

PRAXEOLÓGIA SÚKROMIA



MAX HILLEBRAND

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 predváždať, 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 sebaovládania 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 hľadajú 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 vzdeláť za pomerne málo hodín.

Za takto prístupné informácie by som pred rokmi zaplatil drahú.

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. (Cypherpunkerí sú zástancovia súkromia a šifrovaní.) 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 zoznámí 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 vytlačujú. 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 nahraďiť.

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 voluntaristické 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 zbúrала.

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 Misesa⁴ (konanie) cez Rothbarda⁵ (vlastníctvo), Hoppeho⁶ (argumentácia) a Hayeka⁷ (problém znalostí) po Oppenheimera⁸ (pôvod štátu). Cypherpunkovú líniu tvoria May⁹ a Hughes¹⁰ s úvahami o politickom význame kryptografie, Finney¹¹ s fungujúcim kódom, Nakamoto¹² so zdravými digitálnymi peniazmi a Voskuil¹³

s axiómou odporu. Agoristické a voluntaryistické spisy, ktoré formovali sebapochopenie cypherpunkero, sa objavujú tam, kde majú váhu. Tvrdenia o súkromí, ktoré kniha obhajuje, stoja na troch právach, ktoré sú spoločným základom libertariánsko-rakúskej tradície: na sebvlastníctve 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 predností, 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.

Obsah

Ohlasy	vii
Úvodné slovo	ix
Predslov	xi
Obsah	xv
I Úvod	1
1 Podstata súkromia	3
2 Dve tradície, jeden záver	5
II Filozofické základy	7
3 Axióma konania: súkromie ako štruktúrálna vlastnosť	9
4 Axióma argumentácie a sebvlastníctvo	11
5 Axióma odporu	13
III Ekonomické základy	15
6 Informácia, vzácnosť a vlastníctvo	17
7 Teória výmeny a súkromie	19
8 Teória kapitálu a podnikanie	21
9 Teória peňazí a zdravé peniaze	23
IV Protivník	25
10 Finančné sledovanie a štátna kontrola	27
11 Firemné sledovanie a vyťažovanie údajov	29
12 Analytický stack	31
13 Kryptovojny	33
V Technická implementácia	35
14 Kryptografické základy	37
15 Dôkazy s nulovou znalosťou	39

16	Výpočty nad tajomstvami	41
17	Anonymné komunikačné siete	43
18	Bitcoin a prelom v digitálnych peniazoch	45
19	Bitcoin ako zdravé a odolné peniaze	47
20	Súkromie na Bitcoine a menové vrstvy	49
21	Decentralizovaná sociálna infraštruktúra	53
VI	Prax	55
22	Operačná bezpečnosť	57
23	Stratégia zavádzania	59
24	Dôvera a spory v paralelnej ekonomike	61
25	Budovanie paralelnej ekonomiky	63
	Prečítajte si celú knihu	65

ČASŤ I

ÚVOD

1

PODSTATA SÚKROMIA

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 cieľného 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 štruktúrálna 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 ustaluje slovník, ktorý tieto argumenty predpokladajú.

2

DVE TRADÍCIE, JEDEN ZÁVER

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 centrálného 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 dať odolné systémy postaviť a udržať proti skutočným protivníkom. Konkina kontraekonómia je most: rakúska kritika premenená na program prechodu, ktorý cypherpunkerí 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.

ČASŤ II

FILOZOFICKÉ ZÁKLADY

3

AXIÓMA KONANIA: SÚKROMIE AKO ŠTRUKTURÁLNA VLASTNOSŤ

Ludské 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.

4

AXIÓMA ARGUMENTÁCIE A SEBA-VLASTNÍCTVO

Hoppeho etika argumentácie ukazuje, že účasť v diskurze predpokladá sebvlastníctvo: kto popiera sebvlastníctvo, musí na formuláciu a vyjadrenie poprenia vykonávať výlučnú kontrolu nad telom a mysľou, čo je performatívny rozpor. Vlastnícke práva vyplývajú zo sebvlastníctva 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 sebvlastníctvo, 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 uplatňovanie 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.

5

AXIÓMA ODPORU

Axióma odporu je tretí základ: systémy možno navrhnuť 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, Bitcoinu 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*), pri chybe v implementácii, 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.

ČASŤ III

EKONOMICKÉ ZÁKLADY

6

INFORMÁCIA, VZÁCNOSŤ A VLASTNÍCTVO

Vlastnícke práva sa vzťahujú na vzácne zdroje a vzácnosť vytvára konflikty, ktoré majú vlastnícke práva riešiť. Informačný obsah je nevzácný: 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 nevzácný vzor vydaný pod licenciami, ktoré sa vzdávajú autorskoprávného 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.

7

TEÓRIA VÝMENY A SÚKROMIE

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 zruťenia do vykořisťovania slabšej strany, dôverné podmienky dovoľujú stranám usporiadať dohody, ktoré konkurenti nemôžu skopirovať, 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.

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.

8

TEÓRIA KAPITÁLU A PODNIKANIE

Infraštruktúra súkromia je kapitál v rakúskom zmysle: vyrobené výrobné prostriedky, ktoré vyžadujú obeť dnes výmenou za schopnosť zajtra. Okľukové metódy dosiahnutia súkromia, ktoré budujú kryptografické nástroje a protokoly, prekonávajú priame metódy opreté o služby 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: ostrážiti 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.

9

TEÓRIA PEŇAZÍ A ZDRAVÉ PENIAZE

Peniaze vznikajú trhovým procesom, nie vládny nariadením. Menger ukázal, že jednotlivci, ktorí chcú prekonať dvojité 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 teóremy

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.

ČASŤ IV

PROTIVNÍK

10

FINANČNÉ SLEDOVANIE A ŠTÁT- NA KONTROLA

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 zhľady 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 Zápa-

dom. 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.

11

FIREMNÉ SLEDOVANIE A VYŤAŽOVANIE ÚDAJOV

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 génóm 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 za každým, 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 ďal-

šia regulácia hrozí upevnením existujúcej sledovacej infraštruktúry cez regulačné priekopy, ktoré uprednostňujú zavedených hráčov. Analýza trhu ani neodsudzuje, ani nezavracia viny. Konštatuje, že súčasné podnety formuje intervencia rovnako ako spotrebiteľské preferencie, a že technické a podnikateľské riešenia môžu uspieť tam, kde by regulačné posilnili štruktúru, ktorú sa snažia obmedziť.

12

ANALYTICKÝ STACK

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 efektívnosť 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 útočnickovú nákladovú výhodu. Súčasťou stacku sa líšia aj dosahom a cenou: čítačka evidenčných čísel vytvára záznam pohy-

bu, zatiaľ čo komerčné spyware spôsobí úplnú kompromitáciu zariadenia, a kapitola 22 modeluje hrozby proti každej vrstve osobitne. Právna reforma 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.

13

KRYPTOVOJNY

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 uspíeva 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 kryptografic-

ké základy, ktoré táto kapitola predpokladá, a časť V skúma konkrétne implementácie, ktoré tunajšia politická a ekonomická analýza predpokladá.

ČASŤ V

TECHNICKÁ IMPLEMENTÁCIA

14

KRYPTOGRAFICKÉ ZÁKLADY

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 authority 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 kódach. 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 šifrovaného 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.

15

DÔKAZY S NULOVOU ZNALOSŤOU

Dôkazy s nulovou znalosťou oddelujú 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 veku 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 asociačným

mi 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.

16

VÝPOČTY NAD TAJOMSTVAMI

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 šifrovanými 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 mŕňania 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 viacerých 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.

17

ANONYMNÉ KOMUNIKAČNÉ SIE- TE

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, Bit-Chat, 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 odprieť konektivitu, musel odprieť všetky dostupné kanály naraz.

Protokoly aplikačnej vrstvy postupne rozširovali to, čo šifrovanie chráni. PGP šifroval obsah a všetko ostatné nechal odkryté. OTR pridal dopredné utajenie a popierateľnosť pre živý chat. Signal urobil asynchrónnu komunikáciu s dopredným 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.

18

BITCOIN A PRELOM V DIGITÁL- NYCH PENIAZOCH

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. Dôkaz práce zabrzdil útoky odopretím služby a urobil uvažovanie nákladov merateľným. Výber reťazca vyriešil usporiadanie transakcií bez centrálnej účtovnej knihy: reťazec s najväčšou nahromadenou prácou je reťazec a útočník, ktorý sa snaží prepísať nedávnú 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. Ťažiar 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: pravidiel, ktoré môže nezávisle overiť každý účastník, viažu všetkých k tej istej účtovnej knihe a žiadna jediná autori-

ta 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.

19

BITCOIN AKO ZDRAVÉ A ODOLNÉ PENIAZE

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 splňa 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 zaistujú, 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.

20

SÚKROMIE NA BITCOINE A ME- NOVÉ VRSTVY

Základná vrstva Bitcoinu je transparentná z návrhu a okolo opakovaného používania adries, heuristiky spoločného vlastníctva vstupov, odhaľovania 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, obvyčajne vyzerajúcich transakciách bez odtlačku zmiešavania v reťazci. Konštrukcia je dnes na Bitcoine prevažne teoretická a Lightning slúži ako jej mimo-reťazcový 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 výsornosť 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 šiestimi 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 šesťnásť. 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 účinnú plochu pre odopretie služby, keď spam Sprout nafúkol mempool. Sapling a Orchard tento rozdiel znížili, no neuzavreli.

Základná vrstva Ethereum 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 Ethereum ako calldata. Dôkaz s nulovou znalosťou potvrdzuje správny výpočet na transparentnej účtovnej knihe, nie súkromie na nepriehľadnej. Súkromie na Ethereum 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 vyradovaniu 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 mĺňanie 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 citelné 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 mĺňanie. Źiadna jediná vrstva neposkytuje úplné finančné súkromie: každý nástroj rieši konkrétne problémy s metadáta-mi 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.

21

DECENTRALIZOVANÁ SOCIÁLNA INFRAŠTRUKTÚRA

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 vlastne 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 jednoduchšej 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.

ČASŤ VI

PRAX

22

OPERAČNÁ BEZPEČNOSŤ

Ludské 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 prekriženie 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 protivníkov cyklus pri pozorovaní, kde je prevencia najlacnejšia. Kompartimentalizácia 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 kompartimentalizované 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.

23

STRATÉGIA ZAVÁDZANIA

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 nezobiera 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 prevádzkového prístupu. Prvým zmysluplným úspechom je obchodný okruh, ktorý súkromne zarába a mína 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.

24

DÔVERA A SPORY V PARALELNEJ EKONOMIKE

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 seriózných 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.

25

BUDOVANIE PARALELNEJ EKONOMIKY

PREČÍTAJTE SI CELÚ KNIHU

Úplná *Praxeológia súkromia* s podrobnými odvođeniami, citáciami a technickými podrobnosťami, ktoré tu sumáre iba zhŕňajú, je dostupná na adrese:

<https://towardsliberty.com/pop>

Na tejto stránke nájdete tlačené aj digitálne vydanie. Ak vás niektoré zhrnutie v tomto zväzku priviedlo k otázke, ktorú rieši samotná kapitola, práve tam sa oplatí hľadať ďalej.