňažná náhrada v ruke je sľub. Peniaze v pravom zmysle v ruke sú samotný statok, ceniaci sa pre svoje peňažné služby bez ohľadu na to, kto by ich mal vyplatiť. Fyzické zlato nepotrebuje krytie, lebo držitelia chcú práve ten kov. Papierová poukážka na zlato vyžaduje dôveru, že sľub niekto splní, keď mu ju predložia.

Vytvoriť digitálne peniaze v pravom zmysle chce viac než digitálne sľuby. Systém musí zabrániť dvojitému míňaniu bez centrálnej kontroly a zároveň sám musí byť základnými peniazmi, nie pohľadávkou voči emitentovi. Pred Bitcoinom to nedokázal žiaden systém.

18.2 Predchodcovia a ich zlyhania

Bitcoin nevznikol z ničoho. Spojil skoršie cypherpunkové inovácie a prekročil ich hranice.

DigiCash: súkromie a ochrana pred dvojitým míňaním, ale bez decentralizácie

DigiCash Davida Chauma vyriešil dva problémy naraz. Slepé podpisy umožnili vydávajúcej banke odhaliť a odmietnuť duplicitné tokeny, hoci nevedela prepojiť výbery s vkladmi. Používatelia mohli platiť nevystopovateľne a banka mohla brániť dvojitému míňaniu. Obe úlohy akoby vy-

žadovali protichodné toky informácií, no Chaumova kryptografia medzi nimi našla cestu.[2]

DigiCash zlyhal z iných dôvodov. Vyžadoval centrálny server, teda jediný bod zlyhania, na ktorý mohli úrady zamieriť. A vydával peňažné náhrady: zostatky boli pohľadávkami voči DigiCash Inc., nie peniazmi v pravom zmysle. Keď firma v roku 1998 vyhlásila bankrot, systém zanikol spolu s ňou. Chaum vyriešil kryptografický problém, ale nie inštitucionálny.

E-gold: krytie bez odolnosti

E-gold (1996–2009) sa pokúsil vytvoriť digitálne zlato tak, že zostatky na účtoch kryl fyzickými zlatými rezervami. Prilákal milióny používateľov, no zostal peňažnou náhradou: zostatky boli pohľadávkami voči e-gold Ltd., nie samotným zlatom. Centralizovaná štruktúra ho robila zraniteľným. Americké úrady prevádzku zatvorili a jej zakladateľov stíhali. E-gold ukázal, že ani komoditné krytie nenahradí decentralizáciu.

Hashcash: dôkaz práce ako riadenie prístupu

Hashcash Adama Backa (1997) zaviedol dôkaz práce: na vytvorenie tokenu treba vynaložiť výpočtové úsilie.[3] Pôvodne mal brániť e-mailovému spamu. Tokeny Hashcash mali s peniazmi spoločnú jednu vlastnosť: nepotrebovali sľub ani krytie žiadneho emitenta. Platnosť vychádzala výlučne z dôkazu práce.

Hashcash však nikdy nemal byť peniazmi. Bol to systém riadenia prístupu. Tokeny sa viazali na konkrétnych príjemcov tak, že sa e-mailová adresa príjemcu vložila do údajov, z ktorých sa počíta haš, a každý poštový server viedol vlastnú databázu už videných tokenov a duplicity odmietal. Takýto návrh zabránil opakovanému použitiu tokenu na jednom serveri, ale nevytvoril globálnu vzácnosť. Token minutý na jednom serveri nemal vplyv na žiadny iný a neexistovala spoločná účtovná kniha ani celosieťový stav, ktoré by tokenu dali váhu mimo jeho lokálneho kontextu.

Peniaze vyžadujú globálny konsenzus: všetci účastníci sa musia zhodnúť, aké jednotky existujú a kto ich vlastní. Hashcash mal len lokálne overovanie. Ukázal, že výpočtová práca dokáže vytvárať nepadelateľné tokeny, ale prístupové práva nie sú peniaze. Chýbal spoločný, odsúhlasený záznam o vlastníctve tokenov naprieč všetkými účastníkmi.

B-money a Bit Gold: problém inflácie

B-money Weia Daia (1998) a Bit Gold Nicka Szaba (1998–2005) navrhovali systémy, v ktorých dôkaz práce priamo vytváral peňažné jednotky.[4] V B-money sa mala hodnota jednej jednotky rovnať výpočtovým nákladom na jej výrobu. V Bit Gold boli peňažnými jednotkami samotné platné haše.

Oba trpeli zásadnou chybou: s rastom výpočtového výkonu sa tokeny vyrábajú lacnejšie. Szabo si to výslovne uvedomoval. Ak by sa dalo stať „producentom s nízkymi nákladmi (o niekoľko rádov)“, dalo by sa „zaplaviť trh bit goldom“. Navrhol riešenie v podobe časového pečiatkovania, aby trhy mohli staršie haše (vtedy ťažšie vyrobiteľné) oceniť vyššie než novšie. Tým sa však ničí zameniteľnosť: nie všetky jednotky by boli rovnaké.

Ani jeden z nich nevyriešil problém distribuovaného konsenzu a oba zostali teoretické. Ich najhlbší problém bol však architektonický: zamieňali dôkaz práce s tvorbou peňazí. Ak práca vytvára peniaze, menová politika závisí od ekonomiky hardvéru.

Chýbajúce kúsky

Každý predchodca vyriešil časť hádanky, ale okruh nezatvoril. DigiCash dosiahol súkromie a vyriešil dvojité míňanie, no vyžadoval centralizáciu a vydával peňažné náhrady. E-gold dosiahol komoditné krytie, no zostal pohľadávkou voči správcovi úschovy. Hashcash ukázal nepadelateľné tokeny vytvorené výpočtovou prácou, ale ako systém riadenia prístupu, nie ako peniaze. B-money a Bit Gold opísali architektúru decentralizovaných digitálnych peňazí.

Zostali nevyriešené dva problémy. Po prvé, nikto nedosiahol decentralizovaný konsenzus o spoločnej histórii transakcií, teda mechanizmus potrebný na to, aby boli digitálne jednotky rivalitné bez centrálnej kontroly. Po druhé, systémy, ktoré používali dôkaz práce na tvorbu peňazí, viazali menovú politiku na ekonomiku hardvéru, a s rastom výpočtového výkonu tak vznikala trvalá inflácia.

Nakamoto vyriešil oba. Jeho prelom spojil decentralizovaný konsenzus o poradí transakcií s úplným oddelením dôkazu práce od tvorby peňazí.

18.3 Nakamotov konsenzus

Architektúra

Problémy sú teraz jasné. Dvojité míňanie vyžaduje globálny konsenzus o poradí transakcií. Skoršie systémy ho dosahovali cez centrálne servery, ktoré tvorili jediné body zlyhania. Dôkaz práce dokáže vytvárať nepadelateľné tokeny, ale ak sa použije na tvorbu peňazí, viaže menovú politiku na ekonomiku hardvéru. Úlohou je postaviť systém, v ktorom sa na usporiadaní transakcií môže podieľať ktokoľvek, bez centrálnej autority, na ktorú by sa dalo zamerať, a v ktorom menová politika zostáva pevná bez ohľadu na rast výpočtového výkonu.

Architektúra Bitcoinu spája distribuovanú účtovnú knihu, ktorú môže čítať ktokoľvek, s pravidlami konsenzu, ktoré každý účastník vynucuje samostatne. Spája ich mechanizmus tvorby blokov bez povolení. Účtovná

kniha zaznamenáva históriu transakcií, tvorba blokov ju predlžuje a pravidlá konsenzu určujú, ktoré predĺženia sú platné.

Ktokoľvek môže navrhnúť blok transakcií, ktorý sa pripojí k účtovnej knihe. Nie je potrebné povolenie a žiadny jediný subjekt nekontroluje, čo sa zaznamená. Účasť bez povolení však vytvára problém: čo bráni tomu, aby sa systém zahltil?

Problém odopretia služby

Ak by mohol ktokoľvek vytvárať bloky bez obmedzenia, útočník by mohol sieť zaplaviť. Každý blok musí každý uzol stiahnuť, overiť a uložiť. Aj bez zlého úmyslu by racionálni účastníci, keby bola tvorba blokov zadarmo, vyrábali bloky nepretržite, aby získali poplatky a odmeny. Sieť by sa utopila v údajoch.

Problém je väčší než len šírka pásma, lebo overovanie si vyžaduje aj výpočtové zdroje. Každá transakcia v každom bloku sa musí skontrolovať: platné podpisy, nevyčerpané vstupy, správne sumy. Ak bloky prichádzajú rýchlejšie, než ich uzly stíhajú overovať, uzly zaostávajú, a ak nestíhajú bežné uzly, môžu sa na overovaní podieľať len tí s výnimočnými zdrojmi. Systém by sa centralizoval okolo toho, kto si infraštruktúru môže dovoliť, a stratil by zmysel.

Centralizovaný systém to rieši triviálne: prevádzkovateľ rozhodne, koľko transakcií spracuje. Decentralizovaný systém prevádzkovateľa nemá. Riešenie si vyžaduje mechanizmus brzdenia, ktorý vznikne zo samotného protokolu a spomaľuje tvorbu blokov bez toho, aby nejaká autorita rozhodovala, kto smie bloky tvoriť a ako často.

Cieľom je zhruba jeden blok za desať minút v celej sieti, nech sa o tvorbu blokov pokúša koľkokoľvek účastníkov. Také tempo je dosť pomalé, aby všetky transakcie mohol overiť bežný hardvér, a dosť rýchle na praktické použitie. Otázka znie, ako toto tempo vynútiť bez obmedzovača.

Dôkaz práce ako brzda

Brzdu zabezpečuje dôkaz práce. Myšlienka pochádza z Hashcashu: výpočtová práca, ktorú je ťažké vykonať, ale triviálne overiť. Vytvorenie platného bloku vyžaduje nájsť haš určitého druhu, a to si žiada dlhý výpočet. Na overenie, že ho niekto našiel, stačí jediná operácia s hašom, takmer okamžitá.

Hlavička bloku obsahuje metadáta: haš predchádzajúceho bloku, haš zahrnutých transakcií, časovú pečiatku a nonce (pole, ktoré môže ťažiar voľne meniť). Aby ťažiar vytvoril platný blok, musí nájsť taký nonce, pri ktorom výpočet hašu z celej hlavičky dá číslo pod prahom obtiažnosti.

Kryptografické hašovacie funkcie ako SHA-256[9] dávajú výstup, ktorý je pri danom vstupe prakticky náhodný. Zmena jediného bitu na vstupe dá úplne iný haš. Medzi vstupom a výstupom neexistuje matematický vzťah,

podľa ktorého by sa dalo predpovedať, ktoré vstupy dajú nízky haš. Jediný spôsob, ako nájsť vhodný nonce, je opakovaná skúška: nastaviť nonce, vypočítať haš, skontrolovať, či spĺňa prah, zvýšiť nonce a začať odznova. Ťažiari takých operácií vykonajú miliardy za sekundu.

Tento proces dokázateľne trvá. Prah obtiažnosti určuje, koľko pokusov je v priemere treba. Ak prah vyžaduje haš začínajúci 20 nulovými bitmi, vyhovie približne jeden z milióna hašov. Pri 30 nulových bitoch približne jeden z miliardy. Prácu nemožno sfalšovať ani skrátiť. Overenie spočíva v kontrole, či haš spĺňa prah, a ktokoľvek ju urobí okamžite, jediným výpočtom hašu.

Asymetria je podstatná. Výroba je drahá, overenie lacné. Každý uzol tak môže overovať bloky bez dôvery v ťažiara a tvorba blokov je zároveň dosť nákladná na to, aby sa tempo zbrzdilo.

Úprava obtiažnosti

Dôkaz práce brzdí tvorbu blokov, ale brzda sa musí vedieť prispôsobiť. Keby bola obtiažnosť pevná, rastúci výpočtový výkon by vytváral bloky rýchlejšie a zahltil by sieť. Klesajúci výkon by tvorbu blokov spomalil natoľko, že by sa systém nedal používať. Potrebuje mechanizmus spätnej väzby.

Každých 2016 blokov (pri cieľovom tempe približne dva týždne) protokol prepočíta obtiažnosť. Porovná skutočný čas, ktorý uplynul od predchádzajúcej úpravy, s očakávaným (2016 blokov krát desať minút). Ak bloky v priemere prichádzali rýchlejšie než za desať minút, obtiažnosť sa zvýši: prah klesne a vyžadujú sa haše s viac začiatočnými nulami. Ak prichádzali pomalšie, obtiažnosť sa zníži: prah stúpne a prijmú sa haše, ktoré by predtým boli odmietnuté.

Úprava je ohraničená: obtiažnosť sa v jednom období nemôže zmeniť o viac než štvornásobok v žiadnom smere. Tým sa predchádza extrémnym výkyvom, ak sa hashrate (výpočtový výkon siete) prudko zmení. Hranice zároveň obmedzujú možnú manipuláciu: ťažiari nemôžu hrou s časovými pečiatkami radikálne znížiť obtiažnosť.

Vďaka tomu sa Bitcoin reguluje sám. Keď sa ťažba stane výnosnejšou, napríklad pre rast ceny, do siete vstúpi viac výpočtového výkonu. Bloky by prichádzali rýchlejšie, ale obtiažnosť sa upraví nahor a obnoví desaťminútový priemer. Keď výnosnosť klesne, ťažiari odchádzajú a obtiažnosť sa upraví nadol. Systém nájde rovnováhu pri akejkoľvek úrovni výpočtového výkonu, ktorú trh poskytne.

Výsledkom je, že vyšší hashrate prináša viac bezpečnosti, nie viac blokov a nie viac bitcoinov. Sieť s desaťnásobným výpočtovým výkonom je desaťkrát drahšie napadnúť, no stále vytvára bloky rovnakým tempom s rovnakým harmonogramom odmien. Bezpečnosť sa tak oddeľuje od menovej politiky, čo nedosiahol žiaden predchodca.

Čo dôkaz práce nerobí

Dôkaz práce bitcoin nevytvára. Práve tým sa Bitcoin líši od svojich predchodcov.

V B-money a Bit Gold mal dôkaz práce vytvárať peňažné jednotky priamo: práca sama bola peniazmi. Menová politika tým závisela od ekonomiky hardvéru. Keď výpočtový výkon zlacnel, tvorba peňazí by sa donekonečna zrýchľovala.

Bitcoin tento vzťah obracia. Dôkaz práce brzdí tvorbu blokov a usporadúva transakcie, ale neurčuje, koľko bitcoinov existuje. Blokovú odmenu určujú pravidlá konsenzu, ktoré overuje každý plný uzol, nie množstvo vykonanej práce. Ťažiar, ktorý si nárokuje vyššiu odmenu, vytvorí neplatný blok, nech do neho vložil akúkoľvek prácu. Úprava obtiažnosti zaisťuje, že vyšší výpočtový výkon prináša viac bezpečnosti, nie viac bitcoinov.

Menovú politiku Bitcoinu vynucujú plné uzly, ktoré prevádzkujú ekonomicky relevantní účastníci, nie ťažiari vykonávajúci prácu. Ťažiari navrhujú bloky, uzly ich prijímajú alebo odmietajú podľa pevných pravidiel. Preto sa harmonogram emisie nezmenil, hoci hashrate od spustenia vzrástol o niekoľko rádov.

Spravodlivá emisia cez ťažbu

Ak dôkaz práce bitcoin nevytvára, ako sa nové mince dostávajú do obehu? Odpoveď odhaľuje ďalšiu úlohu ťažby: je to distribučný mechanizmus.

Každý platný blok obsahuje coinbase transakciu, ktorá vytvára nové bitcoiny podľa harmonogramu určeného konsenzom. Počiatočná odmena bola 50 BTC za blok. Každých 210 000 blokov (približne štyri roky) sa odmena polovičí: 25, potom 12,5, potom 6,25 a teraz 3,125 BTC. Polovičenie pokračuje približne do roku 2140, keď sa vyťaží posledný zlomok bitcoinu a celková ponuka dosiahne 21 miliónov.[10]

Ťažiar, ktorý vytvorí platný blok, túto odmenu dostane. Keďže tvorba bloku vyžaduje dôkaz práce a ťažiť sa môže pokúsiť ktokoľvek, emisia funguje ako nepretržitá otvorená lotéria. V priemere každých desať minút sieť pridelí nové bitcoiny tomu, kto nájde ďalší platný blok.

Tento mechanizmus má vlastnosti, ktoré väčšina neskorších peňažných systémov nedosiahla. Nové mince získavajú tí, čo vynakladajú skutočné zdroje na zabezpečenie siete, nie zasvätenci, politickí favoriti či skorí investori. Pred spustením siete nijaký premine nepridelil mince zakladateľom a nijaké ICO nepredávalo tokeny špekulantom. O tom, kto dostane novú emisiu, nerozhoduje žiadna centrálna autorita. Prvý blok, ktorý Satoshi vyťažil, sa riadil rovnakými pravidlami ako každý ďalší.

Kontrast s alternatívami je ostrý. Fiat meny emitujú centrálne banky pre vlády a politicky prepojené inštitúcie. Systémy s dôkazom vkladu odmeňujú existujúcich držiteľov úmerne ich podielu, bohatí teda bohatnú z definície. Mnohé kryptomeny sa spustili s premine alebo s prídelmi pre

zasvätencov, ktoré obohatili zakladateľov skôr, než bola možná verejná účasť.

Ťažobná lotéria Bitcoinu zaisťuje, že o novú emisiu môže súťažiť každý, kto je ochotný vynaložiť zdroje. Na polohe nezáleží. Na politických stykoch nezáleží. Existujúce bohatstvo nedáva žiadny osobitný nárok. Ťažiar v ktorejkoľvek jurisdikcii, s technikou akéhokoľvek rozsahu, má pravdepodobnosť výhry úmernú svojmu podielu na hashrate siete. Ihrisko nie je celkom rovné, lebo priemyselní ťažiari majú úspory z rozsahu, ale je otvorené. Na účasť netreba povolenie.

Emisia sa tak mení z politickej otázky na trhový proces. Nové bitcoiny plynú k tým, čo poskytujú službu, ktorú sieť potrebuje: výpočtovú bezpečnosť. Práca nie je zbytočná. Brzdí tvorbu blokov, usporadúva transakcie a zároveň rozdeľuje nové mince tým, čo chránia účtovnú knihu.

Výber reťazca a konsenzus

Bitcoin udržiava blockchain: usporiadanú postupnosť blokov, z ktorých každý odkazuje na haš svojho predchodcu. Prvý blok (genesis blok)[11] predchodcu nemá; každý ďalší blok sa viaže na celú predchádzajúcu históriu. Zmena ktorejkoľvek transakcie v ktoromkoľvek historickom bloku by zmenila haš daného bloku, tým by sa zneplatnil odkaz v nasledujúcom bloku, zmenil by sa aj jeho haš, a tak ďalej až do súčasnosti. Štruktúra robí každý zásah do histórie viditeľným.

Viditeľnosť zásahu však nie je konsenzus. Mohlo by existovať viacero platných reťazcov. Keď ťažiar nájde platný blok, rozpošle ho po sieti. Ostatní ťažiari po jeho prijatí stoja pred voľbou: stavať na tomto bloku, alebo pokračovať v práci na vlastnom kandidátovi. Pre latenciu siete vidia rôzni ťažiari rôzne bloky v rôznom čase. Dvaja ťažiari môžu nájsť platné bloky takmer naraz, každý bez vedomia o druhom. Sieť má dočasne dva platné konce reťazca.

Protokol považuje dočasný fork za bežnú prevádzku a určuje pravidlo na jeho vyriešenie: uzly nasledujú reťazec s najväčšou nahromadenou prácou. Keď sa jedna vetva predĺži skôr než druhá, má viac práce, ťažiari kratšiu vetvu opustia a stavajú na dlhšej. Opustený blok sa stane osirelým a jeho transakcie sa vrátia do mempoolu, aby sa zaradili do budúcich blokov.

Z pravidla vyplýva, že transakcie sú časom čoraz bezpečnejšie. Transakciu v najnovšom bloku možno vytlačiť, ak sa tento blok stane osirelým. Transakcia pochovaná pod šiestimi blokmi by vyžadovala, aby útočník vytvoril súperiaci reťazec s väčšou prácou, než je práca šiestich blokov, a to je čoraz drahší zámer. Hlboké transakcie sú prakticky nezvratné.

Nakamotova pôvodná analýza ide ďalej. Pokus o dobehnutie sa dá modelovať ako pravdepodobnostný problém, nielen ako ekonomický. V oddiele 11 whitepaperu Bitcoinu je útočník, ktorý sa snaží prepísať nedávnu

históriu, opísaný ako hráč hrajúci proti kasínu. Každý nový blok je súboj, v ktorom čestná sieť buď zväčší svoj náskok, alebo dá útočníkovi šancu ho dobehnúť. Jediný zdroj whitepaperu mimo informatiky, kniha Williama Fellera „Úvod do teórie pravdepodobnosti a jej aplikácií“ (angl. *An Introduction to Probability Theory and Its Applications*, 1957), dodáva matematiku ruinovania hráča (Gambler's Ruin), na ktorej tento obraz stojí.[5] Ak útočník ovláda menej než polovicu výpočtového výkonu siete, pravdepodobnosť, že niekedy dobehne, klesá exponenciálne s počtom potvrdení, ktoré čestný reťazec už nazbieral. Šesť potvrdení, bežné orientačné pravidlo, vyplýva priamo z tejto analýzy. Bezpečnosť Bitcoinu proti hlbokej reorganizácii reťazca je teda výsledkom samotného správania systému: pravdepodobnostná dynamika robí úspech útoku nesmierne nepravdepodobným a táto nepravdepodobnosť sa s každým ďalším blokom znásobuje.

Tento mechanizmus dosahuje konsenzus nahromadenou prácou, bez hlasovania a bez vopred daného súboru overovateľov. Reťazec s najväčšou nahromadenou prácou je zhoda siete o poradí transakcií. Nakamoto ho nazval „reťazcom dôkazov práce“, ktorý slúži ako „dôkaz postupnosti udalostí, ktorých bola sieť svedkom“. Ťažiari nehlasujú, vytvárajú bloky. Uzly si nezávisle vyberú reťazec s najväčším nahromadeným dôkazom práce.

Prečo ťažiari overujú

Ťažiari dostávajú za platné bloky blokové odmeny (novovytvorené bitcoiny) a transakčné poplatky. Prečo sa však obťažujú overovať transakcie a dodržiavať pravidlá protokolu? Mohli by vytvárať bloky s neplatnými transakciami alebo si nárokovať nadmernú odmenu. Dôkaz práce tomu sám nebráni; hašovacia funkcia nevie, či je obsah bloku platný.

Odpoveď spočíva v ekonomickej štruktúre, konkrétne v tom, kto určuje, čo sa počíta ako bitcoin.[6]

Ekonomicky relevantní účastníci, ako obchodníci a burzy, často prevádzkujú plné uzly. Plný uzol samostatne overuje každú transakciu podľa pravidiel protokolu: správne podpisy, nevyčerpané vstupy, platné sumy, riadna bloková odmena. Uzol sa nikoho nepýta, či je transakcia platná, skontroluje to sám. Ak blok porušuje akékoľvek pravidlo, uzol ho odmietne. Dôkaz práce na tom nič nemení; neplatné bloky sa zahodia bez ohľadu na to, koľko výpočtov stálo ich vytvorenie.

Ťažiari tvoria bloky, ale platný reťazec určuje overujúca ekonomika. Ťažiar, ktorý vytvorí neplatný blok, či už s nafúknutou odmenou, s dvojitým míňaním, alebo s porušením ktoréhokoľvek iného pravidla konsenzu, premrhal svoje výpočtové zdroje. Ekonomicky relevantné uzly ten blok odmietnu. Bloková odmena existuje len na reťazci, ktorý širšia ekonomika neuznáva. Nemôže obiehať ako bitcoin, ak ho protistrany odmietajú.

Tým vzniká vynucovací mechanizmus. Ťažiari overujú, lebo overuje širšia ekonomika. Bloková odmena a transakčné poplatky sú bezcenné, kým ich protistrany neprijmú ako platbu. Keďže ekonomicky relevantné uzly prijímajú bitcoin len z platného reťazca s najväčšou nahromadenou prácou, ťažiari sú ekonomicky nútení tvoriť platné bloky práve na ňom.

Vzťah je jemný, ale podstatný. Ťažiari Bitcoin neovládajú, slúžia mu. Ťažiar s 51 % výpočtového výkonu by teoreticky mohol reorganizovať nedávnu históriu alebo cenzurovať transakcie, ale pravidlá zmeniť nemôže. Pokus nárokovať si vyššiu blokovú odmenu alebo minúť mince, ktoré nevlastní, by vytvoril neplatný reťazec, ktorý obchodníci odmietnu. Výpočtový výkon bez platnosti je bezcenný.

Táto štruktúra obracia bežné predstavy o tom, na čom stojí bezpečnosť systému. Bezpečnosť nepochádza z dôveryhodnosti ťažiarov, ale z nezávislého overovania. Každý ekonomicky relevantný uzol je vynucovacím bodom a čím viac účastníkov overuje nezávisle, tým je systém odolnejší. Kto neoveruje a spolieha sa na cudzí uzol, preniesol svoju vynucovaciu moc na iného a závisí od jeho čestnosti.

Bitcoin ako nástroj záväzku

Analýza strategickej interakcie od Thomasa Schellinga z roku 1960 zaviedla nástroj záväzku ako prostriedok, ktorým racionálne strany obmedzujú vlastné budúce konanie tak, aby boli ich hrozby a sľuby dôveryhodné.[7] Vláda, ktorá chce mať povesť štátu s nízkou infláciou, profituje z centrálnej banky, ktorej inštitucionálny návrh robí vysokú infláciu nákladnou pre jej guvernérov. Zmluva, ktorá viaže obe strany, má väčšiu cenu než zmluva, od ktorej môže ktorákoľvek strana odstúpiť. Protokol, ktorého pravidlá prevádzkovateľ zmeniť nemôže, je ako záväzok užitočnejší než protokol, ktorého pravidlá možno prepísať.

Architektúra Bitcoinu je v tomto zmysle nástrojom záväzku. Strop 21 miliónov mincí je číslo v pravidlách konsenzu a dostatočne koordinovaná väčšina ekonomiky by ho mohla zmeniť. Je to však tá istá ekonomika, ktorej úspory strop chráni, a preto obstál šestnásť rokov pokusov o opätovné dohodnutie. Úprava obtiažnosti viaže rast hashrate na časovanie blokov, takže väčšie zdroje vložené do zabezpečenia reťazca nemôžu urýchliť emisiu ani prepísať menový harmonogram. Reťazec dôkazov práce je záväzkom k tomu poradiu transakcií, ktoré nahromadilo najviac práce, a viaže každého účastníka, aby reťazec, ku ktorému sa pripojil, aj predlžoval. Každé z týchto pravidiel je obmedzenie, ktoré si účastníci uložili sami a dodržiavajú ho, lebo hodnota jeho dodržiavania závisí od toho, že ho dodržiavajú aj všetci ostatní.

Skoršie práce Nicka Szaba o inteligentných zmluvách a „Božích protokoloch“ (angl. *The God Protocols*) preniesli rovnaký rámec do cypherpunkovej tradície.[8] Zmluva vykonávaná kódom je nástroj záväzku, ktorého

vynútením je determinizmus kódu, a účastníci dôverujú deterministickému vykonaniu namiesto ľubovôle akéhokoľvek vynucovateľa. Bitcoin funguje ako peniaze, lebo záväzok protokolu je zakódovaný v údajoch, ktoré overuje každý účastník, a overovanie každého účastníka je nezávislé od ochoty ktoréhokoľvek iného účastníka dodržať sľub.

Zhrnutie kapitoly

Digitálne peniaze dlho zlyhávali, lebo dva problémy zostávali nevyriešené naraz. Systémy dokázali chrániť súkromie bez decentralizácie alebo decentralizovať niektoré funkcie bez vytvorenia peňazí v pravom zmysle, ale žiaden nedokázal zabrániť dvojitému míňaniu bez návratu k dôveryhodnej kontrole. Bitcoin uspel tým, že dovtedy oddelené myšlienky spojil do jednej architektúry.[12] Dôkaz práce zabrzdil útoky odopretím služby a urobil uvaľovanie nákladov merateľným. Výber reťazca vyriešil usporiadanie transakcií bez centrálnej účtovnej knihy: reťazec s najväčšou nahromadenou prácou je reťazec a útočník, ktorý sa snaží prepísať nedávnu históriu, hrá ruinovanie hráča, v ktorom pravdepodobnosť úspechu s každým ďalším potvrdením klesá exponenciálne. Ťažba vydáva aktívum tým istým procesom, ktorým sa chráni sieť, čím oddeľuje bezpečnosť od menovej politiky: vyšší hashrate prináša viac bezpečnosti, nie viac bitcoinov. Bitcoin sa tak líši od B-money a Bit Gold, kde dôkaz práce vytváral peňažné jednotky priamo a viazal ponuku na ekonomiku hardvéru.

Bitcoin sú základné peniaze. Na rozdiel od zostatkov v DigiCash či účtov e-gold nie sú jednotky bitcoinu pohľadávkami voči emitentovi. Držitelia vlastnia samotné jednotky, overené plným uzlom podľa pravidiel konsenzu, ktoré nekontroluje žiaden jediný subjekt. Ťažiari tvoria bloky, ale platný reťazec určuje overujúca ekonomika: ťažiar, ktorý sa pokúsi nárokovať si nadmernú blokovú odmenu alebo minúť mince, ktoré nevlastní, vytvorí neplatný reťazec, ktorý obchodníci a burzy odmietnu, a výpočtový výkon bez platnosti je bezcenný. Architektúra je nástrojom záväzku v Schellingovom zmysle: pravidlá, ktoré môže nezávisle overiť každý účastník, viažu všetkých k tej istej účtovnej knihe a žiadna jediná autorita ich nemôže zmeniť bez toho, aby presvedčila sieť na spustenie iného softvéru.

Menové vlastnosti Bitcoinu, jeho odolnosť voči vypnutiu a empirický záznam o prežití patria do kapitoly 19. Jeho model súkromia, transparentnosť základnej vrstvy, hrozby z analýzy reťazca a vrstvené nástroje súkromia vybudované okolo neho patria do kapitoly 20. Kapitola tvrdí, že dôkaz práce vyriešil konkrétne problémy, ktoré jeho predchodcovia vyriešiť nedokázali. Alternatívne mechanizmy konsenzu existujú a ich porovnanie je predmetom samostatnej práce.

Poznámky

[1] Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System" (2008), https://bitcoin.org/bitcoin.pdf. Prvýkrát uvedené v kapitole 2, poznámka 8, ktorá pokrýva kanonické projektové stránky Bitcoinu a kontext jeho spustenia.

[2] David Chaum, "Blind Signatures for Untraceable Payments," *Advances in Cryptology: Proceedings of Crypto 82*, ed. David Chaum, Ronald L. Rivest a Alan T. Sherman (Plenum Press, 1983), 199–203, je zakladajúci článok, ktorý zavádza slepé podpisy. Chaum, "Security Without Identification: Transaction Systems to Make Big Brother Obsolete," *Communications of the ACM* 28, č. 10 (1985): 1030–1044, rozširuje argument na návrh celého systému. O vysvetlení Hala Finneyho z roku 1993, ako ecash podľa Chauma odhaľuje dvojité míňanie a pritom zachováva anonymitu až do druhého míňania, pozri Finney, "Detecting Double Spending," https://nakamotoinstitute.org/library/detecting-double-spending/. Dejiny spoločnosti DigiCash sú zdokumentované v Steven Levy, *Crypto* (Viking, 2001), kap. 8; o bankrote DigiCash (1998) pozri Julian Dibbell, "In Gold We Trust," *Wired* (január 2002). K zatvoreniu e-gold: Ministerstvo spravodlivosti USA obvinilo prevádzkovateľov e-gold Ltd. v apríli 2007 podľa 18 U.S.C. § 1960 (prevádzkovanie nelicencovanej firmy na prevod peňazí); hlavní obvinení sa v roku 2008 priznali a služba v roku 2009 prestala vyplácať. *United States v. e-gold, Ltd.*, No. 1:07-cr-00109 (D.D.C. 2007).

[3] Adam Back, "Hashcash: A Denial of Service Counter-Measure," technická správa (2002), http://www.hashcash.org/papers/hashcash.pdf. Pôvodný návrh bol oznámený v e-mailovej konferencii cypherpunks v marci 1997. O prepojení od neopakovane použiteľných pečiatok Hashcash k prenosným tokenom podloženým dôveryhodným hardvérom pozri oznámenie RPOW od Hala Finneyho (2004), https://nakamotoinstitute.org/library/rpow/. K širšej literatúre o dôkaze práce, z ktorej Hashcash vychádza: Cynthia Dwork a Moni Naor, "Pricing via Processing or Combatting Junk Mail," *CRYPTO '92* (1993), 139–147, zaviedli myšlienku využiť výpočtové náklady ako mechanizmus riadenia prístupu.

[4] Wei Dai, "b-money," nepublikovaný návrh (november 1998), http://www.weidai.com/bmoney.txt. Nick Szabo, "Bit Gold" (1998, publikované na Szabovom blogu v roku 2005), https://unenumerated.blogspot.com/2005/12/bit-gold.html. Szabov neskorší text "Bit Gold Markets" (2008), https://nakamotoinstitute.org/library/bit-gold-markets/, výslovne opisuje problém nezameniteľnosti, ktorý táto kapitola zdôrazňuje: keďže riešenia hlavolamov z rôznych období by mali rôzne výrobné náklady, trhy by ich museli zlučovať a deliť do balíkov so štandardnou hodnotou. K línii časového pečiatkovania, ktorú Bit Gold predpokladá, pozri W. Scott Stornetta a Stuart Haber, "How to Time-Stamp a Digital Document" (1991), https://nakamotoinstitute.org/library/time-stamp-digital-document/. Satoshi Nakamoto citoval Daiovo b-money vo whitepaperi Bitcoinu; vzťah medzi Bit Gold a Bitcoinom je nepriamejší, ale koncepčný dlh je zjavný.

[5] William Feller, *An Introduction to Probability Theory and Its Applications*, vol. 1 (New York: John Wiley & Sons, 1957), je citovaný vo whitepaperi Bitcoinu ako referencia [8] a dodáva analýzu ruinovania hráča, ktorou Nakamoto ohraničuje pravdepodobnosť, že útočník dobehne čestný reťazec. Odolnosť Bitcoinu voči hlbokej reorganizácii nie je múr, ktorý protokol stavia okolo transakcií, ale vlastnosť vyplývajúca z pravdepodobnostnej dynamiky v nepriateľských podmienkach, pričom pravdepodobnosť úspešného útoku klesá exponenciálne s počtom nahromadených potvrdení. Úplné odvodenie obsahuje oddiel 11 whitepaperu.

[6] O ekonomickom vzťahu medzi obchodníkmi a ťažiarmi pozri Eric Voskuil, "Qualitative Security Model," *Cryptoeconomics* (2020), https://github.com/libbitcoin/libbitcoin-system/wiki/Qualitative-Security-Model. Voskuil

zdôrazňuje, že jednotlivci, ktorí sami neoverujú, delegovali overovanie na centrálnu autoritu, čím podkopávajú bezpečnostný model. K širšiemu výkladu bezpečnostného modelu Bitcoinu v tejto knihe pozri kapitolu 5, poznámka 9.

[7] Thomas C. Schelling, *The Strategy of Conflict* (Cambridge, MA: Harvard University Press, 1960), najmä kap. 2 (”An Essay on Bargaining”). Schellingova neskoršia práca *Arms and Influence* (Yale University Press, 1966) rozvíja analýzu nástrojov záväzku pre strategickú interakciu všeobecnejšie. K ekonomickej aplikácii na menové inštitúcie: Finn E. Kydland a Edward C. Prescott, ”Rules Over Discretion: The Inconsistency of Optimal Plans,” *Journal of Political Economy* 85, č. 3 (1977): 473–491, formalizuje problém časovej nekonzistentnosti, ktorý rieši nástroje záväzku centrálnych bánk.

[8] Nick Szabo, ”Smart Contracts: Building Blocks for Digital Markets” (1996) a ”The God Protocols” (1997), obe na `https://nakamotoinstitute.org/the-god-protocols/` a `https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html`. Szabov text ”Shelling Out: The Origins of Money” (2002), `https://nakamotoinstitute.org/shelling-out/`, rozvíja tento rámec naprieč dejinami komoditných peňazí. Ku kryptoekonomickej línii, ktorá spája nástroje záväzku s protokolmi konsenzu, pozri Vitalik Buterin, ”A Next-Generation Smart Contract and Decentralized Application Platform” (2014) a Eric Voskuil, ”Cryptoeconomics” (2020), už citovaný v poznámke 6. K najstarším primárnym prameňom z čias Bitcoinu: príspevky Hala Finneyho do konferencie cypherpunks (1992–2004) a na Bitcointalk (2009–2013) sú archivované na `https://bitcointalk.org/index.php?action=profile;u=2435` a, pre staršiu korešpondenciu z čias cypherpunkerov, na `https://cypherpunks.venona.com`; Finney dostal od Satoshiho prvú transakciu Bitcoinu 12. januára 2009 a uverejnil jednu z prvých verejných analýz vlastností súkromia v Bitcoine. K historickému spracovaniu týchto predchodcov a ich vzťahu k Bitcoinu pozri Finn Brunton, *Digital Cash: The Unknown History of the Anarchists, Utopians, and Technologists Who Created Cryptocurrency* (Princeton University Press, 2019) a Nathaniel Popper, *Digital Gold* (HarperCollins, 2015), kap. 1–3. K byzantskej odolnosti voči chybám (Byzantine fault tolerance), klasickému základnému problému, ktorý konsenzus Bitcoinu rieši pravdepodobnostne, pozri Leslie Lamport, Robert Shostak a Marshall Pease, ”The Byzantine Generals Problem,” *ACM Transactions on Programming Languages and Systems* 4, č. 3 (1982): 382–401, `https://lamport.azurewebsites.net/pubs/byz.pdf`. K porovnávajúcej línii naprieč všetkými týmito predchodcami pozri Arvind Narayanan a Jeremy Clark, ”Bitcoin's Academic Pedigree,” *Communications of the ACM* 60, č. 12 (2017): 36–45.

[9] SHA-256 (Secure Hash Algorithm 256-bit) navrhla americká Národná bezpečnostná agentúra (NSA) a NIST ho publikoval v roku 2001 ako FIPS PUB 180-2. Bitcoin používa dvojité použitie SHA-256 (SHA-256d) na hašovanie blokov a kombináciu SHA-256/RIPEMD-160 na odvodenie adries. Špecifikácia algoritmu je dostupná na National Institute of Standards and Technology, ”Secure Hash Standard (SHS),” FIPS PUB 180-4 (2015), `https://csrc.nist.gov/publications/detail/fips/180/4/final`. K bezpečnostným vlastnostiam, vďaka ktorým je SHA-256 vhodný pre dôkaz práce – odolnosť voči kolíziám, odolnosť voči vzoru (preimage) a lavínový efekt – pozri Alfred J. Menezes, Paul C. van Oorschot a Scott A. Vanstone, *Handbook of Applied Cryptography* (CRC Press, 1996), kap. 9, voľne dostupné na `https://cacr.uwaterloo.ca/hac/`.

[10] Harmonogram emisie Bitcoinu a mechanizmus polovičenia odmeny určuje whitepaper Bitcoinu v oddiele 6 (”Incentive”) a sú zakódované vo funkcii `GetBlockSubsidy()` v Bitcoin Core. Interval polovičenia 210 000 blokov a strop 21 miliónov mincí sú pravidlá konsenzu, ktoré vynucuje každý plný uzol. Záznam každého polovičenia v reťazci pozri na

`https://mempool.space/mining`. Ekonomické dôsledky pevnej ponuky a dezinflačnej emisie analyzuje Saifedean Ammous, *The Bitcoin Standard: The Decentralized Alternative to Central Banking* (Wiley, 2018), kap. 1–3, ktorý harmonogram ponuky Bitcoinu porovnáva s dynamikou pomeru zásob a prírastku (stock-to-flow) pri zlate a striebre. Kritické preskúmanie otázky prechodu na poplatky (čo sa stane s príjmami ťažiarov, keď sa blokové odmeny blížia k nule) pozri Miles Carlsten a kol., "On the Instability of Bitcoin Without the Block Reward," *ACM CCS* (2016).

[11] Genesis blok (blok 0) vyťažil Satoshi Nakamoto 3. januára 2009. Jeho coinbase transakcia obsahuje text "The Times 03/Jan/2009 Chancellor on brink of second bailout for banks," odkaz na titulku z prvej strany *The Times* (Londýn) toho dňa, ktorý slúži ako časová pečiatka a vyhlásenie zámeru. Haš bloku je `000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f`. Dá sa zobraziť na `https://mempool.space/block/000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f`. Odmena 50 BTC z coinbase transakcie genesis bloku je ako jediná nevyčerpateľná: nebola zahrnutá do pôvodnej množiny nevyčerpaných výstupov transakcií. K podrobnej analýze technických vlastností genesis bloku a vloženej správy pozri Jameson Lopp, "Bitcoin's Genesis Block," `https://blog.lopp.net/bitcoins-genesis-block/`.

[12] K učebnicovej syntéze toho, ako Bitcoin spája dôkaz práce, dátovú štruktúru blockchainu a distribuovaný konsenzus, pozri Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller a Steven Goldfeder, *Bitcoin and Cryptocurrency Technologies* (Princeton University Press, 2016), voľne dostupné na `https://bitcoinbook.cs.princeton.edu/`. Kapitola 2 pokrýva kryptografické primitíva (hašovacie funkcie, haš ukazovatele, digitálne podpisy), na ktorých opisovaná architektúra stojí, a kapitola 3 mechaniku konsenzuálneho protokolu Bitcoinu. Sprievodný článok Narayanana a Clarka, "Bitcoin's Academic Pedigree," *Communications of the ACM* 60, č. 12 (2017): 36–45, sleduje, ako každá súčasť návrhu Bitcoinu čerpá z predchádzajúcej akademickej práce, a poskytuje najúplnejšiu mapu intelektuálnej línie Bitcoinu dostupnú v jedinom zdroji.

19

BITCOIN AKO ZDRAVÉ A ODOLNÉ PENIAZE

„Neverím, že budeme mať znova dobré peniaze, kým túto vec nevyberieme z rúk vlády, teda, nemôžeme ju vziať z rúk vlády násilím, môžeme len nejakou záludnou okľukou zaviesť niečo, čo nebudú vedieť zastaviť."

F. A. Hayek, *Denationalisation of Money* (1976)[1]

Úvod

Kapitola 18 ukázala, ako sa Bitcoin stáva možným. Táto kapitola skúma menové vlastnosti zakódované v Bitcoine a vlastnosti odolnosti, vďaka ktorým systém prežije nátlak protivníkov.

Tieto dva rozmery patria k sebe. Digitálne aktívum, ktoré sa dá znehodnotiť infláciou, zmraziť alebo ľahko vypnúť, nie je zdravými peniazmi v žiadnom vážnom zmysle. Bitcoin zabudoval menovú disciplínu aj odolnosť do tej istej architektúry.[2]

19.1 Vlastnosti zdravých peňazí ako Schellingove body

Kapitola 9 určila vlastnosti, ktoré zdravé peniaze vyžadujú. Bitcoin ich má a mechanizmus, ktorý ich udržiava, treba pochopiť hneď na začiatku, lebo od neho závisí každé tvrdenie v tomto oddiele.

Pravidlo konsenzu sa v Bitcoine nevynucuje protokolom tak, ako súd vynucuje zmluvu. Neexistuje autoritatívna kópia súboru pravidiel. Každý plný uzol prevádzkuje vlastný softvér, drží vlastné pravidlá konsenzu a každý blok proti nim overuje nezávisle. Ktorýkoľvek prevádzkovateľ

môže svoje pravidlá upraviť, spustiť fork, ktorý prijíma bloky, čo zvyšok siete odmieta, a na tomto základe vytvoriť alternatívny reťazec. Nikto nemôže iného prevádzkovateľa prinútiť, aby urobil to isté. Pravidlá pretrvávajú, lebo sa na nich nezávislí overovatelia zhodli a odmietajú uznať reťazce, ktoré ich porušujú. Rovnako platí strop, harmonogram emisie, pravidlá podpisov, bloková odmena a každé ďalšie pravidlo konsenzu, o ktorom sa píše nižšie: ide o Schellingov bod, na ktorom sa overovatelia zosúladili, a jednostranná odchýlka vytvorí reťazec bez ekonomickej hodnoty, lebo ho nikto iný neprijme.

Model zhody predpovedá skutočné správanie systému v prípadoch, v ktorých alternatívny pohľad zlyháva. Bitcoin Cash sa od Bitcoinu odštiepil v roku 2017 zmenou pravidla o veľkosti bloku. Vzniknutý reťazec má vlastný trh a držiteľov Bitcoinu sa netýka, lebo overovatelia Bitcoinu sa na novom pravidle nezhodli. Ethereum v roku 2016 vrátilo transakcie DAO späť na základe sociálnej dohody medzi overovateľmi Ethereum. Vrátenie uspelo, lebo sa naň overovatelia zhodli, a menšina, ktorá ho odmietla, prevádzkuje dnes Ethereum Classic.[10] V oboch prípadoch zvíťazilo pravidlo, ktoré udržala zhoda nezávislých prevádzkovateľov, a rovnako to platí o každej vlastnosti v tomto oddiele.

Pevný strop ponuky

Ponuka Bitcoinu je ohraničená stropom 21 miliónov mincí. Strop je pravidlo konsenzu, ktoré každý plný uzol overuje voči prijatým blokom, a blok s transakciami, ktoré vytvárajú mince nad rámec harmonogramu, odmietne ako neplatný každý uzol so zhodnými pravidlami. Ťažiar, ktorý taký blok vytvorí, ho môže zverejniť, ale reťazec, čo z neho vychádza, uznávajú len uzly s upravenými pravidlami a žiadna burza, správca úschovy ani obchodník so štandardnými pravidlami na ňom platby neprijme. Blok nemá nijakú ekonomickú hodnotu, a preto ho žiaden racionálny ťažiar nevytvára.

Strop je teda nezmeniteľný v praktickom zmysle, na ktorom držiteľom záleží: na reťazci, ktorý uzol prevádzkuje, neexistuje iná cesta k zmene pravidla než spustiť iný softvér. Ťažiar alebo vývojár, ktorý chce vyššiu ponuku, sa môže odštiepiť a postaviť reťazec s vyšším stropom, ale pôvodný reťazec so sebou nestiahne. Pôvodný reťazec beží ďalej pre všetkých, čo naďalej používajú pôvodné pravidlá, aj keď ide o menšinu bývalých účastníkov. Pri fyzickom zlate sa dajú objaviť nové náleziská a pri fiat menách môžu centrálne banky tlačiť peniaze. Tu neexistuje nikto, kto by mal moc zvýšiť ponuku na reťazci, ktorý držitelia overujú; pokus o to vytvorí osobitný reťazec, ktorý títo držitelia ignorujú. Vyriešením dvojitého míňania sa jednotky bitcoinu stali rivalitnými (vlastníctvo jedného človeka vylučuje vlastníctvo iného), a preto sa na toto digitálne aktívum môžu vzťahovať vlastnícke práva. Strop na celú triedu aktív je tak sám vlastníckym

právom, ktoré spoločne držia všetci prevádzkovatelia uzlov odmietajúci prijať infláciu.

Predvídateľná emisia

Vďaka úprave obtiažnosti a harmonogramu polovičenia je celá krivka ponuky známa vopred. Budúcu ponuku k ľubovoľnému dňu môže vypočítať ktokoľvek. Neexistuje núdzový dekrét ani voľná úvaha, ktorá by ju mohla zmeniť, lebo neexistuje autorita, ktorá by ju mohla vydať. Zmena harmonogramu naráža na ten istý problém koordinácie ako zmena stropu a overovatelia, ktorí sedemnásť rokov odmietajú infláciu, nemajú dôvod prijať ju teraz. Menová politika je transparentná, lebo je to rovnaké pravidlo na stroji každého prevádzkovateľa, a je trvalá, lebo odchýlka od nej vytvorí reťazec, ktorému nikto nepripisuje hodnotu.

Deliteľnosť

Bitcoin je deliteľný na osem desatinných miest. Najmenšia jednotka, jedna stomilióntina bitcoinu, sa volá satoshi. Umožňuje to transakcie akejkoľvek praktickej veľkosti, od mikroplatieb po veľké vyrovnania. Osemmiestny návrh nebol Satoshiho prvým náčrtom. Skorá korešpondencia s Halom Finneym v januári 2009 tlačila na jemnejšiu deliteľnosť, než počítal pôvodný návrh, a parameter 10^8 satoshi na mincu sa ustálil v tejto výmene skôr, než sa sieť otvorila širšiemu publiku.[3]

Táto deliteľnosť je súčasťou aktuálnej definície jednotky v Bitcoine, nie fyzickým limitom. Ak by si budúce rozšírenie vyžiadalo jemnejšie delenie, ďalšie desatinné miesta by vyžadovali zmenu konsenzu. Deliteľnosť je parameter, nie pevné obmedzenie.

Netreba nič fyzicky rezať ani taviť. Jeden bitcoin sa dá rozdeliť na 100 miliónov satoshi bez straty hodnoty a bez dôvery v tretiu stranu. Je to viac než deliteľnosť ktorejkoľvek fyzickej komodity.

Prenosnosť

Bitcoin možno previesť kamkoľvek na Zemi, kde je sieťové pripojenie. Hodnota prekročí hranice bez fyzickej prepravy, colnej kontroly či rizika konfiškácie na kontrolných stanovištiach.

Súkromný kľúč, ktorý ovláda akékoľvek množstvo bitcoinov, si možno zapamätať, uložiť v zariadení alebo zakódovať v rôznych formátoch. Previezť miliardu dolárov v zlate si vyžaduje nákladiaky a stráže; previezť miliardu dolárov v bitcoinoch si vyžaduje zapamätať si dvanásť slov.

Trvanlivosť

Bitcoin sa nerozpadá. Jednotky vytvorené v roku 2009 sú rovnaké ako jednotky vytvorené dnes. Samotné aktívum nemá žiadne náklady na uloženie, hoci bezpečný prístup k súkromným kľúčom si vyžaduje starostlivosť.

Účtovná kniha je replikovaná na tisíckach uzlov po celom svete. Jednotlivé nosiče sa kazia, ale sieť udržiava nadbytočné kópie. Replikácia chráni pred stratou údajov na úrovni siete, hoci jednotliví používatelia môžu stále stratiť prístup k svojim mincám stratou kľúčov, zabudnutými heslami alebo zničenými zálohami. Táto zraniteľnosť je spoločná zlatu aj bitcoinu: oboje možno stratiť nedbanlivosťou alebo katastrofou. Výhoda Bitcoinu v trvanlivosti oproti fyzickým peniazom je jasnejšia: papierové peniaze chátrajú, mince korodujú, no jednotky bitcoinu zostávajú kryptograficky neporušené na neurčito.

Overiteľnosť

Ktokoľvek, kto prevádzkuje plný uzol, môže overiť celú menovú históriu. Zlato vyžaduje skúšku pravosti a bankovky špeciálne vybavenie na odhaľovanie falzifikátov. Pravosť bitcoinu je oproti nim kryptograficky istá. Platná transakcia buď spĺňa pravidlá protokolu, alebo nie; netreba žiaden úsudok ani odbornosť, len spustiť softvér.

Overovanie siaha aj na ponuku. Každý účastník môže nezávisle potvrdiť, že celková ponuka sleduje harmonogram. Netreba dôverovať vyhláseniu žiadnej centrálnej autority. Dôkazom je samotná účtovná kniha.

Výzvy zameniteľnosti

Zdravé peniaze vyžadujú, aby boli jednotky vzájomne zameniteľné. Dolár je dolár bez ohľadu na svoju históriu. Zlaté tehly sú zameniteľné: jedna unca sa rovná ktorejkoľvek inej uncii rovnakej čistoty.

Transparentný blockchain Bitcoinu vytvára pri zameniteľnosti problémy. Každá transakcia je zaznamenaná a každá jednotka má vysledovateľnú históriu. Niektoré burzy a služby odmietajú mince s históriou spojenou so sankcionovanými adresami, darknetovými trhmi alebo platbami za ransomware. Ak jednotky nie sú zameniteľné pre svoju históriu, zameniteľnosť je narušená.

Narušená zameniteľnosť je skutočné obmedzenie Bitcoinu na základnej vrstve. Nasledujúce oddiely rozoberajú nástroje súkromia, ako CoinJoin,[11] PayJoin, Lightning[12] a ecash,[13] ktoré problém zameniteľnosti riešia tým, že prerušujú väzby umožňujúce diskrimináciu.

Ako overovatelia udržiavajú zdravosť

Tradičná menová zdravosť závisí od inštitucionálnych sľubov. Centrálne banky sľubujú stabilnú politiku a často svoje sľuby porušia. Zlaté štandardy sľubujú vymeniteľnosť za zlato a vlády ju pozastavia.

Zdravosť Bitcoinu udržiava každý účastník, ktorý prevádzkuje overovací softvér a odmieta reťazce, čo porušujú pravidlá, ktoré drží. Plné uzly overujú každú transakciu podľa pravidiel konsenzu, ktoré si každý prevádzkovateľ zvolil. Transakcie, ktoré tieto pravidlá porušujú, vrátane tých,

čo prekračujú limity ponuky, uzol prevádzkovateľa odmietne a nikdy nevstúpia do reťazca, ktorý tento prevádzkovateľ uznáva. Každý uzol drží svoje pravidlá jednostranne; nikto ho nemôže prinútiť prijať reťazec, ktorý ich porušuje. Koordinovaná zmena medzi mnohými prevádzkovateľmi vytvorí fork: pôvodný reťazec beží ďalej pre všetkých, čo zostali pri pôvodných pravidlách, upravený reťazec beží popri ňom pre tých, čo prešli, a otázku, ktorý reťazec nesie menovú hodnotu, rozhodujú trhy, burzy, obchodníci a likvidita, nie nijaký prah účasti overovateľov. Inflácii, cenzúre a spätnému vráteniu transakcií sa v histórii Bitcoinu odolalo, lebo držitelia, ktorí by pri takých zmenách prišli o hodnotu, naďalej používali pravidlá, ktoré ich chránia, a nikto im ich nemohol vziať.

Systém nie je „nevyžadujúci dôveru“ v zmysle, že by nijakú dôveru nevyžadoval. Používatelia dôverujú, že softvér správne implementuje pravidlá, ktoré chcú, a že reťazec, ktorý sledujú, bude naďalej priťahovať ekonomickú činnosť, ktorá dáva ich minciam hodnotu. Prvá dôvera sa dá overiť: ktokoľvek si môže prečítať kód a spustiť uzol, ktorý potvrdzuje, že každý blok dodržiava pravidlá, na ktorých mu záleží. Druhá je empirická: držitelia sledujú trhy, burzy a obchodníkov, ktorí oceňujú a prijímajú reťazec, čo overujú.

Bitcoin a regresná teoréma

Kapitola 9 predstavila regresnú teorému a otázky, ktoré vyvoláva pri nových peniazoch. Tu tento rámec použijeme priamo na Bitcoin.

Problém sa zdá jednoduchý: Mises ukázal, že súčasná hodnota peňazí sa dá vystopovať cez predchádzajúce hodnotenia až do času, keď sa peňažná komodita cenila pre nepeňažné použitie. Zlato bolo ozdobou skôr, než bolo peniazmi. Bitcoin však bol od začiatku navrhnutý ako peniaze. Porušuje teda teorému?

Riešenie spočíva v samotnej subjektívnej teórii hodnoty. Teoréma vyžaduje, aby prví hodnotitelia mali dôvody na ocenenie; neurčuje, aké druhy dôvodov sa počítajú. Prví používatelia Bitcoinu ho cenili z rôznych dôvodov: ideologický záväzok k cypherpunkovým cieľom, technická fascinácia kryptografickou inováciou, špekulatívne očakávanie budúceho rozšírenia alebo praktická túžba po transakciách odolných voči cenzúre. Každé z týchto hodnotení je subjektívne. Praxeológia nedáva dôvod vyhlasovať niektoré hodnotenia za legitímne a iné za nelegitímne.

Pôvodný úžitok Bitcoinu bol skutočný: umožňoval transakcie bez povolení a odolné voči cenzúre, aké žiaden iný systém poskytnúť nemohol. Tento úžitok je odlišný od peňažného použitia; Bitcoin sa dal oceňovať pre túto schopnosť, bez očakávania, že sa stane všeobecne prijímanými peniazmi. Trhová cena bitcoinu vo fiat peniazoch existovala skôr, než sa za ňu obchodovalo s tovarom: prvá burza BTC-USD, BitcoinMarket.com, sa ot-

vorila v marci 2010 a dva mesiace pred udalosťou s pizzou vytvárala nepretržite kótovanú cenu.

Transakcia z 22. mája 2010 je kanonickou ukážkou, ako sa táto cena zakotvuje v obchode. Laszlo Hanyecz uverejnil na fóre BitcoinTalk ponuku 10 000 BTC za dve pizze doručené k jeho dverám a používateľ fóra (Jeremy Sturdivant, „jercos“) ju prijal tak, že objednal pizze z Papa John's za vlastné doláre. Papa John's sa s bitcoinom nikdy nedostal do styku; BTC prešli od Laszla k Jeremymu výmenou za pizze kúpené za fiat. Praxeologický obsah je v tomto obchode medzi rovnocennými: Jeremyho ochota prijať 10 000 BTC za tovar v hodnote zhruba dvadsaťpäť dolárov a Laszlova ochota sa ich za taký kurz vzdať sú dve subjektívne hodnotenia, ktoré sa stretli pri cene už vymedzenej burzovým obchodovaním.

Priame prijímanie bitcoinu obchodníkmi prišlo neskôr. Koncom roka 2010 sa na fóre BitcoinTalk v sekcii Marketplace objavili predajcovia, ktorí prijímali bitcoin priamo za tovar, pričom predajca alpakových ponožiek Michael Stoneman bol pre toto obdobie príznačný. Spustenie Silk Road vo februári 2011 urobilo priamy obchod za BTC bežným vo veľkom: kupujúci a predajcovia sa vyrovnávali end-to-end v bitcoinoch bez sprostredkovateľa vo fiat kanáloch. Regresný reťazec prechádza všetkými týmito krokmi.[4]

Základným poznatkom teorémy je, že peniaze vznikajú trhovým procesom, nie dekrétom. Bitcoin tento poznatok potvrdzuje čistejšie než ktorýkoľvek historický príklad. Nijaký zákon o zákonnom platidle nenútil k prijímaniu, nijaká vládna podpora ho nepodopierala a nijaká vymeniteľnosť za komoditu ho nezakotvovala. Účastníci trhu Bitcoin prijali, lebo cenili jeho vlastnosti, a toto dobrovoľné prijatie mu dalo menový status. Vznik ukazuje, že teoréma vysvetľuje, ako sa peniaze zvyčajne vyvíjajú; neobmedzuje, ktoré statky sa môžu stať peniazmi.[5]

19.2 Vlastnosti odolnosti: prečo Bitcoin prežíva

Decentralizácia bráni vypnutiu na jednom mieste

Bitcoin nemá sídlo ani generálneho riaditeľa. Nemá ani jediný server, ktorý by sa dal zhabať. Sieť tvoria tisíce uzlov na celom svete, z ktorých každý nezávisle overuje transakcie. Zlikvidovať Bitcoin by si vyžadovalo vypnúť všetky uzly naraz vo všetkých jurisdikciách.

Predchádzajúce digitálne meny zlyhali, lebo úrady mohli zasiahnuť ústredné body. Distribuovaná architektúra Bitcoinu takéto ciele odstraňuje.

Globálne rozloženie

Uzly Bitcoinu fungujú v každej významnej krajine. Ťažba prebieha na všetkých kontinentoch. Vývoj sa deje naprieč jurisdikciami. Vďaka ta-

kému zemepisnému rozloženiu nemá sieť pod kontrolou žiadna jediná vláda.

Aj dôsledný medzinárodný postup naráža na problémy s koordináciou, lebo rôzne vlády majú rôzne záujmy. Kým niektoré jurisdikcie Bitcoin obmedzujú, iné ho vítajú a sieť obmedzenia obchádza.

Útoky na úrovni siete

Decentralizácia neodstraňuje všetky vektory útoku. Útoky na úrovni siete môžu Bitcoin narušiť aj bez toho, aby mierili na jednotlivé uzly.[6]

Únos BGP umožňuje autonómnym systémom presmerovať prevádzku Bitcoinu tým, že oznámia nepravdivé informácie o smerovaní. Výskum ukázal, že únos menej než 900 IP prefixov by mohol rozdeliť významné časti siete. Poskytovateľ internetu, cez ktorého prechádza prevádzka Bitcoinu, môže o 20 minút oneskoriť šírenie blokov a zostať pritom neodhalený. Také útoky môžu spôsobiť rozdelenie reťazca a príležitosti na dvojité míňanie počas rozdelenia, ako aj stratu ťažobných príjmov, keď sa po skončení útoku osirelé bloky zahodia.

Útoky typu Eclipse mieria na jednotlivé uzly tak, že monopolizujú ich spojenia s ostatnými uzlami a izolujú ich od čestnej siete. Pôvodný výskum útoku Eclipse (2015) podnietil zlepšenia výberu partnerov a správy spojení v Bitcoin Core. Súčasné verzie používajú viacero opatrení vrátane rôznorodých odchádzajúcich spojení naprieč rôznymi skupinami siete, kotiev, ktoré pretrvávajú po reštartoch, a odhaľovania podozrivého správania partnerských uzlov. Konkrétne útoky opísané v skorom výskume sú z veľkej časti zmiernené, hoci táto trieda útokov zostáva problémom, ktorému sa ďalší vývoj stále venuje.

Útoky cez DNS môžu narušiť vyhľadávanie uzlov a blokovanie na úrovni poskytovateľa internetu môže znemožniť prevádzku v určitých jurisdikciách. Čínsky zákaz ťažby z roku 2021[15] zmenil zemepisné rozloženie ťažby a ukázal, že zásah jurisdikcie môže sieť ovplyvniť, hoci ju úplne nezlikviduje.

Tieto útoky ukazujú rozdiel medzi zraniteľnosťami implementácie a štrukturálnymi obmedzeniami. Zraniteľnosti implementácie (konkrétne vektory útoku Eclipse, slabiny výberu partnerov) rieši priebežný vývoj Bitcoin Core; projekt udržiava aktívnu bezpečnostnú kontrolu a pravidelne vydáva aktualizácie. Štrukturálne obmedzenia (závislosť od infraštruktúry internetového smerovania, zraniteľnosti BGP) sa na aplikačnej vrstve celkom odstrániť nedajú, hoci opatrenia ako používanie Toru a rôznorodé pripojenie pomáhajú. Uzly môžu používať Tor[14] na skrytie svojich IP adries, čím znižujú vystavenie niektorým útokom na úrovni siete.

Koncentrácia ťažby

Ťažobný pool je družstevné usporiadanie medzi mnohými nezávislými ťažiarmi, ktorí spájajú svoj výpočtový výkon, aby si vyrovnali príjem. Samostatná ťažba pri dnešnej obtiažnosti prináša veľmi kolísavé výnosy: malý prevádzkovateľ môže čakať roky medzi blokmi, s dlhými obdobiami nulového príjmu, ktoré občas preruší celá bloková odmena. Pooly to riešia tak, že ťažiarov zoskupia pod koordinátora, ktorý zostavuje kandidátske šablóny blokov, rozdeľuje ich členom, zbiera „shares“ (dôkazy s nízkou obtiažnosťou, že členovia počítajú haše na pridelených šablónach) a nakoniec vyplatí blokovú odmenu v pomere k podielom, ktoré každý člen dodal. Ťažiar vymení malý poplatok prevádzkovateľovi za stály príjem; pool vypláca dosť veľké platby na to, aby pritiahol účastníkov. Ťažobný hardvér zostáva u jednotlivých ťažiarov, no koordinačná vrstva a zostavovanie šablón blokov je centralizované.

Vrstva poolov sa v praxi koncentrovala. Malý počet poolov koordinuje väčšinu hashrate; podľa nedávnych meraní päť najväčších poolov často ovláda viac než 70 % z neho.[7]

Konkrétna zraniteľnosť je zostavovanie šablóny. Keďže kandidátsky blok zostavuje pool, pool vyberá, ktoré transakcie sa v ňom objavia a na ktorý predchádzajúci blok šablóna nadväzuje. Prevádzkovateľ pod právnym alebo politickým tlakom môže odmietnuť zahrnúť konkrétne transakcie a ťažiari, ktorí pre tento pool počítajú haše, vytvárajú cenzurujúce bloky bez toho, aby si rozdielu všimli.

Ten istý mechanizmus umožňuje pokusy o reorganizáciu reťazca. Pool, ktorý nasmeruje svoje šablóny na starší blok namiesto aktuálneho konca reťazca, usmerní výpočtový výkon svojich členov do alternatívneho reťazca, ktorý, ak vyhrá preteky proti čestnému koncu, nahradí nedávnu históriu inou. Či reorganizácia uspeje, závisí od hashrate; väčšinový pool môže plytké reorganizácie vynútiť podľa ľubovôle a pool s významnou menšinou môže občas uspieť proti najnovším blokom, kým nazbierajú potvrdenia.

Pevnou hranicou je krádež. Pool nemôže minúť mince, ktorých súkromné kľúče nedrží, nech má k dispozícii akýkoľvek hashrate. Útoky reorganizáciou môžu dvojito minúť vlastné nedávno odvysielané transakcie útočníka, ale nemôžu vziať prostriedky iných držiteľov. Jednotliví ťažiari môžu pool meniť lacno a pooly, ktoré viditeľne cenzurujú alebo sa pokúšajú o viditeľné reorganizácie, by o nich prišli v prospech konkurentov, čo je disciplinujúci mechanizmus v praxi.

Stratum V2 a Datum riešia architektonický problém priamo. Oba protokoly umožňujú jednotlivým ťažiarom alebo ťažobným farmám zostaviť si vlastné šablóny blokov a odoslať ich poolu, pričom pool si ponecháva len úlohu zhromažďovania podielov a vyplácania. Ťažiar, ktorý používa ktorýkoľvek z nich, zostáva vo výplatnom systéme poolu, ale sám vyberá,

ktorý koniec reťazca predĺži a ktoré transakcie zahrnie, a tým sa cenzúra šablón a smerovanie reorganizácií oddeľujú od rozsahu koordinácie.[8]

Prečo dôkaz práce pripúšťa trvalú súťaž

Vlastnosti odolnosti uvedené vyššie závisia od konkrétnej návrhovej voľby: Bitcoin viaže tvorbu blokov na spotrebu zdroja, ktorý vzniká mimo účtovnej knihy. Ťažiar hlasuje za reťazec tým, že míňa elektrinu na špecializovaný hardvér, ktorý bol vyrobený, dopravený a nainštalovaný vo fyzickom svete. Bezpečnostný zdroj, hashrate, je statok vyššieho rádu poskladaný z kremíka, energie, kapitálu a práce, ktoré existujú nezávisle od samotného Bitcoinu. Z toho vyplýva dôsledok, ktorý väčšina diskusií o konsenze podceňuje: ponuka hashrate je vo vzťahu k protokolu exogénna. Nijaký útočník ju nedokáže skúpiť.

Systémy s dôkazom vkladu fungujú inak. V protokole založenom na vklade je zdrojom, ktorý dáva hlasovacie právo, samotná minca. Útočník, ktorý ovládne väčšinu aktívneho vkladu, nečelí menšine, ktorá by mohla odpovedať tým, že vyrobí viac bezpečnostného zdroja. Menšina môže získať viac mincí len ich kúpou, a v systéme s dôkazom vkladu je útočník z definície najväčším držiteľom mincí. Útočník nemusí predávať a zvyšní držitelia spolu väčšinu neovládajú. Slashing môže zničiť vklad, ktorý sa správal nesprávne, ak sa porušenie kryptograficky zistí, ale väčšina, ktorá koná v rámci pravidiel protokolu a pritom cenzuruje, mení poradie transakcií alebo si privlastňuje odmeny, sa nedopúšťa porušenia, ktoré by protokol dokázal zistiť. Obnova, ak vôbec je možná, závisí od sociálnej koordinácie okolo soft forku aktivovaného používateľmi, ktorý zachytený reťazec zavrhne, a to je presne ten mimoprotokolový politický proces, ktorému sa mal dôkaz práce vyhnúť.[9]

Dôkaz práce tento problém obracia. Držiteľ 51 % hashrate dnes čelí trhu, ktorý môže odpovedať niekoľkými spôsobmi naraz: dajú sa vyrobiť nové ASIC, vypnutý hardvér sa dá zapnúť, ťažiari, ktorým sa politika útočníka nepáči, môžu presmerovať svoj hashrate do iného poolu a úplne noví účastníci sa dajú pritiahnuť ziskovou príležitosťou, ktorú útok vytvára. Útočník súťaží s globálnou kapacitou polovodičového priemyslu a so svetovou cenou elektriny, a žiadnu z nich nezíska tým, že ovláda reťazec. To je to, čo Hugo Nguyen nazval nadčasovosťou práce: elektrina, ktorá zabezpečila minulé bloky, sa nedá znovu minúť, a hardvér, ktorý zabezpečí budúce bloky, môže vyrobiť ktokoľvek, kto je ochotný zaplatiť.

Empirický záznam podporuje tvrdenie o obnove aj pri silnom tlaku. V júni 2021 Čína zakázala ťažbu Bitcoinu, čím v priebehu niekoľkých týždňov zmizli zhruba dve tretiny hashrate siete. Do šiestich mesiacov sa hashrate vrátil na úroveň spred zákazu, rozložený do Spojených štátov, Kazachstanu, Ruska a Kanady. Útočníkom v tom prípade bola jurisdikcia, v ktorej bola väčšina svetovej ťažobnej kapacity, a menšina sa zotavila tak,

že premiestnila hardvér do jurisdikcií, ktoré sa k útoku nepripojili. Reťazec s dôkazom vkladu by v rovnakej situácii nemal porovnateľnú odpoveď: vklad, ktorý držali čínski ťažiari, by sa nedal presunúť k novým overovateľom v iných krajinách, lebo vklad je samotný reťazec, nie hardvér, ktorý naň mieri.

Ekonomické stimuly na obranu

Ťažiari investovali miliardy do vybavenia a infraštruktúry. Táto investícia je bezcenná, ak Bitcoin zlyhá. Ťažiari preto majú silné stimuly brániť sieť pred útokmi.

Aj držitelia bitcoinu majú stimul podporovať zdravie siete. Prevádzkovanie uzlov a obrana siete pred útokmi slúži priamo záujmom držiteľov.

Axióma odporu v historickom zázname

Bitcoin ukazuje axiómu odporu v historickom zázname. Sieť prežila opakované zásahy vlád v rôznych krajinách, zákazy v niektorých jurisdikciách, viaceré zlyhania a hackerské útoky na burzy, dlhodobo negatívne mediálne pokrytie, technické útoky na sieť a regulačnú neistotu s nepriateľskou legislatívou.

Od spustenia Bitcoin nepretržite vytvára bloky približne každých 10 minút. Hashrate (výpočtová bezpečnosť) sa zvýšil o niekoľko rádov. Tento empirický záznam potvrdzuje vlastnosti odolnosti, ktoré teória predpovedá.

Zhrnutie kapitoly

Vlastnosti Bitcoinu ako zdravých peňazí sú Schellingove body, ktoré udržiavajú nezávislí overovatelia, nie sľuby emitentov. Pevná ponuka, predvídateľná emisia, deliteľnosť, prenosnosť, trvanlivosť a verejná overiteľnosť sú pravidlá konsenzu, ktoré každý plný uzol drží lokálne a overuje voči každému prijatému bloku. Pravidlá každého prevádzkovateľa sú len jeho a nikto mu ich nemôže vziať ani ho prinútiť prijať reťazec, ktorý ich porušuje. Koordinovaný posun k iným pravidlám vytvorí osobitný reťazec, ktorý beží popri pôvodnom, a o tom, ktorý reťazec nesie menovú hodnotu, rozhodujú trhy, obchodníci a burzy, nie nijaký prah účasti overovateľov. Skutočným obmedzením základnej vrstvy zostáva zameniteľnosť pri transparentnosti: každá jednotka má vysledovateľnú históriu a niektoré burzy odmietajú mince spojené so sankcionovanou alebo darknetovou činnosťou. Vrstvy súkromia v kapitole 20 existujú preto, aby obnovili to, čo transparentná účtovná kniha sama od seba nedáva. Bitcoin tiež spĺňa regresnú teorému dobrovoľným trhovým prijatím, nie dekrétom. Skoré subjektívne hodnotenia schopnosti uskutočňovať transakcie odolné voči cenzúre poskytli nepeňažné použitie, z ktorého sa peňažný status vyvinul, v súlade s praxeologickým rámcom z kapitoly 9.

Vlastnosti odolnosti a menové vlastnosti sú architektonicky neoddeliteľné. Zdravé peniaze, ktoré možno znehodnotiť infláciou alebo zmraziť dekrétom, nie sú zdravými peniazmi, a decentralizácia Bitcoinu, jeho globálne rozloženie a ekonomické stimuly na obranu zaisťujú, že menové pravidlá nemožno zmeniť vonkajším tlakom. Dôkaz práce viaže tvorbu blokov na zdroj vznikajúci mimo účtovnej knihy, takže útočník, ktorý ovládne väčšinu výpočtového výkonu, čelí trhu, ktorý môže odpovedať výrobou ďalšieho hardvéru, premiestňovaním ťažiarov a pritiahnutím nových účastníkov. Rovnaká odpoveď obnovila hashrate po čínskom zákaze ťažby v roku 2021. Systémy s dôkazom vkladu takto odpovedať nemôžu, lebo bezpečnostným zdrojom je samotná minca. Odolnosť nie je neobmedzená. Útoky na úrovni siete, koncentrácia ťažby a zásahy jurisdikcií môžu narušiť prístup a na okraji znížiť bezpečnosť, a kapitola tieto vektory útoku dokumentuje popri vlastnostiach odolnosti. Empirický záznam podporuje to, že základná vrstva Bitcoinu od januára 2009 pri opakovanom tlaku štátov aj trhov pokračuje vo vytváraní blokov približne každých desať minút, čo je operačný dôkaz, ktorý teoretické kapitoly predpovedali.

Poznámky

[1] F. A. Hayek, *Denationalisation of Money: The Argument Refined*, 3. vyd. (London: Institute of Economic Affairs, 1990; prvé vydanie 1976). Epigraf pochádza z Hayekovej prednášky z roku 1984 "The Future Unit of Value", ktorá sa často cituje ako jeho predpoveď niečoho podobného Bitcoinu. Hayek tvrdil, že konkurujúce si súkromné meny by disciplinovali vlády účinnejšie než akékoľvek pravidlo, ktoré by si vláda mohla uložiť sama, čo je myšlienka, ktorú architektúra Bitcoinu z kapitoly 18 zrealizovala o dvadsaťštyri rokov neskôr iným mechanizmom. Ku kanonickému výkladu rakúskych zdravých peňazí, o ktorý sa táto kniha opiera, pozri Ludwig von Mises, *The Theory of Money and Credit*, prel. H. E. Batson (New Haven: Yale University Press, 1953; nemecký originál 1912), najmä časť III o menovej politike; citované v kapitole 9, poznámka 4.

[2] Ďalšie čítanie o Bitcoine ide viacerými smermi. Technická hĺbka: Andreas Antonopoulos, *Mastering Bitcoin*, 3. vyd. (O'Reilly, 2023) je štandardná príručka pre vývojárov a Kalle Rosenbaum, *Grokking Bitcoin* (Manning, 2019) je najlepší ilustrovaný úvod do fungovania protokolu. Menová a historická perspektíva: Saifedean Ammous, *The Bitcoin Standard* (2018), Nik Bhatia, *Layered Money* (2021) a Lyn Alden, *Broken Money* (2023). Naratívne dejiny: Nathaniel Popper, *Digital Gold* (2015) o vzniku Bitcoinu a Jonathan Bier, *The Blocksize War* (2021) o spore o škálovanie v rokoch 2015–17. Primárne: Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System* (2008), citované v kapitole 18, poznámka 1; a samotný zdrojový strom Bitcoin Core na `https://github.com/bitcoin/bitcoin`. K prevádzkovaniu infraštruktúry: Bitcoin Core (`https://bitcoincore.org/`) pre plné uzly, Sparrow Wallet (`https://sparrowwallet.com/`) pre desktopovú vlastnú úschovu s kontrolou mincí, Specter Desktop pre multisig a hardvérové podpisové zariadenia ako Blockstream Jade, Coldcard (`https://coldcard.com/`) a Trezor.

[3] K návrhu deliteľnosti pozri skorú korešpondenciu Satoshi Nakamoto a Hal Finney, zhromaždenú v Satoshi Nakamoto Institute, `https://satoshi.nakamotoinstitute.org/emails/`, v ktorej Finney nastolil otázku, ako jemne sa dá bitcoin deliť, a Satoshi opísal dôvody osemmiestnej (10^8)

základnej jednotky, z ktorej sa stal satoshi. Z úvah zachovaných v týchto e-mailoch vyplýva, že jednotky sú dimenzované tak, aby ponechali veľký priestor pre mikrotransakcie aj pre veľký rast hodnoty jednotky, bez potreby neskôr meniť konsenzom šírku poľa.

[4] K skorej burze BTC-USD, ktorá založila nepretržitú trhovú cenu pred obchodom s pizzou, pozri oznamovacie vlákno BitcoinMarket.com na BitcoinTalk, `https://bitcointalk.org/index.php?topic=20.0` (marec 2010), ktoré spustil používateľ "dwdollar". K transakcii s pizzou pozri Laszlo Hanyecz, "Pizza for bitcoins?", vlákno na fóre BitcoinTalk, 18.–22. mája 2010, `https://bitcointalk.org/index.php?topic=137.0`, v ktorom Laszlo ponuku urobí a používateľ "jercos" (Jeremy Sturdivant) ju prijme a potvrdí doručenie cez Papa John's; sprostredkovaná štruktúra je zdokumentovaná v samotnom vlákne, pričom Jeremy objednal pizze za vlastné doláre po prijatí Laszlových BTC. K vzniku sekcie Marketplace na BitcoinTalk ako prvého miesta pre priamy obchod tovaru za bitcoin, vrátane predajcu alpakových ponožiek Michaela Stonemana, pozri archívy podfóra Marketplace na `https://bitcointalk.org/index.php?board=2.0` (vlákna od konca roka 2010) a Nathaniel Popper, *Digital Gold* (2015), kap. 4–5, ktorý sleduje cestu od udalosti s pizzou cez skoré prijímanie obchodníkmi. K spusteniu a prevádzkovému modelu Silk Road pozri Nick Bilton, *American Kingpin: The Epic Hunt for the Criminal Mastermind Behind the Silk Road* (Portfolio, 2017) a prevádzkové opisy vo federálnej obžalobe Rossa Ulbrichta (*United States v. Ulbricht*, S.D.N.Y., 2014). Stránka sa spustila začiatkom roka 2011 a fungovala na priamych platbách BTC od kupujúceho k predajcovi, vedených cez centralizovaný escrow prevádzkovaný stránkou.

[5] K diskusiám o regresnej teoréme aplikovaným na Bitcoin pozri Peter Šurda, "Economics of Bitcoin" (2012); Konrad Graf, "On the Origins of Bitcoin" (2013); Eric Voskuil, "Regression Fallacy," *Cryptoeconomics* (2020). Tieto pramene sú zhromaždené v kapitole 9, poznámka 5, ktorá pokrýva debatu o regresii v plnom rozsahu.

[6] K únosu BGP a útokom na úrovni siete proti Bitcoinu pozri Maria Apostolaki a kol., "Hijacking Bitcoin: Routing Attacks on Cryptocurrencies," *IEEE Symposium on Security and Privacy* (2017). K útokom typu Eclipse pozri Ethan Heilman a kol., "Eclipse Attacks on Bitcoin's Peer-to-Peer Network," *USENIX Security* (2015). K nenápadnejšiemu útoku EREBUS pozri Muoi Tran a kol., "A Stealthier Partitioning Attack against Bitcoin Peer-to-Peer Network," *IEEE S&P* (2020).

[7] Údaje o koncentrácii ťažobných poolov: Cambridge Centre for Alternative Finance, "Cambridge Bitcoin Electricity Consumption Index," údaje o rozdelení poolov, `https://ccaf.io/cbnsi/cbeci/mining_map`; rozdelenie hashrate medzi pooly v reálnom čase sleduje `https://mempool.space/mining`.

[8] K Stratum V2 pozri špecifikáciu protokolu a referenčnú implementáciu, ktorú udržiava Stratum V2 Working Group, `https://stratumprotocol.org/`, najmä rolu Job Declaration, ktorá umožňuje ťažiarovi alebo ťažobnej farme zostaviť si vlastné šablóny blokov a pritom sa naďalej podieľať na výplate poolu cez samostatný kanál sledovania podielov. K Datum pozri dokumentáciu projektu od Ocean Mining, `https://ocean.xyz/docs/datum`, ktorá implementuje decentralizované zostavovanie šablón pre členov poolu tak, aby prevádzkovateľ poolu už nevyberal, ktoré transakcie sa objavia v kandidátskych blokoch. Oba protokoly ponechávajú vrstvu zhromažďovania podielov a vyplácania poolu a zostavovanie šablón presúvajú na jednotlivý koncový bod počítajúci haše, čo je architektonické oddelenie, ktoré rieši cenzúru zo strany prevádzkovateľa poolu bez toho, aby ťažiari museli opustiť výplatnú štruktúru poolu vyrovnávajúcu kolísanie.

[9] K argumentu o externalite zdroja, ktorý sa tu rozvíja, pozri Hugo Nguyen, "Proof-of-Stake & the Wrong Engineering Mindset" (2018) a "Work is Timeless, Stake is Not" (2018). K základnej kritike dôkazu vkladu pozri Andrew Poelstra, "On Stake and Consensus" (2015). Protiargumenty Vitalika Buterina rozvíjajú "Proof of Stake: How

I Learned to Love Weak Subjectivity" (2014) a "Why Proof of Stake" (2020); Buterin pripúšťa, že obnova po získaní väčšiny v dôkaze vkladu si vyžaduje koordinovaný sociálny fork. K údajom o obnove po čínskom zákaze pozri Cambridge Centre for Alternative Finance, "Cambridge Bitcoin Electricity Consumption Index," mapa ťažby, `https://ccaf.io/cbnsi/cbeci/mining_map`.

[10] K forku Bitcoin Cash: tvrdý fork z augusta 2017 vyplynul zo sporu o škálovanie veľkosti blokov, ktorý v rokoch 2015 až 2017 rozdelil vývojársku komunitu Bitcoinu. Hlavnými hybnými silami reťazca s väčšími blokmi boli Bitcoin ABC (pod vedením Amaury Sécheta) a obhajoba Rogera Vera cez Bitcoin.com. Jonathan Bier, *The Blocksize War: The Battle for Control over Bitcoin's Protocol Rules* (vlastným nákladom, 2021), je určujúci opis sporu z pohľadu tých, čo fork odmietali. K hackerskému útoku na Ethereum DAO a forku: DAO (Decentralized Autonomous Organization) bola v júni 2016 zneužitá približne o 3,6 milióna ETH útokom typu reentrancy. Ethereum Foundation a väčšina overovateľov vykonali v júli 2016 tvrdý fork, aby prostriedky vrátili, čím vznikli dva reťazce: Ethereum (ETH, forkovaný reťazec) a Ethereum Classic (ETC, reťazec, ktorý pokračoval v pôvodnom stave). K technickým detailom zraniteľnosti reentrancy pozri Phil Daian, "Analysis of the DAO Exploit," *Hacking, Distributed* (18. júna 2016). K dôsledkom pre správu pozri súčasné blogové príspevky Vitalika Buterina na `https://vitalik.eth.limo/` a oznámenie Ethereum Foundation o tvrdom forku na `https://blog.ethereum.org/2016/07/20/hard-fork-completed`.

[11] CoinJoin navrhol Gregory Maxwell v príspevku na fóre BitcoinTalk 22. augusta 2013: "CoinJoin: Bitcoin privacy for the real world," `https://bitcointalk.org/index.php?topic=279249.0`. Technika umožňuje viacerým používateľom spojiť svoje transakcie do jednej transakcie s viacerými vstupmi a výstupmi, čo sťažuje určenie, ktorý vstup zodpovedá ktorému výstupu. Medzi implementácie patrí Wasabi Wallet (`https://wasabiwallet.io/`), ktorý používa CoinJoin s výstupmi rovnakej hodnoty založený na koordinátorovi so slepými podpismi, a JoinMarket (`https://joinmarket.net/`), ktorý používa trh makerov a takerov na koordináciu nevyžadujúcu dôveru. K akademickému spracovaniu súkromia CoinJoinu a jeho obmedzení pri analýze prevádzky pozri Felix Maurer a kol., "Anonymous CoinJoin Transactions with Arbitrary Values," *IEEE TrustCom* (2017) a prácu Sjorsa Provoosta a Adama Gibsona o PayJoin (P2EP), ktorý zlepšuje základný CoinJoin odstránením heuristiky rovnakých výstupov. Kapitola 20 tejto knihy pokrýva CoinJoin a jeho varianty podrobne.

[12] Lightning Network je sieť platobných kanálov postavená na Bitcoine, ktorá umožňuje platby mimo reťazca s vysokou priepustnosťou a nízkou latenciou. Protokol prvýkrát opísali Joseph Poon a Thaddeus Dryja, "The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments" (2016), `https://lightning.network/lightning-network-paper.pdf`. Platby sa smerujú cez sieť obojsmerných platobných kanálov zabezpečených skriptovacím systémom Bitcoinu; v reťazci sa vyrovnávajú len transakcie otvorenia a zatvorenia kanála. Hlavné implementácie sú LND (Lightning Labs, `https://github.com/lightningnetwork/lnd`), Core Lightning (Blockstream, `https://github.com/ElementsProject/lightning`) a Eclair (ACINQ, `https://github.com/ACINQ/eclair`). Z pohľadu súkromia Lightning zlepšuje zameniteľnosť tým, že sumy platieb a identity protistrán drží mimo reťazca, hoci smerovacie uzly majú čiastočný prehľad o tokoch platieb; technický prehľad pozri Bastien Teinturier, "Lightning Network Privacy," `https://github.com/t-bast/lightning-docs/blob/master/lightning-privacy.md`. Kapitola 20 tejto knihy pokrýva model súkromia Lightningu podrobne.

[13] Ecash označuje systémy tokenov so slepými podpismi podľa Chauma, ktoré sa dajú znovu nasadiť nad Bitcoinom, s Cashu (`https://cashu.space/`) a Fedimint (`https://fedimint.org/`) ako hlavnými modernými implementáciami. Cashu

používa schému slepých podpisov Davida Chauma (pozri kapitolu 18, poznámka 2) na vydávanie tokenov na doručiteľa voči mincovni krytej Bitcoinom; mincovňa nevie prepojiť výber s výmenou späť, čím obnovuje neprepojiteľnosť, ktorú transparentná základná vrstva Bitcoinu nemá. Fedimint spája model úschovy federovaného multisigu s vydávaním ecashu podľa Chauma a rozkladá dôveru medzi federáciu strážcov. K špecifikácii protokolu Cashu pozri `https://github.com/cashubtc/nuts`. K dôvodom návrhu Fedimintu pozri Eric Sirion a kol., "Fedimint: Federated E-Cash as a Secondary Layer," `https://fedimint.org/docs/intro`. Kapitola 20 pokrýva systémy ecashu ako nástroje súkromia na Bitcoine podrobne.

[14] Projekt Tor (`https://www.torproject.org/`) vyvíja a udržiava anonymnú sieť Tor, ktorá smeruje prevádzku TCP cez sériu dobrovoľníkmi prevádzkovaných uzlov (relays) pomocou cibuľového šifrovania, takže žiaden jednotlivý uzol nepozná zároveň pôvod aj cieľ spojenia. Bitcoin Core podporuje Tor natívne od verzie 0.12 (2016) a uzly prevádzkované ako skryté služby (adresy `.onion`) nie sú dostupné z verejného internetu (clearnet), čo ukrýva ich IP adresy pred partnerskými uzlami a pozorovateľmi. K integrácii Toru v Bitcoin Core pozri dokumentáciu na `https://github.com/bitcoin/bitcoin/blob/master/doc/tor.md`. K dôsledkom používania Toru pre súkromie a topológiu siete pri uzloch Bitcoinu pozri Ethan Heilman a kol., "Eclipse Attacks on Bitcoin's Peer-to-Peer Network," *USENIX Security* (2015), už citované v poznámke 6, ktoré rieši zraniteľnosť aj zmiernenia založené na Tore.

[15] Čínsky zákaz ťažby Bitcoinu vyhlásili Národná komisia pre rozvoj a reformy (NDRC) a Čínska ľudová banka (PBoC) v máji 2021 a presadzovanie sa v júni 2021 zintenzívnilo. Zákaz spôsobil, že hashrate siete Bitcoin v nasledujúcich týždňoch klesol približne o 50 %. Začiatkom roka 2022 sa hashrate vrátil na predchádzajúcu úroveň a prekročil ju, pričom ťažba sa presunula najmä do Spojených štátov, Kazachstanu a Ruska. K textu predpisu pozri NDRC, "Notice on Rectifying Virtual Currency 'Mining' Activities" (máj 2021). K údajom o obnove hashrate pozri Cambridge Centre for Alternative Finance, "Cambridge Bitcoin Electricity Consumption Index," mapa ťažby, `https://ccaf.io/cbnsi/cbeci/mining_map`, a Nic Carter, "How Much of Bitcoin Mining Is Powered by Clean Energy?" *CoinDesk* (2021), ktorý dokumentuje zemepisné presunutie. Táto epizóda je primárnym empirickým testom odolnosti Bitcoinu voči potláčaniu ťažby na úrovni štátu, ktorý táto kapitola cituje opakovane.

20

SÚKROMIE NA BITCOINE A MENOVÉ VRSTVY

„Bitcoin sám nedokáže udržať používateľa v anonymite; sledovanie IP adries zvonku a analýza transakcií môžu odhaliť identity."

Hal Finney, Bitcoin Forum (2010)[1]

Úvod

Kapitola 19 predstavila Bitcoin ako zdravé a odolné peniaze. Z týchto predností ešte nevyplýva, že Bitcoin je súkromný už v základe. Táto kapitola sa preto venuje tomu, ako súkromie na Bitcoine skutočne funguje. Začína útokmi, pre ktoré je súkromie nevyhnutné, a potom prechádza k primitívam a vrstvám, ktoré vznikli na ich odrazenie.

Nejde o maximalistické kázanie ani o odmietanie. Základná vrstva Bitcoinu odhaľuje skutočné informácie a odvetvie analýzy blockchainu už viac než desať rokov vyvíja nástroje, ktoré toto odhalenie využívajú. Súkromie na Bitcoine a okolo neho vzniká tak, že človek pochopí, čo tieto nástroje vidia, a potom proti nim nasadí vrstvený návrh a disciplínu pri výbere nástrojov. Kapitola sleduje toto poradie: najprv útoky na súkromie základnej vrstvy, potom skriptové primitíva, o ktoré sa vyššie vrstvy opierajú, potom CoinJoin, PayJoin a CoinSwap na základnej vrstve, Lightning, Spark a Ark mimo reťazca, ecash podľa Chauma s jeho kompromisom v podobe úschovy a nakoniec návrhy validácie na strane klienta, ktoré posúvajú súkromie ďalej, no za cenu nižšej vyspelosti.[1]

20.1 Ako zlyháva súkromie na základnej vrstve

Verejná účtovná kniha z princípu

Blockchain Bitcoinu je verejný. Každá transakcia, ktorá kedy prebehla, je viditeľná pre každého. Sumy, adresy aj časy sa zaznamenávajú natrvalo a práve trvalosť je zmyslom veci: vďaka nej môžu uzly overiť účtovnú knihu bez dôvery v akéhokoľvek prevádzkovateľa. Rovnaká vlastnosť, ktorá umožňuje overovanie bez dôvery, však stojí aj za útokmi na súkromie, o ktorých bude reč. Každá heuristika z arzenálu analytikov blockchainu je spôsob, ako vytlačiť informácie z údajov, ktoré protokol musí zverejniť.

Útoky sa skladajú dokopy. Jednotlivo sú väčšinou pravdepodobnostné, spolu však zmenšujú množinu anonymity takmer na jediný bod. Ak ich zoradíme zhruba podľa závažnosti, dostaneme aj ich historický vývoj: opakované používanie adries bolo prvým zdokumentovaným únikom, heuristika spoločného vlastníctva vstupov sa stala priemyselným ťahúňom, odhaľovanie zvyšku predĺžilo zhluky v čase, analýza časovania a siete pridala vrstvu IP adries a prepojenie cez KYC pripojilo celý graf k skutočnej identite.

Opakované používanie adries: základný únik

Adresa použitá pri viacerých platbách zlúči všetky súvisiace výstupy do jedného zhluku, a to bez akejkoľvek ďalšej analýzy. Všetky UTXO na tej adrese ovláda z definície ten istý súkromný kľúč. Každá platba na adresu aj z nej je na blockchaine navždy verejne spojená. Opakované použitie sa navyše šíri ďalej: ten, kto na adresu platil, ten, komu z nej bolo platené, aj každý pozorovateľ reťazca získajú úplný záznam o aktivite majiteľa na danom mieste.

Moderné hierarchické deterministické peňaženky, ktoré v roku 2012 určil BIP32 a ktoré rozšírili BIP44, BIP84 a BIP86, odstraňujú najčastejšiu cestu k opakovanému použitiu. Pri každom prijatí odvodia z jedného seedu novú adresu a zvyšok smerujú na samostatnú odvodzovaciu cestu. Špecifikácie pôvodne riešili problém s trvanlivosťou zálohy: peňaženky spred hierarchických deterministických návrhov držali konečnú zásobu vopred vygenerovaných kľúčov, takže stará záloha zastarala, keď peňaženka túto zásobu vyčerpala. Zisky pre súkromie prišli takmer ako vedľajší produkt.[2] Opakované používanie však pretrváva v kategóriách, ktoré stoja mimo bežného toku peňaženky: darovacie adresy vložené do podpisov na fórach, súborov README na GitHube a sociálnych profilov, ťažobné pooly, ktoré vyplácajú ťažiarov na pevné adresy, staršie vkladové adresy búrz, papierové peňaženky a „brain wallets“ s jednou adresou a adresy na platby výkupného, ktoré útočníci zámerne používajú opakovane u viacerých obetí. Každá opakovane použitá adresa je kotva zhluku, od ktorej môže zvyšok nástrojov analýzy blockchainu rásť do šírky.

Heuristika spoločného vlastníctva vstupov

Ak má transakcia viac než jeden vstup, predpokladá sa, že vstupy ovláda ten istý subjekt. Dôvod je kryptografický: na minutie UTXO treba platný podpis pre jeho scriptPubKey, takže spojenie viacerých vstupov v jednej transakcii vyžaduje súčasný prístup ku všetkým príslušným súkromným kľúčom. Ak sa strany zámerne nedohodnú, jediný dôvod, prečo vstupy spájať, je ten, že ich všetky drží jedna peňaženka.

Heuristika sa objavuje už v diskusii o súkromí vo whitepapere Bitcoinu a na celom reťazci ju sformalizovali v roku 2013 Meiklejohn a spoluautori v práci *A Fistful of Bitcoins*.[3] Práca použila heuristiku spoločného vlastníctva vstupov spolu s odhaľovaním zvyšku a zlúčila približne dvanásť miliónov adries do asi 3,4 milióna zhlukov. Heuristika zostáva ťahúňom odvetvia analýzy blockchainu a dnes ju v rozsahu celého reťazca používa každý veľký dodávateľ compliance nástrojov. Zlyháva, keď vstupy transakcie pochádzajú od rôznych strán, čo je celý cieľ CoinJoinu a PayJoinu. V praxi ale väčšina transakcií nie sú CoinJoiny, väčšina používateľov nepoužíva nijaké nástroje na ochranu súkromia a jediný kontakt s KYC kdekoľvek v histórii zhluku pripojí k celému zhluku označenie zo skutočného sveta, a to navždy.

Odhaľovanie zvyšku

Transakcia s jedným vstupom a dvoma výstupmi, čo je bežný spotrebiteľský vzor, má jeden výstup, ktorý platí protistrane, a jeden, ktorý vracia zvyšok odosielateľovi. Keď analytik rozpozná, ktorý je ktorý, môže zhluk odosielateľa predĺžiť dopredu v čase tak, že výstup so zvyškom použije ako zárodok ďalšej transakcie. V kombinácii s heuristikou spoločného vlastníctva vstupov tak správne odhalený zvyšok vytvára vzor „peel chain“, ktorý poháňa postupný rast zhlukov naprieč reťazcom.[4]

Funguje to vďaka viacerým heuristikám naraz. Najsilnejšia je heuristika opakovane použitej adresy: ak jeden výstup ide na adresu, ktorá sa už použila, a druhý na novú, opakovane použitá je takmer iste platba a nová je zvyšok, lebo peňaženky vytvárajú adresy pre zvyšok automaticky, kým adresy pre platbu zadáva ručne príjemca. Odtlačok peňaženky určí, ktorý výstup vytvoril ten istý softvér, ktorý zostavil transakciu, a to podľa typu skriptu, konvencií o poradí a zvyklostí v správaní.

Heuristika okrúhlych čísel vychádza z toho, že ľudia platia okrúhle sumy, takže výstup rovný jednému bitcoinu alebo stu dolárom podľa aktuálneho kurzu je takmer vždy platba a neokrúhly zvyšok je výstup so zvyškom. Heuristika zbytočného vstupu vychádza z toho, že rozumný výber mincí nikdy nezahrnie vstupy, ktoré nie sú potrebné na pokrytie platby. Ak by sa jeden výstup dal financovať z vlastnej podmnožiny skutočných vstupov, je to zvyšok a druhý výstup je platba. Zhoda typu skriptu pozoruje, že peňaženky zvyčajne míňajú a vracajú zvyšok v rovnakom type

skriptu, takže pri transakcii, ktorej vstupy sú všetky P2WPKH a výstupy jeden P2WPKH a jeden staršieho typu, je zvyškom výstup P2WPKH. Prezradí aj správanie pri replace-by-fee: keď peňaženka zvyšuje poplatok nepotvrdenej transakcie, takmer vždy zaplatí navyše tak, že zníži sumu výstupu so zvyškom. Zvyškom je teda výstup, ktorého hodnota sa medzi dvoma verziami v mempoole zmenšila.

Žiadna z nich nie je sama o sebe rozhodujúca. V kombinácii však určia zvyšok dosť často správne na to, aby sa peel chain mohol ďalej predlžovať. Analytikovi stačí mať väčšinou pravdu.

Analýza časovania a siete

Heuristiky na úrovni reťazca pracujú s tým, čo účtovná kniha zaznamenáva. Analýza časovania a siete pracuje s tým, čo sa deje okolo nej, pred potvrdením aj po ňom.

Najpriamejší útok na sieťovej vrstve prevádzkuje veľa plných uzlov Bitcoinu ako odpočúvacie stanovištia v peer-to-peer sieti. Keď sa objaví nová nepotvrdená transakcia, odpočúvajúce uzly zaznamenajú, ktorý peer im poslal prvé oznámenie. Pri čestnom šírení je prvým peerom, ktorý transakciu oznámi, pravdepodobne pôvodný uzol, a tak sa transakcia spojí s IP adresou. Bitcoin Core pred rokom 2015 vysielal nové transakcie všetkým peerom naraz, čo tento útok robilo takmer triviálnym. Moderný Bitcoin Core používa náhodné exponenciálne oneskorenia pre každého peera, ktoré útok oslabia, ale neznemožnia, ak má protivník veľa pozorovacích bodov. Subjekt LinkingLion, ktorý v roku 2023 zdokumentoval výskumník 0xB10C, vedie tento druh útoku na Bitcoin a Monero z určitých autonómnych systémov minimálne od roku 2018. Otvára krátkodobé odpočúvacie spojenia na dosiahnuteľné uzly a používa k tomu rotujúci súbor falošných user agentov.[5] Dandelion++, obrana, ktorá šíri transakcie najprv náhodným „kmeňom“ relayov a až potom ich normálne vysiela, sa v Monere používa od roku 2020, do Bitcoin Core však zlúčená nebola.

Časovanie uniká aj v samotnej účtovnej knihe. Dve transakcie vysielané v rozmedzí milisekúnd majú pravdepodobne spoločného pôvodcu, denné vzorce aktivity prezrádzajú časové pásmo, a teda geografickú oblasť, a trvalá automatizácia s nízkym kolísaním odhalí výplaty ťažobných poolov, vyvažovače búrz a arbitrážne boty. Vklady a výbery cez mosty medzi reťazcami sa dajú prepojiť podľa sumy a charakteristického oneskorenia. Platby cez Lightning prezrádzajú informácie o smerovaní cez časy podržania HTLC a cez útoky sondovaním, ktoré zisťujú zostatky kanálov posielaním zámerne neplatných platieb. Nič z toho nie je samo osebe rozhodujúce. V spojení s heuristikami v reťazci to však množinu anonymity ďalej zmenšuje.

Kotvy KYC a odvetvie analýzy

Vyššie opísané útoky vytvárajú zhluky adries. Aby sa zo zhluku stal človek, treba kotvu k skutočnej identite a odvetvie analýzy blockchainu postavilo svoje podnikanie na zbieraní týchto kotiev. Každá veľká centralizovaná burza zbiera informácie v rámci KYC podľa predpisov proti praniu špinavých peňazí: zákonné meno, adresu, doklad totožnosti, niekedy aj telefón a bankové údaje. Vkladové a výberové adresy viazané na účty s KYC sa označia vo vnútorných systémoch burzy a zdieľajú sa s dodávateľmi compliance nástrojov na základe komerčných zmlúv, s vládami cez súdne príkazy a zmluvy o vzájomnej právnej pomoci a s externými výskumníkmi cez zber vkladových adries. Jediný kontakt s KYC kdekoľvek v histórii zhluku označí skutočného vlastníka zhluku natrvalo. Pravidlo Travel Rule skupiny FATF, prijaté v roku 2019 a do roku 2024 zavedené globálne, vyžaduje od poskytovateľov služieb s virtuálnymi aktívami, aby pri prevodoch nad určité hranice zdieľali údaje o odosielateľovi a prijímateľovi, čím sa prepojenie cez KYC rozširuje naprieč odvetvím.[31]

Chainalysis, Elliptic, TRM Labs, CipherTrace od Mastercardu a dlhý chvost menších dodávateľov predávajú výsledné schopnosti bankám, burzám, vládam a orgánom činným v trestnom konaní.[29] Nástroje siahajú od hodnotenia transakcií v reálnom čase až po forenzné vyšetrovacie platformy. Pravdepodobnostná povaha heuristík, na ktorých stoja, sa v marketingu aj pred súdom často zamlčuje. Stíhanie Romana Sterlingova v prípade Bitcoin Fog v roku 2024 sa stalo sporným bodom v otázke, či metodika pripisovania v analýze blockchainu spĺňa bežné normy pre vedecké dôkazy.[30] Odvetvie sa tiež stavalo proti vylepšeniam súkromia na Bitcoine, keď ohrozovali jeho produkt. Jeho motivácie sú také, ako vyzerajú.

Synchronizácia peňaženky: kde sa peňaženka stretáva s reťazcom

Predchádzajúce útoky opisujú, čo vidí protivník, ktorý číta reťazec. Skôr než ho prečíta protivník, musí ho prečítať peňaženka používateľa a každý jej dotaz je správou nejakému uzlu o tom, ktoré adresy používateľa zaujímajú. Architektúra synchronizácie je kontrolný bod, kde sa súkromie v reťazci stretáva so súkromím na sieťovej vrstve, a rôzne architektúry vyzradia tomu, s kým peňaženka komunikuje, rôzne veľa.

Vlastný plný uzol je architektúra s najvyšším súkromím. Overujúci uzol stiahne každý blok od genesis bloku (približne 700 GB úložiska, ročný prírastok 80 až 100 GB, 6 až 24 hodín úvodnej synchronizácie na bežnom hardvéri) a drží množinu UTXO lokálne. Peňaženka sa dopytuje uzla cez lokálne RPC a žiadna vzdialená strana sa nedozvie, ktoré adresy peňaženka sleduje, aké výstupy drží ani na ktoré transakcie čaká. Jediný odchádzajúci signál je vysielanie transakcie, jedna správa, ktorú možno zabaliť do Toru. Orezané uzly (znižujú nároky na úložisko na približne 5 až 10 GB) zachovávajú plné overovanie, ale historické bloky z disku zahodia,

takže vlastnosti súkromia platia aj bez plnej archívnej stopy. Štandardné suverénne nastavenie spúšťa Bitcoin Core ako službu na pozadí a s ním lokálne komunikuje desktopová peňaženka (Wasabi, Sparrow alebo vlastná peňaženka Core). Celá synchronizácia histórie, odhad poplatkov a dopyty na zostatok idú cez lokálny uzol.[6]

Peňaženky Electrum a peňaženky s protokolom Electrum používajú inú architektúru: klient posiela dopyty na úrovni adries serveru Electrum, ktorý indexuje celý reťazec podľa haša skriptu. Server vráti UTXO a históriu priamo, v priebehu sekúnd. Z praktických architektúr je to súkromie najslabšie, lebo každá adresa, ktorú peňaženka sleduje, prichádza na server v jedinom spojení. Server sa naraz dozvie celý zhluk peňaženky, zostatok, históriu aj IP adresu. Náprava je prevádzkovať server Electrum sám, na tom istom stroji ako plný uzol. ElectrumX (Python), electrs (Rust) a Fulcrum (C++) sú tri štandardné implementácie na vlastné nasadenie a electrs sa dodáva ako predvolená súčasť vo viacerých distribúciách suverénnych uzlov. Electrum na vlastnom serveri zachová rýchle používanie peňaženky a odstráni únik k tretej strane: keď je serverom používateľ sám, nikto iný nevidí nič.

Bloomove filtre podľa BIP 37, ktoré v roku 2012 priniesli Mike Hearn a Matt Corallo, boli prvým protokolom ľahkého klienta v peer-to-peer sieti Bitcoinu. Návrh bol jednoduchý: peňaženka zostaví Bloomov filter nad svojimi adresami, pošle ho obslužnému plnému uzlu a dostane späť len zodpovedajúce transakcie. Tvrdenie o súkromí znelo tak, že miera falošných pozitív filtra zakryje, o ktoré adresy peňaženka stojí. Toto tvrdenie bolo nepravdivé. Gervais, Karame, Gruber a Capkun v roku 2014 ukázali, že obslužný uzol, ktorý pozoruje čo i len jeden filter, môže množinu adries peňaženky podstatne zúžiť, a že prienik filtrov z tej istej peňaženky obnoví adresy s takmer úplnou istotou. Meranie Jonasa Nicka z roku 2015 na živých nasadeniach BitcoinJ potvrdilo, že skutočný útok obnovil takmer všetky verejné kľúče peňaženky z jediného pozorovaného filtra. Bitcoin Core vypol obsluhu BIP 37 v predvolenom nastavení vo vydaní 0.19.0 (november 2019). Protokol nikdy nebol formálne vyradený, ale väčšina siete ho už neposkytuje.

Kompaktné blokové filtre podľa BIP 157/158, ktoré v roku 2017 určili Olaoluwa Osuntokun, Alex Akselrod a Jim Posen, otočili smer úniku. Peňaženka už neposiela filter serveru. Server vypočíta deterministický filter kódovaný Golombovým kódom (zhruba 20 až 30 KB na blok), ktorý pokrýva každý scriptPubKey v bloku, a každá peňaženka si stiahne ten istý filter a porovnáva ho lokálne. Server nikdy nevidí, čo peňaženka sleduje, pretože filter je pre všetkých rovnaký. Zostávajú úniky na úrovni siete (IP adresa peňaženky ostáva viditeľná) a v časovaní žiadostí o bloky (pri zhode filtra si peňaženka stiahne celý blok a vyžiadanie zriedkavých blokov od jediného peera prezradí, ktoré bloky obsahujú zaujímavé transakcie).

Sťahovanie zodpovedajúcich blokov od rotujúcich odchádzajúcich peerov zmierňuje druhý útok a Tor rieši prvý. Bitcoin Development Kit (BDK) sprístupňuje primitíva filtrov vývojárom peňaženiek a protokol obsluhuje `btcd` aj index kompaktných blokových filtrov v Bitcoin Core.[7]

Wasabi Wallet, ktorú v auguste 2018 spustila firma zkSNACKs, ako prvá použila blokové filtrovanie na strane klienta v spotrebiteľskej peňaženke zameranej na súkromie. Pred verziou 2.6.0 poskytovala Wasabi špeciálne filtre zo svojho backendu, lebo BIP 157/158 v čase návrhu jej architektúry ešte nebol štandardizovaný ani široko nasadený. Tieto filtre používali špecifickú konštrukciu, ktorá zahŕňala len natívne typy skriptov SegWit, vďaka čomu boli v praxi menšie než úplné blokové filtre BIP 158 pokrývajúce každý scriptPubKey. Wasabi prešla na štandardné filtre BIP 158 vo verzii 2.6.0 (máj 2025), čo používateľom umožňuje nasmerovať peňaženku priamo na vlastný uzol Bitcoin Core bez akéhokoľvek sprostredkujúceho servera.

Výsledné úrovne sledujú, koľko peňaženka vyzradí obslužným peerom. Plný uzol nevyzradí nič, čo by sa týkalo konkrétnych adries. Klient BIP 157/158 vyzradí časovanie zhôd v blokoch a IP adresu. Server Electrum na vlastnom stroji nevyzradí nič navonok a zachová pohodlie Electra. Server Electrum od tretej strany vyzradí celý zhluk peňaženky. Klient BIP 37, ak by ešte v produkcii existoval, vyzradí takmer toľko ako Electrum od tretej strany. Poradie odráža, čo synchronizačný kanál peňaženky hovorí protistrane o používateľovi, a v tomto poradí treba architektúry peňaženiek aj uprednostňovať.

Zmeny protokolu na vrstve ťažiarov

Stratum V2, nástupca protokolu pre ťažobné pooly, ktorý Bitcoin používa od roku 2012, je predovšetkým bezpečnostné vylepšenie kanála medzi ťažiarom a poolom. Protokol V1 beží nešifrovane cez TCP, čo prezrádza prúd práce každému sieťovému pozorovateľovi medzi ťažiarom a poolom a umožňuje protivníkovi na ceste presmerovať hashrate útokmi unesenia hashrate, ktoré sa v rokoch 2010 až 2019 opakovane zdokumentovali. V2 šifruje celé spojenie medzi ťažiarom a poolom pomocou rámca Noise s AEAD šifrou, čím sa uzavrie trieda útokov na ceste aj pasívne pozorovanie naraz. Nad týmto bezpečnostným základom umožňuje voliteľné rozšírenie Job Declaration ťažiarovi zostaviť si vlastné šablóny blokov. Pool potom nevyberá, ktoré transakcie vstúpia do poolovanej práce, a prevádzkovateľ poolu, ktorý by sa pokúsil cenzurovať určité transakcie v poolovanom hashrate, by o hashrate prišiel v prospech ťažiara, ktorý si šablóny deklaruje sám.

Braiins Pool, DEMAND Pool a Public Pool sú v čase písania produkčné nasadenia Stratum V2. OCEAN Pool implementuje paralelný protokol DATUM, ktorý používa iný mechanizmus (transparentný záznam o vy-

rovnaní platieb v bitcoinových transakciách samotného poolu) na dosiahnutie rovnakých vlastností bez úschovy a odolnosti voči cenzúre, aké sa snaží dosiahnuť Job Declaration vo V2. Prijatie ktoréhokoľvek mechanizmu je neúplné a krivka prijímania je dôležitejšia pre vlastnosti reťazca z hľadiska cenzúry než pre súkromie ktoréhokoľvek jednotlivého ťažiara.[8]

Dandelion++, obranu pri šírení transakcií, ktorú Monero nasadilo v roku 2020, do Bitcoin Core nezlúčili, pretože návrh prináša vektory útoku odopretím služby na relayoch kmeňa, ktoré revízny proces Bitcoin Core nepovažoval za prijateľné. Praktická alternatíva, ktorú prijali peňaženky zamerané na súkromie, je vysielať každú transakciu pod novou identitou Tor: peňaženka otvorí nový okruh Tor, pripojí sa k jedinému náhodne zvolenému uzlu Bitcoinu, s ktorým sa nikdy predtým nespojila, pošle transakciu a potom zruší spojenie aj okruh. Tento vzor zaviedla Wasabi Wallet a Bitcoin Core ho dnes podporuje cez voľby `-onlynet=onion` a izoláciu okruhu pre každé spojenie. Zostávajúcou útočnou plochou je časová korelácia medzi okruhom Tor peňaženky a tým, ako prvý peer šíri správu do zvyšku siete. Slabší protivníci to využiť nedokážu, globálny pasívny pozorovateľ však stále áno. Štrukturálny záver za všetkými týmito protokolmi je, že súkromie na sieťovej vrstve Bitcoinu je inžiniersky program, ktorý priniesol čiastkové zisky a prevádzkovateľ peňaženky sa musí rozhodnúť ich využiť.

Čo základná vrstva preto neposkytuje

Všetky tieto útoky dokopy vysvetľujú, prečo základná vrstva neposkytuje dôvernosť transakcií (sumy sú viditeľné), neprepojiteľnosť odosielateľa a príjemcu (adresy sú viditeľné a dajú sa zhlukovať), možnosť poprieť, že transakcia prebehla (každá transakcia je verejná), ani ochranu pred analýzou reťazca (vzorce môže analyzovať každý, kto má na to zdroje). Vrstvy postavené nad základnou vrstvou existujú preto, aby porazili konkrétne kombinácie týchto útokov, a každá z nich to robí za konkrétnu cenu. Zvyšok kapitoly skúma, čo každá z nich dosiahne a čo necháva nezmenené.

20.2 Programovateľné peniaze: skriptové primitíva

Bitcoin Script

Každý výstup transakcie obsahuje skript, ktorý určuje podmienky potrebné na jeho minutie. Bitcoin Script je zámerne nie Turingovsky úplný, nevie sa cyklicky opakovať a nemá prístup k vonkajšiemu stavu. Vďaka tomu sú skripty predvídateľné a auditovateľné a programovateľnosť sa obmedzuje na finančné primitíva.

Multisignature

Skripty multisignature (multisig) vyžadujú na schválenie míňania viac kľúčov. Multisig 2 z 3 vyžaduje ľubovoľné dva z troch určených kľúčov, čím umožňuje spoločnú kontrolu bez dôvery v ktorúkoľvek jednu stranu. Staršia podoba multisigu platí za túto kontrolu odhalením v reťazci: skript prezradí verejný kľúč každého účastníka a minutie prezradí, ktoré kľúče podpísali. Podpisy Schnorr umožňujú čistejšiu verziu. MuSig2 a FROST presúvajú prahovú logiku do protokolu súhrnného podpisovania, takže reťazec vidí jeden verejný kľúč a jeden podpis, kým množina účastníkov a prah zostávajú mimo reťazca.[33] Existuje aj prahové ECDSA, no protokoly sú zložitejšie a nemajú rovnako čistý bezpečnostný dôkaz. Firemné pokladnice, dedičské schémy, horúce peňaženky búrz a escrow dohody využívajú toto primitívum na to, aby nahradili dôveryhodného správcu úschovy programovateľnou spoločnou úschovou.

Časové zámky

Časové zámky bránia míňaniu, kým sa nesplnia určené podmienky. Existujú dva druhy:

Absolútne časové zámky (CLTV, CheckLockTimeVerify) bránia míňaniu do určitej výšky bloku alebo časovej známky. Transakciu zamknutú do bloku 900 000 nemožno minúť pred týmto blokom, nech kľúče drží ktokoľvek.

Relatívne časové zámky (CSV, CheckSequenceVerify) bránia míňaniu, kým od vytvorenia výstupu neuplynie určený čas. Výstup zamknutý na 144 blokov nemožno minúť skôr než 144 blokov (približne jeden deň) po jeho vzniku.

Časové zámky umožňujú transakcie s časovým oneskorením, plány postupného uvoľňovania a najmä mechanizmy odvolania, vďaka ktorým sú platobné kanály bezpečné.

Hašové zámky

Hašové zámky vyžadujú odhalenie tajnej hodnoty (vzoru, preimage), ktorej haš zodpovedá určenému hašu. Skript obsahuje haš a na minutie treba predložiť vzor.

Zdá sa to jednoduché, no umožňuje to mocné konštrukcie. Ak chce Alice zaplatiť Carol, ale nemá s ňou priamy kanál, môže platbu smerovať cez Boba pomocou hašových zámkov: Alice zaplatí Bobovi pod podmienkou, že Bob odhalí tajomstvo, ktoré pozná iba Carol. Bob zaplatí Carol rovnakým spôsobom. Keď Carol odhalí tajomstvo, aby si od Boba vyzdvihla platbu, Bob sa tajomstvo dozvie a môže si vyzdvihnúť platbu od Alice. Platba tak v celej ceste buď atomicky uspeje, alebo zlyhá.

Zmluvy so zámkom hašu a času (HTLC)

Spojením hašových zámkov s časovými zámkami vznikajú zmluvy so zámkom hašu a času (Hash Time-Locked Contracts, HTLC). HTLC sa dá minúť dvoma spôsobmi: odhalením vzoru haša (cesta úspechu) alebo po uplynutí časového limitu (cesta vrátenia).

HTLC sú základom siete Lightning. Umožňujú viacskokové platby bez nutnosti dôvery: buď sa platba dokončí na všetkých skokoch, keď konečný príjemca odhalí vzor, alebo všetci účastníci po uplynutí limitu získajú svoje prostriedky späť. Žiadny sprostredkujúci smerovací uzol nemôže ukradnúť prostriedky ani platbu navždy zablokovať.

Čo tieto primitíva robia

Spolu tieto primitíva menia Bitcoin z jednoduchého digitálneho zlata na programovateľné peniaze. Multisig nahrádza dôveryhodných správcov úschovy kontrolou so spoločnými kľúčmi a časové zámky nahrádzajú dôveryhodných plánovačov vynucovaním podľa výšky bloku. Hašové zámky a HTLC idú ďalej: umožňujú podmienené viacskokové platby, pri ktorých nemusí sprostredkovať žiadny escrow agent.

Taproot (BIP 341, aktivovaný v novembri 2021) pridáva k súboru skriptových primitív prínos pre súkromie, ktorý staršie typy výstupov ponúknuť nemohli.[32] Každý výstup Taproot sa zaväzuje k Merkleho stromu alternatívnych skriptov na minutie a ten, kto minie výstup cez ktorýkoľvek list, odhalí len tento list. Ostatné vetvy stromu zostanú nezverejnené a nerozlíšiteľné od bajtov, ktoré sa nikdy nenapísali. Multisig 2 z 3 s kooperatívnou cestou 1 z 1 a obnovovacou cestou s časovým zámkom sa v reťazci míňa ako jediný podpis Schnorr, ak sa použije kooperatívna cesta, a ostatné vetvy sa vôbec neobjavia. Analýza reťazca nevie z minúcej transakcie zistiť, či výstup bol jednoduchý výstup s jedným podpisom, zložitý skript viacerých strán alebo čokoľvek medzi tým. Pravidlo o viditeľnosti cesty skriptu mení vyjadrovaciu silu skriptov Bitcoinu z bremena pre súkromie na prínos pre súkromie: zložitosť, ktorá existuje len pre príležitostné použitie, je predvolene skrytá a odhalí sa len cesta, ktorá sa uplatnila.

Každé primitívum odstraňuje jednu kategóriu dôveryhodného sprostredkovateľa. Spolu umožňujú systémy druhej vrstvy (L2), ako je Lightning, ktoré preberajú bezpečnosť vyrovnania Bitcoinu a pritom získavajú rýchlosť a silnejšie súkromie.

20.3 Riešenia súkromia: spoločné transakcie a výmeny

CoinJoin: spoločné transakcie

CoinJoin spája vstupy viacerých používateľov do jedinej transakcie s viacerými výstupmi.[9] Účastníci si navzájom neplatia, každý posiela prostried-

ky sám sebe. Prínos pre súkromie vzniká prerušením väzby medzi vstupmi a výstupmi: ak Alice, Bob a Carol prispejú každý jedným vstupom a každý dostane jeden výstup rovnakej hodnoty, pozorovateľ nezistí, ktorý výstup patrí ku ktorému vstupu.

CoinJoin si vyžaduje koordináciu medzi účastníkmi. Objavili sa dva hlavné prístupy.

JoinMarket, staršia implementácia, používa trhovú koordináciu: „takeri" (tí, ktorí zadávajú) začínajú kolá CoinJoinu a platia „makerom" (tým, ktorí poskytujú likviditu) za likviditu.[34] Každý taker koordinuje svoju vlastnú transakciu, takže koordinácia je rozložená medzi mnohých účastníkov a nie sústredená v jedinej službe. Transakcia má pre každého účastníka jeden výstup s rovnakou hodnotou a práve táto množina výstupov dostáva anonymitu. Taker môže aj zaplatiť priamo v rámci CoinJoinu, ak pridá samostatný výstup platby a zachová výstup zmiešavania s rovnakou hodnotou. Makeri poskytujú likviditu a zarábajú poplatky, ale výstup platby riadiť nemôžu, pretože neovládajú šablónu transakcie. Takeri musia používať zložitejší softvér a platiť za účasť, no nijakého externého koordinátora nemožno vypnúť.

Wasabi 1.0 používala podobný model s rovnakými hodnotami, s centrálnym koordinátorom a slepými podpismi podľa Chauma, ktoré umožňovali anonymnú registráciu výstupu s rovnakou sumou. Wasabi 2.0 zmenila konštrukciu pomocou WabiSabi, ktorá používa anonymné poverenia s overovaním pomocou kľúča (keyed-verification anonymous credentials, KVAC) na vydávanie slepých podpisov nad ľubovoľnými sumami. Účastníci môžu registrovať vstupy s ľubovoľnou hodnotou a voliť hodnoty výstupov, ktoré sa hodia ich peňaženkám, takže nie je nutné tlačiť každý súkromný výstup do jednej nominálnej hodnoty. Keďže sa WabiSabi vyhýba opakujúcim sa rovnakým kusom, spotrebuje menej miesta v blokoch a zlepší aj efektivitu peňaženky, aj súkromie.

WabiSabi zovšeobecňuje aj platby cez CoinJoin: každý účastník môže počas kola registrovať výstupy platieb a koordinátor nevie rozlíšiť výstup platby od výstupu prevodu sám sebe. Takéto zlučovanie vytvára oveľa väčšie transakcie s vyššími množinami anonymity, než aké zvyčajne dosahuje distribuovaný model JoinMarketu. Kompromis je v tom, že statickí koordinátori prinášajú problémy s cenzúrou: koordinátora možno vyradiť z prevádzky právnym tlakom alebo technickým útokom. Protokol WabiSabi je otvorený, koordinátora môže prevádzkovať ktokoľvek a viac koordinátorov môže fungovať súčasne. Keď pôvodný koordinátor Wasabi ukončil prevádzku pre regulačný tlak, alternatívni koordinátori ukázali, že protokol samotný nie je viazaný na jediného prevádzkovateľa, hoci likvidita a použiteľnosť stále záviseli od podrobností implementácie.[39]

PayJoin: zmiešavanie cez CoinJoin zabudované do platby

PayJoin je navrhnutý výslovne pre platobné transakcie. Alice nepošle Bobovi platbu v jednoduchej transakcii, ale vstupy pridajú Alice aj Bob. Výsledok vyzerá ako bežná platba, nie ako CoinJoin.

PayJoin pracuje s iným modelom súkromia než CoinJoin. Nevytvára anonymitu zmiešaním s inými používateľmi, ale je steganografický: transakcie, ktoré zlepšujú súkromie, nerozoznať od bežných transakcií. Výstupy s rovnakou sumou v CoinJoine zanechávajú na blockchaine zjavný odtlačok, kým transakcie PayJoin vyzerajú ako každá normálna platba.

Prínos pre súkromie je štrukturálny. PayJoin porušuje heuristiku spoločného vlastníctva vstupov, teda predpoklad, že všetky vstupy transakcie patria jedinému subjektu. Analýza reťazca sa na túto heuristiku silno spolieha. Keď sa transakcie PayJoin nedajú odlíšiť od obyčajných, analytici nevedia, ktoré transakcie heuristiku porušujú, a to znižuje spoľahlivosť zhlukovej analýzy pri všetkých transakciách, nielen pri PayJoinoch. Širšie používanie PayJoinu tak zlepšuje súkromie celej siete, lebo vnáša neistotu do predpokladov analýzy reťazca.

PayJoin skrýva aj výšku platby pred obyčajnou aritmetikou reťazca. Pri bežnej platbe je výstup príjemcu rovný sume platby. Pri PayJoine pridá príjemca hodnotu svojho vlastného vstupu navyše, takže výstup, ktorý dostane, sa už nerovná platbe odosielateľa. Ochrana je podmienená: ak protivník neskôr oddelí vstupy odosielateľa od vstupov príjemcu, dá sa skutočná výška platby zrekonštruovať. Rovnaká konštrukcia môže zlepšiť efektivitu využitia blokov. Príjemca môže do tej istej transakcie pridať nesúvisiace platby iným ľuďom alebo koordinovať vstupy a výstupy ďalších účastníkov, čím sa stane koordinátorom viacúčastníckeho CoinJoinu okolo platby. Tým sa ušetrí miesto v blokoch, lebo sa niekoľko ekonomických prevodov spojí do jednej transakcie, no voči koordinátorovi tu súkromie nie je také ako pri WabiSabi: príjemca, ktorý transakciu koordinuje, vidí roly účastníkov, ktoré sám zostavuje.

Obmedzenia

CoinJoin a PayJoin zlepšujú súkromie, ale každý má iné obmedzenia. CoinJoin potrebuje ďalších účastníkov a skutočná anonymita závisí od likvidity dostupnej v kole. WabiSabi odstraňuje obmedzenie pevných nominálnych hodnôt, ktoré pri starších návrhoch koordinátorov vytváralo zjavný zvyšok, takže nerovnaké sumy nie sú hlavným obmedzením. Zostávajú prevádzkové obmedzenia: koordinátor môže odoprieť službu, stanoviť pravidlá prijímania, zvoliť parametre kola alebo zmiznúť pod právnym tlakom. Jeden koordinátor navyše zvykne pritiahnuť väčšinu likvidity, a tak sa stáva praktickým miestom stretnutia, aj keď protokol dovoľuje mnohých koordinátorov. Kolá závisia aj od toho, či sú účastníci k dispozícii. Účastník, ktorý nepodpíše, môže vynútiť kolo na určenie vinníka

a likvidita útočníkov typu Sybil môže skutočnú anonymitu znížiť, ak protivník zaplatí poplatky za vstup s mnohými mincami. Po CoinJoine môže nedbalé míňanie súkromie stále zmariť, ak spojí histórie, ktoré kolo oddelilo.

Obmedzenia PayJoinu sú iného druhu. Steganografické tvrdenie, že PayJoiny vyzerajú ako bežné platby, je podmienené. Heuristika zbytočného vstupu, ktorú proti PayJoinu analyzovali v roku 2018 Adam Gibson a LaurentMT a ktorú v roku 2022 sformalizovali Ghesmati, Fdhila a Weippl, označí transakcie, ktorých vstupy presahujú to, čo by vytvoril rozumný výber mincí. Meranie LaurentMT zistilo, že približne tretina transakcií s dvoma výstupmi porušuje niektorý z variantov, takže PayJoiny, ktoré spadnú do tejto tretiny, sa dajú štatisticky odhaliť.[10] Odtlačky peňaženiek narúšajú toto tvrdenie v ďalších smeroch: najmä zmiešané typy skriptov vo vstupoch prezrádzajú pôvod od viacerých strán tak spoľahlivo, že ich BIP 78 až do septembra 2024 úplne zakazoval. Hodnoty sekvencie, nLockTime, poradie vstupov podľa BIP 69 a vzorce hodnoty R v podpisoch prežijú spojenie s pôvodnými odtlačkami neporušené.

Konštrukcia z princípu vystavuje odosielateľovi jedno z UTXO príjemcu. Zlomyseľný odosielateľ to môže zneužiť ako kanál deanonymizácie proti príjemcovi, ktorému platí. Sondovanie voči verejnému koncovému bodu obchodníka je obmedzené tým, že prvou správou odosielateľa v BIP 78 je plne podpísaná a vysielateľná pôvodná transakcia, takže odosielateľ, ktorý preruší komunikáciu, aby sondoval, riskuje, že príjemca túto záložnú transakciu odvysiela a platbu si ponechá. Prevádzkovo príjemca platí poplatok za vstup, ktorý pridal, zvýšenie poplatku cez replace-by-fee si vyžaduje opätovnú koordináciu oboch strán, lebo obe transakciu podpísali, a predvolené nastavenie BIP 78 o nahradení výstupu dovoľuje kompromitovanému serveru PayJoin presmerovať platbu, pokiaľ sa odosielateľ nerozhodne inak.

Rozhodujúcim obmedzením rozšírenia sa stali náklady na infraštruktúru: BIP 78 vyžadoval, aby príjemca prevádzkoval koncový bod HTTP chránený TLS, dosiahnuteľný v čase platby. Asynchrónny nástupca BIP 77 (zlúčený v máji 2025) túto požiadavku odstraňuje len tak, že vedie prevádzku cez adresár OHTTP, ktorého jediné produkčné nasadenie, payjo.in, sa stáva novým subjektom, ktorému treba dôverovať.[11] Šesť rokov po BIP 78 sa počet produkčných implementácií odosielateľa aj príjemcu pohybuje v jednotkách, Bitcoin Core nemá natívnu integráciu, a prínos neistoty pre analýzu reťazca, na ktorý sa steganografický argument opiera, je preto skutočný, ale malý.

Oba nástroje tiež vyžadujú, aby ich používatelia pochopili a správne uplatnili, čo pridáva zložitosť implementácie k obmedzeniam na úrovni protokolu, ktoré má každý z nich.

CoinSwap: neprepojiteľnosť naprieč transakciami

CoinSwap je druhý prístup v reťazci na pretrhnutie grafu transakcií. CoinJoin spája vstupy a výstupy viacerých používateľov do jednej transakcie, kým pri CoinSwap si dve strany vymenia výstupy v oddelených transakciách: minca Alice ide v jednej transakcii na adresu Boba a minca Boba ide v inej transakcii na adresu Alice. Vonkajší pozorovateľ vidí dve obyčajne vyzerajúce platby. Žiadny odtlačok transakcie nerozlíši CoinSwap od dvojice nesúvisiacich platieb, lebo každá transakcia má jeden vstup a dva výstupy a nenesie nijaký signál o koordinácii v reťazci. Väzba medzi mincou, ktorá bola minutá, a mincou, ktorá bola prijatá, sa pri viacerých skokoch stráca: analýza reťazca vie sledovať mincu dopredu k adrese protistrany výmeny, ale nevie určiť, či hodnota pokračovala týmto smerom, alebo či ďalšie míňanie protistrany pochádza z vymenenej mince, alebo z nesúvisiacej.

Vlastnosť súkromia je tu vierohodná popierateľnosť vo veľkom. Pri CoinJoine vedia nástroje analýzy reťazca rozpoznať transakciu ako zmiešavaciu udalosť, aj keď nevedia určiť, ktorý výstup patrí ktorému účastníkovi. Pri CoinSwape čelia ťažšiemu problému: nie je tam žiadna zmiešavacia udalosť, ktorú by mohli rozpoznať. Výmena vyzerá ako akékoľvek iné míňanie a reťazec výmen cez viacero protistrán vytvára graf transakcií, v ktorom je ekonomický tok nezistiteľný, a nie nejednoznačný tak, ako je nejednoznačný CoinJoin.

Konštrukcia je dnes na Bitcoine hlavne teoretická. Protokol atomickej výmeny, v ktorom zmluva so zámkom hašu a času vynucuje, že obe časti výmeny sa buď dokončia, alebo obe vrátia, pochádza z návrhu Tiera Nolana z roku 2013 na fóre Bitcoin Talk.[35] Výmeny CoinSwap v rámci jedného reťazca, ktoré majú zlepšiť súkromie na základnej vrstve, sa skúmali vo výskume a v raných prototypoch nástrojov, no neexistuje široko nasadená implementácia s významným využitím. Rozhodujúcim obmedzením je koordinačný problém na strane dopytu: nájsť ochotnú protistranu so správnou veľkosťou výstupu v správnom čase vyžaduje buď verejný trh (ktorý prezrádza zámer), alebo dôveryhodné miesto stretnutia (ktoré znovu zavádza koordinačný server).

Lightning je mimoreťazcová podoba toho istého primitíva. Každý skok platby cez Lightning je atomický CoinSwap medzi susednými partnermi kanála, vynútený zmluvami so zámkom hašu a času (HTLC) na tých istých predpokladoch o eliptických krivkách, aké Bitcoin používa na míňanie. Pri platbe z Alice ku Carol cez Boba vykonajú Alice a Bob jednu výmenu, kým Bob a Carol druhú. Ani Bob, ani Carol nevedia bez ďalších informácií prepojiť prichádzajúci HTLC Alice s odchádzajúcou platbou Carol. Konštrukcia presúva koordináciu CoinSwapu úplne zo základnej vrstvy, kde prebieha s latenciou v milisekundách a bez stopy v reťazci pri každej plat-

be. V tomto zmysle je Lightning produkčné nasadenie modelu CoinSwap, presunuté do vrstvy grafu kanálov.

20.4 Platby mimo reťazca bez úschovy u tretej strany

Lightning, Ark a Spark sú tri mimoreťazcové konštrukcie, ktoré tu skúmame. Presúvajú platby v bitcoinoch mimo reťazca a pritom zachovávajú každému používateľovi možnosť jednostranne sa vrátiť na základnú vrstvu bez súčinnosti protistrany. Líšia sa v tom, ako spravujú likviditu, čo vidí prevádzkovateľ a aké skriptové schopnosti konštrukcia ponúka, ale vo všetkých troch ostáva úschova pri používateľovi. Konštrukciám s úschovou u tretej strany sa venuje nasledujúci oddiel.

Sieť Lightning: platobné kanály

Sieť Lightning umožňuje transakcie mimo reťazca cez platobné kanály.[12] Dve strany zamknú bitcoin na adrese s multisigom a potom si vymieňajú podpísané transakcie, ktoré aktualizujú zostatok medzi nimi, bez toho, aby každú aktualizáciu vysielali na blockchain. Kým obe strany spolupracujú, kanál zvládne ľubovoľne veľa platieb a až jeho prípadné uzavretie sa vyrovná na základnej vrstve. Kanály možno aj spájať: Alice zaplatí Carol cez Boba, kedykoľvek existujú kanály Alice–Bob a Bob–Carol, a toto smerovanie rozširuje graf platieb ďaleko za množinu priamych partnerov kanálov. Malý počet dobre prepojených uzlov tak dokáže podporiť veľký počet platieb medzi stranami, ktoré spolu nikdy kanál priamo neotvorili.

Okamžitá finalita

Potvrdenie na základnej vrstve je pravdepodobnostné a pomalé: bloky prichádzajú v priemere raz za desať minút, intervaly sa veľmi líšia a obozretní príjemcovia čakajú na ďalšie potvrdenia pre prípad reorganizácie. Lightning toto čakanie nahrádza okamžite vynútiteľným nárokom v štruktúre kanála, podpísanou transakciou záväzku, ktorú môže príjemca v prípade potreby odvysielať. Vyrovnanie je v rámci kanála kryptografické, nie pravdepodobnostné ako v reťazci: buď príjemca odhalí vzor a platba uspeje atomicky na všetkých skokoch, alebo uplynú časové limity a prostriedky sa vrátia odosielateľom. Platby na predajných miestach, mikroplatby a toky medzi strojmi sa stávajú praktickými, keď réžia platby klesne na milisekundy.

Vlastnosti súkromia a model grafu kanálov

Lightning ponúka vlastnosti súkromia, ktoré základná vrstva nemá. Platby v kanáloch nie sú na blockchaine viditeľné, v reťazci sa objaví len otvorenie a zatvorenie kanála. Cibuľové smerovanie znamená, že každý sprostredkujúci uzol pozná len svojho predchodcu a nasledovníka, nie celú

cestu. Oznámené kapacity kanálov sú viditeľné, ale zostatok medzi dvoma stranami kanála je súkromný.

Model súkromia je iný než na základnej vrstve Bitcoinu, nie jednoducho lepší vo všetkých ohľadoch. Verejný graf kanálov odhaľuje štruktúru siete, kým platobné cesty cez ňu zostávajú súkromné. Smerovacie uzly vidia sumu, ktorá nimi prechádza, ale platby sa dajú rozdeliť na viac ciest, takže jediný smerovací uzol nemusí vidieť celú sumu. Topológia je verejná, skutočné používanie je skryté.

Obmedzenia súkromia

Vlastnosti súkromia na Lightningu sú slabšie, než by sa mohlo zdať.[13]

Zisťovanie zostatkov sondovaním je vážna zraniteľnosť. Protivník môže posielať sondovacie platby cez cieľové kanály a sledovať, ktoré sumy prejdú a ktoré zlyhajú. Výskum ukázal účinný odhad zostatkov za určitých podmienok siete, často s nízkymi nákladmi pre útočníka, lebo sondy sú navrhnuté tak, aby zlyhali. Systematickým sondovaním môžu protivníci odvodiť rozdelenie zostatkov v kanáloch, cez ktoré vedia smerovať.

Smerovacie uzly vidia sumy platieb, ktoré nimi prechádzajú. Cibuľové smerovanie skrýva pôvod a cieľ platby, no sprostredkujúce uzly vidia hodnoty. Smerovací uzol, ktorý sa objavuje v mnohých cestách, získava štatistické informácie o tokoch platieb v sieti.

Poskytovatelia služieb Lightning (LSP) vyvolávajú osobitné obavy o súkromie. Mnohé mobilné peňaženky sa na správu kanálov a smerovanie pripájajú k jedinému LSP. LSP sa dozvie identitu uzla používateľa a jeho sieťovú adresu, a ak platby smerujú cez uzol LSP, aj veľkú časť platobnej aktivity. Tým sa vracia dôveryhodná tretia strana, ktorú mal Bitcoin odstrániť.

Transakcie otvorenia a zatvorenia kanála v reťazci prepájajú aktivitu na Lightningu s transakciami na základnej vrstve. Zhluková analýza ich môže spojiť s ďalšími transakciami používateľa. Transakcie núdzového uzavretia tiež môžu prezradiť stav kanálov v čase uzavretia.

Jedna štúdia z roku 2021 o deanonymizácii naprieč vrstvami zistila, že kombinovanie údajov z reťazca a z Lightningu dokázalo prepojiť 43,7 % uzlov Lightningu v jej súbore údajov so súvisiacimi adresami Bitcoinu.[14] Interakcia medzi vrstvami vytvára únik informácií, ktorý by žiadna z vrstiev sama neodhalila.

Obmedzenia Lightningu a súčasný stav

Lightning má aj prevádzkové obmedzenia, ktoré presahujú súkromie. Kanály vyžadujú uzamknutý kapitál, prijímacia kapacita vyžaduje, aby protistrany uzamkli prostriedky, platby vyžadujú, aby bol príjemca online alebo aby fungovali strážne veže, a optimálna prevádzka vyžaduje správu

likvidity naprieč kanálmi. Veľké platby nemusia nájsť cesty s dostatočnou likviditou.

Vylepšenia súkromia sa aktívne vyvíjajú a nasadzujú. Zakrytie trasy (route blinding), najmä v novších tokoch v štýle BOLT 12, môže zlepšiť súkromie príjemcu tým, že pred protistranami skryje identitu uzla a časti cesty, hoci podpora zostáva závislá od implementácie. Rozdelenie platby na viac ciest znižuje informácie dostupné ktorémukoľvek jedinému smerovaciemu uzlu. Trampolínové smerovanie môže ďalej obmedziť, koľko topológie sa dozvedia niektorí odosielatelia alebo smerovací sprostredkovatelia, no jeho účinky na súkromie závisia od spôsobu implementácie. Protokol Lightning sa neustále vyvíja a špecifikácie sa pravidelne aktualizujú. Mnohé obavy o súkromie, ktoré výskumníci zistili, sa riešia vylepšeniami protokolu, hoci niektoré, napríklad sondovanie zostatkov, ostávajú štrukturálnym problémom vlastným procesu objavovania ciest. Lightning zostáva vyvíjajúcou sa technológiou, ktorej vlastnosti súkromia sa menia podľa volieb pri implementácii aj podľa podmienok v sieti.

Ark: kolá platieb so spoločným UTXO

Ark, ktorý od roku 2023 špecifikuje Burak Keçeli, je mimoreťazcová konštrukcia, ktorá odstraňuje bremeno správy likvidity z Lightningu, no za cenu iného modelu dôvery.[15] Používateľ neotvára kanál s konkrétnou protistranou a nespravuje prichádzajúcu a odchádzajúcu kapacitu, ale pripojí sa ku kolu Ark tak, že odovzdá bitcoin do spoločného UTXO, ktoré ovláda server Ark. Dostane virtuálne UTXO v rámci tohto spoločného UTXO, ktorých hodnotu možno okamžite míňať v protokole Ark, a na konci každého kola sa vyrovná do nového spoločného UTXO. Používatelia môžu prijímať platby bez toho, aby vopred otvárali kanály. Práve tu má Lightning stále medzeru v použiteľnosti pre mobilné peňaženky, ktorých prijímaciu kapacitu oceňujú a zabezpečujú poskytovatelia služieb Lightning.

Model dôvery je odlišný od Lightningu. Protistrana na Lightningu, ktorá sa správa nečestne, nemôže ukradnúť prostriedky kanála, lebo konštrukcia s odvolávacími kľúčmi umožňuje čestnej strane jednostranne uzavrieť kanál pri akomkoľvek zastaranom stave, ktorý druhá strana zverejní. Ani server Ark nemôže ukradnúť prostriedky používateľa, pretože každé vTXO nesie cestu transakcie jednostranného odchodu, ktorú môže jeho majiteľ odvysielať priamo na základnú vrstvu. Útok, ktorý môže server Ark vykonať, je zlomyseľné obťažovanie (griefing): ak odmietne pokračovať v kolách, núti používateľov k odchodom do reťazca, ktoré sú počas preťaženia drahé na poplatkoch.

Konštrukcia tiež odhaľuje serveru viac informácií, než odhaľuje Lightning ktorémukoľvek jedinému partnerovi kanála, pretože server sa podieľa na vyrovnaní každého používateľa a nie len niektorej podmnožiny. Arkade, hlavná produkčná implementácia, časť tohto odhalenia zmierňuje

tým, že podpisový kľúč prevádzkuje v dôveryhodnom prostredí na vykonávanie kódu (TEE) a komunikáciu používateľa s podpisovateľom vedie cez end-to-end šifrovanie, takže infraštruktúra prevádzkovateľa nemôže čítať obsah jednotlivých transakcií, hoci koordinuje dávkové vyrovnanie.

Programovateľné vykonávacie prostredie Arkade podporuje aj podmienky míňania, ktoré presahujú to, čo dokáže vyjadriť Bitcoin Script v reťazci, pretože mimoreťazcová vrstva vTXO nie je obmedzená limitmi skriptov základnej vrstvy. V zásade to zahŕňa platobné schémy s dôkazmi s nulovou znalosťou, v ktorých dôkazy nad výstupmi VTXO nahrádzajú sumy a identity protistrán v čitateľnej podobe. Viditeľnosť prevádzkovateľa sa tak zmenšuje k úrovni, akú dosahuje ecash podľa Chauma, a zároveň sa zachováva jednostranný odchod. Táto schopnosť zostáva v čase písania teoretická a nad Ark neprebieha v produkcii žiadna nasadená schéma ZK. Second je ďalšia implementácia v produkčnom meradle v čase písania. Konštrukcia je dosť nová na to, aby jej správanie v praxi pri nepriateľskom prevádzkovateľovi nebolo vyskúšané v rozsahu Lightningu.

Spark: prevody cez statechain

Spark je mimoreťazcový protokol Bitcoinu postavený na statechainoch a rozšírený o prahové podpisovanie FROST cez viacerých podpisových operátorov (Signing Operators, SO).[36] V základnom modeli statechainu ovláda bitcoinové UTXO kľúč rozdelený medzi súčasného majiteľa a podpisovú službu. Mimoreťazcový prevod mince znamená, že súčasný majiteľ a služba spoločne priradia kľúč príjemcovi a služba vymaže svoj predchádzajúci podiel na kľúči, aby predchádzajúci majiteľ nemohol míňať. Spark to rozširuje na distribuovanú množinu SO s využitím FROST a zavádza architektúru listov, ktorá umožňuje deliť a spájať hodnoty UTXO mimo reťazca, čím odstraňuje obmedzenie celých mincí z raných návrhov statechainu. Reťazec nezaznamená nič, kým list neodíde. V reťazci sa stav Sparku javí ako reťazec výstupov s jedným podpisom.

Model dôvery je na úrovni operátora typu 1 z n: pokiaľ aspoň jeden SO po prevode čestne vymaže svoj predchádzajúci podiel kľúča, schopnosť predchádzajúceho majiteľa míňať je odvolaná a nárok nového majiteľa je zabezpečený. Aj keby sa všetci SO neskôr tajne dohodli alebo boli donútení, nemôžu hýbať prostriedkami bez podpisu súčasného majiteľa, lebo používateľ je povinným spolupodpisovateľom každej transakcie. Operátori si zachovávajú útočnú plochu v dostupnosti: koordinované odmietnutie spolupodpisu vtiahne používateľa do jednostranného odchodu do reťazca cez záložnú transakciu s časovým zámkom, čo sa svojou povahou podobá riziku griefingu zo strany operátora Ark.

Strop súkromia určuje to, čo SO vidia pri podpisovaní. Každý prevod prechádza množinou SO, ktorá pri každom liste pozoruje sumy, odosielateľa aj príjemcu. Vonkajší pozorovateľ sledujúci reťazec vidí len financujú-

ce transakcie a odchody, kým SO vidia celý graf prevodov medzi týmito udalosťami. Rozdelenie roly operátora medzi viacerých SO znižuje riziko jediného bodu nátlaku (súdny príkaz alebo prienik sa musí dostať k prahovému počtu operátorov, aby zrekonštruoval celú históriu), no žiadny jednotlivý SO nie je slepý voči transakciám, ktoré spolupodpisuje. Viditeľnosť operátora je teda pri Sparku vyššia než pri Lightningu, kde každý uzol vidí len susedné skoky, a vyššia než v dávkovom modeli Ark, kde operátor pri vyrovnaní vidí sumy výstupov, ale nie vnútorný graf prevodov medzi kolami.

Porovnanie Lightningu, Ark a Sparku

Lightning, Ark a Spark volia rôzne body na tom istom spektre dôvery a súkromia. Lightning rozkladá dôveru po grafe kanálov, takže každý používateľ dôveruje iba svojim protistranám a voči ktorejkoľvek z nich môže jednostranne odísť. Za toto rozloženie platí zložitou správou likvidity, obmedzeniami prichádzajúcej kapacity a útočnou plochou sondovania zostatkov, ktorý sme opísali vyššie. Ark sústreďuje koordinačnú rolu v jedinom serveri, ktorý nemôže ukradnúť prostriedky, ale môže obťažovať odmietaním kôl a vidí z platobného toku každého používateľa viac, než vidí ktorákoľvek protistrana na Lightningu. Za túto koncentráciu platí tým, že odstraňuje problém prichádzajúcej likvidity, ktorý Lightning pre mobilných príjemcov nevyriešil. Spark, ukotvený v modeli statechainu, rozkladá podpisovú rolu na prahovú množinu operátorov, ktorá spoločne vidí celý graf prevodov, výmenou za okamžité mimoreťazcové prevody bez zamknutej likvidity a bez účasti v kolách.

Architektonický rozdiel medzi Ark a Sparkom, ktorý má pre súkromie najväčšiu váhu, je skriptovateľnosť. Vrstva vTXO v Ark prevádzkuje mimoreťazcové vykonávacie prostredie, ktorého podmienky míňania presahujú to, čo môže v reťazci vyjadriť Bitcoin Script základnej vrstvy. Časové zámky, hašové zámky, prahové podpisy aj konštrukcie s covenantmi sa uplatnia v rámci kola Ark, no mimoreťazcový kontext pripúšťa aj systémy dôkazov ZK, ktoré nemajú priamy ekvivalent v reťazci: platobná schéma ZK nad modelom vTXO v Ark by mohla zaslepiť sumy alebo vzťahy odosielateľa a príjemcu pred operátorom úplne, čím by sa jeho viditeľnosť priblížila tomu, čo dosahuje ecash podľa Chauma, pri zachovaní jednostranného odchodu. Prevody cez statechain takýto povrch nemajú. Každý SO musí spolupodpísať každý prechod stavu a podpisový protokol vyžaduje, aby každý SO transakciu videl. Neexistuje cesta v skripte, ktorou by dôkaz ZK mohol nahradiť príspevky kľúčov od SO. Strop súkromia v Ark je preto otvorený pre budúcu prácu na protokole, kým strop Sparku je štrukturálne nižší už z návrhu.

20.5 Vrstvy súkromia s úschovou u tretej strany

Lightning, Ark a Spark zachovávajú jednostranný odchod, teda každý používateľ môže získať späť prostriedky na základnej vrstve bez súčinnosti protistrany. Druhá rodina vrstiev súkromia sa tejto vlastnosti vzdáva výmenou za silnejšie súkromie pred vonkajšími pozorovateľmi, za dôverné sumy alebo za pohodlie prijímania offline. Model dôvery sa v tejto rodine mení od jediného operátora až po federáciu strážcov a spolu s ním sa mení aj model súkromia. Tento oddiel skúma tri konštrukcie v poradí od najmenšieho po najväčšie rozloženie dôvery: mixéry s jedným operátorom, mincovne podľa Chauma (jednotlivé aj federované) a federovaný sidechain Liquid.

Mixéry s úschovou ako základná úroveň súkromia

Najprimitívnejšia cesta k súkromiu transakcií je združiť prostriedky u správcu úschovy. Centralizovaný mixér Bitcoinu prijíma vklady od mnohých používateľov, mince zmieša a z fondu vráti rovnocenné sumy na tie výberové adresy, ktoré si každý používateľ určí. Pre vonkajšieho pozorovateľa, ktorý sleduje blockchain, sú vklady a výbery od seba odpojené: analýza reťazca vidí, že prostriedky vstúpili do zhluku operátora a iné z neho vystúpili, ale nevidí, kto čo dostal. Voči firmám na analýzu blockchainu a bežným vonkajším protivníkom správca úschovy poskytuje skutočné súkromie a presne to Bitcoin mixéry robili viac než desať rokov.

Správca úschovy však nezaslepuje sám seba. Prevádzkovateľ mixéra drží priradenie medzi vkladmi a výbermi už z konštrukcie, pretože je to on, kto mince presúva. Keď prevádzkovateľ spolupracuje, súkromie používateľa platí voči všetkým ostatným. Keď je nepriateľský, keď mu súd nariadi vydať údaje alebo keď ho niekto napadne, používateľ nemá žiadne súkromie a vnútorná účtovná kniha prevádzkovateľa sa stáva sledovacím dosje každého, kto službu kedy použil. Stíhanie Romana Sterlingova za údajnú prevádzku Bitcoin Fog sa točilo presne okolo tohto: prevádzkovateľ videl všetko a vyšetrovanie sa týkalo rekonštrukcie toho, čo prevádzkovateľ videl. Vrstva súkromia s úschovou, ktorá závisí od čestnosti prevádzkovateľa, problém dôvery len presunula, nevyriešila ho. Rovnakú štruktúru majú aj bežné peňaženky a burzy s úschovou. Držanie bitcoinu u správcu úschovy združuje aktivitu v reťazci za adresami správcu, čo poskytuje skutočné súkromie voči vonkajším pozorovateľom analyzujúcim reťazec. Rozdiely vznikajú v postupoch samotného správcu: burza, ktorá vyžaduje KYC, vedie záznamy výberov podľa identity alebo presúva prostriedky cez zle označené horúce peňaženky, odovzdá tieto informácie každému protivníkovi, ktorý ju dokáže donútiť alebo napadnúť. Prínos úschovy pre súkromie je skutočný, ale úplne závisí od toho, ako prevádzkovateľ nakladá s údajmi, od jeho právnych rizík a od hygieny v reťazci.

Ecash podľa Chauma: zaslepenie operátora

Schéma slepých podpisov Davida Chauma z roku 1982 rieši problém operátora presne tam, kde to mixér s úschovou nedokáže.[16] Používateľ pripraví token so sériovým číslom a pred predložením mincovni na podpis ho zaslepí. Mincovňa podpíše zaslepenú podobu bez toho, aby kedy videla pôvodné sériové číslo. Používateľ potom podpísaný token odslepí a drží platný podpis na sériovom čísle, o ktorom mincovňa nemá žiadny záznam. Keď používateľ token neskôr vymení, mincovňa overí svoj vlastný podpis na novoodhalenom sériovom čísle, ale nemôže vymenenie spojiť s konkrétnou udalosťou vydania.

Pri aplikácii na Bitcoin sa z konštrukcie stane protokol vkladu a výberu, v ktorom operátor skutočne nevie, kto dostal ktoré mince. Používatelia vložia bitcoin do mincovne a dostanú slepo podpísané tokeny, ktoré fungujú ako skladové potvrdenky, teda peniaze na doručiteľa. Medzi sebou s nimi obchodujú peer-to-peer alebo ich vymenia späť za bitcoin, keď chcú odísť. Mincovňa eviduje, kto vložil a kto vymenil, ale obe strany svojej účtovnej knihy nevie prepojiť. Operátor už nemá informácie na to, aby používateľa zradil, ani keby ho k tomu niekto nútil.

Cashu a Fedimint: dve nasadenia, rovnaké zaslepenie

Túto konštrukciu na Bitcoine implementujú dva súčasné projekty. Cashu funguje ako súbor nezávislých mincovní s jedným operátorom, ktoré hovoria spoločným protokolom.[17][37] Každá mincovňa priamo prevádzkuje uzol Lightning, takže Lightning je hlavným platobným kanálom: používatelia vkladajú a vyberajú cez faktúry Lightning. Vlastnosti súkromia vyplývajú priamo z konštrukcie Chauma: operátor vidí sumy a časovanie, ale nie tok tokenov od používateľa k používateľovi, a vonkajší pozorovatelia blockchainu vidia iba kanály Lightning operátora. Prevádzková jednoduchosť je zároveň rizikom: jediný operátor môže zlyhať, byť napadnutý, zmiznúť alebo odmietnuť výmeny a používatelia danej mincovne znášajú celé riziko. Mincovne sú lacné na prevádzku, takže praktickým zmierením je, že používatelia držia na jednej mincovni malé zostatky a vyberajú si operátorov, ktorých povesť vedia posúdiť. Vďaka súkromiu slepých podpisov nemôže mincovňa selektívne cenzurovať jedného konkrétneho používateľa. Môže len nafúknuť množstvo tokenov v obehu alebo globálne odopierať výmenu a ukradnúť prostriedky všetkých používateľov.

Fedimint implementuje rovnaké zaslepenie s federovanou úschovou.[18][38] Viacerí strážcovia spoločne ovládajú bitcoinové rezervy mincovne pomocou prahového multisigu v reťazci, takže žiadny jednotlivý strážca nemôže jednostranne ukradnúť prostriedky, zastaviť výmeny ani nátlakom donútiť používateľa. Na akúkoľvek akciu s podkladovým bitcoinom musí spolupracovať prahový počet strážcov. Spojenie s Lightningom zabezpečujú nezávislé brány Lightning (Lightning Gateways): samostatné uzly,

ktoré federáciu prepájajú so sieťou Lightning a pracujú mimo hranice dôvery federácie, takže prístup k Lightningu nezávisí od toho, či federácia sama drží likviditu kanálov. Samotné vydávanie ecashu používa schému prahových slepých podpisov (threshold blind signature scheme, TBS), v ktorej každý strážca drží len podiel kľúča. Vydanie slepo podpísaného tokenu vyžaduje, aby prahový počet strážcov prispel čiastočnými podpismi, čo znamená, že žiadna podmnožina pod prahom nemôže tokeny jednostranne vydávať ani cenzurovať. Vlastnosti súkromia voči vonkajším pozorovateľom sú rovnaké ako pri Cashu a zaslepenie operátora vychádza z rovnakej myšlienky, no operátor je teraz federácia, ktorej členovia sa navzájom sledujú. Kompromis je prevádzkový: federácie treba zostaviť, koordinovať a udržiavať, čo je náročnejšie než prevádzkovať jedinú mincovňu a náročnejšie než ju používať.

Liquid: federované dôverné transakcie

Liquid je federovaný sidechain Bitcoinu, ktorý prevádzkuje konzorcium búrz a obchodných firiem pod koordináciou Blockstreamu.[19] Jeho menovou jednotkou je Liquid Bitcoin (L-BTC), obojsmerný peg na Bitcoin na základnej vrstve, ktorý spravuje federácia. Pre túto kapitolu je Liquid zaujímavý typom Confidential Transactions (dôverné transakcie), ktorý používa Pedersenove záväzky a dôkazy rozsahu na skrytie súm a typov aktív v reťazci a pritom zachováva schopnosť federácie auditovať ponuku. Čo dôverné transakcie neskrývajú, je graf transakcií: odosielatelia a príjemcovia sú viditeľní pre každého vonkajšieho pozorovateľa a celá topológia platieb zostáva verejná. Zisk pre súkromie oproti Bitcoinu na základnej vrstve je len zaslepenie súm a aktív. Liquid podporuje aj emitované aktíva (tokenizované stablecoiny a tokeny cenných papierov), ktorých sumy využívajú rovnaký mechanizmus dôvernosti.

Model dôvery sa podobá na Fedimint: federácia známych subjektov spoločne ovláda peg, ktorýkoľvek člen môže pozorovať graf transakcií a pri operáciách peg-in a peg-out musí spolupracovať prahový počet členov. Súkromie voči vonkajším pozorovateľom je slabšie než pri Fedimint, pretože graf transakcií je verejný, kým tok ecashu vo Fedimint nie je. Federácia sa môže v princípe dohodnúť na zastavení siete alebo na zvrátení transakcií a peg závisí od toho, že federácia dodrží výmenu. Pre prípady použitia, kde stojí dôvernosť súm a rýchlejšie vyrovnanie za dôveru vo federáciu (vydávanie stablecoinov, dôverné vyrovnanie OTC), Liquid funguje nepretržite od roku 2018 bez incidentu. Tam, kde je požiadavkou súkromie celého grafu transakcií alebo minimalizácia dôvery, sú lepšou odpoveďou konštrukcie, ktoré skúmame na iných miestach tejto kapitoly.

Kompromisy dôvery naprieč spektrom úschovy

Vrstva s úschovou tvorí spektrum pozdĺž dvoch osí, ktoré sa nepohybujú v súlade: rozloženie dôvery a súkromie grafu transakcií. Rozloženie dôvery rastie od mixérov s jedným operátorom cez mincovne Cashu s jedným operátorom a konzorcium viacerých členov v Liquide až po federácie strážcov s prahovým podpisom vo Fedimint. Súkromie grafu transakcií nesleduje rovnaké poradie. Mixéry, Cashu aj Fedimint skrývajú tok platieb pred vonkajšími pozorovateľmi: analýza reťazca vidí vklady a výbery do zhluku operátora, ale nie to, kto komu zaplatil vo vnútri. Liquid skrýva sumy, no celý graf transakcií nechá viditeľný v reťazci, takže voči protivníkovi, ktorý analyzuje reťazec, poskytuje slabšie súkromie než Cashu alebo Fedimint, hoci úschovu rozkladá na väčšiu federáciu.

Jednotné naprieč spektrom je chýbajúci jednostranný odchod. Na rozdiel od Lightningu, Ark a Sparku žiadna z týchto konštrukcií neumožňuje používateľovi získať späť prostriedky na základnej vrstve bez súčinnosti operátora. Ak mincovňa alebo federácia prestane fungovať a rezervy sa stratia alebo sa zhabú, tokeny v obehu sa nedajú vymeniť. Sú to peňažné náhrady v Misesovom zmysle. Federované modely znižujú pravdepodobnosť jednostranného zlyhania operátora, ale riziko úschovy je prítomné vo všetkých. Rozumný postup závisí od toho, o aké sumy ide a aké časové horizonty a modely protivníka musí používateľ pokryť: kto sa obáva hlavne sledovania analýzou reťazca, najviac získa z Cashu alebo Fedimint. Pre viditeľný graf transakcií a väčšie konzorcium, ktoré sa dá ľahšie cenzurovať, je Liquid na oboch osiach najslabšou voľbou, aj keď má dôverné sumy.

20.6 Chránená validácia na strane klienta

Presun validácie mimo reťazca

Všetky doteraz skúmané vrstvy majú spoločnú vlastnosť: každý účastník, ktorý transakciu vidí, sa z nej niečo dozvie. Bitcoin na základnej vrstve zverejňuje celú transakciu každému plnému uzlu. CoinJoin a PayJoin zverejňujú transakciu, ktorej vstupy a výstupy sú všetky viditeľné, a súkromie vzniká len z nejednoznačnosti zmiešania. Lightning skrýva aktivitu na úrovni platieb, no zverejňuje otvorenie a zatvorenie kanálov a jeho graf smerovania je verejný z návrhu. Ecash skrýva graf platieb pred vonkajšími pozorovateľmi a konštrukcia podľa Chauma zaslepuje mincovňu v tom, ktorý token bol vydaný komu. Čo odstrániť nevie, je mincovňa samotná: platnosť každého tokenu ecashu v konečnom dôsledku stojí na slepom podpise mincovne, takže mincovňa je povinná protistrana pri každom vydaní a každej výmene. Používateľ nemôže platnosť mince overiť nezávisle

a trvalá spolupráca mincovne a jej solventnosť sú všade nosnými predpokladmi.

Validácia na strane klienta (client-side validation) to obracia. Namiesto toho, aby každý uzol overoval každú transakciu, overuje príjemca transakcie, ktoré k nemu presúvajú mince, a reťazec sa používa len na určenie poradia a na zabránenie dvojitému míňaniu.[20] Myšlienka pochádza z práce Petra Todda z roku 2013 o konsenzuse dôkazu zverejnenia (proof-of--publication) a najplnšie sa rozvinula v jeho práci z roku 2016 o primitívach konsenzu stavového stroja, ktorá priniesla koncepty jednorazových pečatí, deterministických výrazov transakcií a dôkazu zverejnenia ako stavebných kameňov. UTXO v Bitcoine je už samo jednorazová pečať: outpoint pečať identifikuje, skript povoľuje jej uzavretie a minúca transakcia je dôkazom, že bola uzavretá. Protokoly postavené na tomto pozorovaní, najvýraznejšie RGB a Taproot Assets, používajú Bitcoin ako podklad pre záväzky a určenie poradia pre mimoreťazcový stav zmlúv.

Existujúce protokoly validácie na strane klienta zlepšujú súkromie oproti natívnym transakciám na základnej vrstve, ale únik neodstraňujú. V RGB a podobných návrhoch pri prevode mince vidia odosielateľ aj príjemca celú históriu mince, pretože dôkaz, ktorý overuje súčasný stav, je reťazec predchádzajúcich prechodov stavov. Dôkazy mince rastú s dĺžkou histórie transakcií. Stopa v reťazci závisí od toho, ako je záväzok ukotvený. Odporúčaná metóda RGB, Tapret, vkladá záväzok ako úpravu kľúča Taproot: výsledný výstup je nerozlíšiteľný od obyčajného míňania cez Taproot, takže analýza reťazca nedokáže transakcie RGB identifikovať ani zhlukovať len z reťazca. Alternatíva Opret zverejňuje záväzok vo výstupe OP_RETURN, ktorý je viditeľný a dá sa zhlukovať. Pre používateľov Tapret nie je rozhodujúcim obmedzením súkromia viditeľnosť v reťazci, ale odhalenie protistrane: príjemca musí vidieť celý predchádzajúci reťazec prechodov stavov, aby mincu overil, takže každý prevod vyzradí históriu bezprostrednému príjemcovi.

Shielded CSV: validácia na strane klienta s nulovou znalosťou

Chránená validácia na strane klienta (Shielded Client-Side Validation), ktorú v práci z roku 2025 navrhli Jonas Nick, Liam Eagen a Robin Linus, uzatvára obe tieto medzery aplikáciou dôkazov s nulovou znalosťou na validáciu na strane klienta.[21] Konštrukcia používa Proof-Carrying Data, rekurzívnu formu dôkazu s nulovou znalosťou, takže súčasný držiteľ mince nepotrebuje vidieť celú históriu mince, aby overil jej platnosť. Odosielateľ odovzdá príjemcovi stručný dôkaz, že daná minca vznikla platným reťazcom transakcií Shielded CSV, ktorý končí v legitímnom vydaní, a veľkosť dôkazu aj čas overenia nezávisia od dĺžky tohto reťazca.

Na reťazci Bitcoinu sa pri každej transakcii objaví 64 bajtov nepriehľadných údajov, ktoré práca nazýva nullifier a ktoré vyzerajú pseudonáhodne

pre každého, kto nemá zodpovedajúcu potvrdenku. Nullifiery sa zverejňujú ako užitočný obsah aplikačnej vrstvy vo vnútri obyčajných transakcií Bitcoinu. Plný uzol Bitcoinu, ktorý nie je účastníkom Shielded CSV, s týmto obsahom zaobchádza ako so surovými bajtmi: overí nosnú transakciu podľa bežných pravidiel, nullifier sám neoveruje a množina UTXO zostane nezmenená. Obsah čítajú len účastníci Shielded CSV a pre nich sa cena overenia celej dávky nullifierov zredukuje na jediné overenie podpisu Schnorr vďaka konštrukcii polovičnej agregácie NISSHAC z práce. Úloha základného reťazca sa zužuje na určenie poradia a dôkaz zverejnenia. Zabránenie dvojitému míňaniu vynucujú uzly Shielded CSV na strane klienta tak, že vedú úložisko dvojíc kľúč–hodnota s už videnými verejnými kľúčmi nullifierov a každé opakovanie odmietnu.

Vlastnosti súkromia vyplývajú z konštrukcie. Vonkajší pozorovateľ, ktorý sleduje reťazec Bitcoinu, vidí prúd 64-bajtových blobov: sumy, odosielatelia, príjemcovia, prepojenie medzi transakciami aj akákoľvek mimoreťazcová história sú z konštrukcie nepriehľadné. Príjemca overí to, čo potrebuje na prijatie mince, a nedozvie sa nič o tom, čo odosielateľ robil s mincami, ktoré neprevádzal. História, ktorá je v RGB viditeľná pre protistrany, sa pri Shielded CSV stáva neviditeľnou a graf záväzkov, ktorý by analýza reťazca v RGB mohla zhlukovať, sa zredukuje na množinu nullifierov, ktoré zhlukovaniu z konštrukcie odolávajú.

Vyspelosť a miesto v stacku vrstiev

Shielded CSV je výskumný návrh s prototypovou implementáciou, nie nasadený systém. Práca je nedávna, konštrukcia závisí od rekurzívnych dôkazových systémov, ako sú skladacie schémy (folding schemes) alebo rekurzívne STARKy, a tvrdenia o efektivite, ktoré práca uvádza, stoja na ceste k nasadeniu, ktorá zatiaľ neexistuje.

Jeho miesto v stacku vrstiev je však jasné. Lightning zostáva správnou odpoveďou pre interaktívne platby s nízkou latenciou na spodku stacku vrstiev a ecash dnes poskytuje okamžité súkromie typu peňazí na doručiteľa za cenu úschovy. Shielded CSV ukazuje smer, ktorým sa posúva hranica súkromia bez úschovy: k návrhom, v ktorých reťazec nesie záväzky, ktoré nevie prečítať, príjemca overuje dôkazy, ktorých veľkosť nezávisí od histórie, a informácie unikajúce k vonkajším pozorovateľom sa zredukujú na to, čo Bitcoin absolútne potrebuje pre konsenzus. Či sa konkrétne Shielded CSV stane nasadeným štandardom, alebo ho nahradí iný návrh validácie na strane klienta s nulovou znalosťou, architektonický posun je podstatou.

20.7 Porovnávacie kryptomeny so súkromím

Všetky vrstvy súkromia v tejto kapitole majú spoločný východiskový predpoklad: účtovná kniha základnej vrstvy Bitcoinu je daná a súkromie sa k nej

pridáva dodatočne. Dve rodiny alternatívnych kryptomien tento predpoklad odmietajú a súkromie budujú priamo do základnej vrstvy. Hlavnými porovnaniami sú Monero a Zcash. Obe fungujú nepretržite zhruba desať rokov. Ani jedno nenahrádza analýzu Bitcoinu z kapitoly 18 a ani jedno nemení menový argument pre Bitcoin z kapitoly 19. Obe si tu zaslúžia pozornosť, lebo ukazujú, čo súkromie na základnej vrstve prináša a čo stojí. Tretím porovnaním je Ethereum, ktoré nejde ani cestou súkromia na základnej vrstve, ani vrstvenou cestou Bitcoinu: jeho základná vrstva je plne transparentná, no programovateľné prostredie zmlúv vyprodukovalo súbor nadstavieb súkromia na aplikačnej vrstve. Ich architektonická pozícia objasňuje, čo vrstvený model vyžaduje a kde naráža na hranice presadzovania práva.

Konštrukcia Monera

Monero zapisuje tri vlastnosti súkromia priamo do formátu transakcie. Kruhové podpisy skrývajú, ktorý vstup transakcia míňa. Skryté adresy (stealth addresses) skrývajú, ktorý výstup príjemca ovláda. Ring Confidential Transactions skrývajú sumu. Každá vlastnosť je kryptografické primitívum so súborom recenzovanej teórie za sebou a ich kombinácia vytvára účtovnú knihu, na ktorej príležitostný pozorovateľ nevie povedať, kto komu koľko zaplatil.

Kruhový podpis, ktorý v roku 2001 pôvodne navrhli Rivest, Shamir a Tauman, je schéma podpisu, v ktorej podpisovateľ dokáže, že použil súkromný kľúč k jednému z určenej množiny verejných kľúčov, bez toho, aby prezradil, ku ktorému. Monero zostavuje každú míňajúcu transakciu s kruhom návnad (decoys) vybraných z predchádzajúcich výstupov transakcií. Sieť overí, že sa míňa práve jeden výstup z kruhu, a nedozvie sa, ktorý. Množina anonymity je veľkosť kruhu, v súčasnosti šestnásť, čo znamená, že skutočný odosielateľ transakcie je ukrytý medzi šestnástimi kandidátmi z histórie reťazca. Primitívum niečo stojí. Každý kruhový podpis nesie návnady v reťazci a výsledná transakcia je väčšia než transakcia Bitcoinu s porovnateľným významovým obsahom. Réžia úložiska na transakciu je viditeľnou cenou záruky súkromia.

Kruhové podpisy vytvárajú zdanlivý problém: ak nikto nevie, ktorý výstup z kruhu sa míňa, čo bráni tomu, aby sa ten istý výstup minul dvakrát v rôznych transakciách, vždy ukrytý za iným kruhom? Monero to rieši pomocou key images (obrazov kľúča). Každá míňajúca transakcia obsahuje key image, hodnotu odvodenú deterministicky zo súkromného kľúča míňaného výstupu. Odvodenie je navrhnuté tak, že ten istý výstup vždy vytvorí ten istý key image, nech ho v danom kruhu obklopujú akékoľvek návnady. Uzly udržiavajú globálnu množinu zverejnených key images a odmietnu každú transakciu, ktorej key image sa už objavil. Pokus o dvojité míňanie by znovu použil súkromný kľúč skutočného výstupu, vytvoril

by identický key image a bol by okamžite odmietnutý. Kruh sa dá ľubovoľne premiešať, key image je nemenný. Vďaka tejto konštrukcii môže Monero vynucovať jedno míňanie na výstup bez prepojenia key image s konkrétnym členom kruhu, pretože obraz je odvodený zo skutočného kľúča, ale dôkaz kruhového podpisu neprezradí, ktorý člen kruhu ho dodal.

Kruh veľkosti šestnásť je zmysluplným zlepšením oproti transparentnému reťazcu Bitcoinu, no je ohraničený a hranica je malá v porovnaní s konštrukciami s nulovou znalosťou, ktorých množina anonymity sa môže priblížiť celej populácii výstupov. Jediná transakcia s kruhom šestnásť vytvára pre protivníka bez iných informácií neistotu jedna ku šestnástim. Postupnosť transakcií toho istého držiteľa, analyzovaná spoločne, túto neistotu znižuje. Útoky prienikom, pri ktorých protivník pozoruje niekoľko kruhov, ktoré všetky pravdepodobne obsahujú výstupy od toho istého držiteľa, zužujú množinu kandidátov multiplikatívne naprieč postupnosťou. Empirická literatúra o Monere spred RingCT zdokumentovala vystopovateľnosť podstatnej časti míňaní cez analýzu reťazovej reakcie v uzavretej množine: ak kruh obsahuje iba výstupy, o ktorých sa už vie, že boli minuté v iných kruhoch, plus jeden neznámy výstup, neznámy musí byť skutočné míňanie. Dosah tohto útoku na moderné transakcie RingCT je oveľa užší, no základný princíp znamená, že skutočná anonymita kruhu závisí od toho, či neznáme zostanú neznámymi naprieč celým grafom transakcií.

Výber návnad je prevádzková os, ktorá určuje, ako blízko sa skutočná množina anonymity priblíži nominálnym šestnástim. Konkrétnou hrozbou je heuristika prvého míňania: empirické správanie peňaženiek ukazuje, že používatelia zvyčajne míňajú nedávne výstupy, takže protivník, ktorý tipne, že najnovší výstup v kruhu je skutočné míňanie, uspeje podstatne častejšie než pri náhode. Softvér peňaženky Monero tomu čelí tak, že návnady vyberá z predchádzajúcich výstupov podľa rozdelenia gama so zaťažením na staršie výstupy, takže kruhy s nedávnym výstupom obsahujú staršie návnady, ktoré rozmazávajú časový signál. Rozdelenie gama nezatvorí každú medzeru. Návnady vybrané z výstupov, ktoré sa neskôr ukážu ako minuté v iných kruhoch, znižujú skutočnú anonymitu. Protivníci, ktorí svojimi vlastnými transakciami prispievajú veľkou časťou do fondu výstupov v reťazci, ovplyvňujú rozdelenie návnad dostupné ďalším používateľom. A implementácie peňaženiek, ktoré sa odchyľujú od odporúčaného algoritmu výberu, vytvárajú transakcie, ktorých kruhy sa dajú odlíšiť od hlavnej populácie, a preto sa ľahšie analyzujú. Vývojová komunita Monera odpovedala na každé takéto zistenie vylepšeniami výberu návnad na úrovni peňaženky a zväčšovaním kruhu na úrovni hardforkov, ale základné obmedzenie zostáva: šestnásťčlenný kruh nemôže poskytnúť silnejšie súkromie, než dovoľuje predchádzajúca znalosť protivníka o tom, ktorí zo šestnástich členov sú vierohodne minuteľní.

Skrytá adresa (stealth address) je jednorazová adresa, ktorú odosielateľ odvodí z dlhodobej adresy príjemcu. Príjemca zverejňuje jedinú adresu, ale prostriedky dostáva na inú, neprepojiteľnú adresu v reťazci pri každej transakcii. Konštrukcia používa výmenu kľúčov Diffie–Hellman na eliptických krivkách medzi dočasným kľúčom odosielateľa a kľúčom na prezeranie príjemcu, takže iba príjemca môže prehľadávať reťazec a rozpoznať prichádzajúce platby určené jemu. Reťazec neobsahuje žiadnu opakovane použiteľnú kotvu, ktorú by firma na analýzu blockchainu mohla zhlukovať. Skryté adresy porážajú heuristiku opakovaného používania adries štrukturálne.

Ring Confidential Transactions, nasadené v Monere v roku 2017, rozširujú kruhový podpis tak, že popri odosielateľovi skrývajú aj sumu. Konštrukcia používa Pedersenove záväzky na zašifrovanie súm a dôkazy rozsahu (v súčasnosti Bulletproofs a Bulletproofs+) na preukázanie, že každá skrytá suma je nezáporné celé číslo, ktorého súčet vyvažuje vstupy a výstupy transakcie. Bez dôkazov rozsahu by útočník mohol vytvoriť záporné sumy a nafúknuť ponuku, s nimi protokol zachováva ponuku a skrýva hodnoty. Cena tejto konštrukcie na transakciu je podstatná. Typická transakcia v Monere zaberá zhruba desaťkrát toľko bajtov ako míňanie v Bitcoine cez Taproot a jej overenie stojí zhruba o dva rády viac času procesora na rovnakom hardvéri, pretože každý uzol musí skontrolovať kruhový podpis a dôkaz rozsahu pre každý vstup a výstup. Dávkové spracovanie pomáha pri overovaní Bulletproofs v rámci bloku, no nepomáha pri overovaní podpisov Concise Linkable Spontaneous Anonymous Group (CLSAG), ktoré rastie lineárne s veľkosťou kruhu. Cenu platí každý účastník, v každom bloku, navždy.

Dandelion++, nasadený v Monere v roku 2020, rieši útok na sieťovej vrstve opísaný v oddiele 20.1. Protokol šíri novú transakciu cez náhodne zvolený kmeň relayov a až potom ju odvysiela do širšej siete, takže pozorovateľ, ktorý zachytí prvé vysielanie, nedokáže pôvodnú IP adresu určiť tak ľahko ako pri naivnom šírení. Ochrana je pravdepodobnostná a voči protivníkovi s mnohými pozorovacími bodmi obmedzená, no cenu útoku na sieťovej vrstve výrazne zvyšuje.

Kombinovaná architektúra Monera robí zhlukovanie v reťazci oveľa ťažším než na Bitcoine. Vlastnosti platia voči príležitostným protivníkom a protivníkom so strednými zdrojmi. Neplatia voči protivníkovi, ktorý vie korelovať informácie mimo reťazca, napríklad záznam KYC z burzy viazaný na vkladovú adresu, ani voči protivníkovi, ktorý prevádzkuje veľkú časť návnad kruhu ako svoje vlastné predchádzajúce výstupy. Preteky medzi výberom návnad a ich analýzou stále pokračujú.

Pripravovanou odpoveďou na úrovni protokolu sú Full-Chain Membership Proofs (dôkazy členstva v celom reťazci). Návrhy FCMP a FCMP++, ktoré od roku 2023 vyvíja predovšetkým Luke Parker, nahrádzajú kru-

hové podpisy dôkazom s nulovou znalosťou, že míňaný výstup patrí do množiny všetkých minuteľných výstupov v reťazci. Množina anonymity sa rozšíri zo šestnástich na desiatky miliónov, čo je celá populácia výstupov, a závislosť od výberu návnad na úrovni peňaženky zmizne spolu s triedou útokov na výber návnad. Konštrukcia používa stromy kriviek (curve trees) vyjadrené nad cyklom kriviek Helios a Selene na stručný záväzok k množine výstupov a veľkosť dôkazu aj cena overenia zostávajú uskutočniteľné pre peňaženky spotrebiteľskej veľkosti. Hardfork Monera, ktorý umožní FCMP++, sa v čase písania aktívne pripravuje. Po aktivácii to bude najväčšia úprava architektúry súkromia Monera od RingCT a uzavrie konkrétnu triedu útokov, ktoré využívajú ohraničenú veľkosť kruhu.[22]

Vlastnosti súkromia Monera sú pevne zapísané vo formáte transakcie, nie vyjadrené cez programovateľný skript, takže protokol nemá všeobecnú vykonávaciu vrstvu. Prahový multisig existuje, ale je to mimoreťazcový koordinačný protokol medzi spolupodpisovateľmi, nie programovateľná podmienka v reťazci. HTLC, ktoré pri vyrovnaní vyžadujú odhalenie vzoru haša v reťazci, sú s modelom súkromia Monera nezlučiteľné. Atomické výmeny XMR s Bitcoinom sa stavajú na adaptorových podpisoch, ktoré sa konštrukcii s hašovým zámkom úplne vyhýbajú. Časové zámky existujú v obmedzenej podobe ako hrubý mechanizmus podľa výšky bloku, no podmienené časové zámky, aké umožňujú CSV a CLTV v Bitcoine, chýbajú. Verifikátory ZK v reťazci, ľubovoľné zmluvy viacerých strán a továrne platobných kanálov sú úplne mimo návrhového priestoru. FCMP++ rozširuje množinu anonymity na celú populáciu výstupov, ale nič z toho nemení: je to vylepšenie dôkazu míňania, nie vylepšenie skriptovania. Kompromis je zámerný. Pevný formát transakcie vynucuje súkromie jednotne a odstraňuje priestor, cez ktorý by programovateľná vrstva mohla prezrádzať metadáta. Cenou je, že Monero nemôže hostiť platobné kanály druhej vrstvy, schémy s covenantmi ani nadstavby aplikačnej vrstvy, ktoré dávajú vrstvenému modelu Bitcoinu jeho rozšíriteľnosť.

Konštrukcia Zcashu

Zcash ide inou cestou. Jeho účtovná kniha základnej vrstvy podporuje transparentné aj chránené (shielded) transakcie a chránený fond je zabezpečený dôkazmi s nulovou znalosťou. Plne chránená transakcia neodhalí odosielateľa, príjemcu ani sumu, ani žiadne opakovane použiteľné prepojenie s inými transakciami. V reťazci sa objaví len nullifier a nový záväzok a dôkaz sprevádzajúci transakciu potvrdzuje, že míňajúci vlastnil platnú mincu v chránenom fonde a ešte ju neminul. Kryptografickým jadrom je stručný neinteraktívny argument znalosti s nulovou znalosťou (zero-kno-

wledge Succinct Non-Interactive Argument of Knowledge, zk-SNARK), prispôsobený konkrétnemu tvrdeniu, ktoré musí transakcia dokázať.

Protokol prešiel tromi generáciami dôkazových systémov. Pôvodný fond Sprout, spustený v roku 2016, používal konštrukciu SNARK, ktorá vyžadovala ceremóniu dôveryhodného nastavenia (trusted setup), ktorej kompromitácia by umožnila nezistiteľné falšovanie. Sapling, aktivovaný v roku 2018, nahradil konštrukciu efektívnejšou a viedol druhú, viacstrannú ceremóniu na zníženie rizika dôveryhodného nastavenia. Orchard, aktivovaný pri aktualizácii NU5 v roku 2022, používa dôkazový systém Halo 2, ktorý požiadavku na dôveryhodné nastavenie úplne odstraňuje rekurzívnou konštrukciou dôkazu. Prechod cez tieto tri generácie ilustruje dôležitú vlastnosť návrhov so súkromím na základnej vrstve: kryptografické predpoklady nie sú statické. Kryptomena so súkromím musí počítať s výmenou vlastného základného primitíva a prechody musia zachovať hodnotu pre existujúcich držiteľov bez ohrozenia súkromia skorších transakcií.

Model voliteľného chránenia Zcashu má dôsledky, ktoré model Monera nemá. Transparentné transakcie Zcashu sa správajú ako transakcie Bitcoinu a dajú sa zhlukovať rovnakými heuristikami. Chránené transakcie sú voči všetkým týmto heuristikám súkromné. Súkromie majú tí, ktorí používajú chránený fond, a miera využívania chráneného fondu sa v histórii protokolu menila. Keď je väčšina ekonomickej aktivity transparentná, môže protivník aplikovať zhlukovanie na transparentné hrany prevodov z chráneného do transparentného a nepriamo z nich získať informácie o chránenom fonde. Návrhári protokolu presadzovali zmeny v peňaženkách, aby sa chránené transakcie stali predvolenými pre nových používateľov, a tieto zmeny zlepšujú skutočnú množinu anonymity fondu, ale zmiešaná architektúra je štrukturálna vlastnosť, akú by čisto chránený návrh nemal.

Konštrukcia zk-SNARK, vďaka ktorej sú chránené transakcie súkromné, ich robí aj nákladnými v porovnaní s Bitcoinom. Chránené transakcie Sprout boli niekoľkokrát väčšie než porovnateľné transakcie Bitcoinu a ich dokázanie na spotrebiteľskom hardvéri trvalo desiatky sekúnd. Každý uzol v sieti musel pri overovaní každej z nich vynaložiť výrazný výkon procesora. Náklady na overovanie vytvorili útočnú plochu pre odopretie služby. V septembri 2018, krátko pred aktiváciou Saplingu, útočník zaplavil sieť chránenými transakciami Sprout, nafúkol mempool a prinútil uzly vynaložiť neprimeraný výpočet na blok. Útok citeľne spomalil synchronizáciu plných uzlov a odhalil štrukturálnu vlastnosť súkromia založeného na dôkazoch: ten istý výpočet, ktorý potvrdzuje platnosť transakcie, je mechanizmom, ktorým môže útočník vyčerpať zdroje overovateľov. Sapling znížil veľkosť transakcie aj čas dokazovania o viac než rád a pri parametroch Saplingu urobil túto triedu útokov menej životaschopnou, ale

základná dynamika zostáva. Chránená transakcia stojí na overenie viac než transparentná a každý trh s poplatkami, ktorý presne neocení výpočet na overovanie, necháva priestor pre spam, ktorý je lacný na vytvorenie a drahý na overenie. Orchard ďalej znížil cenu overovania a podporuje dávkové overovanie, čím sa rozdiel zužuje, no prirážka za súkromie v šírke pásma a výpočte je trvalou vlastnosťou architektúry.[23]

Architektúra súkromia na Ethereu

Základná vrstva Etherea je plne transparentná. Všetky údaje o transakciách sa zverejňujú v reťazci a indexujú ich prehliadače blokov. Graf adries je rovnako viditeľný ako na Bitcoine a tie isté heuristiky zhlukovania, ktoré firmy na analýzu blockchainu uplatňujú na Bitcoine, platia na Ethereu s rovnakým alebo väčším účinkom, pretože bohatšie interakcie so zmluvami vytvárajú viac prepájacích signálov, nie menej. Štrukturálny dôvod siaha hlbšie než samotná transparentnosť. Bitcoin používa model UTXO: každá prijatá minca je samostatný výstup na konkrétnej adrese a peňaženka môže pre každú prichádzajúcu platbu vygenerovať novú adresu, čím na vrstve peňaženky pretrhne heuristiku opakovaného používania adries. Ethereum používa účtový model: adresa drží priebežný zostatok a každá prichádzajúca platba sa nahromadí na ten istý účet. Zdieľanie adresy Etherea na prijímanie prostriedkov je nevyhnutné, takže každá protistrana, ktorá na ňu posiela, sa dozvie celý zostatok a históriu transakcií viazanú na túto adresu. Prevody tokenov ERC-20 to ešte zhoršujú: každý prevod tokenu z tej istej adresy prepája aktivitu účtu v ETH s jeho aktivitou s tokenmi cez každú zmluvu, ktorú kedy zavolal. Účtový model robí z opakovaného používania adries platobný mechanizmus základnej vrstvy. Skryté adresy podľa EIP-5564 ponúkajú zmiernenie (odosielateľ odvodí jednorazovú adresu z verejného kľúča príjemcu, takže prichádzajúce prostriedky rozpozná len príjemca), no prijatie zostáva okrajové a štruktúra účtov na základnej vrstve sa nemení pre používateľov, ktorí skryté adresy nevytvárajú pre každú prichádzajúcu platbu.

„ZK rollupy“, vďaka ktorým je Ethereum prominentnou témou v diskusiách o dôkazoch s nulovou znalosťou, na tom nič nemenia. ZK rollupy (zkSync Era, StarkNet, Scroll, Polygon zkEVM) používajú kryptografické dôkazy na potvrdenie, že operátor vypočítal prechod stavu správne, a všetky údaje o transakciách zverejňujú na Ethereu ako calldata, aby ktokoľvek mohol zrekonštruovať celú históriu účtov druhej vrstvy. Dôkaz s nulovou znalosťou odpovedá na otázku, či bol výpočet správny, nie na otázku, kto komu zaplatil. Mechanika je rozobraná v kapitole 15 a architektonický bod je tu ten, že ZK rollup poskytuje záruky platnosti na transparentnej účtovnej knihe, nie súkromie na nepriehľadnej. Vonkajší pozorovateľ, ktorý indexuje calldata, pozná každého odosielateľa, príjemcu aj sumu na každom ZK rollupe, ktorý túto architektúru sleduje.

Súkromie na Ethereu je vlastnosť aplikačnej vrstvy, dosahovaná inteligentnými zmluvami, ktoré implementujú chránené fondy. Dva významné nasadené systémy sú Railgun a Aztec. Railgun funguje ako súbor nemenných inteligentných zmlúv na hlavnej sieti Etherea. Prijíma vklady ETH a tokenov ERC-20 do chráneného fondu, kde vnútorné prevody používajú dôkazy s nulovou znalosťou. Pozorovateľ v reťazci vidí tokeny vstupovať do zmlúv Railgun a vystupovať z nich, no vnútorné prevody medzi chránenými adresami viditeľné nie sú a vklady sa nedajú prepojiť s konkrétnymi výbermi. Množina anonymity pre každý token je obmedzená veľkosťou fondu daného tokenu, čo vytvára rovnaký problém slabého fondu ako model voliteľného chránenia Zcashu: súkromie závisí od toho, koľko ďalších používateľov chráni ten istý token. Aztec spustil svoju hlavnú sieť Alpha v marci 2026 ako druhú vrstvu so súkromím ako predvolenou voľbou. Jeho architektúra je bližšia chránenému modelu Zcashu než ZK rollupu: súkromný stav je reprezentovaný zašifrovanými poznámkami v štýle UTXO, súkromné funkcie sa vykonávajú na strane klienta a v reťazci sa objavujú len nullifiery a zašifrované záväzky. Sieť Alpha niesla pri spustení zverejnenú kritickú zraniteľnosť, ktorej oprava bola naplánovaná na neskoršie vydanie. Projekt ju označil za infraštruktúru v ranom štádiu so známymi bezpečnostnými výhradami. Aztec je najbližší analóg chráneného fondu Zcashu na Ethereu, dostupný ako dobrovoľná druhá vrstva nad inak transparentným základom. Výslovné zameranie Railgunu na súlad cez asociačné množiny (association set), podľa rámca, ktorý v práci o Privacy Pools z roku 2023 opísali Vitalik Buterin a spoluautori, odráža prostredie presadzovania práva, ktoré vytvorilo zaradenie Tornado Cash na sankčný zoznam OFAC v roku 2022. Kapitola 13 sa venuje právnemu vývoju a rozsudku vo veci *Van Loon*, ktorý zaradenie protokolu zrušil.[24]

Porovnávacia analýza

Záruky súkromia, ktoré poskytujú Monero a Zcash, sú silné a systémy chránených fondov na Ethereu poskytujú skutočnú neprepojiteľnosť v rámci svojich fondov. Žiadna zo základných konštrukcií v týchto systémoch nebola prelomená. Rozdiel v architektúre, na ktorom záleží, je šírka predpokladov a veľkosť plochy odporu, nielen sila súkromia.

Konsenzus Bitcoinu na základnej vrstve stojí na dobre pochopených primitívach: podpisoch na eliptických krivkách secp256k1, hašovacej funkcii SHA-256 a bezpečnostnom modeli dôkazu práce, ktorý sa na nich zakladá. Vrstvy súkromia nad Bitcoinom pridávajú primitíva postupne. CoinJoin pridáva len koordináciu a nezavádza nijaký nový kryptografický predpoklad. PayJoin pridáva len konkrétny vzor zostavenia transakcie. Lightning pridáva platby HTLC a osobitný tanec s odvolávacími kľúčmi, oboje zostavené zo základných primitív. Ark pridáva mimoreťazcové vTXO s konštrukciou spoločného UTXO a Spark pridáva mimoreťazcové zostat-

ky cez prahové podpisovanie FROST medzi operátormi statechainu, pričom ani jeden nezavádza nový predpoklad konsenzu v reťazci. Ecash podľa Chauma pridáva slepé podpisy, ktoré sa opierajú o rovnaké predpoklady o eliptických krivkách. Chránená validácia na strane klienta zavádza dôkazy s nulovou znalosťou a tie sa opierajú o ďalšie predpoklady.

Monero a Zcash preberajú ťažší kryptografický aparát ako podmienku účasti v protokole vôbec. Každá transakcia v Monere sa opiera o kruhové podpisy, Pedersenove záväzky a dôkazy rozsahu, a keby niektorá z týchto konštrukcií zlyhala, zasiahlo by to každú transakciu. Každá chránená transakcia v Zcashi sa opiera o dôkazový systém zk-SNARK použitý v čase, keď transakcia vznikla, a zlyhanie dôkazového systému by bolo katastrofou. Prechod na Halo 2 toto riziko znížil odstránením predpokladu dôveryhodného nastavenia, no závislosť od širšej konštrukcie SNARK neodstránil.

Argument o asymetrii nákladov, ktorý kniha rozvíja v kapitole 10, preto pre tieto protokoly prebieha inak. Bitcoin drží plochu odporu základnej vrstvy malú a súkromie presúva do skladateľných vyšších vrstiev, kde sú zlyhania ohraničené. Monero a Zcash budujú súkromie do základnej vrstvy a výmenou prijímajú väčšiu plochu odporu. Oba prístupy sú koherentné. Ktorý je presvedčivejší, záleží na tom, či záruka súkromia na úrovni protokolu váži viac než konzervatívnosť množiny predpokladov.

Druhý architektonický rozdiel ovplyvňuje to, čo sa dá na týchto základných vrstvách postaviť. Bitcoin Script podporuje úschovu cez multisig, časové zámky, hašové zámky, HTLC, konštrukciu odvolávacích kľúčov v Lightningu, discreet log contracts a skriptové záväzky, v ktorých pracuje validácia na strane klienta. Formát transakcie v Monere nemá žiadne skriptovanie dostupné používateľovi a skriptovanie Zcashu zostáva užšie než skriptovanie Bitcoinu aj po tom, čo ponúkajú Sapling a Orchard. Táto absencia nie je nedopatrením: výrazovo bohaté podmienky v reťazci odhaľujú štruktúru, ktorú má vrstva súkromia skrývať, a oba protokoly konflikt dôsledne rozhodli v prospech súkromia. Dôsledkom je, že platobné kanály typu Lightning, atomické výmeny medzi reťazcami smerované cez HTLC a escrow bez úschovy, aký Bitcoin podporuje, natívne na Monere ani Zcashi neexistujú. Škálovanie zachovávajúce súkromie na týchto reťazcoch prebieha na základnej vrstve, s už opísanými dôsledkami pre cenu overovania, a nie v skladateľných vyšších vrstvách, ktoré umožňuje obmedzené, ale použiteľné skriptovanie Bitcoinu. Tretím prístupom, odlišným od anonymity na základnej vrstve aj od vrstveného skriptovania Bitcoinu, je model inteligentných zmlúv s nulovou znalosťou, ktorý rozvíja DarkFi Amira Taakiho: každá zmluva je vyjadrená ako obvod ZK a jeho dôkaz sa zverejňuje v reťazci, takže ľubovoľná programovateľná logika beží bez toho, aby vstupy alebo výstupy odhalila niekomu, kto dôkaz overuje. Tento model ponúka súčasne výrazné zmluvy aj súkromie, za cenu oveľa

ťažšej množiny kryptografických predpokladov a implementácie v ranom štádiu, ktorej výkonnostný rámec sa ešte len určuje.[25]

Regulátori a burzy vyraďujú kryptomeny so súkromím z ponuky už väčšinu desaťročia, od prvých japonských stiahnutí po hacku Coincheck v roku 2018 až po každú ďalšiu vlnu presadzovania pravidla Travel Rule a MiCA. Príčina je štrukturálna: súkromie na základnej vrstve je v konflikte s pravidlom Travel Rule aj s okrajom KYC, ktorý odvetvie analýzy blockchainu používa na ukotvenie zhlukov, takže každá burza, ktorá takúto kryptomenu uvedie, zdedí problém s compliance, ktorý je lacnejšie vyriešiť vyradením z ponuky. Bitcoin na základnej vrstve rovnaký konflikt nevyvoláva a súkromie na Bitcoine je výdobytkom vyšších vrstiev postavených okolo kótovanej základnej meny. Rovnaký tlak compliance však Bitcoin zasahuje užším kanálom. Firmy na analýzu blockchainu označujú výstupy z CoinJoinu ako vysoko rizikové a veľké burzy odmietli vklady vysledované k účasti vo Wasabi alebo JoinMarkete. Používatelia, ktorí takéto výstupy dostanú, mali zmrazené účty alebo zadržané prostriedky do preskúmania pôvodu peňazí, takže používatelia Bitcoinu, ktorí využívajú nástroje súkromia na vyšších vrstvách, platia ich cenu pri vstupe do systému a pri výstupe z neho, nie na úrovni protokolu. Rozdiel medzi tromi režimami je architektonický: Monero a Zcash bojujú o to, aby ich základná vrstva bola vôbec kótovaná, Bitcoin bojuje o to, ktoré konštrukcie na vyšších vrstvách prijmú nadväzujúci správcovia úschovy, a aplikačné zmluvy so súkromím na Ethereu zaujímajú strednú pozíciu: podliehajú priamym sankciám na adresy zmlúv, aké nástroje protokolovej vrstvy Bitcoinu dostať nemôžu, ale netrpia tlakom vyraďovania, ktorému čelia kryptomeny so súkromím na základnej vrstve.[26]

20.8 Kvantový horizont pre Bitcoin

Oprávnenia na míňanie v Bitcoine stoja na probléme diskrétneho logaritmu v grupe eliptickej krivky secp256k1. Shorov algoritmus rieši tento problém v polynomiálnom čase na dostatočne výkonnom kvantovom počítači, takže každá minca, ktorej verejný kľúč je viditeľný v reťazci, sa stane minuteľnou pre toho, kto útok spustí ako prvý. Hrozba sa týka konkrétne schémy podpisov: SHA-256 používaný pre dôkaz práce zostáva pri Groverovom kvadratickom zrýchlení náročný a ohrozený nie je. Zraniteľná populácia sa delí na dve skupiny: mince na adresách Pay-to-Public-Key z úplných začiatkov Bitcoinu (malý počet transakcií, ale veľká hodnota, vrátane väčšiny ponuky pripisovanej Satoshimu) a mince na opakovane použitých alebo už minutých adresách Pay-to-Public-Key-Hash, ktorých verejné kľúče sú už v reťazci. Dôveryhodné zverejnené odhady umiestňujú zhruba štvrtinu obiehajúcej ponuky do jednej z týchto kategórií. Mince na adresách, ktoré svoj verejný kľúč nikdy neodhalili, sú v bezpečí až do chvíle míňania a samotné míňanie sa stáva oknom útoku.

Cesta k aktualizácii má dva kroky, každý je samostatný návrh. BIP-360 definuje Pay-to-Merkle-Root, typ výstupu SegWit verzie 2 s adresami `bc1z`. P2MR odstraňuje míňanie cez kľúčovú cestu z Taprootu a ponecháva len cestu cez strom skriptov, čím uzatvára zraniteľnosť pri dlhodobom vystavení: útočník, ktorý získa verejný kľúč zo starého výstupu P2MR, nezíska nič, pretože kľúčová cesta už neexistuje. Druhý návrh, zatiaľ nenapísaný, pridá k stromu skriptov P2MR opkódy postkvantových podpisov, aby uzavrel okno krátkodobého vystavenia pri vysielaní do mempoolu. Ani jeden krok nie je v čase písania aktivovaný. Ťažšia otázka nie je kryptografická, ale politická a ekonomická: čo urobiť so zhruba štvrtinou ponuky, ktorá je už ohrozená. Návrhy siahajú od povinnej migrácie v stanovenej lehote až po trvalú konfiškáciu nepohnutých mincí v okamihu, keď sa kvantový útok stane uskutočniteľným. Každá možnosť rozdeľuje straty medzi držiteľov inak a komunita túto otázku nevyriešila.

Ekonomickou cenou migrácie je veľkosť podpisu a naráža priamo na každú vrstvu nad základnou. Podpis Schnorr má 64 bajtov. FALCON, kompaktná schéma založená na mriežkach, ktorú NIST vybral na pokračujúcu štandardizáciu, vytvára pri 128-bitovej úrovni bezpečnosti 666 bajtov, desaťnásobok podpisu Schnorr. ML-DSA (FIPS 204, dokončený v auguste 2024) má 2 420 až 4 595 bajtov podľa úrovne bezpečnosti. SLH-DSA (FIPS 205, dokončený v auguste 2024), štandardizovaná rodina založená na hašoch, má 7 856 bajtov v najmenšej množine parametrov a takmer 50 000 bajtov v najrýchlejšej. Kudinov a Nick z Blockstream Research v decembri 2025 ukázali, že varianty SPHINCS+ vyladené na požiadavky Bitcoinu, ktoré znižujú počet podpisov na kľúč a uplatňujú optimalizácie SPHINCS+C a PORS+FP, dosahujú citeľne menšie podpisy než štandardizovaný SLH-DSA, a pritom sa opierajú len o predpoklady o hašoch, ktoré už v bezpečnostnom modeli Bitcoinu sú.[27] Blockstream Research zašiel ďalej so SHRINCS, hybridnou schémou, ktorá spája stavovú cestu odvodenú z XMSS (približne 1 092 bajtov pri prvom míňaní, rastúcich s ďalšími míňaniami z toho istého kľúča) s bezstavovou záložnou cestou so 4 396 bajtmi, nasadenou experimentálne na sidechaine Liquid. Smer výskumu je jasný: návrhy založené na hašoch šité na Bitcoin sa približujú k podpisom v nízkych tisíckach bajtov oproti 64 bajtom Schnorra, s cenou overovania dosť blízkou Schnorrovi na to, aby zostala dostupná pre uzly. Každá vrstva súkromia nad základnou túto cenu zdedí. Otvorenie kanála Lightning, vstup do CoinJoinu, oprávnenie v Shielded CSV: každé nesie nový podpis a aritmetika trhu s poplatkami v postkvantovom protokole je otvorená otázka, ktorú musí komunita vyriešiť skôr, než hrozba nastane.[28]

Zhrnutie kapitoly

Základná vrstva Bitcoinu je transparentná z návrhu a okolo opakovaného používania adries, heuristiky spoločného vlastníctva vstupov, odhaľova-

nia zvyšku, pozorovania na sieťovej vrstve a identifikácie zhlukov ukotvenej v KYC vyrástlo sledovacie odvetvie. Súkromie na Bitcoine je architektonický výdobytok postavený nad týmto základom, pričom každá vrstva prináša osobitné kompromisy na dvoch osiach: v reťazci proti mimo reťazca a bez úschovy proti s úschovou. Skriptové primitíva (multisig, časové zámky, hašové zámky, HTLC) umožňujú vrstvenú konštrukciu bez dôveryhodných sprostredkovateľov. CoinJoin a PayJoin zlepšujú súkromie v reťazci bez zmeny pravidiel konsenzu. CoinSwap pretrhne väzbu medzi minutými a prijatými mincami v oddelených, obyčajne vyzerajúcich transakciách bez odtlačku zmiešavania v reťazci. Konštrukcia je dnes na Bitcoine prevažne teoretická a Lightning slúži ako jej mimoreťazcový produkčný analóg. Lightning, Ark a Spark presúvajú platby mimo reťazca a zachovávajú jednostranný odchod, pri rozdielnych nákladoch vo viditeľnosti operátora, správe likvidity a skriptovacích schopnostiach. Vrstvy s úschovou sa vzdávajú jednostranného odchodu výmenou za silnejšie súkromie pozdĺž spektra rastúceho rozloženia dôvery: mixéry skrývajú toky pred vonkajšími pozorovateľmi, ale nie pred operátorom, ecash podľa Chauma (Cashu a Fedimint) zaslepuje operátora kryptograficky za cenu úschovy a federovaný sidechain Liquid rozkladá úschovu na konzorcium, pričom skrýva sumy, ale graf transakcií nechá viditeľný. Chránená validácia na strane klienta posúva hranicu ďalej tým, že zverejňuje len nepriehľadné záväzky, ktoré reťazec nevie prečítať, výmenou za momentálnu vyspelosť na úrovni výskumu.

Monero a Zcash budujú súkromie do základnej vrstvy a výmenou za predvolené súkromie prijímajú väčšiu množinu kryptografických predpokladov a menšiu programovateľnosť. Kruhové podpisy Monera skrývajú skutočný vstup medzi šestnástimi návnadami, key images bránia dvojitému míňaniu bez odhalenia skutočného míňajúceho, skryté adresy lámu zhlukovanie podľa opakovaného používania adries a Ring Confidential Transactions skrývajú sumy za cenu transakcií zhruba desaťkrát väčších ako porovnateľné míňanie v Bitcoine. Útoky na výber návnad zužujú skutočnú množinu anonymity pod šestnásť. FCMP++ nahrádza kruhy dôkazom s nulovou znalosťou nad celou populáciou výstupov, čím triedu útokov úplne odstráni, a hardfork sa pripravuje. Keďže je súkromie pevne zapísané vo formáte transakcie, Monero nemá skriptovanie dostupné používateľovi: kanály typu Lightning, HTLC a schémy s covenantmi tam z návrhu chýbajú. Zk-SNARKy Zcashu chránia spoločne odosielateľa, príjemcu aj sumu cez tri generácie dôkazových systémov (Sprout 2016, Sapling 2018, Orchard s Halo 2 v roku 2022), pričom Halo 2 odstraňuje predpoklad dôveryhodného nastavenia. Model voliteľného chránenia znamená, že transparentné a chránené transakcie existujú vedľa seba: keď je väčšina ekonomickej aktivity transparentná, analýza reťazca môže z okrajov prevodov z chráneného do transparentného získať informácie o chránenom

fonde. Chránené transakcie stoja na overenie viac než transparentné, čo je štrukturálna vlastnosť, ktorá v roku 2018 vytvorila útočnú plochu pre odopretie služby, keď spam Sprout nafúkol mempool. Sapling a Orchard tento rozdiel znížili, no neuzavreli.

Základná vrstva Etherea je rovnako transparentná ako Bitcoinu a jeho účtový model robí z opakovaného používania adries predvolený platobný mechanizmus: každá protistrana, ktorá na adresu posiela, sa dozvie jej celý zostatok a históriu. ZK rollupy zverejňujú všetky údaje o transakciách na Ethereu ako calldata. Dôkaz s nulovou znalosťou potvrdzuje správny výpočet na transparentnej účtovnej knihe, nie súkromie na nepriehľadnej. Súkromie na Ethereu je vlastnosť aplikačnej vrstvy: Railgun implementuje chránené fondy cez nemenné inteligentné zmluvy na hlavnej sieti a Aztec v marci 2026 spustil hlavnú sieť Alpha so súkromím ako predvolenou voľbou, so zverejnenou kritickou zraniteľnosťou a opravou plánovanou na neskoršie vydanie. Obe čelia osobitnému kanálu presadzovania: OFAC v roku 2022 zaradil na sankčný zoznam priamo adresy zmlúv Tornado Cash, čo je forma tlaku štrukturálne nedostupná voči protokolom súkromia Bitcoinu, ktoré iba koordinujú. Desaťročie regulačných vĺn (Japonsko 2018, Bittrex 2021, vlna okolo MiCA v rokoch 2023–2024) viedlo k postupnému vyraďovaniu kryptomien so súkromím z ponuky, pretože súkromie na základnej vrstve je na úrovni protokolu v konflikte s pravidlom Travel Rule. Tlak compliance dosahuje súkromie na Bitcoine užším kanálom: firmy na analýzu blockchainu označujú výstupy z CoinJoinu ako vysoko rizikové a viaceré burzy odmietli vklady vysledované k Wasabi alebo JoinMarketu, takže používatelia nástrojov súkromia na vyšších vrstvách platia ich cenu pri vstupe do systému a pri výstupe z neho.

Postkvantový horizont ohraničuje každú vrstvu nad podpisovou schémou Bitcoinu. Shorov algoritmus láme secp256k1 na dostatočnom kvantovom počítači. Typ výstupu Pay-to-Merkle-Root z BIP-360 odstraňuje míňanie cez kľúčovú cestu z Taprootu ako prvý krok k migrácii a postkvantové opkódy podpisov majú nasledovať. ML-DSA (FIPS 204) má 2 420 až 4 595 bajtov na podpis podľa úrovne bezpečnosti, SLH-DSA (FIPS 205) má 7 856 až 49 856 bajtov naprieč množinami parametrov, kde malé a rýchle varianty sa líšia kompromisom medzi veľkosťou a rýchlosťou a FALCON, ktorého štandardizácia FIPS bola v čase písania ešte rozpracovaná, má približne 666 až 1 280 bajtov. Kudinov a Nick (2025) ukazujú, že varianty SPHINCS+ optimalizované pre Bitcoin dosahujú citeľné zmenšenie oproti štandardizovanému SLH-DSA a zachovávajú predpoklady zabezpečenia len na hašoch. Každé číslo sa porovnáva s 64 bajtmi Schnorra, takže prechod vyvíja tlak na poplatky naprieč každou vrstvou súkromia, ktorá nesie oprávnenie na míňanie. Žiadna jediná vrstva neposkytuje úplné finančné súkromie: každý nástroj rieši konkrétne problémy s metadátami a iné necháva nevyriešené, a prevádzková disciplína naprieč vrstvami,

ktorú skúma kapitola 22, zostáva nevyhnutná. Základy anonymnej komunikácie pod týmito menovými vrstvami (VPN, Tor, mixnety) patria do kapitoly 17.

Poznámky

[1] Praktické nástroje pre čitateľov, ktorí chcú použiť to, čo kapitola opisuje: Sparrow Wallet (sparrowwallet.com) je najlepšia desktopová peňaženka Bitcoinu pre kontrolu nad mincami, poriadok v označeniach a integráciu PayJoin/CoinJoin. JoinMarket (github.com/JoinMarket-Org/joinmarket-clientserver) zostáva aktívne udržiavanou implementáciou CoinJoinu. Wasabi Wallet (wasabiwallet.io) dodáva CoinJoiny v štýle WabiSabi. Mempool.space, OXT (oxt.me) a KYCP (kycp.org) zobrazujú tú istú analytiku, akú používajú firmy na analýzu blockchainu, čo je užitočné na to, aby sa človek naučil, ako jeho transakcie vyzerajú v ich očiach. Pre vlastnú úschovu na Lightningu dodávajú mobilných klientov s rôznymi profilmi dôvery Phoenix (phoenix.acinq.co), Zeus (zeusln.com) a Breez (breez.technology). Hlavnými implementáciami uzla sú Core Lightning (corelightning.org) a LND (lightning.engineering). Na čítanie: stránka „Privacy“ na Bitcoin Wiki (en.bitcoin.it/wiki/Privacy) je najlepšie udržiavaný encyklopedický zdroj, udržiavaný praktikmi. Andy Greenberg, *Tracers in the Dark* (2022) je smerodajný novinársky opis sledovacieho odvetvia, ktoré kapitola popisuje. Bitcoin Optech (bitcoinops.org) publikuje najlepšie priebežné spravodajstvo o vývoji na úrovni protokolu. Pre Monero ako referenčný alternatívny návrh súkromia stojí za prečítanie správy Monero Research Lab od Saranga Noethera a Brandona Goodella (github.com/monero-project/research-lab).

[2] Pieter Wuille, ”BIP32: Hierarchical Deterministic Wallets” (2012); Marek Palatinus a Pavol Rusnák, ”BIP44: Multi-Account Hierarchy for Deterministic Wallets” (2014); BIP84 a BIP86 rozširujú schému pre výstupy SegWit a Taproot. Praktický prehľad vzorov opakovaného používania a ich rozšírenia pozri Bitcoin Wiki, ”Address reuse,” `https://en.bitcoin.it/wiki/Address_reuse`.

[3] Sarah Meiklejohn, Marjori Pomarole, Grant Jordan, Kirill Levchenko, Damon McCoy, Geoffrey M. Voelker a Stefan Savage, ”A Fistful of Bitcoins: Characterizing Payments Among Men with No Names,” *ACM Internet Measurement Conference* (2013). Heuristika sa spomína aj v Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System* (2008), oddiel 10. K neskoršiemu dôkazu, že opakované používanie spolu so spoločným míňaním vytvára „super-zhluky“ prepájajúce mnohé identity, pozri Martin Harrigan a Christoph Fretter, ”The Unreasonable Effectiveness of Address Clustering,” arXiv:1605.06369 (2016).

[4] Heuristiky zvyšku opísané tu sú zaradené na Bitcoin Wiki, ”Privacy,” `https://en.bitcoin.it/wiki/Privacy`, a čerpajú z Meiklejohn a kol. (2013), Elli Androulaki a kol., ”Evaluating User Privacy in Bitcoin,” *Financial Cryptography* (2013), a Jonas Nick, ”Data-Driven De-Anonymization in Bitcoin,” diplomová práca (MSc), ETH Zürich (2015). Praktický výklad odtlačkov peňaženiek pozri v priebežnej práci 0xB10C na `https://transactionfee.info`.

[5] 0xB10C, ”LinkingLion: An Entity Linking Bitcoin Transactions to IPs?”, príspevok s pozorovaniami, `https://b10c.me/` (2023), s doplnením v roku 2024. K staršej akademickej práci o deanonymizácii na sieťovej vrstve pozri Alex Biryukov, Dmitry Khovratovich a Ivan Pustogarov, ”Deanonymisation of Clients in Bitcoin P2P Network,” *ACM CCS* (2014); a Philip Koshy, Diana Koshy a Patrick McDaniel, ”An Analysis of Anonymity in Bitcoin Using P2P Network Traffic,” *Financial Cryptography* (2014). K Dandelion++: Giulia Fanti a kol., ”Dandelion++: Lightweight Cryptocurrency Networking with Formal Anonymity Guarantees,” *SIGMETRICS* (2018).

[6] Pre prevádzku peňaženky s plným uzlom je referenčnou implementáciou Bitcoin Core na `https://bitcoincore.org/`. Súčasná stopa úložiska je približne 700 GB s ročným prírastkom ~80–100 GB a úvodnou synchronizáciou 6–24 hodín na bežnom SSD. Kanonický sprievodca vlastným hostingom je zbierka zdrojov Jamesona Loppa na `https://github.com/jlopp/civil-disobedience`. Sparrow Wallet (`https://sparrowwallet.com/`) a Specter Desktop (`https://specter.solutions/`) sú dve najbežnejšie desktopové peňaženky, ktoré sa pripájajú k lokálnemu uzlu Bitcoin Core. K všeobecnej architektúre pozri stránku „Privacy" na Bitcoin Wiki, `https://en.bitcoin.it/wiki/Privacy`, najmä §4.3 a §5.3 o získavaní histórie peňaženky.

[7] BIP 157 (Olaoluwa Osuntokun, Alex Akselrod a Jim Posen) a BIP 158 (Olaoluwa Osuntokun a Alex Akselrod), "Client Side Block Filtering" (2017), `https://github.com/bitcoin/bips/blob/master/bip-0157.mediawiki` a `https://github.com/bitcoin/bips/blob/master/bip-0158.mediawiki`. BIP 37 (Mike Hearn a Matt Corallo), "Connection Bloom filtering" (2012), `https://github.com/bitcoin/bips/blob/master/bip-0037.mediawiki`, v predvolenom nastavení vypnutý v Bitcoin Core cez PR #16152 Matta Corallo (zlúčený 2019-07-19, súčasť vydania 0.19.0). Kritika súkromia, ktorá túto zmenu motivovala: Arthur Gervais, Ghassan O. Karame, Damian Gruber a Srdjan Capkun, "On the Privacy Provisions of Bloom Filters in Lightweight Bitcoin Clients," *ACSAC '14* (2014), `https://eprint.iacr.org/2014/763`; Jonas Nick, "Privacy in BitcoinJ" (12. február 2015), `https://jonasnick.github.io/blog/2015/02/12/privacy-in-bitcoinj/`, útok empiricky potvrdzuje. Bitcoin Development Kit (BDK) sprístupňuje primitíva filtrov BIP 157/158 vývojárom peňaženiek na `https://bitcoindevkit.org/` a index filtrov podporujú na strane servera `btcd` (`https://github.com/btcsuite/btcd`) a dobrovoľný `blockfilterindex` v Bitcoin Core. Wasabi Wallet (`https://wasabiwallet.io/`) ako prvá zaviedla filtrovanie na strane klienta v spotrebiteľskej peňaženke s Wasabi 1.0 (august 2018), a to so špecifickým filtrom Wasabi poskytovaným z vlastného backendu. Wasabi 2.6.0 (máj 2025) pridala podporu štandardných filtrov BIP 158 a priameho pripojenia k uzlu Bitcoin Core, poznámky k vydaniu na `https://github.com/WalletWasabi/WalletWasabi/releases/tag/v2.6.0`. Pre servery protokolu Electrum na vlastné nasadenie sú tri štandardné implementácie ElectrumX (`https://github.com/spesmilo/electrumx`), electrs (Roman Zeyde, `https://github.com/romanz/electrs`) a Fulcrum (Calin Culianu, `https://github.com/cculianu/Fulcrum`).

[8] Špecifikácia Stratum V2 na `https://stratumprotocol.org/`, s transportom šifrovaným rámcom Noise a voliteľným rozšírením Job Declaration zdokumentovanými v základnej špecifikácii. Produkčné nasadenia Stratum V2: Braiins Pool (`https://braiins.com/pool`), DEMAND Pool (`https://dmnd.work/`), Public Pool (`https://web.public-pool.io/`). Referenčná implementácia na `https://github.com/stratum-mining/stratum`. OCEAN Pool prevádzkuje namiesto Stratum V2 paralelný protokol DATUM (Decentralized Alternative Templates for Universal Mining), špecifikácia DATUM na `https://ocean.xyz/docs/datum` a zdrojový kód na `https://github.com/OCEAN-xyz/datum_gateway`. K súkromiu vysielania transakcií Bitcoinu cez nový okruh Tor pri každom vysielaní pozri dokumentáciu Wasabi Wallet na `https://docs.wasabiwallet.io/` a `-onlynet=onion` v Bitcoin Core spolu s izoláciou okruhu pre každého peera, ako je opísaná v poznámkach ku konfigurácii Tor na `https://github.com/bitcoin/bitcoin/blob/master/doc/tor.md`. K analýze odopretia služby pri Dandelion++, ktorá držala návrh mimo Bitcoin Core, pozri

diskusiu k PR v Bitcoin Core o pôvodnom návrhu Dandelion++, uvedenú na https://github.com/bitcoin/bitcoin/issues/10054.

[9] Gregory Maxwell, "CoinJoin: Bitcoin Privacy for the Real World," príspevok na Bitcoin Forum (2013). K WabiSabi pozri Yuval Kogman, Max Hillebrand, Alex Wied a Aviv Zohar, "WabiSabi: Centrally Coordinated CoinJoins with Variable Amounts," IACR ePrint 2021/206, https://eprint.iacr.org/2021/206; poznámky k protokolu WabiSabi na https://github.com/WalletWasabi/WabiSabi/blob/master/protocol.md; a Bitcoin Optech Newsletter #102, "WabiSabi coordinated coinjoins with arbitrary output values," https://bitcoinops.org/en/newsletters/2020/06/17/#wabisabi-coordinated-coinjoins-with-arbitrary-output-values.

[10] Heuristiku zbytočného vstupu aplikovali konkrétne na odhaľovanie PayJoin a P2EP Adam Gibson (waxwing) a LaurentMT v decembri 2018 v GitHub gist, ktorý definoval varianty UIH1 a UIH2 a poskytol prvý empirický základ voči histórii hlavnej siete; pozri https://gist.github.com/AdamISZ/4551b947789d3216bacfcb7af25e029e. Neskoršie spresnenie do tvaru súčtu podmnožín sa objavilo v tom istom vlákne a bolo začlenené do implementácie PayJoin v BTCPay cez https://github.com/btcpayserver/btcpayserver/pull/4600. Akademické spracovanie je Simin Ghesmati, Walid Fdhila a Edgar Weippl, "Unnecessary Input Heuristics & PayJoin Transactions," IACR Cryptology ePrint Archive, Paper 2022/589 (2022), https://eprint.iacr.org/2022/589. Všeobecná myšlienka zbytočného vstupu je staršia a je zhromaždená v článku "Privacy" Chrisa Belchera na Bitcoin Wiki, https://en.bitcoin.it/wiki/Privacy, medzi heuristikami odhaľovania zvyšku. Vlastné spracovanie dotknutých heuristík, zmiešaných typov vstupov a obrany proti odtlačkom v BIP 78 je Nicolas Dorier, "BIP 78: A Simple Payjoin Proposal," https://github.com/bitcoin/bips/blob/master/bip-0078.mediawiki.

[11] BIP 77 („Async Payjoin") je Dan Gould a Yuval Kogman, https://github.com/bitcoin/bips/blob/master/bip-0077.md, prvýkrát zlúčený ako návrh v máji 2025. Referenčná implementácia je na https://github.com/payjoin/rust-payjoin, súčasť OHTTP relay na https://github.com/payjoin/ohttp-relay a produkčné nasadenie adresára na https://payjo.in/. Stav prijatia v čase písania sleduje zostavený zoznam na https://en.bitcoin.it/wiki/PayJoin_adoption: BTCPay Server, JoinMarket, Bull Bitcoin Mobile a Cake Wallet dodávajú podporu odosielateľa aj príjemcu, Wasabi, Sparrow, BlueWallet, Mutiny a Sideshift len odosielanie, Bitcoin Core nemá natívnu integráciu (sledovací issue na https://github.com/bitcoin/bitcoin/issues/19148). Vlastné tvrdenie v časti motivácie BIP 77, že "BIP 78's requirements for Payjoin Version 1 have proven to be an obstacle to adoption," je najpriamejším primárnym uznaním infraštruktúrnej prekážky verzie 1.

[12] Joseph Poon a Thaddeus Dryja, "The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments" (2016).

[13] K obmedzeniam súkromia na Lightningu pozri Sergei Tikhomirov a kol., "An Empirical Analysis of Privacy in the Lightning Network," *Financial Cryptography* (2021); Nishanth Chandran a kol., "On the Difficulty of Hiding the Balance of Lightning Network Channels," *IACR ePrint* (2019). Praktický výklad analýzy smerovania, CoinJoinov kanálov, zakrytých ciest a trampolínového smerovania ako vylepšení súkromia na Lightningu pozri ben Carman, Evan Kaloudis, Max Hillebrand, Paul Miller a Tony Giorgio, "Lightning Privacy Research," dostupné na https://lightningprivacy.com a na https://github.com/BitcoinDevShop/lightning-privacy-research.

[14] Matteo Romiti a kol., "Cross-Layer Deanonymization Methods in the Lightning Protocol," *Financial Cryptography* (2021). Výskum ukázal heuristiky zhlukovania, ktoré prepájajú uzly Lightningu s adresami Bitcoinu cez spoločné pomenovanie, informácie o hostingu a interakcie v reťazci.

[15] Burak Keçeli, "Ark: A Privacy-Preserving Layer 2 for Bitcoin" (2023), špecifikácia na `https://arkdev.info/`, s ďalšou dokumentáciou na `https://ark-protocol.org/`. Arkade (`https://arkadeos.com/`) je hlavná produkčná implementácia, ktorú prevádzkuje Ark Labs, jej stack je na `https://github.com/arkade-os`. Second (`https://second.tech/`) je druhá produkčná implementácia, ktorá prevádzkuje server Ark na hlavnej sieti Bitcoinu s paralelným nasadením na signete, jej implementácia peňaženky (bark) je na `https://gitlab.com/ark-bitcoin/bark`. Na porovnanie s modelom likvidity Lightningu, ktorý konštrukcia rieši, pozri Bastien Teinturier, "Ark and the Future of Bitcoin L2s," spravodajstvo v newsletteri *Bitcoin Optech*, 2023–2025, na `https://bitcoinops.org/`.

[16] David Chaum, "Blind Signatures for Untraceable Payments," *Advances in Cryptology: CRYPTO '82* (1983): 199-203. K formulácii problému, ktorý tento oddiel rieši, od Hala Finneyho pozri "Digital Cash & Privacy" (1993), `https://nakamotoinstitute.org/library/digital-cash-and-privacy/`, ktorý tvrdí, že elektronické platby vytvárajú dosje transakcií, pokiaľ sa míňanie neoddelí od záznamov na úrovni účtov. Finneyho "Protecting Privacy with Electronic Cash" (1993), `https://nakamotoinstitute.org/library/protecting-privacy-with-electronic-cash/`, podáva najjasnejší dobový prehľad trojvrstvového stacku: kryptografia s verejným kľúčom, anonymné správy a ecash.

[17] K Cashu pozri `https://cashu.space/`.

[18] K Fedimint pozri `https://fedimint.org/`.

[19] Adam Back, Matt Corallo, Luke Dashjr, Mark Friedenbach, Gregory Maxwell, Andrew Miller, Andrew Poelstra, Jorge Timón a Pieter Wuille, "Enabling Blockchain Innovations with Pegged Sidechains" (2014), `https://blockstream.com/sidechains.pdf`, je zakladajúci dokument o Liquide. Dokumentácia siete Liquid na `https://liquid.net/`, s konštrukciou dôverných transakcií zdokumentovanou na `https://docs.liquid.net/docs/confidential-transactions-how-to` a v Andrew Poelstra, "Confidential Assets" (2017), `https://blockstream.com/bitcoin17-final41.pdf`. Členstvo a správa federácie Liquid sú opísané na `https://liquid.net/about/`; Elements, open source kódová základňa, je na `https://github.com/ElementsProject/elements`.

[20] Peter Todd, "Building Blocks of the State Machine Approach to Consensus" (2016), dostupné na `https://petertodd.org/2016/state-machine-consensus-building-blocks`. Skorší návrh sa objavuje v príspevku Todda z novembra 2013 v e-mailovej konferencii bitcoin-dev o konsenzuse dôkazu zverejnenia. K nasadeniu tohto prístupu v protokole RGB pozri špecifikácie LNP/BP Standards Association na `https://rgb.tech`.

[21] Jonas Nick, Liam Eagen a Robin Linus, "Shielded CSV: Private and Efficient Client-Side Validation," IACR Cryptology ePrint Archive, Paper 2025/068 (január 2025), dostupné na `https://eprint.iacr.org/2025/068`. Prototypová implementácia na `https://github.com/ShieldedCSV/ShieldedCSV`.

[22] Monero zapisuje tri primitíva súkromia na základnej vrstve: kruhové podpisy (Rivest-Shamir-Tauman 2001), skryté adresy a Ring Confidential Transactions s dôkazmi rozsahu Bulletproofs. Šestnásťčlenný kruh je ohraničená množina anonymity, ktorú útoky na výber návnad využívajú a ktorú majú Full-Chain Membership Proofs (FCMP++)

nahradiť anonymitou v rámci celého reťazca. Projekt Monero, https://www.getmonero.org/. Zdrojový kód na https://github.com/monero-project/monero. Technické správy Monero Research Lab, https://github.com/monero-project/research-lab. Pôvodné kruhové podpisy: Ronald L. Rivest, Adi Shamir a Yael Tauman, "How to Leak a Secret," *ASIACRYPT 2001*. RingCT: Shen Noether, "Ring Confidential Transactions," IACR ePrint 2015/1098 (2015). Bulletproofs: Benedikt Bünz, Jonathan Bootle, Dan Boneh a kol., "Bulletproofs: Short Proofs for Confidential Transactions and More," *IEEE Symposium on Security and Privacy* (2018). Bulletproofs+: Heewon Chung, Kyoohyung Han, Chanyang Ju a kol., "Bulletproofs+: Shorter Proofs for Privacy-Enhanced Distributed Ledger," IACR ePrint 2020/735. Dandelion++: Giulia Fanti, Shaileshh Bojja Venkatakrishnan a kol., "Dandelion++: Lightweight Cryptocurrency Networking with Formal Anonymity Guarantees," *ACM SIGMETRICS* (2018). K empirickej vystopovateľnosti Monera spred RingCT a útoku reťazovej reakcie v uzavretej množine ostávajú štandardnými zdrojmi Malte Möser, Kyle Soska, Ethan Heilman a kol., "An Empirical Analysis of Traceability in the Monero Blockchain," *Proceedings on Privacy Enhancing Technologies* 2018, č. 3 (2018): 143–163, a Andrew Miller, Malte Möser, Kevin Lee a Arvind Narayanan, "An Empirical Analysis of Linkability in the Monero Blockchain," IACR ePrint 2017/338. K analýzam výberu návnad a odpovediam na úrovni peňaženiek pozri prehľadovú prácu Justina Ehrenhofera a bulletiny Monero Research Lab na https://www.getmonero.org/resources/research-lab/. K Full-Chain Membership Proofs pozri Luke Parker (kayabaNerve), "FCMP++: Full-Chain Membership Proofs for Monero" (2024), https://www.getmonero.org/2024/04/27/fcmps.html, so špecifikáciou a implementáciou na https://github.com/kayabaNerve/fcmp-plus-plus. K porovnaniu veľkosti transakcií a priepustnosti pozri bulletiny „Empirical Results" Monero Research Lab a širšiu porovnávaciu analýzu v Harry Halpin a Ania Piotrowska, "Forensic Analysis of Privacy Coins" (2020), ako aj priebežné štatistiky na blok na https://moneroblocks.info/ a https://mempool.space/ pre bitcoinový náprotivok.

[23] K porovnaniu veľkosti transakcií a ceny overovania v Zcashi a k spamovému útoku na Sprout zo septembra 2018: útok je zdokumentovaný v retrospektívach Electric Coin Company a na fórach komunity Zcash zo septembra až októbra 2018; nafúknutý mempool a spomalenie uzlov sa spomínajú v komunikácii ECC k spusteniu Saplingu ako súčasť dôvodov na prepracovanie dôkazového systému v Sapling. K zlepšeniam efektivity Saplingu oproti Sprout pozri Sean Bowe, Jack Grigg, Ian Miers a kol., "Sapling," technická špecifikácia Electric Coin Company (2018), https://github.com/zcash/sapling-spec, a špecifikáciu protokolu Sapling na https://zips.z.cash/protocol/sapling.pdf. K dávkovému overovaniu v Orchard pozri špecifikáciu protokolu Zcash na https://zips.z.cash/protocol/protocol.pdf §5.4.

[24] K architektúre súkromia na Ethereu: dokumentácia protokolu Railgun na https://railgun.org/; inteligentné zmluvy Railgun na https://github.com/Railgun-Community/. Dokumentácia siete Aztec na https://docs.aztec.network/; zdrojový kód Aztec na https://github.com/AztecProtocol/aztec-packages. Aztec spustil svoju hlavnú sieť Alpha 31. marca 2026, oznámenie o spustení je na https://aztec.network/blog/announcing-the-alpha-network. Kritická zraniteľnosť v dokazovacom systéme Alpha v4 bola zverejnená 27. marca 2026, s opravou plánovanou vo vydaní v5 v júli 2026; pozri https://aztec.network/blog/critical-vulnerability-in-alpha-v4. Predchodca produktu Aztec, Aztec Connect, prestal prijímať vklady 21. marca 2023 a jeho sequencer sa vypol 31. marca 2024; všetok kód je open source. K rozdielu medzi platnosťou a súkromím pri ZK rollupoch dokumentácia ethereum.org o ZK rollupoch

výslovne uvádza, že rollupy zverejňujú na Ethereu údaje o stave pre každú transakciu spracovanú mimo reťazca, čo umožňuje nezávislú rekonštrukciu stavu rollupu; pozri https://ethereum.org/en/developers/docs/scaling/zk-rollups/. K Tornado Cash: U.S. Department of Treasury, zaradenie Tornado Cash úradom OFAC, 8. august 2022, https://home.treasury.gov/news/press-releases/jy0916. Alexey Pertsev odsúdený v Holandsku, máj 2024. K Privacy Pools: Vitalik Buterin, Jacob Illum, Matthias Nadler, Fabian Schär a Ameen Soleimani, "Blockchain Privacy and Regulatory Compliance: Towards a Practical Equilibrium," SSRN 4563364 (2023), https://ssrn.com/abstract=4563364.

[25] DarkFi je platforma inteligentných zmlúv s nulovou znalosťou od Amira Taakiho. Každá zmluva sa skompiluje do obvodu s nulovou znalosťou a transakcie nesú dôkazy namiesto čitateľných vstupných a výstupných údajov, takže ľubovoľná programovateľná logika sa vykonáva pod šifrovaním. Stránka projektu a dokumentácia na https://dark.fi/. Zdrojový kód na https://codeberg.org/darkrenaissance/darkfi. K širšej Taakiho práci v cypherpunkovej tradícii pozri Carl Miller, "The Death of the Gods: The New Global Power Grab" (Windmill Books, 2018), kap. 8, a rozhovory zhromaždené na https://agorism.dev/.

[26] Zcash uplatňuje zk-SNARKy na chránené transakcie naprieč tromi generáciami dôkazových systémov (Sprout 2016, Sapling 2018, Orchard/Halo 2 2022). Vyraďovanie kryptomien so súkromím z búrz siaha k tlaku japonského FSA v roku 2018, pokračovalo americkým vyradením Bittrexu v januári 2021 a zrýchlilo sa v rokoch 2023–2024, keď sa formovala MiCA. Monero aj Zcash nemajú skriptovanie na základnej vrstve, ktoré umožňuje stack druhej vrstvy Bitcoinu postavený na Lightningu a HTLC. Projekt Zcash, https://z.cash/. Electric Coin Company, https://z.cash/. Špecifikácia protokolu Zcash na https://zips.z.cash/protocol/protocol.pdf. K aktualizácii NU5 a Halo 2 pozri https://z.cash/blog/explaining-halo-2/. Článok o Halo 2: Sean Bowe, Jack Grigg a Daira Hopwood, "Recursive Proof Composition without a Trusted Setup," IACR ePrint 2019/1021. K ceremóniám dôveryhodného nastavenia pozri Matthew Green, "Zcash Counterfeiting Vulnerability Successfully Remediated" (2019), https://z.cash/blog/zcash-counterfeiting-vulnerability-successfully-remediated/. K porovnaniu skriptovania pozri prehľad skriptových primitív Bitcoinu od Jamesona Loppa na https://www.lopp.net/bitcoin-information.html a špecifikácie protokolov Monera a Zcashu uvedené vyššie. Akademické zarámovanie kompromisu medzi súkromím a programovateľnosťou pozri Andrew Poelstra, "Confidential Assets" (2017), https://blockstream.com/bitcoin17-final41.pdf, ktorý analyzuje štrukturálny konflikt. K histórii vyraďovania kryptomien so súkromím z búrz: tlak japonského FSA v roku 2018 a reakcia Coincheck sú pokryté v spravodajstve *Reuters* z júna až septembra 2018; prechod ShapeShift na KYC v roku 2018 a súvisiace vyradenia na https://shapeshift.com/; oznámenie Bittrexu o vyradení v USA (január 2021) na https://bittrex.zendesk.com/; vyradenie Monera na Krakene v EHP (účinné od februára 2024) na https://support.kraken.com/; oznámenie Binance o vyradení Monera (február 2024) na https://www.binance.com/en/support/announcement/; vyraďovanie kryptomien so súkromím na OKX (koniec 2023 až začiatok 2024) sledované v spravodajstve *CoinDesk* a *The Block* na https://www.coindesk.com/ a https://www.theblock.co/. K vzťahu pravidla Travel Rule ku kryptomenám so súkromím pozri usmernenie FATF k odporúčaniu 16 na https://www.fatf-gafi.org/.

[27] Mikhail Kudinov a Jonas Nick, "Hash-based Signature Schemes for Bitcoin," IACR Cryptology ePrint Archive, Paper 2025/2203 (december 2025),

https://eprint.iacr.org/2025/2203. Práca tvrdí, že podpisové schémy založené na hašoch sú pre Bitcoin vhodnejšie než schémy založené na mriežkach (ML-DSA), pretože ich bezpečnosť sa opiera výlučne o predpoklady o hašovacích funkciách, ktoré už sú v návrhu Bitcoinu prítomné. Uplatňuje nedávne optimalizácie (SPHINCS+C, TL-WOTS-TW a PORS+FP) a vytvára varianty s podstatne menšími podpismi než štandardizovaný SLH-DSA a analyzuje obmedzenia špecifické pre Bitcoin vrátane odvodzovania kľúčov, viacnásobných podpisov a prahových podpisov. Kudinov pôsobí v Blockstream Research, Nick je vývojár protokolu Bitcoinu tiež v Blockstream Research a spoluautor práce na MuSig2 a BIP-327. K schéme SHRINCS: implementácia v C++ na https://github.com/BlockstreamResearch/shrincs-cpp; overovač Simplicity na https://github.com/BlockstreamResearch/shrincs-simplicity-verifier; špecifikácia na https://github.com/BlockstreamResearch/shrincs-specification; skripty na skúmanie parametrov na https://github.com/BlockstreamResearch/SPHINCS-Parameters. Uvádzané výkonnostné čísla (1 092 bajtov stavová verzia pri q=1, 4 396 bajtov bezstavová) pochádzajú zo správy o výkone SHRINCS-L na Liquide v repozitári shrincs-cpp, merané na Intel Core i5 so 16 GB RAM; živé transakcie na Liquide sú v tejto správe odkazované.

[29] Chainalysis, založená 2014, https://www.chainalysis.com/. Elliptic, založená 2013, https://www.elliptic.co/. TRM Labs, založená 2018, https://www.trmlabs.com/. CipherTrace od Mastercardu, ktorú Mastercard získal v roku 2021, https://ciphertrace.com/. Každý dodávateľ udržiava vlastnú databázu označených adries zostavenú z partnerstiev s burzami, súdnych príkazov, zberu vkladových adries a spravodajstva z otvorených zdrojov. Komerčné zmluvy, ktorými údaje KYC z búrz plynú k týmto dodávateľom, vo všeobecnosti nie sú verejné. K nezávislej akademickej analýze fungovania ekosystému označovania pozri Kimberly Easton, Malte Möser a Tyler Moore, "An Analysis of the Cryptocurrency Industry's Transaction Monitoring Ecosystem," *Financial Cryptography* (2022).

[30] United States v. Roman Sterlingov, č. 21-cr-00399 (D.D.C.). Sterlingov bol zatknutý v apríli 2021 a porota ho v marci 2024 uznala vinným zo sprisahania na pranie špinavých peňazí v súvislosti s jeho údajnou prevádzkou Bitcoin Fog, centralizovanej zmiešavacej služby činnej v rokoch 2011 až 2021. Proces sa stal významným testovacím prípadom pripisovania pri analýze reťazca: vláda sa silno opierala o svedectvo o Chainalysis Reactor a znalkyňa obhajoby Elizabeth Bisbee spochybnila reprodukovateľnosť metodiky a stav jej recenzovania. Súd dôkazy pripustil, verdikt je predmetom odvolania. K záznamu o procese a prepisom svedectiev znalcov pozri spis PACER 1:21-cr-00399. Novinárske spravodajstvo: Andy Greenberg, *Wired*, 12. marec 2024, "The Controversial Evidence That Convicted Bitcoin Fog's Alleged Operator."

[31] Financial Action Task Force (FATF), "Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers" (jún 2019), https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Guidance-rba-virtual-assets-2019.html. Požiadavka pravidla Travel Rule (odporúčanie 16 FATF uplatnené na VASP) ukladá, aby údaje identifikujúce odosielateľa a príjemcu sprevádzali prevody nad 1 000 USD/EUR. FATF, "Updated Guidance for a Risk-Based Approach: Virtual Assets and VASPs" (október 2021), https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Guidance-rba-virtual-assets-2021.html. Vnútroštátne zavedenie sa líšilo: FinCEN uplatnil existujúce pravidlá BSA, nariadenie EÚ o prevodoch finančných prostriedkov (TFR) rozšírilo Travel Rule na všetky prevody kryptoaktív bez ohľadu na sumu od decembra 2024 v rámci sprievodného nariadenia k MiCA. K prehľadu stavu zavádzania v jednotlivých štátoch z pohľadu odvetvia compliance pozri CipherTrace, "FATF Travel Rule Global Implementation" (2023), https://ciphertrace.com/.

[32] BIP 341 (Taproot), Pieter Wuille, Jonas Nick a Anthony Towns, "Taproot: SegWit version 1 spending rules" (2020), https://github.com/bitcoin/bips/blob/master/bip-0341.mediawiki. Aktivovaný pri bloku 709 632, 14. novembra 2021. BIP 342 (Tapscript), tí istí autori, https://github.com/bitcoin/bips/blob/master/bip-0342.mediawiki. BIP 340 (podpisy Schnorr), Pieter Wuille, Jonas Nick a Tim Ruffing, https://github.com/bitcoin/bips/blob/master/bip-0340.mediawiki. Analýza súkromia pri míňaní cez kľúčovú cestu oproti ceste cez skript je v BIP 341 §Motivation; zásada, že nepoužité vetvy skriptu zostávajú nezverejnené, je pre návrh ústredná. K histórii aktivácie (Speedy Trial, signalizácia, lock-in) pozri Bitcoin Optech Newsletter #139 a #157, https://bitcoinops.org/.

[33] MuSig2: Jonas Nick, Tim Ruffing a Yannick Seurin, "MuSig2: Simple Two-Round Schnorr Multi-Signatures," *CRYPTO 2021*, IACR ePrint 2020/1261, https://eprint.iacr.org/2020/1261. Štandardizovaný ako BIP 327: Jonas Nick, Tim Ruffing, Yannick Seurin a Elliott Jin, "MuSig2: Schnorr Multi-Signature Protocol," https://github.com/bitcoin/bips/blob/master/bip-0327.mediawiki. FROST (Flexible Round-Optimized Schnorr Threshold signatures): Chelsea Komlo a Ian Goldberg, "FROST: Flexible Round-Optimized Schnorr Threshold Signatures," *Selected Areas in Cryptography* (2020), IACR ePrint 2020/852, https://eprint.iacr.org/2020/852. FROST je základom podpisového protokolu Sparku a viacerých implementácií prahovej úschovy v peňaženkách Bitcoinu a je to aj podpisová schéma, na ktorej stoja listové dôkazy FCMP++ v Monere. K prahovému ECDSA ako alternatíve spred Schnorra pozri Rosario Gennaro a Steven Goldfeder, "Fast Multiparty Threshold ECDSA with Fast Trustless Setup," *ACM CCS 2018*.

[34] JoinMarket, dostupný na https://github.com/JoinMarket-Org/joinmarket-clientserver. Pôvodne vyvinuli Chris Belcher a Adam Gibson (waxwing). Návrhové eseje Adama Gibsona, vrátane "JoinMarket: Rethinking Coinjoin" (2017), vysvetľujú model maker/taker a dôvody pre súkromie. Orderbook JoinMarketu (https://joinmarket.me/ob/) zobrazuje aktívnu likviditu makerov v reálnom čase. K rozšíreniu PayJoin vo vnútri JoinMarketu (P2EP) pozri blog Adama Gibsona na https://reyify.com/blog/. Odolnosť protokolu voči zrušeniu koordinátora vyplýva z toho, že každý taker koordinuje svoje kolo priamo s vybranými makermi cez šifrovanú vrstvu správ (v súčasnosti IRC a skryté služby Tor), takže neexistuje jediný koordinačný server, ktorému by sa dal doručiť súdny príkaz alebo ktorý by sa dal zablokovať.

[35] Tier Nolan, "Alt chains and atomic transfers," Bitcoin Forum, máj 2013, https://bitcointalk.org/index.php?topic=193281.msg2003765. Tento príspevok je najstarším zdokumentovaným návrhom atomických výmen medzi reťazcami pomocou zmlúv so zámkom hašu a času. Aplikácia CoinSwapu v rámci jedného reťazca sa rozvinula neskôr. K najstaršiemu formálnemu spracovaniu CoinSwapu ako nástroja súkromia v reťazci pozri diskusiu Grega Maxwella vo vlákne o CoinJoine (2013) a návrh Chrisa Belchera "CoinSwap: Transaction graph disjoint trustless trading" (2020), https://gist.github.com/chris-belcher/9144bd57a91c194e332fb5ca371d0964.

[36] Protokol Spark: Buildonspark, "Spark: A Bitcoin Statechain Protocol," špecifikácia na https://docs.spark.money/ a https://github.com/buildonspark/spark. Spark rozširuje model statechainu, ktorého autorom je Ruben Somsen: Ruben Somsen, "Statechains: Non-custodial Off-chain Bitcoin Transfer," Bitcoin Optech Newsletter #91 (2020), a úplný návrh na https://github.com/RubenSomsen/rubensomsen.github.io/blob/master/img/statechains.pdf. Prahové rozšírenie FROST naprieč

viacerými podpisovými operátormi je hlavnou odchýlkou Sparku od pôvodného návrhu statechainu s jedným operátorom. K pôvodnému návrhu statechainu od Somsena pozri tiež vlákno v e-mailovej konferencii bitcoin-dev z marca 2020.

[37] Špecifikácia protokolu Cashu: `https://github.com/cashubtc/nuts` (Cashu NUTs - Notation, Usage, and Terminology). Referenčná implementácia mincovne: Nutshell, `https://github.com/cashubtc/nutshell`. Referenčná peňaženka: Cashu.me (web), `https://cashu.me`. Protokol Cashu navrhol Calle (`https://github.com/callebtc`) s priamou oporou v konštrukcii slepých podpisov Chauma z roku 1982. K technickému prehľadu cyklu mincovňa/token/výmena a vlastnosti slepoty operátora pozri dokumentáciu Cashu na `https://docs.cashu.space/` a opis Calle "Cashu: A Chaumian Ecash Wallet and Mint with Bitcoin Lightning," `https://github.com/cashubtc/cashu/blob/main/docs/WHITEPAPER.md`.

[38] Koordinátor zkSNACKs (wasabiwallet.io) 1. júna 2024 oznámil, že prestane koordinovať transakcie CoinJoin pre UTXO prepojené s USA po krokoch ministerstva spravodlivosti proti Samourai Wallet (apríl 2024). Koordinátor úplne ukončil prevádzku 1. júna 2024. K stíhaniu Samourai Wallet: United States v. Keonne Rodriguez and William Lonergan Hill, č. 24-cr-00242 (S.D.N.Y.), obžaloba zverejnená 24. apríla 2024, ktorá obviňuje zo sprisahania na pranie špinavých peňazí a z prevádzky neoprávnenej služby prevodu peňazí cez funkcie Whirlpool CoinJoin a Ricochet v Samourai. Alternatívni koordinátori, ktorí vznikli, zahŕňajú koordinátorov kompatibilných s WabiSabi, ktorých prevádzkuje BTCPay Server (`https://btcpayserver.org/`), a nezávislých prevádzkovateľov, ktorých možno nájsť cez mechanizmus zoznamu koordinátorov vo Wasabi; API koordinátora pozri `https://wasabiwallet.io/swagger/index.html`. Špecifikácia protokolu WabiSabi je otvorená na `https://github.com/WalletWasabi/WabiSabi`.

[28] Shorov algoritmus láme podpisy secp256k1 na dostatočnom kvantovom počítači, čím ohrozuje prostriedky Bitcoinu na opakovane použitých adresách a vo výstupoch P2PK. Typ výstupu Pay-to-Merkle-Root (P2MR) z BIP-360 chráni pred útokmi pri dlhodobom vystavení odstránením míňania cez kľúčovú cestu z Taprootu, pričom postkvantové podpisy sa pridajú v samostatnom budúcom návrhu. BIP-360, verzia 0.11.0 (február 2026), "Pay-to-Merkle-Root," Hunter Beast, Ethan Heilman a Isabel Foxen Duke, `https://github.com/bitcoin/bips/blob/master/bip-0360.mediawiki`. BIP sa predtým volal P2QRH (v0.1, september 2024) a P2TSH (v0.10, september 2025), než sa ustálil na P2MR; zoznam zmien v samotnom BIP túto históriu dokumentuje. K rozdielu medzi útokmi pri dlhodobom a krátkodobom vystavení a dôvodom na oddelenie typu výstupu P2MR od práce na postkvantových podpisoch pozri časti BIP-360 o motivácii a slovník pojmov. Postkvantové podpisové štandardy NIST (všetky dokončené 13. augusta 2024): FIPS 204 (ML-DSA, založený na Dilithium), `https://csrc.nist.gov/pubs/fips/204/final`; veľkosti podpisov: ML-DSA-44 = 2 420 bajtov, ML-DSA-65 = 3 293 bajtov, ML-DSA-87 = 4 595 bajtov (FIPS 204 Tabuľka 1). FIPS 205 (SLH-DSA, založený na SPHINCS+), `https://csrc.nist.gov/pubs/fips/205/final`; veľkosti podpisov sa pohybujú od 7 856 bajtov (SLH-DSA-SHA2-128s, malý/pomalý) po 49 856 bajtov (SLH-DSA-SHA2-256f, veľký/rýchly) naprieč dvanástimi množinami parametrov (FIPS 205 Tabuľka 2). FALCON (kompaktná schéma založená na mriežkach, Falcon-512 približne 666 bajtov, Falcon-1024 približne 1 280 bajtov) vybral NIST na pokračujúcu štandardizáciu. V čase písania nebolo pridelené číslo FIPS a štandard nebol publikovaný. Prehľad projektu postkvantovej kryptografie NIST: `https://csrc.nist.gov/projects/post-quantum-cryptography`. K súčasnému konsenzuálnemu časovému plánu pre kryptograficky relevantný kvantový počítač schopný prelomiť secp256k1: prevládajúci odhad vo výskumnej komunite aj medzi bezpečnostnými agentúrami je 10 až 20 rokov, pričom sada CNSA 2.0 americkej NSA

nariaďuje prechody do rokov 2030 až 2035. Práca Alice & Bob z roku 2024 (https://alice-bob.com/blog/computing-256-bit-elliptic-curve-logarithm-in-9-hours-with-126133-cat-qubits/) podstatne znížila predchádzajúce odhady zdrojov a vypočítala, že 126 133 mačacích kvbitov (cat qubits) by v zásade mohlo prelomiť ECC-256 za 9 hodín, hoci stroj s blízkym počtom kvbitov neexistuje. K priebežnej diskusii o kvantovej migrácii v bitcoin-dev a DelvingBitcoin pozri https://gnusha.org/pi/bitcoindev/ a https://delvingbitcoin.org/. K podielu ponuky Bitcoinu vystavenému kvantovému riziku pozri Deloitte, "Quantum Computers and the Bitcoin Blockchain" (2021). Pokrytie postkvantovej témy v Bitcoin Optech na https://bitcoinops.org/.

21

DECENTRALIZOVANÁ SOCIÁLNA INFRAŠTRUKTÚRA

„Najjednoduchší otvorený protokol, ktorý dokáže raz a navždy vytvoriť globálnu ‚sociálnu' sieť odolnú voči cenzúre."

fiatjaf, README protokolu Nostr (2020)[1]

Úvod

Sociálna koordinácia sa sústredila na hŕstke platforiem, ktoré vlastnia vrstvu identity. V tom je hlavná zraniteľnosť: keď účet drží platforma, zákaz neobmedzí len slobodu prejavu, ale zničí aj sociálny graf, ktorý sa okolo účtu vybudoval. Sledujúci, reputácia, história príspevkov i vzťahy s publikom zmiznú naraz jediným administratívnym krokom.

Nostr je protokol, ktorý prenáša kontrolu nad identitou na používateľa. Účet je pár kľúčov, ktorý si používateľ sám vygeneruje a sám ho ovláda. Nie je to pridelenie od nijakého prevádzkovateľa. Relaye ukladajú a preposielajú obsah, ale nad identitou nemajú nijakú moc. Protokol rieši najprv prenosnosť a odolnosť voči cenzúre. Vlastnosti týkajúce sa súkromia vyplývajú z jeho architektúry a rozoberajú ich nasledujúce oddiely.

21.1 Problém centralizovaných platforiem

Sociálne platformy sú osobitne nebezpečné tým, že zachytávajú identitu. Dva podniky, Meta a Alphabet, ovládajú základnú infraštruktúru sociálneho grafu pre väčšinu amerických používateľov internetu. K roku 2025 oslovuje YouTube 84 % dospelých Američanov a Facebook 71 %; samotná Meta vlastní štyri platformy, z ktorých každá má viac než miliardu aktív-

nych používateľov mesačne.[2] Ak sa dohodnú dva-tri podniky, môžu používateľovi prakticky zrušiť verejnú prítomnosť na celom dostupnom internete. Analýza firemného sledovania v kapitole 11 opisuje aj model vyťažovania údajov, ktorý to sprevádza: behaviorálne profilovanie a mapovanie sociálnych grafov, spojené so štátom prostredníctvom výmeny údajov.

Twitter Files (december 2022 až marec 2023) zdokumentovali mechanizmus tohto prepojenia so štátom do prevádzkových podrobností. FBI mala formalizovaný kanál na podávanie žiadostí o preskúmanie účtov tímu Trust and Safety na Twitteri a Ústredné velenie USA (CENTCOM) viedlo skryté účty na vplyvové operácie, ktoré tím Site Integrity na Twitteri zaradil na bielu listinu.[3] Formálne príkazy netreba. Stačí bežná komunikácia medzi vládnymi úradmi a tímami platforiem, ktoré majú na starosti dôveru a bezpečnosť.

Riziko vyradenia z platformy

Vyradenie z platformy (de-platforming) je úplné odstránenie z platformy a zo všetkého, čo platforma o používateľovi uchováva. V auguste 2018 odstránili Alexa Jonesa a InfoWars spoločnosti Apple, Facebook, YouTube a Spotify, a to koordinovane v priebehu 12 hodín. Jones prišiel o kanál na YouTube s približne 2,4 milióna odberateľov a vyše 1,5 miliardy archivovaných zhliadnutí, a to súčasne s odstránením zo všetkých ostatných veľkých platforiem.[20] V januári 2021 Twitter po útoku na Kapitol zrušil vyše 70 000 účtov a Amazon Web Services ukončil hosting platformy Parler. Celá platforma sa tak odmlčala a údaje účtov asi 15 miliónov registrovaných používateľov sa vymazali jediným zásahom do infraštruktúry.[21]

Pri žiadnom z týchto zrušení nebolo nijaké upozornenie vopred. Núdzové bezpečnostné pravidlá dovoľujú okamžitý trvalý zásah bez prechodného obdobia, v ktorom by sa dal obsah exportovať alebo zálohovať kontakty. Vzťahy s publikom, ktoré tvorca budoval roky, sa zmažú spolu s účtom.

Problém prenosnosti

Tvorcovia nikdy nevlastnia vlastné publikum. Keď niekto na centralizovanej platforme sleduje účet, poskytne platforme svoje kontaktné údaje. Tvorca tento zoznam exportovať nemôže. Článok 20 GDPR dáva používateľom právo stiahnuť si vlastné osobné údaje v strojovo čitateľnej podobe a všetky veľké platformy ho dnes dodržiavajú. Kontaktné údaje sledujúcich však patria sledujúcim, nie tvorcovi.[22] Vlastné príspevky si stiahnuť môžete, no kontaktné údaje dvoch miliónov sledujúcich nie.

Prevádzkovateľ e-mailového newslettera so 100 000 odberateľmi môže prejsť od jedného poskytovateľa k druhému exportom súboru CSV. Obdobný mechanizmus pre sledujúcich na sociálnych platformách neexistuje. Sociálny graf je vlastnícky majetok platformy.

Zosobnenie a integrita obsahu

Centralizované platformy nezaručujú kryptograficky, že obsah pripísaný účtu naozaj vytvoril jeho majiteľ. Platforma overuje relácie prihlásenia, nie výroky. Správca s prístupom do databázy môže príspevok upraviť alebo zmazať bez toho, aby po zmene zostala viditeľná stopa. Snímka obrazovky s tweetom nie je dôkaz, že ho niekto odoslal. Platforma môže obsah nepozorovane zmeniť alebo odstrániť a používatelia to nijako nezistia.

Zosobňovanie to ešte zhoršuje. Overovací odznak naznačuje, že platforma potvrdila akýsi vzťah medzi účtom a skutočnou identitou. Je to však len tvrdenie platformy, nie dôkaz, ktorý by si používateľ mohol overiť sám. Platformy presúvali overovacie odznaky medzi účtami a rovno ich predávali. Keď vrstvu overovania ovláda platforma, používatelia nemajú ako rozoznať pravé výroky od vymyslených, iba ak by uverili záznamom samotnej platformy.

Efekty uzamknutia

Sieťové efekty a dynamika uzamknutia, ktoré rozoberá kapitola 11, vysvetľujú, prečo používatelia zostávajú na platformách, ktoré sa im nepáčia. Ak jednotlivec prejde inam, sieť sa s ním nepresunie, a mechanizmy, ktoré to udržiavajú, siahajú hlbšie než len k veľkosti siete.

Archívy obsahu fungujú ako utopené náklady. Všetko, čo používateľ uverejnil, existuje len v databáze platformy. Kto odíde, tento záznam úplne stratí, lebo neexistuje spôsob exportu, ktorý by zachoval sociálnu vrstvu okolo obsahu. Samotné príspevky existujú ako súbory, no reťazce odpovedí a história reakcií, ktoré príspevkom dávajú zmysel, export neprežijú.

Algoritmické zosilňovanie tento efekt umocňuje. Platformy určujú dosah podľa histórie reakcií na tej konkrétnej platforme. Tvorca, ktorý si za päť rokov vybudoval stotisícové publikum, nemôže preniesť signály o reakciách, ktoré to šírenie poháňali. Nový začiatok na inej platforme znamená nulový dosah bez ohľadu na kvalitu obsahu, lebo nová platforma nemá nijaké predošlé údaje o reakciách, ktoré by mohla dodať svojmu odporúčaciemu systému.

Obmedzenia rozhraní API bránia nástrojom tretích strán, aby túto medzeru preklenuli. Platformy môžu odobrať alebo obmedziť prístup k API, ktorý by umožnil automatizovaný kontakt so sledujúcimi alebo presun obsahu, a aj to robia. Zmena cien API na Twitteri v roku 2023 zvýšila náklady o niekoľko rádov a prakticky vypla nezávislé výskumné nástroje i klientov tretích strán na migráciu, ktoré fungovali roky.[23] To, čo je technicky možné, sa bežne robí ekonomicky neuskutočniteľným.

Cena za odchod je kolektívna, lebo vzťahy s publikom si vyžadujú konanie oboch strán. Tvorca môže oznámiť, že sa presúva na novú platformu, ale či publikum nasleduje, je samostatný problém koordinácie, ktorý

jednostranne vyriešiť nevie. Platforma drží používateľa nie zmluvou, ale zlyhaním koordinácie, ktoré by bolo treba prekonať, aby sa dalo odísť.

Algoritmická nepreniknuteľnosť

To, čo používatelia vidia, určujú uzavreté a neauditované proprietárne algoritmy radenia, nastavené podľa komerčných záujmov platformy. Prúd príspevkov nie je chronologický záznam obsahu z účtov, ktoré si používateľ vybral. Je to filtrovaný a pretriedený výber, ktorý vytvára kód s optimalizačnými cieľmi v prospech platformy, nie používateľa.

Skrytým variantom tejto kontroly je shadowban. Účet pod shadowbanom ostáva nominálne aktívny (používateľ môže ďalej písať a vyzerá viditeľne), ale distribučné systémy platformy obsah potláčajú, takže odpovede zostávajú bez reakcie a príspevky sa sledujúcim na časových osiach nezobrazia. Používateľ nedostane nijaké oznámenie a nemá ako sa odvolať. Interné dokumenty samotného Twitteru zverejnené v rámci Twitter Files potvrdili, že platforma viedla osobitné interné úrovne viditeľnosti, ktoré sa líšili od toho, čo videli používatelia na vlastných profiloch.

Nepreniknuteľnosť je štrukturálna. Platformy nemajú dôvod zverejniť kritériá radenia, lebo tie slúžia zároveň ako páky na cielenie reklamy. Tie isté signály, ktoré určujú, kto príspevok uvidí, určujú aj to, aké reklamy sa popri ňom zobrazia. Otvoriť algoritmus kontrole by odhalilo komerčnú logiku prúdu príspevkov. Používatelia pracujú so systémom, ktorého pravidlá nevedia prečítať a môžu ich len odvodzovať z pozorovaného správania. Ani toto odvodzovanie nie je spoľahlivé, lebo algoritmus sa nepretržite mení bez oznámenia.

21.2 Nostr: riešenie na úrovni protokolu

Jednoduchý protokol, zložitá sieť

Nostr (Notes and Other Stuff Transmitted by Relays, teda poznámky a iné veci prenášané cez relaye) je protokol, nie platforma.[4] Určuje, ako sa správy formátujú a ako spolu komunikujú klienti a relaye. Klientov môže implementovať a relaye môže prevádzkovať ktokoľvek.

Jadro protokolu je pozoruhodne jednoduché. Všetok obsah má podobu „udalostí“ (events): textových súborov JSON so štandardným formátom, ktoré obsahujú samotný obsah, časovú značku, verejný kľúč autora, podpis a značky pre metadáta. Udalosť nie je nič iné než podpísaný textový súbor. Vďaka tejto radikálnej jednoduchosti sa udalosti dajú ukladať a prenášať akýmkoľvek kanálom a spracuje ich každý softvér, ktorý vie čítať JSON a overovať podpisy. Relaye sú servery, ktoré udalosti ukladajú a preposielajú, hoci aj platne podpísané udalosti môžu podľa miestnej politiky prijať alebo odmietnuť a niektoré vyžadujú rozšírenia na overenie, napríklad NIP-42. Klienti sú aplikácie, s ktorými používatelia pracu-

jú. Preberajú udalosti z relayov a zobrazujú ich a potom vytvárajú nové udalosti, ktoré používatelia podpisujú.

Táto jednoduchosť umožňuje inováciu bez povolenia. Šikovný vývojár postaví klienta za pár dní. Tvorca nepotrebuje kľúče API ani schvaľovací proces a okrem samotného protokolu nijaké podmienky používania neriadia prístup. Výsledkom sú tisíce klientov s rôznym zameraním: mobilné, desktopové, na dlhé texty, obrázky, video, rozhovory, trhoviská.[5] Nikto nekontroluje, kto môže tvoriť klientov alebo prevádzkovať relaye.

Architektúra poznámok a relayov

Architektúra oddeľuje kontrolu používateľa od úloh klienta a relayu. Používatelia držia súkromné kľúče a vytvárajú podpísané udalosti. Klienti poskytujú rozhranie a spravujú pripojenia k relayom. Relaye udalosti ukladajú a rozširujú, no žiadny z nich nie je autoritatívny. Používatelia sa môžu pripojiť k viacerým relayom naraz a obsah sa replikuje na tie, ktoré si vyberú.

Nijaký relay nemá rozhodujúce slovo. Jeden relay môže používateľa odmietnuť alebo úplne vypadnúť, ale obsah môžu ďalej niesť iné. Používatelia si relaye vyberajú podľa pravidiel a zhody s komunitou.

Systém NIP

Nostr Implementation Possibilities (NIP) sú mechanizmus, ktorým protokol rastie.[6] NIP je písaná špecifikácia: dokument, ktorý definuje nový druh udalosti, nové pole, nové správanie alebo nový vzor interakcie, a to dosť presne na to, aby ho ktorýkoľvek vývojár mohol implementovať samostatne a fungoval s každou inou implementáciou. Špecifikácia je vo verejnom repozitári. Napísať ju môže ktokoľvek.

Proces je otvorený zámerne. Vývojár, ktorý chce do protokolu Nostr pridať funkciu, napíše NIP s presným opisom, ako funkcia pracuje (číslo druhu udalosti, povinné polia, očakávané správanie klientov a relayov), a podá ho. Ostatní vývojári si ho prečítajú, diskutujú o ňom, navrhnú zmeny a rozhodnú sa, či ho implementujú vo vlastných klientoch a relayoch. Nijaký výbor neschvaľuje ani nezamieta, ktoré NIP sa dostanú do protokolu. Rozhoduje iba prijatie. NIP, ktorý rieši skutočný problém, sa implementuje, ten, ktorý nie, sa ignoruje. Repozitár uchováva oba druhy a rozloženie implementácií odráža úsudok vývojárov, nie preferencie nejakého ústredného orgánu.

NIP-01 definuje základný protokol: formát udalosti, model komunikácie s relayom a syntax odberov. Všetko, čo sa na ňom stavia, je voliteľné. Čitateľné identifikátory priradené verejným kľúčom cez DNS pochádzajú z NIP-05 a dávajú používateľom adresy ako `alice@example.com`, ktoré sa vyriešia na kryptografický kľúč Alice. Lightning zapy, teda spôsob, ako používatelia k udalostiam pripájajú bitcoinové mikroplatby, defi-

nuje NIP-57. Overenie voči relayu, vďaka ktorému môže relay požadovať od klientov dôkaz vlastníctva kľúča skôr, než prijme obsah, prináša NIP--42. Šifrované priame správy sú NIP-44. Každý z nich začínal ako dokument, ktorý niekto napísal a zverejnil s pozvaním na nezávislú implementáciu.

Z toho vyplýva, že nijaký jediný subjekt nekontroluje, čo Nostr dokáže. Aplikácia, ktorá chce pridať funkciu, vydá NIP a pozve ostatných, aby ho prijali. Bezpečnostný výskumník, ktorý nájde chybu v existujúcej konštrukcii, napíše náhradný NIP a obhajuje prechod naň. Rozsah protokolu sa rozširuje alebo zužuje podľa toho, čo vývojári postavia a čo používatelia používajú, bez toho, aby k tomu bolo treba povolenie od niekoho.

21.3 Kľúče ako identita: kryptografická suverenita

Verejný kľúč ako identita

V Nostre je identitou verejný kľúč. Celá registrácia spočíva v lokálnom vygenerovaní páru kľúčov. Nijaký server ju neudeľuje a nijaký server ju nemôže odobrať. Nezapája sa do toho ani používateľské meno, ani telefónne číslo.

Verejný kľúč je trvalý identifikátor. Každá uverejnená udalosť sa podpisuje súkromným kľúčom a tento podpis kryptograficky viaže udalosť na verejný kľúč. Kto udalosť dostane, môže podpis overiť bez toho, aby kontaktoval nejakú autoritu. Identita funguje na princípe držby: kto drží súkromný kľúč, ten identitu ovláda, a nijaká tretia strana to nemôže zrušiť.

Rozdiel oproti systémom založeným na účtoch je architektonický. Na tradičnej platforme je účet riadok v databáze, ktorú platforma ovláda a správca ho môže podľa vlastného uváženia upraviť alebo zmazať. V sieti Nostr je identita matematický objekt, ktorý existuje nezávisle od akejkoľvek databázy. Relay môže odmietnuť prenášať udalosti, ale nemôže ich zmeniť ani zneplatniť kľúč. Neexistuje autorita, ktorá by mala moc identitu samotnú pozastaviť.

Identita a profil pod kontrolou používateľa

Keď používateľ vytvorí pár kľúčov, môže celú svoju identitu vyhlásiť sám prostredníctvom udalosti druhu 0. Tento osobitný typ udalosti obsahuje objekt JSON s metadátami profilu: používateľské meno, zobrazované meno, životopis, profilový obrázok, banner, webovú stránku, adresu Lightning na prijímanie platieb a ľubovoľné ďalšie polia, ktoré chce používateľ uviesť. Tieto informácie podpíše súkromným kľúčom a uverejní na relaye.

Nijaká tretia strana nemôže používateľovi zabrániť, aby si zvolil identitu, akú chce. O tom, aké meno alebo profilový obrázok si kto vyberie, nerozhoduje nijaký schvaľovací proces ani kontrola obsahu. Ak jeden re-

lay udalosť odmietne, iné ju môžu prijať. Identita existuje od chvíle, keď ju používateľ podpíše.

Tým sa obracia tradičný vzťah medzi používateľmi a platformami. Na centralizovaných službách vlastní platforma menný priestor a používateľom dovolí zaujať v ňom miesto. V sieti Nostr si používatelia vytvárajú identity, ktoré existujú nezávisle od akejkoľvek infraštruktúry. Profil je len podpísaný textový súbor, ktorý dokáže prečítať a zobraziť ľubovoľný softvér.

Výzvy správy kľúčov

Kontrola nad kľúčom prináša zodpovednosť a výzvy, ktoré tradičné systémy založené na účtoch nepoznajú.

Strata kľúča je trvalá. Kto stratí súkromný kľúč, stratí identitu. Neexistuje obnovenie cez „zabudnuté heslo", zákaznícka podpora ani druhý spôsob overenia. Nahromadená reputácia a história spojená s týmto verejným kľúčom sa stanú nedostupnými.

Kompromitácia kľúča je rovnako trvalá, ale v opačnom smere. Ak útočník získa súkromný kľúč, môže sa za používateľa vydávať donekonečna. V systémoch založených na účtoch môžu správcovia kompromitovaný účet zamknúť a poverenia obnoviť iným spôsobom overenia, v sieti Nostr taká cesta obnovy nie je. Útočník s cudzím kľúčom sa kryptograficky nedá od pôvodného používateľa odlíšiť. Môže písať a podpisovať v jeho mene a nie je autorita, na ktorú by sa dalo odvolať. Kompromitácia je trvalá krádež identity.

Rotácia kľúča má vlastné ťažkosti. Tradičné systémy dovoľujú zmeniť heslo a zachovať kontinuitu účtu. Dnes nemá Nostr široko prijatý mechanizmus, ako prejsť na nový kľúč a zachovať kontinuitu identity. Presun na nový kľúč znamená začať odznova: nový verejný kľúč, nula sledujúcich, žiadna história. Niektorí klienti podporujú oznámenia o rotácii kľúča, v ktorých starý kľúč podpíše správu schvaľujúcu nový, no prijatie je nejednotné a mnohí klienti tieto prechody nerozpoznávajú. Používatelia, ktorí majú podozrenie na kompromitáciu, tak volia medzi pokračovaním s kompromitovaným kľúčom a vzdaním sa nahromadeného sociálneho kapitálu.

Pri správe týchto rizík musia používatelia zvažovať kompromisy. Vlastná úschova dáva najväčšiu kontrolu spolu s najväčšou zodpovednosťou. Riešenia s úschovou u tretej strany dovoľujú službám kľúče držať a umožňujú obnovu, no za cenu dôvery v správcu úschovy. Prahové schémy rozdeľujú kľúče medzi viacero strán, takže na obnovu musí spolupracovať ich podmnožina. Tieto kompromisy sú vlastné systémom pod vlastnou kontrolou používateľa. Nostr ich zviditeľňuje a neskrýva za „účty" ovládané platformou.

Sociálne prístupy môžu problém zmierniť, nevyriešia ho. Používateľ, ktorý ešte ovláda kompromitovaný kľúč, môže zverejniť jasné varovanie, že kľúču sa už nemá dôverovať, a priatelia a protistrany môžu potvrdiť, že nový kľúč je oprávnený nástupca. To pomáha zachovať kontinuitu a varovať širšiu sieť, ale závisí to od podpory klientov, viditeľných konvencií a sociálneho overenia. Obnova identity v sieti Nostr ostáva otvoreným problémom.

21.4 Architektúra relayov a trhová dynamika

Relay môže prevádzkovať ktokoľvek

Na prevádzku relayu v sieti Nostr stačí server a softvér relayu. Nepotrebuje sa povolenie ani schválenie. Softvér relayu je open source a protokol je verejný.

Jednotlivci prevádzkujú osobné relaye, komunity špecializované a podniky komerčné. Prekážka je dosť nízka, aby ju zvládli aj nadšenci a samostatní vývojári, nielen dobre financovaní prevádzkovatelia. Relay sa dá spustiť na telefóne či starom notebooku rovnako ako na VPS za tri doláre mesačne. Nároky na úložisko sú skromné, lebo každý relay ukladá len udalosti, ktoré sa rozhodne prijať, nie celú históriu siete.

Súťaž relayov v kvalite služieb

Relaye súťažia vo viacerých rozmeroch. Spoľahlivosť zahŕňa dostupnosť a čas odozvy. Relay, ktorý zahadzuje spojenia alebo stráca udalosti, posiela používateľov k alternatívam. Politika ukladania určuje, koľko histórie relay uchováva a ktoré druhy udalostí indexuje. Relaye, ktoré agresívne mažú, strácajú používateľov, pre ktorých sú dôležité staršie príspevky. Súbory funkcií sa líšia: niektoré relaye ponúkajú fulltextové vyhľadávanie, iné analytické panely alebo špeciálne spracovanie určitých druhov udalostí, napríklad dlhých článkov či ponúk na trhovisku. Pravidlá určujú, aký obsah relay prijíma alebo odmieta, a to priťahuje komunity s rovnakými hodnotami. Relay, ktorý presadzuje prísne štandardy obsahu, pritiahne používateľov, ktorí také prostredie chcú, a voľnejší relay pritiahne iných.

Používatelia na tieto rozdiely reagujú tak, že si nastavia viac relayov a každému dajú inú váhu. Môžu uverejňovať na platený relay s vysokou dostupnosťou kvôli širokému dosahu a súčasne na komunitný relay, ktorý slúži ich konkrétnemu publiku. Distribúciu spravuje klient, pravidlá určuje používateľ. Relaye, ktoré používateľom slúžia dobre, si ich udržia, ostatné z ich zoznamu vypadnú.

Platené a bezplatné modely relayov

Financovanie relayov má viacero podôb. Relaye dotované prevádzkovateľom ponúkajú bezplatný prístup, ale náklady nesie prevádzkovateľ. Plate-

né relaye účtujú poplatky priamo používateľom, čo prevádzku financuje a zároveň zvyšuje cenu spamu. Freemium relaye dávajú základné používanie zadarmo a za rozšírené funkcie si pýtajú poplatok. Platené relaye riešia problém udržateľnosti a vytvárajú stimuly na kvalitné služby. Bezplatné relaye slúžia používateľom, ktorí zaplatiť nemôžu alebo nechcú, no pri väčšom rozsahu majú problém s udržateľnosťou.

Mechanika platieb sa líši podľa relayu. Predplatné relaye účtujú paušálny poplatok, zvyčajne v satoshi mesačne, dobíjaný platbou cez Lightning. Relay pred prijatím udalostí kontroluje zostatok na účte a keď sa minie, prestane účet obsluhovať. Relaye platiace za udalosť zvolili iný prístup: každá nahraná alebo stiahnutá udalosť stojí malý token ecash, takže cena je jemne odstupňovaná a náklady priamo úmerné používaniu. Tokeny ecash sa dajú vydávať a vymieňať bez odhalenia identity platiteľa, čo na vrstve relayu zachováva časť súkromia používateľa. Prevádzkovatelia relayov, ktorí preferujú bežné účtovanie, môžu prijímať platby vo fiat peniazoch cez štandardných poskytovateľov platieb. Softvér relayu zvyčajne od spôsobu platby abstrahuje a za podmienku prístupu pokladá platné predplatiteľské poverenie, nech bolo financované akokoľvek. Množstvo možností platby odráža, že neexistuje nijaká ústredná autorita pre relaye: prevádzkovatelia si volia vlastný obchodný model a používatelia relayov, ktorých podmienky im vyhovujú.

Súčasné sklony k centralizácii

Napriek decentralizovanému návrhu sa v praxi aj v sieti Nostr prejavujú sklony k centralizácii. Väčšinu prevádzky nesie niekoľko veľkých relayov, lebo používatelia siahajú po známych, a objavovanie obsahu prechádza cez hŕstku indexovacích služieb. Niekoľko klientov priťahuje väčšinu používateľov, lebo sieťové efekty uprednostňujú známy softvér. Tento vzorec odráža bežnú trhovú dynamiku: sieťové efekty ženú koordináciu k spoločnej infraštruktúre bez ohľadu na to, či to podkladový protokol vynucuje. Protokol mení následky tejto koordinácie. Na centralizovaných platformách sa bod koordinácie stáva platformou a platforma jediným miestom, kde môžu používatelia existovať. V sieti Nostr sa bod koordinácie môže posúvať, keď používatelia prechádzajú medzi relayami a klientmi a identitu si nechávajú, takže možnosť odísť (exit) ostáva zachovaná, aj keď jeden relay či klient na čas dominuje.

Otázkou je, či trhová súťaž udrží dostatok alternatív, aby sa zabránilo opätovnej koncentrácii. Protokol decentralizáciu umožňuje, ale o jej pretrvaní rozhodujú trhové výsledky.

21.5 Reputácia bez ústrednej autority

Modely siete dôvery

Ako majú používatelia posudzovať dôveryhodnosť bez ústredného overovania? V modeloch siete dôvery (web of trust) sa používatelia za iných zaručujú a dôvera sa šíri sieťou. Ak niekto dôveruje Alice a Alice dôveruje Bobovi, má určitý dôvod pokladať za dôveryhodného aj Boba. Grafy sledovaných účtov ukazujú štruktúru komunít a používatelia, ktorých účet sledujú ľudia, ktorým dôverujeme, bývajú dôveryhodnejší. Výslovné odporúčania vytvárajú ďalšie signály reputácie. Základná myšlienka je stará: reputácia rastie v komunitách, v ktorých človek pôsobí. Mení sa to, že kryptografické podpisovanie robí potvrdenia výslovnými a overiteľnými pre každého, kto ich dostane.[7]

Sieť dôvery (WoT) je už nasadená ako filter spamu na vrstve relayu. Implementácia wot-relay filtruje udalosti podľa toho, či autor leží v nastaviteľnej vzdialenosti (počte skokov) od grafu sledovaných účtov prevádzkovateľa relayu. Udalosti z účtov mimo tohto okolia sa zahodia, bez toho, aby relay musel posudzovať obsah.[24] Obchod s aplikáciami Zapstore využíva tie isté signály na objavovanie softvéru: aplikácie uverejnené účtami z grafu dôvery používateľa sa zobrazujú prednostne pred aplikáciami od cudzích.[25] Ide o praktické nasadenia WoT ako mechanizmu proti spamu a na kuratorský výber obsahu, ktoré fungujú bez nijakého ústredného registra.

Sledovania a interakcie ako signály reputácie

Reputácia vzniká z pozorovateľného správania v čase. Počet sledujúcich naznačuje vnímanú hodnotu v danom okamihu, zatiaľ čo odpovede, zdieľania a iné reakcie ukazujú, ako čitatelia hodnotia konkrétny obsah. Zavedené účty majú zvyčajne väčšiu váhu než čerstvé, lebo dlhý záznam dôsledného správania sa dá vyrobiť len draho, a čím dlhšie kľúč pôsobí pod jednou personou, tým ťažšie je ju zahodiť a nahradiť bez straty všetkého, čo sa pod ňou nahromadilo. Žiaden z týchto signálov nie je neomylný a všetky sa dajú čiastočne zmanipulovať, no spolu dávajú informáciu o dôveryhodnosti bez toho, aby ústredná autorita vopred rozhodovala, čo sa za dôveryhodné pokladá.

Overenie bez centralizovaných odznakov

NIP-05 v Nostre umožňuje overenie cez DNS.[8] Používatelia môžu prepojiť svoju identitu v sieti Nostr s doménou, ktorú ovládajú: „`user@example.com`“, kde doména example.com toto prepojenie potvrdzuje.

Overenie funguje na základe kontroly nad doménou, nie rozhodnutím platformy. Organizácie overujú zamestnancov tým, že hostujú ich identity,

a jednotlivci sa overujú vlastnými doménami. Nijaká ústredná autorita nerozhoduje, kto je „overený“.

Dôvera je v doméne, nie v odznaku platformy. Právomoc overovať sa tak rozdeľuje namiesto toho, aby sa sústreďovala.

Overenie naprieč anonymnými kanálmi

Sieť dôvery je užitočnejšia, keď prekračuje hranice kanálov. Predstavme si, že nám niekto napíše na anonymnom kanáli a tvrdí, že je vývojár alebo obchodník, ktorého poznáme zo siete Nostr. Okamžitý problém nie je abstraktná reputácia, ale kontinuita: ovláda osoba na tomto kanáli kľúč, ktorého verejnú históriu už poznáme?

Na túto otázku odpovie výzva a odpoveď (challenge-response). Jedna strana vygeneruje nonce a pošle výzvu cez anonymný kanál. Druhá strana výzvu podpíše známym kľúčom zo siete Nostr a podpísanú odpoveď vráti, ideálne jednorazovou šifrovanou správou cez relay, alebo ručným skopírovaním, ak prenos cez relay nie je dostupný. Overovateľ skontroluje podpis a potom sociálny graf okolo toho kľúča. Kto ho sleduje? Má identifikátor NIP-05? Zodpovedá história príspevkov tvrdenej identite?

Tým sa preukáže kontinuita medzi anonymným kanálom a reputačnou identitou. Nedokazuje sa tým nevinnosť ani obchodná spoľahlivosť. To sú väčšie inštitucionálne otázky. Vyrieši to však jeden skutočný problém: ako overiť známy pseudonym naprieč kanálmi bez toho, aby sa žiadala právna identita.

Odpoveď na otázku kontinuity má svoje hranice. Signály reputácie a dôkazy na úrovni protokolu dokážu niesť dôveru len po istú mieru a širšie otázky protistrán a sporov patria do inštitucionálnej vrstvy, ktorou sa zaoberá kapitola 24.

Dôveryhodné tvrdenia: štruktúrované signály reputácie

NIP-85 formalizuje reputáciu ako podpísaný štruktúrovaný dátový produkt.[26] Dôveryhodné tvrdenie (trusted assertion) je parametrizovaná nahraditeľná udalosť, ktorú uverejňuje deklarovaný poskytovateľ služby a ktorá sa týka subjektu určeného verejným kľúčom, ID udalosti, adresovateľnou súradnicou alebo externým odkazom podľa NIP-73. Každé tvrdenie nesie vypočítané hodnoty vo forme štruktúrovaných značiek: skóre poradia od 0 do 100, počet sledujúcich, súčet prijatých zapov, počty nahlásení a odvodené tematické zhluky z histórie príspevkov subjektu. Poskytovateľ tvrdenie podpisuje kľúčom, ktorý patrí konkrétnemu algoritmu, ktorý ho vytvoril. Podpisujúcim je teda algoritmus a jeho deklarovaná metodika, nie jednotlivec, ktorý kľúč poskytovateľa obsluhuje.

Používatelia sa pre konkrétnych poskytovateľov rozhodnú tak, že uverejnia udalosť druhu 10040 so zoznamom kľúčov poskytovateľov, ktorým dôverujú. Voliteľne ju zašifrujú, aby samotná voľba poskytovateľa nebola

verejná. Klienti potom získavajú tvrdenia od deklarovaných poskytovateľov a používajú ich na radenie alebo filtrovanie obsahu, bez toho, aby museli lokálne robiť náročné výpočty nad grafom. Výsledkom je čisté oddelenie tvorby reputácie od jej spotreby: poskytovatelia súťažia v metodike a presnosti, klienti spotrebúvajú podpísané výstupy bez prehľadávania celej siete dôvery a používatelia riadia, ktoré metodiky určujú, čo uvidia. Nič v návrhu nevyžaduje, aby bol niektorý poskytovateľ autoritatívny pre všetkých používateľov, a nijaký ústredný register nerozhoduje, ktoré tvrdenia sa počítajú. Tá istá infraštruktúra kľúčov, ktorá overuje príspevky, overuje aj tvrdenia o reputácii, a tie isté zoznamy dôvery pod kontrolou používateľa, ktoré riadia výber relayov, riadia aj to, ktoré signály reputácie platia.

21.6 Moderovanie ako trhová služba

Žiadne moderovanie na úrovni protokolu

Nostr nemá moderovanie obsahu na úrovni protokolu. Protokol prenáša podpísané udalosti a nehodnotí, či sú prijateľné. Toto posúdenie je celé na vrstvách nad ním. Absencia je zámerná: moderovanie na úrovni protokolu by vyžadovalo autoritu, ktorá by definovala, čo je prijateľné, a tieto definície by presadzovala v celej sieti. To by centralizovalo práve tú moc, ktorej mal protokol zabrániť. Namiesto toho tu je deľba práce medzi relayami, klientmi a kuratorskými službami podľa výberu používateľa, z ktorých každý pôsobí samostatne a súťaží o používateľov kvalitou svojich pravidiel.

Relaye filtrujú prostredníctvom politiky prijímania a blokovania na úrovni kľúčov. Nič v protokole nenúti relay prenášať konkrétnu udalosť, každý prevádzkovateľ rozhoduje, čo je ochotný hostiť. Tá istá udalosť môže jeden relay prijať a druhý odmietnuť. Používateľ, ktorého obsah jeden relay odmietne, uverejní na inom a stratí len dosah na tom konkrétnom hostiteľovi, nie prístup k sieti.

Klienti filtrujú to, čo zobrazujú, okrem iného stlmením a algoritmickým radením. Keďže klienti bežia na používateľovom zariadení, filtrovanie je voľba používateľa, nie nariadenie platformy. Používatelia, ktorým nevyhovuje filtrovanie niektorého klienta, môžu prejsť na iného a o identitu ani sociálny graf neprídu.

Medzi relayom a klientom sa nachádza trh s kuratorskými službami. Poskytovatelia zoznamov blokovaných prinášajú kuratorsky zostavené zoznamy účtov na filtrovanie, filtre spamu odstraňujú nechcený obsah, moderátori komunít udržiavajú miestne štandardy a služby algoritmických prúdov balia radenie ako produkt. Používatelia si volia, ktoré kuratorské služby odoberajú, a poskytovatelia súťažia kvalitou a hodnotami. Výsledkom je moderovanie, ktoré funguje bez jedinej autority rozhodujúcej

o tom, čo uvidí každý: každý používateľ si zloží vlastnú skúsenosť z relayov a kuratorských služieb, ktoré mu vyhovujú, a nezhody o moderovaní sa riešia tým, že rôzni používatelia môžu voliť rôzne.

21.7 Nielen sociálne siete: jeden protokol, mnoho druhov obsahu

Tá istá architektúra podpísaných udalostí a relayov, ktorá nesie krátke sociálne príspevky, dokáže niesť čokoľvek iné, čo chce vývojár definovať, a systém rozšírení NIP sa na to už použil. Dlhý článok, inzerát, živé video vysielanie, záznam vo wiki, zvuková miestnosť, šifrovaná skupinová správa: všetko sú udalosti Nostr určitého druhu, smerované cez tie isté relaye a overované tými istými verejnými kľúčmi. Obsahový záber je široký, mechanika pod ním sa nemení.

Práve táto kontinuita je zaujímavá. Autor, ktorý uverejňuje krátke poznámky pod jedným párom kľúčov, môže pod tým istým párom vydávať dlhé eseje a čitatelia odoberajú oba druhy textov cez ten istý sociálny graf.[9] Vývojár, ktorý si vybudoval sociálnu reputáciu, môže vydávať podpísané verzie softvéru, ktoré používatelia nájdu cez tú istú sieť dôvery, na akej beží každá iná aplikácia v sieti Nostr, čím úplne obíde obchod s aplikáciami v úlohe strážcu prístupu. Obchodník, ktorého verejná história je v sieti viditeľná, môže ponúkať tovar na trhovisku typu peer-to-peer, kde kotvou identity je verejný kľúč a nie účet na platforme, pričom platby zabezpečuje Lightning a zvyšok súkromné správy.[10] Streamer môže vysielať video, ktorého objavovanie a odmeňovanie bežia po tých istých relayoch ako jeho obyčajné príspevky, so sociálnou interakciou votkanou do toho istého prúdu udalostí.[11] Viacerí autori môžu uverejniť konkurenčné heslá wiki na tú istú tému a čitatelia si vyberú, ktorej verzii veria, podľa signálov reputácie, ktoré už používajú na všetko ostatné.[12] Priestory v reálnom čase ako HiveTalk a Nostr Nests overujú účasť cez existujúci pár kľúčov používateľa a na riadenie prístupu alebo na prepitné zapájajú Lightning.[30] Zoznam je dlhý a stále rastie, no tvar každého prípadu je rovnaký.

Všetko to spája reputácia. Tento rozsah je možný vďaka tomu, že všetky aplikácie naraz obsluhuje jediná identita a jediná sieť relayov s jedným sociálnym grafom pod nimi všetkými, a nie každá aplikácia s vlastnou kópiou infraštruktúry. Pár kľúčov, ktorý v jednom kontexte nazbieral dôveru, ju prenáša do ďalšieho, a používateľ môže identity podľa kontextu oddeliť, ak chce oddelenie. Protokol nevie, čo ktorý obsah znamená. Vie len, že je podpísaný a že ho niektoré relaye ochotne prenášajú. Všetko ostatné závisí od toho, ktorí klienti implementujú ktoré druhy udalostí a či ich používatelia považujú za dosť užitočné na to, aby pritiahli ďalších vývojárov, ktorí funkciu pridajú do vlastných klientov.

Schémy súkromných správ rozširujú tú istú infraštruktúru. Šifrované priame správy (NIP-17 so šifrovaním NIP-44) a protokol Marmot na škálovateľné šifrované skupinové správy bežia ako špecializované druhy uda-

lostí na tej istej architektúre podpísaných udalostí a relayov. Verejné použitie bez povolenia aj súkromné šifrované použitie sú špecializácie toho istého systému a rozsah viditeľný dnes je malým zlomkom toho, čo protokol pripúšťa. Táto šírka prináša vlastnosti súkromia, ktoré architektúra predvolene neposkytuje, a práve im sa priamo venuje nasledujúci oddiel.

21.8 Obmedzenia súkromia

Pseudonymné, nie anonymné

Nostr poskytuje pseudonymitu, nie anonymitu. Verejný kľúč je trvalý identifikátor a každá podpísaná udalosť sa na ten kľúč viaže. Postupom času sa vzorce správania, štýl písania, načasovanie a spojenia v sociálnom grafe nazbierajú do profilu, ktorý možno deanonymizovať.

Nové kľúče zaručujú neprepojiteľnosť s predošlou identitou, ale na úkor nahromadenej reputácie. Používateľ, ktorý kľúč opustí, aby unikol sledovaniu, príde o graf sledovaných, históriu príspevkov a postavenie v sieti dôvery, ktoré budoval dlho. Tento kompromis nie je chyba návrhu, ale štrukturálna vlastnosť každého systému s trvalou identitou: tá istá kontinuita, vďaka ktorej je reputácia čitateľná, robí správanie vysledovateľným.

Vystavenie sociálneho grafu

Zoznamy sledovaných, zdieľania, odpovede aj zapy odhaľujú sociálne väzby otvorene. Aj pozorovateľ, ktorý nečíta nijaký obsah, vie zmapovať štruktúru komunity tým, že sleduje, kto s kým komunikuje, ako často a cez ktoré relaye. Graf sledovaných sa uverejňuje ako udalosť druhu 3 a replikuje sa na každý relay, na ktorý používateľ uverejňuje. Kto sa na tieto relaye opýta, dostane celý zoznam. Vzorce reakcií obraz spresňujú: používateľ, ktorý dôsledne posiela zapy a odpovedá malému zhluku účtov, prezradí príslušnosť, aj keby bola každá správa v tom zhluku šifrovaná.

Niektorí klienti podporujú šifrované zoznamy sledovaných podľa NIP-51, no prijatie je nerovnomerné a väčšina používateľov uverejňuje sociálny graf otvorene, bez toho, aby si uvedomovala, čo tým odhaľuje.[27] Toto vystavenie nie je pre návrh protokolu Nostr vedľajšie. Je to mechanizmus, ktorým funguje filtrovanie podľa siete dôvery a objavovanie obsahu. Používatelia, ktorí potrebujú súkromie grafu, si ho musia nastaviť zámerne a prijať, že tým zhoršia funkcie objavovania a reputácie, ktoré na verejnom grafe závisia.

Prevádzkovatelia relayov vidia všetko

Relaye dostávajú udalosti v otvorenom texte a majú plný prehľad o prevádzke, ktorú vybavujú. Prevádzkovateľ relayu vidí, ktoré verejné kľúče uverejňujú aký obsah, ktoré adresy IP žiadajú ktoré udalosti, načasovanie a frekvenciu všetkých interakcií a vznikajúci tvar sociálneho grafu

medzi jeho používateľmi. Táto viditeľnosť vyplýva z toho, že relaye slúžia ako vrstva ukladania a doručovania bez samostatnej anonymizačnej vrstvy pod nimi.

Staršie priame správy podľa NIP-04 používali AES-256-CBC bez autentifikačného kódu správy, takže šifrový text bolo možné upravovať, a šifrovací kľúč odvodzovali z neštandardnej konštrukcie ECDH, ktorá sa odchyľovala od predvoleného nastavenia libsecp256k1. NIP-44 ich nahradil autentifikovaným šifrovaním ChaCha20 s HMAC-SHA256 a riadnym odvodzovaním kľúča pomocou HKDF. Audit NIP-44 od firmy Cure53 zverejnený v decembri 2023 návrh potvrdil.[28] NIP-44 je šifrovací stavebný prvok, nie úplný protokol na výmenu správ. Samotný by nechal identitu odosielateľa viditeľnú pre relaye. NIP-17 skladá šifrovanie NIP-44 so zabalením podľa NIP-59 (gift wrap), aby túto medzeru zacelil: vonkajšiu udalosť (druh 1059) podpisuje nový jednorazový pár kľúčov, jej časová značka `created_at` je náhodne posunutá až o dva dni do minulosti a značka `p` určuje iba príjemcu.[29] Relay, ktorý obsluhuje správy NIP-17, nevidí ani identitu odosielateľa, ani skutočný čas, len to, kedy udalosť na relay prvýkrát dorazila. Obsah aj odosielateľ sú pred relayom skryté.

Zostávajúce vystavenie je na úrovni siete. Relay stále vidí adresu IP, ktorá sa pripojila, aby zabalenú správu doručila alebo prevzala, a používatelia, ktorí uverejňujú na vyhradený relay pre schránku priamych správ (druh 10050), prezrádzajú, že práve tento relay treba sledovať. Kto má pozorovacie body medzi používateľom a týmto relayom, môže priradiť načasovanie spojení k doručeniu správ, aj keď obsah neprečíta.

Verejný dosah ako predvolený postoj

Štandardný postup v Nostre rozosiela poznámky na viaceré relaye, aby dosiahli čo najširšie publikum, a každý relay, ktorý udalosť nesie, ju poskytne komukoľvek, kto sa na ňu opýta. Používateľ, ktorý uverejní poznámku v domnienke, že sa bude šíriť len medzi jeho sledujúcimi, ju v skutočnosti odovzdal každému relayu zo svojho zoznamu na uverejňovanie. Šifrované alternatívy opísané vyššie (priame správy NIP-17, skupinové správy Marmot) existujú ako rozšírenia protokolu, ale vyžadujú zámerné nastavenie a podporu klienta. Používatelia, ktorí prídu s očakávaním predvoleného súkromia, odhalia viac, než chcú, ak si tieto alternatívy výslovne nezvolia.

Marmot: MLS nad Nostrom

Kapitola 17 predstavila Messaging Layer Security, štandard IETF na škálovateľné skupinové šifrovanie. MLS samo o sebe poskytuje dopredné utajenie (forward secrecy), bezpečnosť po kompromitácii a skupinové operácie so zložitosťou O(log N), ale zámerne necháva dve úlohy na okolitý sys-

tém: overovať, kto je členom skupiny, a doručovať šifrový text bez úniku sociálneho grafu. Protokol Marmot používa na obe Nostr.[13]

Marmot berie pár kľúčov Nostr ako autentifikačnú službu MLS: dlhodobý identitný kľúč Nostr používateľa zakotvuje jeho poverenie v MLS, takže v procese nie je telefónne číslo, e-mailová adresa ani certifikačná autorita. Relaye siete Nostr berie ako doručovaciu službu MLS: prenášať prevádzku môže ktorýkoľvek relay, ktorý prijíma druhy udalostí protokolu, a nijaký konkrétny relay sa nevyžaduje. Protokol pokrývajú tri druhy udalostí. Udalosti KeyPackage (druh 30443) sa uverejňujú vopred, aby ostatní mohli používateľa pridať do skupiny asynchrónne, podobne ako model prekľúčov v Signale. Udalosti Welcome (druh 444) sa doručujú novým členom zabalené podľa NIP-59, ktoré používa vrstvenie v štýle cibule, aby pred relayami, ktoré ich smerujú, skrylo odosielateľa. Skupinové správy (druh 445) nesú samotný užitočný obsah MLS.[14]

Referenčnou implementáciou je Marmot Development Kit (MDK), knižnica v Ruste postavená na OpenMLS. Vlajkový klient White Noise vychádza na iOS a Android a ten istý backend v Ruste používa aj cez terminálového klienta pre stolové počítače. Firma Least Authority zverejnila medzi novembrom 2025 a aprílom 2026 tri hodnotenia tohto projektu, ktoré pokrývajú špecifikáciu, knižnicu MDK a backend whitenoise-rs.[15]

Dve rozhodnutia v návrhu dávajú Marmotu ochranu metadát, akú samotné MLS neposkytuje. Po prvé, podpisový kľúč MLS vo vnútri KeyPackages a listových uzlov je odlišný od dlhodobého identitného kľúča Nostr používateľa, takže neskoršia kompromitácia kľúča Nostr neodhalí minulú ani budúcu skupinovú prevádzku, ani to, v ktorých skupinách bol používateľ členom. Po druhé, každá skupinová správa sa uverejňuje pod novým jednorazovým párom kľúčov Nostr namiesto identitného kľúča používateľa a verejný identifikátor skupiny je meniteľné pseudo-ID namiesto skutočného ID skupiny v MLS. Prevádzkovateľ relayu, ktorý sleduje prúd udalostí, vidí šifrový text označený meniacou sa značkou, bez trvalého odosielateľa či stabilného označenia skupiny, podľa ktorých by sa dalo zhlukovať. V spojení s natívnym dopredným utajením a bezpečnosťou po kompromitácii v MLS to zacelí väčšinu medzery medzi šifrovaním obsahu a súkromím metadát.

Zvyškový únik je v samotnom odbere. Klient, ktorý je v niekoľkých skupinách Marmot, odoberá meniacu sa značku `h` každej skupiny v jednom filtri REQ, aby jediné spojenie mohlo doručovať prevádzku zo všetkých. Relay, ktorý ten filter číta, vidí množinu identifikátorov skupín, ktoré klient sleduje, a relay, ktorý obsluhuje veľa používateľov, môže relácie zhlukovať podľa prekrytia ich sledovaných skupín, aj keď sa každý identifikátor skupiny mení a každú udalosť podpisuje nový jednorazový kľúč. Dvaja používatelia, ktorých množiny odberov sa prekrývajú na rovnakej hŕstke skupín, sú viditeľne členmi tých istých skupín, a používateľ, ktorý

odoberá osobitný zhluk skupín, sa identifikuje naprieč reláciami, aj keď jeho prenos beží cez Tor. Štrukturálnym riešením je súkromné získavanie informácií (PIR): s PIR nad relayami siete Nostr by klient mohol stiahnuť udalosti pre množinu skupín bez odhalenia, o akú množinu ide, a prerušil by tak poslednú oporu pre analýzu prevádzky, ktorú Marmot necháva relayu.

Vezmime štandardný protokol skupinového šifrovania, ktorý ide cestou štandardizácie, a zložme ho s prenosom, ktorý nemôže vypnúť žiadny jediný subjekt. Výsledkom je škálovateľná skupinová komunikácia s doprednym utajením a skrytými metadátami, ktorej vrstva identity je pod vlastnou kontrolou používateľov a vrstva doručovania nie je ničím majetkom. Presne tam smeroval vývoj opísaný v kapitole 17, až na vrstvu PIR, ktorá by zavrela únik cez odbery.

Metadáta na úrovni siete

Každé spojenie WebSocket s relayom nesie adresu IP klienta a prevádzkovatelia relayov ju môžu zaznamenávať spolu s používaným verejným kľúčom. Bez Toru alebo VPN môžu prevádzkovatelia relayov aj každý sieťový pozorovateľ medzi klientom a relayom prepojiť verejný kľúč so sieťovou polohou a odtiaľ s fyzickou adresou alebo účtom u poskytovateľa internetu. Problém sa pri viacerých relayoch stupňuje: používateľ, ktorý sa z jednej adresy IP pripája k piatim relayom, spojil päť nezávislých záznamov prevádzkovateľov do jediného profilu identity, aj keď si inak dáva pozor, aby svoju aktivitu medzi tými relayami oddelil.

Protokol neukladá nijakú povinnosť anonymizácie a neposkytuje vstavané súkromie prenosu. Používatelia, ktorí chcú ochranu na úrovni IP, musia spojenia viesť cez Tor alebo dôveryhodnú VPN, ešte než dosiahnu relay, a musia to robiť dôsledne. Stačí jediné nechránené spojenie s relayom, ktorý už ten istý verejný kľúč videl cez Tor, a pseudonym je prelomený. Zodpovednosť nesie výlučne používateľ.

Čo môžu urobiť klienti: Tor, ZK autentifikácia, súkromné získavanie

Súkromie v Nostre je problém klienta, keďže protokol ho necháva na aplikačnú vrstvu. Najjednoduchšie zmiernenie je viesť každé spojenie s relayom cez Tor alebo dôveryhodnú VPN, takže adresa IP zaznamenaná v relayi je výstupný uzol Toru alebo výstup VPN, nie domáca adresa používateľa. Klient, ktorý to robí dôsledne od prvého spojenia, prevádzkovateľovi relayu navždy zabráni priradiť verejný kľúč k sieťovej polohe. Viacerí klienti pre Nostr dodávajú podporu Toru, buď ako vstavaný prenos, alebo odkazom na celosystémové nastavenie Orbot či Tails.[31] Cenou je latencia a disciplína používať chránenú cestu zakaždým, lebo jediné nechránené spojenie prepojí pseudonym späť s jeho skutočným sieťovým domovom.

Hlbšie rozšírenia protokolu sú možné, ale zatiaľ nie sú nasadené vo veľkom. Niekoľko stavebných prvkov z kryptografickej literatúry rieši to, čo relay o pripojenom klientovi dnes vidí: identitu oprávneného používateľa na linke a obsah jeho odberu.[19]

Dôkazy členstva v skupine s nulovou znalosťou skryjú, ktorý oprávnený používateľ sa pripája. Semaphore, konštrukcia overená vo veľkom v projekte Worldcoin, umožňuje relayu zverejniť koreň Merkleovho stromu oprávnených verejných kľúčov a klientovi dokázať „som jedným z týchto členov“, bez odhalenia, ktorým. Nullifier odvodený na epochu zo súkromného kľúča používateľa chráni pred spamom: dva dôkazy z toho istého kľúča v tej istej epoche dávajú ten istý nullifier, takže relay môže duplikáty odmietnuť, bez toho, aby zistil skrytú identitu. Dôkazy na mobile sa generujú niekoľko sekúnd a overujú v milisekundách a knižnice už existujú. Chýba NIP a prijatie.

Súkromné získavanie informácií rieši ťažší problém, totiž ako skryť, čo klient sťahuje. V schéme PIR klient zakóduje dopyt ako vektor a relay nad celou svojou databázou udalostí vykoná výpočet, ktorý vráti požadovaný záznam bez toho, aby zistil, o ktorý index ide. Schémy ako SimplePIR a FrodoPIR priviedli PIR s jedným serverom do rozsahu praktického nasadenia pre ohraničené vzorce dopytov, s latenciou pod sekundu pri stredne veľkých úložiskách. Výpočet na serveri rastie s veľkosťou databázy a komunikačná réžia je o rád vyššia než veľkosť získaných údajov. Táto cena robí PIR použiteľným pre dopyty s vysokou hodnotou (stiahnutie konkrétnej šifrovanej schránky, získanie určitého vlákna), nie pre odbery typu firehose, ktoré sťahujú tisíce udalostí. Prispôsobiť PIR modelu dopytov v sieti Nostr, ktorý funguje na báze odberov, je otvorený výskumný problém, nie riešenie pripravené na nasadenie.

Tieto zmiernenia sa skladajú. Tor skryje IP. ZK autentifikácia skryje, ktorý oprávnený používateľ je na linke. PIR skryje, čo číta. Žiadne z nich nie je samo osebe úplným riešením a nasadiť sa dnes dá Tor na úrovni prenosu, pričom ZK autentifikáciu možno dosiahnuť novým NIP. PIR ostáva ťažším otvoreným problémom a klient dbajúci na súkromie by dnes mal minimálne predvolene používať Tor a plochu dopytov viditeľnú pre relay považovať za stále odhalenú.

Kompromis

Nostr optimalizuje odolnosť voči cenzúre a kontrolu používateľa, nie súkromie. Používatelia vlastnia svoju identitu a nedajú sa vyradiť z platformy, no ich aktivita je široko viditeľná. Je to rozumný kompromis pre verejnú sociálnu komunikáciu, kde cieľom je často dosah, nie skrývanie. Používatelia, ktorí potrebujú silné súkromie, by mali Nostr používať opatrne a doplniť ho nástrojmi na ochranu súkromia, alebo na citlivé interakcie použiť účelovo vytvorené súkromné komunikačné systémy.

21.9 Prečo alternatívy nestačia

Mastodon: federovaný, ale závislý od servera

Mastodon používa federáciu: nezávislé servery komunikujú cez protokol ActivityPub.[16] Používatelia sa registrujú na serveroch (inštanciách), ktoré si medzi sebou preposielajú obsah.

Identita závisí od servera. Identitou je „`user@server.example`“ (server je súčasťou adresy). Ak server zanikne alebo používateľa zablokuje, táto identita je preč. Mastodon pridal v roku 2019 migráciu účtu, ktorá používateľom umožňuje presunúť sa na nový server a preniesť si počet sledujúcich, no obsah sa nemigruje: príspevky a vlákna odpovedí zostávajú na pôvodnom serveri a sú nedostupné, ak ten server prestane fungovať. Migrácia navyše vyžaduje, aby starý server ešte bežal a spolupracoval. Server, ktorý náhle zanikne alebo používateľa najprv zablokuje, migráciu znemožní.

Praktické dôsledky sú vidieť. Keď veľké inštancie Mastodonu zanikli (mastodon.social v roku 2022 pod záťažou dočasne uzavrel registrácie a desiatky menších inštancií zanikli s minimálnym upozornením), ich používatelia prišli o archívy obsahu a často aj o vzťahy so sledujúcimi. Federovaný model rozdeľuje kontrolu prevádzkovateľov medzi mnoho serverov, čo je lepšie než jediná platforma, no identita je stále poverenie, ktoré vydáva prevádzkovateľ servera. Používatelia, ktorí sa často sťahujú za lepším moderovaním či spoľahlivosťou, pri každom presune strácajú históriu obsahu. Mastodon rozdeľuje kontrolu medzi prevádzkovateľov serverov a používateľom nedáva kontrolu nad vlastnou identitou.

Bluesky: dôveryhodná možnosť odchodu, nie dnešná decentralizácia

Bluesky používa otvorený protokol (AT Protocol) s inou architektúrou než Nostr.[17] Kým udalosti v sieti Nostr sú jednoduché podpísané textové súbory, ktoré môže ktorýkoľvek relay uložiť nezávisle, ATProto používa model „zdieľanej haldy“ (shared heap): relaye musia agregovať a indexovať údaje celej siete, aby fungovali. Táto architektonická voľba vytvára vnútorný tlak na centralizáciu bez ohľadu na otvorenosť protokolu.

Rozdiel sa prejavuje v nárokoch na zdroje. Plný relay ATProto vyžaduje úložisko v rádoch terabajtov, ktoré rastie zhruba o osemnásť gigabajtov denne, a plný App View, teda služba, ktorá vykresľuje prúdy príspevkov, pridáva k tomu indexovaciu infraštruktúru za státisíce dolárov. Po väčšinu histórie siete prevádzkovala jediný plný relay celej siete spoločnosť Bluesky PBC. Bluesky dodnes prevádzkuje dominantný firehose a v skutočnosti prevádzkuje vo svojich dátových centrách viacero vlastných inštancií plného relayu. Koncom roku 2025 sa to zmenilo, keď Blacksky spustil druhý nezávislý plný relay celej siete na vlastnej implementácii v Ruste (rsky-relay), čo v októbri 2025 potvrdila aj samotná kontrola protokolu

(protocol check-in) od Bluesky PBC.[18] Popri týchto relayoch vznikli tisíce osobných dátových serverov, no väčšina z nich hostí jeden či dva účty a na dosiahnutie širšej siete stále závisí od väčších relayov a App Views.

Identita v ATProto je prenosnejšia než v Mastodone: používatelia majú DID (decentralizované identifikátory), ktoré teoreticky umožňujú migráciu medzi servermi bez straty sledujúcich. Migrácia účtu v praxi funguje. Adresár PLC (Public Ledger of Credentials), centralizovaná služba, ktorá ukladá záznamy operácií PLC a poskytuje dokumenty DID vrátane koncových bodov služieb a materiálu kľúčov, však ostáva pod kontrolou Bluesky PBC. Pri účtoch hostených na Bluesky sa spoločnosť stále zvyčajne podieľa na správe a obnove kľúčov. Bluesky hovorilo o prenesení správy PLC na nezávislé švajčiarske združenie, čím súčasnú centralizáciu uznáva.

Bluesky dnes zdôrazňuje prenosnosť a dôveryhodnú možnosť odchodu viac než plne decentralizovanú prevádzku: zabezpečiť, aby používatelia a vývojári mohli v prípade potreby odísť, nie že sieť už dnes funguje bez ústrednej kontroly. Blacksky buduje aj paralelný stack nad rámec relayu, vrátane vlastného PDS, labelera, vlastných prúdov príspevkov a App View, ktorý je vo vývoji, a iniciatíva Free Our Feeds oznámila ďalšiu infraštruktúru, ktorá má nasledovať. Architektúra súťaž umožňuje a dôkaz o tom, že druhý nezávislý plný relay celej siete je prevádzkovo udržateľný, už existuje. Väčšina dnešnej prevádzky sa stále sústreďuje v dominantnom relayi, ale „jediný" už situáciu nevystihuje.

Riešenia na blockchaine: nesprávny nástroj na sociálnu koordináciu

Niektoré sociálne protokoly používajú blockchainy, no to odráža kategoriálnu chybu v tom, čo sociálna komunikácia vyžaduje.

Globálny konsenzus sociálna komunikácia nepotrebuje. Hlavná inovácia blockchainu je riešenie dvojitého míňania globálnym konsenzom, čo znamená, že každý účastník sa musí zhodnúť na jedinej histórii transakcií. Pre peniaze je táto záruka nevyhnutná, lebo tú istú mincu nemožno minúť dvakrát. Sociálne príspevky takéto obmedzenie nemajú. Správa môže existovať na viacerých serveroch bez toho, aby vznikol rozpor. Nie je tu čo „minúť dvakrát".

Architektúra blockchainu navyše vynucuje replikáciu údajov, pri ktorej musia všetci účastníci sťahovať všetky údaje. Každý uzol ukladá celú históriu. Pri peňažných transakciách to zaisťuje, že nikto nemôže podvádzať, pri sociálnych príspevkoch to znamená, že každý používateľ musí ukladať obsah každého iného. To sa škáluje katastrofálne a nemá to nijaký účel.

Model globálneho konsenzu vytvára plné vystavenie metadát. Každá transakcia aj každé sledovanie účtu je viditeľné pre každého účastníka. V peňažných systémoch táto transparentnosť umožňuje overovanie, v sociálnych systémoch vytvára sledovanie v plnom rozsahu. Používate-

lia sa nemôžu selektívne podeliť len s dôveryhodnými stranami, keď architektúra vyžaduje univerzálne vysielanie.

Napokon používanie blockchainu zvyčajne vyžaduje tokeny, čo do komunikácie vnáša finančné trenie a láka špekulácie, ktoré skresľujú používanie.

Nostr tieto vlastnosti obracia. Používatelia ukladajú udalosti len na relaye, ktoré ovládajú alebo im dôverujú, a nikde sa nevyžaduje, aby ich videli ostatní. Alice môže uverejniť príspevok na svojom osobnom relayi bez toho, aby ho vysielala svetu, a táto selektívna viditeľnosť je presne to, čo sociálna komunikácia potrebuje a čomu architektúra blockchainu bráni.

Prečo jednoduchosť Nostru prináša výhody

Celý povrch protokolu Nostr tvorí podpísaný súbor JSON a spojenie WebSocket s relayom. Vývojár dokáže implementovať fungujúceho klienta za víkend podľa špecifikácie, ktorá sa zmestí do jediného dokumentu. ActivityPub a ATProto si každý vynucujú zložitú logiku federácie alebo rozsiahlu infraštruktúru na indexovanie firehose a protokoly na blockchaine k tomu pridávajú plnú účasť na vrstve konsenzu. Nostr nevyžaduje nič z toho, a preto je sieť klientov široká: tisíce nezávislých implementácií súťažia dizajnom a cieľovým publikom a každá môže dosiahnuť celú sieť bez osobitného prístupu.

Aj škálovanie relayov je nezávislé. Každý relay ukladá len to, čo sa rozhodne uložiť, a obsluhuje len vlastných používateľov. Relay nemusí o ostatných relayoch vedieť ani sa s nimi koordinovať. Malý osobný relay pre päťdesiat používateľov beží na lacnom VPS a zvláda záťaž bez ohľadu na to, čo robí veľký relay pre milión používateľov. Náklady na zdroje rastú s obsluhovaným publikom, nie s veľkosťou celej siete, preto je prekážka prevádzkovať infraštruktúru dosť nízka pre jednotlivcov a nadšencov.

Zhrnutie kapitoly

Nostr rieši problém zachytenia identity návrhom protokolu. Identita je pár kľúčov pod kontrolou používateľa, obsah je podpísaný a distribuuje sa cez relaye, ktoré si používateľ vyberie, a odísť sa dá bez straty identity. Relay môže prevádzkovať ktokoľvek a moderovanie prebieha na vrstve relayov a klientov prostredníctvom trhových služieb namiesto autority na úrovni protokolu. Reputácia vzniká zo siete dôvery a z overenia cez doménu namiesto odznakov platformy. Architektúra podpísaných udalostí je dosť jednoduchá na to, aby tá istá infraštruktúra popri krátkych sociálnych príspevkoch niesla aj dlhé články, inzeráty, živé video, heslá wiki, zvukové miestnosti, vydania softvéru a šifrované skupinové správy. Jeden pár kľúčov môže slúžiť na mnohé účely a prenášať reputáciu naprieč kontextmi a systém NIP umožňuje vývoj protokolu bez ústrednej autority.

Alternatívy zaostávajú z rôznych dôvodov: Mastodon necháva identitu závislú od servera, referenčná architektúra Bluesky vytvára veľké nároky na relaye a indexovanie, ktoré dodnes koncentrujú veľkú časť siete, aj keď sa prenosnosť zlepšuje, a riešenia na blockchaine vnucujú požiadavky globálneho konsenzu, ktoré sociálna komunikácia nepotrebuje.

Obmedzenia súkromia sú skutočné. Nostr poskytuje pseudonymitu, nie anonymitu. Prevádzkovatelia relayov vidia metadáta a sociálny graf je z veľkej časti verejný. Trvalé kľúče zhromažďujú vzorce správania, ktoré sa časom skladajú do identifikovateľných profilov. Správa kľúčov ostáva nevyriešená: strata kľúča je trvalá a kompromitácia nenapraviteľná, zatiaľ čo konvencie rotácie sú u klientov nejednotné. Tieto problémy sú vlastné systémom identity pod vlastnou kontrolou používateľa a zatiaľ pre ne neexistujú vyspelé riešenia. Protokol Marmot rieši šifrované skupinové správy a skrývanie metadát priamo tým, že skladá MLS so sieťou relayov siete Nostr. Samotný protokol optimalizuje odolnosť voči cenzúre a kontrolu používateľa. Používatelia, ktorí potrebujú silné súkromie, ho dopĺňajú nástrojmi na anonymizáciu alebo účelovo vytvorenými súkromnými systémami.

Napriek decentralizovanému návrhu existujú súčasné sklony k centralizácii. Väčšinu prevádzky nesie niekoľko veľkých relayov a väčšinu používateľov priťahuje niekoľko klientov. Objavovanie obsahu prechádza cez hŕstku indexovacích služieb a reprodukuje tak vzorec koncentrácie, ktorému mal protokol na vrstve identity zabrániť. Či trhová súťaž udrží dosť alternatív, aby sa zabránilo opätovnej koncentrácii, je empirická otázka, na ktorú samotný protokol odpovedať nemôže. Nostr na úrovni protokolu ukazuje, že zložitá koordinácia môže vzniknúť z jednoduchej infraštruktúry bez ústrednej kontroly a že používatelia si môžu zachovať sieťové efekty s menším uzamknutím u platformy a pritom držať identity, ktoré sú zároveň pod ich vlastnou kontrolou a sociálne užitočné. Tento vzorec platí všeobecnejšie než len pre sociálne siete.

Poznámky

[1] fiatjaf, „nostr“, dostupné na `https://fiatjaf.com/nostr.html`. Špecifikácia protokolu na `https://github.com/nostr-protocol/nostr`.

[2] Pew Research Center, „Social Media Use in 2025“, `https://www.pewresearch.org/internet/`. Údaje 84 % pre YouTube a 71 % pre Facebook pochádzajú z výročných prieskumov Pew o sociálnych sieťach. Platformy Meta s viac než miliardou aktívnych používateľov mesačne k roku 2025: Facebook, Instagram, WhatsApp a Messenger; pozri Meta Platforms, Inc., štvrťročné správy o hospodárskych výsledkoch, `https://investor.fb.com/`.

[3] Matt Taibbi a kol., „The Twitter Files“, uverejnené ako séria vlákien na Twitter/X, december 2022 až marec 2023. Kľúčové diely zdokumentovali portál FBI na podávanie žiadostí Twitteru (Taibbi, 2. decembra 2022), systémy filtrovania viditeľnosti (Bari Weiss, 8. decembra 2022) a účty vplyvových operácií Ústredného velenia USA na bielej listine (Lee

Fang, 20. decembra 2022). Hlavný index vlákien viedol *Racket News* (Matt Taibbi, december 2022 až marec 2023).

[4] Špecifikácia protokolu Nostr, dostupná na `https://github.com/nostr-protocol/nostr`. Protokol prvýkrát opísal fiatjaf v roku 2020; repozitár obsahuje základnú špecifikáciu a všetky NIP.

[5] Súhrn siete klientov Nostr k roku 2026. Mobilné: Damus (`https://damus.io`, iOS, jeden z pôvodných klientov), Amethyst (`https://github.com/vitorpamplona/amethyst`, Android), Primal (`https://primal.net`, multiplatformový, s cachovacou službou a vstavanou peňaženkou Lightning), Nos (`https://nos.social`), Freefrom, 0xChat. Desktopové a webové: Coracle (`https://coracle.social`), Snort (`https://snort.social`), Iris (`https://iris.to`), Primal (web), Nostrudel (`https://nostrudel.ninja`), Jumble. Dlhé texty a publikovanie: Habla (`https://habla.news`), Yakihonne (`https://yakihonne.com`), Highlighter, Stemstr (hudba). Trhoviská a obchod: Shopstr, Plebeian Market. Video a streamovanie: Flare, Zap.Stream, Nostr.Build (hosting médií). Rozšírenia prehliadača na podpisovanie: nos2x (`https://github.com/fiatjaf/nos2x`), Alby (`https://getalby.com`), ktorý rieši aj Lightning. Infraštruktúra vzdialeného podpisovateľa na oddelenie kľúčov: nsec.app a protokol bunker (NIP-46). Autoritatívny adresár a index: `https://nostrapps.com` zoraďuje klientov podľa platformy a kategórie; `https://nips.nostr.com` indexuje štandardy, ktoré každý klient implementuje. Správy o protokole a jeho priebežnom vývoji sledujú `https://nostr.how` a podcast Knowledge Is Golden na `https://nostr.fm`.

[6] Nostr Implementation Possibilities (NIPs), dostupné na `https://github.com/nostr-protocol/nips`.

[7] Systémy reputácie založené na sieti dôvery nepovažujú reputáciu za vlastniteľný majetok. Rámec, ktorý rozvíja kapitola 6, vylučuje vlastnícke práva k reputácii, pretože reputácia pozostáva z toho, čomu veria iní ľudia, a nie je vzácnym, rivalitným zdrojom. Graf dôvery nenesie nárok na majetok, ale empirický signál: podpísané potvrdenia a dôsledné správanie v čase, na základe ktorých si ostatní používatelia tvoria vlastný úsudok. Rovnaký princíp vylučuje aj právo proti ohováraniu ako koherentný rámec ochrany tohto signálu: na nepravdivé tvrdenie sa odpovedá protitvrdením a vlastným posúdením dôvery čitateľa, nie štátnym vynucovaním voči hovoriacemu. Pozri Stephan Kinsella, „Defamation as a Type of Intellectual Property“, in Jörg Guido Hülsmann a Stephan Kinsella, eds., *A Life in Liberty: Liber Amicorum in Honor of Hans-Hermann Hoppe* (Mises Institute, 2024), citované v kap. 6, pozn. 11; a Murray N. Rothbard, „Knowledge, True and False“, in *The Ethics of Liberty* (NYU Press, 1998), kap. 16.

[8] NIP-05: Mapping Nostr keys to DNS-based internet identifiers, dostupné na `https://github.com/nostr-protocol/nips/blob/master/05.md`.

[9] NIP-23: Long-form Content, dostupné na `https://github.com/nostr-protocol/nips/blob/master/23.md`. Definuje adresovateľné udalosti pre články a blogové príspevky vo formáte Markdown.

[10] NIP-99: Classified Listings, dostupné na `https://github.com/nostr-protocol/nips/blob/master/99.md`. Implementácie zahŕňajú Shopstr a Plebeian Market.

[11] NIP-53: Live Activities, dostupné na `https://github.com/nostr-protocol/nips/blob/master/53.md`. zap.stream poskytuje referenčnú implementáciu živého video streamovania s integráciou Lightning.

[12] NIP-54: Wiki, dostupné na `https://github.com/nostr-protocol/nips/blob/master/54.md`. Umožňuje decentralizované encyklopedické heslá s kuráciou podľa siete dôvery.

[13] The Messaging Layer Security (MLS) Protocol, RFC 9420, Internet Engineering Task Force (IETF), júl 2023, dostupné na `https://datatracker.ietf.org/doc/rfc9420/`. Dokument o architektúre pozri RFC 9750.

[14] The Marmot Protocol, dostupné na `https://github.com/marmot-protocol/marmot`. Marmot stavia na OpenMLS, implementácii protokolu MLS v Ruste, a spája skupinové šifrovanie s architektúrou relayov v sieti Nostr.

[15] Least Authority, „Audit of White Noise Marmot Protocol Review“, 7. novembra 2025; „Audit of the Marmot Development Kit“, 20. marca 2026; a „Audit of whitenoise-rs“, 7. apríla 2026, všetko na `https://leastauthority.com/blog/`. O zmenách, ktoré audity vyvolali v kóde, pozri „What the Least Authority Audit Changed“, blog White Noise, `https://whitenoise.chat/blog`, s odkazmi na PR vrátane whitenoise-rs#539, #540, #548, #634, #637, #638, #642 a #665 a marmot#38 („MIP-00/02/03: align spec with audit findings“). Publikované audity Least Authority zahŕňajú špecifikácie Zcash a Ethereum 2.0; pozri `https://leastauthority.com/security-consulting/published-audits/`. Správcovia protokolu naďalej označujú Marmot za experimentálny a MDK za alfa, kým po auditoch nenastane obdobie stability špecifikácie.

[16] Dokumentácia Mastodonu, dostupná na `https://docs.joinmastodon.org/`. ActivityPub je štandardný federačný protokol W3C na `https://www.w3.org/TR/activitypub/`.

[17] Bluesky a AT Protocol, dostupné na `https://atproto.com/`.

[18] Bluesky Protocol Team, „Protocol Check-in (Fall 2025)“, blog atproto.com, 20. októbra 2025, potvrdzuje, že „Blacksky currently runs a full-network relay (using the rsky-relay implementation!)“ a buduje plný App View celej siete. K stacku Blacksky pozri `https://github.com/blacksky-algorithms/rsky` a `https://docs.blacksky.community`. O plánovanej ďalšej infraštruktúre pozri projekty Free Our Feeds a Eurosky na `https://freeourfeeds.com`. K širšiemu smerovaniu decentralizácie: Bluesky PBC zakladá nezávislé švajčiarske združenie, ktoré bude prevádzkovať adresár identít PLC (atproto.com/blog/plc-directory-org, september 2025), a pracovná skupina IETF ATP bola zriadená v apríli 2026.

[19] Semaphore: pozri Privacy and Scaling Explorations, „Semaphore Protocol“, `https://docs.semaphore.pse.dev/`, a auditovanú implementáciu na `https://github.com/semaphore-protocol/semaphore`. PIR s jedným serverom s latenciou pod sekundu na praktických databázach: Alexandra Henzinger, Matthew M. Hong, Henry Corrigan-Gibbs, Sarah Meiklejohn a Vinod Vaikuntanathan, „One Server for the Price of Two: Simple and Fast Single-Server Private Information Retrieval“ (SimplePIR), 32nd USENIX Security Symposium, 2023; a Alex Davidson, Gonçalo Pestana a Sofía Celi, „FrodoPIR: Simple, Scalable, Single-Server Private Information Retrieval“, Proceedings on Privacy Enhancing Technologies, 2023. Praktická komunikácia so skrytými metadátami s dvoma servermi: Saba Eskandarian, Henry Corrigan-Gibbs, Matei Zaharia a Dan Boneh, „Express: Lowering the Cost of Metadata-Hiding Communication with Cryptographic Privacy“, USENIX Security Symposium, 2021.

[20] Koordinované odstránenie Alexa Jonesa a obsahu InfoWars z Apple Podcasts, Facebooku, YouTube a Spotify 5. a 6. augusta 2018 prebehlo v 12-hodinovom okne bez predchádzajúcej verejnej koordinácie. Odstránením z YouTube zanikol kanál s približne 2,4 milióna odberateľov; Apple odstránil päť zo šiestich podcastových kanálov Jonesa z iTunes; Spotify odstránil všetok obsah InfoWars. Dobové spravodajstvo: Oliver Darcy, „Apple, YouTube, Facebook and Spotify take action against Alex Jones and InfoWars in a single day“, *CNN Business*, 6. augusta 2018. Jones si ponechal prístup na Twitter/X do 6. septembra 2018;

pozri vyhlásenie Twitteru v správe Casey Newton, „Twitter bans Alex Jones and InfoWars“, *The Verge*, 6. septembra 2018. Táto udalosť je najjasnejším zdokumentovaným prípadom súčasného vyradenia z viacerých platforiem, ktorý predchádzal akýmkoľvek formálnym dohodám medzi platformami o moderovaní obsahu.

[21] Amazon Web Services ukončil hostingovú zmluvu s Parlerom s účinnosťou od 10. januára 2021 s odkazom na porušenie podmienok používania; aplikácia a web Parleru sa odmlčali niekoľko hodín po ukončení. Apple a Google odstránili aplikáciu Parler zo svojich obchodov 8. až 9. januára 2021. K zdôvodneniu AWS pozri e-mail AWS pre Parler zverejnený v spravodajstve: Lauren Feiner, „Amazon says Parler hasn't shown it's able to remove violent content after app store bans“, *CNBC*, 9. januára 2021. Twitter natrvalo pozastavil účet prezidenta Trumpa 8. januára 2021 (Twitter Blog, „Permanent suspension of @realDonaldTrump“, 8. januára 2021) a zrušil vyše 70 000 účtov spojených s koordináciou QAnon; pozri Twitter Safety, „Removal of QAnon accounts“, Twitter Blog, 11. januára 2021. Odstavenie Parleru je hlavným zdokumentovaným prípadom vyradenia z platformy na úrovni infraštruktúry, ktoré jediným krokom vymazalo údaje používateľov celej platformy.

[22] Nariadenie (EÚ) 2016/679 (všeobecné nariadenie o ochrane údajov), článok 20: „Right to data portability“, `https://gdpr-info.eu/art-20-gdpr/`. Článok 20 dáva dotknutým osobám právo získať svoje osobné údaje v štruktúrovanom, bežne používanom a strojovo čitateľnom formáte a preniesť ich k inému prevádzkovateľovi. Rozhodujúcim obmedzením je, že právo na prenosnosť sa vzťahuje na vlastné údaje dotknutej osoby; údaje o tretích stranách (vrátane kontaktných údajov sledujúcich) patria týmto tretím stranám a mimo práva podľa článku 20. Britský ekvivalent pozri UK GDPR článok 20 a pokyny ICO na `https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-data-portability/`.

[23] Twitter (dnes X) oznámil nové cenové úrovne API 2. februára 2023; úroveň Basic (100 USD mesačne, čítanie 10 000 tweetov mesačne) a úroveň Enterprise nahradili predtým bezplatný prístup v2 Academic Research a štandardný prístup. Oznámenie je zdokumentované na `https://developer.twitter.com/en/docs/twitter-api/getting-started/about-twitter-api`. Viaceré akademické výskumné projekty, analytické nástroje tretích strán a migračné klienty ukončili činnosť v priebehu týždňov; pozri spravodajstvo v Casey Newton, „Twitter's new API pricing is a disaster for developers“, *Platformer*, 2. februára 2023; a dokumentáciu Center for Countering Digital Hate o narušení ich výskumného procesu. Efektívny nárast sadzby od bezplatného prístupu cez 100 USD mesačne za základný prístup až po 42 000 USD mesačne za čítanie v rozsahu podnikov bol o niekoľko rádov nad predošlými cenami.

[24] wot-relay: implementácia relayu pre Nostr, ktorá filtruje prichádzajúce udalosti podľa vzdialenosti v sieti dôvery od grafu sledovaných účtov prevádzkovateľa. Zdroj na `https://github.com/bitvora/wot-relay`, udržiava bitvora. Relay prijíma udalosti z účtov v nastaviteľnej vzdialenosti (predvolene 3 skoky) od počiatočného verejného kľúča a udalosti z účtov mimo tohto okolia zahodí bez posudzovania obsahu. Je to praktické nasadenie princípu filtrovania spamu cez WoT: sociálna blízkosť nahrádza moderovanie obsahu a zachováva autonómiu prevádzkovateľa relayu.

[25] Zapstore: decentralizovaný obchod s aplikáciami postavený na protokole Nostr, kde sa vydania aplikácií uverejňujú ako podpísané udalosti Nostr a objaviteľnosť riadi graf siete dôvery používateľa. Aplikácie uverejnené účtami v používateľovom grafe dôvery sa zobrazujú prednostne. Zdroj na `https://github.com/zapstore/zapstore`; aplikácia na `https://zapstore.dev/`. Príslušné NIP sú NIP-51 (zoznamy na kuráciu aplikácií) a návrh NIP pre udalosti vydaní softvéru. Zapstore je hlavným nasadeným príkladom WoT ako mechanizmu dôvery pri distribúcii softvéru v sieti Nostr, ktorý pre používateľov ochotných inštalovať mimo obchodov odstraňuje Apple App Store a Google Play ako strážcov prístupu.

[26] NIP-85: Trusted Assertions, dostupné na https://github.com/nostr-protocol/nips/blob/master/85.md. Definuje parametrizované nahraditeľné udalosti (druh 30382) uverejňované deklarovanými poskytovateľmi služieb, ktoré sa týkajú subjektov určených verejným kľúčom, ID udalosti, adresovateľnou súradnicou alebo externým odkazom podľa NIP-73. Každé tvrdenie nesie vypočítané hodnoty reputácie ako štruktúrované značky. Podpisovateľom je kľúč algoritmu, nie kľúč jednotlivého prevádzkovateľa, čím sa tvorba reputácie oddeľuje od jej spotreby. Udalosť druhu 10040 na prihlásenie používateľom umožňuje určiť, ktoré kľúče poskytovateľov riadia ich signály reputácie, s voliteľným šifrovaním, aby výber poskytovateľa ostal súkromný.

[27] NIP-51: Lists, dostupné na https://github.com/nostr-protocol/nips/blob/master/51.md. Definuje nahraditeľné druhy udalostí pre kuratorské sady vrátane zoznamov sledovaných (druh 3, verejný), zoznamov stlmených (druh 10000) a súkromných zoznamov, ktorých pole obsahu je šifrované pomocou NIP-44. Šifrovaný variant zoznamu sledovaných (zoznam relayov druhu 10002 je samostatný; druh 3 so šifrovaným obsahom je mechanizmus súkromných zoznamov sledovaných) umožňuje používateľovi skryť sociálny graf pred prevádzkovateľmi relayov. Prijatie šifrovaného variantu klientmi je k roku 2025 nejednotné; väčšina hlavných klientov uverejňuje zoznamy sledovaných otvorene ako udalosti druhu 3 bez šifrovania.

[28] Cure53, „Audit of NIP-44 Encryption for Nostr“, december 2023, dostupné na https://cure53.de/audit-report_nip44-implementations.pdf. Audit posúdil špecifikáciu NIP-44 v2, ktorá zahŕňa symetrické šifrovanie ChaCha20, autentifikáciu správ HMAC-SHA256, odvodzovanie kľúča HKDF zo spoločného bodu ECDH a postup odvodenia kľúča konverzácie. Cure53 nenašiel v kryptografickom návrhu nijaké kritické ani závažné problémy. Špecifikácia NIP-44 v2: https://github.com/nostr-protocol/nips/blob/master/44.md. K bezpečnostným slabinám predchodcu NIP-04 (AES-256-CBC bez MAC, neštandardné ECDH) pozri odôvodnenie v NIP-44 a analýzu od Yuki Kishimoto na https://github.com/nostr-protocol/nips/discussions/620.

[29] NIP-17: Private Direct Messages, dostupné na https://github.com/nostr-protocol/nips/blob/master/17.md. Definuje zapečatené správy druhu 14 šifrované pomocou NIP-44 a zabalené do obálok gift wrap podľa NIP-59 (druh 1059). NIP-59: Gift Wrap, dostupné na https://github.com/nostr-protocol/nips/blob/master/59.md. Konštrukcia gift wrap podpisuje vonkajšiu udalosť jednorazovým párom kľúčov a náhodne posúva časovú značku created_at až o 2 dni, takže pre relay nie je viditeľná ani identita odosielateľa, ani skutočný čas správy. Značka p na udalosti druhu 1059 určuje príjemcu; udalosti zoznamu relayov druhu 10050 oznamujú, kde sa nachádza relay so schránkou priamych správ používateľa.

[30] HiveTalk: aplikácia na zvukové a video konferencie postavená na protokole Nostr, ktorá používa WebRTC s pármi kľúčov Nostr na overenie a zapy podľa NIP-57 na prepitné; pozri https://hivetalk.nostr1.com/. Nostr Nests: platforma zvukových miestností natívna pre Nostr, kde sa účasť overuje párom kľúčov používateľa; pozri https://nostrnests.com/. Obe implementujú NIP-53 Live Activities (https://github.com/nostr-protocol/nips/blob/master/53.md) na koordináciu priestorov v reálnom čase, s integráciou Lightning cez zapy podľa NIP-57 na prepitné a riadenie prístupu. Tieto nasadenia ukazujú, že ten istý pár kľúčov a tá istá infraštruktúra relayov, ktorá nesie krátke poznámky, dokáže overovať účasť v interaktívnych aplikáciách v reálnom čase bez samostatnej vrstvy účtov.

[31] Orbot je oficiálna aplikácia projektu Tor pre Android a iOS na smerovanie prevádzky zariadenia cez sieť Tor, dostupná na https://guardianproject.info/apps/org.torproject.android/

a https://orbot.app/. Tails je živý operačný systém, ktorý všetky odchádzajúce spojenia zo svojho návrhu smeruje cez Tor; pozri https://tails.boum.org/. Viacerí klienti pre Nostr integrujú smerovanie cez Tor priamo: Amethyst (Android) podporuje Tor cez transparentný proxy režim Orbotu; komunikáciu Primalu s relayami na strane servera môžu používatelia s celosystémovým Orbotom smerovať cez Tor. K návodu na používanie Toru s protokolom Nostr pozri sekcie o súkromí na https://nostr.how/en/get-started.

ČASŤ VI

PRAX

22
OPERAČNÁ BEZPEČNOSŤ

„Stroje napádajú len amatéri; profesionáli idú po ľuďoch."
Bruce Schneier, *Crypto-Gram Newsletter* (2000)[1]

Úvod

Technické nástroje zlyhajú, ak zlyhajú ľudia. Šifrovanie, ktoré chráni vaše správy, je nanič, ak ten istý obsah zverejníte pod skutočným menom. Anonymita v sieti Tor nepomôže, ak sa cez ňu prihlásite do osobných účtov. Pseudonymita Bitcoinu vás nezachráni, ak nakúpite na burze, ktorá pozná vašu totožnosť, a potom za tie mince zaplatíte citlivé nákupy.

Operačná bezpečnosť (OPSEC) je disciplína, ktorá bráni protivníkom zhromažďovať informácie, čo by mohli bezpečnosť narušiť. Nie je to nástroj, ale prax: trvalá pozornosť voči tomu, ako ľudské správanie dokáže podkopať technickú ochranu.

Čítajte túto kapitolu ako triediaci rámec, nie ako výzvu zaviesť všetky opatrenia naraz. Dobrá OPSEC začína odstránením zjavných slabín vzhľadom na vášho skutočného protivníka. Kapitola 23 túto logiku rozvíja do postupného zavádzania.[2]

22.1 Modelovanie hrozieb: kto je váš protivník?

Určite si konkrétneho protivníka

Bezpečnosť je vždy relatívna voči konkrétnemu protivníkovi. Kým konajúci nevie, proti komu sa chce brániť, sú obranné opatrenia ľubovoľné.

Protivníci sa líšia v dvoch osiach: v schopnostiach a v úmysloch. Lokálny pozorovateľ v zdieľanej sieti WiFi vie zachytávať nešifrovanú prevádzku, no nemá zdroje ani motiváciu sledovať ciele mimo jedného spojenia.

VPN proti takému protivníkovi stačí úplne. Pasívne plošné sledovanie funguje v inej mierke: zachytáva prevádzku hromadne a nemieri na nikoho konkrétneho. Šifrovanie a anonymizačné nástroje zvyšujú náklady na vyťaženie signálu z toho šumu nad rozpočet, ktorý si hromadný zber môže dovoliť. Sledovanie zo strany platforiem je zase iné: služby, ktoré konajúci používa dobrovoľne, sú samy pozorovateľmi, a obranou je vyberať si služby, ktorých obchodný model nestojí na zbere údajov o používateľoch. Tieto tri kategórie majú spoločné, že protivník nehľadá práve vás.

Cielené sledovanie mení ekonomiku. Firma, ktorá aktívne vyšetruje konkrétnu osobu, si môže najať odborníkov a udržať úsilie týždne či mesiace, ale jej zdroje sú konečné a jej zákonná moc obmedzená. Štátny úrad vedúci cielené vyšetrovanie má právomoc nariadiť vydanie dokumentov a technické schopnosti, ktoré ďaleko prevyšujú firemné zdroje, a úsilie dokáže udržať aj roky. Pomer nákladov a prínosov sa mení na každej úrovni: čo odradí pasívneho pozorovateľa, neodradí odhodlaného vyšetrovateľa, a čo zmarí firemného protivníka, nemusí spomaliť spravodajskú službu. Modelovanie hrozieb existuje preto, že to isté obranné opatrenie môže byť proti jednému protivníkovi zbytočne silné a proti inému nebezpečne slabé.

Zhodnoťte schopnosti a zdroje protivníka

Protivníci sa stupňujú od začiatočníkov (script kiddies), ktorí púšťajú nástroje bez toho, aby im rozumeli, cez zručných jednotlivcov schopných nových útokov až po firmy s najatými odborníkmi, orgány činné v trestnom konaní s donucovacími právomocami a spravodajské služby, ktoré majú rozsiahle zdroje aj prepracované schopnosti. Zdroje a vyspelosť skutočného protivníka určujú, ktoré ochranné opatrenia sú nevyhnutné a ktoré zbytočne silné.

Prispôsobte obranu skutočným hrozbám

Brániť sa pred NSA, keď vám hrozí násilný bývalý partner, je plytvanie zdrojmi aj pozornosťou. Brániť sa pred hackerom z kaviarne, keď vás vyšetrujú orgány činné v trestnom konaní, je nebezpečne nedostatočné.

Časté sú dve chyby: preháňať a podceňovať. Preháňať znamená používať Tor na prehliadanie receptov, keď vám hrozí len reklamný sledovač. To je zbytočná komplikácia. Podceňovať znamená spoliehať sa na základné šifrovanie, keď vás aktívne vyšetrujú orgány činné v trestnom konaní, a tým vytvoriť nebezpečne nedostatočnú ochranu. Jemnejšie zlyhanie je nesúlad: prepracované technické opatrenia popri nadmernom zdieľaní na sociálnych sieťach, kde slabý článok prekoná silnú ochranu.

Modelovanie hrozieb sa pýta, kto by mohol chcieť vaše informácie a koľko zdrojov by do ich získania vložil.

Posúdenie osobnej hrozby

Váš profil hrozieb vychádza z toho, kým ste a ako žijete. Záleží na povolaní: novinári, právnici, zdravotníci, aktivisti a ľudia pracujúci s citlivými informáciami čelia vyššiemu riziku. Jurisdikcia ovplyvňuje hrozby aj ochranu, pretože zákony o šifrovaní, slobode prejavu a finančnom súkromí sa výrazne líšia. Verejný profil ovplyvňuje, či sa na vás niekto zameria: zvyšuje viditeľnosť, ak publikujete pod skutočným menom alebo ak máte za sebou kontroverzné výroky. Vzťahy vytvárajú prepojené riziko: sociálne siete príbuzných môžu prezradiť, kde sa zdržiavate, a bezpečnostné návyky obchodných partnerov sa stávajú vašimi zraniteľnosťami. Majetkové pomery určujú niektoré hrozby: bohatstvo priťahuje iné hrozby než chudoba. Politický kontext môže riziko zvýšiť, ak vás presvedčenie alebo činnosť stavajú proti mocným.

Nie všetky informácie vyžadujú rovnakú ochranu. Na vrchole každého vážneho súpisu sú aktíva, ktorých strata by spôsobila skutočnú škodu: finančné prístupové údaje, súkromná komunikácia, zdravotné záznamy a vzorce pohybu, ktoré umožňujú fyzické zacielenie. Pod nimi je vrstva odhalení, čo by priniesli hanbu, ale neohrozili by vás, a pod ňou vrstva informácií, na ktorých nezáleží. Sústreďte úsilie na prvú vrstvu a na druhú míňajte striedmo.

Kalibrácia rizika

Riziko sa dá riadiť, nie odstrániť. Prijateľné zvyškové riziko závisí najprv od závažnosti následkov, ktorá siaha od nepríjemnosti cez finančnú stratu a právne ohrozenie až po fyzické nebezpečenstvo. Kto sa v najhoršom prípade len zahanbí, počíta inak než ten, komu hrozí väzenie, a opatrenia vhodné v jednom prípade môžu byť v druhom zbytočne silné alebo nedostatočné. Záleží aj na pravdepodobnosti a tu väčšina ľudí robí tú istú systematickú chybu: preceňuje šancu, že sa niekto zameria práve na nich, a podceňuje, nakoľko sú už teraz vystavení bežnému plošnému zberu.

Ochrana stojí čas, peniaze, pohodlie aj spoločenské trenie. Opatrenia, ktoré stoja viac než očakávaná škoda, ktorej bránia, sa nevyplatí zavádzať. Základom je udržateľnosť: hrdinské opatrenia, čo vyžadujú stálu ostražitosť, zlyhajú, keď ostražitosť poľaví. Možnosti formujú aj spoločenské obmedzenia: bezpečnostné opatrenia, ktoré vás izolujú od rodiny alebo profesijných sietí, môžu stáť viac, než chránia.

Modely hrozieb nie sú nemenné. Prehodnoťte ich pri zmene okolností: nové zamestnanie, nový vzťah, zmenený verejný profil, politické zmeny alebo po akomkoľvek bezpečnostnom incidente.

Prerušte slučku OODA pri pozorovaní

Kapitola 1 predstavila Boydovu slučku OODA[17] a kapitola 10 ju použila na štátne sledovanie. Ten istý rámec vedie aj osobnú operačnú bezpečnosť.

Každý protivník musí prejsť štyrmi fázami: pozorovanie, orientácia, rozhodnutie, konanie. Vašou prvou prioritou je prerušiť slučku už pri pozorovaní. Ak protivník nevidí vašu činnosť, neskoršie fázy sa mu vykonávajú oveľa ťažšie: orientácia sa zhoršuje a zacielenie je menej spoľahlivé. Zabrániť pozorovaniu je najúspornejšia obrana, lebo dokáže zastaviť reťaz útoku skôr, než sa nasadia vážne zdroje.

Keď posudzujete postup alebo nástroj, opýtajte sa: bráni to pozorovaniu, alebo to len komplikuje neskoršie fázy? Šifrované správy bránia pozorovaniu obsahu správ. VPN môže len skomplikovať pripísanie konania osobe po tom, čo už k pozorovaniu došlo. Obe majú hodnotu, no prvoradé je zabrániť pozorovaniu.

Ak protivník už pozoroval vaše vzorce, prešiel najťažšou fázou. Ďalšie fázy sa mu vykonávajú ľahšie. Preto sú zlyhania operačnej bezpečnosti často katastrofálne: keď k pozorovaniu raz došlo, škoda sa v ďalších fázach zväčšuje. Opakované použitie prezývky a únik metadát sú zlyhania pozorovania, korelácia vzorcov ich rozširuje až k pripísaniu konania osobe. Každé z nich umožňuje to, čo nasleduje.

22.2 Najslabší článok: ľudský faktor

Útoky sociálnym inžinierstvom

Útoky sociálnym inžinierstvom obchádzajú kryptografickú ochranu úplne, lebo mieria na jedinú súčasť, ktorú nijaký protokol nedokáže spevniť: ľudskú psychiku. Útočník šifru neláme, ale presvedčí človeka, aby otvoril dvere.

Phishing funguje, pretože ľudia reflexívne dôverujú správam, ktoré napodobňujú známu autoritu, a dobre urobený falošný e-mail z banky či od zamestnávateľa vyvolá poslušnosť skôr, než sa začne uvažovať. Pretexting funguje, pretože ľudia sú spoločenské bytosti, čo spolupracujú s vierohodnými príbehmi. Útočník, ktorý zostaví presvedčivý scenár („som z IT, potrebujeme overiť váš účet“), využije ochotu pomôcť ako cestu útoku. Návnada (baiting) využíva zvedavosť: infikovaný USB kľúč nechaný na parkovisku sa zasunie do počítača, lebo niekto chce vedieť, čo na ňom je. Vkĺznutie za oprávnenou osobou (tailgating) využíva zdvorilosť: pridržať dvere človeku za sebou je automatické správanie a útočníci sa na ten automatizmus spoliehajú, aby obišli fyzické riadenie prístupu.

Každá metóda uspeje tak, že premení psychologický sklon (dôveru, ochotu pomôcť, zvedavosť, zdvorilosť) na prístupovú cestu. Vzorec je stály: útočná plocha nie je stroj, ale behaviorálne predvolené nastavenie obsluhy. Proti takýmto útokom bránia len ostražitosť a procedurálna disciplína, a obe pri únave slabnú.

Nátlak a právny tlak

Útok kľúčom za päť dolárov, ktorý rozoberá kapitola 5, ukazuje, že fyzický nátlak dokáže vynútiť odhalenie bez ohľadu na silu kryptografie. Prístupová fráza povolí pri dostatočnej fyzickej hrozbe a žiadna dĺžka kľúča na tom nič nezmení. Podobne funguje právny nátlak: súdy môžu potrestať pohŕdaním súdom toho, kto odmietne vydať heslá, a jurisdikcie sa v pravidlách núteného odhalenia podstatne líšia. Britský zákon o vyšetrovacích právomociach (Regulation of Investigatory Powers Act)[18] dovoľuje súdom nariadiť vydanie kľúča a za odmietnutie hrozí trestná sankcia. V Spojených štátoch sa ochrana podľa Piateho dodatku uplatňuje užšie a súdy sa rozchádzajú v tom, či nútené vydanie prístupovej frázy je nútená výpoveď, alebo fyzický úkon.[19]

Technické opatrenia môžu zvýšiť cenu úspešného nátlaku, ale nemôžu ho vylúčiť. Popierateľné šifrovanie, napríklad VeraCrypt[20], dovoľuje, aby jeden šifrovaný kontajner mal dve heslá a každé z nich otvorilo inú sadu súborov. Nútené odhalenie tak ukáže vierohodný obsah a citlivý materiál ostane skrytý. Spínače mŕtveho muža vedia zničiť kľúče alebo poslať upozornenie, ak ich nikto v pravidelných intervaloch neobnoví, čo niektoré formy nátlaku pri zadržaní odrádza. Prahové schémy, ktoré rozdelia kľúčový materiál medzi viacero strán, zaručujú, že nikto nemá v rukách všetko, čo protivník potrebuje. Takéto opatrenia menia protivníkovu úlohu: namiesto vynútenia jedného tajomstva musí kompromitovať naraz viacero ľudí alebo systémov. To zvyšuje náklady, no neposkytuje záruku.

Pohodlnosť a lenivosť

Bezpečnostné opatrenia, ktoré prekážajú pohodliu, sa obchádzajú, a spôsoby zlyhania sú dobre známe. Jedinečné heslá k všetkým účtom je zdĺhavé udržiavať, preto ľudia heslá opakujú a vytvárajú jediné body zlyhania, ktoré sa šíria naprieč službami. Overovanie podpisov a kontrolných súčtov trvá, a ľudia nechcú ten čas venovať, takže sa neoverený softvér nainštaluje aj tak. Oddelenie identít vyžaduje disciplínu, na ktorej unavení ľudia šetria, takže sa prúdy pomiešajú. Aktualizácie prerušujú prácu, takže systémy zostanú bez záplat. Každé z týchto zlyhaní sa dá samo osebe obhájiť, no spolu určujú priepasť medzi bezpečnosťou, akú systém mohol poskytnúť, a tou, akú poskytuje.

Udržateľná bezpečnosť musí počítať s ľudskou lenivosťou, a preto znižuje trenie pri dobrej praxi, až sa stane cestou najmenšieho odporu. Správca hesiel urobí jedinečné heslá jednoduchšie než ich opakovanie. Hardvérový kľúč urobí overenie odolné proti phishingu rýchlejším než prepisovanie jednorazového kódu. Šifrované komunikačné aplikácie[21], ktorých ovládanie sa vyrovná sledovaným alternatívam, sa ujmú, kým aplikácie vyžadujúce ručnú výmenu kľúčov zostanú ležať na poličke. Disciplína narastá len vtedy, keď je bezpečný postup zároveň pohodlný.

Ľudia zlyhajú skôr než technika

Pri mnohých bezpečnostných incidentoch s dobrou kryptografiou je rozhodujúce zlyhanie ľudské: slabé heslá, opakované používanie prístupových údajov v rôznych službách, naletenie na phishing, miešanie identít, nadmerné zdieľanie na sociálnych sieťach alebo dôvera v kompromitovaných spolupracovníkov. Pád Silk Road spôsobilo opakované použitie prezývky a zlá konfigurácia servera. Členov LulzSec chytili preto, že sa delili o informácie so spolupracovníkom, ktorého FBI už obrátilo. Reality Winner odhalili podľa metadát z tlačiarne, nie prelomením kryptografie. V každom z týchto prípadov technická vrstva obstála a ľudská zlyhala.

Vzorec má stále rovnakú podobu. Útočníci, ktorí nezdolajú kryptografiu, skúmajú ľudí okolo nej. Sociálne zmanipulujú správcu, počkajú na chvíľu únavy alebo si vypestujú dôveryhodného zasvätenca. Technická konfigurácia určuje spodnú hranicu, ľudská disciplína rozhoduje, či systém nad ňou zostane. OPSEC je predovšetkým prax riadenia správania tak, aby bol rozdiel medzi spodnou hranicou, ktorú poskytujú nástroje, a stropom, ktorý dovolí ľudská chyba, taký malý, aký len obsluha dokáže docieliť.

22.3 Technické základy bezpečnosti

Zariadenie a operačný systém

Bezpečnosť začína operačným systémom. Ten sprostredkúva každú interakciu medzi aplikáciami a hardvérom, takže kompromitovaný systém podkopáva všetky opatrenia, ktoré na ňom stoja. Preto existujú účelové systémy. Qubes OS[3] izoluje aplikácie v oddelených virtuálnych strojoch, aby sa z kompromitovaného prehliadača nedalo dostať k súborom ani kľúčom v inom oddelení. Architektúra počíta s prelomením jednotlivých súčastí a škodu obmedzuje štruktúrou. GrapheneOS[4] sprísňuje Android lepším izolovaním aplikácií a overeným štartom a namiesto zabudovania služieb Google do systému ponúka izolovaný prístup k Obchodu Google Play. Tým zatvára útočnú plochu, ktorú bežný Android necháva predvolene otvorenú. Keď sa špecializované systémy použiť nedajú, princíp platí aj tak: vypnite telemetriu a nepotrebné služby, bežnú prácu robte z účtov so štandardnými právami namiesto správcovských a na zariadeniach Apple zapnite funkcie ako Lockdown Mode. Každé opatrenie zmenšuje útočnú plochu, ktorú systém ponúka.

Fyzický prístup k nešifrovanému zariadeniu znamená úplnú kompromitáciu a práve proti tejto hrozbe pomáha šifrovanie disku. Šifrovanie celého disku (LUKS v Linuxe, FileVault v macOS, BitLocker vo Windowse)[22] zaručí, že stratené alebo ukradnuté zariadenie neprezradí nič čitateľné bez dešifrovacieho kľúča. Heslá k firmvéru bránia útočníkovi naštartovať neo-

právnené médium a overený štart na podporovanom hardvéri zaisťuje, že samotný zavádzač nikto nezmenil. Zámky obrazovky s krátkym časovým limitom a silnými heslami riešia hrozbu krátkej neprítomnosti. Biometria je pohodlná, no v niektorých jurisdikciách ju možno vynútiť, kým PIN-y a heslá majú silnejšiu právnu ochranu. Rovnaká logika zmenšovania útočnej plochy platí aj pre softvér: každá nainštalovaná aplikácia a každá bežiaca sieťová služba je možný vstupný bod a čo tam nie je, to sa nedá zneužiť.

Sieťová bezpečnosť a správa kľúčov

Sieťová bezpečnosť bráni odpočúvaniu a útokom typu „muž uprostred“ vo vrstvách, kde k nim dochádza. HTTPS používajte všade, overujte certifikáty TLS a používajte rozšírenia prehliadača, ktoré HTTPS vynucujú. Verejnú sieť WiFi považujte za nepriateľskú, takže v sieťach, ktorým neveríte, používajte VPN. Dopyty DNS môžu prezradiť, čo navštevujete, aj keď je samotná prevádzka šifrovaná, preto používajte DNS cez HTTPS alebo nastavte dôveryhodné resolvery DNS.[2323] Firewall nastavte tak, aby blokoval prichádzajúce spojenia, ktoré nepotrebujete, lebo každý otvorený port je možný vstupný bod.

Kryptografické kľúče sú materiál, na ktorom stojí celý systém, a musia byť zároveň chránené aj obnoviteľné. Kľúče by mali byť šifrované pri uložení, najlepšie s hardvérovou ochranou, ako sú HSM alebo hardvérové peňaženky, ktoré držia tajomstvo mimo univerzálnych počítačov. Kľúče bez zálohy ohrozuje strata, no zle navrhnuté zálohy zväčšujú útočnú plochu, takže správny prístup závisí od toho, či je kľúč jednorazový, alebo dlhodobý. Jednorazové a relačné kľúče sa dajú často meniť, čo obmedzuje vystavenie, ak sa jeden kľúč prezradí. Dlhodobé kľúče identity prinášajú iný kompromis, lebo výmena kľúča ničí kontinuitu. Preto vyžadujú plán obnovy s vyskúšanou cestou obnovenia ešte pred akoukoľvek krízou: spínač mŕtveho muža pre prípad nespôsobilosti a viacpodpisová úschova kľúčového materiálu.

Pôvod softvéru a záplatovanie obraz dopĺňajú. Softvér by mal pochádzať z legitímnych zdrojov, ktorých pravosť sa dá overiť. Podpisy PGP na stiahnutých súboroch dokazujú pôvod cez sieť dôvery. Zapstore ponúka iný model: vývojári podpisujú vydania svojimi kľúčmi Nostr a používatelia nachádzajú aplikácie cez odporúčania v sociálnom grafe, pričom podpisy overujú voči verejným kľúčom, ktorých reputáciu vedia posúdiť sami. Haše dokazujú integritu kontrolou kontrolných súčtov a reprodukovateľné zostavenia umožňujú overiť, že binárny súbor zodpovedá zverejnenému zdroju. Závislosti môžu byť kompromitované, preto veľké závislosti si zaslúžia audit. Po inštalácii softvéru treba bezodkladne aplikovať záplaty, lebo známe zraniteľnosti sa aktívne zneužívajú. Treba overovať aj samotné zdroje aktualizácií, pretože falošné výzvy na aktualizáciu sú

častým vektorom útoku. Softvér, ktorý už nedostáva aktualizácie, treba nahradiť.

Kompromitovanie koncového zariadenia: komerčný špionážny softvér a forenzná extrakcia

Zariadenie v rukách obrancu je samo útočnou plochou. Dve triedy útokov na koncové zariadenia sú dnes priemyselné a treba s nimi počítať výslovne.

Komerčný špionážny softvér (spyware) napáda koncové zariadenie vzdialeným zneužitím, zväčša cez zraniteľnosti bez kliknutia (zero-click) v komunikačných klientoch alebo v spracovateľoch médií, ktoré klienti spúšťajú. Útok nainštaluje plnohodnotný nástroj na vzdialený prístup, ktorý číta správy po dešifrovaní, zachytáva obsah obrazovky, vynáša súbory a na požiadanie zapína mikrofón a kameru. End-to-end šifrovanie prenosu správ je proti kompromitovanému zariadeniu zbytočné, lebo protivník číta otvorený text tak isto ako používateľ. Obrana proti komerčnému spyware je disciplína zložená z viacerých návykov, ktoré sa navzájom posilňujú. Obmedzte útočnú plochu, ktorú komunikační klienti a spracovatelia médií vystavujú. Používajte platformy, ktoré rýchlo vydávajú bezpečnostné aktualizácie a obsahujú ochrany proti zneužitiu. Zapnite sprísnený režim platformy (napríklad Lockdown Mode na zariadeniach Apple, ktorý vypína viaceré funkcie rozširujúce útočnú plochu výmenou za menšiu funkčnosť). Zariadenie pravidelne reštartujte, lebo niektorý spyware po reštarte stratí pretrvávanie. A nevysvetliteľné vybíjanie batérie či sieťovú aktivitu berte ako možné príznaky kompromitácie, nie ako bežný šum. Pri cieľoch s vysokou úrovňou hrozby je správnym základom sprísnené zariadenie vyhradené pre citlivú prácu, oddelené od zariadenia na bežný život a vymieňané v pevných intervaloch.[5]

Forenzná extrakcia napáda koncové zariadenie cez fyzické držanie. Nástroje vyvinuté pre orgány činné v trestnom konaní zneužívajú slabiny v reťazci štartu a v uzamknutej obrazovke, aby získali údaje zo zhabaných telefónov. Na rozdiel od komerčného spyware vyžaduje forenzná extrakcia fyzické držanie zariadenia a pohybuje sa v cenovej úrovni, ktorá z nej robí rutinu pri bežných trestných vyšetrovaniach, aj keď zariadenie nie je odomknuté. Každé zatknutie je možnou extrakciou a získané údaje zostávajú v dôkazných systémoch bez ohľadu na to, či príde k stíhaniu. Protiopatrenia obrancu sú tu užšie. Šifrovanie disku s prístupovou frázou s vysokou entropiou určuje dolnú hranicu nákladov na extrakciu. Hranica nie je nekonečná, ale je dosť vysoká na to, aby bežné extrakčné nástroje proti nej zlyhali. Záleží na funkciách, ktoré extrakčnému nástroju berú príležitosť na zneužitie, napríklad na obmedzenom režime USB v GrapheneOS a iOS, ktorý po zamknutí zariadenia vypne dátovú cestu cez USB. Vypnutie zariadenia pred odovzdaním (alebo pred jeho odobratím) ho

prenesie do silnejšieho kryptografického stavu než zamknuté, ale bežiace zariadenie, lebo studený štart odstráni kľúče, ktoré by inak mohli zostať v pamäti. Každé z týchto opatrení zvyšuje náklady a znižuje pravdepodobnosť, že sa daný pokus o extrakciu podarí, a obranou je nahromadené trenie.[6]

Keď je kanál šifrovaný, napáda sa koncové zariadenie. To zistili kapitoly o protivníkovi a táto kapitola to potvrdzuje. Zašifrovať kanál nestačí. Zabezpečenie zariadenia treba udržiavať s predpokladom, že útoky na koncové zariadenia sú dnes rutinou, nie výnimkou.

Integrita dodávateľského reťazca: reprodukovateľné zostavenia a podpísané vydania

Nástroj na ochranu súkromia, ktorý používateľ nevie overiť, je nástroj, ktorému používateľ verí len na slovo. Projekt reprodukovateľných zostavení (reproducible builds), ktorý od polovice desiatych rokov tohto storočia koordinuje väčšina veľkých distribúcií Linuxu, rieši jednu polovicu problému overovania: umožňuje zostaviť binárny súbor zo zdroja a potvrdiť, že vzniknutý súbor sa zhoduje so súborom, ktorý projekt distribuuje.[7] Debian dosiahol do roku 2024 reprodukovateľnosť 95 % hlavného archívu, Arch a NixOS sledujú podobný pokrok, Bitcoin Core sa zostavuje reprodukovateľne už roky a Tor Browser sa dodáva so zdokumentovanými pokynmi na reprodukovateľné zostavenie. Druhou polovicou je transparentnosť podpísaných vydaní, ktorú poskytujú PGP, Sigstore a rámec atestácií in-toto tým, že zverejňujú kryptografické podpisy pôvodu zostavenia v transparentnom zázname, ktorý môže auditovať každý používateľ. Zapstore prenáša tú istú myšlienku do siete Nostr: vývojári podpisujú artefakty vydaní svojimi kľúčmi Nostr a používatelia tieto podpisy nachádzajú a overujú cez sociálny graf namiesto centrálnej autority.

Praktický postup je užší než teoretický program. Väčšina používateľov sťahuje hotové binárne súbory a overuje podpis distribúcie voči kľúču, ktorému správca balíčkov distribúcie už dôveruje. Vlastnosť reprodukovateľnosti má význam, aj keď používateľ zostavenie sám nezopakuje, pretože ktorákoľvek strana (bezpečnostný výskumník, komunitná skupina, nepriateľský recenzent) ho môže zopakovať a spustiť poplach, ak sa výsledok líši. Program reprodukovateľnosti robí podpisovú infraštruktúru verejne vyvrátiteľnou, a práve preto vznikol. Rámec SLSA rozširuje tú istú myšlienku na podnikové dodávateľské reťazce s odstupňovanými požiadavkami na atestáciu, ktoré môžu podniky uplatniť na zoznamy komponentov svojho softvéru. Nástroje na ochranu súkromia závisia od viac než len od licencií open source. Závisia od infraštruktúry reprodukovateľnosti a atestácií, vďaka ktorej sa dá preveriť vzťah medzi zdrojom a binárnym súborom, a táto infraštruktúra robí zo sľubu otvoreného zdroja niečo, čo sa dá skontrolovať.

Hardvérové bezpečnostné tokeny

Vyhradený kryptografický hardvér spadá do dvoch prekrývajúcich sa kategórií.[8] Autentifikačné tokeny FIDO2 (YubiKey ako priemyselný štandard s uzavretým firmvérom, Nitrokey a SoloKey ako alternatívy s otvoreným firmvérom) viažu každé poverenie pri registrácii na konkrétnu doménu, vďaka čomu sú druhé faktory odolné proti phishingu štrukturálne spoľahlivé. Bitcoinové hardvérové peňaženky (Coldcard na podpisovanie len pre Bitcoin v režime fyzicky oddelenom od siete, Trezor a Ledger pre širšie použitie s viacerými aktívami) držia podpisový kľúč mimo univerzálnych počítačov. Rozdiel medzi týmito dvoma kategóriami sa zmenšuje, keďže niektoré zariadenia podporujú obe, a vhodná voľba závisí od toho, ktoré kľúče potrebujú hardvérovú ochranu.

Notebooky s otvoreným firmvérom (Framework, System76, MNT Reform, Purism Librem) umožňujú používateľom spustiť firmvér coreboot alebo Heads namiesto proprietárneho UEFI. Heads pridáva meraný štart, ktorý odhalí fyzické zásahy, aké bežný firmvérový stack nepodporuje.

Fyzická izolácia

Niektoré modely hrozieb vyžadujú popri softvérových aj výslovné opatrenia fyzickej izolácie.[9] Faradayove vaky blokujú mobilné, WiFi, Bluetooth a GPS vyžarovanie z telefónov, ktoré nosíte do citlivého prostredia, takže prítomnosť zariadenia nevytvorí záznam o pohybe, ktorý by sa dal predvolať súdom. Peňaženky blokujúce rádiový signál bránia pasívnemu bezkontaktnému čítaniu pasov a platobných kariet. Notebooky s hardvérovými vypínačmi umožňujú používateľovi fyzicky odpojiť mikrofón a bezdrôtové rádiá, namiesto toho aby sa spoliehal na ich softvérové vypnutie. Spotrebiteľské smerovače s OpenWrt nahrádzajú nepreniknuteľný firmvér domácich brán preskúmateľným stackom a vreckové cestovné smerovače s OpenWrt menia nedôveryhodnú hotelovú či letiskovú sieť na tunel pod kontrolou používateľa už pri prvom skoku.

Fyzická izolácia dopĺňa kryptografické opatrenia a opatrenia kompartmentalizácie opísané vyššie, nenahrádza ich. Nevyhnutnou sa stáva v prípade, keď je softvérový stack kompromitovaný alebo právne vynútený, a fyzická hranica je vtedy posledným prostriedkom, ktorý protivníkovi odoberie kanál, aký nijaká softvérová záruka nedokáže uzavrieť.

22.4 Kompartmentalizácia a oddelenie identít

Nikdy nekrížte prúdy identít

Najčastejšie zlyhanie OPSEC je prekríženie identít: jediný bod korelácie, ktorý spojí anonymnú identitu so skutočnou. Kompartmentalizácia (rozdelenie na oddelené celky) funguje tak, že protivník, ktorý pozoruje jed-

nu identitu, ju nedokáže spojiť s inou. Akýkoľvek spoločný prvok medzi identitami tento zámer maria a spoločný prvok nemusí byť zjavný.

Prezývka opakovaná v rôznych prostrediach dáva protivníkovi korelačný bod zadarmo: jedno vyhľadávanie spojí anonymnú persónu so skutočným účtom. Osobné e-mailové adresy použité na registráciu anonymných účtov ich zväzujú na úrovni poskytovateľa. Zdieľané prehliadače nesú údaje pre odtlačok prehliadača (nainštalované písma, rozlíšenie obrazovky, konfiguráciu zásuvných modulov, vykresľovanie canvasu), ktoré dokážu identifikovať ten istý stroj naprieč reláciami aj bez cookies. Adresy IP spájajú identity na sieťovej úrovni a záznamy poskytovateľa internetu môžu potvrdiť, že obe identity pracovali z toho istého pripojenia. Aj štýl písania môže slúžiť ako korelátor: jazyková analýza výberu slov a stavby viet dokáže prepojiť texty napísané pod rôznymi menami.

Kľúčová vlastnosť prekríženia identít je nezvratnosť. Keď sa prepojenie medzi identitami raz dostane do protivníkovho súboru údajov, už sa nedá zrušiť. Zmazanie prezývky alebo zatvorenie e-mailového účtu koreláciu z už zozbieraných záznamov nevymaže. Kompartmentalizácia je vlastnosť celej histórie systému, nie jeho súčasného stavu, a preto sa musí dodržiavať od prvého úkonu pod každou identitou.

Jedna identita na jeden účel

Každý účel by mal mať vlastnú identitu a účely by sa nemali miešať. Skutočná identita je na úradné veci: zamestnanie, rodinu, bankovníctvo, všetko, čo sa musí viazať na občianske meno. Pseudonymná profesijná identita je na prácu, ktorú chcete pripísať stálej persóne, ale nie občianskemu menu za ňou. Anonymné identity sú na činnosti, pri ktorých nie je žiaduci ani stály pseudonym. Miešanie účelov v rámci jednej identity vytvára väzby, ktoré sa už nedajú prerušiť, lebo keď sa čo i len jedna informácia zo skutočného sveta dotkne pseudonymnej persóny, tá už nie je pseudonymná v nijakom zmysluplnom význame.

Hardvérové oddelenie identít

Ideálne oddelenie používa pre rôzne identity rôzny hardvér. Notebook používaný len na anonymnú činnosť nemôže cez odtlačok zariadenia prezradiť informácie o vašej skutočnej identite. Rôzne operačné systémy slúžia rôznym potrebám kompartmentalizácie. Tails[10] je živý operačný systém, ktorý sa spúšťa z USB a smeruje všetku prevádzku cez Tor bez stopy v hostiteľskom počítači. Hodí sa na jednorazové citlivé činnosti, pri ktorých nechcete žiadny trvalý stav a potrebujete úplnú sieťovú anonymitu. Qubes je desktopový operačný systém, ktorý rozdeľuje rôzne činnosti do oddelených virtuálnych strojov bežiacich súčasne. Hodí sa na trvalú prácu vo viacerých bezpečnostných kontextoch, kde potrebujete udržiavať oddelené identity dlhodobo a počas dňa medzi nimi prepínať. GrapheneOS je

sprísnený mobilný operačný systém pre telefóny Pixel. Poskytuje silnú bezpečnosť a súkromie zariadenia pri mobilnej práci, ale je to systém pre telefón, nie riešenie pre desktop. Voľba závisí od použitia: Tails na anonymné relácie bez pretrvávania, Qubes na kompartmentalizovanú každodennú prácu na počítači, GrapheneOS na bezpečný mobil. Menej ideálne, ale praktickejšie pre tých, čo špecializované systémy zaviesť nemôžu: rôzne prehliadače, rôzne profily, rôzne používateľské účty na štandardnom operačnom systéme.

Sieťové a časové oddelenie

Rôzne identity by mali používať rôzne sieťové cesty, pretože sieťová korelácia je jednou z najspoľahlivejších techník deanonymizácie a najľahšie sa uplatňuje vo veľkom. Domáci internet je spojený so skutočnou identitou a mal by s ňou zostať spojený. Verejná WiFi alebo anonymne zakúpené mobilné dáta slúžia na anonymnú činnosť. Ak sa používa VPN, rôzni poskytovatelia by mali pokrývať rôzne identity. Keď to riziko odôvodňuje, skutočná identita môže používať obyčajný internet a anonymná Tor. Seriózna kompartmentalizácia vyžaduje, aby identity nezdieľali sieťovú adresu ani vzorec prevádzky viditeľný tomu istému pozorovateľovi.

Časová korelácia je druhá strana toho istého problému. Vzorce aktivity spájajú identity aj vtedy, keď ich nespájajú mená ani adresy. Ak sú dve identity vždy aktívne v tých istých hodinách, môže ísť o jednu osobu s jedným rozvrhom. Rýchla reakcia oboch identít na tú istú vonkajšiu udalosť môže prepojenie potvrdiť už len načasovaním. Dve identity, ktoré obe stíchnu počas tej istej dovolenky, sú silnejší signál než ktorákoľvek z nich osamote. Zámerne meniť vzorce aktivity a zavádzať oneskorenia tam, kde stoja málo, dokáže zmariť naivnú podobu útoku. Sofistikovanú podobu zmarí len dôsledné oddelenie zariadení a rozvrhov.

22.5 Organizačná bezpečnosť a problém infiltrácie

Operačná bezpečnosť sa týka skupín rovnako ako jednotlivcov. Hnutie alebo miestny obchodný kruh môže zlyhať rovnakými únikmi, aké odhalia jednotlivca, ale skupiny čelia nebezpečenstvu, ktoré jednotlivci nepoznajú: infiltrácii.

Každá organizácia, na ktorej záleží, by mala počítať s tým, že sa do nej budú pokúšať vniknúť nepriateľskí aktéri, lebo záznamy štátu nenechávajú v tomto bode veľa miesta pre nevinnosť. Keď úrady rozhodnú, že na hnutí, redakcii, aktivistickej sieti či disidentskom trhu záleží, nespoliehajú sa len na pasívne pozorovanie. Pestujú si informátorov a umiestňujú agentov tam, kde sa už tvorí dôvera. Správnou odpoveďou na túto skutočnosť je návrh, nie panika. Štrukturálne usporiadania, čo obmedzujú, koľko môže prezradiť ktorýkoľvek jeden kompromitovaný účastník, majú väčšiu cenu než nahodilé podozrievanie toho, kto sa práve zdá nezapadať.

Odhaľovanie nestačí

Väčšina rád o infiltrácii začína odhaľovaním: všímajte si životopisy, ktoré nesedia, náhly prístup k zdrojom, aké obyčajný účastník nemá, a človeka, čo skupinu stále tlačí k bezhlavému konaniu. Niečo z týchto rád je rozumné a stojí za to ich osvojiť si. Žiadna z nich však nerieši hlavný problém: schopných infiltrátorov na práve takéto podozrenia vycvičili a prejdú nimi.

Hnutie, ktoré sa spolieha len na intuíciu, často minie skutočného informátora a obviní nesprávnych ľudí. Toto zlyhanie má druhú cenu popri bezprostrednom justičnom omyle: skupiny posadnuté odhaľovaním zparanoidnia a zrútia sa zvnútra, keď vzájomné podozrievanie a skúšky lojality stravia samotnú prácu. Štát nepotrebuje mať v skupine každého informátora, aby dosiahol stíhanie. Často stačí, aby sa organizácia zvnútra sama zožrala, kým si vonkajšie vyšetrovanie robí svoje.

Ostražitosť stále platí. Je to druhá obranná línia. Prvou byť nemôže.

Návrh na obmedzenie škody

Prvotná obrana je štrukturálna. Budujte tak, aby ani úspešná infiltrácia nedosiahla svoj cieľ.

Kryptografia už takto funguje. Bezpečný systém predpokladá, že protivník pozná protokol a kód, ale nie tajné kľúče. Organizačná bezpečnosť potrebuje rovnaký postoj. Predpokladajte, že nepriateľský aktér môže vstúpiť do miestnosti, a že niekoho môžu neskôr zatknúť, tlačiť naň alebo ho obrátiť. Potom sa opýtajte, čo by taký človek mohol prezradiť.

Keď jeden účastník drží priveľa informácií, infiltrácia sa vypláca. Keď sú citlivé znalosti rozdelené a rizikové činnosti kompartmentalizované, hodnota krtka ďalej klesá, ak je súkromná komunikácia chránená end-to-end. Informátor môže oznámiť, čo odznelo na jednom stretnutí, ale nevie zmapovať celú sieť ani prezradiť plány, ktoré mu nikdy nedovolili vidieť.

Kompartmentalizujte znalosti, nielen zariadenia

Tá istá disciplína, čo platí pre zariadenia a siete, platí aj pre znalosti v rámci skupiny.

Nie každý potrebuje úplný zoznam členov alebo mapu infraštruktúry a nie každý potrebuje poznať dodávateľský reťazec, štruktúru peňaženiek, miesta meetupov či núdzový plán. Spolupracovník má vedieť to, čo vyžaduje jeho rola, a o málo viac.

Ohraničená znalosť je znakom schopnosti, nie nedôvery. Zrelé organizácie si nezamieňajú vrelosť s odhalením a chápu, že dôvera môže byť úprimná a pritom ohraničená.

To isté pravidlo platí pre komunikáciu. Úplné prevádzkové podrobnosti nepatria do najširšieho kanála a nijaká jediná chatová miestnosť by sa nemala stať archívom celého projektu. Rozhovory rozdelené podľa ro-

ly a časového horizontu obmedzia prípadný kompromis na jedno miesto, takže ak jeden účastník prejde na nepriateľskú stranu alebo padne jeden účet, vonkajšia strana nedostane celý projekt naraz.

Redundancia a ploché štruktúry

Hierarchie robia infiltráciu výnosnou, lebo vytvárajú zjavné vysokohodnotné ciele. Kompromitujte vodcu, pokladníka, prevádzkovateľa relayu alebo jedinú osobu, ktorá vie, ako všetko do seba zapadá, a škoda sa rýchlo rozšíri.

Redundancia mení ekonomiku opačným smerom než ohraničená znalosť. Každú kritickú funkciu by mal vedieť vykonať viac než jeden človek. Pre kritickú komunikáciu by mal existovať viac než jeden kanál. A na stretnutia a obchod by malo byť viac než jedno miesto. Primerane plochá štruktúra túto zásadu posilňuje, takže nijaké zmiznutie ani prebehnutie nemôže zmraziť celú sieť. Oba princípy stoja vedľa seba: informácie kompartmentalizujte, aby sa kompromitovanie ktoréhokoľvek človeka dalo prežiť, a schopnosti zdvojte, aby sa dala prežiť aj strata ktoréhokoľvek človeka.

Skupiny stále potrebujú koordináciu a štandardy, ale v podobe, ktorá z každej kľúčovej roly nerobí jediný bod zlyhania.

Seriózna sieť na ochranu súkromia počíta s tým, že ku kompromitácii dôjde a že sieť musí fungovať aj nasledujúci deň, namiesto predpokladu, že všetci vnútri sú čistí.

22.6 Bezpečnosť miesta stretnutí a fyzické uzly

Skupiny, ktoré sa stretávajú osobne, zdedia druhý problém. Opakujúca sa miestnosť alebo zadná izba u obchodníka je užitočná, lebo ľudia vedia, kde sa nájsť. Tá istá stálosť však uľahčuje miesto sledovať. Fyzické uzly potrebujú vlastné pravidlá.

Na prvom mieste je riadenie prístupu. Citlivé miesto drží svoju skutočnú funkciu pred ulicou skrytú a hostí zdržiava len v priestoroch, ktoré ich návšteva vyžaduje. Verejný priestor by sa mal oddeliť od skladu a od priestoru na citlivé rozhovory, ak to prípad dovoľuje. Zoznamy hostí majú byť minimálne a niekto musí stále vedieť, kto koho pozval a kto zodpovedá za nováčika. Zmyslom je zabrániť, aby sa náhodná zvedavosť a oportunisti dozvedeli celé usporiadanie zadarmo.

Prístupové cesty si zaslúžia rovnakú pozornosť ako miestnosť. Miesto používané na obchod alebo koordináciu by nemalo všetkých navyknúť na jednu viditeľnú rutinu. Opakovaný čas stretnutia, jedna vstupná cesta, domáca sieť WiFi, ktorú používa každý účastník, a jeden vzorec parkovania dávajú pozorovateľom rovnaký dar: stály vzorec na zmapovanie. Lepší postup je jednoduchý: meňte trasy a časy tam, kde to stojí málo, a citlivé zariadenia držte mimo siete miesta. Vopred sa dohodnite na signáli, kto-

rým ľudí odvrátite od kompromitovaného miesta. Miestnosť, ktorú možno nahradiť, je bezpečnejšia než tá, ktorú považujete za nenahraditeľnú.[11]

22.7 Odhaľovanie sledovania

Prevencia je lepšia než odhaľovanie, no odhaľovanie umožňuje reakciu. Ak rozpoznáte, že vás sledujú, fyzicky či digitálne, môžete upraviť správanie skôr, než sa kompromitácia dokončí.

Znaky fyzického sledovania

Fyzické sledovanie zanecháva stopy, ak viete, čo pozorovať. Jedným z najsilnejších znakov je tá istá osoba na viacerých nesúvisiacich miestach. Jeden výskyt môže byť náhoda, no opakované výskyty si zaslúžia pozornosť. Pozornosť si zaslúžia aj vozidlá, ktoré sa objavujú opakovane, najmä ak v nich sedia ľudia, čo nevystupujú. Ľudia, ktorí sa zdajú bez účelu, motajú sa bez zjavného dôvodu, dlho čítajú noviny alebo telefonujú bez konca, môžu vykonávať sledovanie. Náhle zmeny v prostredí, napríklad nové „stále" tváre na vašich obvyklých miestach, treba preveriť.

Odhaľovanie vyžaduje poznať základnú líniu bežnej činnosti. Vedzte, kto zvyčajne obýva vaše pravidelné prostredie: kaviareň, cestu do práce, štvrť. Bez poznania toho, čo je bežné, nepoznáte, čo sa zmenilo.

Protisledovacie trasy preverujú, či vás niekto nasleduje. Rutinu meňte nepredvídateľne. Používajte trasy, ktoré nútia sledujúcich odhaliť sa: slepé ulice, náhle obrátenie sa, vstup do budov s viacerými východmi a rýchly odchod. Cieľom nie je uniknúť, ale odhaliť. Ak odhalenie sledovanie potvrdí, môžete sa rozhodnúť, či pokračovať, zmeniť správanie, alebo požiadať o pomoc.

Znaky digitálneho sledovania

Digitálne sledovanie sa odhaľuje ťažšie, ale tiež zanecháva stopy. Neočakávaná aktivita účtu, napríklad oznámenia o prihlásení z neznámych miest alebo zariadení, naznačuje možnú kompromitáciu. E-maily s obnovením hesla, o ktoré ste nežiadali, nasvedčujú, že vám niekto skúša účty. Zariadenia, ktoré sa správajú nezvyčajne, hrejú sa v pokoji, vybíjajú batériu rýchlejšie než zvyčajne, alebo majú sieťovú aktivitu, keď ich nepoužívate, môžu byť kompromitované.

Kanárikové služby dokážu odhaliť niektoré druhy sledovania. Vyhradený e-mailový účet, ktorý nikdy nepoužívate a len občas skontrolujete, ukáže prihlásenia len vtedy, ak sa doňho dostal niekto iný. Súbory s jedinečnými názvami uložené v cloudovom úložisku možno monitorovať, a prístup od niekoho iného než vás znamená kompromitáciu. Takéto „nástražné drôty" sledovaniu nebránia, ale ho odhalia.

Monitorovanie siete môže odhaliť neočakávané spojenia. Nástroje, ktoré zobrazujú aktívne sieťové spojenia, ukážu, s čím vaše zariadenie komu-

nikuje. Spojenia na neznáme servery, najmä v čase nečinnosti, treba vyšetriť. Dopyty DNS na neočakávané domény môžu naznačovať škodlivý softvér alebo monitorovací softvér.

Všímajte si aj znaky zákonného sledovania. Nezvyčajný záujem orgánov činných v trestnom konaní o vašich známych alebo súdne príkazy doručené vašim poskytovateľom služieb môžu naznačovať vyšetrovanie. Niektoré jurisdikcie vyžadujú oznámenie po skončení určitých druhov sledovania. Neprítomnosť takého oznámenia neznamená, že sledovanie nebolo.

Hranice odhaľovania

Odhaľovanie nie je spoľahlivé. Sofistikovaní protivníci vedú sledovanie navrhnuté tak, aby ho obišli, a neodhalené sledovanie ešte nedokazuje, že nič nebolo. Nesie aj vlastné riziká: viditeľné protisledovacie signály prezrádzajú, že ste si vedomí, a môžu urýchliť postup protivníka. Paranoja poškodzuje vzťahy aj úsudok a falošné poplachy míňajú zdroje, ktoré by si neskôr vyžiadali skutočné hrozby. Cieľom je informovaná, primeraná reakcia, nie istota ani ochrnutie.

22.8 Bežné spôsoby zlyhania (prípadové štúdie)

Opakované použitie prezývky a prekríženie identít

Zatknutie Rossa Ulbrichta vyplynulo zo zlyhaní operačnej bezpečnosti, nie z kryptografických slabín.[12] Rozhodujúce chyby boli opakované použitie prezývky (používateľské meno „altoid“ sa objavilo v anonymných propagačných príspevkoch aj na osobných účtoch) a zlá konfigurácia servera. Technológia fungovala, zraniteľnosti vytvorili ľudské prevádzkové zlyhania. Tento vzorec sa opakuje v mnohých prípadoch: prevádzkovatelia opakujú používateľské mená v rôznych prostrediach alebo vkladajú do nahrávaných súborov identifikovateľné metadáta.

Zrada dôveryhodného spolupracovníka

LulzSec bol hackerský kolektív, ktorý počas päťdesiatdňovej série útokov v roku 2011 prenikol okrem desiatok ďalších vysokoprofilových cieľov aj do Sony a CIA. Hectora Monsegura („Sabu“), jedného z jeho vodcov, zatkli a ten okamžite začal spolupracovať s FBI.[13] Naďalej pôsobil v LulzSec a pritom odovzdával informácie vyšetrovateľom.

Ostatní členovia LulzSec Sabuovi dôverovali a zdieľali s ním informácie, ktoré viedli k ich zatknutiu. Technická bezpečnosť ich komunikácie nehrala rolu, komunikovali totiž s informátorom. Nijaké technické opatrenie nechráni pred dôveryhodným spolupracovníkom, ktorého obrátili. Dôveru nemožno úplne odstrániť. Dôkladne si vyberajte, komu dôveruje-

te, a kompartmentalizujte, čo kto vie, lebo ku kompromitácii môže dôjsť aj vnútri miestnosti.

Tlačiarenská steganografia: Reality Winner

V roku 2017 Reality Winner, dodávateľka pre NSA, vytlačila utajovaný dokument a poslala ho poštou novinárom.[14] Identifikovali ju a zatkli v priebehu niekoľkých dní. Prezradil ju samotný dokument.

Farebné laserové tlačiarne vkladajú takmer neviditeľné žlté bodky, ktoré kódujú sériové číslo tlačiarne a presný dátum a čas tlače,[25] a tie bodky prežili aj sken uniknutej strany. NSA preto vedela, ktorá tlačiareň dokument vyrobila a kedy. Interné záznamy ukázali, že Winner bola jednou zo šiestich ľudí, čo ten dokument tlačili, a ďalšie vyšetrovanie odhalilo kontakt medzi jej pracovným počítačom a novinármi. Odsúdili ju na päť rokov väzenia.

Poučenie siaha ďaleko za tlačiarne. Fyzické dokumenty nesú niekoľko druhov metadát, vrátane sledovacích bodiek tlačiarne, údajov o šarži papiera a stôp manipulácie, ktoré papier sám zaznamenáva. Digitálne dokumenty nesú vlastnú sadu v poliach autora, v histórii revízií, vo vložených súradniciach GPS a v dlhom zozname artefaktov špecifických pre aplikácie, ktoré pretrvajú, aj keď si autor myslí, že ich odstránil. Bezpečný predpoklad je, že každý dokument, fyzický či digitálny, obsahuje informácie, ktoré autor nemienil zahrnúť, a bezpečný postup je zámerne ich odstrániť, dokument znova vytlačiť alebo prepísať vždy, keď to riziko odôvodňuje.

Analýza blockchainu: sledovanie Bitcoinu

Pseudonymita Bitcoinu sa často zamieňa s anonymitou. V roku 2019 medzinárodné orgány činné v trestnom konaní oznámili veľkú operáciu, ktorá viedla k 337 zatknutiam v 38 krajinách.[15] Vyšetrovanie sa opieralo predovšetkým o analýzu blockchainu, nie o prelomenie šifrovania ani o kompromitovanie siete Tor.

Metóda bola priama. Firmy zaoberajúce sa analýzou blockchainu vystopovali toky Bitcoinu od cieľa až k burzám kryptomien a burzy, ktoré zo zákona zbierajú údaje o totožnosti, poskytli záznamy spájajúce transakcie s konkrétnymi osobami. Trvalý a verejný záznam blockchainu, navrhnutý na overovanie bez nutnosti dôvery, sa stal dôkazom obžaloby. Používatelia, ktorí verili, že Bitcoin poskytuje anonymitu, zistili, že každá transakcia, akú kedy urobili, je trvale zaznamenaná a dá sa im pripísať, len čo sa ktorýkoľvek koniec reťazca dotkol identifikovanej služby.

Poučenie: Bitcoin poskytuje pseudonymitu, nie anonymitu. Blockchain na základnej vrstve je trvalý verejný záznam. Súkromie vyžaduje ďalšie opatrenia: vyhýbať sa identifikovaným burzám, používať CoinJoin, platiť cez sieť Lightning s vhodnou správou kanálov alebo používať systémy

ecash, ktoré prerušujú graf transakcií. Pseudonymita je užitočná, no nie je to to isté čo anonymita.

Metadáta fotografií: vystavenie cez EXIF

V roku 2012 sa softvérový podnikateľ John McAfee skrýval pred úradmi v Strednej Amerike. Novinári ho sprevádzali a zverejnili fotografie dokumentujúce jeho útek.[16] Jedna fotografia obsahovala metadáta EXIF vrátane súradníc GPS. Do niekoľkých hodín pozorovatelia určili jeho presnú polohu v rezorte v Guatemale. O pár dní ho zatkli.

Novinári o rizikách metadát vedeli, navzájom sa varovali. K zlyhaniu došlo pri spracovaní súboru v sídle vydavateľstva. Niekto nahral pôvodný súbor, očistená verzia bez metadát nikdy nevyšla. Stačila jedna chyba v reťazci inak opatrného zaobchádzania.

Moderné smartfóny vkladajú do fotografií predvolene rozsiahle metadáta: súradnice GPS presné na metre, model zariadenia, dátum a čas, niekedy nastavenia fotoaparátu a miniatúry predchádzajúcich úprav. Tieto metadáta prežijú bežnú kontrolu, pri prezeraní fotky sa skryté údaje neukážu. Zdieľanie fotografie bez odstránených metadát môže prezradiť vašu polohu aj model zariadenia až po sériové číslo. Pred zdieľaním akéhokoľvek obrázka metadáta odstráňte.[24] Ešte lepšie je v citlivých situáciách vypnúť značkovanie GPS priamo vo fotoaparáte.

22.9 Hranice OPSEC

Dokonalá operačná bezpečnosť je nemožná

Nikto neudrží dokonalú operačnú bezpečnosť navždy. Stála ostražitosť vyčerpáva, ľudia sa pošmyknú a čím viac bezpečnostných opatrení, tým viac príležitostí na chyby. Skutočný život vytvára situácie, v ktorých sa bezpečnosť musí obetovať, a nemožno sa brániť útokom, o ktorých neviete, že existujú.

Chybovať môže každý. Dlhé operácie neustále zvyšujú pravdepodobnosť osudovej chyby.

Cieľavedomí sofistikovaní protivníci môžu uspieť

Proti dostatočne odhodlanému protivníkovi s dostatkom zdrojov nemusí OPSEC stačiť. Spravodajské služby majú viac zdrojov než jednotlivci a súdne príkazy a medzinárodná spolupráca môžu ich dosah natiahnuť ďalej, než siahne obrana ktoréhokoľvek jednotlivca. Ak sa protivník dostane k zariadeniam alebo k človeku, technické opatrenia zlyhajú. Ak dokáže kompromitovať dodávateľský reťazec hardvéru alebo softvéru, získa prístup, ktorý mu nijaká disciplína na nižšej úrovni nezamedzí. Tieto hranice sú štrukturálne a správnou reakciou je pochopiť, kde ležia, nie si namýšľať, že ich zdolá samotná disciplína.

Cieľom OPSEC nie je byť dokonale v bezpečí, ale zvýšiť cenu útoku na vás nad to, čo sú protivníci ochotní zaplatiť. Proti protivníkom s neobmedzenými zdrojmi sa to dosiahnuť nemusí.

Prijatie rizika ako nevyhnutná súčasť

Každá činnosť nesie riziko a dokonalá bezpečnosť je nemožná. Vážna otázka je, aká úroveň rizika je pre danú činnosť prijateľná. Disciplinovaná podoba tej otázky má štyri časti. Po prvé, posúďte pravdepodobnosť zlyhania a jeho následky. Po druhé, určte, ktoré opatrenia znížia pravdepodobnosť či následky na prijateľnú mieru. Po tretie, zistite, aké zvyškové riziko po týchto opatreniach zostáva a či je znesiteľné. Po štvrté, výslovne uznajte, že určité riziko zostáva, čo je vždy úprimnejšie než predstierať, že ho zmiernenie odstránilo.

Bezpečnosť bez prijatia rizika je divadlo. Uznanie hraníc umožňuje racionálne rozhodovanie.

Vedieť, kedy prestať

Na OPSEC sa vzťahujú klesajúce výnosy. Prvé opatrenia prinášajú veľký prínos: šifrované správy namiesto nešifrovaných sú obrovským zlepšením bezpečnosti. Neskoršie opatrenia prinášajú menší prínos: tri vrstvy VPN namiesto dvoch znamenajú zlepšenie na okraji. Nadmerné opatrenia vytvárajú nové riziká, lebo zložitosť zvyšuje šancu chybnej konfigurácie.

Od istého bodu sa ďalšie opatrenia nevyplatia, ak ich cena je zložitosť a strata použiteľnosti. Vedieť, kedy prestať, je súčasťou dobrej OPSEC.

Zhrnutie kapitoly

Ľudské správanie je najslabším článkom každého bezpečnostného systému. Silk Road padol pre opakované použitie prezývky a zlú konfiguráciu servera, nie pre zlyhanie siete Tor ani Bitcoinu na úrovni protokolu. Členov LulzSec chytili preto, že dôverovali Sabuovi, ktorý už bol informátorom. Reality Winner identifikovali podľa steganografických bodiek tlačiarne vložených do dokumentu, ktorý prezradila. Analýza blockchainu vystopovala transakcie Bitcoinu k identifikovaným burzám a viedla k stovkám zatknutí. Polohu Johna McAfeeho odhalili súradnice GPS v metadátach fotografie. V každom z týchto prípadov premenilo fungujúce nástroje na kompromitáciu operačné odhalenie, kryptografia sama nezlyhala. Sociálne inžinierstvo, pohodlné skratky, opakované použitie prezývky a prekríženie identít prekonávajú technickú ochranu z boku, kde sa brániť nevie.

Modelovanie hrozieb musí predchádzať obranným opatreniam. Bezpečnosť je relatívna voči konkrétnemu protivníkovi a to isté opatrenie môže byť proti jednému zbytočne silné a proti inému nebezpečne slabé. Rámec OODA z kapitoly 1 poskytuje strategické vodidlo: prerušte protivní-

kov cyklus pri pozorovaní, kde je prevencia najlacnejšia. Kompartmentalizácia je operačná disciplína, ktorá túto zásadu presadzuje, a po porušení je nezvratná. Keď protivník raz prepojí dve identity, koreláciu už nemožno zrušiť. Preto rôzne identity vyžadujú od prvého úkonu oddelené prezývky, hardvér, siete a vzorce aktivity. Skupiny čelia infiltrácii ako štrukturálnej hrozbe, nie ako personálnemu problému. Organizácie musia počítať s tým, že sa nepriateľskí aktéri pokúsia vniknúť, a navrhovať obmedzenie škody cez kompartmentalizované znalosti a redundanciu, pretože samotné odhaľovanie proti schopnej infiltrácii nestačí. Rovnaká logika platí aj pre opakovane využívané fyzické priestory. Fyzické miesta stretnutí prežijú dlhšie, keď sú prístup a núdzové plány ohraničené a znalosť miesta sa nešíri za okruh účastníkov, ktorí ju potrebujú.

Dokonalá OPSEC je nedosiahnuteľná. Únava spôsobuje chyby a zložitosť vytvára nové spôsoby zlyhania, a dostatočne vybavení protivníci môžu uspieť bez ohľadu na jedno aj druhé. Prijatie rizika je nevyhnutnou súčasťou racionálnej bezpečnostnej praxe: výslovné priznanie zvyškového rizika namiesto predstierania, že ho zmiernenie odstránilo. Operačná disciplína nenahrádza kryptografické nástroje ani inštitucionálne štruktúry z kapitol 24 a 25, je jednou vrstvou obrany, nie celým systémom. Vedieť, kedy ďalšie opatrenia nestoja za svoju cenu, je súčasťou dobrej bezpečnosti. Kapitola 23 mení triediaci rámec na postupné zavádzanie prispôsobené modelom hrozieb.

Poznámky

[1] Bruce Schneier, *Cryptogram Newsletter*, 15. októbra 2000. Postreh odráža skutočnosť, že technická bezpečnosť často zlyhá na ľudských faktoroch skôr, než sa do hry dostanú kryptografické slabiny.

[2] Na hlbšie štúdium OPSEC je najlepšou praktickou príručkou Michael Bazzell, *Extreme Privacy: What It Takes to Disappear*, 5. vyd. (2023); pokrýva taktické podrobnosti, ktoré táto kapitola uvádza len v zásade. Bazzellov podcast *The Privacy, Security, and OSINT Show* ju dopĺňa. Ross Anderson, *Security Engineering*, 3. vyd. (Wiley, 2020) pokrýva OPSEC v širšom kontexte návrhu systémov a Bruce Schneier, *Secrets and Lies* (2000) je, hoci starší, štrukturálne stále spoľahlivý pokiaľ ide o ľudský faktor. Edward Snowden, *Permanent Record* (2019) a Andy Greenberg, *Sandworm* (2019) a *Tracers in the Dark* (2022) poskytujú hĺbku prípadových štúdií. Hlavné nástroje s otvoreným zdrojom, na ktoré sa kapitola odvoláva: Qubes OS (qubes-os.org), Tails (tails.net), GrapheneOS (grapheneos.org) na hardvéri Pixel, KeePassXC (keepassxc.org), Bitwarden (bitwarden.com), hardvérové tokeny YubiKey (yubico.com), Signal (signal.org), age (age-encryption.org), VeraCrypt (veracrypt.fr) a OnionShare (onionshare.org). Príručka EFF Surveillance Self-Defense (ssd.eff.org) zostáva najlepším bezplatným zdrojom pre konkrétne postupy podľa modelu hrozieb.

[3] Qubes OS, `https://www.qubes-os.org`. Bezpečnostne zameraný operačný systém, ktorý od roku 2010 vyvíja Joanna Rutkowska a tím Qubes. Rozdeľuje činnosti používateľa do viacerých ľahkých virtuálnych strojov na báze Xen s riadenou komunikáciou medzi strojmi. Vyžaduje hardvérovú podporu VT-x / VT-d, zoznam kompatibility je na `https://www.qubes-os.org/hcl/`. Dokument o architektúre: Joanna Rutkowska

a Rafal Wojtczuk, „Qubes OS Architecture“ (2010), https://www.qubes-os.org/attachment/wiki/QubesArchitecture/arch-spec-0.3.pdf.

[4] GrapheneOS, https://grapheneos.org. Sprísnený operačný systém na báze Androidu, ktorý podporuje nedávne zariadenia Google Pixel; projekt na ne cieli pre ich podporu overeného štartu a hardvérového uloženia kľúčov. Medzi funkcie patrí sprísnený alokátor pamäte (hardened_malloc), hardvérové značkovanie pamäte na podporovaných čipsetoch a izolované služby Google Play ako voliteľná aplikácia bez zvýšených oprávnení. Dokumentácia funkcií je na https://grapheneos.org/features, model hrozieb projektu na https://grapheneos.org/faq#relationship-google.

[5] Komerčný spyware (Pegasus, Predator, Graphite) používa zraniteľnosti typu zero-click na kompromitovanie koncových bodov komunikácie a čítanie obsahu po dešifrovaní. Lockdown Mode od Applu a pravidelné reštarty zariadenia sú hlavné obrany dostupné spotrebiteľom. Podrobnosti o odvetví pozri v kapitole 12, poznámka 7. Dokumentácia Apple Lockdown Mode na https://support.apple.com/guide/iphone/turn-on-lockdown-mode-ipho2a2a00ea0/ios. Citizen Lab, https://citizenlab.ca/, sleduje priebežné nasadzovanie. Forenzná metodika Amnesty International Security Lab na https://www.amnesty.org/en/tech/. Prehľad odvetvia (NSO Group, Intellexa, Paragon, Candiru, výkonný príkaz č. 14093) pozri v kapitole 12, poznámka 7.

[6] Cellebrite a Magnet Forensics (ktorá získala GrayKey) predávajú zariadenia na forenznú extrakciu nasadené v policajnom meradle po celom svete. Obmedzený režim USB v iOS a jeho ekvivalenty v Androide, silné šifrovanie disku, vypnutý stav a sprísnené distribúcie ako GrapheneOS zvyšujú náklady extrakcie na strane obrancu. Podrobnosti o odvetví pozri v kapitole 12, poznámka 7. Dokumentácia Apple USB Restricted Mode na https://support.apple.com/en-us/HT208857 (cesta v nastaveniach: Settings → Face ID/Touch ID & Passcode → USB Accessories). Režim uzamknutia Androidu od Googlu a ovládanie zámku obrazovky na https://support.google.com/android. Cellebrite, https://cellebrite.com/. Magnet Forensics (GrayKey), https://www.magnetforensics.com/. GrapheneOS, https://grapheneos.org/features, pre automatický reštart do stavu Before First Access a obmedzenia periférií USB. Úniky o schopnostiach Cellebrite z roku 2024 sú zdokumentované v komunitných bezpečnostných správach na https://9to5mac.com/ a https://grapheneos.org/articles. Príručka Electronic Frontier Foundation o zhabaní zariadenia na https://ssd.eff.org/.

[7] Projekt Reproducible Builds koordinuje prácu na reprodukovateľnosti v distribúciách Debian, Arch, Fedora, NixOS a vo veľkých projektoch s otvoreným zdrojom vrátane Bitcoin Core a Tor Browser. Sigstore a in-toto poskytujú doplnkovú infraštruktúru transparentnosti podpisov a SLSA rozširuje rámec na podnikovú atestáciu dodávateľského reťazca. Reproducible Builds project, https://reproducible-builds.org/, so stavom Debianu na https://tests.reproducible-builds.org/debian/ a základným článkom: Gernot Heiser, Gerwin Klein a Toby Murray, „Binary Analysis Is the Only Reliable Way to Trust a Compiler“ (2014). Zostavenia Bitcoin Core cez Gitian/Guix na https://github.com/bitcoin/bitcoin/tree/master/contrib/guix. Dokumentácia reprodukovateľného zostavenia Tor Browser na https://2019.www.torproject.org/docs/verifying-signatures.html. Sigstore, https://www.sigstore.dev/. In-toto, https://in-toto.io/. Rámec SLSA, https://slsa.dev/. Zapstore, https://zapstore.dev/, so zdrojom na https://github.com/zapstore. Architektúra používa udalosti Nostr (metadáta súborov NIP-94 a zoznamy aplikácií NIP-51) na prenos podpisov artefaktov vydaní, takže dôvera overovateľa spočíva vo verejnom kľúči vývojára, nie v kontrole obchodu s platformou. K základnému modelu hrozieb, ktorému reprodukovateľné zostavenia a transparentnosť podpísaných vydaní čelia, pozri Ken

Thompson, „Reflections on Trusting Trust“, *Communications of the ACM* 27, č. 8 (1984): 761–763, klasická esej o útoku na dodávateľský reťazec na úrovni prekladača.

[8] YubiKey, Nitrokey, SoloKey a OnlyKey pokrývajú vrstvu autentifikačných tokenov FIDO2 (Nitrokey a SoloKey s otvoreným firmvérom). Coldcard, Trezor Safe a Ledger pokrývajú vrstvu bitcoinových hardvérových peňaženiek, pričom Coldcard je referenčné riešenie len pre Bitcoin fyzicky oddelené od siete a SeedSigner je dostupný ako domáca bezstavová zostava pre tých, čo si chcú zostaviť vlastný. Framework, System76, MNT Reform a Purism Librem sú platformy notebookov s otvoreným firmvérom. Coreboot a Heads nahrádzajú proprietárne UEFI na podporovanom hardvéri. YubiKey, `https://www.yubico.com/`. Nitrokey, `https://www.nitrokey.com/`, s otvoreným firmvérom na `https://github.com/Nitrokey`. SoloKey, `https://solokeys.com/`, so zdrojom na `https://github.com/solokeys`. OnlyKey, `https://onlykey.io/`. Coldcard, `https://coldcard.com/`. SeedSigner, `https://seedsigner.com/`. Trezor Safe, `https://trezor.io/`. Ledger, `https://www.ledger.com/`. Framework, `https://frame.work/`. System76 Thelio, `https://system76.com/desktops/thelio`. MNT Reform, `https://mntre.com/`. Purism Librem, `https://puri.sm/`. Coreboot, `https://www.coreboot.org/`. Firmvér Heads, `https://osresearch.net/`. Dokumentácia k FIDO2/WebAuthn na `https://fidoalliance.org/` a špecifikácia W3C WebAuthn na `https://www.w3.org/TR/webauthn-3/`.

[9] Faradayove vaky (Silent Pocket, Mission Darkness), peňaženky blokujúce rádiový signál, hardvérové vypínače Librem, domáce smerovače Turris Omnia a OpenWrt a cestovné smerovače GL.iNet tvoria stack fyzickej izolácie. Nevyhnutným sa stáva v prípade, keď je softvérový stack kompromitovaný alebo právne vynútený. Silent Pocket, `https://silent-pocket.com/`. Mission Darkness (MOS Equipment), `https://mosequipment.com/`. OpenWrt, `https://openwrt.org/`. Turris Omnia a MOX, `https://www.turris.com/`. GL.iNet, `https://www.gl-inet.com/`. Hardvérové vypínače Purism Librem sú zdokumentované na `https://puri.sm/learn/hardware-kill-switches/`. K širšiemu modelu hrozieb pri fyzickom zhabaní zariadenia a použití Faradayovej izolácie pozri Matt Blaze, „Is Your Computer Listening to You?“ *Communications of the ACM* 2015 a pokyny Freedom of the Press Foundation k operačnej bezpečnosti pri protestoch na `https://freedom.press/training/`.

[10] Tails (The Amnesic Incognito Live System), `https://tails.net`. Živý operačný systém na báze Debianu, ktorý sa spúšťa z USB kľúča, smeruje všetku sieťovú prevádzku cez Tor a medzi reláciami nezanecháva na hostiteľskom počítači nijakú stopu. Vznikol v roku 2009 ako vývoj Incognito Live CD a spravuje ho projekt Tails s financovaním od Freedom of the Press Foundation a ďalších. Bezpečnostná dokumentácia na `https://tails.net/doc/about/warnings/`.

[11] K bezpečnosti miest stretnutí, bezpečnostnej kultúre a ohraničeným fyzickým uzlom v širšom nepriateľskom prostredí pozri Smuggler a XYZ, *The Second Realm: Book on Strategy* (Liberty Under Attack Publications, rok neoverený), Kyle Rearden a Shane Radliff, *Just Below the Surface: A Guide to Security Culture* (Independently Published, 2019) a Shane Radliff a Tom Marshall, *Going Mobile* (*#VanLife Zine*) (CreateSpace Independent Publishing Platform, 2019). Ide o texty o stratégii hnutí a o bezpečnostnej kultúre, nie o náhradu technických a právnych zdrojov inde v tejto kapitole.

[12] K rozboru Ulbrichtovho zatknutia a zlyhaní OPSEC pozri Andy Greenberg, „How the Feds Took Down the Dread Pirate Roberts“, *Wired*, 18. novembra 2013, a súdne dokumenty United States v. Ross William Ulbricht, 14-cr-68 (S.D.N.Y.).

[13] K Sabuovi a LulzSec pozri Parmy Olson, *We Are Anonymous: Inside the Hacker World of LulzSec, Anonymous, and the Global Cyber Insurgency* (New York: Little, Brown, 2012).

[14] K Reality Winner a tlačiarenskej steganografii pozri vyhlásenie FBI pod prísahou v United States v. Reality Leigh Winner, 1:17-MJ-590 (S.D. Ga. 2017). K rozboru sledovacích bodiek tlačiarní pozri dokumentáciu Electronic Frontier Foundation o tlačiarenskej steganografii.

[15] U.S. Department of Justice, „South Korean National and Hundreds of Others Charged Worldwide in the Takedown of the Largest Darknet Child Pornography Website", tlačová správa, 16. októbra 2019. Nástroje na analýzu blockchainu použité pri vyšetrovaní poskytla firma Chainalysis.

[16] K incidentu s metadátami EXIF u McAfeeho pozri Graham Cluley, „Fugitive John McAfee's location revealed by photo meta-data screw-up", 3. decembra 2012. Súradnice GPS z fotografie umiestnili McAfeeho do konkrétneho rezortu v Guatemale.

[17] John Boyd vyvinul rámec slučky OODA (Observe, Orient, Decide, Act) ako model rozhodovacieho cyklu pre vzdušný boj, neskôr zovšeobecnený na akékoľvek súťažné prostredie. Primárnym zdrojom je jeho prezentácia „Patterns of Conflict" (nepublikovaná, 1986), archivovaná na `https://www.dnipogo.org/boyd/patterns_ppt.pdf`. Robert Coram, *Boyd: The Fighter Pilot Who Changed the Art of War* (Little, Brown, 2002) je štandardný životopis. Chet Richards, *Certain to Win: The Strategy of John Boyd, Applied to Business* (Xlibris, 2004) uplatňuje rámec mimo vojenských súvislostí. Kapitola 1 tejto knihy predstavila slučku OODA ako rozhodovací cyklus protivníka, ktorý majú nástroje na ochranu súkromia prerušiť.

[18] Regulation of Investigatory Powers Act 2000 (RIPA), c. 23 (UK), Part III (Investigation of Electronic Data Protected by Encryption), `https://www.legislation.gov.uk/ukpga/2000/23/contents`. Oddiel 49 oprávňuje úrady vydať oznámenie, ktoré vyžaduje vydanie šifrovacieho kľúča alebo otvoreného textu chránených údajov. Oddiel 53 robí z nesplnenia trestný čin s trestom odňatia slobody až do dvoch rokov (do piatich rokov v prípadoch národnej bezpečnosti). Investigatory Powers Act 2016 (IPA 2016), c. 25, rámec RIPA aktualizoval a rozšíril, `https://www.legislation.gov.uk/ukpga/2016/25/contents`. Ku komentáru pozri Ian Brown a Douwe Korff, „Terrorism and the Proportionality of Internet Surveillance", *European Journal of Criminology* 6, č. 2 (2009): 119–134.

[19] Súdy v Spojených štátoch sa rozchádzajú v tom, či nútené vydanie prístupovej frázy podozrivým porušuje ochranu podľa Piateho dodatku pred sebaobviňovaním. Hlavné prípady: *In re Grand Jury Subpoena Duces Tecum Dated March 25, 2011*, 670 F.3d 1335 (11th Cir. 2012) (nútené dešifrovanie nie je výpoveď, ak je obsah vopred známy), *United States v. Doe*, 670 F.3d 1335 (11th Cir. 2012), *Commonwealth v. Gelfgatt*, 11 N.E.3d 605 (Mass. 2014) (nútené dešifrovanie je prípustné podľa doktríny vopred známeho záveru) a *State v. Stahl*, 206 So. 3d 124 (Fla. Dist. Ct. App. 2016). Opačný názor pozri v *United States v. Kirschner*, 823 F. Supp. 2d 665 (E.D. Mich. 2010). Orin Kerr a Bruce Brown, „The Dog That Did Not Bark: Steganography, Fifth Amendment Limitations, and the Need for Decryption Transparency", *Iowa Law Review* 96 (2011): 777, mapuje doktrinálnu krajinu. Electronic Frontier Foundation sleduje prebiehajúce spory na `https://www.eff.org/issues/coders/right-encrypt`.

[20] VeraCrypt, `https://veracrypt.fr/`, je nástroj na šifrovanie diskov s otvoreným zdrojom, odvodený od TrueCrypt po jeho zastavení v roku 2014 a nezávisle auditovaný v rokoch 2016 a 2020. Podporuje šifrovanie zväzkov, systémových oddielov a skrytých zväzkov za chodu. Funkcia skrytého zväzku (vierohodná popierateľnosť) dovoľuje, aby jeden šifrovaný kontajner obsahoval dva samostatné šifrované zväzky odomykané rôznymi prístupovými frázami, takže nútené vydanie jednej frázy odhalí vierohodný návnadový zväzok a citlivý zväzok zostane skrytý. Zdrojový kód na `https://github.com/veracrypt/VeraCrypt`. Správy z auditu (fáza 1 od Quarkslab, 2016, fáza 2 od Quarkslab, 2020) na

https://veracrypt.fr/en/Security%20Audits.html. K modelu hrozieb, ktorý skryté zväzky odôvodňuje, pozri dokumentáciu VeraCrypt na https://veracrypt.fr/en/Plausible%20Deniability.html.

[21] Signal, https://signal.org/, je referenčná aplikácia na end-to-end šifrované správy, ktorú vyvinul Open Whisper Systems (dnes Signal Foundation) a prvýkrát vydal v roku 2013. Používa protokol Signal (algoritmus Double Ratchet v kombinácii s dohodou o kľúči X3DH), ktorý poskytuje dopredné utajenie (forward secrecy) a obnovu po prelomení. Špecifikácia protokolu je na https://signal.org/docs/specifications/doubleratchet/. Signal zbiera minimum metadát: uchováva len telefónne číslo použité pri registrácii a dátum posledného pripojenia. Minimalizácia metadát je zdokumentovaná na https://signal.org/bigbrother/. K prijatiu medzi novinármi, aktivistami a bezpečnostnými výskumníkmi pozri školenie digitálnej bezpečnosti Freedom of the Press Foundation na https://freedom.press/training/. Kapitola 17 tejto knihy rozoberá Signal a protokol Double Ratchet do hĺbky.

[22] LUKS (Linux Unified Key Setup), https://gitlab.com/cryptsetup/cryptsetup, je štandardná špecifikácia šifrovania diskov pre Linux, implementovaná nástrojom cryptsetup a predvolene zahrnutá vo väčšine veľkých distribúcií. FileVault je zabudované šifrovanie celého disku v Apple macOS, používa šifrovanie XTS-AES-128 s 256-bitovým kľúčom, dokumentácia na https://support.apple.com/guide/mac-help/encrypt-mac-data-with-filevault-mh11785/mac. BitLocker je funkcia šifrovania zväzkov v Microsoft Windows, dostupná vo vydaniach Pro a Enterprise, dokumentácia na https://learn.microsoft.com/en-us/windows/security/operating-system-security/data-protection/bitlocker/. K porovnávaciemu rozboru modelov hrozieb týchto troch implementácií pozri zdroje o aplikovanej kryptografii od Bruce Schneier a príručku EFF Surveillance Self-Defense o šifrovaní zariadení na https://ssd.eff.org/en/module/how-encrypt-your-iphone.

[23] DNS cez HTTPS (DoH) šifruje dopyty DNS v spojeniach HTTPS, takže sieťový pozorovateľ nevidí, ktoré doménové mená sa prekladajú. Štandardom je RFC 8484 (IETF, 2018), https://www.rfc-editor.org/rfc/rfc8484. DNS cez TLS (DoT) poskytuje rovnakú ochranu cez vyhradené spojenie TLS na porte 853, RFC 7858 (IETF, 2016), https://www.rfc-editor.org/rfc/rfc7858. Resolvery rešpektujúce súkromie zahŕňajú Quad9 (https://www.quad9.net/, prevádzkuje ho švajčiarska nezisková organizácia s politikou bez zaznamenávania), Cloudflare 1.1.1.1 (https://1.1.1.1/, s nezávislým auditom tvrdení o nezaznamenávaní) a resolver zabudovaný v klientovi VPN Mullvad. K modelu hrozieb úniku DNS pozri EFF Surveillance Self-Defense na https://ssd.eff.org a IETF DNS Privacy Considerations, RFC 7626 (2015), https://www.rfc-editor.org/rfc/rfc7626.

[24] ExifTool, ktorý napísal Phil Harvey, https://exiftool.org/, je referenčný nástroj s otvoreným zdrojom na čítanie, zápis a odstraňovanie EXIF a iných metadát zo súborov obrázkov, zvuku, videa a dokumentov, zdroj na https://github.com/exiftool/exiftool. MAT2 (Metadata Anonymisation Toolkit 2), https://0xacab.org/jvoisin/mat2, je jednoduchší nástroj v Pythone zameraný na odstraňovanie metadát, predvolene súčasť Tails. Úplnú taxonómiu typov metadát vložených v bežných formátoch súborov (EXIF, IPTC, XMP, GPS, profily ICC, cache miniatúr, história úprav) pozri v dokumentácii EFF o metadátach súborov na https://ssd.eff.org. Systém strojových žltých bodiek (MYD / tlačiarenská steganografia), podľa ktorého identifikovali Reality Winner, EFF zdokumentovala v „Is Your Printer Spying on You?“ https://www.eff.org/pages/list-print

ers-which-do-or-do-not-display-tracking-dots, kde vedie aj zoznam modelov tlačiarní, o ktorých je známe, že vkladajú sledovacie bodky.

[25] Systém strojových žltých bodiek (MYD) tlačiarenskej steganografie kóduje sériové číslo tlačiarne a dátum a čas tlače do vzoru takmer neviditeľných žltých bodiek na celej strane. Kódovanie je voľným okom neviditeľné, ale zistiteľné pod modrým svetlom LED alebo digitálnou analýzou obrazu. EFF spätne analyzovala kódovanie používané tlačiarňami Xerox a zverejnila špecifikáciu na https://www.eff.org/pages/list-printers-which-do-or-do-not-display-tracking-dots. Edward Snowden varoval novinárov pred týmto sledovacím mechanizmom ešte pred prípadom Reality Winner. Vyhlásenie FBI pod prísahou v United States v. Reality Leigh Winner, 1:17-MJ-590 (S.D. Ga. 2017) opisuje, ako sa bodky použili na zúženie okruhu podozrivých na šiestich a potom na jedného. K širšiemu obrazu nechcených identifikátorov dokumentov (kódy šarží papiera, chemické podpisy tonera, odtlačky vzoru kvapiek atramentových tlačiarní) pozri dokumentáciu (Mikko Hyppönen) a akademickú prácu o digitálnych vodoznakoch (Edward Delp a kolegovia, Purdue), https://www.ece.purdue.edu/~ipl/.

[17] John Boyd vyvinul rámec slučky OODA (Observe, Orient, Decide, Act) pri práci ako stíhací pilot amerického letectva a vojenský stratég. Kanonický sekundárny zdroj je Frans Osinga, *Science, Strategy and War: The Strategic Theory of John Boyd* (Routledge, 2007), ktorý systematicky rekonštruuje Boydove prezentácie. Boydove vlastné prezentačné dokumenty vrátane „Destruction and Creation“ (1976) a súboru snímok „Patterns of Conflict“ sú archivované na https://www.dnipogo.org/john-r-boyd/. Použitie slučky OODA v kybernetickej bezpečnosti a v nepriateľských rozhodovacích cykloch rozvíja Robert Coram, *Boyd: The Fighter Pilot Who Changed the Art of War* (Little, Brown, 2002).

[18] Regulation of Investigatory Powers Act 2000 (RIPA), c. 23 (UK), Part III („Investigation of Electronic Data Protected by Encryption“), https://www.legislation.gov.uk/ukpga/2000/23/part/III. Oddiel 49 zakladá právomoc požadovať vydanie šifrovacieho kľúča alebo informácií v zrozumiteľnej podobe. Oddiel 53 robí z nesplnenia trestný čin s trestom odňatia slobody až do dvoch rokov (do piatich rokov v prípadoch národnej bezpečnosti). Investigatory Powers Act 2016, c. 25 (UK), https://www.legislation.gov.uk/ukpga/2016/25, tieto právomoci aktualizoval a rozšíril. K praktickému rozboru pozri Open Rights Group, https://www.openrightsgroup.org/.

[19] Súdy USA dospeli k protichodným záverom v otázke, či nútené poskytnutie prístupovej frázy podozrivým porušuje ochranu Piateho dodatku pred sebaobviňovaním. Hlavné prípady: *United States v. Fricosu*, 841 F. Supp. 2d 1232 (D. Colo. 2012) (nariadené dešifrovanie), *In re Grand Jury Subpoena Duces Tecum*, 670 F.3d 1335 (11th Cir. 2012) (uplatnená ochrana podľa Piateho dodatku), *Commonwealth v. Gelfgatt*, 468 Mass. 512 (2014) (doktrína vopred známeho záveru uplatnená na vynútenie dešifrovania), *State v. Stahl*, 206 So. 3d 124 (Fla. Dist. Ct. App. 2016) (nútené biometrické odomknutie) a *United States v. Apple MacPro Computer*, 851 F.3d 238 (3d Cir. 2017) (uplatnená ochrana podľa Piateho dodatku). EFF vedie sledovač prípadov núteného dešifrovania na https://www.eff.org/issues/coders/crypto-cases. K akademickému spracovaniu pozri Orin Kerr a Bruce Brown, „The Law of Encryption“, *University of Pennsylvania Law Review* 170 (2022).

[20] VeraCrypt, https://veracrypt.fr/, je nástroj na šifrovanie diskov s otvoreným zdrojom, odvodený od TrueCrypt (zastavený v roku 2014) a udržiavaný firmou IDRIX. Podporuje vierohodnú popierateľnosť cez skryté zväzky: jeden šifrovaný kontajner obsahuje dva samostatné šifrované zväzky prístupné rôznymi heslami, takže nútené vydanie jedného hesla odhalí len návnadové súbory. Zdroj na https://github.com/veracrypt/VeraCrypt. Dokumentácia VeraCrypt o skrytých zväzkoch je na

https://veracrypt.fr/en/Hidden%20Volume.html. Nezávislé bezpečnostné audity vykonali Quarkslab (2016), https://ostif.org/the-veracrypt-audit-results/, a NCC Group (2020). K širšiemu modelu hrozieb popieratelného šifrovania pozri Niels Ferguson, Bruce Schneier a Tadayoshi Kohno, *Cryptography Engineering* (Wiley, 2010), kapitola 8.

[21] Signal, https://signal.org/, je end-to-end šifrovaná komunikačná aplikácia, ktorú vyvinuli Signal Foundation (nezisková organizácia) a Signal Messenger LLC. Používa protokol Signal, ktorý kombinuje algoritmus Double Ratchet s dohodou o kľúči X3DH a poskytuje dopredné utajenie (forward secrecy) a obnovu po prelomení. Špecifikácia protokolu je na https://signal.org/docs/. Signal uchováva minimum metadát: nezaznamenáva obsah správ, zoznamy kontaktov, členstvo v skupinách ani metadáta konverzácií. K uchovávaniu metadát pozri odpoveď Signalu na predvolanie federálnou veľkou porotou (2016), ktorá vydala len dátum registrácie účtu a dátum posledného pripojenia. Moxie Marlinspike a Trevor Perrin, „The Double Ratchet Algorithm“, Signal (2016), https://signal.org/docs/specifications/doubleratchet/. Porovnateľné end-to-end šifrované komunikátory zahŕňajú Briar (https://briarproject.org/, peer-to-peer cez Tor, bez centrálneho servera), SimpleX Chat (https://simplex.chat/, bez identifikátorov používateľov, nevyžaduje telefónne číslo) a Wire (https://wire.com/, open source).

[22] LUKS (Linux Unified Key Setup), https://gitlab.com/cryptsetup/cryptsetup, je štandardná špecifikácia šifrovania diskov pre Linux, udržiavaná ako súčasť projektu cryptsetup. Ako šifrovaciu vrstvu na úrovni jadra používa dm-crypt. FileVault je zabudované šifrovanie celého disku v Apple macOS, zdokumentované na https://support.apple.com/guide/mac-help/protect-data-on-your-mac-with-filevault-mh11785/mac. Používa šifrovanie XTS-AES-128 s 256-bitovým kľúčom. BitLocker je funkcia šifrovania celého disku v Microsoft Windows, zdokumentovaná na https://learn.microsoft.com/en-us/windows/security/information-protection/bitlocker/bitlocker-overview. Na podporovanom hardvéri vyžaduje čip TPM. K porovnávaciemu rozboru týchto implementácií a ich modelov hrozieb pozri Bruce Schneier, *Practical Cryptography* (Wiley, 2003) a wiki Arch Linuxu o šifrovaní diskov na https://wiki.archlinux.org/title/Disk_encryption, ktorá pokrýva technické kompromisy naprieč platformami.

[23] DNS cez HTTPS (DoH) šifruje dopyty DNS v spojeniach HTTPS, takže poskytovatelia internetu a sieťoví pozorovatelia nevidia, ktoré domény používateľ prekladá, RFC 8484, https://datatracker.ietf.org/doc/html/rfc8484. DNS cez TLS (DoT) poskytuje rovnakú ochranu cez vyhradené spojenie TLS, RFC 7858, https://datatracker.ietf.org/doc/html/rfc7858. Resolvery rešpektujúce súkromie zahŕňajú Quad9 (https://www.quad9.net/, prevádzkuje ho švajčiarska nezisková organizácia s politikou bez zaznamenávania) a Cloudflare 1.1.1.1 (https://1.1.1.1/). K nastaveniu DoH na úrovni prehliadača pozri dokumentáciu Mozilly na https://support.mozilla.org/en-US/kb/firefox-dns-over-https. K širšiemu modelu hrozieb súkromia DNS pozri Geoff Huston, „DNS Privacy“, APNIC Blog (2019), https://blog.apnic.net/, a rozbor sledovania DNS od EFF na https://www.eff.org/deeplinks/2019/09/encrypted-dns-could-help-close-biggest-privacy-gap-internet.

[24] Nástroje na odstraňovanie EXIF a iných vložených metadát zo súborov obrázkov a dokumentov zahŕňajú ExifTool (Phil Harvey, https://exiftool.org/, referenčný nástroj príkazového riadka podporujúci stovky formátov), MAT2 (Metadata Anonymisation Toolkit 2, https://0xacab.org/jvoisin/mat2, nástroj

používaný v Tails a odporúčaný Freedom of the Press Foundation) a funkciu exportu bez metadát v prehliadači dokumentov GNOME. Na online kontrolu umožňujú inšpekciu nahraných súborov Jeffrey's Exif Viewer na `https://exifdata.com/` a prehliadač metadát na `https://www.metadata2go.com/`. Dokumentácia SecureDrop od Freedom of the Press Foundation, `https://docs.securedrop.org/`, pokrýva odstraňovanie metadát v rámci svojho postupu na ochranu zdrojov. K modelu hrozieb pozri Harlo Holmes, „Metadata: The Biggest Little Privacy Problem", Freedom of the Press Foundation, 2014.

23
STRATÉGIA ZAVÁDZANIA

„Svet, v ktorom sa kryptografia používa, už nie je svetom, pre ktorý bola navrhnutá.“

Moxie Marlinspike, „The Network in Motion“ (2016)[1]

Úvod

Zavádzanie súkromia nie je jednorazové rozhodnutie, ale priebežný proces. Vyžaduje presný obraz o súčasnej situácii, jasné vedomie vlastných rizík a postupné rozvíjanie zručností v rámci komunity. Cieľom nie je dokonalosť, ale zlepšovanie: posúvať sa z miesta, kde ste, smerom k väčšej autonómii.

23.1 Začíname tam, kde sa nachádzate

Úprimné zhodnotenie súčasného vystavenia

Účinné zavádzanie súkromia začína presným obrazom o tom, ako ste na tom teraz. Väčšina ľudí po zamyslení zistí, že o sebe odhalila viac, než si myslela.

Predstavte si, čo by odhodlaný vyšetrovateľ zistil iba z verejných informácií. Digitálna stopa zahŕňa profily na sociálnych sieťach, príspevky vo fórach, verejné registre, súhrny od dátových brokerov, zmienky v správach a profesijné adresáre. Finančné záznamy prezrádzajú vlastníctvo nehnuteľností, súdne spisy, politické dary a obchodné registrácie. Vzorce správania vyplývajú z check-inov na sociálnych sieťach, označených známych, verejne sledovaných účtov a lajkov, a z času príspevkov, podľa ktorého sa dá odčítať denný režim. Vystavenie z minulosti problém znásobuje: materiály zverejnené pred rokmi zostávajú dostupné v archívoch

a opakovane použité prezývky umožňujú prepojenie, ktoré nezavrie žiadne jednotlivé vymazanie.

Takéto zhodnotenie má byť nepríjemné. Nejde o sebakritiku, ale o triezve pochopenie východiskového bodu. Zlepšovať súkromie sa dá len vtedy, keď viete, čo už je odhalené.

Čo sa dá zmeniť a čo nie

Niečo je odhalené natrvalo. Informáciu, ktorá raz bola verejná, nemožno úplne stiahnuť späť, údaje, ktoré už zhromaždili firmy a vlády, nemožno získať späť a vzorce, ktoré sa už vytvorili, nechávajú stopu, do ktorej nijaké neskoršie vymazanie nedosiahne.

Priebežné vystavenie sa však meniť dá. Medzi ovplyvniteľné činitele patrí budúce správanie pri zverejňovaní, voľba služieb, spôsoby komunikácie a finančné nástroje. Čiastočne ovplyvniteľné sú profesijné požiadavky (môžu si vyžadovať určité odhalenie) a rodinné väzby (to, čo zverejnia iní, sa týka aj vás); staré účty možno zmazať, ale ich archivované kópie už nie. Z veľkej časti neovplyvniteľné sú vládne záznamy a údaje, ktoré už boli predané brokerom; staré príspevky ležia v archívoch, kam žiadosť o vymazanie nedosiahne. Dobrá stratégia sústreďuje sily na to, čo sa zmeniť dá, a zvyšok prijíma. Posadnutosť minulým vystavením plytvá zdrojmi, ktoré sa lepšie využijú na zlepšenie budúcej praxe.

Postupné zlepšovanie namiesto dokonalosti

Dokonalé súkromie sa dosiahnuť nedá. Hon za dokonalosťou vedie k ochromeniu alebo vyhoreniu. Praktický cieľ je neustále zlepšovanie: aby ste na tom boli dnes lepšie než včera a tento rok lepšie než minulý.

K tomu patrí zmieriť sa s nedokonalosťou, lebo každý systém má slabiny a každý postup obmedzenia; nejde o to, či slabiny existujú, ale či sa vaša pozícia zlepšuje. Uprednostnite zmeny s veľkým dosahom: niektoré úpravy prinesú veľký prínos pre súkromie takmer bez námahy, iné vyžadujú veľa úsilia a dajú len okrajové zlepšenie. Budujte udržateľné návyky, lebo postupy, ktoré si vyžadujú stálu ostražitosť, zlyhajú, keď ostražitosť pominie; udržateľné súkromie vzniká z návykov, ktoré sa stanú automatickými, nie z hrdinských výkonov, ktoré sa nedajú udržať. Vyhnite sa uvažovaniu „všetko alebo nič“: čiastočné zavedenie dáva čiastočnú ochranu. Šifrovaná komunikácia s niektorými kontaktmi a SMS s ostatnými je lepšia než SMS so všetkými. Nedokonalý pokrok je lepší než dokonalé ochromenie.

23.2 Skôr než začnete: použite model hrozieb

Skôr než si vyberiete kroky zavádzania, použite na svoju situáciu rámec modelovania hrozieb z kapitoly 22.[2] Vaše povolanie, jurisdikcia, verejný profil, vzťahy, finančná situácia aj politický kontext určujú, ktoré opatrenia sú vhodné a ktoré zbytočné. Určite si, ktoré informácie by pri odhalení

spôsobili vážnu škodu a ktoré by vás len zahanbili. Zdroje sústreďte na ochranu tých prvých; chrániť všetko rovnako znamená nechrániť účinne nič.

Toto zhodnotenie má predchádzať výberu nástrojov. Všeobecné rady rátajú so všeobecnými hrozbami, ale vaša situácia je konkrétna. Kroky nižšie sú usporiadané postupne, no ktorá úroveň je vhodná pre vás, závisí od vášho modelu hrozieb, nie od univerzálneho štandardu.

Pomôže hrubé pravidlo. Čitatelia, ktorým hrozí hlavne bežné vyťažovanie údajov alebo prienik do účtov, by mali začať základnou úrovňou. Tí, ktorí chcú znížiť finančné sledovanie alebo závislosť od platforiem, zvyčajne potrebujú aj strednú úroveň. Keď hrozba zahŕňa cielené vyšetrovanie alebo vážne oddelenie identít, pokročilá úroveň už nie je voliteľná.

23.3 Postupné kroky: od jednoduchých k pokročilým

Tieto úrovne sú prahy, nie vyznamenania za vážnosť. Zastavte sa, keď je váš model hrozieb pokrytý a postup je udržateľný.[3]

Začiatočnícka úroveň: základy

Základná úroveň rieši protivníkov, s ktorými sa stretáva väčšina ľudí: automatizované krádeže prístupových údajov a pasívne zbieranie údajov platformami a dátovými brokermi. Každé z nasledujúcich opatrení vychádza z konkrétnej hrozby, nie zo všeobecného odporúčania „buďte bezpečnejší“.

Opakované používanie hesiel je najbežnejšia slabina pri overovaní, lebo únik z jednej služby dá útočníkovi platné prihlasovacie údaje do každej ďalšej služby s rovnakým heslom. Správca hesiel túto triedu útokov odstráni, pretože vytvára pre každý účet jedinečné prihlasovacie údaje, a dosah škody pri jednom úniku sa tak zúži na danú službu.[4] Dvojfaktorové overenie rieši ďalší druh zlyhania: ukradnuté prihlasovacie údaje, ktoré fungujú, aj keď sú jedinečné. Hardvérové bezpečnostné kľúče s WebAuthn alebo FIDO2 odolávajú phishingu, lebo každé poverenie je pri registrácii kryptograficky viazané na konkrétnu doménu, ktorá ho vydala; prehliadač tento rozsah pri prihlásení vynucuje, takže falošná stránka nezíska podpis, ktorý by skutočná služba prijala. Kódy z autentifikačných aplikácií nie sú voči phishingu odolné v tom istom zmysle, pretože stránka, ktorá kód v reálnom čase prepošle, ho môže odovzdať skutočnej službe skôr, než vyprší, no stále pomáhajú proti hromadnému skúšaniu uniknutých hesiel (credential stuffing). Kódy v SMS sú najslabšie, lebo popri rovnakej zraniteľnosti voči preposielaniu pridávajú riziko prevzatia SIM karty (SIM swap)[22] a zachytenia u operátora.

Nešifrovanú komunikáciu vidí každý sprostredkovateľ, cez ktorého prechádza. Signal poskytuje end-to-end šifrovanie s minimálnym uchovávaním metadát. E-mail zo svojej povahy nie je súkromný; správy putujú cez

viaceré servery v otvorenom texte, ak odosielateľ aj príjemca nepoužívajú PGP alebo S/MIME, a aj vtedy zostávajú metadáta odhalené. Poskytovatelia, ktorí rešpektujú súkromie, znižujú vystavenie na strane servera pri nepracovnej komunikácii.[5]

Šifrovanie zariadenia rieši hrozbu fyzického prístupu: stratené alebo ukradnuté zariadenie bez šifrovania disku vydá celý svoj obsah tomu, kto ho drží. Prehliadač zameraný na súkromie zmenšuje plochu na sledovanie pri bežnom prehliadaní. Spoľahlivé prehliadače tohto druhu dnes zahŕňajú Mullvad Browser (práca Tor Browseru proti rozpoznávaniu prehliadača, prebalená na použitie v ľubovoľnej sieti) a LibreWolf (Firefox s predvolene použitým zosilňujúcim profilom arkenfox). Oba robia odtlačok prehliadača nerozlíšiteľným od odtlačkov ostatných používateľov toho istého prehliadača, a to je štrukturálna záruka, ktorú samotné blokovanie sledovačov nedá.[6]

E-mailové adresy slúžia ako univerzálne sledovacie identifikátory naprieč službami. Služby e-mailových aliasov vydávajú pre každú službu inú preposielaciu adresu, takže únik z ktorejkoľvek služby sa nedá prepojiť s inými službami, a existujú aj varianty na vlastný hosting pre tých, ktorí chcú, aby preposielacia infraštruktúra bežala na ich hardvéri.[7] Tieto opatrenia riešia najčastejšie slabiny s minimálnou zmenou životného štýlu; väčšina ľudí ich zvládne zaviesť cez víkend.

Stredná úroveň: rozšírenie ochrany

Stredná úroveň rieši inú triedu protivníkov: infraštruktúru finančného sledovania a zhromažďovanie údajov na úrovni platforiem. Základné opatrenia chránia pred príležitostnými útočníkmi; tieto začínajú odolávať systémovým pozorovateľom.

Kapitola 10 ukázala, že finančné sledovanie funguje hlavne cez kontrolné body, kde sa k transakciám pripája identita. Bitcoin získaný na burzách s plným KYC túto zraniteľnosť opakuje v novom médiu.[8] Burzy typu peer-to-peer a zarábanie bitcoinov priamo za tovar či služby znižujú prepojenie s identitou v mieste získania; bankomaty v niektorých jurisdikciách vyžadujú ľahšie overenie, no mnohé už žiadajú overenie totožnosti aj pri malých sumách, takže miestnu prax si treba overiť, skôr než sa na súkromie spoliehate.[23]

Míňanie je druhý povrch sledovania a Lightning rieši jeho časť. Platby idú cez kanály mimo reťazca s cibuľovým smerovaním, takže jednotlivé transakcie sa nezapisujú do základného blockchainu a každý sprostredkujúci uzol vidí len susedné skoky; tým odpadá trieda útokov závislých od verejného grafu transakcií, vrátane zhlukovania podľa opakovane použitej adresy a odhaľovania zvyšku. Súkromie je čiastočné, nie absolútne: otvorenia a uzavretia kanálov sa stále vysporiadavajú v reťazci ako UTXO, ktoré môže analytika reťazca skúmať; verejná topológia smerovania v spo-

jení s údajmi o čase a sumách môže prezradiť informácie, ak má peňaženka málo kanálov; a peňaženky smerujúce platby cez infraštruktúru jedného poskytovateľa vystavujú tok svojich platieb tomuto poskytovateľovi. Klient s vlastnou úschovou, pripojený k uzlu, ktorý používateľ sám prevádzkuje (jednou z možností je Zeus), zachová viac súkromia než riešenia závislé od poskytovateľa, ako je Phoenix, za cenu, že uzol musíte prevádzkovať sami.[9]

VPN (Mullvad, IVPN) rieši sieťového pozorovateľa tým, že šifruje prevádzku medzi zariadením a serverom VPN, čo bráni poskytovateľovi internetu alebo prevádzkovateľovi lokálnej siete skúmať, čo prehliadate. Obmedzenie je štrukturálne: VPN presúva dôveru z jedného sprostredkovateľa na iného a pozorovanie neodstráni, iba ho premiestni. Pochopiť toto obmedzenie je súčasťou modelu hrozieb, nie argument proti používaniu VPN.[10]

Útoky zamerané na ľudí, rozobrané v kapitole 22 (phishing, pretexting, sociálne inžinierstvo), nadobúdajú význam, keď sa súkromie konajúceho zlepšuje, pretože človek sa stáva najlacnejšou zostávajúcou plochou na útok. Povedomie o bezpečnosti je v tejto fáze hlavnou obranou proti útokom, na ktoré technické opatrenia nestačia, a kto ho považuje za doplnok, necháva otvorenú najväčšiu dieru. Podľa rovnakej logiky fungujú aj migrácia služieb (nahradenie platforiem nepriateľských voči súkromiu platformami, ktoré ho rešpektujú) a oddelenie identít (samostatné e-mailové adresy a účty na samostatné účely): každé znižuje počet bodov prepojenia, ktoré môže protivník využiť.

Pokročilá úroveň: silnejšia ochrana

Pri zvýšených modeloch hrozieb sú vhodné silnejšie opatrenia. Táto úroveň si vyžaduje značnú technickú investíciu, no dáva ochranu, ktorú nižšie úrovne dosiahnuť nevedia.

Pri sieťovej anonymite sa Nym snaží o silnejšiu ochranu proti časovej analýze, než dáva nízkolatenčný návrh Toru. Používa architektúru mixnetu, ktorá prevádzku zoskupuje do dávok a mení jej poradie. Tor však zostáva vyspelejšou a rozšírenejšou voľbou, s väčšími množinami anonymity a lepšími nástrojmi na každodenné použitie; na anonymné prehliadanie webu používajte Tor Browser. Prihlásenie do osobného účtu cez Tor vás neskryje pred samotnou službou, ktorá už vie, kto ste, ale reláciu stále chráni pred poskytovateľom internetu a každým pozorovateľom medzi vami a službou, takže voľba závisí od toho, ktorému protivníkovi sa chcete vyhnúť. Rozhoduje disciplína pri oddeľovaní identít: nemiešajte anonymné prehliadanie a osobné prihlásenia v tej istej relácii Tor Browseru a pri prechode medzi kontextmi použite funkciu New Identity alebo nový profil, aby sieťový pozorovateľ nemohol tieto dve veci prepojiť cez spoločný okruh. Na maximálnu ochranu slúži systém Tails, ktorý sa spúšťa z USB,

všetku prevádzku vedie cez Tor a na hostiteľskom počítači nezanechá nijakú stopu.[11]

Qubes OS izoluje aplikácie v oddelených virtuálnych strojoch: prehliadač v jednom, e-mail v druhom, a ani jeden sa v prípade kompromitácie nedostane k ostatným. Kompatibilita hardvéru je obmedzená (potrebné sú VT-x a VT-d, pozrite si zoznam kompatibility), no Qubes izoluje silnejšie než akýkoľvek prístup s jediným operačným systémom. Whonix[25] spúšťa dva virtuálne stroje (bránu, ktorá vedie všetku prevádzku cez Tor, a pracovnú stanicu izolovanú od fyzickej siete) a môže bežať aj v Qubes, čím spojí kompartmentalizáciu s anonymitou. GrapheneOS je zosilnený Android pre zariadenia Pixel s overeným štartom (verified boot) a zosilneným prideľovaním pamäte, navyše s voliteľným Google Play v izolovanom prostredí pre tých, ktorí potrebujú konkrétne aplikácie, ale nechcú Googlu dať práva na úrovni systému.[12]

Pri vážnej kompartmentalizácii (rozdelení na oddelené celky) majte pre oddelené identity oddelené zariadenia, kúpené za hotovosť a používané len z miest, ktoré s vami nikto nespája. Rôzne identity majú používať rôzne sieťové cesty: domáci internet pre skutočnú identitu, verejné WiFi alebo Tor pre anonymné činnosti, a pri VPN rôznych poskytovateľov, ak VPN slúžia na rôzne účely.

Vlastný hosting (e-mail cez Mail-in-a-Box, súbory cez Nextcloud) dáva maximálnu kontrolu, ale vyžaduje stálu údržbu. Pustite sa doň, len ak na to máte technické schopnosti aj čas.[13]

Fyzická bezpečnosť je základom digitálneho súkromia. Používajte heslá k firmvéru, zapnite overený štart a v nepriateľskom prostredí nikdy nenechávajte zariadenia bez dozoru. Pri vysokej hrozbe kupujte zariadenia nepredvídateľnými cestami, aby ste sa vyhli kompromitácii cez dodávateľský reťazec.

Jurisdikcia je štrukturálna premenná. Niektoré jurisdikcie chránia pred nútením k odhaleniu, iné nie. Svoje činnosti usporiadajte tak, aby ste mali úžitok z ochranných právnych rámcov.

Úroveň suverénneho hostiteľa

Nad pokročilou úrovňou leží užšia kategória praxe, ktorá presúva infraštruktúru zo vzťahu používateľa s komerčnými poskytovateľmi do jeho vlastnej domácnosti. Úroveň suverénneho hostiteľa je kategória, ktorú kniha architektonicky opisuje v každej kapitole o systémoch s vlastným hostingom, a za posledných niekoľko rokov dozrela do praktickej konfigurácie.

Základné súčasti tvorí bežný hardvér so špecifickými softvérovými stackmi. Malý server (často jednodoskový počítač alebo malý úsporný počítač) beží na distribúcii pre osobný server, ako je Start9 alebo Umbrel. Každá z nich balí desiatky aplikácií s predvoleným nastavením, ktoré uprednost-

ňuje súkromie pred pohodlím. Rovnako dobre poslúži starý notebook s voľným SSD a mnohé prvé nasadenia začínajú na hardvéri, ktorý mal skončiť v zásuvke alebo na recykláciu. Na tom istom hardvéri beží plný uzol Bitcoinu, takže peňaženka používateľa sa pýta jeho vlastného uzla, nie komerčného poskytovateľa. Popri uzle beží relay Nostr, takže sociálna prevádzka používateľa nejde cez cudzí relay, pokiaľ sa sám nerozhodne príspevky zdieľať aj inde. Úložisko je lokálne; zálohy sa šifrujú kľúčmi, ktoré používateľ ovláda, ešte skôr, než opustia zariadenie, takže externé kópie môžu ležať v cloudovom úložisku alebo na disku priateľa, a ten, kto ich drží, ich nemôže prečítať. Sieťová cesta vedie cez domáci internet a pre vybrané služby je k dispozícii Tor alebo I2P[24].

Architektonická vlastnosť suverénneho hostiteľa spočíva v tom, že odstraňuje cestu trojuholníkovej intervencie opísanú v kapitole 10. Komerčného poskytovateľa možno prinútiť, aby sledoval svojich zákazníkov; suverénny hostiteľ odpovedá len fyzickej kontrole svojho majiteľa. Cesta nátlaku, s ktorou počíta regulačná architektúra, stále existuje pri poskytovateľovi domáceho internetu, ale údaje, ktoré cez toto potrubie tečú, sú šifrované, a vzorce prevádzky viditeľné pre poskytovateľa prezrádzajú, že používateľ hostuje vlastné služby, nie čo hostuje.

Štruktúra nákladov sa zmenila tak, že táto úroveň je dostupná. Malý server, ktorý zvládne plný uzol Bitcoinu aj relay Nostr, stojí zhruba toľko ako smartfón strednej triedy a znovu využitý starý notebook nestojí nič. Softvérové stacky sú zadarmo a spravujú ich aktívne komunity. Údržba je reálna (bezpečnostné aktualizácie a disciplína pri zálohovaní), no pre používateľa so základnou technickou zručnosťou sa zmestí do niekoľkých hodín mesačne. Táto úroveň sa z profesionálnej správy systémov presunula do praxe odhodlanej podskupiny strednej úrovne.

Čo suverénny hostiteľ v predvolenom stave nedáva, je anonymita polohy. Hostiteľ stojí na domácej adrese používateľa a jeho IP adresa označuje domácnosť pre každého, kto vie priradiť IP adresu k polohe pomocou bežných komerčných geolokačných databáz. Používateľ vo zvýšenom ohrození môže túto medzeru zatvoriť tak, že služby hostiteľa sprístupní ako skryté služby Tor, alebo pripojenie zakryje dôveryhodnou VPN, takže prichádzajúce dotazy domácu IP adresu nikdy nevidia. Ani bez týchto opatrení hodnota architektúry nezaniká: bežný občan tak odopiera komerčnému sledovaciemu aparátu rutinnú prevádzku, ktorú by inak zozbieral. Model hrozieb je nižší než model anonymity na pokročilej úrovni a investícia je úmerne menšia.[14]

Lokálna inferencia AI na suverénnom hostiteľovi

Veľké jazykové modely sa stali ďalšou kategóriou infraštruktúry, ktorú môže suverénny hostiteľ prevziať. Požiadavka (prompt) poslaná modelu v cloude je odhalená preferencia vydaná prevádzkovateľovi v otvorenom

texte a o tom, čo sa s ňou stane potom, rozhodujú prevádzkovateľove podmienky služby a pravidlá uchovávania. Požiadavka spracovaná lokálne spusteným modelom zariadenie používateľa nikdy neopustí, a preto žiadne podmienky služby nerozhodujú, čo s ňou prevádzkovateľ urobí, lebo prevádzkovateľ neexistuje. Zdravotné, finančné, právne a osobné otázky, ktoré by používatelia neradi zverili hostovanej službe, možno spracovať lokálne bez toho, aby ich niekomu odhalili.

Nástroje za posledné tri roky dozreli. llama.cpp je referenčný inferenčný engine v C++, ktorý spúšťa kvantizované modely s otvorenými váhami na bežnom hardvéri vrátane spotrebiteľských notebookov a mobilných zariadení; kvantizačný formát GGUF je de facto výmenný formát pre modely s otvorenými váhami. Ollama obaľuje llama.cpp rozhraním pre vývojárov, ktoré rieši sťahovanie modelov a lokálne poskytovanie API; LM Studio a GPT4All ponúkajú grafické rozhrania pre používateľov, ktorí nie sú vývojári. Framework MLX od Applu cieli priamo na Apple Silicon a rozhranie Foundation Models od Applu sprístupňuje aplikáciám tretích strán modely s 3 miliardami parametrov priamo na zariadení, a to od vydaní operačných systémov z roku 2025. Nvidia NIM poskytuje modely v kontajneroch pre firemné nasadenie s vlastným hostingom. Nič z toho nie sú modely so špičkovými schopnosťami v zmysle najväčších hostovaných modelov a rozdiel medzi špičkovými a lokálnymi modelmi sa každý rok zmenšuje.[15]

Kompromis, ktorý táto kategória ukladá používateľovi, je schopnosť oproti súkromiu. Špičkový model hostovaný poskytovateľom cloudu dá pri mnohých úlohách lepšie odpovede než najväčší lokálne nasaditeľný model a používateľ, ktorý cloudový kompromis prijme, prijal aj tok údajov, ktorý z neho vyplýva. Používateľ, ktorý ho odmietne, prijme zníženie špičkových schopností a dostane za to štrukturálnu záruku: nijaká vzdialená strana požiadavku nevidí, pretože zo zariadenia nič neodchádza. Pri väčšine otázok dôležitých pre súkromie (zdravotných, finančných, osobných) je lokálne nasaditeľný model dosť schopný a záruka súkromia platí bez ohľadu na správanie akéhokoľvek poskytovateľa. Suverénny hostiteľ je miesto, kde táto kategória v praxi žije: ten istý hardvér, ktorý poháňa uzol Bitcoinu a relay Nostr, poháňa aj lokálny model a inferenčná záťaž prirodzene zapadá medzi ostatné služby s vlastným hostingom na tom istom zariadení.

Čo postupné zavádzanie prináša

Postupné zavádzanie slúži viacerým účelom. Každá úroveň buduje schopnosti pre ďalšiu: používanie správcu hesiel pripravuje na správu kľúčov a základné šifrovanie na sofistikovanejšie kryptografické nástroje. Postupná zmena dáva novým postupom čas stať sa návykmi, než pribudnú ďalšie, pretože pokus o všetko naraz vedie k vzdaniu sa. Začať opatreniami

s veľkým dosahom zaručí, že obmedzené zdroje pokryjú najzávažnejšie slabiny ako prvé. Každý krok niečo naučí; praktická skúsenosť ukáže, ktoré hrozby sú dôležité a ktoré nástroje sú pre vás udržateľné.[16]

23.4 Hľadanie komunity

Úloha komunity

Súkromie sa často vníma ako individuálna prax, no komunita rozširuje to, čo jednotlivci dokážu. Prijatie nástroja si vyžaduje protistrany: šifrovaná komunikácia potrebuje ďalších, ktorí používajú kompatibilné nástroje, a transakcie v Bitcoine potrebujú ľudí, ktorí Bitcoin prijímajú. Vďaka sieťovým efektom rastie užitočnosť nástroja s jeho rozšírením vo vašej sieti. Členovia komunity sa delia o poznatky o nástrojoch a nových hrozbách; učenie sa zo skúseností iných urýchľuje rozvoj zručností a pomáha vyhnúť sa bežným chybám. Technické problémy a nepriaznivé situácie sa dajú ľahšie zvládnuť s podporou komunity; izolácia sťažuje udržať prax súkromia. Niektoré postupy súkromia si vyžadujú dôveryhodné protistrany, lebo obchodovanie peer-to-peer aj spoločné projekty potrebujú ľudí, ktorým môžete dôverovať.

Miestne komunity okolo Bitcoinu a súkromia

Miestne komunity dávajú osobný kontakt, ktorý buduje dôveru účinnejšie než samotná online interakcia. V mnohých mestách sa pravidelne konajú bitcoinové meetupy (stretnutia komunity), ktoré poskytnú úvod do komunity a možné obchodné vzťahy; kvalita sa líši, preto ak je z čoho vyberať, navštívte viac z nich. Makerspacy a hackerspacy sa často prekrývajú s komunitami zameranými na súkromie a ponúkajú prostredie na učenie aj spoločenské väzby. Konferencie o Bitcoine a súkromí dávajú intenzívny kontakt s komunitou, hoci kvalita je rôzna a pred účasťou je vhodné si veci preveriť. Komunita môže vzniknúť aj prirodzene z existujúcich vzťahov: priatelia či kolegovia, ktorí zdieľajú obavy o súkromie, sa môžu stať sieťou vzájomnej podpory.

Tieto komunity fungujú aj ako fyzické predmostia. Meetup je miesto, kde sa online prezývky menia na zapamätané tváre a kde budúce protistrany zistia, kto sa ukazuje. Paralelná ekonomika rastie rýchlejšie, keď sa digitálna dôvera stretne s fyzickou prítomnosťou.

Opakovaný workshop alebo stretnutie v makerspace sa často stane miestom, kde ľudia vyskúšajú nástroje a uskutočnia prvé malé obchody, kým miestna dôvera nenarastie natoľko, že väčší obchod sa dá aspoň zvážiť. Hranica medzi komunitou a obchodom je často tenká z dobrého dôvodu: opakovaná výmena je jeden zo spôsobov, ako komunity zisťujú, či spolu môžu uniesť skutočný hospodársky život.[17]

Online komunity

Online komunity siahajú za geografické hranice. Nostr, decentralizovaný sociálny protokol, umožňuje pseudonymnú účasť s odolnosťou voči cenzúre; hľadanie komunít zameraných na súkromie v sieti Nostr dáva kontakt bez kontroly zo strany platformy.[18] Matrix a Element ponúkajú federovaný chat so šifrovaním a existujú rôzne miestnosti zamerané na súkromie.[26] IRC je stále živé v technických komunitách a komunitách zameraných na súkromie. O nástrojoch a postupoch súkromia sa diskutuje na rôznych fórach a diskusných tabuliach, hoci kvalita je rôzna a zdroje treba hodnotiť kriticky.

Online komunity nesú riziko protistrany, ktoré miestne meetupy môžu čiastočne vyriešiť fyzickou prítomnosťou. Online sa nedá overiť, s kým komunikujete, a tá istá pseudonymita, ktorá chráni poctivých účastníkov, chráni aj zlých aktérov. Orgány činné v trestnom konaní si pestujú informátorov v online priestoroch rovnako ochotne ako vo fyzických a deklarované hodnoty komunity nedávajú nijakú záruku skutočného zloženia jej členstva. Dôvera by sa mala vyvíjať pomaly, cez pozorované správanie v mnohých interakciách, nie cez tvrdené poverenia alebo rýchlu intimitu. Ten, kto sám ponúka informácie o vašej identite, nezvyčajne rýchlo tlačí na dohodnutie osobného stretnutia alebo kladie podrobné otázky o operačných podrobnostiach skôr, než existuje nejaká história, si zaslúži opatrnosť, nie zapojenie.

Rozvoj dôvery v čase

Dôvera sa získava dôsledným správaním v čase.[19] Mechanizmus je jednoduchý a pomalý: opakované interakcie s nízkou stávkou vytvárajú históriu a tá sa stáva dôkazom, na ktorom stoja väčšie záväzky. Začnite účasťou v diskusiách a komunitných aktivitách, ešte než sa pustíte do čohokoľvek s vysokou stávkou. Dôsledné a spoľahlivé správanie počas mesiacov je skutočný dôkaz; nedôslednosť či nespoľahlivosť je tiež skutočný dôkaz. Dôveru rozširujte postupne podľa skúsenosti a stiahnite ju, keď správanie odporuje doterajšiemu vzorcu. Skratka, ktorá by vytvorila skutočnú dôveru rýchlejšie než čas, neexistuje a pocit rýchleho spojenia s novým členom komunity je pravdepodobnejšie znak sociálneho inžinierstva než dôkaz skutočnej blízkosti.

Kompartmentalizácia platí vo vnútri dôveryhodných komunít rovnako ako mimo nich. Dôveryhodný kontakt sa dozvie to, čo potrebuje pre danú interakciu, nie všetko, na čom pracujete. Členstvo v komunite neodstraňuje riziko, že účastník je informátor, je pod tlakom alebo raz urobí chybu, ktorá odhalí, čo vie. Disciplína obmedzeného odhaľovania nie je nedôvera voči jednotlivcovi; je to uznanie, že dôvera a vystavenie sú dve rôzne otázky a treba ich riadiť osobitne.

Budovanie obchodných vzťahov

Obchodovanie peer-to-peer vyžaduje dôveryhodné protistrany a hlavným filtrom je reputácia. Zavedení členovia komunity s verejnou históriou poctivých obchodov sú pre vás menším rizikom než cudzí ľudia, lebo majú čo stratiť. Prvé obchody majú byť také malé, aby sa strata dala zniesť; veľkosť sa zvyšuje, až keď sa opakovanými úspešnými výmenami vytvorí história. Ponáhľať sa s veľkým obchodom skôr, než história existuje, je častá chyba, ktorá sústredí všetko učenie do jednej drahej udalosti.

Escrow (úschova s podmienkou uvoľnenia) znižuje riziko pre obe strany pri obchodoch s neznámymi protistranami: prostriedky sú pod spoločnou kontrolou, kým sa nepotvrdí dodanie, nie pod jednostrannou mocou jednej strany. Mechaniku rozoberá kapitola 24. Pri každej dokumentácii, ktorá chráni niektorú stranu, treba kompromis medzi dôkazom a vystavením súkromia posúdiť podľa skutočného modelu hrozieb. Podpísaná potvrdenka, ktorá dokazuje dodanie, vytvára aj záznam; či je tento záznam záťažou, závisí od toho, kto ho môže niekedy vidieť.[20] [21]

23.5 Od individuálnej praxe k spoločnej praxi

Prax súkromia sa začína u jednotlivcov, lebo jednotlivci môžu svoje návyky zmeniť ako prví, a trvalou sa stane až vtedy, keď podľa nej začnú konať aj ľudia okolo nich v tej istej infraštruktúre. Domácnosť, ktorá používa šifrovanú komunikáciu, alebo miestny okruh obchodníkov, ktorí obchodujú cez opakujúce sa protistrany, prekročili prah. Súkromie už nie je izolovaná preferencia. Mení sa na hospodársku prax.

Koordinácia v domácnosti

Domácnosti potrebujú spoločné pravidlá. Jeden človek, ktorý verejne zdieľa rodinné rozvrhy, môže zmariť starostlivú disciplínu pri ochrane polohy u iného. Jeden z manželov, ktorý používa mince spojené s burzou na citlivé nákupy, môže vystaviť toho druhého. Jedno dieťa, ktoré používa rodinný tablet s účtami na skutočné meno, môže zrútiť oddelenie identít pre všetkých, ktorí zariadenie zdieľajú.

Začnite jednoduchými dohodami. Rozhodnite, ktoré komunikačné nástroje bude domácnosť používať na citlivé veci a ktoré zariadenia sú spoločné a ktoré osobné. Určte, čo si pred odhalením vyžaduje spoločný súhlas. Ak domácnosť používa Bitcoin, rozhodnite, ktoré zostatky sú na míňanie a ktoré dlhodobé úspory, a ako sa uložia záložné materiály.

Malé tímy a podnikanie

Rovnaká logika platí pre tímy a malé firmy. Podnik, ktorý chce mať aspoň trochu súkromia, nemôže fungovať s predpokladom, že každý zamestnanec používa tú istú identitu a rovnaké komunikačné návyky pri každej

úlohe; roly treba oddeliť a verejný účet nie je to isté ako prevádzkový kľúč. Komunikácia s dodávateľmi nie je to isté ako verejný marketing. Zákaznícka podpora nie je to isté ako správa pokladnice.

Začnite jednou obchodnou líniou, ktorá sa dá vyrovnať po čistejších kanáloch. Bitcoin zarábajte priamo, kde sa dá. Medzi verejnou reputáciou a súkromnou prevádzkou držte jasnú hranicu a správu pokladnice oddeľte od oboch. Najprv používajte malé protistrany. Skôr než poskytnete veľkú dôveru, vybudujte opakovaný obchod. Ak podnik závisí od súkromia, má vedieť, ktoré záznamy potrebuje, kde ležia, kto k nim má prístup a koľko jeho činnosti stále závisí od kontrolných bodov bánk alebo platforiem.

Jedným praktickým vstupným bodom je sprostredkujúci obchodník (proxy merchant). V jednom prípade je touto rolou OTC zmenárnik[27], v inom nákupný agent alebo koordinátor osobného odberu. Rola sústreďuje vystavenie na jedno miesto. Jeden dôveryhodný špecialista zvládne hranicu a ocení riziko, takže desiatim ľuďom odpadne desať samostatných kontaktov so sledovanou stranou ekonomiky. Nebezpečná je koncentrácia, preto majú tieto roly zostať viaceré a nahraditeľné.

Prvý obchodný okruh

Prvým cieľom nie je rozsah. Prvým cieľom je jeden uzavretý okruh: zarobiť súkromne, minúť súkromne a znova. Dizajnér, ktorý prijme platbu v Bitcoine a v Bitcoine zaplatí dodávateľa, takýto okruh začal. Miestny obchodník, ktorý nakupuje od jedného dodávateľa dbajúceho o súkromie a predáva stálym zákazníkom cez priame správy, ho začal tiež. Malý tím ho začal, keď sa koordinuje cez šifrované kanály a kľúče od pokladnice drží oddelene od každodenných správ.

Keď okruh funguje, môže zhustnúť. Protistrana sa stane známou, obchod sa opakuje; čo sa zdalo ako pokus, sa stane obyčajným. Súkromná prax sa zmení na návyk.

23.6 Čo nerobiť

Neohlasujte svoje úmysly verejne

Častá chyba začiatočníkov je verejné ohlasovanie úmyslu chrániť súkromie. Oznámenie, že „idete do súkromia“, púta pozornosť tých, ktorí by si vás inak nevšimli; protivníci, ktorí nevedeli, že existujete, teraz vedia, že sa čosi snažíte skryť. Verejné oznámenie vytvára východisko, voči ktorému sa zmeny merajú, a váš posun sa stáva viditeľným, hoci tichú zmenu by bolo ťažšie odhaliť. Vytvára tiež spoločenský tlak buď uspieť úplne, alebo byť vnímaný ako neúspešný, a ten je zbytočný a kontraproduktívny. Oznámenie často obsahuje aj informácie o zamýšľaných metódach, čím vzniká plán pre protiopatrenia protivníka.

Lepší postup: zavádzajte potichu. O postupoch súkromia nehovorte s tými, ktorí to nepotrebujú vedieť. Ak sa vás niekto spýta, dajte minimum informácií.

Nedôverujte príliš rýchlo

Komunita je cenná, no dôveru si treba zaslúžiť. Informátori existujú: orgány činné v trestnom konaní si pestujú informátorov v komunitách, ktoré ich zaujímajú, a nadšení nováčikovia niekedy nie sú tým, čím sa zdajú. Podvodníci cielia na komunity s cennými aktívami, ako sú kryptomeny, alebo so zneužiteľným idealizmom. Existujú aj ľudia pod nátlakom: tí, ktorí čelia právnemu tlaku, môžu s protivníkmi spolupracovať, aby znížili vlastné riziko, a dobre mienení ľudia so slabou bezpečnostnou praxou môžu neúmyselne vystaviť tých, s ktorými sú spojení.

Dôvera sa má vyvíjať pomaly, cez pozorované správanie. Mimoriadne tvrdenia alebo rýchla intimita sú varovné znaky.

Nekomplikujte zbytočne

Zložitosť je nepriateľ bezpečnosti. Zložité systémy majú viac spôsobov zlyhania: každá ďalšia súčasť je ďalší možný bod zlyhania, a jednoduché systémy sa dajú lepšie zabezpečiť a udržiavať. Zložité postupy sa opúšťajú: tie, čo si vyžadujú stálu pozornosť alebo veľké úsilie, sa zahodia, keď do života vstúpi niečo iné, takže udržateľné postupy musia byť zvládnuteľné. Zbytočne prepracované nástroje tam, kde stačia jednoduché, môžu pútať pozornosť; opatrenia primerané vášmu modelu hrozieb sú lepšie než maximálne opatrenia bez ohľadu na hrozbu. Zložité systémy navyše spotrebúvajú viac duševných zdrojov a obmedzená pozornosť sa má sústrediť na hrozby, na ktorých záleží, nie na teoretické hrozby, ktoré riešia sofistikované opatrenia.

Opatrenia prispôsobte skutočným hrozbám. O vhodných opatreniach rozhoduje protivník, ktorému čelíte, nie ten, ktorému by ste teoreticky čeliť mohli.

Nepodceňujte schopnosti protivníka

Opačná chyba je rovnako nebezpečná. Existujú sofistikovaní protivníci: spravodajské služby a dobre financovaní zločinci majú schopnosti, ktoré presahujú bežné poznanie, a preto nepredpokladajte, že všeobecne známe protiopatrenia pokryjú všetky útoky. Schopnosti sa vyvíjajú: čo je dnes bezpečné, zajtra už nemusí byť, a včerajšia najlepšia prax môže byť dnešnou slabinou. Neznáme zraniteľnosti existujú a nemožno sa brániť proti útokom, o ktorých neviete, že existujú; pokora voči hraniciam vlastného poznania je namieste. Sociálne inžinierstvo obchádza technické opatrenia: najsofistikovanejšie šifrovanie nechráni pred protivníkom, ktorý vás oklame, aby ste informácie vyzradili.

Bezpečnosť vyžaduje rovnováhu: ani paranoju, ktorá bráni konať, ani sebauspokojenie, ktoré pozýva kompromitáciu.

Časté chyby, ktorým sa vyhnúť

Disciplína pri zálohovaní je vyvažovanie: kľúče bez zálohy sa stratia, keď zariadenie zlyhá, no neopatrné zálohy zväčšujú útočnú plochu. Fyzická bezpečnosť je základom všetkého, lebo digitálna bezpečnosť nič neznamená, ak protivník môže pristúpiť k vašim zariadeniam alebo sledovať vaše obrazovky. Jediné body zlyhania si vyžadujú redundanciu a kompartmentalizáciu. Známe zraniteľnosti sa aktívne zneužívajú, preto je treba bezpečnostné aktualizácie inštalovať bezodkladne. Zanedbanie metadát je obzvlášť zákerné: šifrovaný obsah neskrýva, kto s kým komunikuje ani kedy, a analýza metadát zmarí šifrovanie, ktoré chráni iba obsah.

Zhrnutie kapitoly

Zavádzanie súkromia je postupné, nie binárne. Účinná prax sa buduje od základných opatrení (správa hesiel, dvojfaktorové overenie, šifrovaná komunikácia, šifrovanie zariadení) cez stredné kroky (Bitcoin, Lightning, VPN, kompartmentalizácia) až po pokročilé postupy (Tor, Qubes, GrapheneOS, úplné oddelenie identít). Každá úroveň buduje schopnosti pre ďalšiu a zároveň dáva okamžitú ochranu, pričom to, ktorá úroveň je vhodná, závisí od modelu hrozieb, nie od univerzálneho štandardu. Nad pokročilou úrovňou stojí úroveň suverénneho hostiteľa: malý server alebo znovu využitý starý notebook s Start9 či Umbrel, ktorý na domácom pripojení používateľa hostí plný uzol Bitcoinu a relay Nostr spolu s celou sadou aplikácií s vlastným hostingom. Cena hardvéru klesá od ceny smartfónu strednej triedy až na nulu, keď je platformou notebook, ktorý mal skončiť v zásuvke. Táto úroveň odstraňuje cestu trojuholníkovej intervencie, ktorá núti komerčných poskytovateľov sledovať zákazníkov, lebo suverénny hostiteľ odpovedá len fyzickej kontrole svojho majiteľa. Ten istý hardvér dnes môže spúšťať aj lokálnu inferenciu AI, takže požiadavky natoľko zdravotné, právne či osobné, že by ich používatelia cloudovému poskytovateľovi nezverili, zariadenie vôbec neopustia. Anonymitu polohy táto úroveň neponúka; ponúka to, že komerčný sledovací aparát nezozbiera rutinnú prevádzku, ktorú by inak získal.

Komunita rozširuje to, čo jednotlivci dokážu sami. Prijatie nástroja si vyžaduje protistrany a dôvera vzniká opakovanou interakciou. Miestne meetupy fungujú ako fyzické predmostia, kde sa online prezývky menia na zapamätané tváre a paralelná ekonomika rastie cez opakovaný obchod. Zavádzanie presahuje aj osamelého používateľa. Domácnosti a malé podniky potrebujú spoločné pravidlá: ktoré komunikačné kanály používať na citlivé veci a ako oddeliť kľúče od pokladnice od každodenného prevádz-

kového prístupu. Prvým zmysluplným úspechom je obchodný okruh, ktorý súkromne zarába a míňa a potom sa opakuje.

Sprostredkujúci obchodníci pomáhajú okruhu rozbehnúť sa skôr. OTC zmenárnici a nákupní agenti umožňujú malým sieťam obchodovať skôr, než sa každý účastník dokáže celkom spoľahnúť na súkromné kanály.

Nijaký jediný nástroj ani konfigurácia nedáva sama o sebe dostatočnú ochranu. Nástroje slúžia modelom hrozieb a všeobecné rady rátajú so všeobecnými hrozbami; účinná ochrana si vyžaduje osobné zhodnotenie, ktoré rozvíja kapitola 22. Paralelná ekonomika tiež nie je pripravená na úplný odchod zo systémov pod dohľadom štátu. Zavádzanie je postupné a dnešná paralelná ekonomika starý systém dopĺňa, nenahrádza. Kapitola 25 zhrnie celý argument, posúdi, čo už pracovné nástroje dosiahli a čo ešte nie je vybudované, a priamo odpovie na úvodnú výzvu knihy. Súkromie je priebežná prax; treba sa pýtať, či sa z miesta, kde ste teraz, posúvate dopredu, a odpoveď závisí od toho, že tam začnete, zlepšíte, čo sa zlepšiť dá, a nájdete komunitu, vďaka ktorej je prax udržateľná.

Poznámky

[1] Moxie Marlinspike, „The Network in Motion“, Moxie Marlinspike (blog), 2016, `https://moxie.org/2016/01/17/network-protocols.html`. Marlinspike je spoluzakladateľ Signalu a píše o návrhu kryptografických protokolov; esej tvrdí, že statické predpoklady o protokoloch sa rozpadajú, keď sa sieťová vrstva pod nimi vyvíja.

[2] Metodiku modelovania hrozieb zrozumiteľnú aj pre nešpecialistov nájdete v „Your Security Plan“, Electronic Frontier Foundation, Surveillance Self-Defense guide, `https://ssd.eff.org/en/module/your-security-plan`. Formálne spracovanie z pohľadu bezpečnostného inžinierstva je Adam Shostack, *Threat Modeling: Designing for Security* (Wiley, 2014), ktoré pokrýva STRIDE a príbuzné rámce a je štandardnou referenciou. Ross Anderson, *Security Engineering*, 3. vyd. (Wiley, 2020), citované v kapitole 22, pozn. 2. Kratší praktický sprievodca pre novinárov a aktivistov sú školiace materiály o digitálnej bezpečnosti od Freedom of the Press Foundation na `https://freedom.press/training/`.

[3] Micah Lee, „A DIY Guide to Feminist Cybersecurity“, *The Intercept*, November 12, 2017, `https://theintercept.com/2017/11/12/a-diy-guide-to-feminist-cybersecurity/`, je najlepší krátky úvod do postupného zavádzania súkromia pre čitateľov bez technického zázemia. Martin Shelton udržiava aktuálne odporúčania krok za krokom na `https://martinshelton.medium.com`. Príručka Surveillance Self-Defense od Electronic Frontier Foundation na `https://ssd.eff.org` obsahuje návody na modelovanie hrozieb, tutoriály k nástrojom a taktické scenáre („Attending a Protest“, „Crossing the US Border“ a ďalšie). Pre najprísnejšie taktické oddelenie je rozhodujúcou príručkou Michael Bazzell, *Extreme Privacy: What It Takes to Disappear*, 5. vyd. (2023); Bazzellov sprievodný podcast *The Privacy, Security, and OSINT Show* udržiava techniky aktuálne.

[4] KeePassXC (`https://keepassxc.org`) je multiplatformový správca hesiel s otvoreným zdrojovým kódom, ktorý ukladá lokálnu šifrovanú databázu; Bitwarden (`https://bitwarden.com`) je alternatíva s otvoreným zdrojovým kódom a synchronizáciou cez cloud, s voliteľnými servermi na vlastný hosting (Vaultwarden,

https://github.com/dani-garcia/vaultwarden, je obľúbený kompatibilný server na vlastný hosting napísaný v Ruste). Metodiku a návody na modelovanie hrozieb nájdete v príručke Surveillance Self-Defense od Electronic Frontier Foundation o správcoch hesiel na https://ssd.eff.org/en/module/animated-overview-using-password-managers-stay-safe-online. K zlyhaniam overovania heslom vo veľkom rozsahu pozri prácu Troya Hunta na https://haveibeenpwned.com. K prístupovým kľúčom (passkeys) a štandardu WebAuthn/FIDO2, o ktorý sa opiera overovanie viazané na hardvér, pozri špecifikáciu W3C na https://www.w3.org/TR/webauthn-3/ a prehľad FIDO Alliance na https://fidoalliance.org/how-fido-works/.

[5] Softvér základnej úrovne spomenutý v tomto odseku: Signal (https://signal.org) je end-to-end šifrovaný komunikátor rozobraný v kapitole 17; špecifikácia jeho protokolu Double Ratchet je na https://signal.org/docs/specifications/doubleratchet/. ProtonMail (https://proton.me/mail) je švajčiarsky poskytovateľ e-mailu so šifrovaním na strane klienta pre správy medzi používateľmi Protonu a s podporou OpenPGP pre správy na externé adresy. Tutanota (premenovaná na Tuta, https://tuta.com) je nemecký poskytovateľ e-mailu s end-to-end šifrovaním pre správy medzi používateľmi Tuty. Pri šifrovaní uložených údajov na disku je FileVault vstavané šifrovanie celého disku v Apple macOS, BitLocker v Microsoft Windows a LUKS (Linux Unified Key Setup, https://gitlab.com/cryptsetup/cryptsetup) je štandard šifrovania diskov v Linuxe, ktorý používa väčšina veľkých distribúcií. Firefox (https://www.mozilla.org/firefox/) so zosilnenou konfiguráciou user.js zameranou na súkromie (arkenfox-user.js na https://github.com/arkenfox/user.js je najlepšie udržiavaný profil) zmenšuje plochu pre rozpoznávanie prehliadača a telemetriu; Brave (https://brave.com) je fork Chromia so vstavaným blokovaním sledovačov a odtlačkov. uBlock Origin (https://github.com/gorhill/uBlock) je referenčný blokovač obsahu s otvoreným zdrojovým kódom. K nástrojom na šifrovanie obsahu všeobecnejšie: GnuPG (https://gnupg.org) zostáva referenčnou implementáciou OpenPGP a age (https://age-encryption.org), ktorý navrhol Filippo Valsorda, je moderný nástroj na šifrovanie súborov s malou plochou a oveľa jednoduchším modelom hrozieb než PGP.

[6] Mullvad Browser je práca Tor Browseru proti rozpoznávaniu prehliadača prebalená na použitie v ľubovoľnej sieti; LibreWolf je Firefox s predvolene použitými nastaveniami arkenfox. Oba dbajú predovšetkým na to, aby sa odtlačok prehliadača nedal rozlíšiť od odtlačkov ostatných používateľov toho istého prehliadača. Mullvad Browser, https://mullvad.net/en/browser, spolupráca projektu Tor a Mullvadu. LibreWolf, https://librewolf.net/, so zdrojovým kódom na https://codeberg.org/librewolf. Profil Arkenfox user.js, https://github.com/arkenfox/user.js. K modelu hrozieb pri rozpoznávaní prehliadača, ktorému sa tieto prehliadače venujú, pozri Peter Eckersley, „How Unique Is Your Web Browser?“ *Privacy Enhancing Technologies Symposium 2010*, a EFF Cover Your Tracks, https://coveryourtracks.eff.org/. Tor Browser, https://www.torproject.org/download/, zostáva referenčným štandardom pre prehliadanie s anonymitou cez Tor a obsahuje tie isté obrany proti rozpoznávaniu, ktoré preberá Mullvad Browser.

[7] SimpleLogin (Proton AG) a Addy.io sú služby e-mailových aliasov s otvoreným zdrojovým kódom, ktoré sa dajú hostovať vo vlastnej réžii; DuckDuckGo Email Protection a Apple Hide My Email sú pohodlné riešenia, pri ktorých preposielajúci poskytovateľ vidí e-mail v otvorenom texte; štrukturálny prínos je rôzna preposielacia adresa pre každú službu, takže únik z ktorejkoľvek služby sa nedá prepojiť s inými. SimpleLogin, https://simplelogin.io/, so zdrojovým kódom na

https://github.com/simple-login/app. Addy.io (predtým AnonAddy), https://addy.io/, so zdrojovým kódom na https://github.com/anonaddy/anonaddy. DuckDuckGo Email Protection, https://duckduckgo.com/email/. Proton Pass (s integráciou SimpleLogin), https://proton.me/pass. Apple Hide My Email, https://support.apple.com/en-us/HT210425. Firefox Relay od Mozilly, https://relay.firefox.com/, je ďalšia hlavná alternatíva. K všeobecnej kritike univerzálnych sledovačov, ktorá e-mailové aliasy odôvodňuje, pozri prácu OpenWPM Arvinda Narayanana a spolupracovníkov na Princetone, https://webtransparency.cs.princeton.edu, ktorá dokumentuje sledovanie naprieč službami na základe e-mailu.

[8] Stránka o súkromí na Bitcoin Wiki, https://en.bitcoin.it/wiki/Privacy, je najlepšie udržiavaná encyklopedická referencia o praxi súkromia špecifickej pre Bitcoin; pokrýva opakované používanie adries, odhaľovanie zvyšku, heuristiky spoločného vlastníctva vstupov, varianty CoinJoin a súkromie vo vrstve Lightning. Praktické spracovania: priebežná analýza 0xB10C na https://b10c.me/ a https://transactionfee.info pokrýva techniky analýzy reťazca a obrany. Dokumentácia Sparrow Wallet na https://sparrowwallet.com/docs pokrýva kontrolu mincí (coin control), hygienu štítkov a integráciu PayJoin. Kapitola 20 rozvíja celý model hrozieb pre graf transakcií; jej pozn. 14 uvádza úplný súbor funkčných nástrojov.

[9] Zeus je peňaženka Lightning s vlastnou úschovou, ktorá sa pripája k uzlu Lightning prevádzkovanému používateľom a zachováva súkromie platieb tým, že informácie o smerovaní ostávajú na používateľovom vlastnom uzle, nie v infraštruktúre poskytovateľa; https://zeusln.app/, so zdrojovým kódom na https://github.com/ZeusLN/zeus. Phoenix je peňaženka Lightning s vlastnou úschovou, ktorá na správu kanálov používa LSP (ACINQ); zjednodušuje nastavenie za cenu viditeľnosti smerovania pre poskytovateľa; https://phoenix.acinq.co/, so zdrojovým kódom na https://github.com/ACINQ/phoenix. K širšiemu modelu súkromia v Lightningu a predpokladom dôvery voči LSP pozri lightningprivacy.com a kapitolu 20, pozn. 12.

[10] Mullvad VPN, https://mullvad.net/, je švédsky poskytovateľ VPN bez záznamov, ktorý prijíma anonymné platby; IVPN, https://www.ivpn.net/, je poskytovateľ bez záznamov registrovaný na Gibraltári, s uverejneným warrant canary. Obaja patria k poskytovateľom, ktorých nezávislé audity odporúčajú najčastejšie. K nezávislým auditom VPN pozri audity uverejnené Mullvadom na https://mullvad.net/en/blog/tag/audits a IVPN na https://www.ivpn.net/blog/. K štrukturálnemu obmedzeniu, že všetky VPN dôveru presúvajú, nie odstraňujú, pozri vysvetlenie EFF na https://ssd.eff.org/en/module/choosing-vpn-thats-right-you.

[11] Nym je protokol mixnetu, ktorý dáva silnejšiu ochranu metadát než nízkolatenčné cibuľové smerovanie Toru tým, že pakety zoskupuje do dávok a mení ich poradie cez zmiešavacie uzly; https://nymtech.net/, so špecifikáciou protokolu na https://github.com/nymtech/nym. Tor Browser, referenčný nástroj pre anonymitu na webe v sieti Tor, je na https://www.torproject.org/download/. Tails je amnezický živý operačný systém, ktorý sa spúšťa z USB, vedie všetku prevádzku cez Tor a na hostiteľovi nezanecháva trvalú stopu; https://tails.boum.org/. K rozdielom medzi Torom a návrhmi mixnetu z hľadiska množiny anonymity a časových útokov pozri Claudia Diaz, „Measuring Anonymity“, *Privacy Enhancing Technologies Symposium 2002*.

[12] Dokumentácia funkcií GrapheneOS na https://grapheneos.org/features. GrapheneOS ako samostatné funkcie dokumentuje izolovaný Google Play, alokátor pamäte hardened_malloc a hardvérové značkovanie pamäte na podporovaných zariadeniach. Súčasná podpora GrapheneOS je obmedzená na zariadenia Google Pixel, ktoré poskytujú

overený štart a bezpečnostný hardvér, na ktoré projekt cieli. Qubes OS, `https://www.qubes-os.org/`, izoluje aplikácie v oddelených virtuálnych strojoch založených na Xene; požiadavky na kompatibilitu hardvéru (VT-x/VT-d) a zoznam certifikovaného hardvéru sú na `https://www.qubes-os.org/hcl/`. Pozri tiež Synacktiv, „Exploring GrapheneOS Secure Allocator: Hardened Malloc“ (2024).

[13] Mail-in-a-Box, `https://mailinabox.email/`, je e-mailový server na vlastný hosting inštalovaný na jedno kliknutie, ktorý spája Postfix, Dovecot a filtrovanie spamu; zdrojový kód na `https://github.com/mail-in-a-box/mailinabox`. Nextcloud, `https://nextcloud.com/`, je vedúca platforma na vlastný hosting pre synchronizáciu súborov, kalendár a spoluprácu; zdrojový kód na `https://github.com/nextcloud/server`. Obe vyžadujú stálu údržbu: bezpečnostné záplaty, disciplínu pri zálohovaní a konfiguráciu DNS. Širší prehľad alternatív k cloudovým službám, ktoré rešpektujú súkromie a dajú sa hostovať vo vlastnej réžii, je na `https://github.com/awesome-selfhosted/awesome-selfhosted`.

[14] Start9 a Umbrel sú dve vedúce distribúcie pre osobný server, ktoré balia aplikácie na vlastný hosting (uzol Bitcoinu, relay Nostr, server Matrix, Nextcloud a ďalšie) s predvoleným nastavením uprednostňujúcim súkromie; referenčný hardvér je Raspberry Pi 5 alebo miniatúrny počítač triedy Intel NUC, no znovu využitý starý notebook s voľným SSD zvláda rovnaké záťaže rovnako dobre a na tom istom zariadení beží plný uzol Bitcoinu, takže peňaženka sa pýta používateľovho vlastného uzla, nie komerčného poskytovateľa. Start9, `https://start9.com/`, so zdrojovým kódom na `https://github.com/Start9Labs`. Umbrel, `https://umbrel.com/`, so zdrojovým kódom na `https://github.com/getumbrel`. Yunohost, `https://yunohost.org/`, je tretia veľká možnosť v tejto kategórii, so zdrojovým kódom na `https://github.com/YunoHost`. K prevádzke plného uzla Bitcoinu: Bitcoin Core na `https://bitcoincore.org/` a vybrané návody na `https://github.com/jlopp/civil-disobedience` (zdroje Jamesona Loppa o vlastnom hostingu Bitcoinu). K relayom Nostr: strfry (`https://github.com/hoytech/strfry`) je najrozšírenejšia implementácia. K hraniciam modelu hrozieb pri hostingu na domácej IP adrese: praktické kompromisy pokrývajú priebežné komentáre Matta Odella a Jamesona Loppa na `https://citadeldispatch.com/` a `https://www.lopp.net/`.

[15] Lokálna inferencia na LLM s otvorenými váhami vykonáva výpočet na hardvéri samotného používateľa a žiadna požiadavka zariadenie neopúšťa; llama.cpp a Ollama sú referenčné vývojárske stacky, LM Studio a GPT4All spotrebiteľské rozhrania, Apple MLX a Foundation Models stacky na zariadení pre Apple Silicon. Kategória za posledných niekoľko rokov dozrela, no schopnosťami špičkových hostovaných modelov sa ešte nevyrovná. llama.cpp, Georgi Gerganov, `https://github.com/ggerganov/llama.cpp`, so špecifikáciou formátu GGUF na `https://github.com/ggerganov/ggml/blob/master/docs/gguf.md`. Ollama, `https://ollama.com/`, so zdrojovým kódom na `https://github.com/ollama/ollama`. LM Studio, `https://lmstudio.ai/`. GPT4All, Nomic AI, `https://gpt4all.io/`. Jan, `https://jan.ai/`. Framework Apple MLX, `https://github.com/ml-explore/mlx`, a dokumentácia API Foundation Models na `https://developer.apple.com/documentation/foundationmodels/`. Nvidia NIM, `https://www.nvidia.com/en-us/ai/`. K výskumu strojového učenia zachovávajúceho súkromie vo všeobecnosti: Reza Shokri, Marco Stronati, Congzheng Song a Vitaly Shmatikov, „Membership Inference Attacks Against Machine

Learning Models“, *IEEE Symposium on Security and Privacy 2017*, je základná práca o triede útokov, ktorej sa lokálna inferencia úplne vyhýba.

[16] Čitateľom, ktorí chcú praktického sprievodcu krok za krokom k tejto kapitole, odporúčame Michael Bazzell, *Extreme Privacy: What It Takes to Disappear*, 5. vyd. (2023), rozhodujúcu taktickú referenciu o oddeľovaní identity od sledovacej infraštruktúry. K širšiemu kontextu: Carissa Véliz, *Privacy Is Power* (2020) a Shoshana Zuboff, *The Age of Surveillance Capitalism* (2019) rozoberajú politické súvislosti; Bruce Schneier, *Data and Goliath* (2015) mapuje infraštruktúru. K vystupovaniu z konkrétnych tried sledovania: reportáže Kashmir Hill v *The New York Times* sú dlhodobo vynikajúce v téme ekosystému dátových brokerov a príručka Surveillance Self-Defense od EFF (ssd.eff.org) zostáva aktuálna pokiaľ ide o nástroje.

[17] K strategickej literatúre, ktorá berie meetupy, obchodné miestnosti, OTC zmenárne, sprostredkujúcich obchodníkov a bezpečnostnú kultúru ako most medzi individuálnou praxou súkromia a fungujúcim paralelným trhom, pozri Smuggler and XYZ, *The Second Realm: Book on Strategy* (Liberty Under Attack Publications, 2018); Kyle Rearden a Shane Radliff, *Just Below the Surface: A Guide to Security Culture* (Independently Published, 2019); a Shane Radliff a Tom Marshall, *Going Mobile* (*#VanLife Zine*) (CreateSpace Independent Publishing Platform, 2019). Najlepšie sa čítajú ako praktické a strategické sprievodné texty k tejto kapitole, nie ako náhrada vyššie citovaných primárnych technických zdrojov.

[18] Nostr (Notes and Other Stuff Transmitted by Relays) je decentralizovaný sociálny protokol odolný voči cenzúre, v ktorom používatelia ovládajú svoju identitu cez kryptografické páry kľúčov; `https://nostr.com/`, so špecifikáciou protokolu na `https://github.com/nostr-protocol/nostr`. Protokol je podrobne rozobraný v kapitole 21. Matrix je federovaný komunikačný protokol s end-to-end šifrovaním; referenčný klient je Element (`https://element.io/`) a špecifikácia je na `https://matrix.org/`.

[19] Robert Axelrod, *The Evolution of Cooperation* (Basic Books, 1984), zostáva klasickým teoreticko-herným spracovaním toho, ako sa spolupráca medzi sebeckými konajúcimi stabilizuje opakovanou interakciou. Elinor Ostrom, *Governing the Commons: The Evolution of Institutions for Collective Action* (Cambridge University Press, 1990), empiricky dokumentuje mechanizmy dôvery v komunitách pri správe skutočných spoločných zdrojov a je kanonickým zdrojom o neštátnych inštitúciách kolektívneho konania. K reputácii v online a pseudonymných kontextoch: Paul Resnick a Richard Zeckhauser, „Trust Among Strangers in Internet Transactions: Empirical Analysis of eBay's Reputation System“, v *The Economics of the Internet and E-Commerce*, ed. Michael Baye (Elsevier, 2002), je základná empirická práca. Chrysanthos Dellarocas, „The Digitization of Word of Mouth“, *Management Science* 49, č. 10 (2003): 1407–1424, prehľadovo spracúva návrh mechanizmov reputácie. Kapitola 24 podrobne rozvíja pseudonymnú reputáciu, poverenia a decentralizované inštitúcie.

[20] Angor je funkčná implementácia vzoru multisig s postupným uvoľňovaním prostriedkov v rozsahu koordinácie investícií. Každý projekt je financovaný zmluvou 2 z 2 medzi investorom a zakladateľom a vyplácanie je podmienené časovo zamknutými medzníkmi, nie uvoľnené vopred; zakladateľ na každej etape ukazuje pokrok a investor si zachováva možnosť zastaviť zostávajúce tranže. Metadáta projektu a komunikačný kanál medzi investorom a zakladateľom bežia na protokole Nostr, nie cez hostovaného sprostredkovateľa, a vrstva v reťazci používa Bitcoin s Taprootom, aby štruktúra zmluvy zostala súkromná pre účastníkov. Protokol je otvorený a zdokumentovaný na `https://angor.io` s technickou špecifikáciou na `https://docs.angor.io` a zdrojovým kódom na `https://github.com/block-core/angor`; aplikácia je na `https://hub.angor.io`. Angor rozširuje logiku escrow, ktorú tento oddiel opisuje, z jednotlivých obchodov na viacstupňové obchodné vzťahy a je najbližším dnes nasadeným príkladom obchodu s postupnou dôverou medzi pseudonymnými protistranami.

[21] ShopinBit prevádzkuje vzor sprostredkujúceho obchodníka v rozsahu maloobchodu a concierge služieb z Nemecka, od decembra 2018, a prijíma Bitcoin a Monero výmenou za tovar, ktorý ShopinBit obstará od bežných dodávateľov s cenami vo fiat mene a pošle zákazníkovi. Súkromie tu zaisťuje zakrytie identity na rozhraní s dodávateľom: ShopinBit drží vzťah KYC s dodávateľom vyššie v reťazci a koncový zákazník nikdy nemusí tomuto dodávateľovi odhaliť identitu. Zákaznícke účty sú voliteľné, obchod nenačítava nijakú marketingovú analytiku, údaje zákazníkov sa po tridsiatich dňoch automaticky mažú a platba kryptomenou má oproti fiat mene zľavu tri percentá. Služba Concierge rozširuje rovnakú logiku na čokoľvek, čo sa dá zohnať na voľnom trhu, vrátane áut, rezervácií ciest a firemného obstarávania, pričom požiadavka sa odosiela cez rozhranie chatu, ktoré nevyžaduje e-mail ani účet. Vzor sprostredkujúceho obchodníka rieši iný problém než mechaniku escrow, ktorú tento oddiel opisuje: dodávateľ vyžaduje identitu, ktorú zákazník nechce poskytnúť, a sprostredkovateľ túto medzeru preklenie tak, že od zákazníka prijme kryptomenu a voči dodávateľovi vystúpi s bežnou platbou a identitou. Medzi ďalšie príklady tejto kategórie patrí Bitrefill, ktorý predáva darčekové karty uplatniteľné u bežných maloobchodníkov, a rad regionálnych maloobchodníkov prijímajúcich Bitcoin na podobných princípoch. Pozri `https://shopinbit.com` a dokumentáciu k službe Concierge na `https://shopinbit.com/Concierge/`.

[22] Útoky SIM swap nastanú, keď protivník sociálnym inžinierstvom alebo úplatkom prinúti zamestnanca mobilného operátora previesť obeti telefónne číslo na SIM kartu, ktorú protivník ovláda, a presmeruje tak všetky SMS správy vrátane overovacích kódov. Útok úplne obchádza dvojfaktorové overenie cez SMS. Medzi významné prípady SIM swap patria únosy účtov na Twitteri v roku 2019 a prelomenie Coinbase v roku 2022, ktoré umožnilo rozsiahle prevzatia účtov. Podrobnú technickú a sociálnu analýzu nájdete v dokumentácii Rachel Tobac a tímu SocialProof Security; pozri tiež Joseph Cox a Lorenzo Franceschi-Bicchierai, „T-Mobile Hack“, *Vice Motherboard*, 2021; a pokyny FTC na `https://www.ftc.gov/business-guidance/resources/ftcs-guide-protecting-consumers-sim-swap-scams`. Štandard hardvérových kľúčov FIDO2/WebAuthn bol navrhnutý práve tak, aby bol štrukturálne odolný voči tejto triede útokov, lebo poverenie je viazané na doménu kryptografickým hardvérom, nie doručované telefónnym kanálom.

[23] Burzy Bitcoinu typu peer-to-peer umožňujú kupujúcim a predávajúcim obchodovať priamo, bez centralizovaného sprostredkovateľa, ktorý by držal prostriedky alebo vyberal doklady totožnosti. Medzi aktívne platformy patrí Bisq (`https://bisq.network/`), decentralizovaná aplikácia s multisig escrow a rozhodcovským riešením sporov bez centrálneho servera; RoboSats (`https://learn.robosats.com/`), P2P burza natívna pre Lightning, ktorá používa hold invoices a koordinátora na riešenie sporov; Peach Bitcoin (`https://peachbitcoin.com/`), európska P2P platforma určená primárne pre mobil; a AgoraDesk/LocalMonero (dnes zatvorené) ako ekvivalent pre Monero. Bankomaty Bitcoinu, ktoré pracujú bez požiadaviek KYC, sú katalogizované na `https://coinatmradar.com/` s filtrami podľa úrovne overenia, hoci regulačný tlak posunul väčšinu amerických bankomatov nad prah KYC. K kritike KYC burz ako sledovacej infraštruktúry pozri kapitolu 10 a pokyny Financial Action Task Force (FATF) k poskytovateľom služieb s virtuálnymi aktívami na `https://www.fatf-gafi.org/en/publications/Fatfgeneral/Virtual-assets-guidance.html`, čo je medzinárodný štandard, ktorý požiadavky KYC presadzuje.

[24] I2P (Invisible Internet Project) je peer-to-peer anonymizačná prekryvná sieť s jednosmernými tunelmi, cesnakovým smerovaním (garlic routing, zoskupovanie viacerých správ dokopy) a distribuovanou sieťovou databázou; je optimalizovaná pre interné služby (eepsites, aplikácie natívne pre I2P), nie na prístup do bežného internetu, a preto Tor dopĺňa, nenahrádza. Stránka projektu: `https://geti2p.net/`, so zdrojovým kódom na `https://github.com/i2p/i2p.i2p`. Java I2P je referenčná implementácia; i2pd (`https://i2pd.website/`,

https://github.com/PurpleI2P/i2pd) je implementácia v C++ s nižšími nárokmi na zdroje. K technickému porovnaniu modelov hrozieb Toru a I2P pozri zdroje EFF a dokumentáciu modelu hrozieb samotného projektu I2P na https://geti2p.net/en/docs/how/threat-model. Konfigurácia suverénneho hostiteľa v oddiele 23.3 môže sprístupniť služby cez skryté služby I2P ako alternatívu k službám onion v Tore.

[25] Whonix je desktopový operačný systém navrhnutý na anonymitu, ktorý beží ako dva virtuálne stroje: Gateway VM, ktorý vedie všetku prevádzku cez Tor, a Workstation VM, ktorý je od siete úplne izolovaný okrem cesty cez Gateway. Aj keď je Workstation kompromitovaný, útočník sa nedozvie skutočnú IP adresu používateľa, lebo Workstation nemá priamy prístup do siete. Whonix beží nad hostiteľským OS (typicky Debian alebo Qubes OS) a je dostupný ako zariadenia (appliances) pre KVM/VirtualBox. Stránka projektu: https://www.whonix.org/, so zdrojovým kódom na https://github.com/Whonix. Keď Whonix beží v Qubes OS (Qubes-Whonix), oba prístupy sa spoja: kompartmentalizácia založená na Xene z Qubes a anonymizácia siete cez Tor z Whonixu. K modelu hrozieb a odôvodneniu návrhu pozri https://www.whonix.org/wiki/Main_Page a technickú dokumentáciu Patricka Schleizera na https://www.whonix.org/wiki/Dev/Design-Principles.

[26] SimpleX Chat (https://simplex.chat/, zdrojový kód na https://github.com/simplex-chat/simplex-chat) je end-to-end šifrovaná komunikačná aplikácia s novým návrhom: každému vzťahu s kontaktom priraďuje vlastnú nezávislú frontu a kľúčový materiál, bez telefónneho čísla, používateľského mena či trvalého verejného kľúča zdieľaného medzi kontaktmi, takže metadáta sa medzi nimi nedajú prepojiť. Špecifikácia protokolu je na https://github.com/simplex-chat/simplex-chat/blob/stable/docs/SIMPLEX.md. Briar (https://briarproject.org/, zdrojový kód na https://code.briarproject.org/briar/briar) je peer-to-peer šifrovaná komunikačná aplikácia navrhnutá na odolnosť voči cenzúre a prerušeniam: dokáže synchronizovať správy cez Bluetooth, WiFi direct alebo Tor podľa toho, čo je k dispozícii, bez centrálneho servera. Obe sú aktívne udržiavané a Freedom of the Press Foundation a EFF ich odporúčajú používateľom s vysokým modelom hrozieb. Matrix (https://matrix.org/) s klientom Element (https://element.io/) poskytuje federovaný šifrovaný chat; model federácie rozkladá dôveru medzi prevádzkovateľov serverov, no nedáva takú minimalizáciu metadát ako návrh SimpleXu bez serverov.

[27] Obchodovanie s Bitcoinom OTC (over-the-counter) znamená priame vyjednávanie medzi kupujúcim a predávajúcim, osobne alebo cez dôveryhodného sprostredkovateľa, bez použitia verejnej knihy objednávok burzy. OTC pulty slúžia pri veľkých obchodoch, kde by obchodovanie na burze pohlo cenou; miestne OTC obchodovanie slúži účastníkom dbajúcim o súkromie, ktorí sa chcú záznamom identity spojeným s burzou celkom vyhnúť. K regulačnému rámcu, ktorý poháňa požiadavky na súlad pri OTC v rôznych jurisdikciách, pozri odporúčanie 15 FATF a nariadenie EÚ o prevodoch finančných prostriedkov (Transfer of Funds Regulation, TFR), ktoré rozšírilo požiadavky Travel Rule na poskytovateľov služieb s kryptoaktívami v roku 2023. K praktickej dokumentácii procesu OTC obchodovania a jeho vlastností z hľadiska súkromia pozri zdroje Matta Odella na https://mattodell.com a newsletter Bitcoin Optech na https://bitcoinops.org/; pre väčšie OTC pulty pozri dokumentáciu River Financial k OTC službám na https://river.com/learn/bitcoin-otc-trading/.

[22] Útoky SIM swap zneužívajú proces prevodu účtu u mobilného operátora na presun telefónneho čísla obete na SIM kartu, ktorú ovláda útočník; potom každý kód dvojfaktorového overenia cez SMS ide útočníkovi. Technika sa použila na kompromitáciu

kryptomenových búrz, e-mailových účtov a profilov na sociálnych sieťach. K zdokumentovaným prípadom pozri Brian Krebs, „The SIM Swap Problem“, Krebs on Security, https://krebsonsecurity.com/category/sim-swapping/; pokyny FTC pre spotrebiteľov na https://www.ftc.gov/business-guidance/resources/ftcs-guide-protecting-consumers-sim-swap-scams; a formálne oznámenie FCC o navrhovanom pravidle k podvodom SIM swap (2023), https://www.fcc.gov/consumers/guides/sim-swapping-and-port-out-scams. GSMA uverejnila pokyny určené odvetviu, „Mobile Identity: SIM Swap API“, https://www.gsma.com/solutions-and-impact/technologies/open-gateway/gsma-open-gateway-api-descriptions/sim-swap/. Hardvérové bezpečnostné kľúče (FIDO2/WebAuthn) sú štrukturálna obrana: nie sú založené na SMS a SIM swap ich nedokáže presmerovať.

[23] Firmy na analýzu blockchainu používajú heuristiky analýzy grafu na množinu UTXO v Bitcoine, aby vystopovali prostriedky a prepojili pseudonymné adresy so skutočnými identitami. Chainalysis je najväčšia firma v tejto kategórii; jej produkt Reactor je hlavným nástrojom amerických federálnych orgánov činných v trestnom konaní. Elliptic a TRM Labs pokrývajú podobnú oblasť pre zákazníkov z oblasti súladu s reguláciou a orgánov činných v trestnom konaní. Základnou akademickou prácou o heuristikách zhlukovania je Meiklejohn et al., „A Fistful of Bitcoins: Characterizing Payments Among Men with No Names“, *ACM Internet Measurement Conference* (2013), https://dl.acm.org/doi/10.1145/2504730.2504747, ktorá zaviedla heuristiku spoločného vlastníctva vstupov. K praktickému spracovaniu tejto triedy útokov a obrán pozri analýzy 0xB10C na https://b10c.me/ a wiki Bitcoin Privacy na https://en.bitcoin.it/wiki/Privacy. Burzy peer-to-peer pracujúce bez povinného KYC zahŕňajú Bisq (https://bisq.network/), decentralizovanú desktopovú aplikáciu s multisig escrow a bez centrálneho servera; Peach Bitcoin (https://peachbitcoin.com/), mobilnú P2P platformu; a RoboSats (https://learn.robosats.com/), P2P platformu natívnu pre Lightning, ktorá na vyrovnanie v štýle atómových swapov používa hold invoices.

[24] I2P (Invisible Internet Project) je anonymizačná sieťová vrstva s šifrovanou komunikáciou cez cesnakové smerovanie medzi aplikáciami bežiacimi vnútri siete; https://geti2p.net/. Na rozdiel od Toru, ktorý primárne sprostredkúva prevádzku bežného internetu, je I2P optimalizovaná pre interné služby (eepsites) a peer-to-peer aplikácie. Architektúra smerovania používa jednosmerné tunely a smerovacie informácie rozširuje cez distribuovanú hašovaciu tabuľku, čo sťažuje analýzu prevádzky oproti okruhovému modelu Toru, ale obmedzuje prístup do širšieho internetu. I2P sa hodí najmä pre služby s vlastným hostingom (relaye Nostr, zdieľanie súborov, komunikácia), kde obe strany používajú I2P, a je predvoleným anonymizačným transportom viacerých aplikácií zameraných na súkromie vrátane I2P-Bote (e-mail) a vstavaného torrentového klienta Invisible Internet Project. Zdrojový kód na https://github.com/i2p/i2p.i2p. K technickému porovnaniu s Torom pozri Roger Dingledine a Nick Mathewson, „Tor: The Second-Generation Onion Router“, *USENIX Security Symposium* (2004), https://www.usenix.org/legacy/events/sec04/tech/full_papers/dingledine/dingledine.pdf.

[25] Whonix, https://www.whonix.org/, je desktopový operačný systém navrhnutý na pokročilú anonymitu, ktorý beží ako dva samostatné virtuálne stroje: Gateway VM, ktorý vedie všetku prevádzku cez Tor, a Workstation VM, ktorý je od fyzickej siete úplne izolovaný a na internet sa dostane len cez Gateway. Architektúra znamená, že aj keď je Workstation kompromitovaný, útočník nezistí skutočnú IP adresu používateľa, lebo Workstation nemá priamy prístup do siete. Whonix môže bežať ako samostatné virtuálne stroje vo VirtualBoxe alebo KVM, alebo vnútri Qubes OS ako súbor Qubes AppVM; vtedy Qubes dáva vrstvu kompartmentalizácie a Whonix vrstvu smerovania cez Tor. Zdrojový kód na https://github.com/Whonix. Dokumentácia na

https://www.whonix.org/wiki/Documentation. K odôvodneniu architektúry pozri návrhový dokument Whonixu na https://www.whonix.org/wiki/Design.

[26] Matrix je federovaný komunikačný protokol s otvoreným štandardom, ktorý podporuje end-to-end šifrovanie cez implementáciu double ratchet Olm/Megolm; špecifikácia je na https://matrix.org/. Element (https://element.io/) je referenčný klient udržiavaný firmou Element Matrix Services. Protokol Matrix umožňuje domovské servery na vlastný hosting, ktoré sa federujú so širšou sieťou, takže je ťažšie ho vypnúť než centralizovanú službu. SimpleX Chat (https://simplex.chat/, zdrojový kód na https://github.com/simplex-chat/simplex-chat) volí iný architektonický prístup: nijaké používateľské identifikátory, nevyžaduje telefónne číslo ani e-mail a kontakt sa nadväzuje jednorazovými pozývacími odkazmi; správy idú cez servery relay, ktoré si vyberie používateľ. Briar (https://briarproject.org/, zdrojový kód na https://code.briarproject.org/briar/briar) je peer-to-peer šifrovaný komunikátor, ktorý vedie prevádzku cez Tor a pri chýbajúcom internete sa dokáže synchronizovať cez Bluetooth alebo WiFi, vďaka čomu sa hodí do prostredí s vysokou cenzúrou alebo narušenou infraštruktúrou. Tieto tri nástroje predstavujú rôzne body v priestore kompromisov medzi použiteľnosťou, federáciou a minimalizáciou dôvery voči serverom.

[27] OTC (over-the-counter) zmenárnici Bitcoinu obchodujú priamo s protistranami, nie cez knihu objednávok, a typicky prijímajú hotovosť alebo bankový prevod výmenou za Bitcoin bez povinného overenia totožnosti. Kategória siaha od neformálnych miestnych obchodníkov nájdených cez komunitné meetupy až po poloprofesionálne služby inzerované na platformách, ako sú Bisq (https://bisq.network/) a Peach Bitcoin (https://peachbitcoin.com/). K modelu sprostredkujúceho obchodníka ako vrstvy sprostredkovania zachovávajúcej súkromie pozri Smuggler and XYZ, *The Second Realm: Book on Strategy* (Liberty Under Attack Publications, 2018), ktorá rozvíja logiku špecializácie na hranici sledovania. Bitrefill (https://www.bitrefill.com/) je najväčší maloobchodný sprostredkujúci obchodník v tejto kategórii; predáva darčekové karty a dobitie kreditu uplatniteľné u bežných obchodníkov s cenami vo fiat mene výmenou za platbu v Bitcoine alebo cez Lightning, takže držitelia Bitcoinu môžu nakupovať u maloobchodníkov, ktorí Bitcoin priamo neprijímajú, bez toho, aby tým maloobchodníkom odhalili identitu.

24

DÔVERA A SPORY V PARALELNEJ EKONOMIKE

„Reputácia bude mať v obchodných stykoch ústredný význam, oveľa väčší než dnešné úverové ratingy."

Timothy C. May, *The Cyphernomicon* (1994)[1]

Úvod

Predchádzajúca kapitola ukázala jednotlivcov a malé skupiny, ktoré budujú prax súkromia od základov: modelujú hrozby, vyberajú nástroje, vytvárajú komunity a rozbiehajú prvé obchodné okruhy v kruhu dôveryhodných ľudí. Tak sa začína prijímanie týchto nástrojov. Kapitola 23 necháva otvorenú otázku, čo sa stane, keď sa kruh rozšíri. Ako obchodujú cudzí ľudia a ako riešia neistotu, keď odmietajú štátny systém identity a nedôverujú štátnym súdom?

Súkromie je podmienka konania a sledovanie narúša výmenu a oslabuje kalkuláciu. Kryptografické systémy môžu zvýšiť náklady kontroly natoľko, že mnohé útoky prestanú byť výhodné. Bitcoin dáva peniazom odolný základ, anonymné siete chránia komunikáciu a dôkazy s nulovou znalosťou umožňujú dokázať úzky fakt bez otvárania celého spisu. Nostr dáva používateľom identity pod ich kontrolou na sociálnom médiu, ktoré nemôže zhabať žiaden majiteľ platformy.

Odpoveď na uvedenú otázku si však vyžaduje viac než nástroje. Kryptografický stack prenáša bity a vysporiadava platby, no nezaručuje spoľahlivosť v čase a nerozhodne, čo sa stalo, keď obchod zlyhá. Obe úlohy sú inštitucionálne. Paralelná ekonomika potrebuje inštitúcie, ktoré ich plnia bez toho, aby sa spoliehali na štátny systém identity alebo štátne súdy.[2]

24.1 Prečo samotné nástroje trh nevytvoria

Niektoré výmeny takmer nevyžadujú dôveru. Keď kupujete paradajky od farmára a platíte hotovosťou v tej istej chvíli, keď vám ich podá, obchod sa uzavrie na mieste. Platba aj dodanie prebehnú naraz a obe strany odchádzajú s konečným vyrovnaním.

Problém dôvery sa objaví, hneď ako sa vyrovnanie natiahne v čase alebo vo vzdialenosti. Obchodník žiada platbu teraz a sľubuje zásielku zajtra. Vývojár predáva aktualizácie, ktoré dorazia v priebehu nasledujúceho roka, a zakladateľ chce postupné financovanie ešte pred dokončením produktu. Pseudonymný predajca môže tvrdiť, že má za sebou poctivé obchodovanie, ktoré kupujúci zatiaľ nevie overiť.

Šifrovanie na tieto otázky neodpovedá a Bitcoin ani Nostr samy osebe tiež nie. Tieto nástroje riešia prenos, kontrolu nad identitou, zverejňovanie a vysporiadanie platieb. Spoľahlivosť v čase a rozdiel medzi podvodom a poctivou chybou patria iným mechanizmom.

Moderný štát spája niekoľko odlišných funkcií do jedného balíka a potom ho predstavuje ako nenahraditeľný. Viaže identitu na právne dokumenty a spory usmerňuje do štátnych súdov, všetko s oporou regulátorov a polície. Registruje aj firmy a drží poslednú vynucovaciu poistku. Trhy sa na niektoré z týchto funkcií spoliehajú odjakživa. Nepotrebujú však, aby zostali pod štátnym monopolom.

Paralelná ekonomika nemusí dôveru zrušiť. Potrebuje spôsoby, ako dôveru vytvárať bez toho, aby všetkých vydala napospas trvalej identifikácii a sledovaniu. Potrebuje spôsoby, ako dôveru zúžiť, oceniť, rozložiť a obmedziť škody, keď zlyhá.

Je to inštitucionálny problém. Timothy May to videl včas. Anonymné obchodovanie a elektronické zmluvy podľa neho boli možné, no reputácia sa mala stať ústrednou.[1] Eric Hughes povedal to isté z iného uhla: súkromie v otvorenej spoločnosti si vyžaduje anonymné systémy transakcií a každá strana transakcie má vedieť len to, čo je pre ňu priamo nevyhnutné.[4] Nick Szabo išiel v analýze ďalej. Vo svete digitálneho obchodu sa podľa neho dominantné náklady presúvajú k jurisdikcii, dôvere a bezpečnosti. Vyhľadávanie, vyjednávanie, záväzok, plnenie aj rozhodovanie sporov potrebujú štruktúru.[5]

Technický stack opísaný v tejto knihe už existuje. Zostáva otázka, ktorú May a Szabo nechali visieť vo vzduchu: ako tento stack podporuje obchod medzi ľuďmi, ktorí sa poznajú len cez kľúče a záznam o plnení záväzkov?

24.2 Reputácia pri pseudonymite

Reputácia potrebuje kontinuitu. Kupujúci musí vedieť povedať: s týmto predajcom som už obchodoval, tovar dorazil, kvalita zodpovedala tvrde-

niu, správy chodili rýchlo a vrátenie peňazí prišlo, keď malo. Pamäť vyžaduje kontinuitu a reputácia vyžaduje pamäť.

Silná anonymita pôsobí proti tejto kontinuite. Ak každá interakcia používa novú identitu bez väzby na predošlú históriu, pozorovatelia sa dozvedia menej, ale rovnako aj protistrany. Tá istá neprepojiteľnosť, ktorá bráni sledovaniu, bráni aj hromadeniu dôvery.

Toto napätie nezmizne len preto, že sa nám nepáči. Systém, ktorý v jednom kanáli sľubuje silnú anonymitu aj trvalú reputáciu, spravidla zamlčuje niektorý z kompromisov. Na mnohých trhoch sa osvedčil kompromis v podobe pseudonymity.

Trvalý pseudonym môže zhromažďovať históriu a pritom odmietať občiansku identitu. Kľúč musí vydržať dosť dlho na to, aby ľudia mohli sledovať správanie v čase. Nemusí však odkazovať na pas ani na štátny register. Pseudonym sa stáva drahým na opustenie, lebo opustiť ho znamená spáliť nahromadenú dôveru. Táto cena disciplinuje správanie. Predajca, ktorý dva roky budoval meno v sieti Nostr, odpovedal kupujúcim, posielal tovar, vracal peniaze pri chybách a písal pod tým istým kľúčom, má čo stratiť, ak podvádza. Jeho identita je ekonomická, nie právny fakt. To stačí.

Nostr je tu dôležitý, lebo bežné sociálne správanie mení na čitateľné podpísané dôkazy. Sledovanie účtov, odpovede, zdieľanie, stlmenie, zapy, dlhšie články, vydania softvéru aj ponuky na trhovisku sa môžu viazať na ten istý kľúč. Žiaden z týchto signálov nie je dokonalý a každý sa dá na okraji zmanipulovať. Celkový obraz však stále nesie informáciu.

Účet, ktorý sledujú ľudia, ktorým už dôverujete, nie je dokázane poctivý, ale ľahšie ho vezmete vážne. Obchodník s niekoľkoročnou verejnou históriou pod jedným kľúčom nemá zaručené, že splní záväzok, no porušenie dohody ho stojí viac než nový kľúč bez záznamu. Vývojár, ktorého vydania podpisuje tá istá identita, čo publikuje eseje, prijíma kritiku, reaguje na hlásenia chýb a získava podporu od ďalších vývojárov, dáva hustejší signál než anonymný odkaz na stiahnutie.

Signál môže zostať aj lokálny. Reputácia nemusí byť jedno globálne skóre zhora od centrálnej autority. Dôvera závisí od kontextu a jednému účtu môžete veriť ako vývojárovi a inému ako obchodníkovi. Môj graf sa líši od vášho a ten rozdiel je výhoda, nie slabina. Centralizované platformy sploštťujú dôveru do jedného odznaku, kým trhové systémy nechávajú dôveru rozloženú a rozmanitú.

Zostáva problém studeného štartu. Noví účastníci začínajú bez histórie, preto spravidla začnú malými obchodmi, odporúčaniami alebo dôkazom o sebe viazaným na doménu v nejakom užšom kontexte. Niektorí sa opierajú o escrow (úschovu s podmienkou uvoľnenia), kým si nevybudujú meno, iní si získajú dôveru v miestnej komunite skôr, než sa pokúsia predávať cudzím. Nič z toho nie je bez trenia a obchod bez strážcov prí-

stupu má stále svoje filtre. Filtre sa len presúvajú od povolenia udeleného správcami k úsudku, ktorý vykonávajú samotní účastníci.[6]

Negatívna história vytvára druhý tlak. Predajca, ktorý spáli jeden pseudonym, môže otvoriť iný a vrátiť sa ako nováčik. Čisto lokálne systémy reputácie sú preto slabé proti opakovanému podvodu. Paralelné trhy potrebujú dosť kontinuity, aby porušenie dohody bolo drahé, a pritom nesmú z každej trhovej identity urobiť univerzálny identifikátor.

Dôkazy s nulovou znalosťou otvárajú čiastočnú odpoveď na toto napätie, hoci nasadenie v praxi je zatiaľ v počiatkoch. Trvalé pseudonymy riešia napätie medzi anonymitou a kontinuitou tak, že kľúč zostáva v prevádzke. Všetko pod ním sa tým stáva prepojiteľné výmenou za viditeľný záznam. Iný kompromis sa ponúka, keď sa reputačné tvrdenia dajú oddeliť od konkrétnych transakcií a identít, z ktorých vznikli. Protokoly založené na atestáciách fungujú tak, že atestujúci podpíšu výroky o používateľovi a ten ich neskôr dokazuje s nulovou znalosťou. Vďaka nim je možné tvrdiť „dokončil som aspoň N obchodov s hodnotením aspoň R, s ľuďmi, ktorých sledujete“ alebo „za mňa ručilo K členov tejto skupiny obchodníkov“ bez toho, aby sa odhalilo, ktoré obchody alebo ktoré iné identity sú moje.[7] Tieto systémy sa stále opierajú o atestujúcich, ktorí pozorujú podkladové fakty, takže studený štart a odolnosť voči útokom typu Sybil nezmiznú. Dostatočne veľký počet atestujúcich v tajnej dohode môže stopu opäť poskladať. S dozrievaním nástrojov by sa mohla zmeniť predvolená podoba reputácie: tvrdenia sa hromadia pod pseudonymami a predkladajú sa v mieste použitia, pričom každá interakcia odhalí len ten kúsok, ktorý transakcia potrebuje.

Takýto posun je zdravý. Štát chce reputáciu viazať na občiansku identitu, lebo človeka s občianskou identitou je ľahké zdaniť a ľahké prinútiť. Paralelná ekonomika chce reputáciu viazať na plnenie záväzkov. Práve plnenie je informácia, ktorú obchod potrebuje.[3]

24.3 Poverenia a selektívne odhaľovanie

Reputácia je mäkký dôkaz. Vzniká z pozorovaného správania. Mnohé transakcie potrebujú niečo tvrdšie.

Jeden kupujúci môže potrebovať dôkaz, že predajca ovláda známu doménu. Iný používateľ môže potrebovať dôkaz, že vydanie pochádza od vývojára, ktorý sa hlási k autorstvu. Inokedy je relevantným faktom kontinuita toho istého kľúča v dvoch kanáloch, alebo dôkaz, že za nováčika ručil existujúci člen a že spĺňa pravidlo, ktoré riadi účasť.

Štát tieto problémy rieši nadmerným odhaľovaním. Žiada celý balík: pas, vodičský preukaz, účet za energie, zákaznícky profil. Inštitúcia dostane spis dosť hrubý na to, aby sa dal použiť na oveľa viac, než vyžaduje samotná transakcia.

To je zlý návrh.

Väčšina transakcií potrebuje úzky fakt. Overovateľ nepotrebuje celého človeka. Potrebuje len ten kúsok informácie, o ktorý sa transakcia opiera.[4]

Jednoduchý model ponúka už samotný Nostr. NIP-05 umožňuje priradiť verejný kľúč k identifikátoru opretému o DNS a HTTPS, bez toho, aby bolo treba žiadať platformu o odznak.[8] Dôvera však stále spočíva v doméne, v subjekte, ktorý za ňou stojí, a vo webovej PKI, ktorá obsluhuje súbor `nostr.json`. Firma môže potvrdiť, že daný kľúč patrí jednému z jej vývojárov. Jednotlivec môže potvrdiť, že daný kľúč je ten, ktorý patrí k jeho webovej stránke. Systém dôveru neruší. Zužuje ju na konkrétne tvrdenie.

Rovnaká logika sa dá rozšíriť. Známy kľúč môže podpísať jednorazovú výzvu a odpoveď sa pošle iným kanálom. Overovateľ tak zistí, že osoba na anonymnom kanáli ovláda ten istý kľúč, ktorého verejnú históriu už pozná. Právne meno sa nedozvie a nepotrebuje ho, lebo pre túto interakciu je podstatná kontinuita medzi známou reputačnou identitou a súčasnou konverzáciou.[9]

Systémy s nulovou znalosťou posúvajú ten istý princíp do zložitejších problémov s poverením. Kapitola 15 už ukázala všeobecný vzor. Systém dokáže preukázať vek nad prahovou hranicou bez odhalenia dátumu narodenia. Dokáže tiež preukázať členstvo alebo ovládanie poverenia bez toho, aby poverenie odovzdal. Pre paralelnú ekonomiku to nahrádza hromadné vyťažovanie identity úzkym dôkazom.

Cieľom je selektívne odhaľovanie: odhaliť ovládanie vývojárskeho kľúča, nie bydlisko, a odhaliť oprávnenie podľa vekového pravidla, nie dátum narodenia. Rovnakú disciplínu vyžaduje aj postavenie v trhovej komunite: ukázať tvrdenie, ktoré transakcia potrebuje, a nie sieť vzťahov, ktorá za ním stojí.

Selektívne odhaľovanie neodstráni všetko riziko. Poverenia sa môžu stať infraštruktúrou sledovania, ak sa zaznamenávajú alebo centralizujú, najmä keď sa stanú povinnými vo všetkých kontextoch. Pseudonymný trh môže potichu znovu postaviť ten istý systém dosjé, ktorý chcel odmietnuť, ak každý obchod vyžaduje ešte jeden podpísaný dôkaz a každý dôkaz sa ukladá navždy. Odpoveďou je stále disciplína. Odhaľte, čo transakcia potrebuje, a nič viac.

Toto pravidlo spája cypherpunkovú stránku knihy s praxeologickou. Informačnú požiadavku určuje transakcia. Všetko, čo ju presahuje, je vyťažovanie prebytku.

Nástroje, ktoré tento princíp podporujú, dosiahli za posledných niekoľko rokov produkčnú úroveň. Atestácie členstva v skupine cez protokoly ako Semaphore sa nasadili na podujatiach konferenčného rozsahu na vstupenky a predkladanie poverení, pričom kryptografické základy zvládli stovky až tisíce používateľov na jedno nasadenie. Postupy na vytvorenie peňaženky, ktoré odvodia pseudonymnú peňaženku z existujúceho účtu u poskytovateľa identity bez toho, aby poskytovateľ odvodenie poznal,

bežia v produkcii minimálne na jednom blockchaine. Štandardy overiteľných poverení od konzorcia World Wide Web Consortium dávajú všeobecný formát, v ktorom sa dajú vyjadriť dôkazy selektívneho odhaľovania. Štátom vydávaná strana tej istej infraštruktúry tiež dozrieva: mobilné vodičské preukazy podľa medzinárodného štandardu sa už akceptujú na kontrolných miestach identity v niekoľkých krajinách.[10]

Rámec tejto knihy trvá na výhrade, ktorú dokumenty štandardov neuvádzajú. Systém poverení, ktorý selektívne odhaľovanie ponúka ako funkciu, nie je to isté ako systém poverení, v ktorom sa selektívne odhaľovanie naozaj uplatňuje. Štátom vydávané varianty zvyčajne používajú selektívne odhaľovanie ako pohodlie (rýchlejšie overenie na letisku), nie ako základ súkromia (minimálne vystavenie v bežnom živote), a stimuly na strane overovateľov tlačia k požiadavkám nad rámec transakcie. Pseudonymné komunitné varianty ho zvyčajne používajú tak, ako sa má, pretože účastníkom na základnom princípe záleží. Nástroje sú čoraz viac tie isté. O tom, či chránia súkromie, alebo len znovu stavajú dosje s ďalšími krokmi, rozhoduje postoj ich používateľov.

24.4 Escrow a jednoduché riešenie sporov

Niektoré transakcie súd nepotrebujú. Potrebujú podmienku uvoľnenia.

Ak sú kupujúci a predajca cudzí ľudia a tovar sa odošle neskôr, jednoduchou odpoveďou je escrow. Prostriedky sú pod kontrolou tretej strany, kým sa nepotvrdí dodanie, alebo v multisig usporiadaní, ktoré vyžaduje dohodu medzi obchodujúcimi stranami a rozhodcom. Kupujúci už nemusí veriť naslepo a predajca neposiela tovar bez záruky platby, takže plocha dôvery sa zmenšuje na oboch stranách.

Bitcoin robí tieto usporiadania konkrétnymi. Multisig typu dva z troch môže rozdeliť kľúče medzi kupujúceho a predajcu, pričom tretí kľúč drží rozhodca. Ak obchod prebehne hladko, kupujúci a predajca uvoľnia prostriedky spolu. Ak nastane problém, rozhodca sa pridá k jednej strane a prostriedky sa presunú s dvoma podpismi. Nikto nemá jednostrannú kontrolu. To je už lepšia štruktúra než bežný model platforiem, kde firma vezme peniaze a napíše pravidlá.[14]

Malé trhy často pridávajú ku kryptografii sociálne praktiky. Nové protistrany obchodujú najprv v malom rozsahu a predajcovia pošlú jednu položku skôr, než požiadajú o väčšie objednávky. Komunity odporúčajú známych escrow agentov, ktorým záleží na dobrom mene. Opakovaný obchod znižuje neistotu, lebo každá úspešná výmena je dôkazom pre ďalšiu, a nahromadené dôkazy sú samy súčasťou sociálneho dôkazu, ktorý sa neskôr ponúka nováčikom.

Tieto mechanizmy fungujú, lebo mnohé spory sú jednoduché. Niekedy ide o otázku, či balík dorazil, či repozitár vydal sľúbenú verziu, či prostriedky prešli, alebo či jedna strana porušila dohodnuté pravidlo, ktoré vi-

dia obe. V takých prípadoch väčšinu práce urobia jasné podmienky uvoľnenia.

Zisk je skutočný, no treba ho vyjadriť presne. Escrow a multisig dôveru neodstraňujú, len ju presúvajú a zužujú. Strany stále dôverujú kľúčom a softvéru a niektoré usporiadania vyžadujú aj dôveru v rozhodcu. Zúžená dôvera však často stačí, lebo mnohé trhové problémy nevyžadujú dokonalú istotu, ale len štruktúru, ktorá robí podvod nákladným a poctivý obchod ľahším než podvádzanie.

Na význame nadobúdajú aj postupné záväzky. Financovanie, ktoré uvoľňuje peniaze po etapách, dáva investorom vyjednávaciu silu počas celého života projektu. Kupujúci, ktorý môže získať späť prostriedky ešte neuvoľnené, má reálnu pozíciu na vyjednávanie. Zmluva o službe, ktorá zakóduje čiastočnú platbu a podmienené uvoľnenie, vnáša disciplínu do samotnej zmluvy. Zmluva sa tu začína sťahovať z papiera do protokolu. Stroj úsudok nenahrádza. Drží ho v užšom rámci.

24.5 Arbitráž a sporné fakty

Escrow funguje dobre, keď je sporný fakt jasný. Horšie funguje, keď konflikt závisí od sporov o kvalite alebo od dôkazov, ktoré skript nerozhodne.

Balík môže byť vedený ako doručený, hoci kupujúci tvrdí, že škatuľa bola prázdna. Dodávateľ môže trvať na tom, že práca zodpovedala dohodnutej špecifikácii, kým klient tvrdí, že je nepoužiteľná. Inokedy predajca obhajuje popis produktu alebo vývojár tvrdí, že etapa bola splnená, kým kupujúci alebo financujúci hovoria, že dodaný výsledok nezodpovedá sľubu.

Sú to problémy úsudku, ktoré stoja nad vrstvou vysporiadania, a samotné vysporiadanie ich nevyrieši.

Moderné súdy spájajú niekoľko funkcií naraz: zbierajú dôkazy, určujú postup, vykladajú sporné fakty, vynášajú rozsudky a spájajú ich s donucovacou silou. Veľká časť hodnoty tohto balíka nepochádza zo samotného monopolu. Pochádza z existencie postupov, záznamov, procesného postavenia a fóra, o ktorom strany očakávajú, že ho ostatní uznajú.

Paralelná ekonomika musí tento stack rozdeliť a niektoré časti sú už k dispozícii. Reputácia dokáže potrestať zjavný podvod a escrow zmrazí prostriedky, kým nepríde rozhodnutie. Postavenie v komunite môže tlačiť nepoctivého obchodníka alebo skorumpovaného rozhodcu k lepšiemu správaniu. V ohraničených komunitách môže byť vylúčenie prísnou sankciou: obchodník, ktorý podvedie, si môže nechať jednu platbu, no stratí ďalších sto, a to často stačí, aby bol bežný obchod poctivý.

Ťažšie prípady zostávajú nedostatočne vybudované.

Vážny systém arbitráže potrebuje viac než chat a peňaženku.[11] Potrebuje postupy na predkladanie dôkazov a pravidlá na posudzovanie svedectiev. Potrebuje tiež normy pre konflikty záujmov a nejaký spôsob, ako uro-

biť precedens čitateľným, aby každý nový spor nezačínal od nuly. Účastníci musia mať aj dôvod veriť, že rozhodcovia majú čo stratiť, ak rozhodnú zle. V niektorých kontextoch to môže zabezpečiť zložená zábezpeka. V iných bude mať väčšiu váhu opakovaná reputácia alebo technické postavenie.

Obchodníci sa od dávna spoliehajú na súkromné usporiadanie vzťahov a opakované obchodovanie, často popri mestských alebo štátnych súdoch, aby disciplinovali obchod tam, kde bolo formálne právo pomalé alebo zle prispôsobené danému obchodu. Digitálne siete menia rozsah a nástroje, ale nie podstatu problému: obchod medzi cudzími ľuďmi stále potrebuje spôsob, ako naložiť s porušením zmluvy. Jednou súčasnou odpoveďou je kodifikovať výslovný libertariánsky základ súkromného práva, na ktorý sa môžu dobrovoľní prijímatelia odvolávať vo svojich zmluvách a rozhodcovských doložkách. Dáva tak spoločný právny východiskový bod, ktorý rozdelenej vrstve stále chýba.[12]

Táto vrstva zostáva nezrelá.

Existujú pokusy s rozhodcami so zábezpekou a komunitnými porotami, popri rade protokolom riadených mechanizmov.[15] Niektoré fungujú v úzkych prípadoch. Žiadny zatiaľ nemá legitimitu ani procesnú zrelosť súdneho systému opretého o dlhú prax. Tú medzeru netreba skrývať. Paralelná ekonomika vyriešila vysporiadanie čistejšie, než vyriešila rozhodovanie sporov.

Smer je však jasný. Súdy sú inštitúcie a inštitúcie môžu súťažiť, špecializovať sa, zlyhávať, zlepšovať sa a štiepiť sa na užšie služby. Paralelná ekonomika zatiaľ nepostavila úplný poriadok súkromného práva. Podstatná otázka je, či diely, ktoré na neho treba, môžu vzniknúť z opakovanej výmeny pod reputačným tlakom a z kryptografickej kontroly nad prostriedkami. Môžu.

24.6 Objavovanie obchodníkov a vznik inštitúcií

Trhy nevznikajú preto, že ich niekto vyhlási za otvorené. Trhy vznikajú, keď sa ľudia nájdu a obchodujú znova.

Preto je inštitucionálna vrstva väčšia než escrow a arbitráž. Zahŕňa aj objavovanie.

Obchodník s dobrým produktom je kupujúcemu k ničomu, ak ho nevie nájsť. To isté platí o zručnom vývojárovi, ktorého vydanie nemožno odlíšiť od falzifikátu, alebo o spravodlivom rozhodcovi, ktorého nepoznajú strany, čo ho potrebujú. Trh rastie, keď sa cesty medzi týmito rolami stanú lacnými a čitateľnými.

Nostr tu pomáha, lebo jedna identita môže prechádzať viacerými kontextmi naraz. Ten istý kľúč, ktorý uverejňuje príspevky, môže podpisovať vydania softvéru, zverejňovať ponuky na trhovisku, prijímať platby, odpovedať na otázky a ukazovať dlhú verejnú históriu správania. Kupujúci

neskúma jedinú izolovanú ponuku, aby sa rozhodol vo vákuu. Môže skúmať celú stopu: kto predajcu sleduje, ako dlho kľúč publikuje a či sa sťažnosti riešili na verejnosti, alebo sa odpovedalo mlčaním.

Výsledkom je hustota. Hustý trh uchováva informácie o správaní v čase a zvyšuje cenu straty postavenia, keď sa opakovaná výmena zahusťuje. Umožňuje tiež protistranám porovnávať alternatívy. Riedky trh posiela účastníkov po každom zlyhaní späť na nulu.

Zhusťovanie prebieha cez opakovaný kontakt. Prispievajú k nemu meetupy (stretnutia komunity), workshopy, obchodnícke kruhy, súkromné skupinové chaty, hlásenia chýb, odporúčania escrow a podpísané ponuky. Digitálne a fyzické inštitúcie sa navzájom posilňujú. Obchodníkovi, ktorého ste stretli osobne, sa online dôveruje ľahšie. Vývojárovi, ktorého kód používate dva roky, sa dôveruje ľahšie, keď začne predávať hardvér. Miestny bitcoinový meetup, z ktorého sa stane pravidelný obchod, prestáva byť spoločenskou udalosťou a stáva sa infraštruktúrou.

Sprostredkujúci obchodníci a premosťujúce roly

Trhy sa zhusťujú aj špecializáciou. Jedna z najužitočnejších rolí na okraji paralelnej ekonomiky je sprostredkujúci obchodník (proxy merchant): osoba alebo malá firma, ktorá sa stýka s odkrytou stranou ekonomiky, aby ostatní účastníci mohli zostať mimo tejto hranice. Niekedy je to OTC zmenárnik, ktorý prevádza medzi bitcoinom a miestnou menou. Inokedy je to nákupný agent, ktorý nakupuje od dodávateľov napojených na starý systém v mene protistrany, ktorá chce mať svoje meno a adresu mimo objednávky, alebo prevádzkovateľ odkladacích miest a preposielacích trás, vďaka ktorým sa kupujúci a predajca nemusia stretnúť priamo. Funkcia zostáva rovnaká. Usporiadanie sústreďuje vystavenie u vybraného špecialistu, ktorý riziko oceňuje a buduje si povesť, že ho zvláda dobre.[13]

Tieto roly zužujú dôveru a dávajú jej cenu. Vytvárajú aj známe nebezpečenstvo: most, ktorý používajú všetci, je most, ktorý sleduje každý. Inštitucionálna odpoveď je tá istá, akú kapitola už dala pri escrow a arbitráži: pluralita a ľahká vymeniteľnosť. Zdravý paralelný trh drží v hre veľa sprostredkujúcich obchodníkov a príbuzných premosťujúcich služieb, aby sa žiadny jediný prevádzkovateľ nestal úzkym hrdlom.

Pojem paralelná ekonomika znamená presne to, čo hovorí: druhú sadu kanálov, po ktorých môže bežať komunikácia, platba, reputácia, objavovanie aj obchod. Tieto kanály môžu existovať v tom istom meste a na tých istých uliciach ako starý systém. Zostávajú odlišné, keď tok obchodu a informácií už nezávisí od sprostredkovateľov pod štátnou kontrolou.

Inštitúcie vznikajú používaním. Žiadna komisia nemôže vopred navrhnúť celý poriadok. Obchodníci s dobrou praxou pri sporoch získavajú viac obchodu a poskytovatelia escrow, ktorí spravodlivo riešia konflikty, majú opakovaný dopyt. Trhoviská s lepším vyhľadávaním a lepšou

odolnosťou voči spamu získavajú používateľov a meetupy, ktoré dôsledne združujú serióznych obchodníkov, sa stávajú uzlami ekonomickej hodnoty. Postupom času sa tieto praktiky stvrdnú na normy a normy na inštitúcie.

Ten proces je pomalší než nasadzovanie softvéru. Takto však trhy rástli vždy.

24.7 Súčasné limity a čestné hranice

Inštitucionálna vrstva sa stále buduje.

Reputácia vytvára jedno zjavné nebezpečenstvo. Tá istá kontinuita, ktorá umožňuje iným dôverovať vám, umožňuje aj sledovať vás. Pseudonymita funguje, lebo nesie históriu, a tá istá história môže odhaliť vzorce a protistrany každému, kto pozoruje dosť dlho. Obchodník môže chcieť jednu reputáciu na verejný obchod a inú na citlivý, vývojár jednu identitu na softvér a inú na politické písanie. Oddelenie identít zostáva v praxi ťažké, lebo úspech vytvára viditeľnosť, ktorej sa mal vyhnúť.

Escrow vytvára ďalšie nebezpečenstvo. Dôveryhodná tretia strana môže byť užšia a menej invazívna než platforma regulovaná štátom, no stále sa môže stať kontrolným bodom: escrow agent s dostatočným objemom priťahuje nátlak a známeho rozhodcu možno zatlačiť alebo urobiť z neho úzke hrdlo pre obchod, ktorý ním prechádza. Decentralizácia tieto riziká znižuje, no nevymaže.

S fyzickým tovarom je to stále ťažké. Kryptografia chráni správy, no neskryje adresu napísanú na balíku ani rozvrh, v ktorom prichádza kuriér. Osobný odber, schránky, odkladacie miesta a preposielacie služby v niektorých prípadoch znižujú vystavenie, ale žiadna z nich nedáva hmote slobodu, akú Tor dáva paketom. Digitálny obchod sa môže stať súkromným rýchlejšie, než sa to kedy podarí fyzickému.

Rozhodovanie sporov je stále tenšie než vysporiadanie. Pohyb prostriedkov v pseudonymných usporiadaniach už teraz prekonáva bežné financie v minimalizácii dôvery, no zložité riešenie sporov nedosiahlo porovnateľnú zrelosť. Tá medzera je skutočná.

Za ňou čaká ďalšia. Peniaze prenášajú hodnotu v priestore, kým úver prenáša hodnotu v čase. Trh, ktorý zvláda obchod s okamžitým vyrovnaním, stále potrebuje spôsoby, ako financovať výrobu a zásoby. Zmenky, obchodný úver, úver so zábezpekou a ďalšie formy komerčnej dôvery patria do ďalšej vrstvy výstavby a nástroje na platby a komunikáciu predbehli inštitúcie na financovanie prebiehajúceho podnikania.

Tieto limity argument knihy neoslabujú. Dávajú mu tvar.

Architektúra existuje na to, aby ľudia mohli začať presúvať ekonomický život mimo systémov postavených na pozorovanie a kontrolu. Nástroje sú tu. Prvé inštitúcie sa objavili a zostávajúce medzery sú dosť viditeľné na to, aby sa na nich dalo pracovať.

To stačí na to, aby sme mohli pokračovať ohraničeným obchodom a inštitucionálnym experimentovaním.

Nasledujúca kapitola sa vracia k najväčšiemu tvrdeniu knihy. Čo sa stane, keď tieto nástroje a inštitúcie prestanú byť izolovanými praktikami a začnú sa skladať do skutočnej ekonomiky?

Zhrnutie kapitoly

Nástroje riešia prenos a vysporiadanie, nevyriešia však spoľahlivosť ani problémy úsudku, ktoré vznikajú, keď cudzí ľudia obchodujú pod pseudonymami. Paralelná ekonomika potrebuje popri technickom stacku aj inštitucionálnu štruktúru a východiskom je reputácia pri pseudonymite. Trvalé pseudonymy môžu hromadiť dôveru a pritom odmietať občiansku identitu, a cena opustenia nahromadenej reputácie disciplinuje správanie. Napätie spočíva v tom, že tá istá kontinuita, ktorá umožňuje dôveru, umožňuje aj sledovanie. Žiaden nasadený systém nemaximalizuje reputáciu a neprepojiteľnosť naraz, a systémy reputácie sa môžu znovu zmeniť na infraštruktúru dosjé, ak každý obchod vyžaduje podpísaný dôkaz a každý dôkaz sa ukladá natrvalo. Potrebnou disciplínou je selektívne odhaľovanie: odhaliť, čo transakcia potrebuje, a nič viac. Poverenia s nulovou znalosťou a reputačné protokoly založené na atestáciách, stále nezrelé, otvárajú vyhliadku na oddelenie reputačných tvrdení od konkrétnych transakcií a identít, z ktorých vznikli.

Escrow, multisig usporiadania, postupné záväzky a podmienky uvoľnenia robia podvod nákladným a poctivý obchod ľahším pri väčšine ohraničených sporov. Tieto mechanizmy dôveru presúvajú, nie odstraňujú: strany stále dôverujú kľúčom a softvéru a niektoré usporiadania vyžadujú aj dôveru v rozhodcu, no úzka dôvera často stačí. Ťažšie prípady so spornou kvalitou alebo nejasným plnením vyžadujú štruktúry arbitráže, ktoré v porovnaní so štátnymi súdmi zostávajú nezrelé. Paralelná ekonomika vyriešila vysporiadanie čistejšie, než vyriešila rozhodovanie sporov, a súkromná arbitráž nedosiahla procesnú hĺbku, ktorú buduje dlhá prax. Inštitúcie vznikajú používaním: obchodníci s dobrou praxou pri sporoch získavajú opakovaný obchod a meetupy, ktoré združujú serióznych obchodníkov, sa stávajú ekonomickou infraštruktúrou.

Sprostredkujúci obchodníci patria k tomu istému vzoru. Zmenárne a prevádzkovatelia preposielania vznikajú, lebo riešia skutočné úzke hrdlo na okraji trhu, a zdraví zostávajú len dovtedy, kým ich rola ostáva konkurenčná a vymeniteľná.

Inštitucionálna vrstva nie je úplná. Úver a financovanie obchodu zostávajú pre pseudonymný obchod z veľkej časti nevybudované a nástroje na platby a komunikáciu predbehli inštitúcie na financovanie prebiehajúceho podnikania. Fyzický tovar naďalej obmedzuje medzera v anonymite, ktorú digitálne nástroje neprekonajú. Tieto limity dávajú projektu tvar bez

toho, aby podkopali jeho smer. Architektúra existuje na to, aby mohol pokračovať ohraničený obchod a inštitucionálne experimentovanie, a kapitola 25 sa vracia k väčšej otázke, čo sa stane, keď sa tieto praktiky začnú skladať.

Poznámky

[1] Timothy C. May, *The Cyphernomicon* (September 10, 1994), obsiahly dokument s najčastejšími otázkami, ktorý May rozposlal v konferencii Cypherpunks a ktorý pokrýva kryptografiu, anonymitu, digitálnu hotovosť a politické dôsledky silného šifrovania, https://nakamotoinstitute.org/library/cyphernomicon/. Epigraf pochádza z oddielu 12.3. Kratšie programové vyjadrenia pozri May, „The Crypto Anarchist Manifesto“ (1988), https://nakamotoinstitute.org/library/crypto-anarchist-manifesto/, a „Crypto Anarchy and Virtual Communities“ (1994), https://nakamotoinstitute.org/library/virtual-communities/.

[2] Pre čitateľov, ktorí chcú prejsť literatúru o súkromných inštitúciách a polycentrickej správe: Elinor Ostrom, *Governing the Commons* (Cambridge, 1990) je základná empirická štúdia samoorganizovaných inštitúcií, ktoré riešia koordinačné problémy bez štátneho vynucovania. Bruce Benson, *The Enterprise of Law* (Pacific Research Institute, 1990) a *The Law* v *To Serve and Protect* (NYU Press, 1998) sa venujú historickým príkladom súkromného práva a súkromnej polície. Edward Stringham, *Private Governance* (Oxford, 2015) uplatňuje rovnaký prístup na moderné finančné a online systémy. Z teoretickej strany je David Friedman, *The Machinery of Freedom*, 3. vyd. (2014) najčitateľnejším argumentom v prospech polycentrického práva; Tom W. Bell, *Your Next Government?* (Cambridge, 2017) sa venuje súčasným jurisdikčným inováciám. K reputácii a obchodu pri slabom vynucovaní je kľúčovou prácou Paul Milgrom, Douglass North a Barry Weingast, „The Role of Institutions in the Revival of Trade: The Law Merchant, Private Judges, and the Champagne Fairs“, *Economics and Politics* 2, č. 1 (1990). Pre širší civilizačný rámec zostáva James Dale Davidson a William Rees-Mogg, *The Sovereign Individual* (1997), hoci v detailoch zastarané, najambicióznejším pokusom opísať inštitucionálne dôsledky silnej kryptografie.

[3] Rámec, ktorý rozvíja kapitola 6, vylučuje reputáciu ako vlastnícky nárok. May, Hughes aj Szabo pomenúvajú empirickú úlohu, ktorú reputácia zohráva v anonymnom obchode: protistrany sa rozhodujú na základe podpísaných atestácií a konzistentného správania v čase, nie na základe nejakého vlastníckeho práva byť dobre hodnotený. Systémy reputácie, ktoré kapitola opisuje, nesú empirické signály; neuplatňujú vlastnícke nároky na to, čo si myslia iní. Pozri kapitolu 6, oddiel 6.5; kapitolu 21, oddiel 21.5; a Stephan Kinsella, „Defamation as a Type of Intellectual Property“, v *A Life in Liberty* (Mises Institute, 2024).

[4] Eric Hughes, „A Cypherpunk's Manifesto“ (1993), https://www.activism.net/cypherpunk/manifesto.html: „Keďže chceme súkromie, musíme zabezpečiť, aby každá strana transakcie poznala len to, čo je pre túto transakciu priamo nevyhnutné.“ (Since we desire privacy, we must ensure that each party to a transaction have knowledge only of that which is directly necessary for that transaction.)

[5] Nick Szabo, „Formalizing and Securing Relationships on Public Networks“ (1997), https://nakamotoinstitute.org/library/formalizing-securing-relationships/. Szabo určuje vyhľadávanie, vyjednávanie, záväzok, plnenie a rozhodovanie sporov ako fázy, ktoré musia riešiť inteligentné zmluvy a digitálne inštitúcie.

[6] Nick Szabo, „Negative Reputations“ (1996), https://nakamotoinstitute.org/library/negative-reputations/.

Szabo vymedzuje napätie, ktoré opisuje hlavný text: lokálne nymy zachovávajú vzájomnú zmluvnú väzbu (privity), ale keď pseudonym nazbiera príliš veľa negatívnych informácií, možno ho zahodiť v prospech nového, pokiaľ protistrany nežiadajú silnejšiu kontinuitu alebo nenegatívne poverenia.

[7] Jan Camenisch a Anna Lysyanskaya, „An Efficient System for Non-Transferable Anonymous Credentials with Optional Anonymity Revocation“, EUROCRYPT 2001, je základná práca o anonymných povereniach; podpisy BBS+ a štandard W3C Verifiable Credentials prenášajú myšlienku do novšej praxe. Semaphore, ktorý spravuje Ethereum Privacy and Scaling Explorations (`https://semaphore.pse.dev`), poskytuje anonymné dôkazy členstva v skupine vhodné na signalizáciu proti útokom typu Sybil a používal sa v projektoch vrátane Zupass, Worldcoin a Bandada. UniRep (`https://developer.unirep.io`) je protokol založený na atestáciách zameraný priamo na reputáciu: atestujúci podpisujú výroky o používateľovi, používateľ neskôr dokazuje súhrnné vlastnosti s nulovou znalosťou a prepojiteľnosť medzi dôkazom a podkladovou históriou atestácií sa preruší. Tieto systémy zostávajú vo výskumnej fáze alebo v ranej produkcii, zatiaľ nie sú nasadenou infraštruktúrou trhovísk, ale základné stavebné prvky sú preukázané.

[8] Nostr Improvement Proposal 05 (Mapping Nostr keys to DNS-based internet identifiers) definuje mapovanie identifikátorov opreté o DNS a HTTPS, používané pre ľudsky čitateľné mená v protokole Nostr, `https://github.com/nostr-protocol/nips/blob/master/05.md`.

[9] Nostr už obsahuje časti protokolu užitočné na dôkaz ovládania kľúča metódou výzvy a odpovede. NIP-42 štandardizuje výzvy na overenie voči relayu (`https://github.com/nostr-protocol/nips/blob/master/42.md`), kým NIP-59 definuje gift wrapping: trojvrstvovú schému rumor, seal a gift wrap, ktorá zakrýva metadáta správy vrátane odosielateľa, príjemcu a časovej pečiatky (`https://github.com/nostr-protocol/nips/blob/master/59.md`). NIP-59 poskytuje súkromie pri smerovaní správ, ale sám o sebe nie je dôkazom identity.

[10] Nástroje selektívneho odhaľovania dosiahli produkčný rozsah na komunitnej aj štátnej strane: Semaphore a Zupass na podujatiach konferenčného rozsahu, zkLogin pre peňaženky odvodené cez OAuth na Sui, W3C Verifiable Credentials ako všeobecný formát, mobilné vodičské preukazy ISO/IEC 18013-5 v niekoľkých krajinách; či nástroje poskytujú súkromie, ktoré v sebe nesú, závisí od postoja overovateľov, nie od súboru funkcií protokolu. Semaphore, `https://semaphore.pse.dev/`. Zupass, `https://zupass.org/`. zkLogin on Sui, `https://docs.sui.io/concepts/cryptography/zklogin`. W3C Verifiable Credentials Data Model, `https://www.w3.org/TR/vc-data-model/`. ISO/IEC 18013-5:2021, „Personal identification, ISO-compliant driving licence, Part 5: Mobile driving licence (mDL) application“, `https://www.iso.org/standard/69084.html`. Podpora vodičského preukazu v Apple Wallet a postupné zavádzanie v štátoch na `https://support.apple.com/guide/wallet/use-your-drivers-license-or-state-id-apd1b8b6b87e/web`. Referenčná implementácia EU Digital Identity Wallet na `https://github.com/eu-digital-identity-wallet`. K problému stimulov na strane overovateľov pozri Center for Democracy & Technology, „The Limits of Zero-Knowledge Proofs as a Privacy Solution“, `https://cdt.org/`.

[11] Nick Szabo, „Rights, Remedies, and Security Models“ (2004), `https://nakamotoinstitute.org/library/rights-remedies-and-security-models/`. Szabo tvrdí, že digitálne systémy dokážu vynucovať len úzku podmnožinu toho, čo súdy riešia v plnom rozsahu sporov, pretože počítačová bezpečnosť sa opiera o samovynucujúce mechanizmy a záznamy, kým právo sa opiera o nápravu, postup a silu za rozsudkom. Práve tento rozdiel oddiel opisuje.

[12] Stephan Kinsella, Alessandro Fusillo, David Dürr a Patrick C. Tinsley (Hans-Hermann Hoppe, poradca), *The Universal Principles of Liberty* (August 14, 2025), `https://stephankinsella.com/principles/`, je jedným z takýchto pokusov. Formuluje systematický libertariánsky základ súkromného práva vrátane neagresie, sebavlastníctva, prvotného privlastnenia, dobrovoľnej výmeny a nápravy, spolu s článkom IV o „Decentralised Legal Order", ktorý výslovne podporuje súťažnú arbitráž a zvykový vývoj práva bez nátlakového monopolu. Oddiel Scope and Hierarchy výslovne uvádza, že prijímatelia môžu na tomto základe budovať sekundárne kódexy a zákony, pričom spory o nezlučiteľnostiach rozhoduje nestranná arbitráž. Samotný dokument bol vpísaný do blockchainu Bitcoinu, čo ukazuje, ako môžu kryptografické kanály niesť inštitucionálne artefakty, od ktorých paralelná ekonomika závisí.

[13] K sprostredkujúcim obchodníkom a príbuzným hraničným rolám pozri Smuggler a XYZ, *Second Realm: Book on Strategy* (Liberty Under Attack Publications, 2015), najmä oddiely o špecializácii, sprostredkujúcich obchodníkoch, zdieľaných službách a OTC zmenárnikoch. K staršej logike prechodu, ktorá stojí za tým istým krokom, pozri Samuel Edward Konkin III, *New Libertarian Manifesto* (1980). Tieto zdroje sú tu užitočné, lebo pomenúvajú skutočnú inštitucionálnu funkciu, ktorú samotný kryptografický stack nepomenúva.

[14] Satoshi Nakamoto, „Bitcoin: A Peer-to-Peer Electronic Cash System" (2008), `https://bitcoin.org/bitcoin.pdf`. Oddiel 4 opisuje reťazec digitálnych podpisov, ktorý v protokole Bitcoinu tvorí vlastníctvo; multisig rozšírenie – umožňujúce usporiadania kľúčov M z N – bolo zavedené cez opkód OP_CHECKMULTISIG v pôvodnom kóde a neskôr štandardizované v P2SH (BIP 16, január 2012) a P2WSH (BIP 141, november 2015). Špecifikáciu BIP 16 pozri `https://github.com/bitcoin/bips/blob/master/bip-0016.mediawiki`. K BIP 141 pozri `https://github.com/bitcoin/bips/blob/master/bip-0141.mediawiki`. Usporiadanie dva z troch opísané v hlavnom texte je štruktúra, ktorú Bisq používa pre svoj mechanizmus escrow: `https://bisq.network/faq`.

[15] Kleros je najrozšírenejší protokolom riadený systém riešenia sporov: systém na báze Ethereum, v ktorom sa spory podávajú na reťazci, porotcovia so vkladom v tokenoch PNK sa vyberajú koordináciou na Schellingovom bode a rozhodnutia sa vynucujú uvoľnením prostriedkov cez inteligentné zmluvy. Kleros, `https://kleros.io`; technický whitepaper: Clément Lesaege a Federico Ast, „Kleros: Short Paper v1.0.7", `https://kleros.io/whitepaper.pdf`. K variantu Aragon Court (dnes Aragon Govern) pozri `https://aragon.org`. Akademické spracovanie mechanizmu koordinácie na Schellingovom bode, na ktorom stojí výber porotcov cez tokeny, je Thomas Schelling, *The Strategy of Conflict* (Harvard University Press, 1960), kapitola 3. Tieto systémy spoľahlivo riešia úzke spory na reťazci; ich procesná hĺbka pri zložitých sporoch o fakty mimo reťazca zostáva obmedzená tým, že porota nevie preskúmať dôkazy mimo toho, čo sa predložilo na reťazci.

[16] K úveru, financovaniu obchodu a kapitálovej štruktúre výroby na slobodnom trhu pozri Murray N. Rothbard, *Man, Economy, and State*, 2. vyd. (Ludwig von Mises Institute, 2004), kapitoly 5–6, ktoré analyzujú kapitálové statky, štádiá výroby a teóriu úroku založenú na časovej preferencii, bez ktorej sa úver nedá pochopiť. Jesús Huerta de Soto, *Money, Bank Credit, and Economic Cycles*, 3. anglické vyd. (Ludwig von Mises Institute, 2012), sleduje historický vývoj úverových nástrojov vrátane zmeniek a inštitucionálne podmienky, za ktorých komerčná dôvera umožňuje financovanie výroby. Medzera uvedená na konci oddielu 24.7 – že nástroje na platby a komunikáciu predbehli inštitúcie na financovanie prebiehajúceho podnikania – presne zodpovedá rozlíšeniu, ktoré Rothbard robí medzi peňažným vzťahom a úverovým vzťahom: peniaze prenášajú kúpnu silu v priestore, úver v čase a inštitucionálne predpoklady každého z nich sú odlišné.

25

BUDOVANIE PARALELNEJ EKONOMIKY

> *„Vytvoríme civilizáciu Mysle v kyberpriestore. Nech je ľudskejšia a spravodlivejšia než svet, ktorý predtým vytvorili vaše vlády.“*
>
> John Perry Barlow, „Vyhlásenie nezávislosti kyberpriestoru“ (1996)[1]

Úvod

Táto kniha sa začala výzvou: „Ak nemáte čo skrývať, nemáte sa čoho báť.“ Sľubovala úplnú odpoveď, ktorá spojí ekonómiu s kryptografiou a filozofiu s inžinierstvom.

Predchádzajúce kapitoly stavali argument po etapách: základy v časti II, výmenu a zdravé peniaze v časti III, protivníka v časti IV a súbor nástrojov v časti V, od kryptografie a anonymných sietí cez Bitcoin a dôkazy s nulovou znalosťou až po decentralizovanú sociálnu infraštruktúru.

25.1 Zbiehanie základov

Tri axiómy knihy pôsobia na rôznych úrovniach, no ukazujú rovnakým smerom.

Axióma konania zakladá súkromie ako štrukturálnu vlastnosť. Ľudské konanie je účelné správanie, ktoré vyžaduje vnútorné uvažovanie, a konajúci nevyhnutne vie niečo, čo ostatní nevedia: má preferencie a plány, ktoré existujú v jeho mysli skôr, než ich odhalí. Táto asymetria je súčasťou konania, pretože ľudia uvažujú a vyberajú. Súkromie teda existuje

ako opisný fakt ešte predtým, než sa o ňom vysloví akékoľvek normatívne tvrdenie.

Axióma argumentácie zakladá, že súkromie sa nedá súvisle poprieť. Kto vôbec argumentuje, ovláda svoje telo a myseľ, a predpokladá tak sebavlastníctvo, z ktorého súkromie vyplýva. Zástanca sledovania, ktorý obhajuje sledovanie, samotným argumentovaním dokazuje autonómiu, ktorú chce upierať iným. Tento bod je silnejší než samotné presviedčanie. Odhaľuje performatívny rozpor priamo v diskurze proti súkromiu.

Axióma odporu zakladá, že súkromie sa dá technicky brániť. Predpoklady o výpočtovej náročnosti, preverené desaťročiami neúspešných útokov, dávajú základ systémom, ktoré môžu v nepriateľských podmienkach prudko zvýšiť náklady kontroly. Na rozdiel od axiómy konania je toto tvrdenie empirické a nie je samozrejmé, no záznam ho podporuje: Tor funguje, Bitcoin spracúva bloky, šifrované správy prichádzajú k adresátom a odolné systémy prežili dlhodobý tlak aj v praxi.

Dohromady tieto axiómy tvoria úplný základ. Súkromie existuje ako fakt. Podporuje aj obhájiteľnú normu a za nepriateľských podmienok zostáva technicky možné. Paralelná ekonomika vyrastá z tohto zbiehania: z systémov, ktoré uskutočňujú to, čo ustanovuje teória a čo vyžaduje etika.

25.2 Syntéza

Osobitný prínos knihy je v tom, čo vznikne, keď sa jednotlivé súčasti spoja.

Kapitola 2 ukázala, že praxeológia a cypherpunková kryptografia, ktoré sa vyvíjali nezávisle, dospeli k rovnakým záverom o súkromí, spontánnom poriadku a zdravých peniazoch. Zhoda naznačovala, že obe tradície objavili niečo pravdivé. Táto kapitola sa pýta, čo umožňujú ich spojené poznatky.

Technický stack má vlastnosti, ktoré sa navzájom posilňujú. Každý nástroj rieši jednu zraniteľnosť a spolu podporujú formy obchodu a spolupráce, ktoré boli predtým krehké alebo drahé. Obchodník môže prijať platbu v bitcoinoch cez Tor, so zákazníkmi komunikovať šifrovanými kanálmi, preukázať poverenia bez odhalenia identity a budovať reputáciu cez Nostr, pričom menej závisí od sledovaného finančného systému. Tieto súčasti už fungujú, hoci celý stack je zatiaľ nerovnomerný a neúplný.

Syntéza prichádza v určitej historickej chvíli, keď sú nástroje konečne zrelé. Bitcoin beží bez prerušenia viac ako pätnásť rokov, Tor viac ako dvadsať a end-to-end šifrovanie je súčasťou aplikácií na posielanie správ, ktoré ľudia používajú každý deň. Hrozba medzitým rastie: CBDC postupujú k nasadeniu, infraštruktúra sledovania sa rozširuje, regulačný tlak na burzy a poskytovateľov infraštruktúry sa stupňuje. Skorší cypherpunkeri mali víziu bez infraštruktúry, skorší rakúski ekonómovia teóriu bez uskutočnenia. Dnešok ponúka oboje naraz.

25.3 Prerušenie slučky pozorovania

Zdaňovanie aj konfiškácia vyžadujú, aby sa dal bohatstvo identifikovať a prinútiť jeho vlastníka, aby sa ho vzdal. Inflácia funguje rovnako na menovej vrstve: znehodnotiť menu sa dá len vtedy, ak je jediným prostriedkom v obehu. Keď je identifikácia menej spoľahlivá alebo drahšia, prevod sa sťažuje a predražuje. Jedna transakcia, ktorá unikne pozorovaniu, je malý efekt. Ak však pozorovaniu rutinne uniká veľa transakcií, výber príjmov je menej účinný a kontrola menej presná. Aby tento posun mal váhu, štát nemusí zmiznúť. Stačí, ak sa sledovanie stane slabším a drahším základom vlády.

CBDC sú protiťahom štátu: prebudovať samotné peniaze tak, aby pozorovanie bolo automatické a nevyhnutné, pretože ak všetky transakcie prebiehajú cez infraštruktúru pod kontrolou štátu, fáza pozorovania je triviálna. Paralelná ekonomika je protiťahom na tento protiťah. Každá transakcia mimo infraštruktúry sledovania ukazuje, že pozorovanie nie je nevyhnutné. Súťaž prebieha medzi infraštruktúrou sledovania, ktorá udržiava kontrolu lacnú, a infraštruktúrou súkromia, ktorá robí kontrolu drahšou a menej spoľahlivou.

25.4 Čo sa podarilo

Kryptoanarchistická vízia z kapitoly 2 sa sčasti zhmotnila. Záznam začína tým, čo funguje.

Bitcoin beží bez prerušenia od januára 2009. Žiadna vláda ho napriek vytrvalým pokusom nezlikvidovala: keď Čína v roku 2021 zakázala ťažbu bitcoinov,[10] hashrate siete sa za niekoľko mesiacov obnovil, pretože sa ťažba rozptýlila medzi jurisdikcie. Konsenzus pretrval pod dlhodobým tlakom protivníkov, a to je prevádzkový dôkaz, ktorý teoretické kapitoly predpovedali.

Cez Tor prechádza značný objem prevádzky používateľov a sieť nekontroluje žiadny jednotlivý subjekt. Skryté služby hostia trhy a komunikačné kanály, ktoré pretrvávajú napriek zásahom orgánov činných v trestnom konaní. Keď sa služby zhabú, objavia sa nové. Architektúra útoky pohlcuje a ďalej funguje.

Šifrovaná komunikácia sa rozšírila tak, ako sa to cypherpunkerom z deväťdesiatych rokov zdalo nemožné. Signal je dnes bežná celosvetová aplikácia a end-to-end šifrovanie je vo veľkom meradle súčasťou spotrebiteľských aplikácií na posielanie správ. Problém „going dark“ (strata prístupu k obsahu komunikácie), na ktorý sa orgány činné v trestnom konaní sťažujú, je dôkazom úspechu: komunikácia, ktorú nemožno odpočúvať ani so zákonným oprávnením, je presne to, čo cypherpunkeri chceli.[12]

Teoretický rámec tento výsledok predpovedal. Praxeológia tvrdí, že spontánny poriadok vzniká z dobrovoľnej výmeny bez centrálneho plá-

novania, a paralelná ekonomika ukazuje tento princíp v praxi. Axióma odporu tvrdí, že správne navrhnuté systémy môžu kontrole odolať, a záznam za uplynulých pätnásť rokov toto tvrdenie podporuje. Teória a dôkazy sa stretávajú na prevádzkovom prahu, ktorý ani jedna strana sama nedosiahla.

Paralelné inštitúcie na tom istom území

Paralelná ekonomika rastie v tých istých mestách a obchodných štvrtiach, kde už funguje oficiálna ekonomika, a nečaká na vlastnú geografiu. Súkromná dielňa stojí o ulicu ďalej od regulovaného kancelárskeho parku. Bitcoinový meetup sa koná pár blokov od pobočky banky. Obchodník, ktorý prijíma bitcoin a koordinuje sa cez šifrované kanály, si môže prenajímať priestor v meste, ktoré štát úplne zmapoval.

Tým sa mení, čo znamená úspech. Úspech nie je územná čistota, ale rast paralelných inštitúcií, ktoré sa môžu stretávať, obchodovať, učiť a vyrovnávať účty bez toho, aby pri každom kroku žiadali o povolenie staré kanály. Digitálny stack to umožnil, fyzické predmostia to robia trvalým.

Hakim Bey priniesol prvé pomenovanie dočasnej autonómnej zóny. Praktická podoba, o ktorú ide v tejto knihe, je užšia a trvácnejšia. Sú to opakujúce sa ostrovy miestnej autonómie: meetupy, dielne, obchodné miestnosti a obchodné uzly zasadené do bežných miest, kým sa čoraz viac ich koordinácie presúva na súkromné kanály.[2]

Kryptografický stack dozrel

Primitíva, ktoré sme rozoberali v častiach IV a V, prešli z výskumu do reálneho nasadenia počas písania tejto knihy. Dôkazy s nulovou znalosťou, ktoré pred desiatimi rokmi vyžadovali dôveryhodné nastavenie, dnes bežia na rekurzívnych konštrukciách, ktoré nastavenie úplne odstraňujú. Systémy ako Semaphore, Zupass a zkLogin od Sui ich prinášajú do predaja vstupeniek na podujatia, vydávania poverení a odvodzovania peňaženiek cez OAuth v spotrebiteľskom meradle. Úplne homomorfné šifrovanie sa dnes nasadzuje v úzkych aplikáciách, po tom, čo sa od Gentryho konštrukcie z roku 2009 zlepšilo o štyri rády.[11] Bezpečný výpočet viacerých strán chráni prahovým podpisovaním približne dvetisíc inštitucionálnych zákazníkov úschovy. Prahové schémy MuSig2 a FROST založené na Schnorrovi robia z multisig transakcií n z n aj t z n v reťazci nerozoznateľné od transakcií s jedným podpisom. Dôveryhodné prostredia na vykonávanie kódu sú v hardvéri stoviek miliónov spotrebiteľských zariadení a dnes stoja aj za atestovanými službami v meradle cloudu: Apple Private Cloud Compute, Azure Confidential Computing, AWS Nitro Enclaves a Google Cloud Confidential Computing. Diferenciálne súkromie chráni zverejnenie výsledkov sčítania ľudu v USA v roku 2020 aj telemetriu každého novšieho iPhonu. Súkromné získavanie informácií sa dostalo do praxe v obja-

vovaní kontaktov v aplikácii Signal a v otvorených implementáciách okolo SealPIR a SimplePIR. Postkvantový prechod sa začal v protokole PQXDH aplikácie Signal, v iMessage PQ3 od Applu, v hybridnej výmene kľúčov prehliadača Chrome a na okrajových serveroch firmy Cloudflare. Mriežkové a hašové štandardy NIST sú dokončené a návrh prechodu Bitcoinu (Pay-to-Merkle-Root podľa BIP-360) sa aktívne spresňuje. Pripravuje sa aj aktualizácia FCMP++ v sieti Monero, ktorá má nahradiť kruhové podpisy dôkazmi členstva v celom reťazci.

Transportná vrstva sa rozšírila za bežný internet. Siete Meshtastic rástli na veľkých podujatiach, kde je konvenčná sieť preťažená alebo nedôveryhodná. Reticulum oddeľuje kryptografické adresovanie od akéhokoľvek konkrétneho fyzického média. Sieť FIPS (Free Internetworking Peering System) poskytuje prekryvnú sieť nezávislú od transportu, v ktorej sú smerovacie adresy samy vygenerované kryptografické identity bez závislosti od poskytovateľa internetu, registrátora či certifikačnej autority. BitChat priniesol správy cez Bluetooth mesh masovému publiku. Satelitné konštelácie Iridium, OneWeb, Starlink a Globalstar prenášajú prevádzku, ktorá nezávisí od pozemnej infraštruktúry žiadneho jedného štátu.

Spolu s obranou dozrel aj protivník. Kapitola 12 opísala analytický stack, ktorý štát dnes kupuje od komerčných dodávateľov: siete senzorov, sprostredkovateľov lokalizačných údajov, platformy na zlučovanie údajov poháňané umelou inteligenciou, komerčný špionážny softvér a atestované rozhodovacie systémy, ktoré celú slučku OODA stláčajú do priemyselného procesu. Odpoveď obrancu sa vyvíja spolu s protivníkom. Šifrovanie obsahu zostáva nevyhnutné, no už nestačí, pretože model schopný pracovať s metadátami vyvodzuje závery z načasovania, sociálneho grafu, polohy a frekvencie aj vtedy, keď obsah nemá. Anonymita prenosu, mesh smerovanie, súkromné získavanie informácií a výpočty nad tajomstvami sú praktické odpovede na tú časť stacku, ktorá analyzuje metadáta. Ich zrelosť je dôvod, prečo ich táto kniha považuje za infraštruktúru prvej úrovne.

Stack, ktorý tu opisujeme, v podobe, akú si predstavovala pôvodná cypherpunková vízia v kapitole 2, neexistoval. Dnes existuje. Teoretická architektúra, ktorú kniha sledovala v predchádzajúcich kapitolách, je to, čo svet už postavil.[3]

Empirický záznam a čo preveruje

Paralelná ekonomika je ústredné prevádzkové tvrdenie tejto knihy a každé prevádzkové tvrdenie sa musí dať preveriť porovnaním s tým, čo svet vytvára. Záznam nazbieraný za posledné desaťročie je neúplný a práve neúplnosť je poučná. Každý prípad potvrdzuje časť teórie a ilustruje konkrétne štrukturálne tlaky, ktoré predchádzajúce kapitoly pomenovali abstraktne.

„Kruhové" bitcoinové ekonomiky (circular economies) vznikli tam, kde spolu platili dve podmienky: miestne regulačné prostredie, ktoré to dovoľovalo, a podnikavá komunita odhodlaná robiť experiment dosť dlho, aby dosiahol prahovú hustotu. Kde obe podmienky platili, obchodníci prijímali bitcoin, mzdy a úspory sa počítali v bitcoinoch, a to všetko bez toho, aby v tomto médiu pôsobila štátna menová autorita. Kde chýbala čo i len jedna z podmienok, experimenty hustotu nedosiahli. Teória to predpovedá. Spontánny poriadok vzniká z dobrovoľnej výmeny tempom, aké účastníci udržia, a rozhodujúcim obmedzením je ich ochota výmenu udržiavať, nie nejaká technická vlastnosť peňazí.

Zrušenie štatútu zákonného platidla pre Bitcoin v Salvádore na začiatku roka 2025 pod tlakom financovania z MMF stojí za pomenovanie, lebo preveruje jedno konkrétne vedľajšie tvrdenie a hlavné necháva na pokoji. Hlavné tvrdenie tejto knihy znie, že paralelné inštitúcie sa dajú postaviť na kryptografických kanáloch a môžu fungovať bez povolenia štátu. Vedľajšie tvrdenie, ktoré občas šíria nadšenci, znie, že prijatie Bitcoinu štátom je samo osebe zmysluplným krokom k paralelnej ekonomike. Zrušenie vedľajšie tvrdenie vyvracia a hlavného sa nedotýka. Štát, ktorý prijme Bitcoin pod domácim nadšením a potom sa tohto štatútu pod vonkajším tlakom financovania vzdá, ukázal, že prijatie nebolo štrukturálnou zmenou. Štrukturálna zmena sa deje v dobrovoľnej ekonomike obchodníkov a držiteľov, ktorí konajú bez požehnania štátu, a v tejto ekonomike kruhová činnosť v Bitcoin Beach, v El Zonte a okolitých komunitách pokračovala aj po zrušení štatútu zákonného platidla. Čo štát vyhlásil za zákonné platidlo, mohol odvolať. Čo sa účastníci rozhodli obchodovať, nemohol zvrátiť.[4]

Druhý empirický vzorec je gentrifikácia, ktorú vidno na viacerých prvých miestach s kruhovou ekonomikou. Keď sa malé pobrežné mestečko stane cieľom bohatých návštevníkov s bitcoinmi, ceny pozemkov prudko stúpnu a miestni obyvatelia, ktorým mal experiment slúžiť, sa môžu dostať do situácie, že si vlastnú štvrť už nemôžu dovoliť. Je to všeobecný vzorec každého miesta, ktoré sa stane atraktívnym pre bohatších ľudí zvonka, a v univerzitných mestách a rekreačných dedinách ho vidno v každej krajine už sto rokov. Bitcoin pridáva k starému javu novú premennú. Paralelné ekonomiky majú, tak ako každé ekonomiky, distribučné dôsledky a prvotné výhody novej menovej architektúry nepripadnú automaticky tým účastníkom, ktorých pomenovala raná rétorika.

Tretí vzorec je krehkosť centralizovaných peer-to-peer trhovísk. Postupné vlny služieb, ktoré sprostredkúvali obchody bitcoinov za hotovosť bez KYC, sa zatvorili pod regulačným tlakom alebo z dôvodov na strane ich prevádzkovateľov. Decentralizované alternatívy, ktoré prežili, vrátane Bisq a RoboSats, mali architektúry, v ktorých nijaký jednotlivý prevádzkovateľ nemohol byť nútený službu vypnúť. Vzorec potvrdzuje teoretický bod, ktorý kniha opakovane uvádza. Decentralizácia chráni systémy spo-

ľahlivejšie než ľudí, ktorí ich používajú, a ľudia, ktorí proti vôli štátu prevádzkujú centralizované služby, zostávajú krehkým bodom systému.[5]

Tieto empirické pozorovania tézu knihy neoslabujú. Spresňujú ju. Paralelná ekonomika funguje a jej fungovanie je nerovnomerné. Nerovnomernosť sa dá predvídať: decentralizácia na úrovni protokolu umožňuje systémom prežiť tlak, ktorý ničí služby závislé od prevádzkovateľa; kultúrne odhodlanie udržiavať prax umožňuje, aby kruhové ekonomiky zakorenili tam, kde samotný technický prístup nestačí; a distribučné tlaky, ktoré prvotné výhody pritiahnu, sú problémy, ktoré ďalšia iterácia projektu musí predvídať a riešiť.

Správne čítanie záznamu nie je ani triumfalistické, ani podceňujúce. Je to čítanie, ktoré už naznačuje axióma odporu: hodnota systému je úmerná nákladom potrebným na jeho prelomenie a tieto náklady sa merajú empiricky, podľa toho, čo konkrétne tlaky dosiahli proti konkrétnym nasadeniam. Nasadenia vstrebali značný tlak. Odhalili tiež konkrétne body krehkosti, ktoré bude musieť ďalšia fáza inžinierstva a budovania inštitúcií riešiť. Obe polovice tejto vety sú rovnako dôležité a obe tento oddiel dokladá.

25.5 Hranice a otvorené otázky

Paralelná ekonomika je skutočná, ale obmedzená. Obmedzenia, ktoré nasledujú, určujú, čo sa dnes dá prijatím reálne dosiahnuť, a každé z nich preváži akékoľvek všeobecné tvrdenie o úspechu.

Obmedzenia meradla a výkonu

Bitcoin, Lightning, Tor aj Signal fungujú v absolútnych číslach vo významnom meradle, no voči svetovým financiám a komunikácii sú malé. Nejde o dominanciu, ale o životaschopnosť: každý systém ukázal, že jadro architektúry môže fungovať v skutočne nepriateľských podmienkach. To teoretické kapitoly predpovedali a na túto otázku musel odpovedať empirický záznam.

Meradlo však stále obmedzuje v niekoľkých konkrétnych smeroch. Priestor v blokoch Bitcoinu zostáva vzácny a tlak na poplatky pri vysokom dopyte môže malé transakcie na základnej vrstve urobiť ekonomicky nezmyselnými. Lightning výrazne zvyšuje frekvenciu platieb, no stále závisí od vstupu a výstupu v reťazci a správa kanálov vyžaduje dlhodobú pozornosť, ktorú väčšina používateľov nevenuje. Tor je pomalší a menej spoľahlivý než centralizované alternatívy, pretože cibuľové smerovanie cez dobrovoľnícke uzly pridáva latenciu, ktorú nijaká optimalizácia neodstráni bez obetovania anonymity, ktorú smerovanie zabezpečuje. Nástroje na ochranu súkromia dôsledne vyžadujú viac úsilia než sledované alternatívy, lebo réžia, ktorá súkromie vytvára, je štrukturálna: množiny anonymity potrebujú účastníkov, dôkazy s nulovou znalosťou potrebujú výpočty

a distribuovaný konsenzus potrebuje koordináciu. Centralizované služby založené na sledovaní nič z toho nehradia a zisk z efektívnosti si pripisujú ako výhodu produktu.

Napätie medzi reputáciou a anonymitou

Kapitola 24 toto napätie rozobrala podrobne. Zhrnutie je tu stručné, lebo argument už zaznel: kompromis je skutočný a štrukturálny, nie dočasný nedostatok, ktorý čaká na lepšiu implementáciu. Pseudonym, ktorý nadobúda dôveru, to robí tým, že je konzistentný a trvalý, takže jeho správanie sa dá prepojiť naprieč kontextmi. Nový kľúč, ktorý zachováva neprepojiteľnosť, nemá históriu, a protistrany preto nemajú dôvod dôverovať nad rámec minima, ktoré si vyžaduje samotná interakcia. Schémy atestácie s nulovou znalosťou ponúkajú čiastočný únik, lebo oddeľujú reputačné tvrdenia od identít, ktoré ich vytvorili. Nasadenie je však ešte v začiatkoch a schémy stále závisia od atestujúcich, ktorí podkladové fakty pozorujú. Napätie určuje, čo môže paralelná ekonomika v danom kontexte dosiahnuť, a aké veľké trenie musí znášať obchod závislý od reputácie, kým nástroje nedozrejú.

Fyzický tovar a medzera v anonymite

Digitálne nástroje súkromia chránia digitálnu činnosť. Fyzický tovar vytvára medzeru v anonymite, ktorú technológia neprekoná.

Doručenie vyžaduje fyzické adresy. Žiadne šifrovanie nechráni cieľ vytlačený na balíku, colná kontrola odhalí obsah a kuriéri sledujú doručenie. Problém „poslednej míle“ je fyzický, nie technický: tovar musí niekam doraziť a toto niekde sa dá pozorovať.

Čiastočné zmiernenia existujú. Prevzatie na neutrálnych miestach, napríklad na poštových priehradkách alebo vo výdajných boxoch, presúva vystavenie z domácej adresy na miesto odberu. Preposielacie služby a prepošťovne pridávajú sprostredkovateľov, ktorí pozorovanie otupujú. Každé z nich prináša oneskorenie a nové body zlyhania a medzeru neuzatvára. Žiadne z nich nedosahuje pri fyzickom tovare to, čo Tor dosahuje pri digitálnej prevádzke.

Akademická práca o anonymnom fyzickom doručovaní existuje (APOD, Lelantos), no do praktického nasadenia sa nedostala.[13] Problém nie je čisto technický: fyzické predmety sa nedajú kopírovať a presmerovávať ako dátové pakety. Fyzika hmoty obmedzuje, čo môže kryptografia dosiahnuť.

Toto obmedzenie pozorovali a merali agoristickí teoretici ešte pred existenciou kryptografických trhov. Rayo (Tom Marshall) vo svojom texte z roku 1973 sformalizoval tento vzťah pod hlavičkou vonu (skratka z „voluntary not vulnerable“, teda dobrovoľný, nie zraniteľný). Vynášal to, čo nazval priemerný čas do obťažovania (Mean Time to Harassment), proti osi činnosti, ktorá viedla od letného prežitia cez celoročné prežitie, pohodl-

ný domov, malú dielňu a malú výrobu až po ľahký a ťažký priemysel. Každé zvýšenie činnosti o jeden rád si vyžadovalo približne desaťnásobok prevádzkovej zručnosti, aby sa čas do odhalenia udržal na rovnakej úrovni. Spodnú hranicu zmysluplnej alternatívnej ekonomiky videl na úrovni malej dielne.[6] Osi sú dnes rovnako kryptografické ako geografické, ale krivka sa nezmenila. Malá digitálna činnosť sa dá s miernym úsilím skrývať roky, kým výroba a distribúcia vo fyzickom meradle zostávajú obmedzené rovnakou medzerou v anonymite, akú opísal Rayo pred polstoročím.

Ekonomická činnosť zahŕňa fyzický tovar. Paralelná ekonomika digitálnych služieb je dnes možná. Paralelnú ekonomiku postavenú okolo fyzickej výroby a distribúcie medzera v anonymite stále obmedzuje.

Obmedzenia súkromia v sieti Lightning

Kapitola 20 predstavila sieť Lightning (Lightning Network) ako sieť s lepším súkromím platieb než základná vrstva Bitcoinu. Je to pravda, ale vyžaduje to spresnenie.

Súkromie v Lightningu nie je absolútne.[7] Transakcie otvárajúce a zatvárajúce kanály sú viditeľné v blockchaine; môžu prezradiť približnú kapacitu a spojiť kanály s činnosťou v reťazci. Ak sú bitcoiny, ktoré kanál financujú, prepojené s identitou (zvyčajne cez burzy s KYC), toto prepojenie pretrváva. Mobilné peňaženky sa zvyčajne pripájajú k poskytovateľom služieb Lightning (LSP), ktorí vidia všetku platobnú činnosť používateľa, a dôvera sa tak z celej siete presúva na LSP. Analýza smerovania môže v niektorých prípadoch odvodiť platobné trasy, najmä pri veľkých platbách s niekoľkými použiteľnými trasami.

Osvedčené postupy tieto obmedzenia zmierňujú: otvárať kanály s prostriedkami po CoinJoine a uprednostňovať vlastné uzly pred službami s úschovou. Tieto postupy však vyžadujú technickú zdatnosť, ktorú väčšina používateľov nemá. Predvolené používanie Lightningu poskytuje oveľa lepšie súkromie než predvolené používanie Bitcoinu v reťazci, ale k ideálnej anonymite má ďaleko.

Postkvantový prechod

NIST dokončil základné štandardy podpisov založené na mriežkach a hašoch (ML-KEM, ML-DSA, SLH-DSA) v auguste 2024 a v marci 2025 vybral záložný KEM HQC založený na kódoch.[8] Bežné nasadenie sa už začalo: protokol PQXDH aplikácie Signal od septembra 2023, iMessage PQ3 od Applu od februára 2024, hybridná výmena kľúčov X25519MLKEM768 v prehliadači Chrome počas roka 2024 a okrajové servery Cloudflare, ktoré do polovice roka 2025 prenášali postkvantové TLS pri významnej časti nadviazaných spojení. Prechod Bitcoinu zaostáva, pretože každý návrh soft forku sa musí zaoberať nielen novým míňaním, ale aj zaobchádzaním s už existujúcimi ohrozenými výstupmi.[9] Súčasný pracovný návrh

je typ výstupu Pay-to-Merkle-Root (P2MR) podľa BIP-360, čo je Taproot bez možnosti míňať cez cestu kľúča; postkvantové podpisové opkódy sú samostatná budúca vrstva nad ním. Ani jedno nebolo aktivované.

Kvantové počítače v praktickom meradle zostávajú pod prahom, ktorý Shorov algoritmus vyžaduje, no stratégia „zbieraj teraz, dešifruj neskôr" robí horizont prechodu kratším, než naznačuje časový plán hardvéru. Prechod Bitcoinu sa musí dokončiť skôr, než sa objaví kvantový počítač schopný prelomiť šifry. Cesta aktivácie je prvým podstatným rozhodnutím na úrovni protokolu od Taprootu.

Riešenie sporov bez súdov

Kapitola 24 obsahovala úplné spracovanie súkromného riešenia sporov. Krátka verzia patrí aj sem: ohraničené spory už majú použiteľné nástroje. Escrow, multisig dohody a postupné záväzky zvládajú veľkú väčšinu trhových sporov, teda spory o doručenie, platbu a porušenie jasných pravidiel, nie sporné výklady zložitých skutkových okolností. Ťažké spory, ktoré zahŕňajú posudzovanie kvality, nejasné plnenie alebo sporné svedectvo, zostávajú tenšie než štátne súdy, pretože súkromná arbitráž nemá procesnú hĺbku, precedensy ani vonkajšiu vynucovaciu právomoc, ktoré štátne súdy nahromadili za stáročia praxe. Táto medzera je skutočná, nebráni paralelnej ekonomike rásť vďaka oveľa väčšiemu objemu jednoduchých sporov a vyznačuje jednu jasnú hranicu inštitucionálneho budovania, ktoré bude trvalá obchodná činnosť nakoniec vyžadovať.

Prekážky masového prijatia

Nástroje súkromia stále vyžadujú viac technických znalostí než sledované alternatívy a tento rozdiel pretrváva, aj keď sa jednotlivé nástroje zlepšujú. Nový používateľ, ktorý si zriaďuje peňaženku Lightning s vlastnou úschovou, spúšťa okruh Tor a spravuje pár kľúčov Nostr, nesie záťaž nastavovania, ktorú nemá nový používateľ, ktorý si otvára bankový účet alebo sťahuje sledovanú aplikáciu na správy. Sieťové efekty problém prehlbujú: hodnota každého komunikačného nástroja závisí od toho, či ho používajú aj ľudia, ktorých treba osloviť, takže nástroje súkromia súťažia s platformami, ktorých používateľská základňa už zahŕňa každého, koho nový používateľ pozná. Sledované služby často poskytujú v rámci svojich návrhových obmedzení lepší zážitok, pretože sa môžu agresívne optimalizovať na rýchlosť a pohodlie bez toho, aby platili réžiu, ktorú vyžadujú vlastnosti súkromia.

Právna neistota vytvára druhú prekážku, ktorú technické zlepšenie nevyrieši. Jurisdikcie sa výrazne líšia v tom, čo dovoľujú: tá istá burza, nástroj alebo prax, ktoré sú v jednej krajine bežné, môžu byť v inej porušením predpisov. Regulačný tlak na burzy a poskytovateľov infraštruktúry môže odstrániť vstupné a výstupné body, ktoré robia súkromné finančné

nástroje použiteľnými v bežnom obchode. Koncoví používatelia nevedia, či je ich vlastné používanie nástrojov súkromia zákonné a či sa tento právny stav nezmení. Stíhanie Tornado Cash, ktoré sme rozoberali v kapitole 13, ukázalo, že právne riziko dosahuje nielen používateľov, ale aj tvorcov: písanie a zverejňovanie kódu, ktorý sa štátu neskôr nebude páčiť, môže viesť k trestnému stíhaniu a odrádzací účinok siaha ďaleko za konkrétnych stíhaných vývojárov.

Čo tieto hranice znamenajú

Uvedené hranice nie sú námietkou proti projektu. Sú jeho čestným opisom. Väčšina ľudí stále pri väčšine činností závisí od systémov pod dohľadom štátu a paralelná ekonomika dnes funguje ako doplnok starého systému, nie ako jeho náhrada. Tak to v roku 2026 je. Náhrada, ak príde, je neskoršou etapou, ktorá vyplynie zo súčasnej: nástroje sa zlepšia, komunity vyrastú, inštitucionálna infraštruktúra dozrie a každý ďalší účastník, ktorý presunie časť činnosti na súkromné kanály, robí sieť o niečo užitočnejšou pre ďalšieho.

Správny rámec nie je, či paralelná ekonomika vyhrala, ale či poskytuje hodnotu už teraz a či smer zmeny vedie k väčšiemu súkromiu a autonómii, alebo od nich. V oboch ohľadoch je odpoveď áno. Nástroje opísané v tejto knihe spracúvajú skutočné transakcie, chránia skutočnú komunikáciu a podporujú skutočný obchod v nepriateľských podmienkach, ktoré by zničili skoršie pokusy. Hranice sú skutočné, konečné a zmapované. To stačí na to, aby sme mohli pokračovať.

25.6 Odpoveď na „nemám čo skrývať``

Kapitola 1 položila výzvu: „Ak nemáte čo skrývať, nemáte sa čoho báť.“ Toto tvrdenie ospravedlňuje sledovanie tým, že súkromie potrebujú len ľudia, ktorí robia zlo. Po predchádzajúcej analýze vyplýva úplná odpoveď.

Na štrukturálnej úrovni tvrdenie nechápe, čo súkromie je. Kapitola 3 ukázala, že súkromie je vlastné ľudskému konaniu, pretože ľudské konanie nevyhnutne zahŕňa vnútorné uvažovanie a subjektívne hodnotenie v podmienkach informačnej asymetrie. Súkromie je priestor, v ktorom vzniká myšlienka a vyberá sa konanie, a potrebuje ho každý človek, nech robí čokoľvek.

Na informačnej úrovni nejde o to, či niekto skrýva zlo, ale o to, ako sa vôbec riadi tok informácií. Kapitola 7 ukázala, že výmena funguje najlepšie, keď strany kontrolujú odhaľovanie. Znalosť preferencií a plánov umožňuje vykorisťovanie a transparentné vyjednávanie sa zrúti vo výhodu pre zúfalejšiu stranu. Súkromie chráni uvažovanie a umožňuje dobrovoľnú výmenu.

Na ekonomickej úrovni sledovanie deformuje trhové procesy. Cenové signály sa zhoršujú, keď sa účastníci boja pozorovania, a kapitál nasleduje regulačnú viditeľnosť namiesto ekonomických zásluh. Ekonomická kalkulácia závisí od informácií, ktoré sledovanie narúša.

Politický rozmer je priamejší. Sledovanie umožňuje kontrolu nezávisle od stíhania. Opozíciu, ktorú možno monitorovať, možno zneškodniť: darcov identifikovať a tlačiť na nich, organizátorov sledovať a obťažovať, plány odhaliť a predísť im. Totalitné režimy potrebujú sledovanie nie preto, že by všetci občania boli zločinci, ale preto, že sledovanie umožňuje kontrolu. „Nemám čo skrývať" prehliada, že hrozbou je samotné sledovanie.

Problém definície ide hlbšie než čokoľvek z uvedeného. „Nemám čo skrývať" predpokladá stabilnú, poznateľnú hranicu medzi nevinným a podozrivým. Kto však určuje, čo je „niečo na skrývanie"? Štát určuje, čo je zakázané, a zákazy sa menia. Činnosť, ktorá je dnes zákonná, môže byť zajtra trestná. Otázka nie je, či máte niečo na skrývanie teraz, ale či by ste mohli mať niečo na skrývanie podľa akéhokoľvek budúceho výkladu akejkoľvek budúcej moci.

Priznať túto neistotu neznamená, že súkromie nemá náklady alebo že kompromisy neexistujú. Nástroje súkromia môžu poskytnúť úkryt zlu. Anonymita môže chrániť zločincov popri disidentoch. Paralelná ekonomika funguje mimo právneho aparátu štátu, teda mimo jeho ochrany rovnako ako mimo jeho obmedzení, a súkromnoprávne inštitúcie, ktoré by mohli nahradiť štátne súdy, ešte dozrievajú, ako argumentovala kapitola 24. Tieto náklady sú skutočné a nemožno ich odmietnuť.

Súkromie má náklady. Sledovanie deformuje trhy a umožňuje kontrolu, čím ohrozuje podmienky, za ktorých dobrovoľná spolupráca funguje. Tieto náklady sú väčšie a ťažšie zvratné než náklady, ktoré ukladá súkromie.

Odpoveď na „nemám čo skrývať" je jednoduchá. Súkromie nie je o skrývaní. Chráni podmienky potrebné na ľudské konanie a na spoluprácu prostredníctvom trhov.

„Nemám čo skrývať" obracia dôkazné bremeno. V každom systéme, ktorý rešpektuje ľudskú schopnosť konať, otázka nie je „prečo potrebujete súkromie?", ale „na základe akého práva žiadate prístup?". Sebavlastníctvo znamená, že to, čo človek myslí a čo robí, je predvolene súkromné. Zásah si vyžaduje odôvodnenie, kým odopretie nie.

Cypherpunková odpoveď pridáva tvrdší praktický bod: aj keby sa sledovanie vyhlásilo za legitímne, nemusí zostať lacné a rutinné vo veľkom meradle. Matematika poskytuje nástroje, ktoré môžu veľa foriem sledovania urobiť nespoľahlivými a drahými. Tým sa otázka odôvodnenia neodstráni. Mení sa terén, na ktorom sa o nej bojuje.

25.7 Záver

Táto kniha sledovala argument od axiómy po uskutočnenie, od teórie po prevádzkovú realitu.

Súkromie je štrukturálnou vlastnosťou ľudského konania. V racionálnom diskurze ho nemožno súvisle poprieť. Dá sa brániť kryptografickými nástrojmi, ktoré zvyšujú náklady kontroly a zachovávajú priestor pre dobrovoľnú spoluprácu.

Štáty sledujú, pretože pozorovanie umožňuje cielenie a vyberanie a pretože oboje podporuje kontrolu. Keď sa pozorovanie stane nespoľahlivým alebo drahým, tieto mechanizmy slabnú. Aparát finančného sledovania a požiadaviek na identitu spolu so širšou regulačnou kontrolou závisí od toho, že hospodársky život zostáva dosť čitateľný na to, aby sa dal sledovať a prerušovať.

Matematika konflikt neodstránila, ale zmenila jeho ekonómiu. Obrana môže byť lacná, kým útok sa stáva drahým. Transakciu skrytú pred rutinným pozorovaním je ťažšie zdaniť; peňaženku, ktorú nemožno s istotou prepojiť, je ťažšie zhabať. Keď tieto náklady rastú naprieč dostatočným množstvom činnosti, kontrola stráca účinnosť a dosah.

Paralelná ekonomika už spracúva transakcie, ktoré štát neschválil, a smeruje správy, ktoré úrady nevedia rutinne čítať. Uchovávanie hodnoty mimo bežných kanálov zhabania a predvolené šifrovanie komunikácie odstraňujú činnosť z rutinného pozorovania. S rozširovaním prijatia sa tieto zisky násobia.

Štát si nárokuje monopol na peniaze a komunikáciu, a tým aj na spoluprácu, ktorá na oboch stojí. Tento nárok je už slabší, než sa zdá. Bitcoin funguje, Tor ďalej smeruje, Signal ďalej doručuje, primitíva pre výpočty nad tajomstvami fungujú v meradlách, pre ktoré boli postavené, a postkvantový prechod sa v produkčných systémoch začal. Monopol pretrváva tam, kde ľudia stále závisia od kanálov postavených na sledovanie a kontrolu, a ustupuje tam, kde nie.

Práca je praktická: spustite uzol, vygenerujte kľúče, šifrujte predvolene, transakcie robte súkromne, pridajte sa k meetupu alebo ho založte, prispievajte do otvorenej implementácie a budujte návyky a inštitúcie, vďaka ktorým sa nástroje navzájom posilňujú. Nástroje existujú a ich dosah závisí od toho, či ich ľudia používajú.

Budujte.

Poznámky

[1] John Perry Barlow, „A Declaration of the Independence of Cyberspace“, prednesené v Davose vo Švajčiarsku 8. februára 1996, `https://www.eff.org/cyberspace-independence`. Barlow spoluzaložil Electronic Frontier Foundation a Vyhlásenie napísal ako reakciu na americký zákon

o reforme telekomunikácií z roku 1996 (Telecommunications Act). Záverečné riadky citované vyššie vystihujú argument paralelnej ekonomiky, ktorý táto kapitola rozvíja: civilizácia postavená na iných kanáloch nie je len možná, ale už sa buduje, nech vlády robia čokoľvek. K sprievodnému vyhláseniu cypherpunkového hnutia pozri Eric Hughes, „A Cypherpunk's Manifesto“ (1993), `https://www.activism.net/cypherpunk/manifesto.html`.

[2] Hakim Bey, *T.A.Z.: The Temporary Autonomous Zone, Ontological Anarchy, Poetic Terrorism* (Autonomedia, 1991), priniesol tento pojem. K neskoršiemu strategickému textu, ktorý túto myšlienku prekladá do opakujúcich sa fyzicko-digitálnych paralelných inštitúcií, pozri Smuggler and XYZ, *Second Realm: Book on Strategy* (Liberty Under Attack Publications, 2015). Použitie v tejto kapitole je užšie než rétorika oboch textov. Označuje trvalé miestne uzly opakovaného obchodu a spolupráce na tom istom území ako oficiálny poriadok.

[3] Odkazy na jednotlivé kapitoly k novým primitívam zhrnutým v tomto oddiele: dôkazy s nulovou znalosťou v kapitole 15 (poznámky 10, 11); prahové podpisovanie a MPC v kapitole 16 (poznámka 4); dôveryhodné prostredia na vykonávanie kódu v kapitole 16 (poznámka 5); atestované dôverné vyvodzovanie LLM v kapitole 16 (poznámka 6); súkromné získavanie informácií v kapitole 16 (poznámka 7); diferenciálne súkromie v kapitole 16 (poznámka 8); postkvantové podpisy v kapitole 14 (poznámka 10) a kapitole 20 (poznámka 17); Monero FCMP++ v kapitole 20 (poznámka 15); FIPS a stack mesh transportu v kapitole 17 (poznámky 17–22); obraz protivníka s analytickým stackom v kapitole 12 (poznámky 1–9). Tieto poznámky nesú podrobné odkazy; tento oddiel zhŕňa, čo stack ako celok dnes predstavuje.

[4] Salvádor prijal Bitcoin ako zákonné platidlo v septembri 2021 za vlády Bukeleho a v januári 2025 štatút zákonného platidla zrušil v rámci dohody o financovaní s MMF; kruhová ekonomická činnosť (obchodníci, cestovný ruch, miestne platby v bitcoinoch) pokračovala aj po zrušení, čo ukazuje, že prijatie štátom a dobrovoľné prijatie sú oddeliteľné. El Salvador Ley Bitcoin, Decree 57 (8. júna 2021); zrušenie v hlasovaní Legislatívneho zhromaždenia 29. januára 2025, spracované v *Reuters* a *Bloomberg*. IMF Extended Fund Facility for El Salvador (schválený v decembri 2024), `https://www.imf.org/en/Countries/SLV`. K pokračovaniu kruhovej ekonomiky pozri dokumentáciu Bitcoin Beach na `https://www.bitcoinbeach.com/` a spravodajstvo prispievateľa *Forbes* Francisa Pouliota a reportáže z terénu z *El Salvador in English* (`https://elsalvadorinenglish.com/`). K širšiemu salvádorskému bitcoinovému experimentu pozri Nicolás Cachanosky, Bryan Cutsinger a Alexander Salter, „Bukelenomics: Radical Policymaking and Economic Development in El Salvador“, *Journal of Private Enterprise* (2023), a priebežné spravodajstvo Human Rights Foundation na `https://hrf.org/`.

[5] Bisq a RoboSats sú decentralizované bitcoinové trhy bez KYC, ktoré prežili postupné vlny zatvárania centralizovaných p2p služieb; architektonická decentralizácia ochránila systémy tam, kde nedokázala ochrániť prevádzkovateľov centralizovaných alternatív. Bisq, `https://bisq.network/`, zdrojový kód na `https://github.com/bisq-network/bisq`. RoboSats, `https://learn.robosats.com/`, zdrojový kód na `https://github.com/RoboSats/robosats`. K historickému záznamu zatvorených centralizovaných p2p služieb vrátane LocalBitcoins (ukončenie činnosti vo februári 2023) a Paxful (odchod z regulačných dôvodov) pozri verejné oznámenia na stránkach príslušných firiem a spravodajstvo v *CoinDesk* a *Bitcoin Magazine*. K stíhaniu Tornado Cash ako susednému vzorcu rozlíšenia protokolu a prevádzkovateľa pozri obžalobu Ministerstva spravodlivosti USA na `https://www.justice.gov/usao-sdny/pr/tornado-cash-founders-charged-money-laundering-and-sanctions-violations`. Kapitola 13 rozvíja analýzu tohto vzorca z hľadiska rozlíšenia protokolu a tvorcu.

[6] Rayo (Tom Marshall), „Vonu: Mean-Time to Harassment“, *VonuLife* (1973); dotlač v *Vonu: The Search for Personal Freedom*, ed. Shane Radliff (Liberty Under Attack Publications, 2020). Rayo vynášal MTH na zvislej osi, ktorej každá jednotka predstavovala desaťnásobné zvýšenie počtu rokov neviditeľnosti, proti osi činnosti s rozpätím od letného prežitia cez celoročné prežitie, pohodlný domov, malú dielňu alebo laboratórium, malú výrobu, ľahký priemysel až po ťažký priemysel, s uhlopriečkami prevádzkovej zručnosti vo vzdialenosti jedného rádu. Jeho výslovný záver znel: „E-level [small workshop] is probably minimum for development of much of an alternative economy worthy of the name.“ Vonu patrilo do rovnakého libertariánskeho prostredia sedemdesiatych rokov ako raná agoristická a kontraekonomická myšlienka, ktorú neskôr systematizoval Samuel Edward Konkin III, a táto metrika sa čisto prekladá do kryptografických trhov: obe merajú slobodu ako veličinu času do odhalenia voči donucujúcemu pozorovateľovi a líšia sa len tým, či sa utajenie dosahuje geograficky, alebo kryptograficky.

[7] K úplnej analýze obmedzení súkromia v sieti Lightning pozri lightningprivacy.com, najmä „Routing Analysis“ a „Introduction to Lightning Privacy“. Akademické spracovania zahŕňajú Nisslmueller et al., „A Cryptoeconomic Traffic Analysis of Bitcoin's Lightning Network“ (2019), a Romiti et al., „An Empirical Analysis of Privacy in the Lightning Network“, *Financial Cryptography* (2021).

[8] K odhadom časového plánu CRQC (Cryptographically Relevant Quantum Computer, kvantový počítač schopný prelomiť šifry) pozri PostQuantum.com, „Q-Day Predictions: Anticipating the Arrival of CRQC“ a „Q-Day Revisited: RSA-2048 Broken by 2030“, obe na `https://postquantum.com`. Pozri tiež a16z crypto, „Quantum Computing and Blockchains: Matching Urgency to Actual Threats“ (2024), `https://a16zcrypto.com`. Postkvantové kryptografické štandardy NIST, najmä FIPS 203 (ML-KEM / Kyber), FIPS 204 (ML-DSA / Dilithium) a FIPS 205 (SLH-DSA / SPHINCS+), dokončené v auguste 2024, sú na `https://csrc.nist.gov/projects/post-quantum-cryptography`. HQC (Hamming Quasi-Cyclic), KEM založený na kódoch, ktorý NIST vybral v marci 2025 ako zálohu k ML-KEM založenému na mriežkach, je zdokumentovaný v NIST IR 8545 a na `https://csrc.nist.gov/projects/post-quantum-cryptography`. K širšiemu akademickému prehľadu zostáva štandardným odkazom Bernstein, Buchmann a Dahmen, eds., *Post-Quantum Cryptography* (Springer, 2009), o konštrukciách založených na mriežkach, kódoch, hašoch a viacpremenných konštrukciách.

[9] Project Eleven, „Quantum Vulnerability of Bitcoin Addresses“ (2025), `https://web.archive.org/web/20250501000000*/https://project11.xyz`, odhaduje približne 6,5 milióna BTC držaných na adresách s odhalenými verejnými kľúčmi. Pozri tiež River, „Will Quantum Computing Break Bitcoin?“ `https://river.com/learn/will-quantum-computing-break-bitcoin/`. Približne 1,9 milióna BTC je na adresách P2PK (coinbase výstupy z rokov 2009–2011) a ďalších vyše 4 milióny BTC je na adresách, ktorých verejný kľúč bol odhalený opakovaným použitím po minutí. K diskusii o postkvantovej ochrane špecifickej pre Bitcoin pozri dlhodobé vlákna v konferencii bitcoin-dev o podpisoch odolných voči kvantovým počítačom, kompatibilných s Taprootom, a návrh soft forku QuBit, ktorý vypracoval Hunter Beast a ďalší, na `https://github.com/cryptoquick/bips`.

[10] Štátna rada Číny oznámila zákaz ťažby bitcoinov v máji 2021 a presadzovanie v júni a júli 2021 vyústilo do vytlačenia približne 50–65 % celosvetového hashrate v priebehu týždňov. Hashrate siete klesol z približne 180 EH/s v máji 2021 na minimum okolo 84 EH/s v júli 2021, než sa do januára 2022 vrátil na predchádzajúcu úroveň, keď sa ťažba presunula do Spojených štátov, Kazachstanu, Ruska a Kanady. Spravodajstvo: *Cambridge Centre for Alternative Finance*, údaje o hashrate z Cambridge Bitcoin Electricity Consumption Index, `https://ccaf.io/cbnsi/cbeci`; Wolfie Zhao, „Bitcoin Hashrate Recovers to Pre-China Ban Levels“, *The Block* (január 2022); Nic Carter, „How Much of Bitcoin Mining Uses Renewable Energy?“ *CoinDesk* (2021).

[11] Úplne homomorfné šifrovanie (FHE) ako prvý dokázal za možné Craig Gentry, „A Fully Homomorphic Encryption Scheme“, dizertácia PhD, Stanford (2009), dostupné na https://crypto.stanford.edu/craig/craig-thesis.pdf. Zlepšenie efektívnosti o štyri rády, uvedené v hlavnom texte, odráža vývoj od Gentryho pôvodnej schémy založenej na mriežkach cez rad BGV, BFV, CKKS a TFHE; užitočný prehľad je Ilaria Chillotti, Nicolas Gama, Mariya Georgieva a Malika Izabachène, „TFHE: Fast Bootstrapping over the Torus“, *Journal of Cryptology* 33 (2020), https://eprint.iacr.org/2018/421. Súčasné produkčné nasadenia zahŕňajú knižnice Concrete a TFHE-rs od Zama (https://github.com/zama-ai/tfhe-rs), používané v inteligentných zmluvách s FHE v reťazci, a Intel HEXL pre hardvérovo urýchlené primitíva HE.

[12] Rámec „going dark“ pre výzvu, ktorú pre orgány činné v trestnom konaní predstavuje end-to-end šifrovanie, formálne vyjadril riaditeľ FBI James Comey pred Justičným výborom Senátu (8. júla 2015) a opakovane ho preberá vedenie FBI a Ministerstva spravodlivosti. Celosvetové nasadenie aplikácie Signal sleduje https://signal.org; k roku 2024 Signal uvádzal vyše 40 miliónov mesačných aktívnych používateľov. K debate o šifrovacej politike pozri Riana Pfefferkorn, „The ‚Going Dark‘ Problem“, Center for Internet and Society, Stanford Law School (2021), https://cyberlaw.stanford.edu/; a Susan Landau, *Listening In: Cybersecurity in an Insecure Age* (Yale University Press, 2017), ktoré zostáva technicky najpodloženejším spracovaním debaty o prístupe k odpočúvaniu.

[13] Protokol APOD (Anonymous Package on Demand) je opísaný v Ulrich Flegel, „Privacy-Respecting Intrusion Detection“ (Springer, 2007) a príbuzné návrhy sa objavujú v literatúre o anonymnom doručovaní. Lelantos je peer-to-peer systém anonymného doručovania navrhnutý v Giulia Fanti a Pramod Viswanath, „Anonymity Properties of the Bitcoin P2P Network“ (2017); variant systému doručovania prispôsobuje podobné myšlienky cibuľového smerovania fyzickej logistike. Ani jeden nedosiahol praktické nasadenie mimo výskumných prototypov. K prehľadu medzery v anonymite pri fyzickom doručovaní pozri prehľad v George Danezis a Claudia Diaz, „A Survey of Anonymous Communication Channels“, Microsoft Research Technical Report MSR-TR-2008-35 (2008), https://www.microsoft.com/en-us/research/publication/a-survey-of-anonymous-communication-channels/.