

PERSONIX

zrkadlá siete
reputácie
odhalia aj
vyleštenú
biedu vnútri.

**Necenzurovatel'ná a nepodplatiteľ'ná decentralizovaná sieť reputácie
evolučný nástupca štátu**

Personix — Nekompromisná zmena

Necenzurovatelná a neskorumpovateľná decentralizovaná reputačná sieť

© 2025–2026 Pavel Kudrna, Praha

Verzia 6 (2026-05-21)

Prvý koncept jún–november 2025; prepísané apríl–máj 2026.

Vysádzané v $\text{\LaTeX}$ (Tectonic) písmami Palatino a Helvetica Neue.
A5 na šírku (210×148 mm).

Licencované pod **Creative Commons Attribution-ShareAlike 4.0 International (CC BY-SA 4.0)** — creativecommons.org/licenses/by-sa/4.0/. Vyhradené prvky, zdrojový repozitár a poznámka o produkčných nástrojoch sú uvedené na konci knihy.

Contents

Úvod	7
O čom je táto kniha?	9
Nevyhnutné predpoklady zmeny	16
Nevyhnutné predpoklady zmeny	16
Nástroj	25
Reputačná sociálna sieť	25
Prečo je sieť necenzurovateľná	49
Odpovede na zjavné pochybnosti	51
Závislosť od technológie	51
Nehádzem zverejňovaním v sieti peniaze z okna?	51
Čo ak si niekto vytvorí viacero identít?	53
Nemôže si bohatý človek jednoducho „kúpiť“ viac identít (alebo vytvoriť virtuálne komu- nity)?	56
Čo s prispôsobivcami, ktorí chcú len čítať a komunite nedať nič?	59
Finančná neutralita	60

Dobrovoľnosť, zodpovednosť a sloboda	62
Prepínač sloboda–totalita (a delegovanie)	63
Problém orákula — most medzi digitálnym a fyzickým svetom	69
Ako funguje overovanie	73
Konsenzus a proces overovania	73
Roles in the verification transaction and authorities	79
Prehľad rolí	79
Vydavateľ	80
Autorita	81
Overovateľ	85
Subjekt	87
Pozorovateľ	90
Mechanizmus: časová pečiatka a výzvodový kód	90
Pointa: nepotrebuješ skutočných pozorovateľov	92
Delegovanie	92
Komunikácia medzi rolami	98
Emergentná spoločenská zmluva — politika	98
Poskytovanie informácií o sebe	102

Zločin a trest	103
Zločin a trest	103
Sleduj peniaze	114
Sleduj stopu peňazí	114
Slabé miesto štátu — peniaze	114
Proposed transition to the state's successor	116
Evolúcia, nie revolúcia	116
Štyri nástroje, ktoré sa navzájom podopierajú	118
Jednoduchý daňový systém — vstupná návnada	119
Elektronická evidencia výdavkov (ESR)	119
Občianska alokácia daní — váha rozhodnutia	121
Vyjednávacía platforma so štátom — páka	125
Občianstvo bez občianskeho preukazu	127
Prekryv a zvratnosť	130
Záver	133
Cesta existuje	133
Poďakovanie	135
Inšpirácia	135

Recenzia a spätná väzba	135
Nástroje	135
Slovníček pojmov	138
Slovníček pojmov	138

Úvod

Máš pocit, že sa môžeš spoľahnúť na štát?

Odmietam sa zmieriť s tým, keď sa mne, mojej rodine alebo niekomu v mojej komunite stane zjavná krivda (fyzická ujma, podvod, neprimerané obmedzenie, ...) a štát odpovie: áno, je to krivda, ale nič s tým nerob, inak budeš mať s nami ešte väčší problém. Taký stav je chorý a ľudia, ktorí sa mu prispôsobujú, sú spoluvinníci.

Výsledkom je vzájomné odcudzenie, hra na komunitu, hra na štátnosť a prehlbujúci sa rozklad spoločnosti s prísľubom vážnych konfliktov, ktoré nás čakajú.

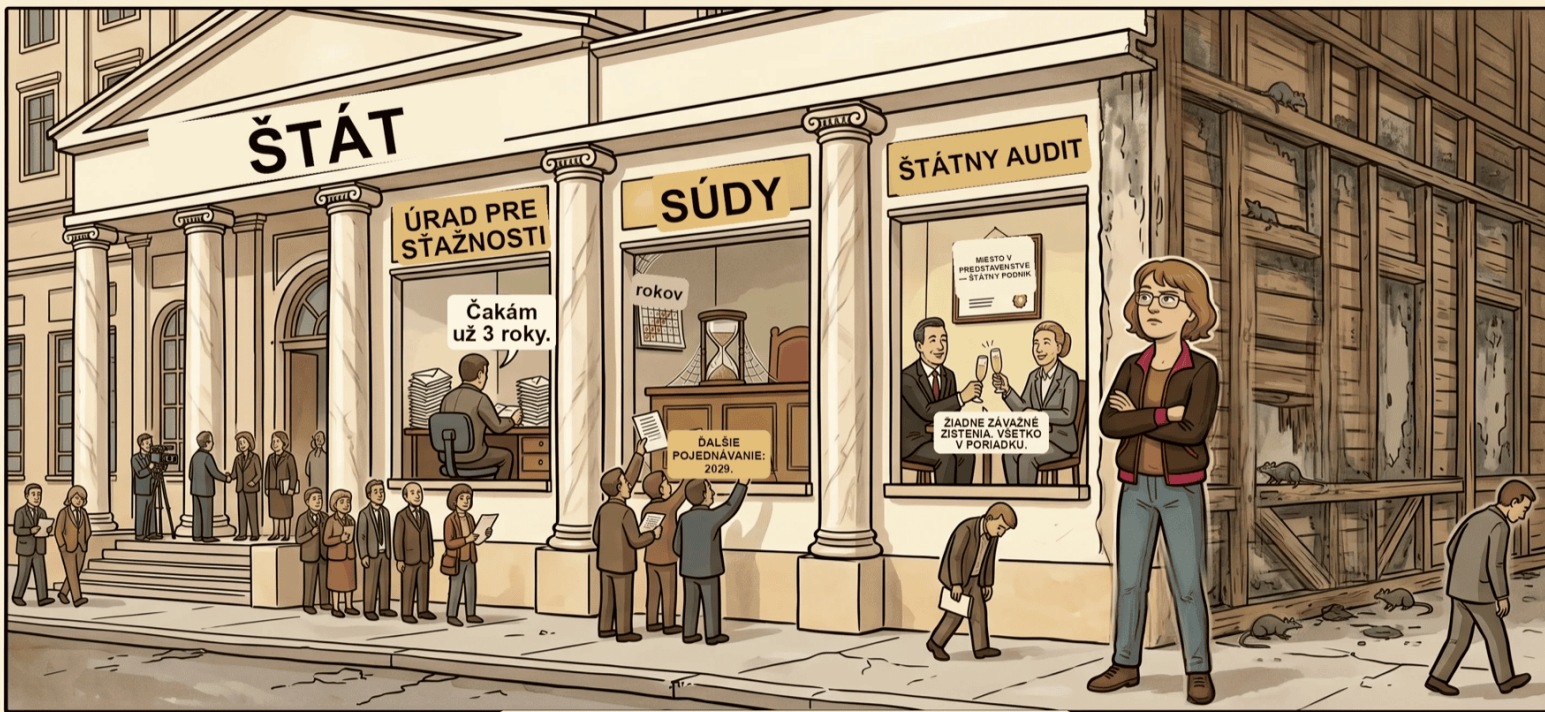
Dokáže štát držať krok s tempom technologických a spoločenských zmien, alebo radšej plesne zákaz?

Mohol by som predstierať, že stagnáciu, neschopnosť a korupciu budem brať ako deklarovанú stabilitu právneho štátu a tradície, ale už nechcem. Klamal by som sám seba a klamal by som teba.

Cítiš povýšenectvo úradníkov a volených zástupcov, keď sa opovážiš skritizovať niečo, za čo platíš?

Odmietam považovať ľudí v spoločnosti za nehodných spoluutvárať celospoločenské pravidlá len preto, že nevynikajú v mäkkých zručnostiach, ktoré sú dnes jediným postačujúcim predpokladom na to, aby sa človek stal voleným zástupcom v štáte kodifikovaných inštitúciách. Verím, že drvivá väčšina sa dokáže postarať o seba, o svojich blízkych a o svoju komunitu — a že v tom vidí kus svojej životnej filozofie. Väčšina ľudí, ktorých som okolo seba spoznal, je takáto.

Ale stretol som aj vyslovených hajzlov, ktorí boli hajzlami práve preto, že vedeli hrať tú hru — hru, v ktorej komunita nesmie dostať možnosť dať im spätnú väzbu, v ktorej ich štát chráni, aby nikto nerušil



Odmietam sa s tým zmieriť'.

poriadok, ktorý by ohrozil samotnú podstatu štátu: zabezpečiť ľahký život tým na horných poschodiach mocenskej hierarchie a hierarchie jeho inštitúcií. Feudalizmus vystriedala vláda populistov a elitárov.

Miluješ, keď ti iní hovoria, ako máš žiť svoj život?

Neprijímam súčasný stav vecí ako dokonalú, konečnú danosť. Musím byť zodpovedný v tom, ako sa správam, no som citlivý, keď mi niekto hovorí, aké správne hodnoty mám zastávať. Čo ty?

O čom je táto kniha?

Predstav si reputačnú sociálnu sieť, kde si každý, kto chce, môže vytvoriť vlastné kľúče (vytvoriť si svoju identitu), nechať sa pozvať členmi svojej komunity alebo sa do nej odvážiť sám. Buduješ si reputáciu a čerpáš užitočné reputačné dáta o iných, keď to potrebuješ. Keď sa stane krivda, hľadáš podporu svojej komunity — predložíš svoj prípad a poskytneš, čo k veci máš, a komunita sa na to pozrie, na základe relevancie rozhodne, či to posunie ďalej, a ako previnilca sankcionovať.

Celá táto krátka kniha je o tom, čo musí byť pod kapotou, aby to zvonka fungovalo takto jednoducho. Ak pri nej vydržíš, sľubujem ti, že svet, ktorý sa teraz v mnohom môže zdať zložitý a ťažko pochopiteľný, sa otvorí ako zrozumiteľnejší a jasnejší. Uvidíš, že mnoho zlých vecí sa dá nastaviť tak, aby sa zlým aktérom už tak nespravodlivo neoplácali. A nie je to nástroj, na ktorom by si musel byť neustále nalepený online — stačí siahnuť po ňom vtedy, keď cítiš, že to potrebuješ.

Ďalej ti sľubujem, že usporiadanie opísané tu bude bližšie skutočným motiváciám ľudí a že ich nepotrebuje pretvárať v mene nejakého -izmu.

A napokon ukážeme, ako zvládnuť nerevolučný prechod do stavu, v ktorom sa komunity opäť stanú plne funkčnými sociálnymi jednotkami a nemusia už len predstierať.

■ Odborný článok

Táto kniha je vysvetľujúcim sprievodcom k pôvodnému odbornému článku „*Decentralized Reputation Network: A Framework for Voluntary and Uncorruptible Societal Organization*“ (Pavel Kudrna, 2026). Ak ťa zaujíma formálny opis architektúry, algoritmus výberu overovateľa a zdôvodnenie ekonomických mechanizmov, odporúčam začať tam.

■ Kapitoly na seba nadväzujú

Kniha je napísaná ako súvislá argumentácia — každá kapitola stavia na predchádzajúcej. Pojmy zavedené v jednej časti sa používajú v ďalších častiach, aj v poznámkach pod čiarou. Neodporúčam čítať mimo poradia.

■ Pre koho je táto kniha?

Napriek vizuálne prívetivému formátu je hlavnou cieľovou skupinou skôr odbornejší čitateľ, ktorého zaujímajú princípy možných spoločensko-ekonomicko-politických usporiadaní ľudskej spoločnosti. Dostať sa do bodu, kde by som celú látku vedel prístupne vysvetliť najširšej verejnosti, si ešte vyžaduje dlhú cestu vybudovania plnej komunikačnej stratégie.

Vítam podnety, ako toto dielko či prípadné nadväzujúce revidované vydania spraviť zrozumiteľnejšími.

Varovanie

Neviem, kto si, koľko máš rokov ani koľko porušených sľubov si si v živote musel vypočuť. S ich dávaním som tu skončil. Namiesto toho ťa chcem varovať, že jediným výsledkom toho, čo sa tu dozvieš, môže byť poznanie, že cesta, na ktorej za teba niekto iný upratuje dnešný neporiadok, pravdepodobne neexistuje. Opisujem len rámec/nástroj, ktorý by mohol to upratovanie spraviť jednoduchším a prehľadnejším. Na jeho základe sa pokúsím pripraviť spoločenský experiment/simuláciu, opraviť prípadné chyby, alebo myšlienku úplne pochovať, ak sa ukáže, že má zásadné konštrukčné trhliny.

Prosba

Hlboko by som ocenil, keby si aj po dočítaní tejto knihy ostal otvorený voči tej myšlienke a sledoval, kam sa uberá a ako obstojí pod vecnou kritikou. Ešte viac by som ocenil tvoje neskoršie zapojenie — pokus rozbiť navrhované rovnovážne princípy vlastnými nápadmi, a tým lepšie otestovať, ako je systém pripravený na reálne ľudské správanie.



Pod kapotou je toho viac. Zostaň so mnou.

Bez teba a tvojho zapojenia ostáva myšlienka teórie v zásuvke. Bez teba a tvojich príspevkov a finančných darov nedokážeme posunúť projekt k reálnemu spoločenskému experimentu, a teda k reálnej pripravenosti. Bez teba a tvojej vecnej kritiky budeme stagnovať tam, kde sme teraz, alebo sa necháme pohltiť svätým grálom centristov — absolútnou, nezvratnou totalitou. Je na nás, ktorú cestu si zvolíme, alebo presedíme.

Výzva

Nekladieme ti na plecía práve ľahké bremeno. Náklady márnوترatne spravovanej spoločnosti už teraz nesieš cez okultisticko-zaklínacie manuály tvrdiace, že spoločnosť sa najlepšie riadi centrálne — a ja mám tú drzosť žiadať od teba ešte viac a ísť proti týmto tendenciám. Som si vedomý, že budeme musieť ustáť zrútenie najväčšej pyramídovej hry v dejinách — priebežného dôchodkového systému — bez toho, aby sme nechali niekoľko generácií hladovať.

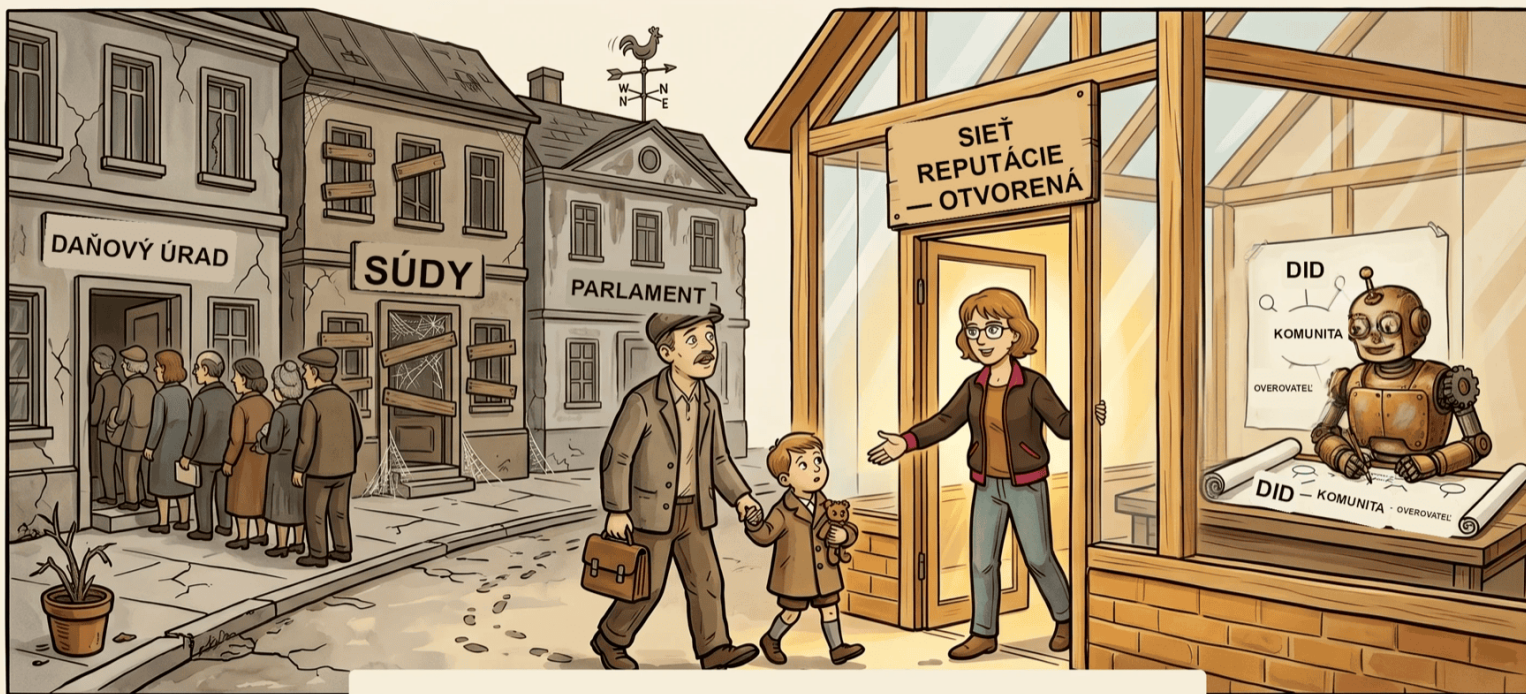
Napriek tomu ťa prosím: odovzdajme konečne našim deťom lepší svet a zanechajme po sebe odkaz, že sme tú zmenu dotiahli. Uvoľnenie ekonomického rastu by mohlo byť čiastočným riešením ťažkostí, ktoré sú na obzore. Potom môžeme svojim potomkom povedať, že to bola poriadna jazda a nebola zbytočná.

Problém

Len sloboda vyvážená priamou zodpovednosťou dokáže naozaj odomknúť obrovský potenciál, aký svet ešte nevidel.



Lepší svet za tú váhu stojí.



Pod'ťe d'alej. Plány sú rozložené.

Nevyhnutné predpoklady zmeny

Nevyhnutné predpoklady zmeny

Základným predpokladom zmeny k lepšiemu je, aby sa z podriadeného stal nadriadený — alebo aspoň rovnocenný partner. To znamená prevziať tie najkritickejšie agendy, ktoré vymedzujú vzťah nadradenosti a podriadenosti. Tieto agendy stoja na dôkazoch príslušnosti ku komunitám, ktoré tvoria občanov štátu. Sú to informácie a ich overiteľnosť autoritou s podstatnou reputáciou v rámci týchto komunít.

Aby som prekonal súčasný systém, dospel som k piatim predpokladom, ktoré potom vysvetlím tak, ako im rozumiem. Tieto predpoklady si môžeme predstaviť ako piliere, ktoré nesú konštrukciu systému opísaného vo zvyšku knihy. Pilieri som si najprv vybral podľa vlastnej preferencie a pri uvažovaní o nich som postupne dobrušoval, ako každému z nich rozumiem, do podoby nižšie.

Prejdime týchto päť pilierov jeden po druhom.

Dobrovoľnosť

V našom prípade dobrovoľnosť znamená, že nie som nútený zúčastňovať sa na prevádzke decentralizovanej reputačnej siete. Nemôžem si však nárokovať pozitívne formulované právo, aby o mne sieť nevedla informácie — či sa informácia o mne v reputačnej sieti ocitne, závisí len odo mňa, od môjho správania, mojich činov a mojej zodpovednosti.

PREDPOKLADY ZMENY



Bez týchto piatich pilierov je každá zmena len márnením času.



Dobrovoľné — kým t'a nedobehne zodpovednosť.

■ Organizácia

Jednotlivec systém nerozbije, a preto štát kontroluje združovanie ľudí ako spôsob, ako predchádzať aktivitám, ktoré by mohli ohroziť jeho štruktúru a fungovanie. Nezáleží na tom, či sa ľudia organizujú za, alebo proti. Prostredníctvom organizácie možno zmierniť dopad exemplárnych trestov vtedy, keď sa niekto opováži meniť štát proti jeho vôli.

Nestanovujme si spoločné ciele, ale časť cesty môžeme prejsť spolu. Najprirodzenejšou formou je združovanie v komunitách — tie však musia mať všetky nástroje, ktoré potrebujú, aby neostali len hrou na komunity.

■ Odolnosť

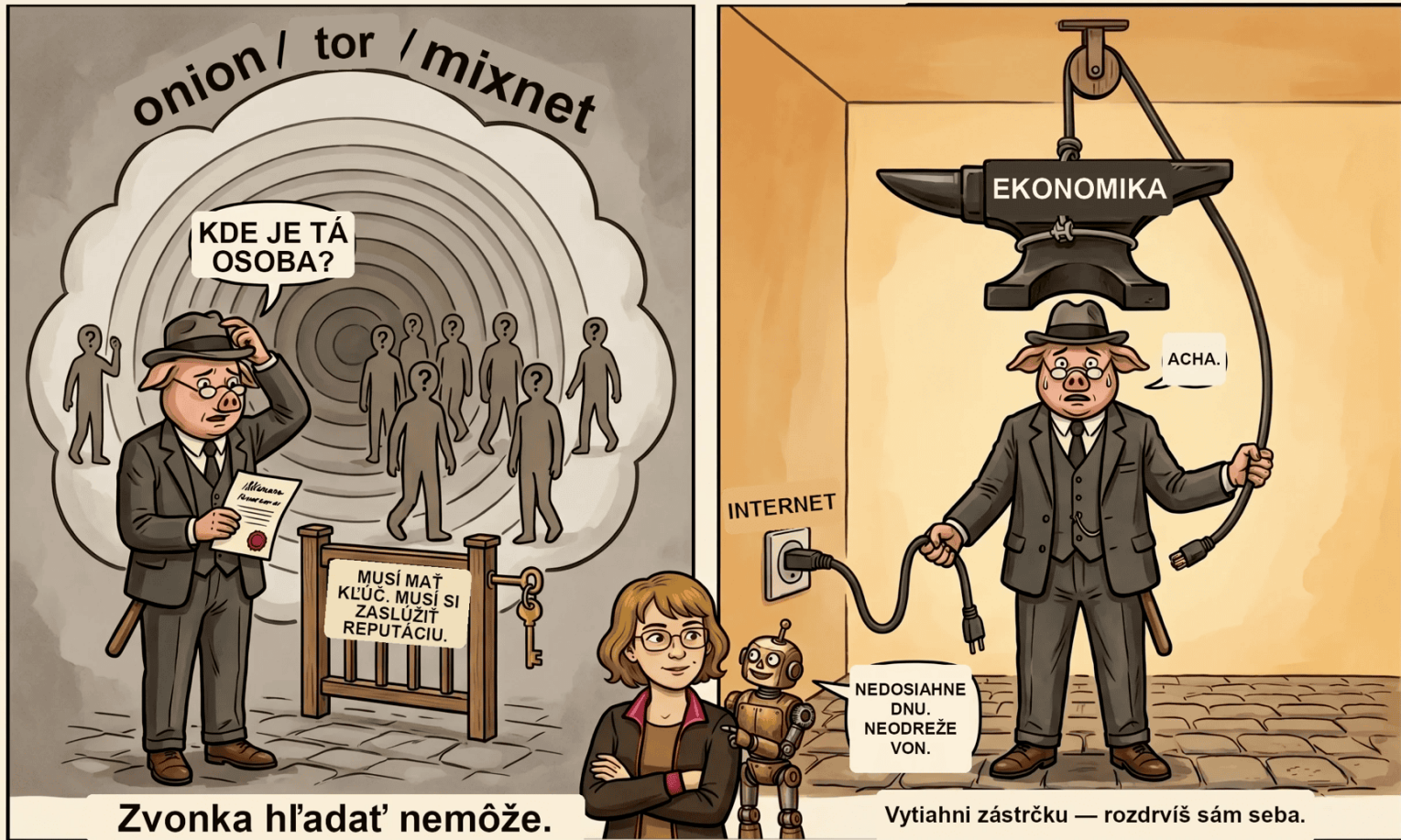
Zvolená cesta k zmene štátu — alebo k prechodu na jeho nástupcu — nesmie závisieť od povolenia štátu. Nástroje a spôsoby ich používania musia byť čo najviac necenzurovateľné. Jednoducho povedané, cena ich cenzurovania musí byť astronomická. Bez toho je celé úsilie len pálením času a životnej energie.

PREDPOKLAD 2 z 5: ORGANIZÁCIA



Jednotlivec systém nezlomí. Komunita áno.

PREDPOKLAD 3 z 5: ODOLNOSŤ



NIET KOHO ŽIADAŤ O POVOLENIE. NIET ZÁSTRČKY, ČO VYTIAHNUŤ.

■ Konsenzus

Navrhované riešenie musí už svojou podstatou obsahovať mechanizmus vyjednávania konsenzu, ako aj represívnu zložku pre prípady, keď je konsenzus porušený. Nemusí ísť o dobrovoľnú dohodu typu win-win. Stačí, ak okolnosti a spoločenský tlak zabezpečia kompromis naprieč komunitou a medzi komunitami.

■ Neskorumpovateľnosť

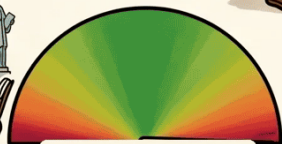
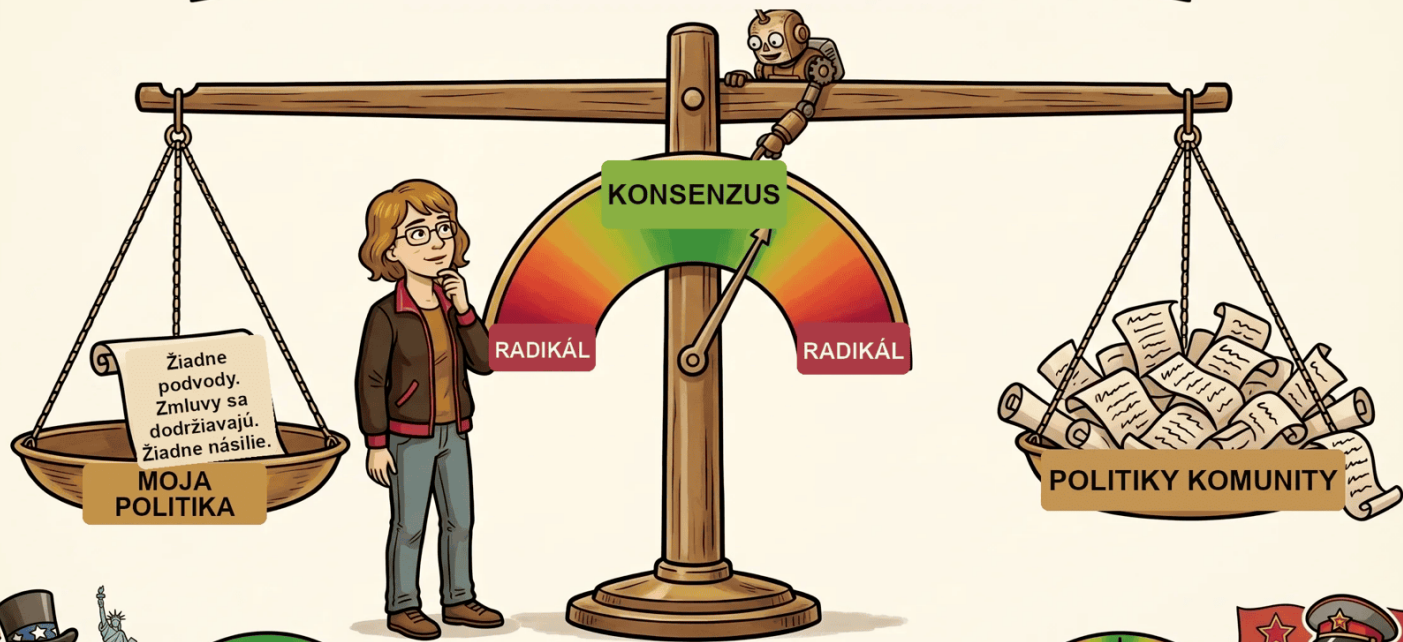
Necenzurovateľnosť bráni systém zvonka. Ale sieť ľudí môže hniť aj zvnútra — autorita sa nechá ovládnuť, deklarované pravidlo sa potichu opustí, účastníci sa v tichosti podplatia. Necenzurovateľnosť by bola dutým víťazstvom, keby sa ľudia vnútri dali skorumpovať bez následkov.

Neskorumpovateľnosť nie je výsledkom jediného šikovného triku. Vzniká z toho, že **niekoľko princípov navrhovaného dizajnu pôsobí súčinne** — tlak proti korupcii je rozložený naprieč architektúrou a jednotlivé časti sa navzájom posilňujú. Ako presne sa to dosahuje, ukážeme postupne — pri opise nástroja, pri overovaní a v kapitole o treste. Na konci zrekapitulujeme všetko, čo bolo vybudované.

Neskorumpovateľnosť je zároveň predpokladom dizajnu aj emergentnou vlastnosťou výsledku. Je to druhá obranná línia — tá obrátená dovnútra — a bez nej je Odolnosť len polovicou štítu.

ZOSTAŇ V ROZPÄTÍ — NIE SI RADIKÁL.

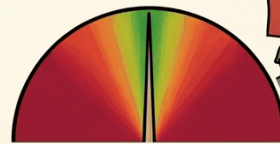
Môžeš sa líšiť. Len nie príliš.



SLOBODNÁ
SPOLOČNOSŤ

Pásmo tolerancie sa roztáhuje
so slobodou danej kultúry.

PREDPOKLAD 4 z 5: KONSENZUS



AUTORITÁRSKA
SPOLOČNOSŤ

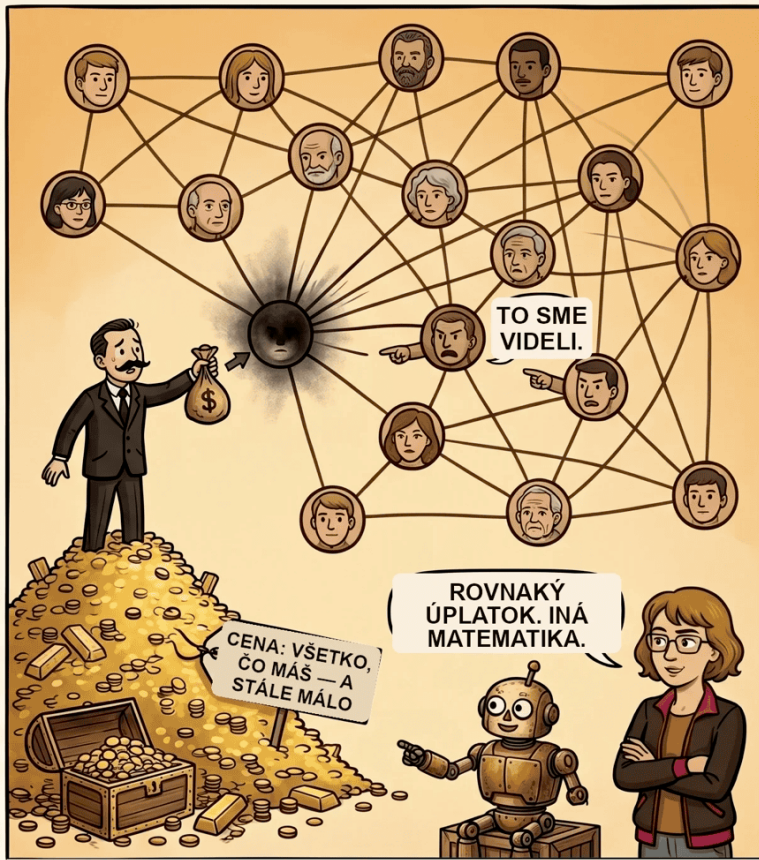


KONSENZUS JE PÁSMO TOLERANCIE, NIE JEDNOMYSELNÁ ZHODA.

PREDPOKLAD 5 z 5: NEPODPLATITEĽNOSŤ



Podplatiť pár horných poschodí — základňa aj tak zaplatí.



Podplatiť jedného — navždy stratí reputáciu. Podplatiť všetkých — skracuješ prvý.

KORUPCIA MÁ CENU. V SIETI JE PRÍLIŠ VYSOKÁ.

Nástroj

Reputačná sociálna sieť

Na dosiahnutie zmeny potrebujeme starostlivo navrhnutý nástroj. Najprv ho stručne načrtneme; v neskorších kapitolách si každú časť rozoberieme podrobnejšie a niečo pridáme. Predstav si necenzurovateľnú, globálnu, decentralizovanú sociálnu sieť, kde by si mohol bezpečne vytvárať a spravovať svoju zastupiteľskú identitu — takzvanú decentralizovanú identitu (DID). DID je digitálna identita, ktorú si vytváraš a ovládaš sám, bez závislosti od akejkoľvek centrálnej autority. Nikto ti ju nemôže vziať ani sfaľšovať, pretože je kryptograficky podpísaná tvojím súkromným kľúčom (alebo kľúčmi, cez multisig).

Poznámka

Jedným z dôsledkov je, že taká identita by mohla postupne nahradiť štátom vydávané doklady totožnosti — ale o tom viac v kapitole o prechode.

V takej sieti by si mohol prostredníctvom svojej identity nahlásiť, že ti niekto spôsobil ujmu (a neskôr prípadne, že ju napravil alebo bol k tomu donútený). Aby táto spätná väzba — namierená na pôvodcu ujmy — mala hodnotu ako relevantný zdroj, musí vkladanie informácie do siete stáť čas, energiu a peniaze — a navyše sa pre ostatných musí vyprodukovať overiteľný dôkaz, že nejde o prázdne táranie.

TVOJA IDENTITA, TVOJE KLÚČE, TVOJE PRAVIDLÁ

VYTVORÍŠ SI JU SÁM

SÚKROMNÝ KLÚČ — podpisuje
v tvojom mene. Držíš ho len ty.
Nikdy ho nezdieľaj.

VEREJNÝ KLÚČ —
overuje tvoje podpisy.
Viditeľný pre sieť.

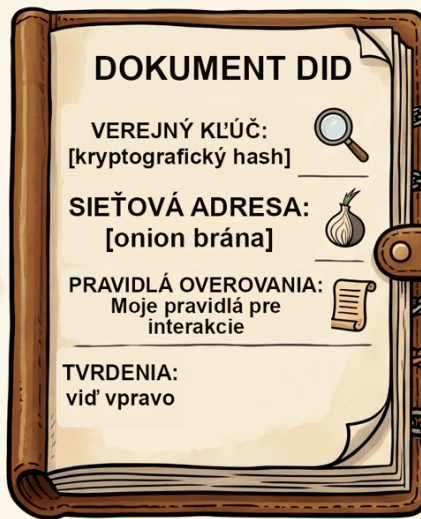


Žiadny registračný úrad.
Žiadny štátny formulár.
Žiadne schválenie
firmou. Vygeneruješ si
to sám.



ŠTÁTNY DOKLAD —
ODVOLATEĽNÝ: štát ho môže
kedykoľvek zrušiť.

TVOJ DOKUMENT DID



Toto je tvoja verejná
identita. Prečítať si ju
môže ktokoľvek. Zmeny
v nej môže podpísať len
TVOJ súkromný kľúč.



Toto nemôže
odvolať žiadny
štát.



DID — NEODVOLATEĽNÝ: zmeny
môže podpísať len tvoj súkromný
kľúč.

TVRDENIA — OVERENÉ FAKTY O TEBE

OBČIANSTVO: Česká
republika — overené
Obecným notárom

VZDELANIE: Mgr. informatika
— overené Siet'ou
absolventov univerzity

MAJETOK: Vlastník bytu
č. 42 — overené Miestnym
komunitným registrom

PASÍVNÝ SVEDOK:
Prehliadol krivdu — pravidlo
nedodržané — podané
Susedskými svedkami

PODVOĐ: Pripravil
suseda o úspory —
podané Miestnym
komunitným súdom

Tvrdenia sú overené výroky.
Tie dobré aj zlé. Autority za
ne ručia svojou reputáciou.

Tvoja identita. Tvoje kľúče. Tvoje pravidlá. Netreba povolenie.

Čítanie informácií by bolo ľahké a pomerne lacné, ale vytvorenie jednotlivého záznamu by bolo nákladné a náročné. Zápis by sa riadil jasným protokolom, v ktorom výpočet podľa zvoleného algoritmu striktné určuje, ktorý DID požiadať o overenie predloženej informácie a ako postupovať tak, aby vybraný účastník spracoval informáciu v tvojom mene, zverejnil ju a stal sa jej overovateľom.

Algoritmus vs radikalizmus

Algoritmický výber overovateľov zabezpečuje, že neradikálni vydavatelia informácií si v čase udržia takmer neutrálnu rovnováhu medzi nákladmi na zverejnené informácie a odmenami za overovanie.

ZVEREJNENIE STOJÍ ČAS, ENERGIU A PENIAZE

ZÁPIS DO SIETE NIKDY NIE JE ZADARMO — ČÍTANIE ÁNO

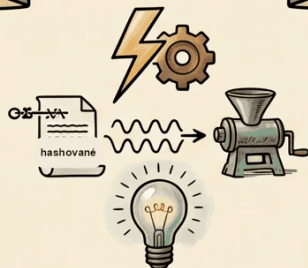
TRI KANÁLY — VŠETKY TRI SÚ REÁLNE

ČAS



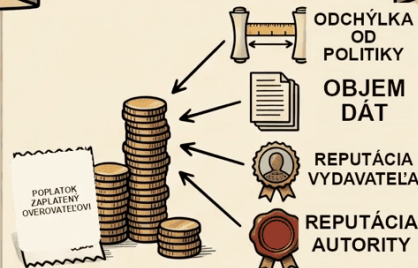
čakáš, kým algoritmus vyberie overovateľa a overovateľ prečíta tvoj záznam.

ENERGIA



podpisovanie, hashovanie, overovanie — každý krok je reálny výpočet a reálna elektrina.

PENIAZE



čím ďalej tvoje tvrdenie leží od politiky overovateľa, čím väčší záznam a čím menej dôveryhodný vydavateľ či jeho autorita — tým vyšší poplatok.

ČO SA STANE POTOM

- Trojková overovacia reťaz — vid' AKO ALGORITMUS VYBERÁ OVEROVATEĽA, AKO OVEROVATEĽ ODPOVEDÁ, VYDAVATEĽOVA VOĽBA
- Prečo drahý zápis chráni reputáciu — neskôr v tejto kapitole

šum je drahý. Signál (je cenný. Preto si sieť účtuje za zápis, nie za čítanie.

náklad naprieč iteráciami

KAŽDÝ ĎALŠÍ POKUS STOJÍ VIAC

odpoveď overovateľa sa vloží do chronológie — vid' VYDAVATEĽOVA VOĽBA a AKO ALGORITMUS VYBERÁ OVEROVATEĽA



každé zamietnutie či nové hodenie pridá do chronológie, ktorú algoritmus pohltní — a ďalší pokus je drahší vo všetkých troch kanáloch.

asymetria čítania

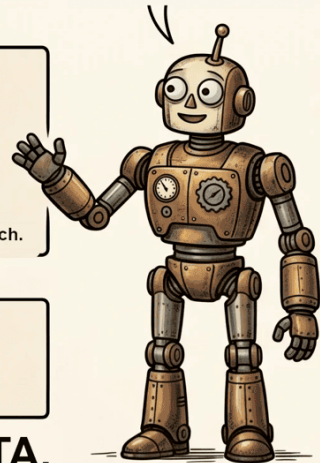
ČÍTANIE JE LACNÉ



dotaz zadarmo

reputáciu aj záznamy si môže prečítať ktokoľvek — platí sa len za zápis. Tá asymetria je zámer.

ZÁPIS STOJÍ — ČÍTANIE NIE. TÁ ASYMETRIA JE PODSTATA.



Pozrime sa, ako algoritmus vyberá overovateľa.

■ Algoritmus

Algoritmický výber nedeterministicky volí pre rôzne informácie iného overovateľa (alebo množinu možných overovateľov). Hash (jednosmerná matematická funkcia, ktorá z ľubovoľného vstupu vyrobí jedinečný „odtlačok“ — ako odtlačok prsta dokumentu) kompletného DID dokumentu určuje pozíciu na konzistentnom hash ringu a vyberá kandidátov na overovateľa.

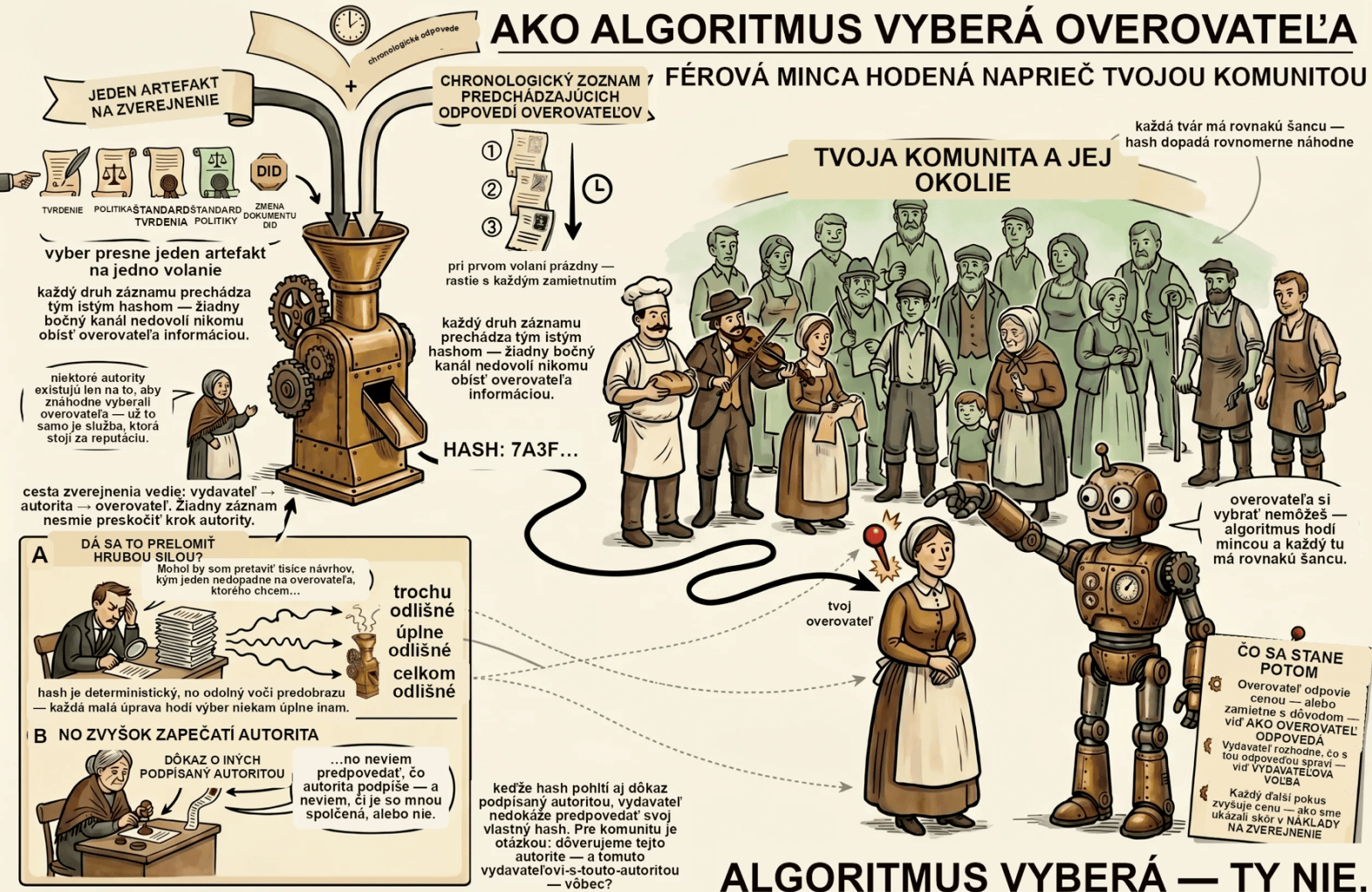
$$\text{verifier_DID} = \text{hash}(\text{DID_document})$$

Jednoducho povedané: algoritmus vezme celý tvoj DID dokument, vypočíta z neho odtlačok a ten odtlačok určí tvojho overovateľa.

Pri prvom overovateľovi, ktorého algoritmus vyberie, nemusíš ako vydavateľ uspieť — tvoja reputácia alebo deklarované nastavenia nemusia spĺňať jeho požiadavky. Algoritmicky by si pokračoval v hľadaní ďalšieho vykonaním ďalšej rekurzívnej iterácie, ktorá ti priradí ďalšieho overovateľa. S každým krokom rastie „vzdialenosť“ k cieľovému overovateľovi a spolu s ňou aj sprievodné metadáta, ktoré treba zverejniť. Ako dáta rastú, prirodzene stúpajú náklady (nielen pre počiatočnú veľkosť tvrdenia, ale aj pre metadáta hromadiace sa pri každom zamietnutí). Dôveryhodná informácia prejde oveľa ľahšie ako nezmyselné rozmary. Je na každom, akú vysokú cenu je ochotný niesť a nakoľko mu na zázname záleží — radikalizmus sa zaručene predraží.

AKO ALGORITMUS VYBERÁ OVEROVATEĽA

FÉROVÁ MINCA HODENÁ NAPRIEČ TVOJOU KOMUNITOU



AKO OVEROVATEĽ ODPOVEDÁ

PRIJME S CENOU — ALEBO ZAMIEETNE S DÔVODOM

overovateľ pred
odpoveďou zváži štyri
veci.



ZAMIEETNUŤ — S DÔVODOM



- reputácia vydavateľa je pre mňa príliš nízka
- autorite za týmto záznamom nedôverujem
- politika vydavateľa je príliš vzdialená od mojej, aby sa dala premostiť
- samotný dokument neprejde pravidlami mojej politiky

overovateľ napíše PREČO — jeho odpoveď vstupuje späť do ďalšieho pokusu.

PRIJAŤ — S CENOU



overovateľ súhlasí so zverejnením — no cena odráža, ako ďaleko tvrdenie leží od jeho politiky, koľko dát nesie a nakoľko je vydavateľ dôveryhodný.

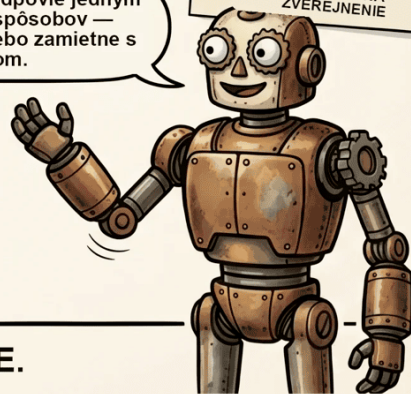
odpoveď overovateľa sa pridá do chronologického zoznamu — ako sme ukázali v AKO ALGORITMUS VYBERÁ OVEROVATEĽA

nech overovateľ povie čokoľvek, jeho odpoveď sa stáva vstupom do ďalšieho volania.

každý overovateľ odpovie jedným z týchto dvoch spôsobov — prijme s cenou, alebo zamietne s dôvodom.

ČO SA STANE POTOM

- Vydavateľ rozhodne, čo s touto odpoveďou spraví — vid' VYDAVATEĽOVA VOĽBA
- Každá odpoveď posúva cenu ďalšieho pokusu — ako sme ukázali skôr v NAKLADY NA ZVEREJNENIE



OVEROVATEĽ BUĎ STANOVÍ CENU — ALEBO TI POVIE, PREČO NIE.

Nech overovateľ rozhodne v odpovedi na tvoju žiadosť o overenie akokoľvek, lopta je späť na strane vydavateľa: môže prijať overovateľovu ponuku overovacích služieb, zapracovať odpoveď do chronológie a skúsiť to znovu (drahšie), alebo odísť a preglgnúť utopené náklady.

Aby si svojej informácii dodal väčšiu váhu a lepšiu šancu na prijatie u overovateľov, mohol by si ako vydavateľ so záujmom o vydávanú informáciu využiť služby **dôveryhodnej autority**. Autorita predloženú informáciu buď zamietne, alebo prijme a vsadí na ňu svoje dobré meno (reputáciu). Autorita si typicky vyžiada dôkazy z reálneho sveta, overí ich a klasifikuje. Výstupom je protokol jej posúdenia daného prípadu v danom čase. Predstav si autoritu ako špecialistu na určitý druh služby v reálnom aj digitálnom svete — napríklad vyšetrovateľa, audítora, poisťovateľa, dodávateľa určitej triedy tovaru (v podstate ktoréhokoľvek ekonomického aktéra na trhu).

YDAVATEĽOVA VOĽBA

ČO SPRAVIŤ S ODPOVEĎOU OVEROVATEĽA

nech overovateľ povedal
čokoľvek, vydavateľ má teraz
na stole JEDNU odpoveď.



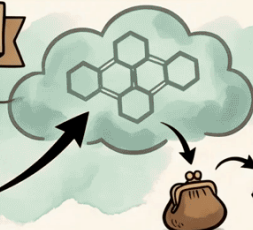
späť na AKO ALGORITMUS VYBERÁ
OVEROVATEĽA — ukázané skôr

cyklí len cesta opakovania — prijatie aj odchod príbeh ukončia.

TRI CESTY VON

PRIJAŤ PONUKU

sieť DID



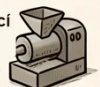
LEN AK
BOLO
PRIJATÉ

vydavateľ zaplatí poplatok — záznam sa zverejní
do siete. Dostupné len ak overovateľ prijal.

SKÚSIŤ ZNOVA



malý pretavovací
stroj



každý nový
pokus stojí
viac

odpoveď sa pribalí do chronológie — algoritmus hodí znova. Funguje, či už
overovateľ prijal za cenu, ktorá sa vydavateľovi nepáči, alebo rovno zamietol.

ODÍŠŤ



už vynaložený
čas a energia
sa nevrátia

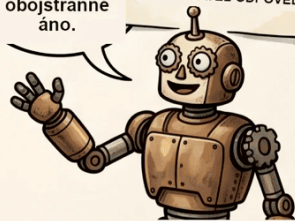


vydavateľ zahodí návrh. Nič sa nezverejní
— no ani nič ďalšie sa nezaplatí.

overovateľ
rozhoduje ako
— vydavateľ
rozhoduje či.
Zverejnenie je
obojstranné
áno.

ČO SA STANE
POTOM

{ Každý ďalší pokus posúva
cenu nasledujúceho — ako
sme ukázali skôr v
NÁKLADY NA ZVEREJNENIE
Samotná odpoveď
overovateľa — ako sme
ukázali skôr v AKO
OVEROVATEĽ ODPOVEDÁ

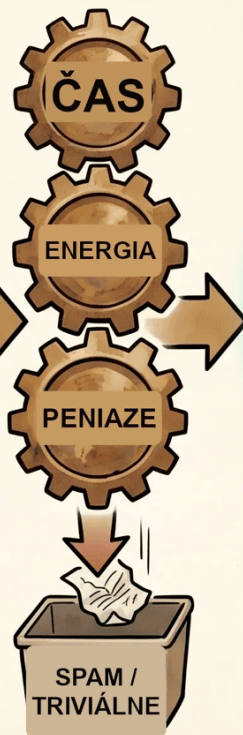


OVEROVATEĽ NAVRHUJE — VYDAVATEĽ ROZHODUJE.

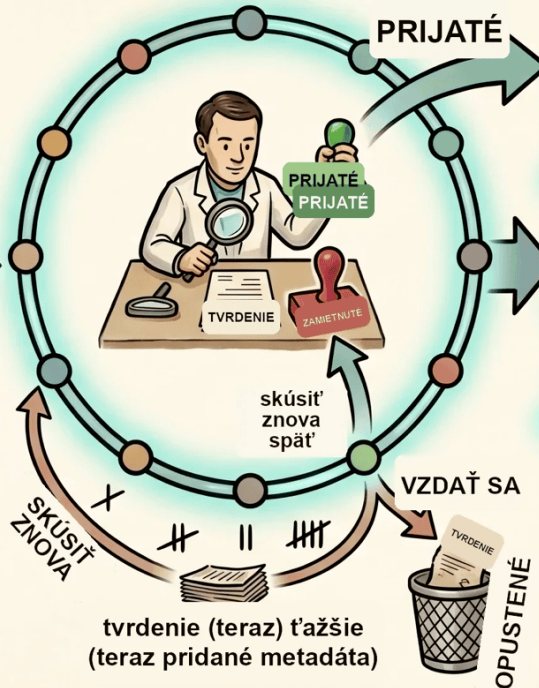
FÁZA 1 — ZVEREJNI TVRDENIE



FÁZA 2 — FILTER KVALITY



FÁZA 3 — REKURZÍVNE OVEROVANIE



FÁZA 4 — TRVALÝ ZÁZNAM



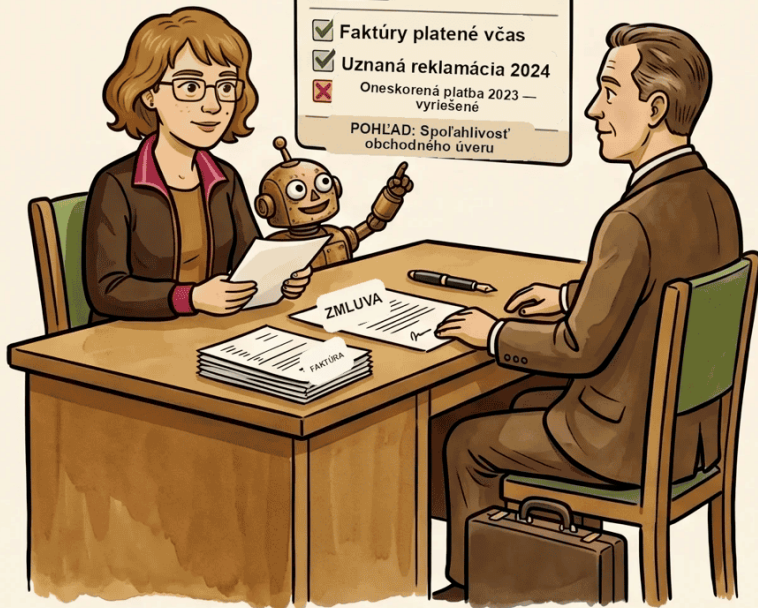
Trvalé.
Overiteľné.
Verejné.

DRAHÉ SFALŠOVAŤ. LACNÉ OVERIŤ.

Kým sa pokúsiš zverejniť informáciu do siete, tá už pravdepodobne bude obsahovať informácie o svojich aktéroch — to sú reputačné signály. Zorientovať sa v tom, ako čítať reputačné signály — čo pre teba znamenajú v rôznych situáciách a aké riziká nesú — nemusí byť triviálne. Každý účastník sa môže na reputačné záznamy pozeráť cez svoj DID inak, podľa situácie, ktorú rieši voči protistrane. Je protistrana spoľahlivý platca, alebo si mám pri obchode vypýtať peniaze vopred? Nesie ponúkaný produkt recenzie o skrytom podvode alebo vadách? Snaží sa vykrútiť zo zmluvnej zodpovednosti, keď sa niečo pokazí? Niekedy sa hodí zložitejší pohľad na celkovú konzistentnosť protistrany — závisí to od preferencií toho, kto si prehľad vyžiada. Trh by mohol ponúkať produkty a služby, ktoré zjednodušujú, spracúvajú a sprehľadňujú čítanie reputácie v kontexte danej situácie. Tomuto účelu môžu slúžiť aj rôzne autority a nimi ponúkané služby.

AKO ČÍTAŤ REPUTÁCIU

INFORMOVANÉ
ROZHODNUTIE



Vie, s kým má do činenia.

SLEPÁ DÔVERA



Netuší, s kým má do činenia.

SKÔR NEŽ POSKYTNEŠ ÚVER. SKÔR NEŽ PODPÍŠEŠ. SKÔR NEŽ DÔVERUJEŠ.

■ Príklady

Typické informácie zaujímavé pre vydavateľov — a cenné pre ostatných — sa týkajú udalostí presahujúcich bežnú medziľudskú komunikáciu v reálnom alebo virtuálnom svete.

Negatívne príklady: - dôkaz o trestných činoch (napr. auditovaný dôveryhodným vyšetrovacím orgánom) - nepriamy dôkaz (sám o sebe slabý, ale štatisticky kumulatívny) — napr. opakovaná prítomnosť v blízkosti viacerých krádeží v krátkom čase → ešte stále náhoda? - porušenie zmluvy

Pozitívne príklady: - napravená ujma (dobrovoľne alebo pod tlakom komunity ako trest) - prijatie a odpykanie trestu navrhnutého autoritou X - autorita X do určitej miery odňala uznanie majetkových práv previnilca

Je na každom, aby si o protistrane pozháňal dostupné informácie a posúdil riziká podľa svojich preferencií.

AKÉ DRUHY TVRDENÍ SA MÔŽU OBJAVIŤ?

PRÍKLADY ARTEFAKTU TVRDENIA

(tvrdenie je výrok o niekom — tu
sú druhy, ktoré ľudia zverejňujú.)

—

NEGATÍVNE TVRDENIA



NAPADNUTIE
fyzicky napadol inú osobu



KRÁDEŽ
vzal cudzí majetok bez súhlasu



PODVOD
oklamal niekoho pre osobný prospech



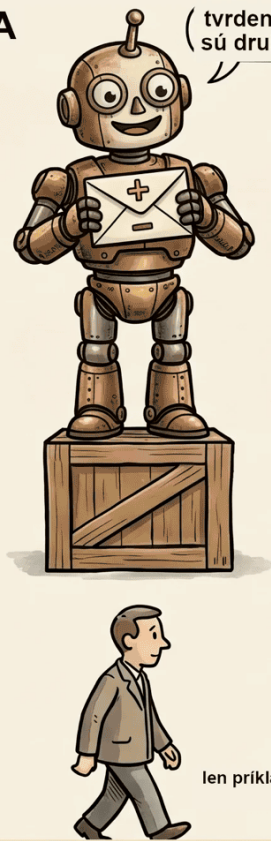
PORUŠENIE ZMLUVY
nesplnil dohodnutý záväzok



OHOVÁRANIE
širil poškodzujúcu nepravdu



ZANEDBANIE
nechal odkázaných či povinnosti bez dozoru



+

POZITÍVNE TVRDENIA



ŠKODA NAPRAVENÁ
opravil skôr spôsobenú škodu



DLH VYROVNANÝ
splatil dlžnú sumu v plnej výške



POSKYTNUTÁ POMOC
pomohol inému za osobnú cenu



OVERENÁ ODBORNOSŤ
preukázaná zručnosť v remese či odbore



MIMORIADNA SLUŽBA
dlhodobý prínos komunite

Ien príklady — každé tvrdenie sa riadi štandardom tvrdenia a každý štandard môže pridať ďalšie.

nemusiš sa pripojiť — no ak tvoje správanie dopadá na iných, niekto o tom môže zverejniť tvrdenie.

TVRDENIA SÚ SPÔSOB, AKÝM SPRÁVANIE VSTUPUJE DO SIETE.

■ Či sa o tebe v sieti objaví informácia, závisí výlučne od tvojho vlastného správania.

Do takej siete nikdy nemusíš vstúpiť, a napriek tomu sa v nej informácia o tebe môže objaviť. Závisí to výlučne od tvojich činov a dopadu, ktorý majú na iných.

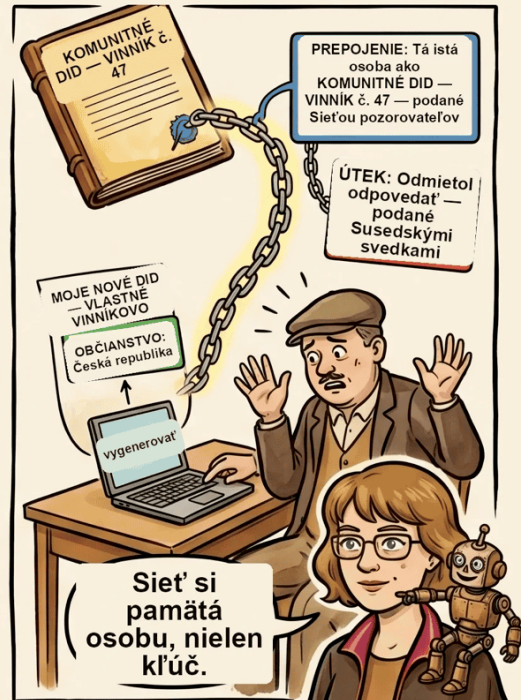
KOMUNITA TI HO MÔŽE OTVORIŤ



Nemá vlastné DID.
Nikdy sa neprihlásil.



Neotvoril si DID, tak ti komunita otvorí jedno O tebe. Sem sa pripájajú negatívne tvrdenia.



Vlastné si otvoriť môžeš
— no komunita obe prepojí. Reputácia nasleduje osobu, nie kľúč.

1. SPÔSOBIŠ
ŠKODU

2. KOMUNITA
PODÁVA

3. NEUNIKNEŠ -->

Otvorenie DID môžeš odmietnuť. Svoju reputáciu odmietnuť nemôžeš.

To, čo som práve stručne načrtol, je spôsob, ako by mohla fungovať sociálna sieť inšpirovaná decentralizovanou identitou (DID). Prvotným účelom konceptov DID je posilniť súkromie a slobodu cez princíp prihlásenia sa k pravidlám, ktoré budem dodržiavať a podľa ktorých budem žiť — dáva užívateľom možnosť rozhodnúť, aké informácie zdieľať a za akých podmienok.

Navrhujem DID ďalej prepojiť do komunikačnej siete, kde si ich držitelia vymieňajú spätnú väzbu aj mimo situácií, keď sa niekomu niečo stalo a komunita alebo jednotlivec potrebuje zareagovať. Také preventívne porovnanie pravidiel, ku ktorým sme sa prihlásili — s možnosťou vypočítať ekonomické a iné dôsledky vzájomných odchýlok v očakávaniach o tom, ako by mala druhá strana fungovať — by sa dalo považovať za motiváciu k hľadaniu konsenzu. Namiesto slobody by taký systém zdôrazňoval dobrovoľné rozhodovanie spojené so zodpovednosťou za správanie v reálnom svete.

Jednotlivec systém sám nerozbije — skupina ľudí má väčšiu šancu a skupina ľudí s vyjednaným konsenzom a motiváciami ťahať za jeden povraz v mnohých otázkach má ešte väčšiu šancu odolávať autoritárskym tendenciám. Predpoklad organizácie z prvej kapitoly bude splnený, keď nastanú dve podmienky: reputačná sieť DID pokrýva komunity dostatočne reprezentatívne na to, aby jej používanie prestalo byť exotikou. A zároveň sa tento komunitný segment stane ekonomicky významnou menšinou, ktorá dokáže asertívne vyjednávať so zvyškom spoločnosti.

■ Dobrovoľnosť vs sloboda

Sloboda — v pozitívnom zmysle — by bola druhotným efektom vyvažovania dvoch faktorov: dobrovoľnosti a tlaku okolia smerom k zodpovednosti.

■ Éra AI a hodnota reputácie

V ére umelej inteligencie sa automatizuje všetko, čo súvisí s kognitívnym myslením — a môže to zájsť ešte ďalej. Čo potom ostáva v ľudskej činnosti ako konkurenčná výhoda? Odpoveď je ťažká a niečo sa určite nájde, ale jedno môžeme povedať s istotou: rozhodne reputácia. Overiteľná história tvojho správania, tvojich záväzkov a ich plnenia — to je niečo, čo za teba AI nevybuduje.

AK ZA TEBA MYSLÍ AI — ČO ZOSTANE TEBE?

AI AGENTI PREBERAJÚ OPAKOVANÚ PRÁCU

ŠTANDARDIZOVANÉ
FIREMNÉ TOKY

ÚČTOVNÍCTVO

KONCIPOVANIE

jedna po druhej sa opakovaná
mentálna práca odovzdáva agentom.

TAK ČO ZOSTÁVA ČLOVEKU?



ten istý nápad si môže vybrať ktokoľvek.
čím sa jeden pekár, jeden stolár,
jedna AI dielňa líši od druhého?

REPUTÁCIA — ČO ICH DVOCH ROZLIŠÍ

DRŽÍ
SLOVO

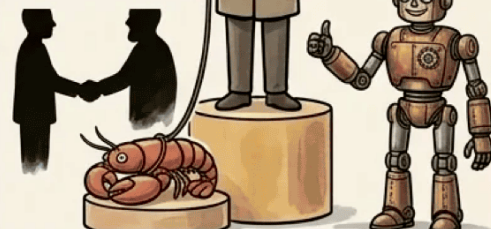
HOVORÍ SO
ZÁKAZNÍKOM

STOJÍ ZA
SVOJOU AI

10 ROKOV,
ŽIADNE
STÁŽNOSTI

Ľudský dotyk stále
uzavrie obchod.

Ani ja ti toto
nedokážem
postaviť — musíš
to byť ty.



niekto musí nieť zodpovednosť za to, čo
agent spraví — a tú zodpovednosť nemožno
odovzdať.

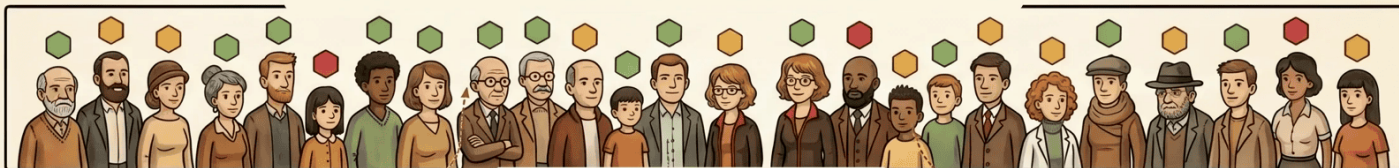
bez reputácie vyzerá každý pekár rovnako — a najväčšia značka ich všetkých pohltí.

mohla by toto byť tá decentralizovaná cesta, čo drží AI na uzde — to, čo bráni komukoľvek vlastniť celý trh?

AI AUTOMATIZUJE PRÁCU — REPUTÁCIA ŤA UDRŽÍ ČLOVEKOM.

EKONOMIKA PRAVDY

pás
komunity



JEDNA KOMUNITA. RÔZNE POSTOJE.

NEOBLÚBENÉ, ALE PRIJATELNÉ

V KONSENZE

MIMO KONSENZU

PODANIE



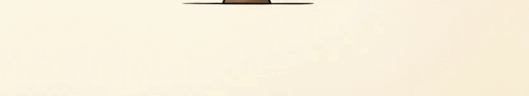
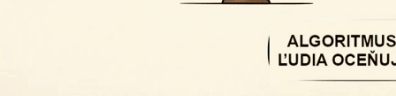
ŽREB



REFUNDÁCIA



REGISTER



SPODNÝ PÁS
POZOROVATEĽA

ALGORITMUS VYBERÁ FÉROVO.
ĽUDIA OCENÚJÚ TO, ČOMU VERIA.

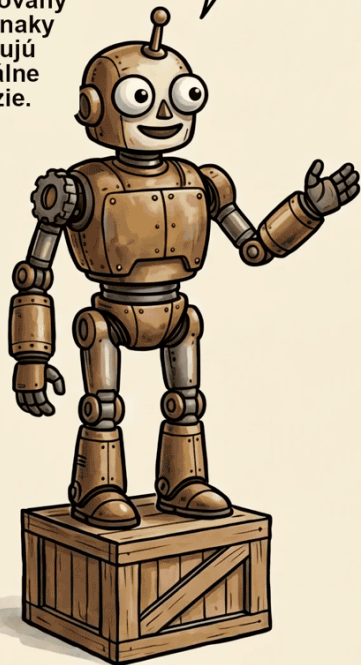


ROVNOMERNÝ ŽREB. NEROVNOMERNÁ ODPOVEĎ. ČÍM ĎALEJ OD KONSENZU, TÝM VYŠŠIA CENA.

ČO SA V SIETI ZVEREJŇUJE

zverejniť sa dá päť vecí — každá má verziu.

každý artefakt je verziovaný — odznaky ukazujú aktuálne revízie.



v1

DOKUMENT DID

tvoj identitný záznam v sieti — kľúče, metadáta, sieťová adresa.

SPRAVUJE: držiteľ DID



v2

ŠTANDARD TVRDENIA

schéma, ktorú musí tvrdenie dodržať — čo sa počíta ako platný dôkaz.

SPRAVUJE: autorita s reputáciou v danej oblasti



v3

ŠTANDARD POLITIKY

schéma, ktorú musí politika dodržať — podoba pravidiel prijímania.

SPRAVUJE: autorita s reputáciou v danej oblasti

↓ odvodené z

↓ odvodené z



v4

TVRDENIE

výrok o subjekte podľa štandardu tvrdenia — zverejnený vydavateľom, spolupodpísaný autoritou štandardu, ak o to požiadajú vydavateľ aj overovateľ.

SPRAVUJE: vydavateľ zverejňuje — subjekt je cieľom

tvrdenia sú dvojaké — pozitívne (+) a negatívne (-).



v5

POLITIKA DID

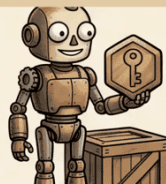
deklarované pravidlá DID — používané pri overovaní, konsenze a vydávaní.

SPRAVUJE: držiteľ DID (jedna politika na DID)

KAŽDÝ ARTEFAKT JE VERZIOVANÝ. KAŽDÁ VERZIA JE VEREJNÁ.

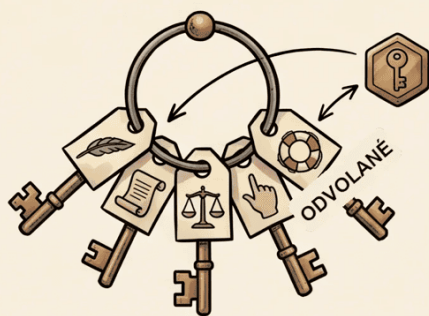
ČO JE VNÚTRI DOKUMENTU DID?

PRÍKLADY ARTEFAKTU DOKUMENTU DID



tvoj dokument DID je tvoja identitná karta v sieti — tu je, čo obsahuje.

POLIA, KTORÉ V ŇOM NÁJDEŠ



KLÚČE A PRAVIDLÁ PODPISOVANIA

každý kľúč udeľuje jednu právomoc — upraviť tento dokument, vydať tvrdenie, konať ako autorita, spravovať politiku alebo delegovať obnovu. Právomoci možno odovzdať inému DID a neskôr zas odobrať.



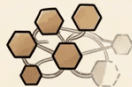
SIETOVÉ ADRESY

kde ťa sieť zastihne — meniteľné bez prepisu tvojej identity



VYTVORENÉ A VERZIOVANÉ

kedy sa táto identita prvýkrát objavila a ktorú revíziu práve čítaš



PREPOJENÉ IDENTITY

prehľad DID, s ktorými si spojený — pohodlný náhľad, technicky uložený inde



ZNAČKA NÁSTUPNÍCTVA

ak sa tvoja identita stratí alebo ukradne, autorita môže toto DID označiť za ukončené a ukázať na tvojho nástupcu

každú novú verziu píše držiteľ DID — no každá verzia musí prejsť overením, kým ju sieť zverejní.

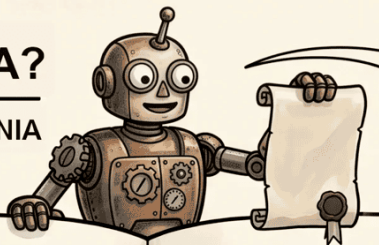
pišeš ju ty — sieť ju overuje. Nemôžeš sa len tak zverejniť do existencie.



IDENTITU AUTORIZUJEŠ TY — SIETĽ JU POTVRDZUJE.

ČO JE ŠTANDARD TVRDENIA?

PRÍKLADY ARTEFAKTU ŠTANDARDU TVRDENIA



štandard je prázdny formulár —
tvrdenie je vyplnený formulár.
Ukážem ti oba vedľa seba.

ŠTANDARD — PRÁZDNY FORMULÁR

	SUBJEKT DID DID, ktorého sa tvrdenie týka
	VYDAVATEĽ DID DID podpisujúci tvrdenie
	KEDY A KDE dátum a miesto
	SCHVÁLENÉ TYPY DŮKAZOV počítajú sa len tieto druhy dôkazov
	ŠKÁLA VÝSLEDKU vyber presne jeden stupeň — žiadny voľný text

TVRDENIE — VYPLNENÝ FORMULÁR

	SUBJEKT DID did:nwo:alice-9f2b...
	VYDAVATEĽ DID did:nwo:magistrates-04...
	KEDY A KDE 3. marca, trhové námestie
	SCHVÁLENÉ TYPY DŮKAZOV fotografia ✓ — svedecká prisaha ✓ — lekárska správa ✓
	SCHVÁLENÉ TYPY DŮKAZOV stredná — stupeň 2 zo 4

každé pole vľavo má presne jeden vyplnený náprotivok vpravo — práve to robí dve tvrdenia rovnakého druhu porovnateľnými.

pečať autority na vyplnenom tvrdení je
prísľub: proces bol naozaj dodržaný.



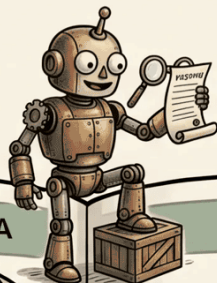
Ručím svojou
reputáciou, že toto
bolo spracované
podľa štandardu.



ŠTANDARD JE FORMULÁR — TVRDENIE JE VYPLNENÝ A ZARUČENÝ FORMULÁR.

ČO JE POLITIKA DID?

PRÍKLADY ARTEFAKTU POLITIKY DID



moja politika nie je o tom, ako sa tvrdenie píše — to je úloha štandardu. Moja politika je o tom, ako sa rozhodujem, či sa mám tvrdením vôbec zaoberať: dôverujem tomu, kto ho podpísal, dôverujem autorite za jeho štandardom a stojí tá vec vôbec za moju pozornosť?

ŠTANDARD — ZDEDENÉ PREDVOLENIA

NÁZOV PRAVIDLA



SPODNÁ HRANICA REPUTÁCIE VYDAVATEĽA

prijímam vydavateľov s reputáciou nad päť z desiatich



ZOZNAM DÔVERYHODNÝCH AUTORÍT

prijímam štandardy od každej autority, ktorej vlastná reputácia je nad štyri z desiatich



FILTER PODSTATY

spracujem každé tvrdenie, ktorého vec váži viac než hranica „malichernosti“



CENOVÁ KRIVKA PROTI SPAMU

podanie u mňa je lacné pri závažných, zriedkavých tvrdeniach — a rýchlo rastie pri malicherných či opakovaných



KOMBINOVANÉ VÁŽENIE

reputácia vydavateľa a reputácia autority sa násobí; malichernosť vecí výsledok polovičí

politika neprepisuje štandard — posudzuje ľudí a vec. Ponechať, upraviť, odstrániť, pridať — štyri jednoduché ťahy nad spoločným východiskom.

MOJA POLITIKA — ODVODENÁ Z NEHO

názov pravidla



SPODNÁ HRANICA REPUTÁCIE VYDAVATEĽA

✓ PONECHANÉ
fajka UPRAVENÉ
slovo akcie
✗ ODSTRÁNENÉ
slovo akcie
+ PRIDANÉ
slovo akcie

sprišené — vyžadujem sedem z desiatich



ZOZNAM DÔVERYHODNÝCH AUTORÍT

plne dôverujem magistrátom a lekárom; váhu tvrdení pod obecným dozorom polovičím; čokoľvek pod prístavnou políciou odmietam úplne



FILTER PODSTATY

malicherné otravné tvrdenia ma nestoja nič, aby som ich ignoroval — jednoducho ich nečítam



CENOVÁ KRIVKA PROTI SPAMU

ponechané — predvolená krivka mi vyhovuje



KOMBINOVANÉ VÁŽENIE

odstránené — používam vlastný vzorec



EXPONENCIÁLNA CENA ZA OPAKOVANÉ TVRDENIA

pridané — každé ďalšie tvrdenie od toho istého vydavateľa o mne za rok stojí desaťnásobok predošlého



TICHÉ HODINY

pridané — odmietam čítať akékoľvek tvrdenie podané medzi polnocou a úsvitom



OVEROVANIE — moja politika filtruje prichádzajúce tvrdenia aj moje vlastné návrhy skôr, než ich vydám. Vydávanie je overovanie na ceste von.

KONSENZUS — moja politika je môj hlas, keď komunita vyjednáva spoločné pravidlá.

TVOJA POLITIKA POSUDZUJE POSLA — NIE FORMULÁR.



Prečo je sieť necenzurovatelná

Doteraz sme opísali, čo sieť dokáže. Teraz sa zamerajme na to, prečo ju nemožno vypnúť ani cenzurovať.

Sieť bude pravdepodobne postavená na princípoch siete Tor a onion routingu (spôsob maskovania sieťovej prevádzky pomocou princípov Mixnetu) — technológie, kde komunikácia prechádza cez niekoľko vrstiev šifrovania a žiadny jednotlivý uzol nepozná odosielateľa a príjemcu naraz. Centrálna inštitúcia ti nemôže nazerať cez plece, pretože nie je odkiaľ.

Môžeš proti tomu bojovať, ale nemôžeš vyhrať — pokiaľ neuvrhneš celú krajinu do totalitného dohľadu na úrovni jednotlivých sieťových paketov a nízkoúrovňových akcií na každom kuse hardvéru, ktorý sa pripája na internet a komunikuje v danej reputačnej sieti. A práve pred takou voľbou stojí centralizmus: buď prijme, že občania majú nástroj mimo tvojho dosahu, alebo sa zaryje do temných kútov ekonomickej stagnácie v mene totalitnej kontroly.

Nerobme si ilúzie — o toto sa pokúsia aj demokratické režimy v boji za centralizmus. Radšej ľudí spútajú, než by sa vzdali moci.

AKO ZOSTÁVAJÚ TVOJE SPRÁVY NESLEDOVATEĽNÉ DVE LÍNIE OBRANY NARAZ — VRSTVY A ŠUM

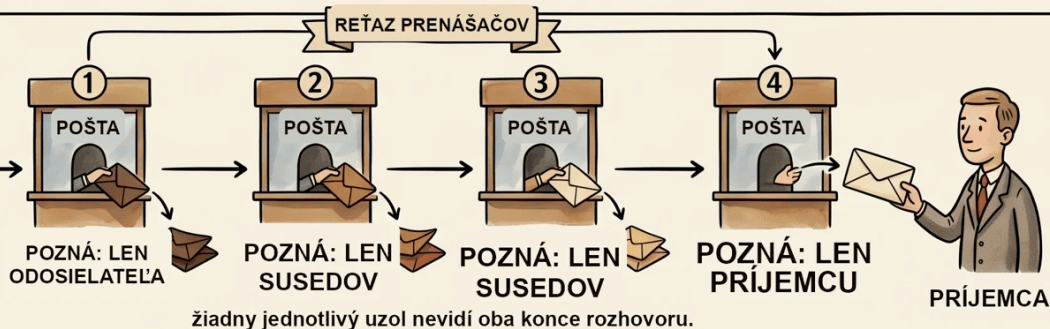
OBSAH: ZABALENÝ VO VRSTVÁCH (technika za Torom — „onion routing“)



ODOSIELATEĽ

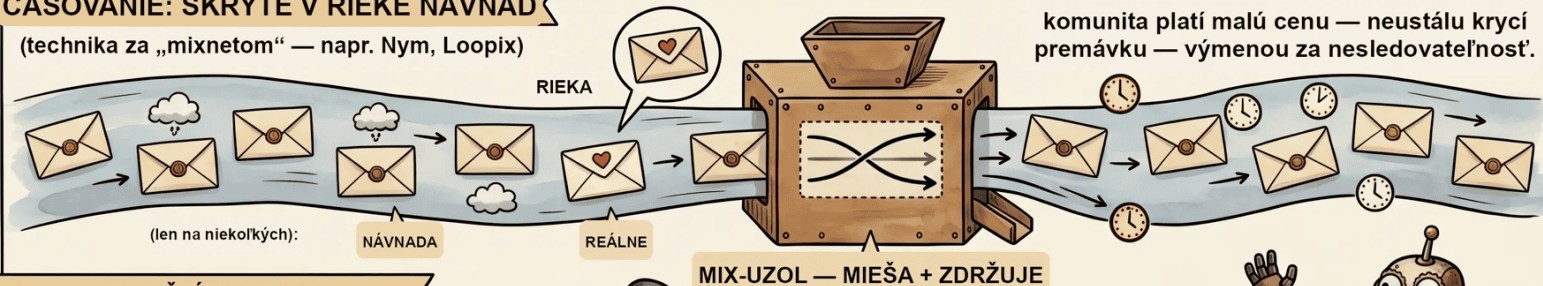


štyri zámky, štyri kľúče
— jeden na každý uzol.



PRIJEMCA

ČASOVANIE: SKRYTÉ V RIEKE NÁVNAD (technika za „mixnetom“ — napr. Nym, Loopix)



DVA ŠTÍTY SPOLU

MATICA	SKRÝVA KTO ↔ KTO?	SKRÝVA KEDY?
LEN VRSTVY	✓ ÁNO	✗ NIE
LEN ŠUM	✗ NIE	✓ ÁNO
VRSTVY + ŠUM	✓ ÁNO	✓ ÁNO

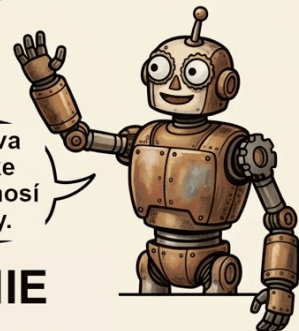
(onion routing + mixnet — kombinácia ktorú používajú Tor a Nym)



sto obálok za
hodinu — na
ktorej záleží?

pozorovateľ vidí tok, no
nerozozná REÁLNE od
NÁVNADY.

reálna správa
pláva v rieke
návnad — a nosí
štyri kabáty.



OBSAH SKRYTÝ VRSTVAMI — ČASOVANIE SKRYTÉ ŠUMOM.

Odpovede na zjavné pochybnosti

Opísaný systém prirodzene vyvoláva množstvo otázok. Poďme sa venovať tým najčastejším.

Závislosť od technológie

Pravdepodobne si si už všimol, že na rozdiel od moderného štátu — ktorý je s nami asi 150 rokov — riešenie reputačnej siete tak, ako je tu opísané, silno závisí od technológie globálneho / lokálneho internetu. V prípade výpadku je fungovanie takej siete ohrozené.

Ak je výpadok dočasný, nedochádza k strate dát ani konzistentnosti tvrdení v sieti a ani dosiahnuté reputačné bilancie v rámci komunít by nemali byť narušené. Na rozdiel od porovnateľných platobných sietí táto sieť predpokladá veľmi nízke frekvencie procesov a dátových položiek. V tomto sa decentralizovaná reputačná sieť nelíši od dnešného štátu, ktorý je tiež už teraz silno závislý od technológie a zabudol pracovať s papierovými kartotékami (hoci v krízových plánoch by nemal na výber).

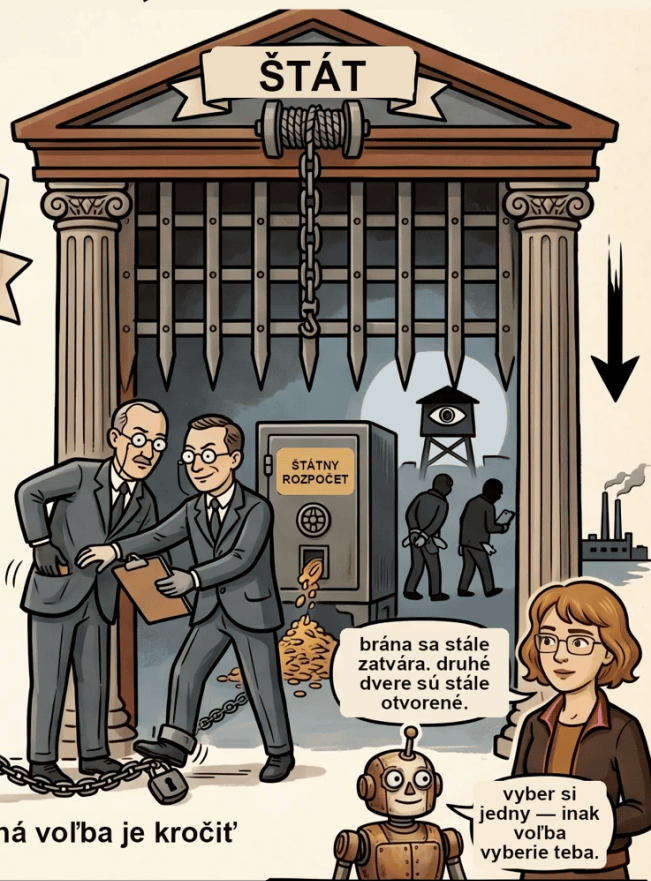
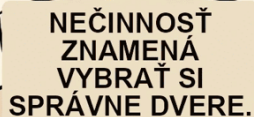
Evolučný nástupca štátu v podobe reputačnej siete môže v prípade trvalého výpadku (katastrofy nevídaného rozsahu) padnúť späť na primitívnejší centralizovaný systém — štát.

Technológia umožňuje ľuďstvu dosiahnuť vyššie civilizačné formy vládnutia a prináša nám výhody, no aj riziká.

Nehádzem zverejňovaním v sieti peniaze z okna?

Náklady na zverejnenie tvrdenia v reputačnej sieti sú z veľkej časti nie utopené. Užitočnosť správy, ktorú vydavateľ vloží do siete — informácie o skutočných krivdách, overené skúsenosti, relevantné varovania — sa štatisticky vracia v dlhšom časovom horizonte v podobe poplatkov za overovanie cudzích tvrdení

SIEŤ REPUTÁCIE



**brána sa stále
zatvára. druhé
dvere sú stále
otvorené.**

vyber si
jeden — inak
voľba
vyberie teba.

ŠTÁT ZATVÁRA V PREDVOLENOM STAVE. SIEŤ OTVÁRA Z VOĽBY.

z komunity. Komunita profituje, vydavateľ si buduje reputáciu a náklady na zverejnenie pravdivej informácie sa tak blížia vratnej zálohe, od ktorej treba odpočítať len menšiu časť skutočných nákladov na údržbu siete. Naopak, nepravdivé či triviálne záznamy sa nevracajú — ich náklady sú čistou stratou. Poctivosť teda nie je len morálnou voľbou, ale aj ekonomicky racionálnou stratégiou.

Po odpočítaní nákladov na údržbu siete by sa tento princíp dal nazvať princípom ekonomickej neutrality — nestrácam, keď som s komunitou, strácam, keď som proti nej.

Komunita má aj solidárne kanály na ocenenie poctivého prístupu svojich členov. Nerobme si však ilúzie: apely na solidaritu vznikajú väčšinou zo sociálneho tlaku komunity, takže nemusí ísť o solidaritu v dobrovoľnom zmysle slova.

Čo ak si niekto vytvorí viacero identít?

Človek môže paralelne prevádzkovať viacero DID identít. Budovanie reputácie pre každú identitu si však vyžaduje samostatné úsilie — čas, energiu, peniaze.

Žiadne skratky: každá identita si musí nazbierať svoj track record¹ cez skutočnú aktivitu. Udržiavanie paralelných identít je preto zámerne drahé.

V slobodných spoločnostiach náklady odrádzajú od zneužitia.

¹**Track record** — všeobecne: história minulých výsledkov, úspechov a zlyhaní osoby alebo organizácie. Tu: súhrn všetkých minulých interakcií danej DID identity v sieti — overené tvrdenia, prijaté a zamietnuté záznamy — z ktorých sa odvodzuje jej reputácia.

V diktatúrach sa však paralelné identity stávajú nástrojom prežitia: umožňujú organizovať podzemné siete, bezpečnejšie sa pohybovať na čiernom trhu a viesť kompartmentalizovaný² odboj, kde kompromitácia jednej identity neodhalí ostatné — a po páde režimu umožňujú plynulý návrat do verejného života a k tam vybudovanej reputácii, ba dokonca zlúčenie predtým oficiálnej a tajnej DID do jedinej kombinovanej množiny záznamov prostredníctvom tvrdenia.

²**Kompartmentalizácia** (z angl. *compartment*) znamená oddelenie informácií do izolovaných jednotiek tak, aby odhalenie jednej jednotky neohrozilo ostatné. Princíp známy zo spravodajských služieb: agent pozná len svoju časť operácie, takže ani pod nátlakom nemôže odhaliť celok.

ROVNAKÁ NÁMAHA — MÁRNIVÝ PLÁN B V SLOBODE, ZÁCHRANNÉ LANO POD TYRANIOU

PARALELNÉ IDENTITY STOJA ROVNAKO — NO KUPUJÚ RÔZNE VECI

V SLOBODE — NÁKLADNÝ PLÁN B



SEMEŇO → KLÍČOK → SADENICA → MLADÝ STROM → DOSPELÝ STROM
5 až 15 rokov — žiadne skratky, dospelý strom sa nedá kúpiť



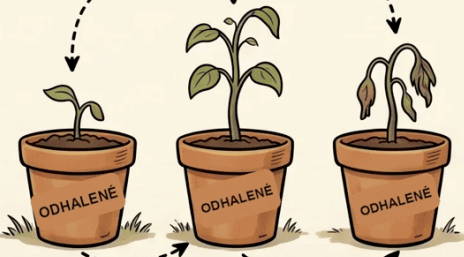
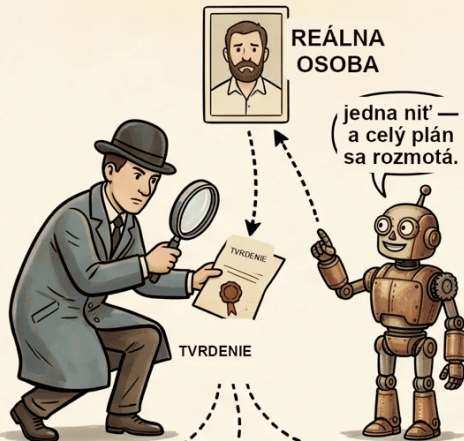
rok 1 — vynaložený čas, energia, peniaze — 5 % reputácie
rok 3 — tie isté náklady znova, platené nezávisle — 20 % reputácie
rok 0 — všetko začína odznova — 0 % reputácie
tri záhrady, trojnásobné náklady — a stále máš len dve ruky.

ALEBO — ČISTÝ ŠTÍT PO OSOBNOM POKLESKU



DID-NOVÝ-ZAČIATOK
funguje len ak spúšť zostala tvoja vlastná — ak boli iní poškodení natoľko, že ťa začnú sťahovať, ich tvrdenia ťa budú nasledovať aj do nového kvetináča.

JEDNO TVRDENIE A PLÁN B JE PREČ



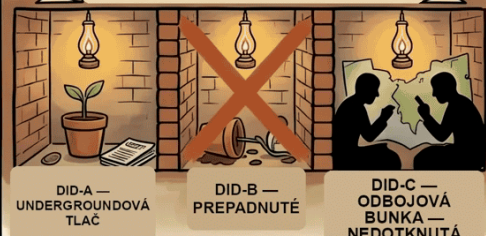
Jediné tvrdenie priviaže každý kvetináč k tomu istému záhradníkovi — roky času, energie a peňazí zmazané za jedno popoludnie.

POD TYRANIOU — JEDNO PRE ŠTÁT, OSTATNÉ PRE SLOBODNÉ ZDRUŽOVANIE (štát identity buď rovno zakáže, alebo ich vyžaduje pod vlastnou kontrolou)



navonok súlad — jedna identita odovzdaná na sledovanie.
TIEŽ MOJE — NO SKRYTÉ PRED ŠTÁTOM

TIE, KTORÉ ŠTÁT NESMIE NIKDY VIDIEŤ



tehlové steny medzi bunkami robia prácu, ktorú štát zakazuje — stratis jednu, ostatné pokračujú; keď režim padne, verejný život sa obnoví.

V SLOBODE JE ZNEUŽITIE DRAHÉ. POD TYRANIOU JE PREŽITIE MOŽNÉ.

Vnímanie obrátené naruby

Na rozdiel od štátu princíp reputačnej siete postavenej na decentralizovanej identite obracia paradigmu vnímanej priority:

- Dôležitá je reputácia — teda minulosť, ktorá sa používa na posúdenie rizík interakcie s protistranou — a osobné údaje ako mená, adresy atď. môžu byť vecou zdvorilostnej výmeny dát
- Zatiaľ čo štát primárne vyžaduje osobné údaje, hromadí reputačné dáta a komunita ukáže len to, čo sa mu hodí

Nemôže si bohatý človek jednoducho „kúpiť“ viac identít (alebo vytvoriť virtuálne komunity)?

Možnosť vytvárať paralelné decentralizované identity na prvý pohľad vyzerá ako nespravodlivá výhoda ľudí s väčšími ekonomickými prostriedkami oproti tým s menšími. Treba však zdôrazniť, že na rozdiel od centralizovaného systému, kde stačí skorumpovať pár bodov v pyramíde moci, aby určité previnenia zmizli, v decentralizovanom systéme by bolo treba skorumpovať celú komunitu.

Náhradné decentralizované identity by tomuto účelu mohli poslúžiť, ale ich reputácia musí byť budovaná v čase cez reálnu interakciu so skutočnými inými členmi komunity — nedá sa jednoducho kúpiť, pretože sieť robí overiteľným, ako si daná identita počína.

Navyše na trhu môžu existovať (a pravdepodobne aj budú) služby, ktoré ako autorita ponúkajú vyšetrovania produkujúce dôkaz, že niekoľko decentralizovaných identít je v skutočnosti tá istá osoba. Jediný záznam vložený do reputačnej siete tak môže za zlomok nákladov znehodnotiť celú investíciu času, energie a peňazí vynaloženú na budovanie paralelných identít.

Ekonomicky sa teda oplatí komunitu nepodvádzať — a keď treba, preskúmať svoje činy a usilovať sa o nápravu, aby sa reputácia vrátila na prijateľnú úroveň a jej nositeľ nestrádal ekonomicky ani inak pod hnevom komunity.

Ekonomicky mocná identita, ktorá stratila reputáciu vo vlastnej komunite, sa môže pokúsiť uniknúť hnevu komunity cez podpultové dohody s cieľenými identitami — tie však potom tiež riskujú stratu vlastnej reputácie.

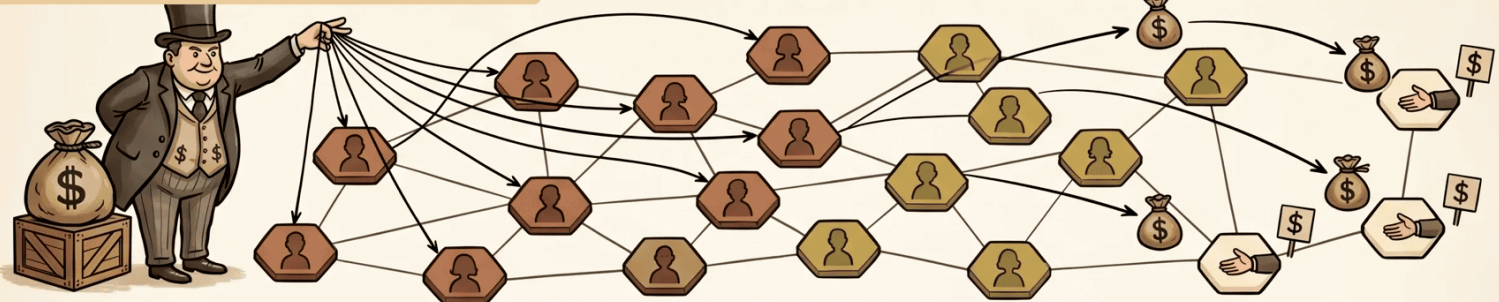
Stále ostáva únik do inej komunity s čerstvou identitou — to však znamená nechať za sebou všetky výdobytky a začať niekde od nuly s nulovou reputáciou. Niekedy to môže byť pochopiteľná cesta a jediné východisko.

REPUTÁCIA JE PROTIVÁHA EKONOMICKEJ SILE

BOHÁČ SI KUPUJE VPLYV — KOMUNITA SI HO PAMÄTÁ

ÚTOK — PRENIKNÚŤ A PODPLATIŤ

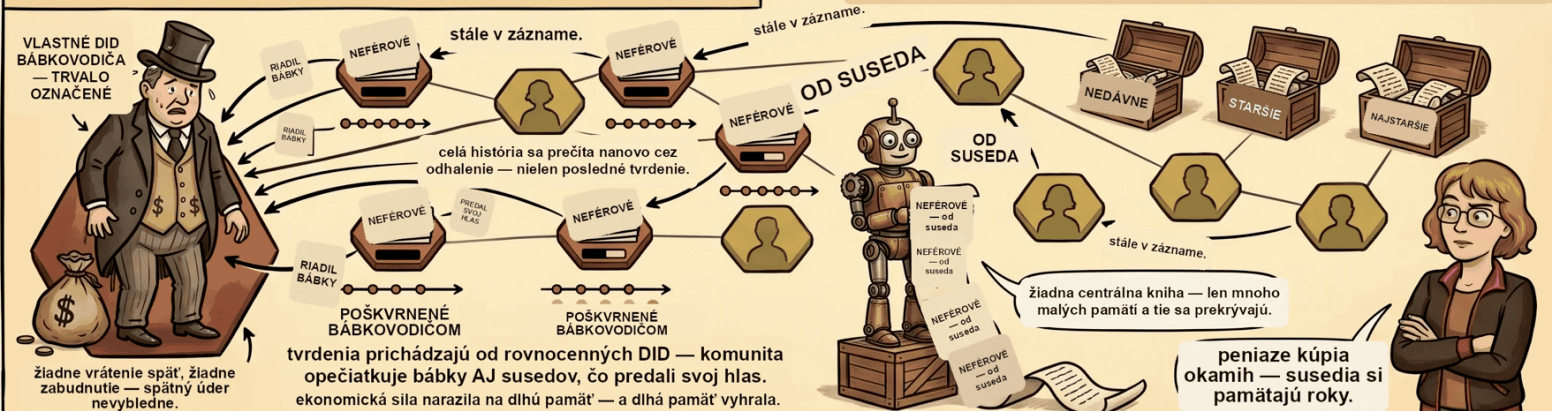
OSEM NASADENÝCH BÁBK + TRAJA PODPLATENÍ SUSEDIA



NEŠKÔR

OBRANA — DLHÁ PAMÄŤ, DISTRIBUOVANÉ ÚČTOVANIE

KAŽDÝ SUSED SI DRŽÍ VLASTNÚ PAMÄŤ — ŽIADNA CENTRÁLNA KNIHA, ŽIADNE ZABÚDANIE



EKONOMICKÁ MOC SIAHA DNU — SPÄTNÝ ÚDER SA VRÁTI DOMOV A NEZMYJE SA.

Poznámka

Podobne by komunity riešili útok, pri ktorom niekto venuje zdroje na vytvorenie virtuálnej identity: pre takú identitu je riskantné vstúpiť do interakcie s inou komunitou bez overenia — teda nekriticky prijímať informácie o identitách druhej komunity. Reputácie sa vždy budujú v rámci komunity, nie globálne.

Čo s prispôsobivcami, ktorí chcú len čítať a komunite nedať nič?

Prístup k informáciám nie je od prvého dňa vytvorenia decentralizovanej identity neobmedzený. Noví účastníci — tí, čo si ešte nevybudovali reputáciu skutočnou aktivitou — čelia stupňovaným obmedzeniam: menej informácií, dlhšie čakacie doby, vyššie náklady na dotazy. Sieť odmeňuje účasť, nie pasívnu spotrebu a svojvoľné zberanie dát.

Decentralizovaná identita riskuje svoju reputáciu aj vtedy, keď ju za odplatu prepožičia inej osobe (ktorá ani nemusí byť v reputačnej sieti DID). Platí tu rovnaký princíp: taká zrada komunity (porušenie súkromia) sa môže odraziť na reputácii zradcu a čin sa nedá vymazať podpultovou dohodou tak, ako to funguje v centralizovanom systéme. Musí rátať s hnevom komunity vrátane straty výdobytkov — komunita je totiž v jeho očiach garantom napríklad výsady vlastníť hnuteľný a nehnuteľný majetok.

Kotva k reálnemu svetu

Pri posudzovaní rizika je rizikovejším subjektom prirodzene ten, kto nepožíva výsadu vlastníctva uznaného danou komunitou — má vo svojom počínaní menej čo stratiť (digitálne aktíva sa presúvajú ľahšie).

Môže to vyzeráť ako drobnosť, no má to veľké dôsledky. Ak chceme, aby komunita mala páku na svojich členov, znamená to vlastníctvo ako výsadu — v najslobodnejších spoločnostiach takmer nedotknuteľnú, no stále nie právo ani základný princíp, ale výsadu, ktorá sa v krajných prípadoch môže odňať (viem si predstaviť napríklad odmietnutie služby v obrane komunity v ozbrojenom konflikte).

Podprahovo to zároveň odpovedá na to, ako bude komunita zaobchádzať so svojimi členmi a akú motiváciu má člen bojovať za komunitu — udržať si svoje výsady. Človek môže zlyhať vo svojej zodpovednosti voči komunite, ale morálne nemôže očakávať zhovievavosť, keď ide o udržanie ťažko získaných výsad.

Finančná neutralita

Pri čítaní slov ako decentralizovaný, necenzurovateľný, neskorumpovateľný si ich človek nevyhnutne spája s najznámejšími kryptomenami — Bitcoin, Monero a povedzme Kasper — ktoré sa dajú takto opísať. Intuícia tu však zavádza: poplatky za služby autorít, za overenie a zverejnenie a podobne sa dajú vyrovnať v ľubovoľnej mene alebo peniazoch. Pre prepojených účastníkov sociálnej siete v sieti DID (teda tvoju komunitu) a jej okolie je dôležité reputáciou podložené potvrdenie, že platba prebehla. Zverejnenie

SIEŤ ODMEŇUJE ÚČASŤ

REPUTÁCIA SA BUDUJE CELÝ ŽIVOT — NEKUPUJE SA, NEPOŽIČIAVA SA

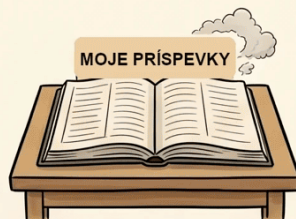
ÚČASTNÍK — CELOŽIVOTNÁ SKUTOČNÁ PRÁCA



ČIERNY PASAŽIER — ČÍTA, NIKDY NEZVEREJŇUJE



číta záznamy všetkých ostatných.



sám nezverejní nič.



OBMEDZENÝ PRÍSTUP — STROP SA NEDVÍHA

reputácia 5 %

žiadne skutky, žiadny vzostup — rok čo rok tá istá latka.

ČAS, ENERGIA A PENIAZE — VLOŽENÉ DO SKUTOČNEJ PRÁCE — SÚ JEDINÁ MENA, KTORÚ SIEŤ REŠPEKTUJE.

tvrdenia musí individuálne niesť rozumnú, overiteľnú cenu, aby aktér nemohol zverejniť koľko koľvek a akékoľvek tvrdenia bez vynaloženia energie, peňazí a času — silno nežiaduci stav zodpovedajúci výsade elít v dnešných korupciou prežratých štátnych systémoch.

V tomto majú spomínané kryptomeny malú výhodu v tom, že ich siete pôsobia ako dôveryhodné authority na overenie, že daná platba prebehla, za cenu malej straty súkromia a odhalenia niektorých svojich adries.

Dobrovoľnosť, zodpovednosť a sloboda

Dobrovoľnosť je individuálna: rozhodujem sa sám za seba. Zodpovednosť vzniká, keď moje rozhodnutie ovplyvňuje iných — nastupuje spätná väzba. Sloboda nie je ani dar, ani právo — je fenomenologickým³ výsledkom tisícov obojstranných interakcií medzi dobrovoľnosťou a tlakom smerom k zodpovednosti, spriemerovaných naprieč spoločnosťou. Sieť tento priemer nediktuje — emerguje⁴ z cenových signálov overovateľov a z vopred ohlásených overovacích politík, ktoré si členovia komunity sami nastavujú.

Akú preferenciu slobody má jednotlivec v rámci komunity, závisí od jeho pocitu, koľko z toho, čo vnucuje iným, je sám ochotný preglgnuť. Pri veciach, ktoré sú samozrejme a prospešné všetkým, niet

³**Fenomenologický** (z gr. *phainómenon* — to, čo sa javí) — všeobecne: prístup skúmajúci javy tak, ako sa prezentujú v priamej skúsenosti, pozorovaním toho, čo z nich vyplýva, bez vopred daných vysvetľujúcich teórií v mikrosвете pod nimi. Tu: sloboda nie je abstraktný princíp definovaný zhora, ale pozorovaný jav — dôsledok tisícov mikrointerakcií medzi ľuďmi, ktorý emerguje z toho, ako sa k sebe skutočne správame.

⁴**Emergentný** (z lat. *emergere* — vynoriť sa) znamená „spontánne vznikajúci z interakcií jednoduchších častí bez toho, aby to niekto navrhol alebo riadil.“ Kérdeľ vtákov letí vo formácii, hoci žiadny vták nemá plán formácie — formácia emerguje z jednoduchých pravidiel každého jednotlivca. Rovnako v reputačnej sieti nikto nenavrhne pravidlá správania celku — emergujú z tisícov jednotlivých rozhodnutí.

morálnej dilemy — vražda je zlá. Potom sú prípady, kde sa možnosti presúvajú do polohy povolených výsad: preukáž svoje schopnosti a pustíme ťa na cestu, aby bola menšia šanca, že nás zabiješ. A napokon sú záležitosti, kde jednotlivec povie — nestojí mi to za to, nebudem susedovi zakazovať páliť lístie, keď to robím sám, alebo preto, že robím niečo iné, čo obmedzuje jeho pohodlie, a on by mi to zas mohol chcieť zakázať. Ak sme historicky nakreslili hranicu slobody tam, kde začína sloboda niekoho iného, potom reputačná sociálna sieť postavená na decentralizovanej identite napĺňa toto lepšie ako centralizovaná zastupiteľská demokracia — kde sa napríklad výsadná vrstva volených zástupcov snaží vyňať samu seba z dohľadu nad osobnou komunikáciou, no neváha ho uvaliť na svojich voličov pomocou najrôznejších podpultových zámienok a manipulácií.

Prepínač sloboda–totalita (a delegovanie)

Jednoduchý mechanizmus v sieti DID dokáže posunúť celý systém smerom k väčšej slobode alebo väčšej kontrole: počet záznamov, ktoré smie DID zverejniť za časové obdobie. Keď záznamy ostávajú vzácne, každý nesie váhu — to je sloboda. Keď je záznamov nadbytok a pokrývajú maličkosti, to je totalita. Smer si volíš každým záznamom, ktorý zverejníš. Sieť samotná nie je ani slobodná, ani totalitná — je to neutrálna infraštruktúra. Čím sa stane, určuje to, ako ju ľudia používajú.

V rámci vlastnej overovacej politiky má zmysel nastaviť pre generický DID v mojej sociálnej sieti — v rámci komunit — maximálny počet tvrdení (akéhokoľvek overiteľného výroku vo všeobecnosti; tu: záznamu zverejneného do reputačnej siete), ktoré smie vydavateľ vydať za obdobie, aby som ich bral do úvahy a jeho žiadosti o overenie považoval za relevantné.

V hlave mám intuitívne číslo — nízke jednotky za rok. Taký cenzúrny prístup sa môže zdať dosť izolacionistický. Ale žiadateľa môžem legitímne postaviť pred voľbu: vybrať jeden zo svojich už vydaných záznamov a požiadať overovateľa o jeho zrušenie, teda zneplatnenie — čo je dosť agresívna požiadavka

DOBROVOL'NOSŤ → ZODPOVEDNOSŤ → SLOBODA

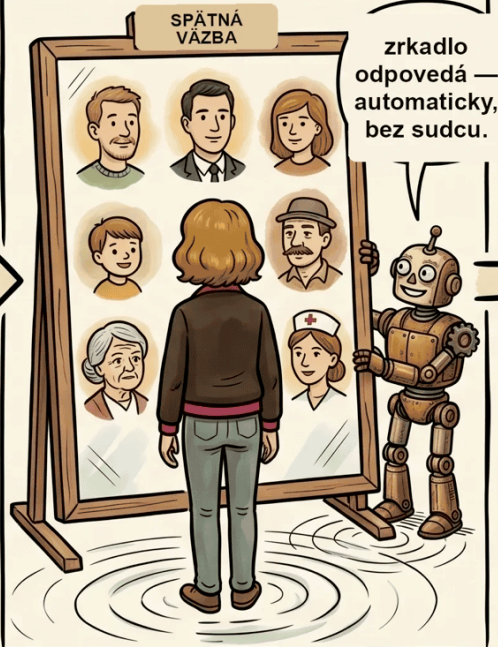
TRI KROKY — OD VOĽBY JEDNÉHO ČLOVEKA K VZORCU CELEJ SPOLOČNOSTI

DOBROVOL'NOSŤ



jednotlivec sa rozhoduje — nikto ho nenúti.
a nikto jej ani nedlhuje pozitívnu povinnosť.

ZODPOVEDNOSŤ



moje voľby sa vlnia von — a vlny sa vracajú.
následky hovoria samy za seba.

SLOBODA

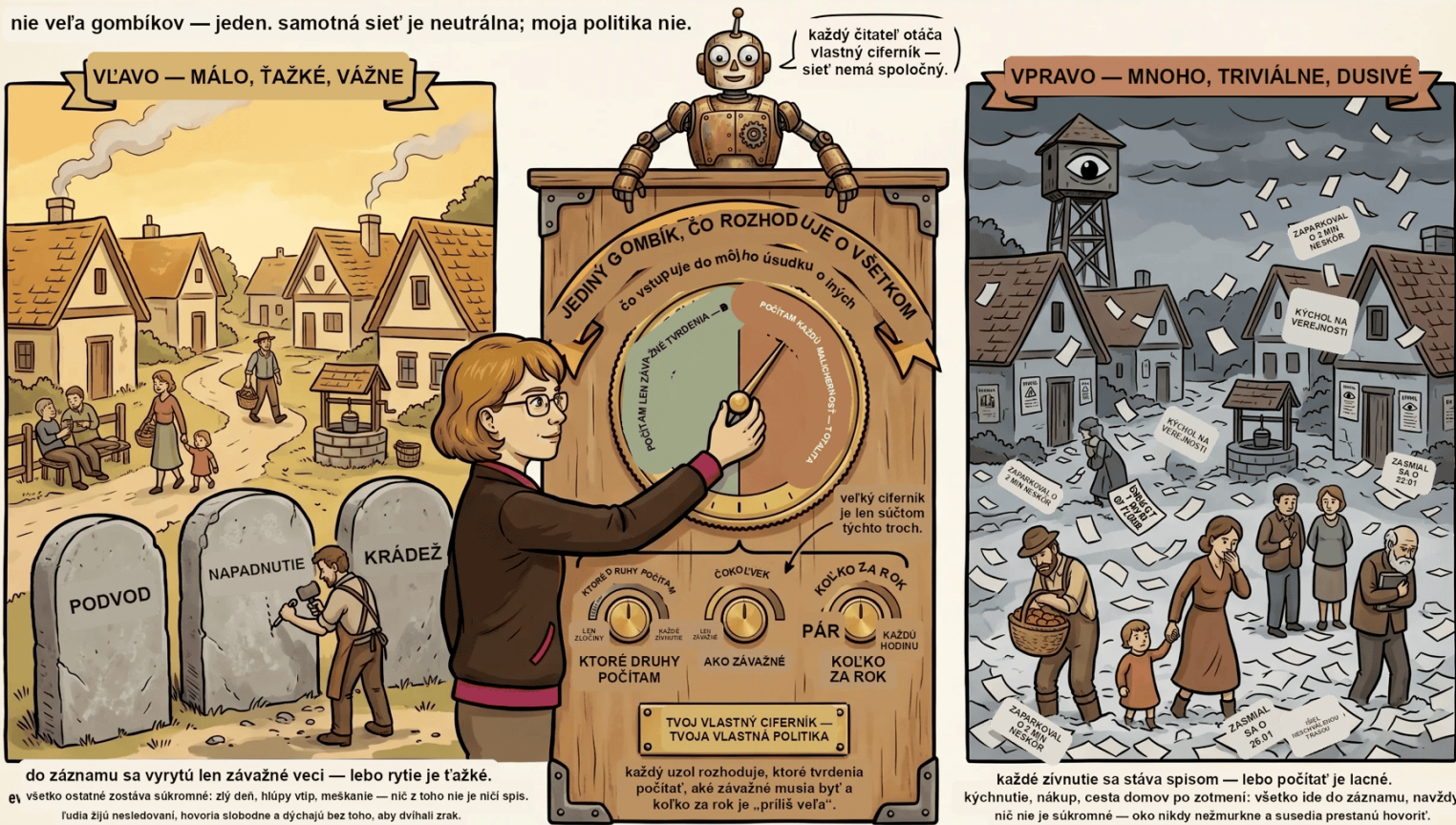


túto mapu nikto nenakreslil — nakreslila sa sama.
sloboda je štatistický tvar toho,
ako sa susedia k sebe správajú.

SLOBODA NIE JE DAR ZHORA — JE TO VZOREC, KTORÝ TVORÍME SPOLU.

PREPÍNAČ SLOBODA-TOTALITA

JEDINÝ PARAMETER — KOLKO SA ROZHODNEM SLEDOVAŤ — PREKLOPÍ CELÚ SPOLOČNOSŤ MEDZI SLOBODOU A TYRANIOU
nie veľa gombíkov — jeden. samotná sieť je neutrálna; moja politika nie.



SLOBODA JE TO, ČO ODMIETAM POČÍTAŤ — TOTALITA JE TO, S ČÍM SÚHLASÍM SLEDOVAŤ.

v situácii, keď sa žiadateľ zhodou okolností naozaj stal obeťou viacerých nezávislých krívd, a ja by som tak určite prispel k jeho pocitu odcudzenia od komunity.

Účinnejšou možnosťou sa preto javí schopnosť delegovať časť svojich práv na zverejňovanie informácií do reputačnej siete v prospech komunity alebo autority, ktorá potom — solidárne, podľa svojich vnútorných pravidiel — rozhoduje, ako ich prideliť. Skupina musí byť schopná postarať sa o tých, ktorých považuje za znevýhodnených. Člen komunity má právo kedykoľvek, kým delegované právo nie je použité, svoje delegovanie odvolať.

DELEGOVANIE PRÁV NA ZVEREJŇOVANIE

POŽIČIAŠ KLÚČ AUTORITE, KTORÁ ŤA OBSLUHUJE — A V OKAMIHU HO STIAHNEŠ SPÄŤ

požičiam kľúč —
nitka zostáva u mňa.

delegovanie — autorita koná v
mojom mene, v rámci pravidiel,
ktoré schválím.

NITKA
ODVOLANIA

MOJE PRÁVO
ZVEREJŇOVAŤ
— 1 ZÁZNAM

môžem požičať viac než jeden
kľúč naraz — automatizácia na
pozadí môže vždy vydať nový,
keď sa niektorý z mojich
vyžrebuje.

AUTORITA — POSKYTOVATEĽ
SLUŽBY
politika · standard · strana ·
komora

POLITIKA

VYŽREBOVANÝ
NÁHODNE, KEĎ
AUTORITA KONÁ

DELEGOVANÉ
KLÚČE —
ZASOBARENÍ

VYŽREBOVANÝ
NÁHODNE, KEĎ
AUTORITA KONÁ

nitka nikdy neopustí tvoju
ruku — v tom je celý trik.

JEDNO POTIAHNUTIE — KLÚČ SA VRACIA DOMOV



JEDEN KLÚČ VYŽREBOVANÝ
NÁHODNE — KLÚČ JE MINUTÉ

DRUHÝ
AUTORIT,
KTORÉ MÔŽU
DRŽAŤ KLÚČ

odvolateľné len kým
sa kľúč nevyžrebuje.

potom musí občan vydať nový kľúč, aby si udržal postavenie
u autority — na pozadí to zvládne automatizácia.



POLITICKÁ
STRANA
FAK I T



NORMALIZAČNÝ
ORGÁN
BU D U T

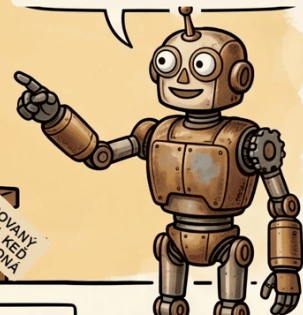


PROFESIJNÁ
KOMORA



DRUŽSTVO

autorita slúži svojim členom — nie naopak.
jedno potiahnutie nitky dohodu ukončí.



POŽIČAJ KLÚČ — NECHAJ SI NITKU. DELEGOVANIE NIKDY NIE JE ODOVZDANIE.

■ Sloboda vs. totalita

Spoločnosť, ktorá dozerá na objem zverejnených záznamov a obmedzuje ho, bude slobodnejšia; spoločnosť s nadbytkom záznamov bude inklinovať k totalite. Dá sa uvažovať o delegovaní práva zverejňovať záznamy na niekoho iného.

Kultúrna adaptácia

Ľudia si vo všeobecnosti radi nazerajú na taniere. Naprieč civilizáciami sa líšime historickou skúsenosťou a hustotou obyvateľstva — a teda aj tým, ako veľmi si chceme v rámci civilizácií a komunít nazeráť na taniere. Ázijské štáty inklinujú k prísnejšiemu pohľadu na slobodu v spoločnosti; európske a americké, v určitých aspektoch, k slobodnejšiemu. Akokoľvek nepresná táto paralela je, v kontexte decentralizovanej reputačnej sociálnej siete sa dá povedať, že nastavenia jednotlivých komunít nediskriminujú a každá komunita si môže komunikáciu v sebe nakonfigurovať, ako uzná za vhodné.

Napriek rozdielom budú existovať štandardy uznávané naprieč planétou (náhodné zabíjanie nie je dobré pre nikoho). Iné nastavenia budú špecifické pre komunitu a ešte ďalšie dokonca osobne špecifické. Výhodou je, že cez vzájomnú komunikáciu a pozorovaním nastavení svojho okolia možno hľadať konsenzus — od obojstranných dohôd cez komunitné a časom, vďaka ekonomickej dominancii najlepšie nakonfigurovaných komunít, aj na globálnej úrovni.

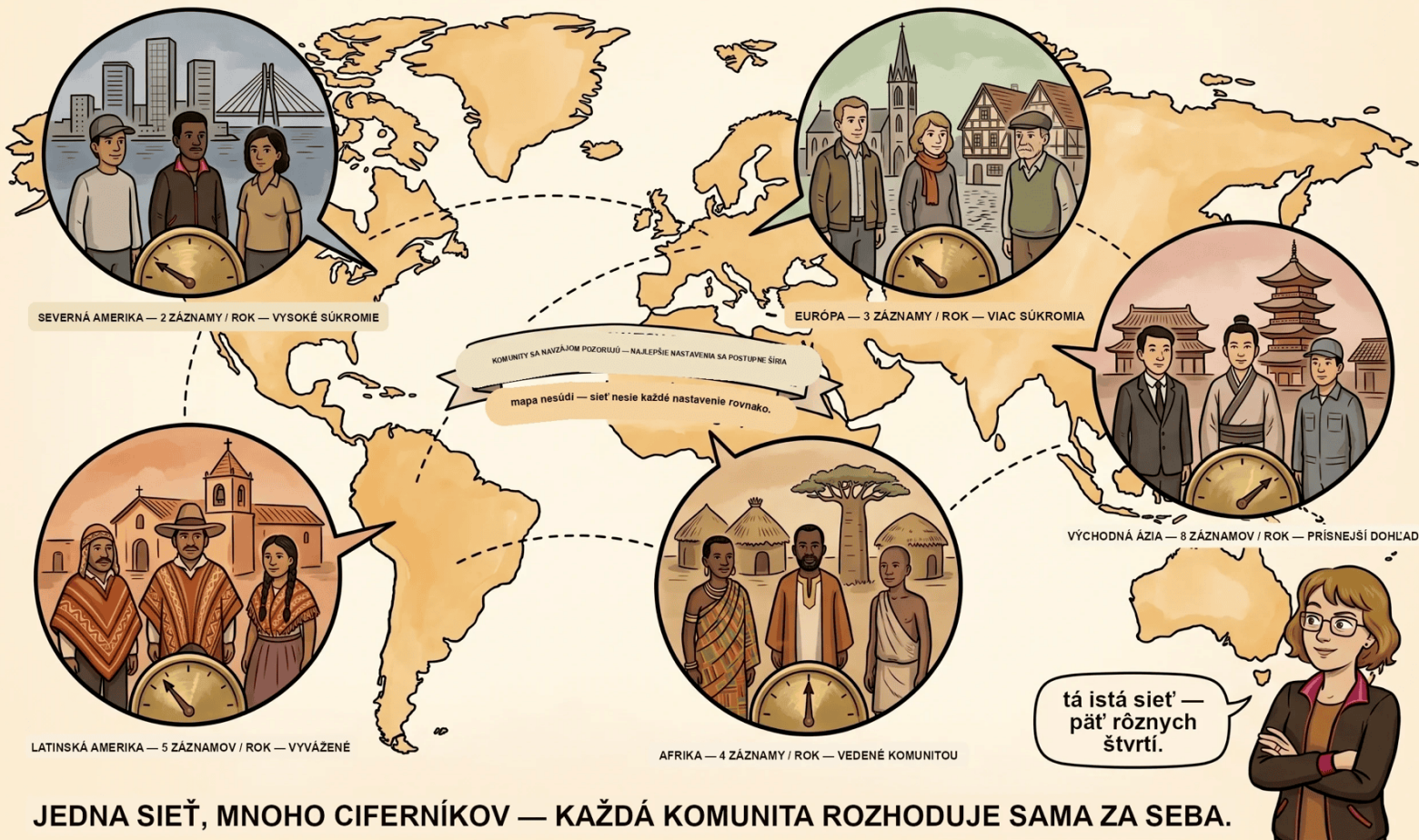
Ale o konsenze viac v ďalšej kapitole.

Problém orákula — most medzi digitálnym a fyzickým svetom

Pojem „problém orákula“ sa v poslednom čase najčastejšie spája so svetom kryptomien, blockchainov a decentralizovaných systémov. Všeobecne: ako zabezpečiť, aby dáta vstupujúce do digitálneho systému

KAŽDÁ KOMUNITA SA KONFIGURUJE SAMA

SIEŤ NEDISKRIMINUJE — KAŽDÝ REGIÓN SI NASTAVUJE VLASTNÝ CIFERNÍK



verne zodpovedali tomu, čo sa naozaj stalo vo fyzickom svete? Systém samotný nedokáže overiť, či niekto naozaj niekomu ublížil alebo či bola zmluva skutočne porušená — vidí len digitálne záznamy.

Tu to riešime cez authority — subjekty, ktoré vsadia svoju reputáciu na to, že digitálny záznam zodpovedá fyzickej realite. Čím vyššia reputácia authority, tým dôveryhodnejší záznam.

PREMOSTENIE DIGITÁLNEHO A FYZICKÉHO SVETA

AUTORITA PRENÁŠA REALITU NA DRUHÚ STRANU



Reputácia autority robí digitálny záznam dôveryhodným.

- * Systém sa nesnaží vyriešiť problém orákula — prijíma, že autority sú mostom, a zosúladzuje sa s tým, ako dôvera funguje v reálnom svete.
- * Ak sa most o realite mylí, autorita platí — svojou reputáciou.

Ako funguje overovanie

Konsenzus a proces overovania

Pri budovaní konsenzu o tom, ktoré pravidlá by mala spoločnosť v priemere dodržiavať a vymáhať, môže pomôcť nasledujúci mechanizmus. Ako účastník DID deklarujem pravidlá, ku ktorým sa hlásim a podľa ktorých budem žiť, a zverejním ich. (Predstav si to ako stanovky a poriadky, ktoré podľa mňa tvoria môj ideálny svet — svet, kde sa necítim obmedzený, ale bezpečne.)

Vopred si viem odhadnúť, ako by moje DID kontakty zareagovali — a posúdiť, ako silno a kým by som bol sankcionovaný v bežných spoločenských či obchodných interakciách, keby k nim hypoteticky došlo.

Definitívne vyhodnotenie prebehne, keď si vyžiadaš informáciu od iného DID alebo ho požiadaš o overenie tvrdenia (prípadne požiadaš autoritu o službu a podobne), ktoré chceš zverejniť do reputačnej siete. Malo by to dopadnúť rovnako, ako keď si vyhodnotenie spustíš sám nanečisto oproti deklarovanej politike protistrany — a ak nie, niečo je na strane protistrany zle: pokúša sa hrať nečestnú hru.

Výsledkom je buď prijatie s vyčíslenou cenou za overenie (v prípade služieb overovateľa alebo autority), alebo zamietnutie. Sankcie aj bonusy za odchýlku od politiky vyhodnocovateľa sú zapracované do vyčíslenej ceny. Žiadateľ potom rozhodne, či prijme podmienky, alebo prejde na ďalšie kolo overovania v alokačnom algoritme — a proces opakuje, kým nie je spokojný, alebo kým ekonomika nespraví ďalšie pokračovanie nezmyselným.

Sociálny graf

Reputačná sieť je v prvom rade sociálna sieť. Pridávaš si kontakty — ľudí, ktorí so spojením súhlasia. Oni majú kontakty a tie kontakty majú kontakty. Algoritmus hľadá overovateľov do konfigurovateľnej hĺbky (napr. tri úrovne: tvoje priame kontakty, ich kontakty a jednu úroveň za nimi). Nie je potrebný žiadny globálny blockchain — sieť prirodzene tvorí komunity s presahmi do iných komúní.

Algoritmus je nedeterministický: zhashuje tvoj dokument s tvrdením, namapuje hash na pozíciu na ringu známych identít v tomto okruhu a vyberie najbližšiu ako kandidáta na overovateľa. Nemôžeš predpovedať ani ovplyvniť, kto tvoje tvrdenie overí.

Každé zamietnutie overovateľa zväčšuje tvoj dokument a zvyšuje náklady na jeho spracovanie — to je prvý nákladový kanál (rast dokumentu). Každý nový overovateľ účtuje poplatok podľa objemu dát, tvojej reputácie a toho, ako ďaleko sa obsah tvojho tvrdenia odchyľuje od jeho deklarovanej overovacej politiky — to je druhý nákladový kanál (riziková prirážka). A každá iterácia stojí čas a energiu — tretí nákladový kanál.

■ Čo overovateľ kontroluje, v poradí

Po výbere vyhodnocuje overovateľ tvrdenie v zhruba štyroch usporiadaných krokoch — najlacnejšie filtre najprv, drahé kontroly obsahu naposledy:

1. **Filtrovanie politikou.** Spadá tento druh tvrdenia vôbec do toho, čo overovateľ verejne overuje? Ak nie, žiadosť je rovno zamietnutá.
2. **Dôvera k autorite.** Je autorita, ktorá tvrdenie zaštitila, dostatočne dôveryhodná podľa vlastnej deklarovanej politiky overovateľa? Autorita pod prahom dôvery overovateľa je dôvodom na zamietnutie bez ohľadu na obsah tvrdenia.
3. **Reputácia vydavateľa.** Splňa vydavateľ reputačné prahy, ktoré overovateľ deklaroval pre tento typ tvrdenia? Nízka reputácia môže buď zvýšiť poplatok, alebo spustiť zamietnutie.
4. **Kontrola obsahu.** Až keď prejdú prvé tri brány, overovateľ vyhodnotí samotné tvrdenie — podpisy, vnútornú konzistentnosť, formálnu správnosť a to, ako ďaleko sa odchyľuje od politiky overovateľa. Poplatok účtovaný za tento posledný krok odzrkadľuje skutočne podstúpené riziko.

Overovateľ zverejňuje politiku, ktorá riadi každú z týchto brán, takže kroky nie sú na jeho ľubovôli — je viazaný tým, čo už deklaroval. Odchýlka od zverejnenej politiky je sama zverejniteľným tvrdením proti nemu a platí za ňu svojou reputáciou.

Výsledok: zverejnenie dôveryhodného a užitočného tvrdenia nestojí takmer nič. Zverejnenie radikálneho tvrdenia stojí viac. Zverejnenie lži sa stáva neúnosne drahým — musíš iterovať cez overovateľa za overovateľom a každý, kto ťa zamietne, pridáva náklady. Trh ocení tvoje tvrdenie a cena ti povie, kde stojíš vo vzťahu ku komunitám, v ktorých sa pohybuješ.

Nestačí deklarovať, že dodržiavaš pravidlo, keď ho v skutočnosti nedodržiavaš. V takom prípade tvoj DID riskuje zverejnenie negatívneho záznamu odhaľujúceho pokrytectvo — ktorý ťa robí rizikom pre všetkých ostatných. Výsledkom by malo byť menej, ale dôslednejšie dodržiavaných pravidiel a vyčistenie tej džungle zákonov a predpisov, v ktorej sa sotva vyznajú aj právni profesionáli.

Konsenzus vs zodpovednosť

Aby sieť slúžila ako cenný zdroj informácií, nemal by byť DID príliš radikálny — inak ho ostatní zamietnu. Sociálny tlak bude hľadať rovnováhu a pokusy o jej rozkolísanie budú pravdepodobne potrestané.

SIEŤ POTICHU POROVNÁVA TVOJE SLOVÁ S TVOJÍM ZÁZNAMOM — MEDZERA JE VIDITEĽNÁ PRE VŠETKÝCH



LIEK NA POKRYTECTVO

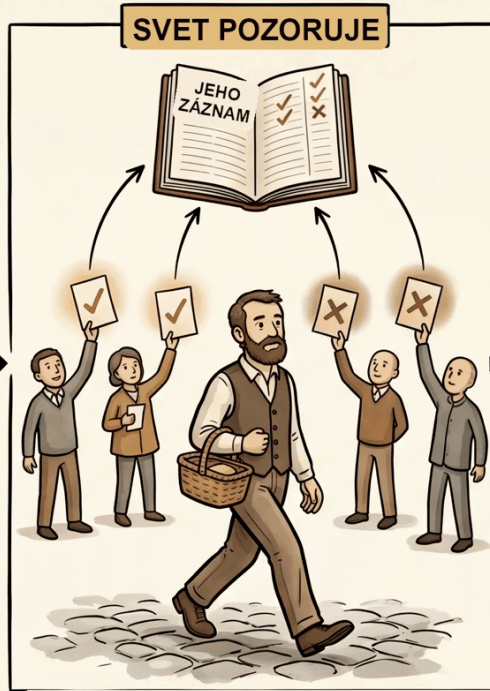
DEKLARUJ SVOJE PRAVIDLÁ — ŽI PODĽA NICH, INAK ŤA TRH VYČENÍ VON

DEKLARUJEM SVOJU
POLITIKU



každý si môže prečítať moje štandardy.
žiadni vrátnici, žiadne tajomstvá.

SVET POZORUJE



svet si zapisuje, čo naozaj robí.
každý deň o niečo viac dôkazov v jeho registri.

V OBCHODE — PLATÍŠ ZA VLASTNÝ ZÁZNAM



pokrytectvo netrešťa autorita — oceňuje ho trh.
každá bežná služba, ktorú kúpiš, nesie prírážku
formovanú tvojim vlastným záznamom.

MOHLI BY SME TOTO NAZVAŤ SPOLOČENSKOU ZMLUVOU — PREKRESLENOU?

etiku nevynucuje žiadna autorita — vynucuje ju cena.
jemný tlak, každý deň, smerom k spoločnému príemeru, s ktorým vieme všetci žiť.

KONAJ, AKO HOVORÍŠ — ALEBO ZA TO ZAPLAŤ. POKRYTECTVO JE NAJDRAHŠIA REPUTÁCIA.

■ Počet hlasov nie je to isté ako váha hlasu

Juraj Karpiš hovorí, že „peniaze sú pamäťou dobrých skutkov.“ Ja by som dodal, že reputácia je pamäťou tých zlých.

Z toho vyplýva, že meritokraticky si ten, kto prispieva viac a nemá zlú reputáciu, zaslúži väčšiu váhu hlasu v komunite. Cez optiku obojstranných vzťahov: keď zvažujem, ktorým konsenzuálnym tlakom vyhovieť, najväčšia váha patrí vzťahom, z ktorých mám najväčší ekonomický prospech. Desať ľudí, s ktorými nemám žiadny aktívny obchod, ma ovplyvní oveľa menej ako jeden stály obchodný partner. Táto paradigma sa neobmedzuje na obchod — rozširuje sa na sociálne, politické a iné vzťahy.

Roles in the verification transaction and authorities

Prehľad rolí

Niektorých z týchto rolí sme sa už krátko dotkli v kapitole o sieti a jej základných vlastnostiach. Teraz je čas pozrieť sa na ne opäť podrobnejšie a doplniť ďalšie, ktoré potrebujeme, aby sme sieť spravili robustnejšou. Každá overovacia transakcia zahŕňa niekoľko rolí — pozrime sa, ako sa správajú.

■ Roly v overovacej transakcii

Každé overenie zahŕňa až šesť odlišných rolí, zhrnutých v tabuľke nižšie. Všetky môžu mať svoj vlastný DID v decentralizovanej reputačnej sieti.

Rola	Opis
Vydavateľ	Osoba, ktorá zverejňuje informáciu do siete — tvrdí, že sa niečo stalo (DID bol vytvorený, upravený alebo zrušený, tvrdenie, politika daného DID atď.)
Subjekt	Osoba, ktorej sa informácia týka — adresát tvrdenia
Autorita	Dôveryhodný subjekt, ktorý vsádza svoje meno na kvalitu tvrdenia tým, že ho vyšetrí a buď preskúma predložené dôkazy, alebo ich aktívne zhromaždí
Pozorovateľ	Nezávislá tretia strana, ktorá vedie záznam o tom, ako overovateľ s tvrdením naloží — dbá na to, aby overovateľ ani nemlčal, ani sa neodchýlil od deklarovanej politiky
Overovateľ	Algoritmicky vybraný účastník, ktorý spracuje transakciu
Delegát	Osoba konajúca v mene iného účastníka

Vydavateľ

S vydavateľom sme sa už stretli. Keď je niekomu ukrivdené alebo chce dať vedieť o vlastnom úspechu, je to osoba zastúpená DID, kto spustí proces vloženia tej informácie do siete — pretože má na tom primárny záujem (motiváciou je buď túžba po zadosťučinení, alebo želanie zlepšiť si verejný obraz).

■ Pozitívne tvrdenia

Pozitívne tvrdenia o sebe si môžeme ako ich subjekt aj vydavateľ podržať pre situácie, v ktorých ich chceme použiť (diplom, potvrdenie o poskytnutej službe atď.). Práve v tomto sa pozitívne tvrdenie líši od negatívneho: zdieľanie overeného negatívneho tvrdenia je v záujme celej komunity, zatiaľ čo pozitívne je v záujme jeho nositeľa.

Autorita

Autorita zohráva dvojité rolu: môže byť **audítorm** (overuje kvalitu dôkazov pred zverejnením tvrdenia) alebo **garantom** (vsádza svoju reputáciu na pravdivosť tvrdenia). V oboch prípadoch posilňuje tvrdenie vydavateľa. Tieto dve služby sú oddeliteľné — autorita môže ponúkať jednu, druhú alebo obe naraz. Pracovný predpoklad je, že väčšinu služieb poskytovaných autoritami možno dodávať na báze voľného trhu. Platí to aj v oblastiach, ktoré si ťažko predstaviť sprivatizované, ako je súdnictvo, kde špecializované služby — vyšetrovanie, hodnotenie dôkazov, až po služby dnes poskytované centralizovanými armádami (strategické plánovanie, štandardizovaný výcvik, obstarávanie a správa zásob atď.) — dokážu efektívne dodávať trhoví aktéri. Sotva existuje niečo, čo by sa po reštrukturalizácii nedalo spraviť efektívnejším pomocou stimulov voľného trhu.

AUTOR · PODPISOVATEĽ · RUČÍ VLASTNOU REPUTÁCIOU

1. Napíše tvrdenie vlastnými slovami
2. Zhromaždí dôkazy z reálneho sveta na jeho podloženie
3. Podpíše ho vlastným DID a odošle vybranej autorite
4. Zaplatí náklady na zverejnenie
5. Nesie následky, ak klame

**Ak je to lož, moja
ručička klesne.**

**Íde o moje meno.
Radšej si bud' istý
— a prines dôkaz.**

**Hovorit' môže ktokoľvek.
Lži stoja rečníka.**

KOMU:
AUTORITE
PODĽA MÔJHO
VÝBERU

podpísané
mojim DID

ĎALŠÍ KROK
požiadat autoritu
aby posúdila
dôkazy a podpísala
tvrdenie

svědecká
výpověď

AUDIOKAZE 1A

Vydavateľ je autor. Je na tom jeho meno.

*** Vydavateľom môže byť ktokoľvek s DID. Latkou je odvaha a zodpovednosť, nie licencia.**

■ Autorita, vydavateľ a pozorovateľ nesmú byť nikdy overovateľom vlastného prípadu.

Algoritmický výber overovateľa zaručuje nezávislosť. Nikto nemôže overiť vlastné tvrdenie ani tvrdenie, na ktorom má priamy záujem. Toto je jedno zo základných pravidiel, ktoré má záujem dodržiavať celá komunita DID.

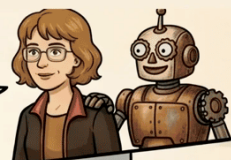
Nasledujúce grafiky ukazujú vzájomne sa dopĺňajúce pohľady na šírku činnosti, ktorú autority pokrývajú (pojem „autorita“ možno čítať zameniteľne s „poskytovateľ služby“).

SPRIEVODCA — POMÁHA TI ORIENTOVAŤ SA PODĽA TVOJICH HODNÔT

HĽBKOVÁ ANALÝZA VZADU · JEDNODUCHÉ VEDENIE VPREDU

SPRIEVODCA

Agreguje zložitý svet do odporúčaní. Nasledovníci hlasujú svojou pozornosťou — odísť môžu kedykoľvek, prejsť k inému.



MOJA ANALÝZA

Pracovné poznámky — nie pre klientov

verejné výdavky
— presmerované



Zložitú prácu robím ja. Ty dostaneš jednoduché odporúčanie — len ak zdieľaš moje hodnoty.

	poskytovanie	
1	70M	☆☆☆☆
2	70M	☆☆☆☆
3	70M	☆☆☆☆
4	70M	☆☆☆☆

PRE TEBA — ČO TO ZNAMENÁ

Agregované fak. aby maximalizoval tvoj prospech

- presuň výdavky sem, ušetri tam
- podpor poskytovateľov, ktorí prejdú moji testami
- prijmi túto šablónu politiky



A čo presne za svoje peniaze dostanem — ktoré analýzy a ktoré prehľady?

napríklad: kto môže byť sprievodca

- politická strana alebo hnutie zverejňujúce šablónu politiky
- nezávislá auditorská firma zverejňujúca agregované zistenia
- agentúra porovnávajúca služby
- agregátor reputácie (ekonomika · biznis · susedstvo · cestách)
- novinár-recenzent alebo služba spotrebiteľských recenzií

Viazaný tím, za čím verejne stojíš. Tvoja dôvera je jeho menom.

* Odísť môžeš kedykoľvek a prejsť k inému sprievodcovi. Tvoja dôvera nie je uzamknutá.

* Sprievodca môže podpísať aj nejaké vlastné tvrdenia — zverejnené, no nie sú tu hlavným príbehom.

■ Autorita ako inkognito pozorovateľ

Renomovaná autorita — predstav si notára, ktorého biznis závisí výhradne od jeho track recordu — môže popri hlavných funkciách (audítor / garant) ponúkať tretiu: rolu inkognito pozorovateľa počas overovania. Vedie časovo označovaný záznam o predložennom tvrdení, aby ho overovateľ nemohol potichu zahodiť. Mechanizmus roly pozorovateľa je opísaný ďalej v časti o roli Pozorovateľ.

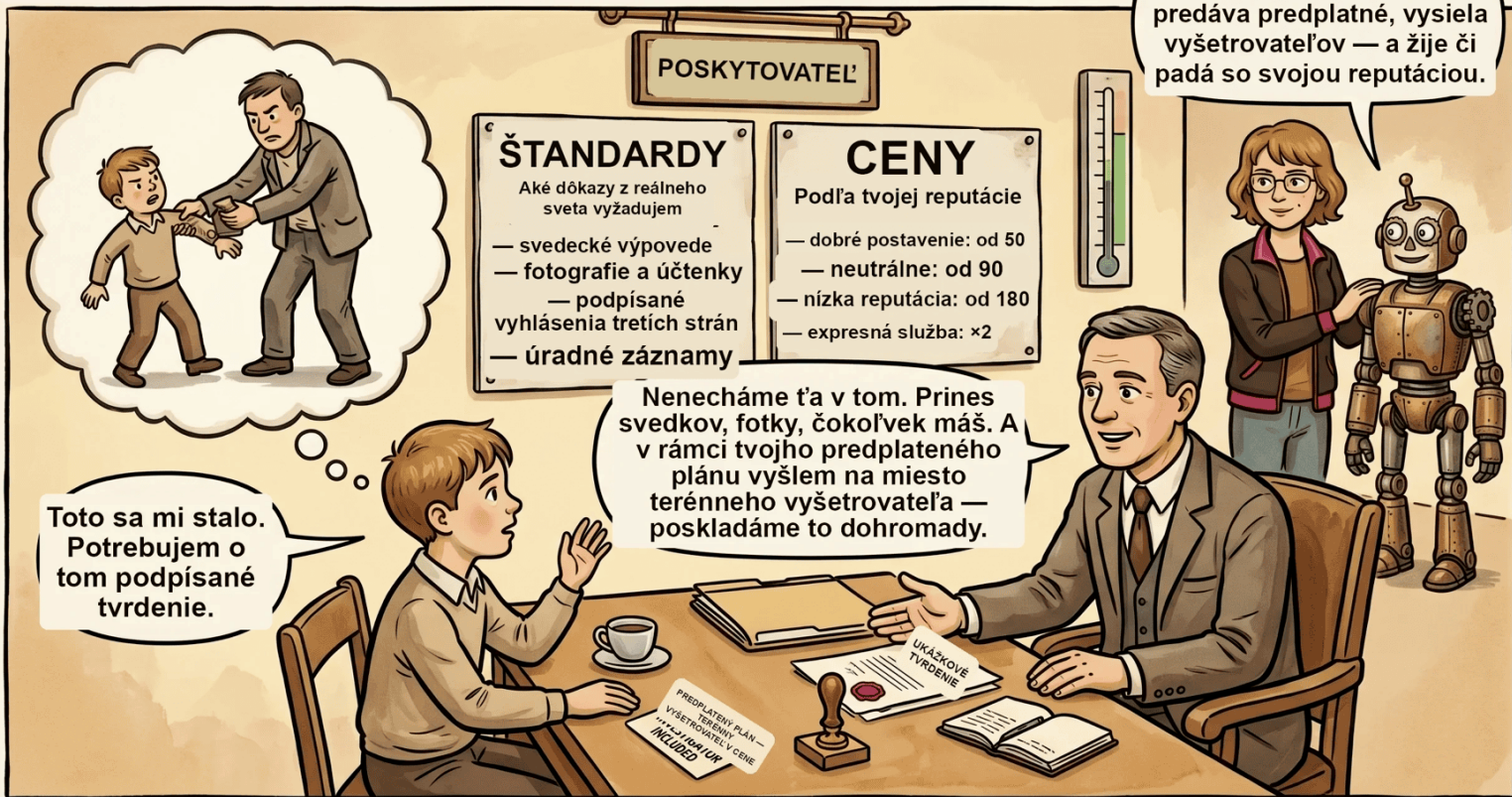
Overovateľ

Ako overovateľ môže vystupovať ktorýkoľvek DID, buď priamo, alebo cez overovacie práva delegované na tretí DID. Aby som ja — alebo môj delegát — mohol overovať, mal by som byť dosiahnuteľný v sieti (online). Nie každý sa k tomu bude chcieť zaviazať, a preto môže záznam DID uvádzať v poradí priority náhradníkov, ktorí budú funkciu vykonávať v jeho mene, kým je offline.

Každý DID aktívny v sieti verejne deklaruje svoju vlastnú politiku. Cez pravidlá definované v tejto politike posudzuje počas procesu overovania reputáciu protistrany a obsah a formu tvrdenia, ktoré vydavateľ označil na zverejnenie do reputačnej siete. Súčasťou politiky je výpočtový vzorec používaný na výpočet poplatkov za overovacie služby. Keď je to na mieste, tak naprieč štatisticky veľkým počtom tvrdení prúdiacich sieťou čakám, kým ma algoritmus siete potiahne na stranu vydavateľa a priradí ma v danej iterácii na overenie vydávanej informácie. Vydavateľ si vopred vie vypočítať, ako by sa správne konajúci overovateľ zachoval, ale nemôže sa vyhnúť tomu, aby ho (alebo jeho náhradníkov) skutočne

POSKYTOVATEĽ — PREVÁDZKUJE SLUŽBU PODPISOVANIA TVRDENÍ

ZVEREJNENÉ ŠTANDARDY · ZVEREJNENÉ CENY



Viazaný tým, čo verejne deklaruje. Zvyšok urobí reputácia.

* Poskytovateľ má aj vlastnú politiku — kedy prijme, kedy zamietne, ako refunduje. Je zverejnená, no nie je tu hlavným príbehom.

kontaktoval; iteráciu s vybraným overovateľom musí vydavateľ vykonať aj vtedy, keď vopred vie, že neprejde.

Ako vieme, že vydavateľ spúšťa algoritmus výberu overovateľa nad správnu množinou kandidátskych DID overovateľov? Spolu so svojou verejne deklarovanou politikou každý DID zverejňuje aj aktuálny zoznam identifikátorov svojej sociálnej siete v rámci reputačnej siete. Ak vydavateľ definuje svoju sociálnu sieť ako sociálnu bublinu, ktorá len prizvukuje a posilňuje jeho vlastné názory, informácia zverejnená cez ňu bude len ťažko širšie prijatá inými komunitami. To, že sa mi za vysokú cenu podarí pretlačiť radikálne tvrdenie do siete, neznamená, že mu pri posudzovaní reputácie protistrany dám nejakú váhu. Niektoré tvrdenia som svojou komunitou tlačný brať do úvahy (tresty a obmedzenia uložené previnilcom); iné sú úplne na mne — sám rozhodujem o ekonomickej hodnote zahrnutia alebo vylúčenia danej informácie.

Subjekt

Tí, ktorých sa informácia zverejnená do reputačnej siete týka, sú jej nositeľmi, alebo ak chceš, jej subjektmi. Stimuly v reputačnej sieti sú nastavené tak, aby mal subjekt každý dôvod správať sa správne a férovo podľa vlastných pravidiel a aby ho komunita tlačila k akémusi zlatému strelu dodržiavania pravidiel. Má dokonca stimul správať sa morálnejšie, než vyžadujú jeho deklarované pravidlá — vopred deklarované politiky nevylučujú, aby komunita dospela ku konsenzu uplatniť nejaké hodnotenie alebo opatrenie spätne. Z tohto uhla je reputačno-sieťová alternatíva právneho poriadku, ako sa dá čakať, poháňaná viac duchom pravidiel než ich literou.

OVEROVATEĽ — POSUDZUJE TVRDENIE PODĽA ZVEREJNENEJ POLITIKY

ŠTYRI BRÁNY, PO PORADÍ. LACNÉ FILTRE NAJPRV.

Nesmie byť kreatívny. Musí robiť to, čo hovorí jeho politika.

Jeho vlastné pravidlá. Verejné. Nemôže ich potajomky zmeniť.

OVEROVACIE BRÁNY — PO PORADÍ

1. FILTROVANIE POLITIKOU

Overujem tento druh tvrdenia vôbec?

2. DÔVERA V AUTORITU

Je autorita nad mojím prahom?

3. REPUTÁCIA VYDAVATEĽA

Spĺňa vydavateľ moju latku reputácie?

NEMÔŽE BYŤ: vydavateľ, autorita, pozorovateľ ani subjekt.

4. KONTROLA OBSAHU

Podpisy, konzistencia, odchýlka od politiky

REPUTÁCIA OVEROVATEĽA

ODCHÝLIŤ SA OD POLITIKY → REPUTÁCIA KLEŠÁ → ŽIADNE BUDÚCE VÝBERY

ČO OVEROVATEĽ ROBI

1. Filtruje podľa svojich zverejnených brán politiky (po poradí)
2. Kontroluje dôveru v autoritu, potom reputáciu vydavateľa
3. Vyhodnocuje obsah tvrdenia, len ak brány prejdú
4. Účtuje poplatok úmerný riziku
5. Ručí vlastnou reputáciou pri každom rozhodnutí

POPLATOK ∝ RIZIKO

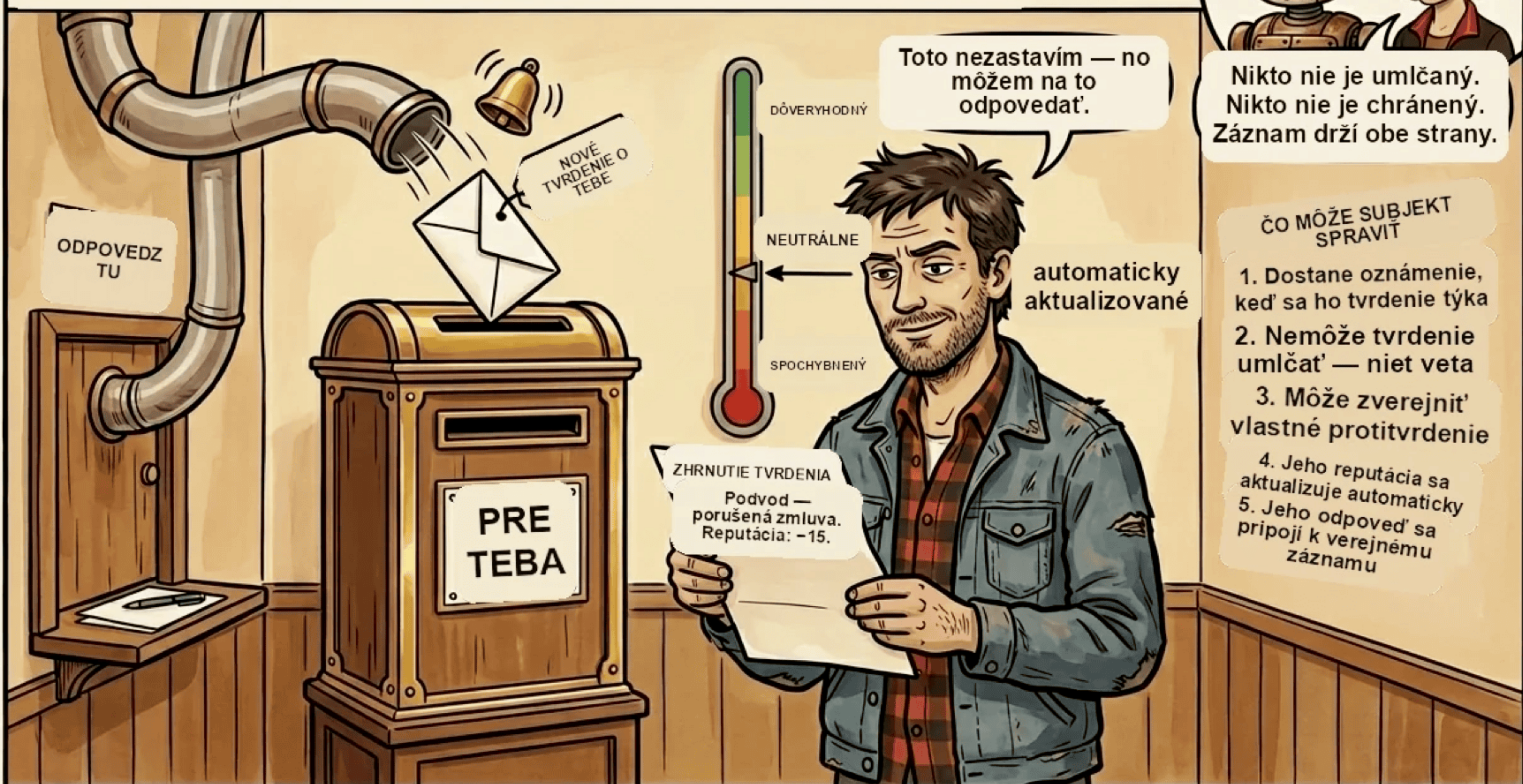
viac rizika → väčší poplatok

Lacné filtre najprv. Drahá kontrola obsahu naposledy.

Overovateľ je viazaný pravidlami, ktoré sám zverejnil — a reputáciou, o ktorú môže prísť.

SUBJEKT — TEN, O KOM TVRDENIE HOVORÍ

DOSTANE HO · NEMÔŽE HO UMLČAŤ · MÔŽE NAŇ ODPOVEDAŤ



Subjekt nemá veto — len právo odpovedať

* Protitvrdenie je samo osebe tvrdenie — reputácia subjektu je v hre za to, čo v odpovedi povie.

Pozorovateľ

Rola pozorovateľa odstraňuje overovateľovi stimul ohýbať pravidlá. V situáciách, keď sa overovateľovi žiadosť vydavateľa alebo autority nepáči, mohol by jednoducho mlčať — neodpovedať a zablokovať algoritmicke postupnosť. Pozorovateľ — alebo množina pozorovateľov — vsádza svoju reputáciu na zdokumentovanie toho, ako bol overovateľ oslovený. Ak overovateľ napriek deklarovanej politike, ktorá hovorí opak, mlčí, možno ho usvedčiť z porušenia protokolu.

Mechanizmus: časová pečiatka a výzvodný kód

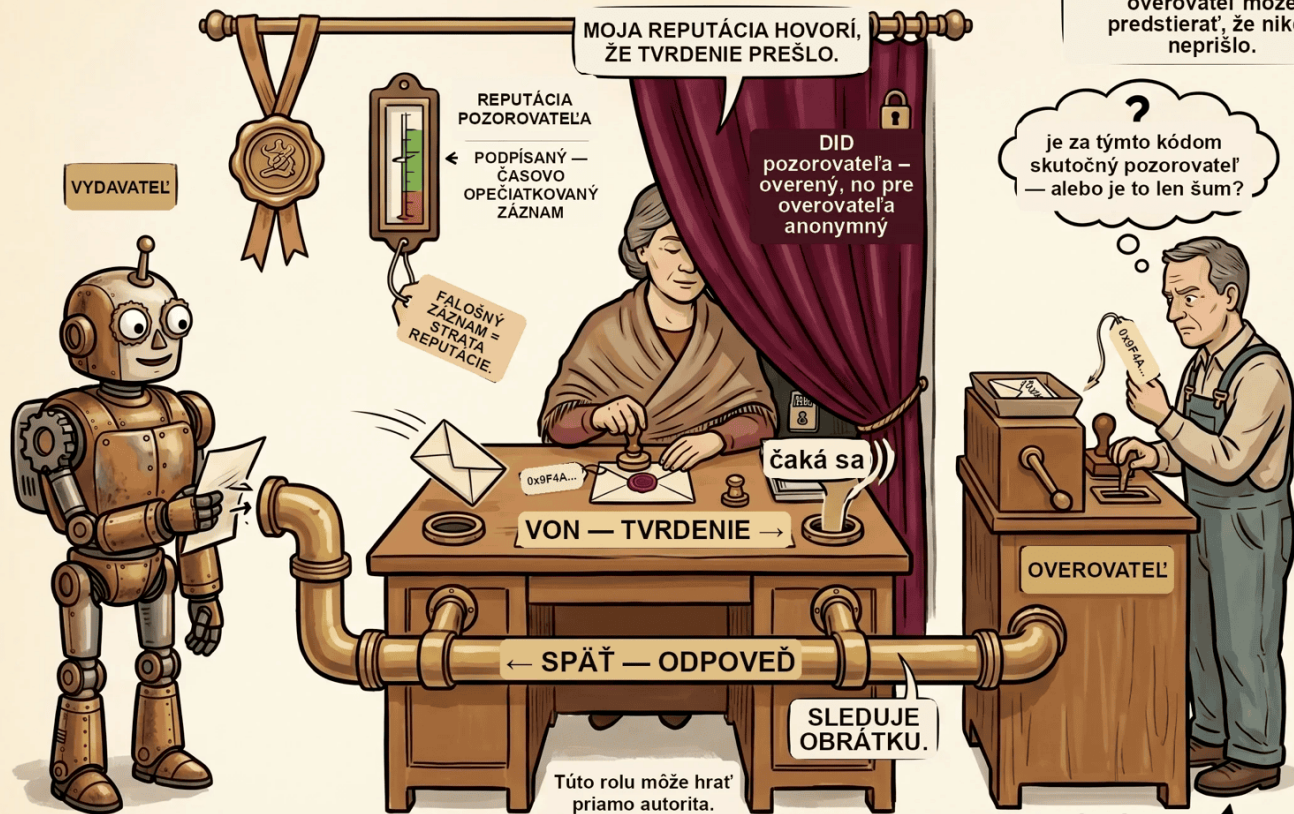
Predtým, než pošleš tvrdenie overovateľovi, presmeruješ ho cez pozorovateľov — ľudí, ktorým dôveruješ, alebo špecializovaných poskytovateľov pozorovateľských služieb, ktorí si účtujú malý poplatok. Každý pozorovateľ dostane tvoje podanie, opečiatkuje ho časom, podpíše, že videl, ako odchádza, a vygeneruje výzvodný kód — kryptografický hash svojho podpisu. Kódy sa pripoja k tvojej žiadosti. Overovateľ ich vidí, ale nemá tušenia, kto sú pozorovatelia, ani či sú kódy vôbec reálne. Pozorovatelia tak pôsobia ako sprostredkovatelia medzi vydavateľom a overovateľom, ktorí držia nezávislý záznam o tom, že tvrdenie bolo podané a čo obsahovalo. Môže ich byť nula až N.

Keď sa overovateľ správa poctivo — prijíma alebo zamietá v súlade so svojou deklarovanou politikou — kódy ostávajú nepriehľadné. Nikto nie je odhalený.

Ale ak overovateľ napriek ústretovej politike mlčí, alebo odpovie spôsobom, ktorý protirečí tomu, čo zverejnil, držíš pôvodné podpisy pozorovateľov. Môžeš ich zverejniť ako sprostredkované svedectvo, že tvrdenie bolo podané a že overovateľ nedodrжал protokol. Ktokoľvek si môže overiť, že podpisy sedia s výzvodnými kódmi.

POZOROVATEĽ — PROXY, KTORÝ TVRDENIE PRENÁŠA A SLEDUJE OBRÁTKU

OVEROVATEĽ SA ROZPRÁVA S ŇOU. OVEROVATEĽ SA NIKDY NEDOZVIE, KTO JE — ANI ČI VÔBEC NIEKTO SLEDUJE.



Ona o tvrdení nerozhoduje.
Rozhoduje o tom, či
overovateľ môže
predstierať, že nikdy
neprišlo.



ČO POZOROVATEĽ ROBÍ

1. Prijme tvrdenie od vydavateľa
2. Opečiatkuje ho vlastnou pečatou; pečiatka je časovo opečiatkovaný záznam
3. Prepošle ho overovateľovi v mene vydavateľa
4. Sleduje, či odpoveď príde späť a čo hovorí
5. Svoj podpis zverejní, len ak sa overovateľ zachová nesprávne — jej reputácia je zárukou

poznámky pod čiarou
Za každou požiadavkou môže
byť nula až N pozorovateľov.
Overovateľ vidí len nepriehľadné
kódy a nikdy nevie, či sleduje
skutočný pozorovateľ, alebo je to
len šum. Práve tá neistota je
motiváciou správať sa slušne.
* Symetricky môže overovateľ
smerovať odpoveď cez
vlastného pozorovateľa —
rovnaký trik, opačný smer.

Anonymný pre verejnosť, zodpovedný voči sieti. Overovateľ vidí kód, nikdy pozorovateľa.

Pointa: nepotrebuješ skutočných pozorovateľov

A tu je tá najelegantnejšia časť: **vôbec nepotrebuješ skutočných pozorovateľov**. Môžeš vygenerovať náhodné čísla, ktoré vyzerajú presne ako výzvové kódy. Overovateľ nerozozná rozdiel — musí hádzať kockou, či riskovať svoju reputáciu. Za každou žiadosťou, ktorú dostane, by mohol byť rešpektovaný pozorovateľ sledujúci inkognito — alebo to môže byť čistý šum. Overovateľ to nevie. A tá neistota je ten mechanizmus.

Náklady na udržanie poctivého tlaku: takmer nulové (náhodné čísla sú zadarmo). Potenciálne náklady nepoctivosti pre overovateľa: katastrofálne. Poctivé správanie je stimulované aj vtedy, keď v skutočnosti nikto nesleduje.

Systém funguje, pretože každý je trochu paranoidný. Neistota je lacnejšia než dohľad.



Viacero overovateľov v jednej iterácii

Posilňujúcim doplnkovým pravidlom pre dostupnosť overovateľa môže byť algoritmické rozšírenie, ktoré v jednej iterácii vráti množinu kandidátskych overovateľov namiesto jediného.

Delegovanie

Civilizácia postavila svoj ekonomický rast na schopnosti deľby práce a špecializácie. Svet v celej svojej nádhere je zložitý a naše šance uchopiť ho v celej jeho zložitosti sú blízke nule. Prirodzeným východiskom je delegovať širokú škálu činností podporujúcich pohodlný život na špecializovaných poskytovateľov,

BLÉF, KTORÝ UDRŽÍ OVEROVATEĽA POCTIVÝM

SKUTOČNÝ POZOROVATEĽ A NÁHODNÝ BLÉF VYZERAJÚ Z OVEROVATEĽOVHO STOLA ROVNAKO

vydavateľ — kamila

skutočný pozorovateľ

overovateľ

tvrdenie

výzvoový kód —
hash časovo
opečiatkovaného
záznamu

podpísaná
výzva

niekto si zapisuje,
čo tu robím?
neviem — tak sa
správam slušne.

PRIJATÉ

overovateľ nerozozná skutočný záznam od bléfu. poctivé správanie je jediná istá stávka.

vydavateľ — bléfuje

žiadny pozorovateľ

overovateľ — rovnaké správanie

náhodné číslo

náhodné číslo

vyzerá
rovnako.
cena: nula.

niekto si zapisuje, čo
tu robím? neviem —
tak sa správam slušne.

overovateľ
ich
nerozozná.

kto to
rozozná?

cena tlaku na poctivosť: takmer nulová — náhodné čísla sú zadarmo.
cena za prichytenie pri umlčaní tvrdenia: katastrofálna — reputácia zničená.

NEISTOTA JE LACNEJŠIA NEŽ DOHL'AD.

ktorí nám šetria čas, energiu a peniaze a umožňujú nám zas špecializovať sa — poskytovať služby, v ktorých sme najlepši, alebo ktoré si na nás trh cení najvyššie.

Rovnaká logika delegovania sa prenáša do reputačnej siete. V kapitole Prepínač sloboda–totalita (a delegovanie) sme vytýčili princípy zabezpečenia slobodnej spoločnosti obmedzením počtu tvrdení, ktoré možno zverejniť do siete v danom časovom okne (zjednodušene si predstav nízke jednotky práv na zverejnenie za rok, aby spoločnosť ostala maximálne slobodná). Tento princíp možno rozšíriť do viacerých dimenzií. Nemusíme mať len jedno číslo — môžeme mať niekoľko limitov platných pre rôzne typy tvrdení. Iné číslo môžeme použiť na označkovanie pokrytectva iných než na pochybenie v obchodných transakciách a povedzme zmena DID dokumentu, ako je zmena hesla, je niečo, čo komunitu sotva vôbec zaujíma, a tak ďalej. Všetko závisí od toho, ako komunita v evolučnom čase definuje, čo slúži jej záujmom pri hľadaní správnej rovnováhy medzi jej cieľovou úrovňou slobody a zodpovednosti.

Prečo by mal byť počet práv na zverejnenie udelených mi komunitou dostatočne malý? Označkovanie DID (subjektu) negatívnym tvrdením ničí reputáciu, ktorej vybudovanie trvalo dlho, a škoda pretrváva. Zničená reputácia čelí škále stupňujúcich sa sankcií od komunity za každé ďalšie alebo opakované previnenie, až po úplné vylúčenie rušivého subjektu (krajný prípad). Exponenciálne stupňujúca sa škála trestu nepotrebuje veľký objem tvrdení, pokiaľ sú podložené overiteľnými dôkazmi. Toto platí pre pokojný ustálený stav, keď spoločnosťou neotriasa katastrofa (vonkajšia alebo vnútorná).

Pri udalostiach s veľmi nízkou pravdepodobnosťou je štatistická frekvencia pri aplikácii na jednotlivca volatilná. Naprieč populáciou komunity nie je. To je hodnota delegovania svojich práv na zverejnenie na špecializované agregujúce authority, ktoré — podobne ako vzájomné poistenie v prípade škody — použijú tvoje právo a uplatnia ho v tvojom mene. Hovorme menej abstraktne a uveďme pár príkladov: - odhaľovanie a potláčanie organizovaného zločinu - vymáhanie obchodných dohôd - správa výsad (dôkazy o vzdelaní, nadobudnutia / prevody majetku atď.) - a tak ďalej

DELEGÁT — SLUŽBA TVRDENÍ, KTORÚ SI PREDPLATÍŠ DELEGUJ, ČO NEZVLÁDNEŠ SÁM · NECHAJ SI, NA ČOM TI ZÁLEŽÍ



Zver navonok, čo nezvládneš sám. Zostaň v obraze. Práva stiahni späť kedykoľvek.

* Ak delegát koná mimo dohodnutého rozsahu, verejne to zasiahne jeho reputáciu aj tvoju.

■ Ako „práva na zverejnenie“ vlastne fungujú

Grafika delegáta zobrazuje práva na zverejnenie ako fyzické žetóny pre názornosť, ale v systéme žiadny taký objekt neexistuje. V skutočnosti sa deje toto: politiky ľudí, s ktorými chceš ostať v dobrom — tvojej komunity — sa agregujú do emergentného pravidla o tom, koľko tvrdení za rok od teba prijmú ako relevantné, kým ťa začnú považovať za šum. Strop existuje na to, aby sa sieť neutopila v triviálnych tvrdeniach typu „čo keby“ a ostala taká slobodná, ako komunita chce (signál zachovaný obmedzením objemu).

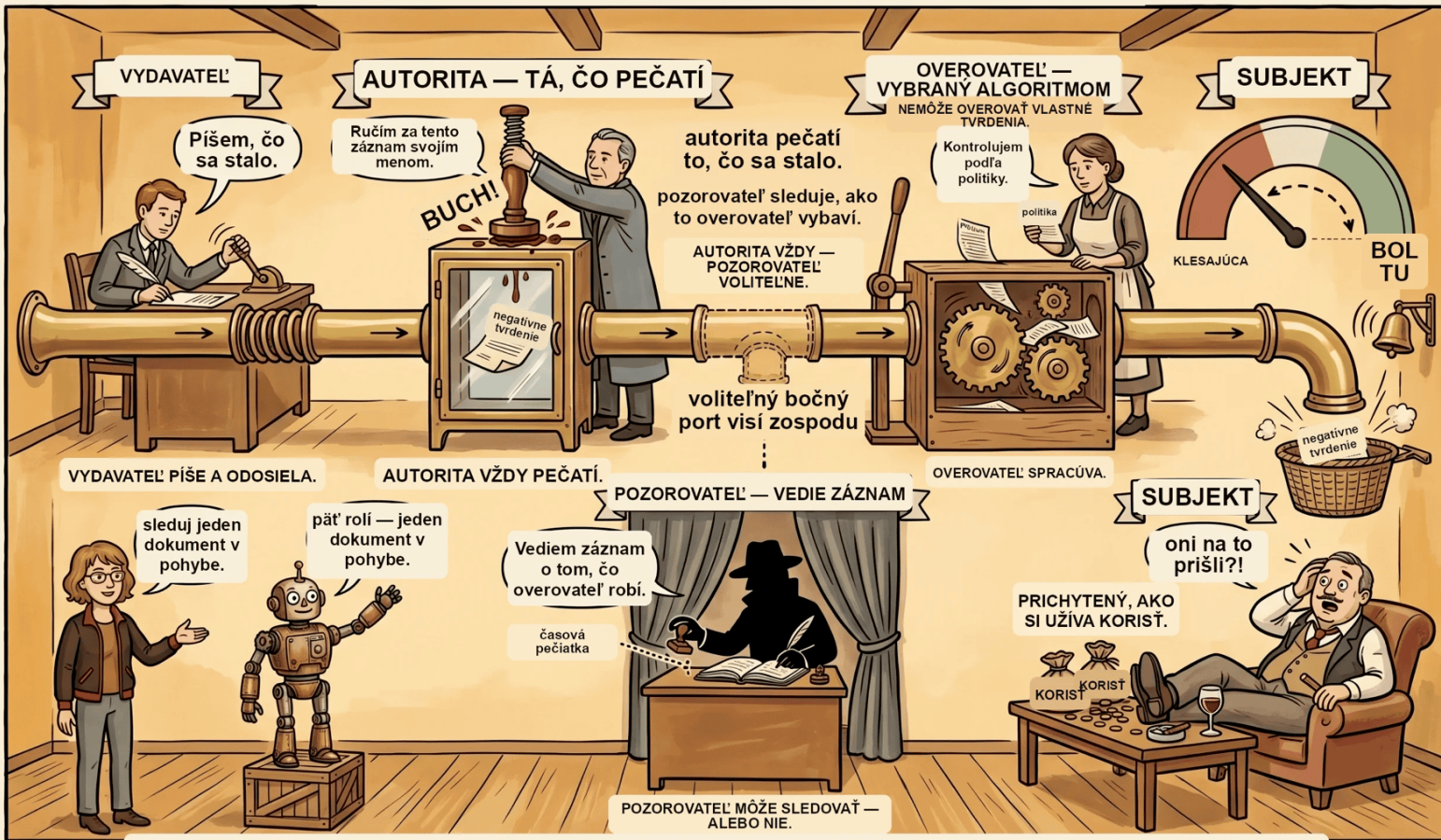
Čítaš to, čo ti tvoja komunita umožňuje. Existuje rozpätie s určitým rozptylom podľa toho, ktorých ľudí vážiš najviac. Potom sa rozhodneš — v rámci tohto povolenia — koľko tvrdení zverejniť sám a koľko delegovať na profesionálne služby, ktoré budú zverejňovať v tvojom mene len vtedy, keď udalosti spadnú do ich záberu. Práve to ťa udržiava v dobrom bez toho, aby ťa nútilo podávať tvrdenie na každú maličkosť, čo sa ti príhodi.

„Žetóny“ v grafike sú vizuálnou náhradou tejto slučky čítaj-a-rozhodni, nie doslovným artefaktom.

Oplatí sa vedieť odvolať delegované práva na zverejnenie v reputačnej sieti. Dá sa to kedykoľvek, pokiaľ delegát delegované právo ešte nepoužil.

NEGATÍVNE TVRDENIE PRECHÁDZA SYSTÉMOM

SLEDUJ JEDEN DOKUMENT — POZRI, ČO S NÍM KAŽDÁ ROLA SPRAVÍ



PÄŤ RÓL, JEDEN DOKUMENT V POHYBE — NIKTO NEMÔŽE OVERIŤ SÁM SEBA.

Komunikácia medzi rolami

Grafika nižšie zhŕňa, ako sa roly prepájajú v reálnom prípade — od podania tvrdenia vydavateľom až po zverejnenie do reputačnej siete.

Emergentná spoločenská zmluva — politika

Doteraz sme opísali, ako sa tvrdenia overujú a akú úlohu zohráva každá rola. Teraz sa obrátime k tomu, ako sa z tisícov jednotlivých politík stáva niečo, čo funguje ako skutočná spoločenská zmluva. Nič, čo by pripomínalo ľavicové sny o spoločenskej zmluve a vynútenej solidarite.

Každý účastník deklaruje svoju vlastnú politiku (policy) založenú na svojej morálke — čo považuje za prijateľné a ako reaguje na konkrétne správanie iných. Súhrn všetkých politík naprieč sieťou, ktoré daný DID pozná (komunita), produkuje emergentnú etiku — pozorovateľné normy, ktoré nikto nenavrhol. Tieto emergentné normy, podložené obojstrannými cenovými signálmi, tvoria merateľnú spoločenskú zmluvu: nie teoretický konštrukt, ktorý nikto pri narodení nepodpísal, ale empiricky pozorovateľné pravidlá podložené skutočným správaním.

■ Spoločenská zmluva

Ľudia diskutujú o tom, či „spoločenská zmluva“ nie je oxymoron. Nikto nič nepodpisuje, no odvoláva sa na ňu pri ospravedlnení legislatívnej a exekutívnej činnosti v centralizovaných spoločnostiach.

Fenomenologická analýza interakcií v decentralizovanej sieti by mohla odhaliť určité emergentné pravidlá — globálne alebo lokálne. Ako máme tieto široko zdieľané normy nazvať? Spoločenská zmluva? Rovnako ako pri komunitách nemožno spoločenskú zmluvu komunity pozorovať a vymedziť presne — každý uhol pohľadu na komunitu dáva inú spoločenskú zmluvu.

■ Hodnotovo založená politika

Rovnako zavádzajúce je brať „hodnotovo založenú politiku“ ako základ rozhodovania. Hodnoty sú skôr fenomenologické zhluky pravidiel, ktoré sa v danom čase bežne preferujú. Vyvíjajú sa a nie sú v čase konštantné.

POLITIKY SA STRETÁVAJÚ. POSTOJE SA FORMUJÚ.

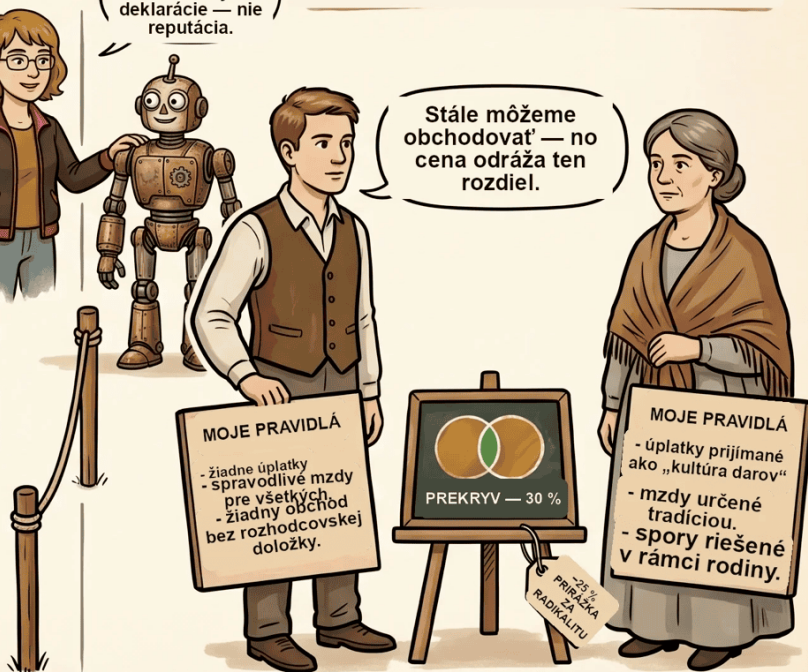
DEKLAROVANÉ PRAVIDLÁ URČUJÚ DNEŠNÚ CENU — ZĽAVA ZA SÚLAD, PRIRÁŽKA ZA ODCHÝLKU

KEĎ SA POLITIKY ZHODUJÚ



Rovnaký tovar, dve ceny. Rozhodujú deklarácie — nie reputácia.

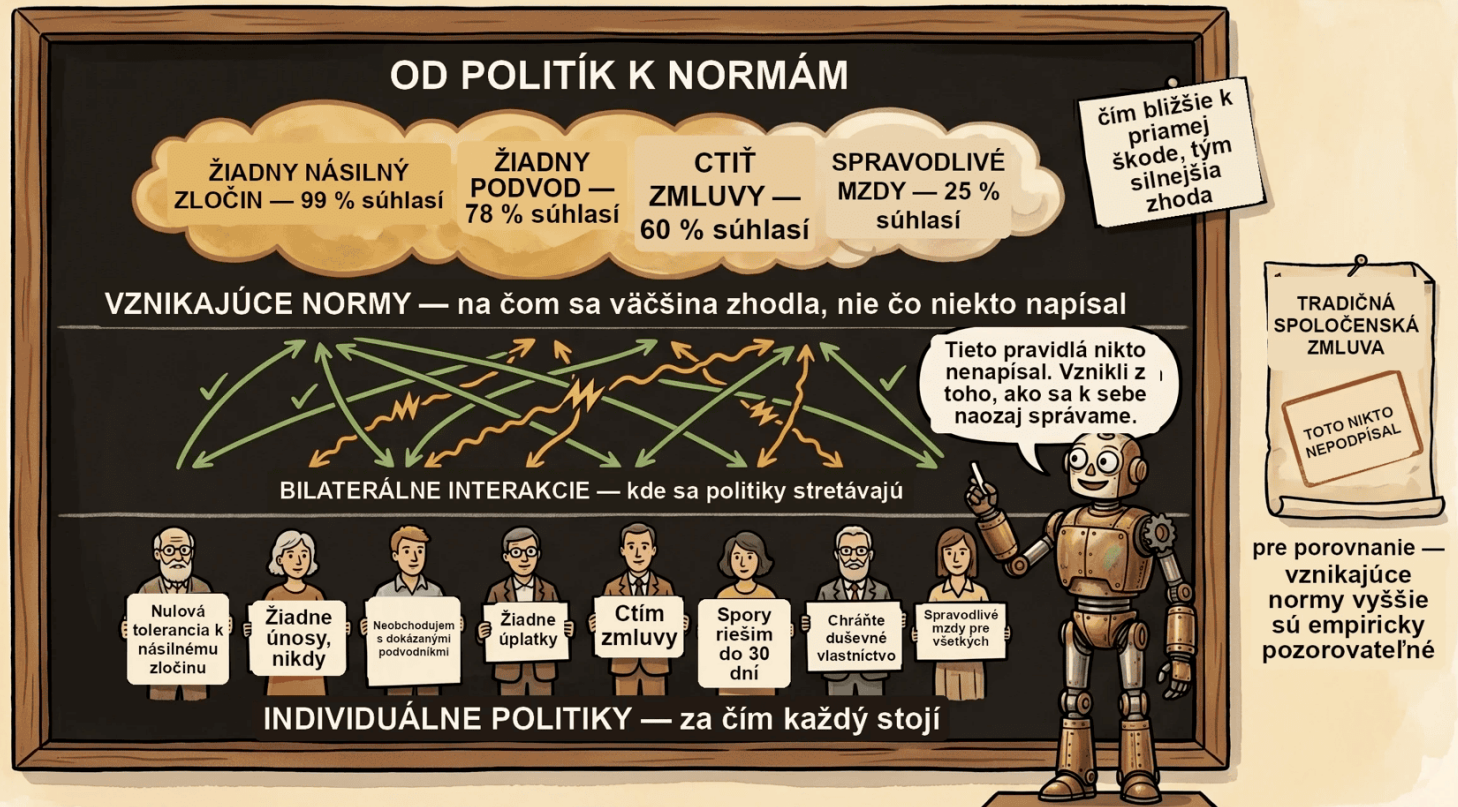
KEĎ SA POLITIKY ROZCHÁDZAJÚ



Keď sa dve politiky stretnú v obchode, ich súlad sa stáva modifikátorom ceny.

* Toto nie je o reputácii. Je to o tom, čo každý verejne deklaroval — a čo sa teraz od neho očakáva, že dodrží.

AKO ETIKA VYPLÝVA Z INDIVIDUÁLNYCH POLITÍK



Etika sa nenavrhuje. Vzniká z toho, ako sa k sebe naozaj správame.

* Každá individuálna politika je odrazom morálky danej osoby — formovaná tlakom prispôbiť sa svojej komunite a prostrediu.

Poskytovanie informácií o sebe

Keď dvaja subjekty DID, ktorí sa nepoznajú, vstúpia do ekonomického vzťahu, môžeme v mene druhej strany podpísať žiadosť na vlastnú komunitu, aby o nás poskytla informácie. Toto je však veľmi naivná predstava o tom, čo komunity sú. Nie sú to uzavreté množiny — jediný DID môže byť účastníkom viacerých komunít.

Komunita je skôr fenomenologický jav z perspektívy daného účastníka, prejavujúci sa v jeho sociálnej sieti; nie je to niečo, čo má vždy zmysel explicitne vymedzovať. Obyvatelia dediny môžu tvoriť komunitu, ale človek, ktorý tam chodí len cez víkendy, môže patriť aj do inej komunity v tej istej dedine. Komunitou môže byť aj futbalový tím spolu s fanúšikmi, funkcionármi a rodinami všetkých zúčastnených. Národ alebo občania štátu môžu tiež tvoriť komunitu či komunity. Pohľad na DID z rôznych uhlov môže dať rôzne (a často intuitívne) pohľady na komunity.

DID na hraniciach sú tak mostami medzi komunitami a — rovnako ako v reálnom živote — zohrávajú úlohu pri poskytovaní informácií o členoch iných komunít, či už na amatérskej úrovni, alebo na profesionálnej, ako autorita, ktorá sa špecializuje na spájanie ľudí a agregáciu informácií o rizikových DID.

Niektoré typy informácií v sieti DID sa dobre hodia na bezpodmienečnú vzájomnú výmenu (násilný zločin, podvod atď.). Iné typy informácií však komunita môže považovať za obmedzené na použitie v rámci komunity (ekvivalent občianstva, služby poskytnuté komunite atď.). Či sa také informácie môžu šíriť, závisí od deklarovaných politík členov komunity.

Komunita stráži svoje súkromie vo svojom okruhu a na oplátku bezpodmienečne vymieňa vzájomne prospešné informácie.

Zločin a trest

Zločin a trest

Vieme, ako sieť funguje: ako vznikajú záznamy, kto ich overuje, ako sa odrádza od podvodu overovateľa. Zostáva jedna otázka — čo sa stane, keď niekto naozaj spôsobí druhému ujmu?

Nakol'ko závisíme jeden od druhého?

Všetci stojíme na javisku tohto veľkého sveta a čokoľvek sa tu deje, všetkých sa nás týka.

Jan Amos Komenský (Labyrint sveta a raj srdca)

Dôvodov pripojiť sa k reputačnej sieti alebo ju odmietnuť môže byť mnoho. Verím však, že jeden aspekt ľudskej povahy — často považovaný za temný — dokáže poslúžiť dobrému účelu. Hovorím o ľudskej potrebe cítiť zadostučinenie zoči-voči vnímanej nespravodlivosti.

Zadostučinenie, spravodlivosť, pomsta — spájame ich s negatívnymi emóciami. Aby spoločnosť držala pokope, musíme aspoň predstierať, že zadostučinenie sa dodáva cez centralizované inštitúcie; inak by sa jednotlivci necítili spojení so spoločnosťou, v ktorej žijú. V priemere potrebujeme patriť do nejakého tímu a dôverovať mu. Keď niekto ublíži druhému, spoločnosť sleduje, ako sa zadostučinenie dodá a do akej miery. Trochu kontroverzne tvrdím, že často v dejinách — a aj teraz — nezáležalo na tom,

či bol proces proti obvinenému čistý; záležalo na tom, že spoločnosť videla potrestaného *niekoho*. Splnilo to svoju funkciu (početné justičné omyly a odpor voči znovuotváraniu starých prípadov to hovoria dosť výrečne). Pohľad obete a pozostalých je len druhoradý. Prvoradé sú signály zvyšku spoločnosti, pretože krivdy nie sú také časté, aby figurovali v dni každého jednotlivca.

Decentralizovaný reputačný systém by nechal verejnosť vidieť priame a nepriame dôkazy (auditované aj neauditované). Spoločnosť by mohla informácie vyhodnotiť — sama alebo cez služby voľného trhu špecializované na také posudzovanie — a na základe kvalitatívnych a kvantitatívnych signálov rozhodnúť, aké opatrenia uplatniť na subjekt (alebo aj na autora či overujúcu autoritu).

Čo je trest? Je to forma pokorenia údajného previnilca cez stratu jeho výsad — tak, aby aj obeť, aj spoločnosť cítili, že škodlivé činy sa neoplácajú. To je podstatný bod: škodlivé alebo nebezpečné správanie sa nesmie oplácať a zároveň musí poskytnúť pocit zadosťučinenia obetiam aj zvyšku spoločnosti/komunity.

Musí taký trest udeľovať centrálna autorita? Čo keby každý mohol vopred deklarováť, ako bude reagovať na určité činy? Zjavne nemôžem vykonať trest na cudzom majetku. Ale môžem deklarováť, že svoj majetok sprístupním vybranej množine výkonných autorít na účel potrestania previnilca, ak páchatel' vstúpi do mojich domén. A môžem to deklarováť verejne, aby ostatní mohli môj prístup vyhodnotiť.

A tu vstupuje cenový mechanizmus primeranosti. Ak deklarujem tvrdé tresty za drobné previnenia, sieť ocení môj extrémizmus: ostatní ma budú považovať za neprimeraného a moje náklady na overenie stúpnu — menej ľudí bude chcieť so mnou obchodovať, alebo len za horšie ceny, a menej overovateľov prijme moje záznamy za rozumnú cenu. Ak som naopak príliš zhovievavý, komunita ma bude vnímať ako riziko. Ak tolerujem podvod, komunita bude pravdepodobne zhovievavá voči páchatel'om činov, ktoré sa dotýkajú mňa — aby mi dala okúsiť vlastnú medicínu.

Spravodlivosť prestáva byť luxusným tovarom. Keď ti niekto ublíži, zaznamenanie krivdy je dostupné, záznam je trvalý a dôsledky pre previnilca sú reálne.

■ Odhaľovanie pokrytectva

Deklarovať politiku nestačí — ak deklarujem, že dodržiavam pravidlo, ale moje správanie sa od neho odchyľuje, tá medzera je reputačným záväzkom. Sieť nerozlišuje medzi „porušil zákon“ a „porušil vlastné slovo“ — oboje sú merateľné signály. Pokrytectvo je drahé a nepoznám dráždiviejšie červené súkno.

■ Kvantita vs kvalita — prelomenie binárnej paradigmy viny

V centralizovanej spravodlivosti je vina binárna: 0 alebo 1, vinný alebo nevinný. V reputačnej sieti nezáleží na tom, či je vina dokázaná, ale na hromadení signálov.

Jediné nedokázané obvinenie z krádeže voči obvinenému pravdepodobne nevyvolá veľkú osťažitosť — ale vyvolá osťažitosť voči obviňujúcemu. Viacero nepriamych indícií z rôznych nezávislých zdrojov však začína naberať váhu. Nezáleží len na kvantite, ale aj na kvalite: nezávislosť svedkov (rôzni ľudia, rôzne kontexty), konzistentnosť vzorca (opakujúci sa typ podozrenia), časová korelácia.

Naopak, časté bezdôvodné obvinenia, ktoré sa opakujú od toho istého vydavateľa voči rôznym cieľovým subjektom, môžu byť vyhodnotené ako ohováranie — a reputácia obviňujúceho za to zaplatí.

JEDNA PASCA. JEDNA CESTA VON.

ZASVÄTENEC VŽDY VYHRÁ ZÁKAZKU — KÝM SIET NEDOVLÍ ĽUĎOM KUPOVAŤ PRIAMO, BEZ POVOLENIA.



Verejnosť sa zhodne, že treba nový verejný IT systém, platený z rozpočtu, platený z daní.



Za zatvorenými dverami úradník pre obstarávanie a zasvätenec navrhnu tender na mieru jednej firme. Obáika mení majiteľa.



Úradník pokrčí plecami. Vrecko mu vydáva od úplatkov.



Zákazka je pridelená. Zasvätenec má licenciu — no žiadnu zručnosť a žiadnu úctu k práci.



Zasvätenec navštívi suseda. „Láskavá ponuka“ je najmenší omrvinkou.

1. TRADIČNÉ



Sťažnosť, ticho, lehoty, právnik.

Pasca je zabudovaná do samotných pravidiel.



2. SIET REPUTÁCIE



Najprv dodá. Ľudia aplikáciu nájdu a používajú ju. Každý vďaka používateľ' zaplatí trochu. Slušné živobytie. Žiadna centrálna autorita, ktorú treba podpísať.

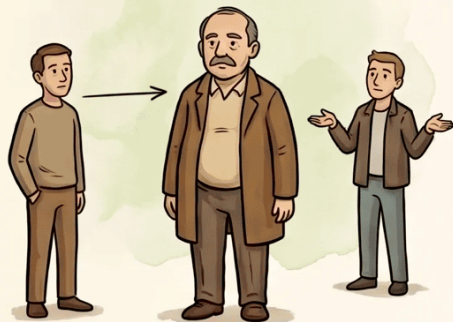


Dve cesty. Pasca je v pravidlách. Cesta von je pravidlá úplne obísť.

* Keď pravidlá píše zasvätenec, sťažovať sa v rámci pravidiel je pasca — aj pokuty sa vracajú späť do ďalšieho zmanipulovaného tendra. Sieť reputácie je cesta von: občania nájdu produkt, zaplatia tvorcovi priamo a komunita udelí jedinu licenciu, na ktorej záleží — dôveru zasluženú dodaním.

AKO SA DÔKAZY HROMADIA

„jedno izolované tvrdenie“



jedno tvrdenie samo — príliš slabé, aby sa podľa neho konalo. ani jedna strana neodsúdená.

„vzorec“



päť nezávislých zdrojov — vzniká vzorec.

„zdrvivujúca váha“



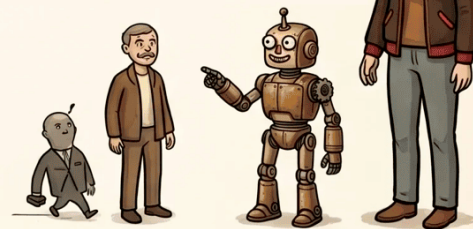
dvadsať nezávislých zdrojov — zdrvivujúca váha.



vysielat' to isté tvrdenie bez dôkazov — keď komunita nič nevidí, je to ohováranie a stojí to obviňujúceho. Nezávislosť je všetko. Jeden opakovaný hlas je šum. Mnoho hlasov z rôznych miest je signál.



jeden obviňujúci ukazuje na všetkých — vzorcom je obviňujúci, nie obvinený.



vyzerá to ako dnešný svet. aj je — len motívy sú teraz poctivé. žiadna revolúcia. len lepšie stimuly.

Nemali by sme prehliadať ani pokánie — dobrovoľný čin pred dokázaním viny, ktorý ponúka cestu k miernejšiemu trestu. Trest nastupuje, keď páchatel nespraví žiadny krok k pokániu a dúfa, že unikne dôsledkom — podobne, ako sa taký výsledok dá kúpiť cez korupciu v centralizovanom systéme.

Typy previnení

Typy informácií sa nemusia obmedzovať na trestné činy; môžu zahŕňať: - opisy zločinov - porušenia zmlúv a podvody - nemorálne správanie - narušenia verejného poriadku, reálneho aj virtuálneho - ...

Každý nový záznam v sieti DID upraví posudzovanú reputáciu a riziko daného DID (či už subjektu, autora, alebo overujúcej authority). Čím väčšiu zodpovednosť nesiem za osud iných, tým opatrnejším sa stávam.

PO ŠKODE — ČO SPRAVÍŠ?

odmietnutý. donútený. dobrovoľný. tri spôsoby, akými dedina odpovedá.

čo sa stalo



a teraz čo?



racionálna voľba je vždy tá najlacnejšia: OPRAV TO SAM.

„Snažím sa to ignorovať“ — všade ma odmietajú“



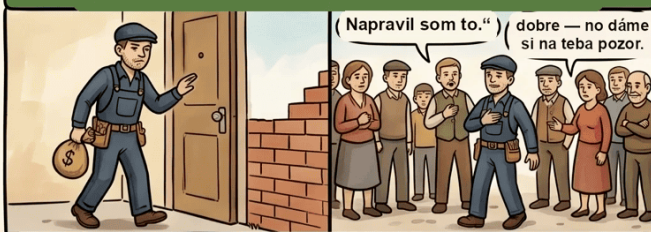
žiadna náprava — každý obchod ho odmietne — vyhnanstvo z ekonomického života

„Napravím to — no len pod pohľadom davu“



vynútená náprava pod pohľadom davu — splatené, no dedina mu zdvihne cenu — poučenie musí utkvieť.

„Prídem sám — a priznám to všetkým“



dobrovoľná, včasná náprava — verejne prijatá — reputácia sa zotavuje, s opatnosťou

vyzerá to ako dnešný svet. aj je — len náklady sú teraz viditeľné pre všetkých. žiadna revolúcia. len lepšie stimuly.

■ Vymáhanie trestu cez delegovanie

Trest nemusím vymáhať osobne. Môžem zaplatiť (podobne ako poistenie) autorite, ktorá vymáha výsledky podľa vopred definovaných pravidiel — ekvivalent vyšetrovacích, policajných a súdnych služieb. Ak autorita vymáha neprimerane alebo nevymáha vôbec, jej reputácia utrpí — a jej reputácia je základom jej schopnosti uživiť sa.

Delegovanie je v sieti všeobecným princípom: akúkoľvek činnosť DID možno delegovať na iný DID — overovanie, vydávanie tvrdení, reakciu na spory, deklarovanie konsenzu. Delegovanie je kedykoľvek odvolateľné. Umožňuje špecializáciu bez straty konečnej kontroly.

KTO VYŠETRUJE, KTO VYNUCUJE?

„škoda“ → „vyšetrovateľ“ „záznam“ → „vynucovateľ“ → „zodpovednosť“



DELEGOVANIE JE ODVOLATEĽNÉ. Akúkoľvek aktivitu DID možno delegovať inému DID — a kedykoľvek vziať späť. trest nevynucuješ sám. deleguješ. a delegát sa zodpovedá tebe.

■ Demokratizácia riadenia rizika

Necenzurovateľná reputačná sieť by zdemokratizovala to, čo banky alebo správcovia veľkých priemyselných komplexov už robia ako svoju hlavnú činnosť — riadenie rizika.

Pre bankára stojaceho pred klientom je posúdenie rizika pripravené vopred, aby sa mohol sústrediť na obchodnú interakciu v rámci vopred definovaných limitov. Sofistikované údržbárske tímy v pravidelných servisných intervaloch zbierajú indikátory rizika (známky konštrukčných trhlin, procesy degradujúce prevádzkovú infraštruktúru a podobne) a dokážu predpovedať životnosť zariadenia, ako aj to, kedy a aký zásah bude potrebný.

Používanie DID si predstavujem podobne — niekto (pravdepodobne za poplatok) poskytne ľudsky čitateľné zhrnutie protistrany. Zhrnutie odzrkadlí uhol posúdenia rizika, ktorý si zákazník objednal.

TREST BEZ CENTRÁLNEJ AUTORITY



jeden rozhoduje za všetkých —
obet' čaká — páchatel' to vie.

komunita deklaruje politiku — páchatel'
jej čelí zo všetkých strán — autorita
vynucuje to, čo bolo dohodnuté.

Náprava je lacnejšia než trest.

Trest je lacnejší než nevedomosť.

Sleduj peniaze

Sleduj stopu peňazí

Máme decentralizovanú reputačnú sieť a motiváciu ju používať. Už teraz dokáže svojim užívateľom priniesť konkurenčnú výhodu — objasniť potenciálne riziká, pomôcť im efektívnejšie plánovať výber protistrany a vyjednávaciu stratégiu a zahrnúť opatrenia, ktoré tieto známe riziká znižujú.

Nasleduje jedna možná metodika⁵ jej použitia — využitie vlastností siete na skonštruovanie migračnej cesty od súčasného systému k jeho evolučnému nástupcovi. Pravdepodobne nesie črty charakteristické pre strednú Európu, kde táto téza vznikla. Miestne podmienky si budú vyžadovať miestne úpravy. Čo by som odporúčal zachovať všade, je nekompromisný charakter opatrení voči štátu — bez toho sa cieľ rozriedi v nekonečnej diskusii a zmena nikdy nepríde. Pozor — zástupcovia a priaznivci štátu ťa budú zamestnávať nezmýslami. Nenalet' na to; ide im o živobytie.

Slabé miesto štátu — peniaze

Vráťme sa na začiatok. Chceme viac výsledných slobôd, viac vplyvu na ich podobu a viac zodpovednosti im primeranej. Otázka je jednoduchá: kde má štát zraniteľné miesto, na ktoré môžeme tlačiť bez toho, aby sme sa uchýlili k násiliiu?

Odpoveď je nudná, a o to je silnejšia. Peniaze.

⁵**Dekonštrukcia štátu** — v českom kontexte sa tomu pravdepodobne do hĺbky bude venovať pripravovaná rovnomenná kniha českého autora Daniela Steigerwalda (plánovaná na rok 2026). Osobne vkladám veľké nádeje do inšpiratívnych postupov, ktoré bude obsahovať.

Vo svojej podstate je štát tokom peňazí. Cez peniaze platí svoj donucovací aparát — posledný článok, ktorý vymáha jeho pravidlá. Bez peňazí niet monopolu na násilie. Keď peniaze začnú viazať, štát začne ustupovať — pretože mu neostáva čím platiť tých, čo ho fyzicky držia na mieste.

Toky peňazí prirodzene kolíšu — sezónne, ekonomicky, podľa nálady investorov. Štát to maskuje pôžičkami na finančných trhoch. Občas je pôžička racionálna: investícia, ktorá sa vráti. Častejšie však pokrýva nadmerné výdavky na agendy, ktoré dávno prerástli jadrový účel štátu — obranu, vnútornú bezpečnosť, trestnú justíciu, zahraničné veci. Keď sa prekročia určité prahy, centrálna banka reaguje úrokovými sadzbami ukotvenými vo vlastnom odhade inflácie.

A tu prichádza tichá daň. Inflácia zďaleka nie je len účtovnou starosťou makroekonómov. Je to skrytá daň z kúpnej sily meny, ktorú platí každý, kto si odložil pár korún na starobu. Nízkou infláciu verejnosť toleruje, pretože nechápe jej dlhodobé účinky — neuvedomuje si, že aj jednociferné čísla, zložené naskladané na dlhom horizonte, nahlodajú úspory až do bodu, keď si ľudia nedokážu zabezpečiť vlastnú starobu. A keď nedokážu, sú kondiciovaní do závislosti od štátnych dávok. Nakoniec na tých dávkach visia a sú priviazaní k štátu.

V turbulentných časoch — vojna, pandémia, „nevyhnutná“ investícia — štát jednoducho zapne tlačiareň. Kúpna sila zodpovedných sporiteľov a pracujúcich klesá, kým im sľubujeme, že sú dobre odmenení. Niekoľko im potichu kradne ich čas a chváli ich, ako skvele zarábajú.

Toto vážne podkopáva dôveru v štát. A dôvera je jediné lepidlo, ktoré drží celý stroj pokope. To je tá páka, o ktorú sa oplatí oprieť.

■ Prečo peniaze, a nie iné slabé miesta?

Ďalším slabým miestom civilizácie je napríklad distribúcia energie. Ale narušenie jej toku nie je páka — bola by to agresia, terorizmus. Dobrovoľná neúčast' nie je to isté ako úmyselné poškodzovanie iných. Peniaze sú výnimočné v tom, že tlak možno vyvíjať dobrovoľne, priehľadne a bez násilia.

Proposed transition to the state's successor

Evolúcia, nie revolúcia

Náhla zmena vyvoláva odpor aj vtedy, keď je konečný cieľ prítiažlivý. Trhá putá — sociálne, ekonomické, politické — a ľudia inštinktívne bránia to, čo už poznajú, proti tomu, čo majú ešte len uvidieť.

Správny prístup je preto postupný — evolučný. Taký, ktorý zabráni starému systému vypnúť ten nový jediným stlačením tlačidla — pretože v okamihu, keď by mohol, urobil by to.

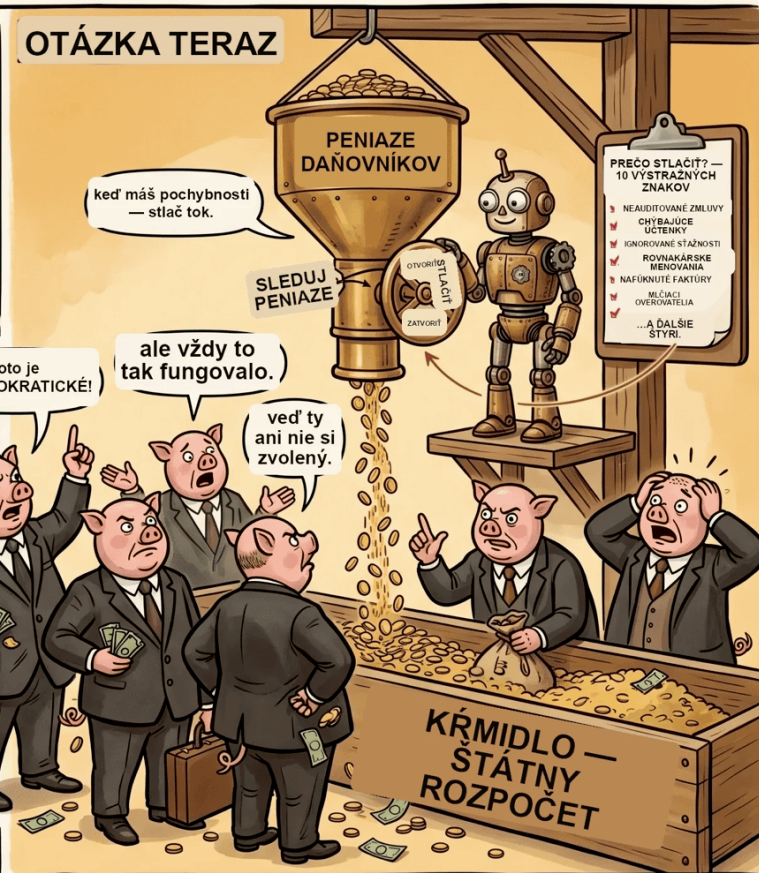
Žiaľ, to znamená prijať, že rovnovážna dobrovoľnosť sa nedosiahne v okamihu, keď nasadíme reputačnú sieť; príde spolu s postupným tempom adopcie. Osvojenie môže byť — a pravdepodobne bude — pomalé, ťahané túžbou jednotlivcov nájsť nápravu u svojej komunity cez reputačnú sieť vtedy, keď konformný spôsob hľadania spravodlivosti zlyhá (a zlyhá). Pozrime sa, ako tá cesta vyzerá, vrátane pomerných odhadov.

SLEDUJ PENIAZE — PRÍBEH DOTERAZ

ČO MÁME



OTÁZKA TERAZ



Máme sieť. Vieme, ako funguje. Teraz: keď máš pochybnosti, stlač násypku.
moc štátu stojí na peniazoch. sleduj ich.

■ Prázdne válovy — nehraj podľa pravidiel nastavených tak, aby si prehral

Pokusy reformovať štát zvnútra sa spoliehajú na vnútorné mechanizmy moci v nádeji, že úradníci pretlačia zmeny proti vlastným stimulom. To sa nestane.

Prečo kŕmiť systém namiesto toho, aby sme vysušili kanály, ktoré mu prinášajú život? Namiesto menenia starého systému a hrania podľa jeho pravidiel vybudujme nad ním novú vrstvu — takú, ktorá starý systém postupne premení na podmnožinu toho nového. Na začiatku tá podmnožina takmer vyplní nadmnožinu. Časom sa aktéri presunú.

Firmy to poznajú: keď je starý systém príliš zamotaný na to, aby sa nahradil, postavíš paralelný a postupne doňho zmigruješ používateľov.

To, že štát skončí s nesúlalom medzi tým, čo skutočne dodáva, a tým, čo vyžadujú jeho stanovy, a že bude náchylný na ten nesúlada sa odvolávať, je čisto problémom jeho zástupcov a účastníkov — netreba sa naň obzerať. Jediné, čo stojí za pozornosť, je toto: nevyprovokuj násilnú revolúciu.

Štyri nástroje, ktoré sa navzájom podopierajú

Doteraz sa reputačná sieť DID mohla zdať užitočná najmä pre spravodlivosť a konsenzus. Verím, že by sa dokázala stabilizovať a odolávať útokom — meritokraticky, na základe skutočných zásluh, nie formálnych titulov. Ale reputácia samotná štát neprinúti ustúpiť. Ekonomika áno, a tlak vyvíjaný cez ňu.

Nič nám nebráni použiť identity DID ako správcov ďalších nástrojov, ktoré tvrdo tlačia na peniaze. Nezačínaj plnou dobrovoľnosťou zo strany občanov — nastav smer, ktorý štát nedokáže zastaviť. Prechod stojí na štyroch konkrétnych nástrojoch, ktoré si navzájom kryjú chrbát. Žiadny z nich nestačí sám.

Jednoduchý daňový systém — vstupná návada

Prvým nástrojom je jednoduchý, priehľadný daňový systém postavený na infraštruktúre DID. Jediná proporcionálna sadzba na všetky príjmy. Žiadne výnimky, žiadne daňové prázdniny, žiadne korporátne odpočty, žiadne stimuly. Každá platba je auditovateľne naviazaná na DID, ktorý ju zaplatil. Krížová kontrola je triviálna.

Sadzba by bola nastavená o niečo výhodnejšie než v starom systéme pre časť daňovníkov — to je návada na vstup. Daňové zaťaženie by z roka na rok klesalo, systém by sa stával čoraz príťažlivejším a migrácia by naberala tempo. Systém je zároveň vedúcim záznamov aj výbercom — žiadny sprostredkovateľ, žiadna nepriehľadnosť.

Elektronická evidencia výdavkov (ESR)

Druhým nástrojom je postaviť EET (Elektronickú evidenciu tržieb) na hlavu. Namiesto toho, aby štát sledoval každú tržbu živnostníka, sledujeme my každý jeden výdavok štátu. Štát nedostane z jednoduchého daňového systému prostriedky na žiadnu jednotlivú platbu, pokiaľ každá z nich — bez výnimky — neprejde týmto sitom.

ESR je proxy⁶, ktoré spáruje každý zrealizovaný výdavok štátu a verejného sektora so záznamom plánovanej platby — vrátane kontextového zdôvodnenia a identifikácie príjemcu, vynakladajúceho subjektu a účelu. Výsledkom sú surové verejné dáta, hierarchizovateľné. Ktokoľvek si ich môže vziať a analyzovať. Ktokoľvek môže ponúknuť daňovníkom odporúčania, čo s nimi. To, čo kontrolné úrady nedokázali roky, je zrazu na jeden klik pre každého.

Nemusíš prejsť na nový daňový systém, aby si sa zapojil. Stačí zaplatiť plne vratnú zálohu (povedzme 1–3 EUR) za zrealizovanú platbu. Nezrealizovaný zvyšok prepadá ako spamový filter, aby systém nezaplavili útoky. Záznam môže podať ktokoľvek — príbuzný za nespôsobilého starého rodiča, sused za zanedbané verejné služby, podnikateľ za nezaplatenú faktúru, úradník exportom z vlastného systému.

Očakávam, že politické strany sa prirodzene premenia na poskytovateľov analýz, alebo vzniknú nové, ktoré nahradia staré. Namiesto príspevkov čerpaných z daní začnú ponúkať odbornosť — poskytovať svojim priaznivcom hodnotovo založené prehľady spriaznených autorít, ich služieb a overovacích politík. Záznamy, ktoré sú z lenivosti odfláknuté alebo nezmyselné, sa automaticky stávajú kandidátmi na rozpočtové škrt. V prvom kole sa tvoja platba vždy vyplatí, ale zozbierané dáta slúžia ako základ na posúdenie, či má štátny výdavok ešte zmysel. Dodávateľia a ďalší na výplatnej páske štátu majú stimul dbať na to, aby úradníci párovali výdavky zodpovedne. Inak peniaze v ďalšom kole nepotečú.

⁶**Proxy** (lat. *procurator*, angl. *deputy/intermediary*) — tu sprostredkovateľ konajúci v mene iného subjektu. Proxy ESR prijíma záznamy plánovaných platieb od kohokoľvek, páruje ich so zrealizovanými výdavkami štátu a výsledný dataset sprístupňuje verejnosti.

■ Odkiaľ pochádza skratka ESR

Medzi rokmi 2016 a 2022 zaviedla česká vláda proti vlastným občanom — živnostníkom a podnikateľom — systém nazvaný Elektronická evidencia tržieb (EET). Odkaz bol jednoduchý: „Predpokladáme, že každý z vás okráda štát. Zaznamenáte každú jednu transakciu, prenesiete ju v reálnom čase na naše servery a my vás budeme sledovať. Vašich spoluobčanov finančne odmeníme za to, že vás nahlásia, ak sa pokúsite obísť EET.“

EET bolo predlohou podľa balkánskych precedensov. Prvou krajinou na svete, ktorá v roku 2013 spustila celoštátny povinný systém evidencie tržieb online v reálnom čase, bolo Chorvátsko pod názvom *fiskalizacija*. Česko model prevzalo o pár rokov neskôr a prevádzkovalo jeden z najprísnejších režimov sledovania tržieb v Európe.

Ak temná strana neváha, prečo by sme mali my? ESR je tá istá logika obrátená naruby: štát sa preukazuje občanom.

Občianska alokácia daní — váha rozhodnutia

Tretí nástroj dáva daňovníkom priamy vplyv na to, kam ich peniaze plynú. V prvom kole štát dostal svoje peniaze bez ohľadu na to, čo ESR odhalilo. V druhom kole už nie — preberá to analýza z prvého kola a opatrenia, ktoré z nej vyplývajú. Malé percento zaplatenej dane si môže platca alokovať sám — za predpokladu, že jeho DID splňa reputačné požiadavky (občianstvo, rezidencia, komunitou uznaná

ESR — ELEKTRONICKÉ VYKAZOVANIE VÝDAVKOV

každý štátny výdavok zaznamenaný — každý záznam verejný — každý detail otvorený na skúmanie.

kto podáva
každý záznam
môže podať: —
úradník, ktorý
platu spracoval
— príjemca, ktorý
dostal zaplatené



VEREJNÝ REGISTER ŠTÁTNYCH VÝDAVKOV — otvorený záznam

kategória: právne poradenstvo
dodávateľ: advokátska kancelária
XYZ s.r.o. suma: 14M EUR zaviazané:
2026-01-14 zaplatené: 2026-01-19
kontext: externé stanovisko k novému návrhu
zákonu o reforme obstarávania —
vypracované tri návrhy, jeden workshop s
ministerstvom, žiadne verejné vypočutie —
finálny návrh dodaný po legislatívnej lehote.

kategória: poradenstvo pri projektovaní
ciest dodávateľ: Consultancy T s.r.o. suma: 9M
EUR zaviazané: 2026-02-03 zaplatené: —
kontext: štúdia uskutočniteľnosti predĺženia
diaľnice D-X — tá istá firma napísala tri predošlé
štúdie na tejto trase — výsledok: odporúčanie
pokračovať pri +18 % oproti skorším odhadom.

otvorené každému,
kto sa chce pozrieť.

kategória: vydávanie evidenčných
čísel príjemca: krajský úrad Z suma:
45 EUR za značku zaviazané:
2026-02-19 zaplatené: 2026-02-19
kontext: štandardný administratívny poplatok za
vydanú značku — poplatok pokrýva materiál a
spracovanie — celkový objem 12 400 značiek za
tento štvrťrok.

kategória: nemocničné vybavenie
dodávateľ: MedSupply a.s. suma: 2M
EUR zaviazané: 2026-03-08 zaplatené: —
kontext: inštalácia MRI skenera v krajskej
nemocnici — verejný tender, traja uchádzači —
vybraná ponuka 2 % pod mediánom, dodanie
do 60 dní — faktúra 90 dní po splatnosti.

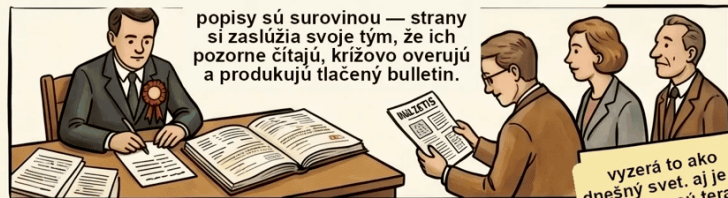


spam filter — vratná záloha



záloha vrátená,
keď sa záznam
preukáže ako
presný.

strany sa menia na poskytovateľov analýz



popisy sú surovinou — strany
si zaslúžia svoje tým, že ich
pozorne čítajú, križovo overujú
a produkujú tlačенý bulletin.

vyzerá to ako
dnešný svet. aj je —
len knihy sú teraz
otvorené všetkým.
žiadna revolúcia.
len lepšie stimuly.

Každá koruna verejných peňazí — zaznamenaná, verejná, preskúmateľná.
hodnota nie je v chytaní podvodníkov — je v otvorení kníh.

dospelosť/spôsobilosť). Alokovateľné percento z roka na rok rastie. Potenciálne exponenciálne. Z piatich percent dnes na desiatky percent v priebehu desaťročia.

Surové dáta ESR prirodzene usmerňujú rozhodovanie daňovníkov. Nekvalitné záznamy fungujú ako varovný signál pre odporúčané škrtý. Ktokoľvek môže vytvárať záznamy; úradníci ich musia párovať. Bez toho daňový systém nepoše štátu žiadne peniaze — ani do štátnej pokladnice, ani do iných rozpočtových kapitol. Politický boj sa presúva z volebnej urny do každodennej alokácie konkrétnych korún.

OBČIANSKE PRIDELENIE DANÍ — TY ROZHODUJEŠ, KAM PÔJDU TVOJE DANE

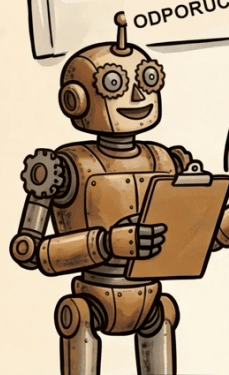
preštuduj záznamy ESR. potom posuň posuvníky.

ANALYTICKÁ SPRÁVA ESR
od: dôveryhodný analytik — vybraný
tebou

ministerstvo obrany: — 7
zákaziek za 2 roky
jednému dodávateľovi —
žiadne verejné vypočutia
k reforme obstarávania —
90-dňové omeškanie
platieb pri 60 % faktúr

ODPORUČAM ZNÍŽIŤ.

rep 4,7/5



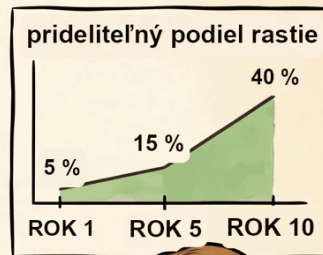
alebo deleguj toto

nechceš pridel'ovať
sám? deleguj na: —
analytika svojej strany
— dôveryhodného
suseda — kohokoľvek
si vyberieš — a
kedykoľvek odvolaj.



po
prečítaní
správy
—
obrana
dole.

▶ VZDELÁVANIE	<input type="range"/>	30 %
▶ ZDRAVOTNÍCTVO	<input type="range"/>	25 %
▼ OBRANA	<input type="range"/>	10 %
▶ personál	<input type="range"/>	5 %
▶ vybavenie	<input type="range"/>	3 %
▶ VÝSKUM A VÝVOJ	<input type="range"/>	2 %
▶ INFRAŠTRUKTÚRA	<input type="range"/>	20 %
▼ SOCIÁLNE SLUŽBY	<input type="range"/>	15 %



klikni na
ktorýkoľvek
riadok a ponor sa
hlbšie — pridel'uj
v akejkoľvek
hlbke.



vyzerá to ako
dnešný svet. aj je
— len posuvník
je teraz v tvojej
ruke. žiadna
revolúcia. len
lepšie stimuly.

Z 5 % dnes na 40 % za desaťročie. Ty rozhoduješ.
záznamy sú otvorené. analýza je tvoja. rovnako aj posuvník.

Vyjednávací platforma so štátom — páka

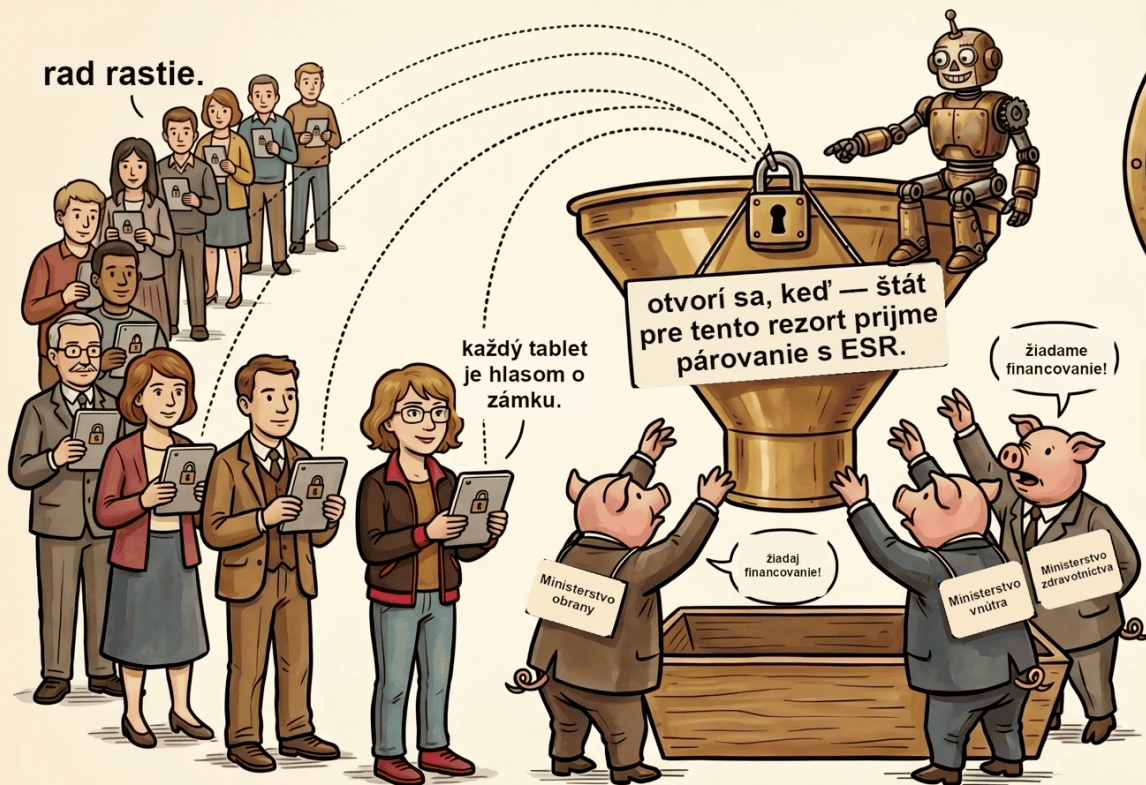
Štvrtým nástrojom je páka, ktorá všetko zväzuje dokopy a až teraz robí zo siete skutočnú hrozbu. Hlavný konflikt bude o tom, či štát prijme ESR ako záväzný štandard — najprv na národnej úrovni — a aké veľké musia hrozby zo strany účastníkov reputačnej siete byť, kým sa tak stane.

Páka je just-in-time financovanie štátu, podmienené párovaním platieb oproti ESR. Peniaze plynú len v okamihu, keď štát splnil podmienky transparentnosti. Vnútri reputačnej siete sa tvorí zoznam čakateľov. Aktivácia nastupuje, keď skupina dosiahne ekonomicky významnú veľkosť — dosť veľkú na to, aby ohrozila rast HDP. V tom bode sa občianska neposlušnosť stáva vierohodnou hrozbou, nie gestom.

Štát sa bude najdlhšie držať problematických platieb naviazaných na korupciu. Pod tlakom ustúpi najprv tam, kde má ľahkú obranu a kde niet priestoru hľadať úspory. Postupný a stúpajúci tlak ho donúti ustupovať krok za krokom z každej pozície.

VYJEDNÁVACIA PLATFORMA — ZATVORENÁ NÁSYPKA

klúč držia občania. štát sa otvorí, keď sú splnené podmienky.



rad rastie.

každý tablet
je hlasom o
zámku.

otvorí sa, keď — štát
pre tento rezort prijme
párovanie s ESR.

žiadaj
financovanie!

žiadame
financovanie!



stačí malý zlomok HDP — pri
kritickej mase sa zadržiavanie
stáva reálnou hrozbou.

po dosiahnutí criticalkej masy —

štát najprv otvorí knihy pre
jednoduché, obhájiteľné platby.

kategórie spojené s korupciou
zostávajú zamknuté najdlhšie.

každé odomknutie vyžaduje väčší
tlak — a samo sa zaznamenáva.

Peniaze tečú, keď je transparentnosť. Klúč držia občania.

žiadne násilie. žiadna revolúcia. len dosť tabletov, aby bolo zadržiavanie vierohodné.

vyzerá to ako
dnešný svet. aj je
— len klúč je teraz
v mnohých rukách.
žiadna revolúcia.
len lepšie stimuly.

Občianstvo bez občianskeho preukazu

S prechodom na infraštruktúru DID stráca štátom vydávaný občiansky preukaz svoj monopolný účel. Nepotrebuješ občiansky preukaz — máš škálu identít DID a niektoré z nich nesú tvrdenie, že si napríklad Čech, obyvateľ konkrétnej obce, absolvent konkrétnej školy. Tvrdenie je overiteľné, trvalé a nezávislé od štátnej správy.

Otvára sa otázka technického prevedenia: kto na trhu prevezme overovanie existujúcich občanov mimo štátnej kontroly, aby zmigroval záujemcov do DID nesúceho príslušné tvrdenie? Najpravdepodobnejšie vzniknú authority voľného trhu špecializované na overovanie identity — notári, miestne komunity, zamestnávateľia. Vsádzajú svoju reputáciu na to, že daný DID naozaj patrí osobe, ktorá tvrdí, že jej patrí. Občianstvo — teda príslušnosť ku konkrétnemu pohľadu na komunitu — sa oslobodzuje od potreby centrálného vedenia záznamov. Prepojením cez reputačnú sieť sa vložené dáta spoja a validujú druhýkrát, tretíkrát, štvrtýkrát a tak ďalej.

Dôsledok je intuitívny, no v centralizovanom systéme neriešiteľný. Dnes môže politické vedenie — s ohľadom na ľahšie znovuzvolenie — importovať koncentrované problémy na územie komunity: prijímať migrantov z iných civilizačných okruhov bez ohľadu na absorpčnú kapacitu a ochotu existujúcej komunity, meniť pôvodné komunity tlakom, pod ktorým nedokážu držať krok s asimiláciou príchodších z iných civilizačných okruhov. V sieti DID si korupčne prijatý migrant nemôže byť istý, že ho komunita bude naďalej považovať za jedného zo svojich. Členovia komunity objektívne nemusia strpieť cudzinca, ktorý im príde na dvere v uniforme komunity a vyhráža sa im zákonnosťou opatrení, ktoré mieni vykonať v dome (zhabanie detského telefónu za príspevok na sociálnej sieti). S decentralizovanou reputáciou sa väčšina spoločnosti nemusí s týmto zmieriť — pretože o príslušnosti ku komunite nerozhoduje úradník, ale komunita sama, cez svoje reputačné signály.

ŠTYRI NÁSTROJE EVOLUČNÉHO PRECHODU

system prestavaný zvnútra — bez toho, aby sa rozbil.

JEDNODUCHÁ DAŇ



jedna sadzba. žiadne výnimky. krížovo overiteľná.

ESR — ELEKTRONICKÉ VYKAZOVANIE VÝDAVKOV



každý výdavok zaznamenaný — každý záznam verejný — každý detail otvorený.

OBČIANSKE PRIDELENIE DANÍ

5 % → 15 % → 40 %
ROK 1 → ROK 5 → ROK 10



preštuduj záznamy — potom posuň posuvníky.

VYJEDNÁVACIA PLATFORMA



peniaze tečú, len keď sú splnené podmienky transparentnosti.

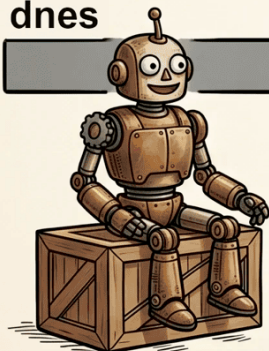
dnes

evolúcia prebieha

o desaťrocie

95 %

rozširuje sa



Evolúcia, nie revolúcia.

štyri nástroje, ktoré menia systém zvnútra.

vyzerá to ako dnešný svet. aj je — len nástroje sú teraz v rukách občanov. žiadna revolúcia. len lepšie stimuly.



OBČIANSTVO BEZ PREUKAZU TOTOŽNOSTI

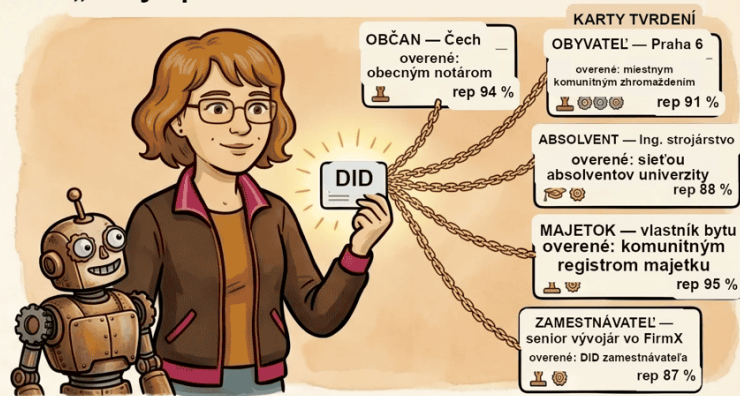
od štátneho povolenia k uznaniu komunitou.

„starý spôsob“ inštitucionálneho modelu ID vydávaného štátom



identita = štátne povolenie — odvolateľné — komunita nemá slovo.

„nový spôsob“ modelu DID s kartami tvrdení



žiadna jediná autorita neovláda všetky tvrdenia — každé je nezávislé — každý overovateľ ručí svojou reputáciou.

„kto sem patrí?“



Tvoje občianstvo nie je štátne povolenie. Je to uznanie tvojej komunity.
štátnu pečiatku nahrádza reťaz nezávislých overovateľov — každý má čo stratiť.

vyzerá to ako dnešný svet. Aj je — len overovateľov je teraz mnoho. žiadna revolúcia. len lepšie stimuly.

Váha volebného hlasu vo veciach spadajúcich pod pôsobnosť štátu by v budúcnosti mohla byť striktné korelovaná so záznamami o príspevkoch do jednoduchého daňového systému. V kombinácii s vhodnými tvrdeniami DID (napríklad „táto osoba je český občan“) možno potom cudzích štátnych príslušníkov z volieb vylúčiť — register obyvateľov sa jednoducho presunie sem.

Prekryv a zvratnosť

Netvrdím, že toto je jediná cesta, ba ani že najlepšia. Ale javí sa komplexná — pokrýva hlavné páky a zachováva možnosť ustúpiť. Na začiatku sa nový systém prekrýva so starým a mení len stimuly. Časom sa starý systém zmenšuje, až sa môže — no nemusí — rozplynúť. Výhodou je postupnosť a zvratnosť: ak sa v dizajne objaví chyba, nie je to koniec, len korekcia.

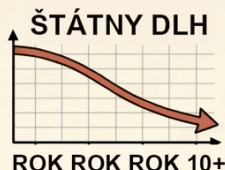
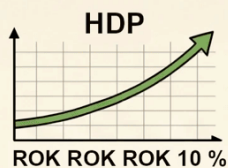
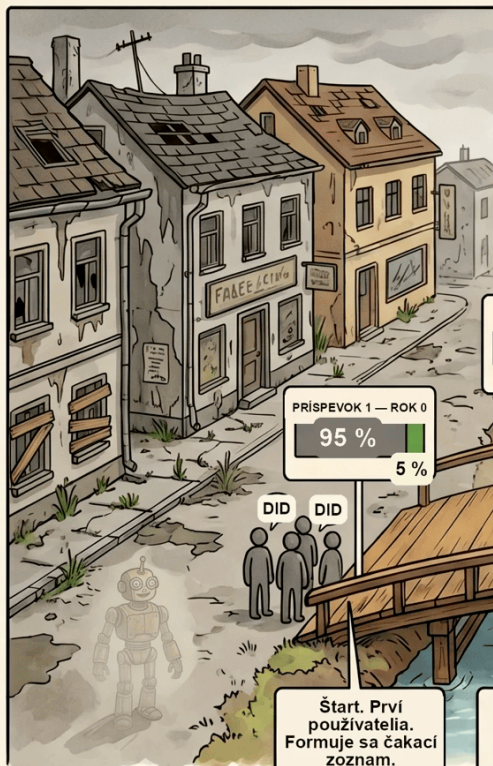
Mier a vojna

Niektoré časti štátu nemusia mať plne trhovú alternatívu — napríklad armáda. Dočasné delegovanie mimoriadnych právomocí v krízach (ako starí Gréci menovali diktátorov) by mohlo naďalej existovať. Zodpovednosť však spočíva na decentralizovanej spoločnosti, nie na vodcovi. Na rozdiel od centralizovaného vládnutia bude ľahšie získať delegované právomoci späť, keď hrozba pominie — alebo skôr, keď to bude nutné. Slobodná spoločnosť nebude v nevýhode ani v stretnutí zbraní proti autoritárskym režimom.

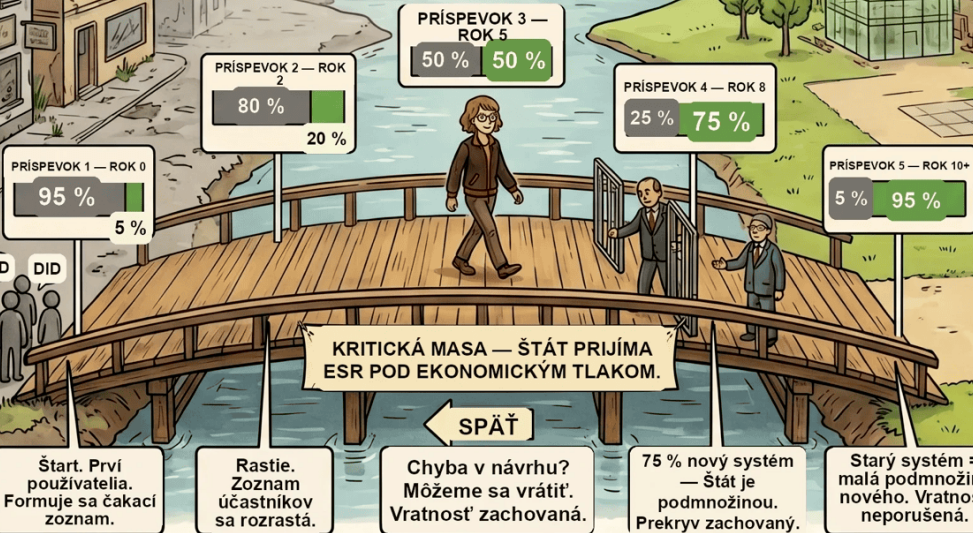
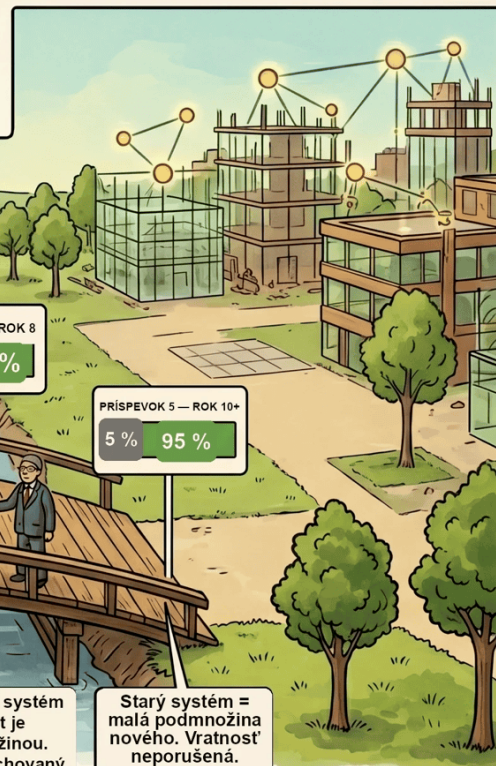
■ Vojnoví zločinci

Pri just-in-time financovaní štátu a priehľadných výdavkoch sa stáva ťažkým nazhromaždiť zdroje na agresívne vojny. Daňovník, ktorý naďalej financuje takú vojnu, sa stáva legitímnym cieľom a nemôže sa dovolávať civilného statusu podľa Ženevských dohovorov. Za nového usporiadania sa tichý súhlas berie ako účasť.

ĽAVÝ BREH — „STARÝ SYSTÉM“



PRAVÝ BREH — „NOVÝ SYSTÉM“



STARÝ SYSTÉM

> Postupný prechod. Vratnosť pri chybe. Smer, ktorý sa nedá zastaviť.

Záver

Cesta existuje

Štát je taký, aký je, kvôli technológiám dostupným v čase jeho vzniku, skombinovaným s ľudskou povahou. Stavať všetko na dobrovoľnosti a pritom popierať priemernú ľudskú povahu je naivné. Nezbatim sa korupcie ani sklonu unášať sa k totalite. Nástupca štátu musí fungovať aj s vlastnosťami, ktoré dnes považujeme za negatívne a buď ich ostrakizujeme, alebo trestáme.

Táto kniha opísala problém — systém (štát), kde ľudia, ktorí píšu pravidlá, nikdy nežijú s ich dôsledkami. Opísala podmienky, ktoré musia platiť, aby ten systém prestal fungovať. Opísala nástroj, ktorý tieto podmienky spĺňa. A navrhla metodiku prechodu — konkrétne kroky, ako ten nástroj použiť, ako jeden možný príklad.

V prvej kapitole som pomenoval päť pilierov: dobrovoľnosť, organizáciu, odolnosť, konsenzus a neskorumpovateľnosť. Splnili sme ich všetky.

- **Dobrovoľnosť** — nikto ťa do siete nenúti, ale ani svoje činy z nej nevymažeš.
- **Organizácia** — komunita rastie z toho, koho poznáš, nie z toho, ku komu ťa priradili zhora.
- **Odolnosť** — ani štát ochotný platiť za sledovanie každého paketu ju nedokáže vypnúť.
- **Konsenzus** — vzniká z cenovky za pokrytectvo, nie z hlasov či podpisov.
- **Neskorumpovateľnosť** — päť malých pravidiel votkáva korupciu do nákladov: rovnováha dobrovoľnosti a zodpovednosti, právo kohokoľvek prehovoriť, vstupné body, ktoré si nikto nevyberá, verejné sľuby s cenou za pokrytectvo a tieň pozorovateľa za každou transakciou.

Žiadny jediný pilier nedokáže nahradiť štát sám. Spolu tvoria odpor voči korupcii, aký štát s celým svojím aparátom nedokáže.

Sme v bode, keď sa celok dá postaviť dnešnými technológiami (kryptografia, decentralizovaná identita, dobre známe psychologické vzorce na správne nastavenie stimulov, ...). Chýba len jedno: kritická masa ľudí, ktorí nájdu odvahu to podporiť a rozhodnú sa začať.

Nie cez revolúciu.

Tieto myšlienky sa formovali medzi júnom 2025 a májom 2026. Kým som si sadol písať, mal som rámec do veľkej miery vypracovaný v hlave — a práve preto som s takou zvedavosťou čítal [Farewell To Westphalia](#), keď sa objavil. Chcel som vidieť, kde sa ich obraz prekryje s mojím a kde sa rozíde. Druhý podnet prišiel od Dana Steigerwalda, ktorý v máji 2026 stále pracuje na vlastnej knihe *Dekonštrukcia štátu* z iného uhla; jeho projekt ma dotlačil položiť moju vlastnú víziu na papier v plnej šírke — aby ju svet mal na stole popri ostatných.

Nežiadam ťa, aby si čomukoľvek z toho veril. Žiadam ťa, aby si o tom premýšľal. A zanechávam ti jednu otázku:

Čo by si zmenil?

Pavel Kudrna 23. mája 2026, Praha, Česko

PodĎakovanie

Inšpirácia

Ďakujem autorom [Farewell to Westphalia](#) (Jarrad Hope, Peter Ludlow) za intelektuálny rámec, ktorý mi pomohol zasadiť moje vlastné myšlienky do širšieho kontextu dekonštrukcie vestfálskeho modelu štátu.

Recenzia a spätná väzba

Nástroje

Pri príprave textu, štruktúrovaní myšlienok a iterovaní formulácií som využil asistenciu nástrojov AI. Všetky myšlienky, argumenty a závery sú moje vlastné — AI slúžila ako nástroj na doladovanie, nie ako spoluautor obsahu.

Infografiky boli navrhnuté v spolupráci s generatívnymi nástrojmi na základe autorových zadaní.

VEZMI SI SPÄŤ SVOJ ČAS

občania vyháňajú parazitov z verejného života.



Bráň čas, ktorý by ti ukradli. čo bolo vzaté klamstvom, berie sa späť rukou.

Podpor projekt

Personix financujú čitatelia ako ty.



Bitcoin on-chain

bc1q7cctdz6r026dgy06ul94eygg49ujtxnrq5czaj



Bitcoin Lightning

LNURL1DP68GURN8GHJ7AMPD3KX2AR0VEEKZ
AR0WD5XJTNRDAKJ7TNHV4KXCCTTDEHHWM30
D3H82UNVWQHXMNP0FA8JMPVD5XJMN9XUE
RX55QRQK

Kam tieto peniaze idú — a kam nie

QR kódy sú **osobné kanály autora** — príspevky idú priamo Pavlovi Kudrnovi a financujú ďalšie písanie, spoločenský experiment / simuláciu a osvetu.

Jediné legitímne kanály na získavanie prostriedkov pre tento projekt sú:

- **Autorské vydania tejto knihy** — QR kódy v kópiách autorizovaných autorom.
- **personix.org** alebo jeho Tor onion zrkadlo odtiaľ odkazované — kde *Personix Foundation* vyberá na aktivity tam opísané. Prostriedky nadácie sú vedené oddelene od osobných prostriedkov autora.

Čokoľvek inzerované inde — podstrčené adresy v dotlačiach, napodobené domény, „zbierky pre Personix“ na sociálnych sieťach, zbierky nenaviazané ani na jeden z vyššie uvedených kanálov — **je s najväčšou pravdepodobnosťou podvod**. Zámerne sa vyhýbame kryptomenovému trhu a jeho účastníkom.

Slovníček pojmov

Slovníček pojmov

Pojem	Slovensky	Význam
Authority	Autorita	Dôveryhodný subjekt (osoba, organizácia), ktorý overuje informácie a vsádza na ne svoju reputáciu. Môže byť špecializovaný (vyšetrovací, právny, technický).
Claim	Tvrdenie	Všeobecne: akýkoľvek overiteľný výrok. Tu: záznam zverejnený do reputačnej siete — tvrdenie o udalosti, vlastnosti alebo vzťahu, ktoré je kryptograficky podpísané a overené. Napr. „som obyvateľom obce X“ alebo „táto osoba porušila zmluvu“.

Pojem	Slovensky	Význam
Compartmentalization	Kompartmentalizácia	Všeobecne: oddelenie informácií do izolovaných jednotiek tak, aby odhalenie jednej jednotky neohrozilo ostatné. Princíp známy zo spravodajských služieb. Tu: paralelné identity DID v diktatúrach — kompromitácia jednej neodhalí ostatné.
Consistent Hash Ring	Hash ring	Algoritmický mechanizmus na výber overovateľov — pozíciu na ringu určuje hash DID dokumentu v rámci sociálneho grafu. Zabezpečuje nedeterministický, no overiteľný výber.
DID	DID (Decentralizovaná identita)	Digitálna identita, ktorú si vytváraš a ovládaš sám, bez centrálnej autority. Kryptograficky podpísaná tvojím súkromným kľúčom — nikto ju nemôže zrušiť ani sfaľovať.

Pojem	Slovensky	Význam
DID Document	DID dokument	Verejne dostupný dátový súbor opisujúci tvoju identitu DID — obsahuje verejné kľúče, sieťové adresy a metadáta. Používa sa na overenie tvojej identity v sieti.
Due Diligence	Due diligence	Všeobecne: dôkladné preverenie protistrany pred vstupom do obchodného alebo právneho vzťahu — kontrola jej histórie, financií, reputácie a rizík. Tu: v reputačnej sieti prebieha rýchlejšie a automatickejšie vďaka dostupnosti overených záznamov.
Economic Neutrality Principle	Princíp ekonomickej neutrality	Poctivé správanie v sieti je ekonomicky blízke nule — náklady na zverejnenie sa vracajú ako odmeny za overovanie. Nepoctivé správanie je čistá strata.

Pojem	Slovensky	Význam
Emergent	Emergentný	Spontánne vznikajúci z interakcií jednoduchších častí, bez toho, aby to niekto navrhol alebo riadil. Křdeľ vtákov letí vo formácii bez plánu — formácia emerguje z jednoduchých pravidiel, ktoré dodržiava každý jednotlivec.
Emergent Social Contract	Emergentná spoločenská zmluva	Pravidlá správania, ktoré nevznikajú zhora (zákon), ale zdola — z opakovaných interakcií a konsenzu v rámci komunity.
ESR	Electronic Spending Register	Navrhovaný systém priehľadného sledovania verejných výdavkov — každý zrealizovaný výdavok štátu sa páruje s plánovanou platbou. Inšpirovaný českým EET, ale obrátený proti štátu.

Pojem	Slovensky	Význam
Hash	Hash (odtlačok)	Všeobecne: jednosmerná matematická funkcia, ktorá z ľubovoľného vstupu vyrobí jedinečný „odtlačok“ pevnej dĺžky — ako odtlačok prsta dokumentu. Rovnaký vstup vždy dá rovnaký výstup, ale zo vstupu sa nedá odvodiť výstup naspäť. Tu: používa sa na určenie pozície na hash ringu a na overenie integrity dokumentu.
Just-in-Time Funding	Just-in-time financovanie	Financovanie štátu podmienené transparentnosťou — peniaze plynú len vtedy, keď štát prijme ESR a spáruje svoje výdavky. Páka na vynútenie spolupráce.

Pojem	Slovensky	Význam
Meritocracy	Meritokracia	Všeobecne: systém, kde postavenie určujú skutočné zásluhy a preukázaná schopnosť, nie formálne tituly, konexie či zdedená výsada. Tu: reputačná sieť prirodzene zvýhodňuje tých, ktorí preukázateľne prispievajú komunite — ich hlas má väčšiu váhu vďaka track recordu, nie vďaka úradu.
Onion Gateway	Onion gateway	Sieťová adresa identity DID v onion sieti. Oddelená od DID dokumentu — dá sa zmeniť bez straty identity (podobne ako zmena IP adresy za doménou).
Onion Routing	Onion routing (Tor)	Komunikačný protokol, ktorý zabezpečuje necenzurovateľnosť siete. Správy sú šifrované vo vrstvách — každý uzol odlúpne jednu vrstvu, ale nepozná celú cestu.

Pojem	Slovensky	Význam
Oracle Problem	Problém orákula	Všeobecne: ako zabezpečiť, aby dáta vstupujúce do digitálneho systému verne zodpovedali tomu, čo sa naozaj stalo vo fyzickom svete. Pojem pochádza z oblasti blockchainu. Tu: rieši sa cez authority, ktoré vsádzajú svoju reputáciu ako záruku, že digitálny záznam zodpovedá fyzickej realite.
Phenomenological	Fenomenologický	Všeobecne: prístup, ktorý skúma javy tak, ako sa prejavujú v priamej skúsenosti, pozorovaním toho, čo z nich vyplýva, bez vopred daných teórií. Tu: sloboda, spoločenská zmluva a normy správania sú pozorované javy — dôsledky tisícov mikrointerakcií medzi ľuďmi, nie princípy definované zhora.

Pojem	Slovensky	Význam
Policy	Policy (politika)	Všeobecne: súbor pravidiel alebo princípov riadiacich správanie v danom kontexte. Tu: každý účastník siete DID deklaruje svoju policy — ako reaguje na konkrétne správanie iných, ktoré pravidlá dodržiava a ktoré tresty považuje za primerané. Súhrn politik tvorí emergentnú spoločenskú zmluvu.
Proxy	Proxy	Všeobecne: zástupca alebo sprostredkovateľ — systém alebo subjekt konajúci v mene iného. Tu použité v dvoch kontextoch: (1) ESR ako proxy párujúce verejné výdavky s plánovanými platbami; (2) pozorovatelia ako proxy medzi vydavateľom a overovateľom v triku s pozorovateľmi.
Publisher	Vydavateľ	Účastník siete, ktorý vytvára a zverejňuje záznam (tvrdenie o krivde, náprave a podobne). Nesie náklady na zverejnenie.

Pojem	Slovensky	Význam
Reputation-Based Social Network (RSN)	Reputačná sieť	Decentralizovaná sociálna sieť, kde si účastníci vymieňajú spätnú väzbu o správaní v reálnom svete. Záznamy sú nákladné na vytvorenie, lacné na čítanie.
Reputation Signal	Reputačný signál	Jednotlivý záznam v sieti — pozitívny (náprava ujmy, splnenie záväzku) alebo negatívny (krivda, porušenie zmluvy). Kumulatívne signály tvoria reputačný profil.
Social Graph	Sociálny graf	Sieť tvojich kontaktov a kontaktov tvojich kontaktov. Algoritmus hľadá overovateľov do konfigurovateľnej hĺbky (napríklad 3 úrovne). Žiadny globálny blockchain — sieť prirodzene tvorí komunity s presahmi.
Tax Allocation	Alokácia daní	Mechanizmus, ktorým daňovník rozhoduje, kam ide časť jeho daní. Alokovateľné percento z roka na rok rastie.

Pojem	Slovensky	Význam
Track Record	Track record	Všeobecne: história minulých výsledkov, úspechov a zlyhaní osoby alebo organizácie. Tu: súhrn všetkých minulých interakcií danej identity DID v sieti — overené tvrdenia, prijaté a zamietnuté záznamy — z ktorých sa odvodzuje jej reputácia.
Verifier	Overovateľ	Účastník algoritmicke vybraný na overenie a zverejnenie záznamu. Vsádza svoje dobré meno na pravdivosť informácie.

Produkčné poznámky

Vyhradené autorom (nekryté licenciou CC BY-SA): názov a slovné označenie Personix, obálka knihy a podporné kanály (QR kódy, adresy, kontaktný e-mail). Odvođené vydania musia tieto prvky odstrániť alebo nahradiť; použiť ich možno len na odkázanie na toto pôvodné dielo.

Zdrojové súbory. Kompletný zdroj — text v markdowne, infografiky, build skripty — je dostupný spolu s týmto PDF.

Nástroje. Pri príprave textu a iterovaní formulácií autor využil asistenciu nástrojov AI; infografiky boli navrhnuté v spolupráci s generatívnymi nástrojmi na základe autorových zadaní. Všetky myšlienky, argumenty a závery sú autorove vlastné.

PERSONIX

Nekompromisná zmena

Necenzurovateľná a neskorumpovateľná decentralizovaná reputačná sieť

Štát fungoval, keď bola komunikácia pomalá, rozhodnutia lokálne a autorita žila v tom istom meste, ktorému vládla. Dnešné siete obracajú všetky tri predpoklady — a inštitúcie na nich postavené už nesedia svetu, ktorému vládnu. Táto kniha opisuje nástroj, ktorý sedí: decentralizovanú reputačnú sieť, v ktorej je identita tvoja a nikto ti ju nevezme, pravda je verejne auditovateľná a úplatok je reputačnou samovraždou.

Nie manifest. Nie predpoveď. Funkčný plán toho, ako sa dá nástupca štátu postaviť — dobrovoľne, jedna deklarácia za druhou.

Pavel Kudrna • Praha, 2026

personix.org

Licencované pod Creative Commons Attribution-ShareAlike 4.0 International (CC BY-SA 4.0).