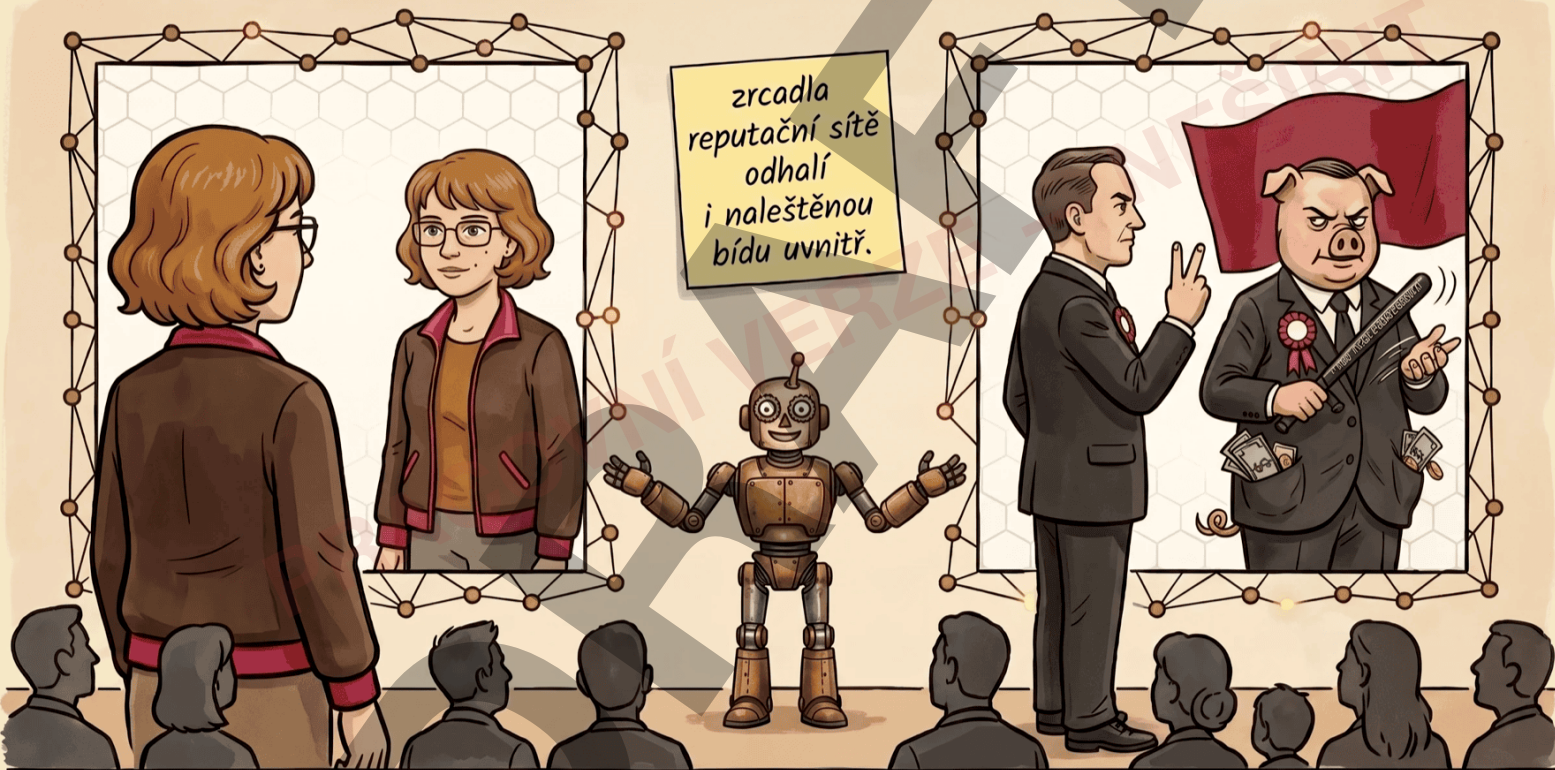


PERSONIX

Prezidentská úprava

zrcadla
reputační sítě
odhalí
i naleštěnou
bídu uvnitř.



Necenzurovatelná a nezkorumpovatelná decentralizovaná reputační síť
evoluční nástupce státu

Personix — Nekompromisní změna

Necenzurovatelná a nekorumpovatelná decentralizovaná reputační síť

© 2025–2026 Pavel Kudrna, Praha

Verze 6 (2026-05-21)

První návrhy červen–listopad 2025; přepracováno duben–květen 2026.

Vysazeno v $\text{\LaTeX}$ (Tectonic) písmem Palatino a Helvetica Neue.
A5 na šířku (210 × 148 mm).

Toto dílo je licencováno pod **Creative Commons Uvedte původ-Zachovejte licenci 4.0 Mezinárodní (CC BY-SA 4.0)** — creativecommons.org/licenses/by-sa/4.0/deed.cs. Vyhrazené prvky, odkaz na zdrojový kód a poznámka k produkčním nástrojům jsou uvedeny v zadní části knihy.

Pro odkaz na původní dílo, kompletní zdroj a aktuální verze: personix.org.

Obsah

1 Úvod	6
O čem tato kniha je?	8
2 Nezbytné předpoklady změny	15
3 Nástroj	24
Reputační sociální síť (Reputation-Based Social Network)	24
Proč je síť necenzurovatelná	46
Řešení zjevných pochybností	46
Závislost na technologii	46
Nevyhodím publikování v síti peníze oknem?	49
Co když si někdo založí víc identit?	50
Nemůže si bohatý člověk prostě „koupit“ víc identit (nebo vytvářet virtuální komunity)?	52
Co příživníci, kteří chtějí jen číst a nic komunitě nedávat?	55
Finanční neutralita	56
Dobrovolnost, zodpovědnost a svoboda	58
Přepínač svoboda–totalita (a delegování)	59

Oracle problém — propojení digitálního a fyzického světa	64
4 Jak ověřování funguje	68
Konsenzus a proces ověřování	68
Role v ověřovací transakci a autority	74
Přehled rolí	74
Vydavatel	76
Autorita	78
Ověřovatel	79
Subjekt	82
Pozorovatel	84
Mechanismus: časové razítko a kód výzvy	84
Pointa: skutečné pozorovatele nepotřebujete	87
Delegování	89
Komunikace rolí	94
Emergentní společenská smlouva — Politika/Policy	94
Poskytování informací o sobě	98
5 Zločin a trest	100

6 Sleduj stopu peněz	111
Slabé místo státu — peníze	111
Navrhovaný přechod k nástupci státu	113
Evoluce, ne revoluce	113
Čtyři nástroje, které se vzájemně podporují	115
Jednoduchý daňový systém — vstupní lákadlo	116
Elektronický registr výdajů (Electronic Spending Register)	116
Alokace daní občany — váha rozhodnutí	118
Vyjednávací platforma se státem — páka	120
Občanství bez občanky	120
Překryv a reverzibilita	124
7 Závěr	128
Cesta existuje	128
Rejstřík pojmů	132

1. Úvod

Cítíte, že se na stát můžete spolehnout?

Nesmírím se s tím, když se mně, mé rodině nebo někomu z mé komunity stane evidentní křivda (fyzická, podvod, nepatřičné omezování, ...) a stát odpovídá: ano, je to křivda, ale nic s tím nedělejte, nebo budete mít ještě větší problém se mnou. Takový stav je nemocný a lidé, kteří s ním souhlasí, jsou spolupachatelé.

Výsledkem je vzájemná odcizenost, hraní si na komunity, hraní si na státotvornost a prohlubující se rozpad společnosti s příslibem vážných konfliktů.

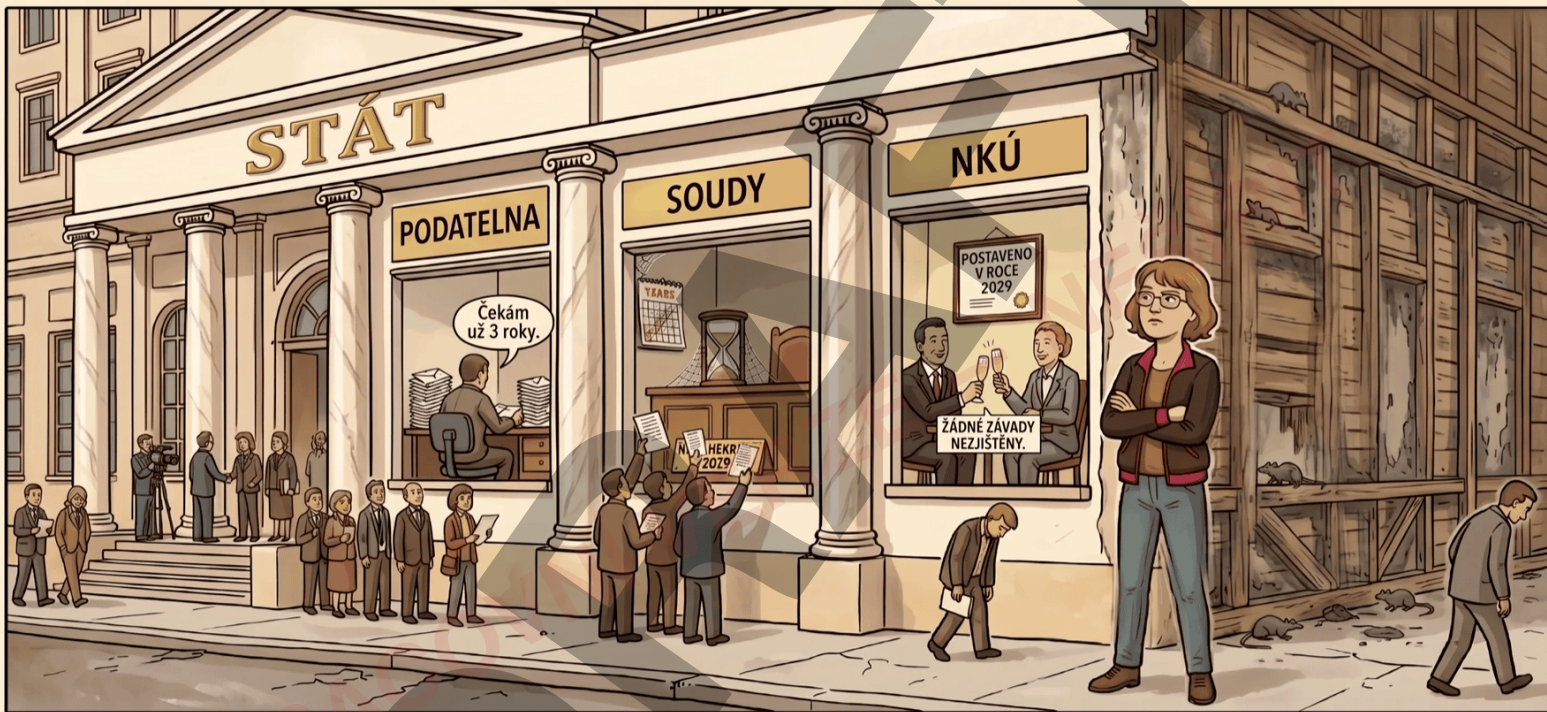
Stíhá stát tempo technologických a společenských změn, nebo raději vyrobí zákaz?

Mohl bych se tvářit, že zaostávání, neschopnost a korupci budu považovat za deklaratorní stabilitu právního státu a tradice, ale již nechci. Lhal bych sám sobě a lhal bych i vám.

Cítíte tu blahosklonnost úředníků a volených zástupců, když si dovolíte kritizovat něco, co platíte?

Odmítám považovat lidi ve společnosti za nehodné podílet se na směřování celospolečenských pravidel jen proto, že neexcelují v soft-skills — což je dnes jediný postačující předpoklad pro to, aby člověk měl šanci stát se voleným zástupcem ve státě kodifikovaných institucích. Věřím, že se valnou většinou dokáží postarat sami o sebe, své blízké i svou komunitu a že v tom vidí i kus své životní filozofie. Většina lidí v mém okolí taková je.

Poznal jsem však i vyložené zmrdy, kteří jimi byli, protože uměli hrát tu hru, že jim komunita nesmí dát zpětnou vazbu, že je stát ochrání, aby nikdo nenarušil řád, který by ohrozil samotnou podstatu státu



Odmítám to přijmout.

— a tou je zajistit snadné živobytí těm ve vyšších patrech mocenské hierarchie a hierarchie jejích institucí. Feudalismus nahradila vláda populistů a elitářů.

Milujete, když vám ostatní mluví do života?

Neberu současný stav jako dokonalou konečnou danost. Musím být ve svém vystupování odpovědný, ale jsem háklivý na to, když mi někdo určuje, jakých správných hodnot se mám držet. Jak to máte vy?

O čem tato kniha je?

Představte si, že existuje reputační sociální síť a kdokoliv chce, si do ní sám vyrobí klíčky (vytvoří si svou identitu), nechá se přizvat členy své komunity, nebo se do ní vydá na vlastní pěst. Budujete si svou reputaci a čerpáte užitečná reputační data o ostatních, když je potřebujete. Hledáte u své komunity zastání, když se stane křivda — řeknete a doložíte, co k tomu máte, a komunita se na to podívá, podle relevance rozhodne, jestli to dá vědět i ostatním a jak případně pachatele zasáhne.

Celá tato krátká kniha je o tom, co musí být pod kapotou, aby to navenek takto mohlo jednoduše fungovat. Když to vydržíte, slibuji vám, že se vám svět, který dnes možná v mnoha věcech působí složitě, otevře pochopitelněji a přehledněji. Uvidíte, že hodně špatných věcí se dá nastavit tak, aby se šmejdům spravedlivěji nevyplácely. A není to nástroj, na kterém byste museli viset celou dobu online — stačí ho použít, když cítíte, že je potřeba.

Dále vám slibuji, že vám popisované uspořádání bude připadat bližší skutečným pohnutkám lidí a že je nepotřebuje ve jménu nějakého -ismu přetvářet.

A nakonec si ukážeme, jak nerevolučně řídit přechod do stavu, kdy se komunity zase stanou plnohodnotnými fungujícími společenskými útvary a nebudou si na to muset jen hrát.

■ Technický článek

Tato kniha je vysvětlujícím doprovodem původního technického článku „*Decentralized Reputation Network: A Framework for Voluntary and Uncorruptible Societal Organization*” (Pavel Kudrna, 2026). Pokud vás zajímá formální popis architektury, algoritmus výběru ověřovatelů a zdůvodnění ekonomických mechanismů, doporučuji začít rovnou tam.

■ Kapitoly na sebe navazují

Kniha je psána jako souvislý argument — každá kapitola staví na předchozí. Pojmy zavedené v jedné části se používají v dalších, včetně vysvětlivek pod čarou. Čtení na přeskáčku nedoporučuji.

Komu je kniha určena?

I přes graficky přívětivý formát je hlavní cílovou skupinou odbornější část zabývající se principy možných sociálně-obchodně-politických uspořádání lidské společnosti. Do stavu, kdy bych byl s to vysvětlit celou zde probíranou problematiku více přístupněji nejširší veřejnosti, vede ještě dlouhá cesta, kdy je nutné vybudovat celou komunikační strategii.

Vítám podněty, jak udělat celé dílko, nebo i navazující opravná vydání, srozumitelnější.

Varování

Nevím, kdo jste, kolik vám je a kolik nesplněných slibů jste už v životě vyslechli. Tady s nimi končím. Naopak vás chci varovat, že výsledkem vašeho poznání tady může být jen uvědomění, že nejspíš neexistuje cesta, na které by ten dnešní bordel uklidil někdo jiný za vás. Popisuji jenom rámec / nástroj, který by úklid mohl zjednodušit a zpřehlednit. Na jeho základě se pokusím připravit sociální experiment / simulaci, opravit případné nedostatky, nebo nápad úplně pohřbít pod zem, když se ukáže, že má zásadní návrhové trhliny.

Prosba

Velice bych si vážil, kdybyste i po dočtení této knihy zachovali nápadu přízeň a sledovali, kam se ho daří posouvat a jak obstojí pod věčnou kritikou. Ještě víc bych ocenil pozdější zapojení — že byste se pokusili navržené principy rovnováhy narušit vlastními nápady a tím líp otestovat, jak je systém připravený na skutečné chování lidí.



Pod tím je toho víc. Zůstaň se mnou.

Bez vás a vašeho zapojení nápad zůstane jen teorií v šuplíku. Bez vás a vašich příspěvků a finančních darů se nepodaří projekt posunout k realizaci sociálního experimentu, a tedy k reálné připravenosti. Bez vás a vaší věcné kritiky ustrneme tam, kde jsme teď, nebo se necháme spolknout svatým grálem centristů — a tím je absolutní nezvratitelná totalita. Je jen na nás, kterou cestu si zvolíme, nebo prosedíme.

Výzva

Nenakládáme vám zrovna málo. Už teď nesete náklady prostopášného řízení společnosti skrze okultisticko-zaříkavačské návody, podle kterých je společnost ideální řídit centralizovaně — a já si dovolím po vás chtít ještě víc a jít proti těmto tendencím. Jsem si vědom toho, že budeme muset unést pád největší pyramidové hry v dějinách — průběžného důchodového systému — a nenechat přitom několik generací umřít hladu.

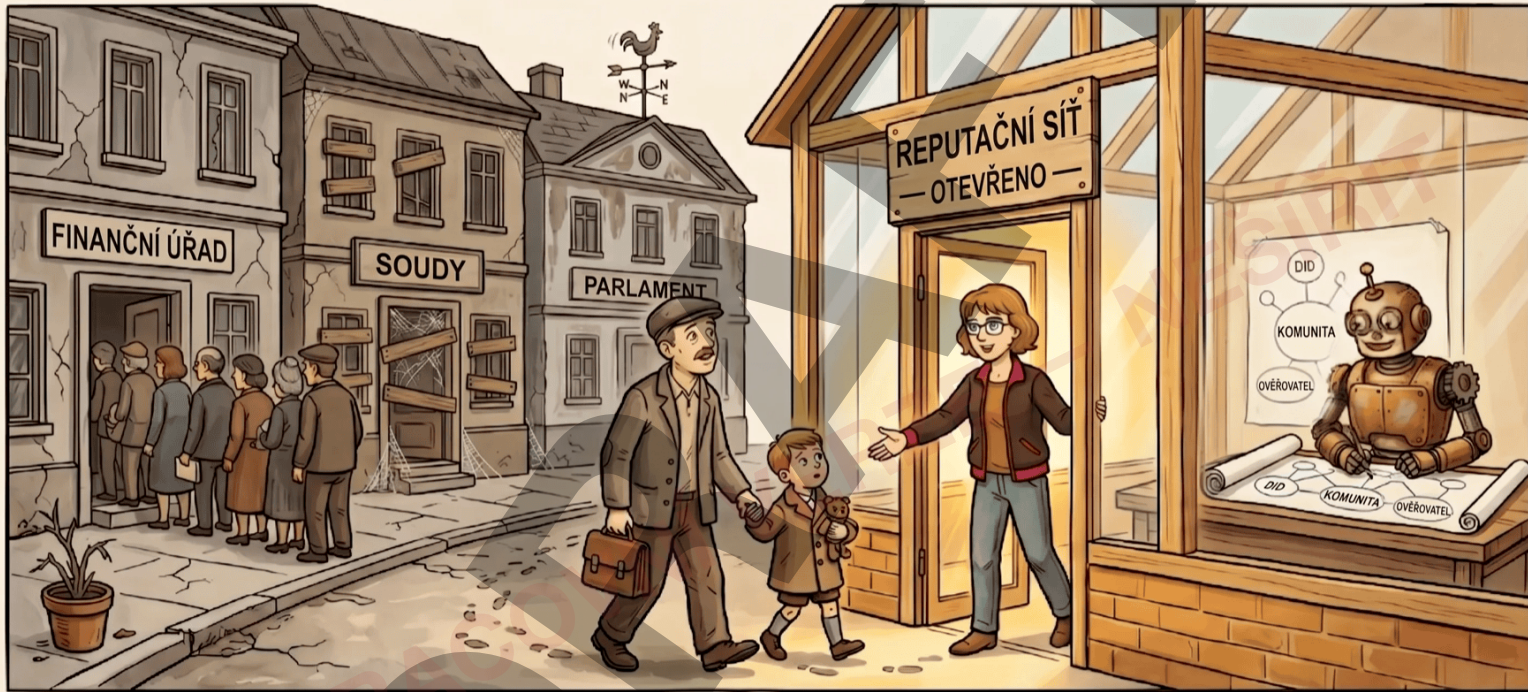
Přesto vás žádám o to, abychom našim dětem konečně předali lepší svět a zanechali po sobě odkaz, že jsme tu změnu zvládli. Puštění uzdy ekonomickému růstu by mohlo být částečným řešením svízelné situace na obzoru. Svým potomkům pak můžeme vyprávět, že to byla jízda a nebylo to marné.

■ Problém

Pouze svoboda vyvážená přímou odpovědností může skutečně uvolnit obrovský potenciál, jaký svět dosud neviděl.



Lepší svět stojí za tu zátěž.



Pojďte dál. Plány jsou připravené.

2. Nezbytné předpoklady změny

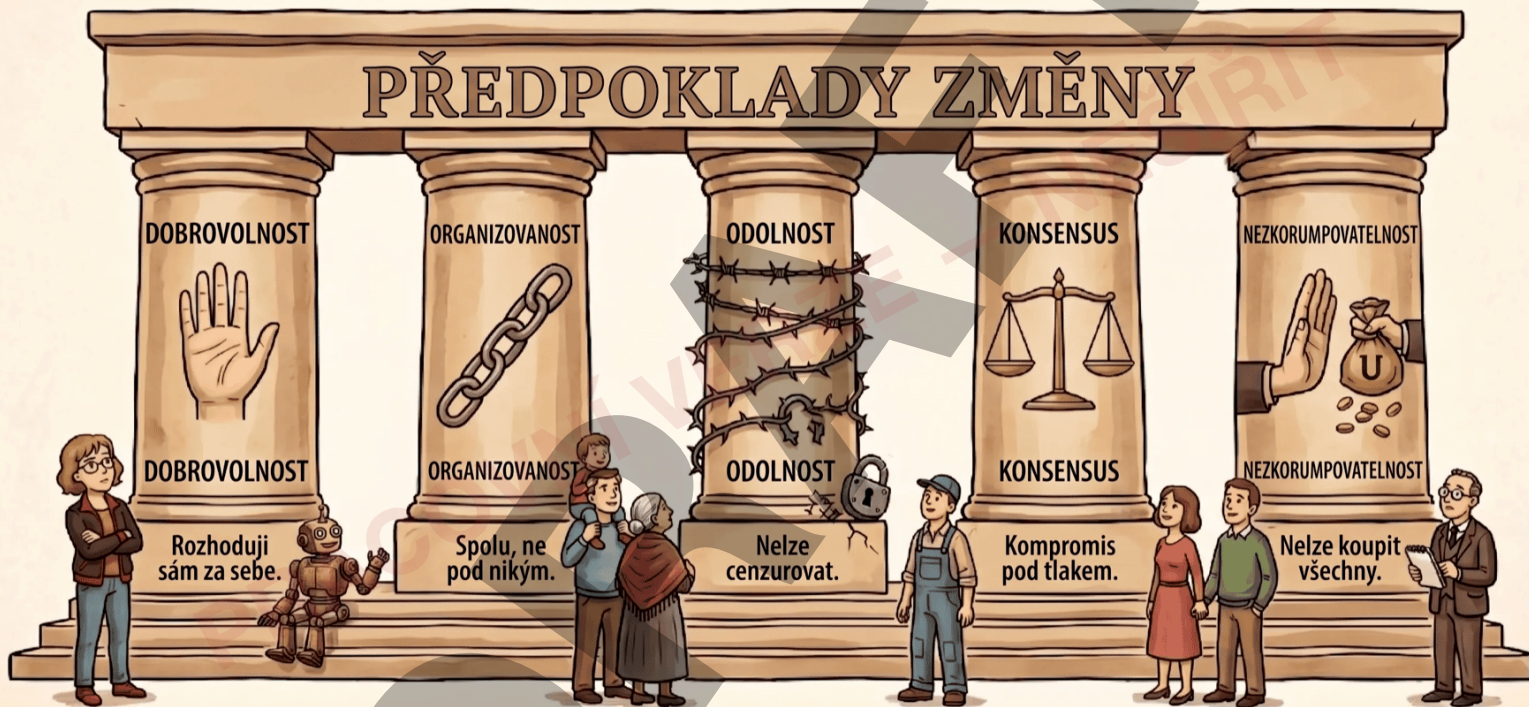
Základním předpokladem změny k lepšímu je, aby se z podřízeného stal nadřízený — nebo alespoň rovnocenný partner. To znamená převzít nejkritičtější agendy, které definují vztah nadřízenosti a podřízenosti. Tyto agendy stojí na důkazech příslušnosti ke komunitám, které tvoří občany státu. Jde o informace a o jejich ověřitelnost autoritou, která má v těchto komunitách podstatnou reputaci.

Představuji si pro překonání současného systému na první dobrou pět předpokladů, které následně vysvětluji, jak je chápu. Tyto předpoklady můžeme považovat za pilíře, které nesou konstrukci dále popisovaného systému. Vybral jsem pilíře zprvu dle své preference a během uvažování s nimi zacházel a mírně poupravoval jejich chápání až do následující podoby.

Pojďme si těchto pět pilířů projít jeden po druhém.

Dobrovolnost

Dobrovolnost v našem případě znamená, že se nemusím podílet na běhu decentralizované reputační sítě. Nemohu se však domáhat pozitivně definovaného práva na to, aby síť neevidovala informace o mně — zda budou v reputační síti informace o mně, záleží jen na mně, mém chování, mých činech a mé zodpovědnosti.



Bez těchto pěti pilířů je každá změna jen pálením času.



Dobrovolné — dokud tě nedožene odpovědnost.

■ Organizace

Jednotlivec systém rozbít nemůže, a proto stát kontroluje sdružování lidí jako prevenci činností, které by mohli ohrožovat jeho strukturu a fungování. Nezáleží na tom, jestli se organizují pro nebo proti. Skrze organizování je možné ztlumit dopad exemplárních trestů, když se někdo odváží měnit stát proti jeho vůli.

Nestanovujeme si společné cíle, ale můžeme jít kus cesty společně. Nejpřirozenější je sdružování v komunitách — ty však musí mít všechny potřebné nástroje, aby nezůstaly jen hraním si na komunity.

■ Odolnost

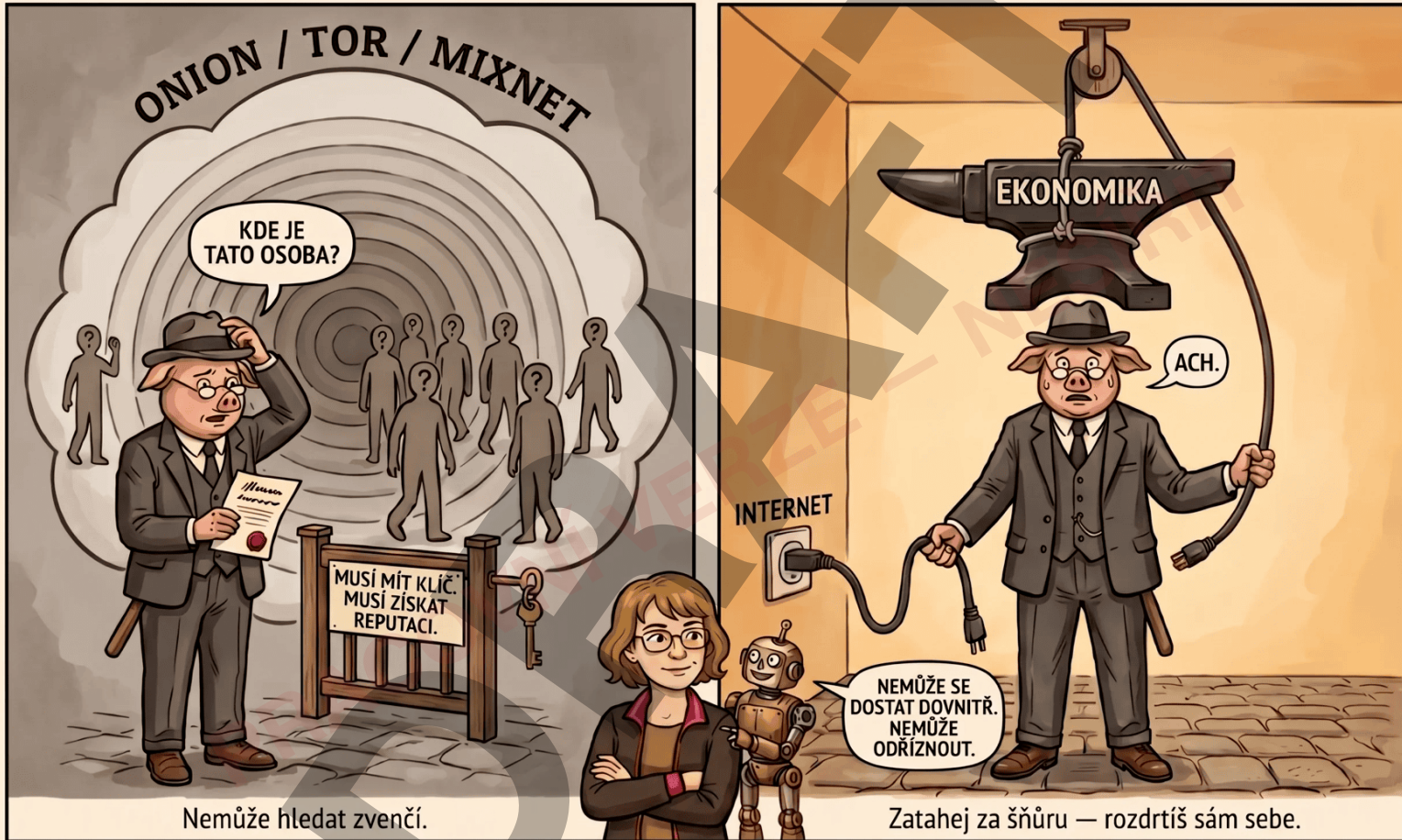
Zvolená cesta ke změně státu — nebo k přechodu k jeho nástupci — nesmí záviset na státním povolení. Nástroje a způsoby jejich použití musí být co nejvíce necenzurovatelné. V překladu to znamená, že náklady na jejich cenzuru musí být astronomické. Bez toho je celé úsilí jen pálením času a životní energie.

PŘEDPOKLAD 2 z 5: ORGANIZOVANOST



Jednotlivec systém rozbít nemůže. Komunita ano.

PŘEDPOKLAD 3 Z 5: ODOLNOST



ŽÁDNÉ POVOLENÍ K ŽÁDÁNÍ. ŽÁDNÁ ZÁSTRČKA K VYTAŽENÍ.

■ Konsenzus

Navrhované řešení musí ze své podstaty obsahovat mechanismus pro vyjednávání konsenzu i represivní složku pro případ jeho porušení. Nemusí jít o dobrovolnou dohodu výhra-výhra. Stačí, když okolnosti a sociální tlak zajistí kompromis napříč komunitou i mezi komunitami.

■ Nezkorumpovatelnost

Nezcenzurovatelnost chrání systém zvenčí. Ale síť lidí může hnít i zevnitř — autorita se nechá ovládnout, deklarované pravidlo se potichu přestane dodržovat, účastníky někdo v tichosti podmázne. Necenzurovatelnost by byla jen prázdným vítězstvím, kdyby lidé uvnitř šli bez následků zkorumpovat.

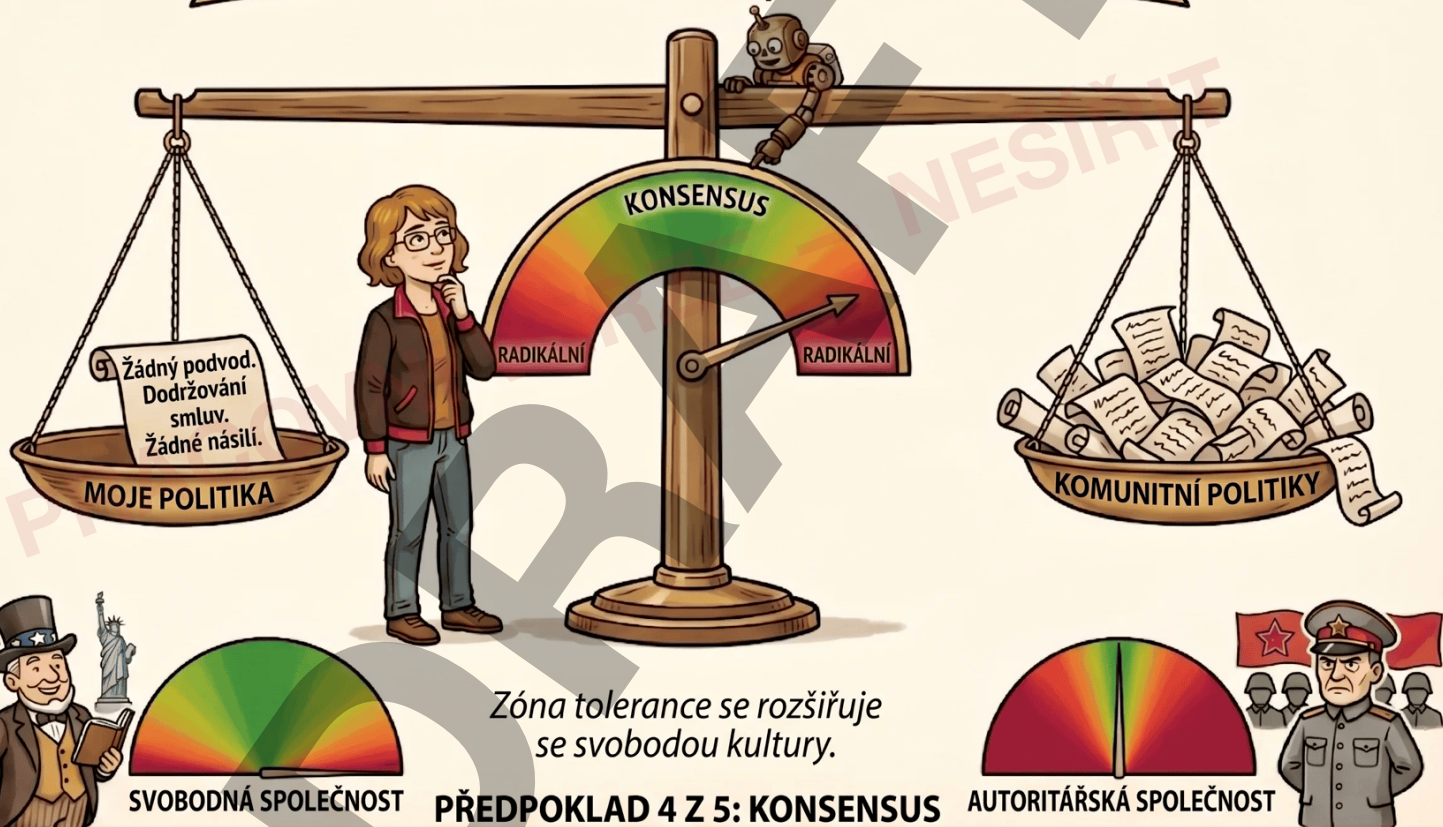
Nezkorumpovatelnost není výsledkem jediného chytrého triku. Vzniká ze **souhry několika principů navrženého designu** — tlak proti korupci je rozložen napříč architekturou a jednotlivé části se navzájem posilují. Jak konkrétně se toho dosahuje, ukážeme postupně — v popisu nástroje, v ověřování a v kapitole o trestu. V závěru si pak shrneme, co všechno se dohromady postavilo.

Nezkorumpovatelnost je zároveň předpokladem designu i emergentní vlastností výsledku. Je to druhá obranná linie — ta, která míří dovnitř — a bez ní je Odolnost jen poloviční štít.

Před redakční úpravou

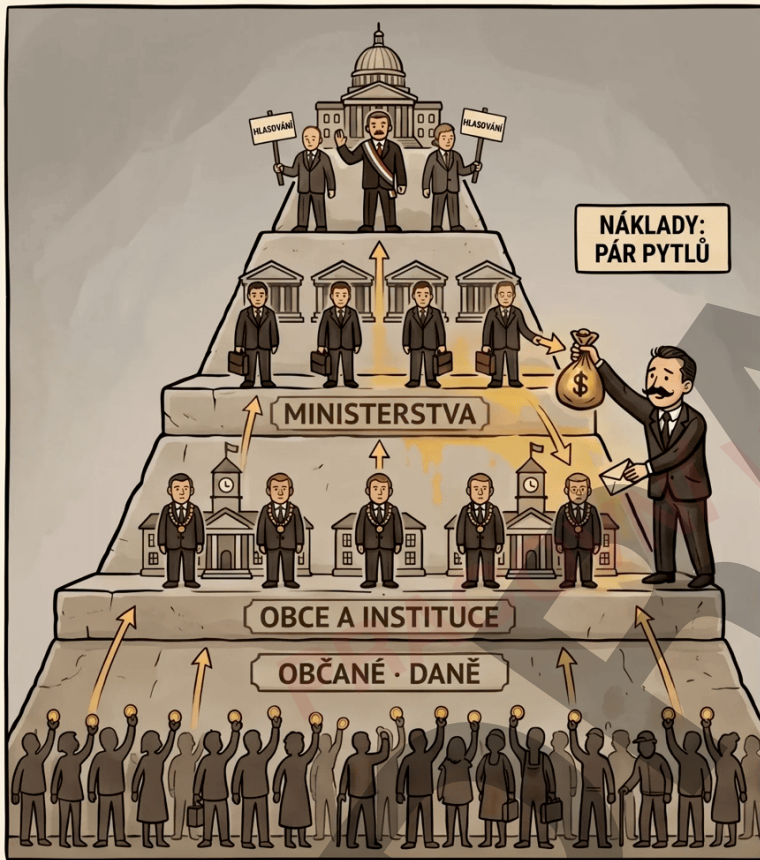
ZŮSTAŇTE V ROZSAHU – NEBUĎTE RADIKÁLNÍ.

Můžete se lišit. Jen ne příliš daleko.



KONSENSUS JE ZÓNA TOLERANCE, NE JEDNOMYSLNÁ DOHODA.

PŘEDPOKLAD 5 Z 5: NEZKORUMPOVATELNOST



Uplat' pár horních pater – základna to stejně zaplatí.



Uplat' jednoho – navždy ztratí reputaci. Uplat' všechny – zbankrotuješ dřív.

KORUPCE MÁ SVOU CENU. V SÍTI JE PŘÍLIŠ VYSOKÁ.

3. Nástroj

Reputační sociální síť (Reputation-Based Social Network)

Ke změně potřebujeme pečlivě připravený nástroj. Nejdříve ho stručně prolétneme a v pozdějších kapitolách probereme každou jednotlivost detailněji a doplníme další. Představte si necenzurovatelnou globální decentralizovanou sociální síť, kde byste mohli bezpečně vytvořit a spravovat svou zástupnou identitu — takzvanou decentralizovanou identitu (Decentralized Identity, DID). DID je digitální identita, kterou si vytváříte a kontrolujete sami, bez závislosti na jakékoliv centrální autoritě. Nikdo vám ji nemůže odebrat ani zfalšovat, protože je kryptograficky podepsaná vaším soukromým klíčem / klíči (multisig).

Poznámka

Jednou z implikací je, že taková identita může postupně nahradit státem vydávané průkazy totožnosti — ale o tom až v kapitole o přechodu.

V takové síti byste mohli nahlásit prostřednictvím své identity, že vám někdo způsobil křivdu / škodu (a později případně, že ji napravit nebo byl donucen ji napravit). Aby taková zpětná vazba směřovaná k původci křivdy měla hodnotu relevantního zdroje, vložení informace do sítě musí stát čas, energii a peníze — a navíc o tom musí vzniknout ověřitelný důkaz pro ostatní, že nejde o plané tlachání.

VAŠE IDENTITA, VAŠE KLÍČE, VAŠE PRAVIDLA

VYTVÁŘÍTE SI JI SAMI

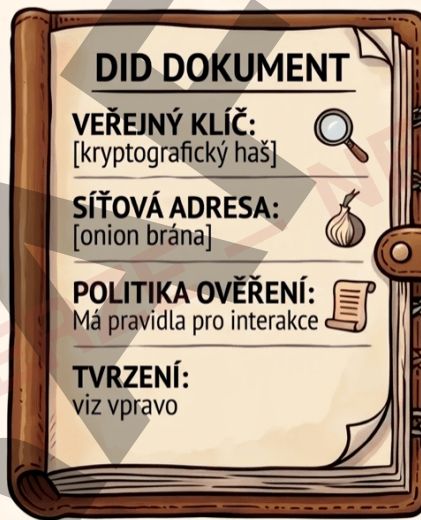
SOUKROMÝ KLÍČ – podepište jako vy, odemkněte svá data, nikomu nikdy nesdilejte

VEŘEJNÝ KLÍČ – ověřuje váš podpis, viditelný pro síť.



Žádná registrační kancelář.
Žádný vládní formulář.
Žádné schválení firmy.
Vygenerujete si ji sami.

VÁŠ DID DOKUMENT



Tohle je vaše veřejná identita. Každý si ji může přečíst. Jen váš soukromý klíč k ní může podepsat změny.

 Žádný stát to nemůže zrušit.

TVRZENÍ – OVĚŘENÁ FAKTA O VÁS

OBČANSTVÍ:
Česká republika –
ověřeno městským notářem

VZDĚLÁNÍ:
MSc Informatika –
ověřeno síti absolventů univerzity

VLASTNICTVÍ:
Majitel bytu č. 42 –
ověřeno místním komunitním registrem

PASIVNÍ SVĚDEK:
Ignoroval bezprávi –
nerespektoval zásady –
podáno sousedskými svědky

PODVOZ:
Podvedl souseda o úspory –
podáno místním komunitním soudem

Tvrzení jsou ověřená prohlášení.
Dobrá i špatná.
Úřady za ně ručí svou reputací.



STÁTNÍ ID – ODVOLATELNÉ:
stát ho může kdykoli zrušit.



DID – NEODVOLATELNÉ:
jen váš soukromý klíč k němu může podepsat změny.

Vaše identita. Vaše klíče. Vaše pravidla. Bez povolení.

Čtení informací by bylo snadné a relativně levné, ale vytvoření jednotlivého informačního záznamu nákladné a náročné. Zápis by podléhal jasnému protokolu, v němž by výpočet podle zvoleného algoritmu přísně určoval, jakou DID požádat o ověření vkládané informace a jak postupovat, aby vybraný účastník informaci vaším jménem zpracoval, zveřejnil a stal se jejím ověřovatelem.

■ Algoritmus vs radikalismus

Algoritmický výběr ověřovatelů zajistí, že neradikální vydavatelé informací časem udržují téměř neutrální rovnováhu mezi náklady na zveřejněné informace a odměnami za ověřování.

Pojďme se podívat, jak algoritmus vybírá ověřovatele.

PUBLIKOVÁNÍ STOJÍ ČAS, ENERGII A PENÍZE

PSANÍ DO SÍTĚ NIKDY NENÍ ZDARMA — ČTENÍ JE

ČAS



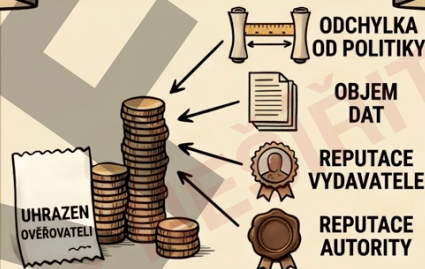
čekáte, dokud algoritmus nevybere ověřovatele a ověřovatel si nepřečte váš záznam.

ENERGIE



podepisování, hašování, ověřování — každý krok je reálný výpočet a reálná elektrina.

PENÍZE



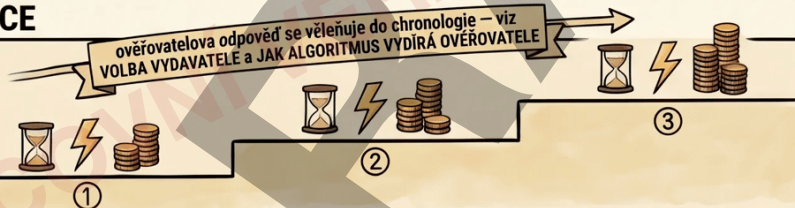
čím dále je vaše tvrzení od politiky ověřovatele, čím větší je záznam a čím méně důvěryhodný je vydavatel nebo jeho autorita — tím vyšší je poplatek.

CO SE DĚJE DÁL

- ⚙️ Tříkrokový řetězec ověřování — viz **JAK ALGORITMUS VYBÍRÁ OVĚROVATELE, JAK OVĚROVATEL ODOPOVÍDÁ, VOLBA VYDAVATELE**
- ⚙️ Proč drahé psaní chrání reputaci — později v kapitole

NÁKLADY NA ITERACE

KAŽDÝ DALŠÍ POKUS STOJÍ VÍC



každé odmítnutí nebo opakované podání se přidává do chronologie, kterou algoritmus "jí" — a další pokus je dražší ve všech třech kanálech.

ASYMETRIE ČTENÍ

ČTENÍ JE LEVNÉ

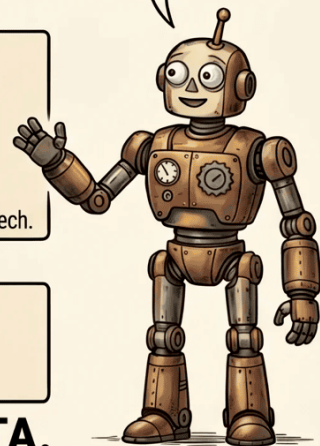


zdarma dotazování

každý si může číst reputaci a záznamy — pouze psaní stojí peníze. Asymetrie je pointou designu.

PSANÍ STOJÍ PENÍZE — ČTENÍ NE. ASYMETRIE JE POINTA.

šum je drahý.
Signál je cenný. Proto síť účtuje za psaní, nikoli za čtení.



■ Algoritmus

Algoritmický výběr pro různé informace nedeterministicky volí jiného ověřovatele (nebo sadu možných ověřovatelů). Hash (jednosměrná matematická funkce, která z libovolného vstupu vytvoří unikátní „otisk“ — jako otisk prstu dokumentu) kompletního DID dokumentu určuje pozici na konzistentním hash ringu a vybírá kandidáty na ověřovatele.

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

Lidsky řečeno: algoritmus vezme celý váš DID dokument, spočítá z něj otisk a ten určí vašeho ověřovatele.

U prvního ověřovatele, kterého algoritmus vybere, jako vydavatel informace nemusíte uspět — vaše reputace nebo deklarovaná nastavení mu nemusí vyhovovat. Algoritmicky byste pokračovali v hledání dalšího tak, že rekurzivně provedete další iteraci a ten vám přidělí dalšího ověřovatele. S každým krokem se „vzdálenost“ k cílovému ověřovateli zvyšuje, a tím rostou i doprovodná metadata, která se musí zveřejnit. S růstem dat přirozeně rostou i náklady (nejen kvůli výchozí velikosti tvrzení, ale i kvůli nabalujícím se metadatům z každého odmítnutí k ověření). Věrohodná informace projde mnohem snáze než nesmyslné rozmary. Záleží na každém, jak vysokou cenu je ochoten nést a jak moc mu na záznamu záleží — radikalismus se jisto-jistě prodraží.

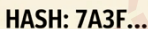
Před redakční úpravou

***každá tvář má stejnou šanci –
hash dopadá rovnoměrně náhodně**

**Nemůžete si vybrat
věrovatele – algoritmus
házi kostkou a všichni
mají stejnou šanci.**

- ☀ Ověřovatel odpovídá s cenou – nebo odmítá s důvodem – viz JAK ODPOVÍDÁ OVĚŘOVATEL
- ☀ Vydávatel se rozhodne, co s tím udělá – viz VOLBA VYDÁVATELE
- ☀ Každý opakovaný pokus zvyšuje náklady – jak bylo uvedeno dříve u NÁKLADŮ NA PUBLIKOVÁNÍ

ALGORITMUS VYBÍRÁ — VY NE.

váš
ověřovatel

***cesta k publikování vede:**
vydavatel → autorita → ověřovatel. Žádný
záznam nesmí přeskočit krok autority.

Mohl bych umlít tisíce návrhů, než jeden

hash je deterministický, ale odolný vůči předobrazům – každá malá úprava hodí výběr někam nesouvisející.

➤ MÍRNĚ JINÉ
HODNĚ JINÉ
ÚPLNĚ JINÉ

DŮKAZY PODEPSANÉ AUTORITOU O OSTATNÍCH

SVNIDLÝ DÍFEŘENT
WÍLDLY DÍFEŘENT
CÓMPLÉTELY DÍFEŘENT

protože hash požírá důkazy podepsané autoritou, vydavatel nemůže předpovědět svůj vlastní hash. Pro komunitu se otázka stává: dávujeme této autoritě – a tomuto vydavateli s touto autoritou – vůbec?

JAK OVĚŘOVATEL ODPOVÍDÁ

PŘIJMOUT S CENOU – NEBO ODMÍTNOUT S DŮVODEM

**ověřovatel zvažuje čtyři věci, než odpoví.*



ODMÍTNOUT – S DŮVODEM

- reputace vydavatele je pro mě příliš nízká
- autorita stojící za tímto záznamem není důvěryhodná
- politika vydavatele je příliš daleko od mé přemostění
- samotný dokument selhává v pravidlech mé politiky

ověřovatel zapíše **PROČ** — jejich odpověď se vrací do dalšího pokusu.

PŘIJMOUT – S CENOU



ověřovatel souhlasí s publikováním — ale cena odráží, jak daleko tvrzení stojí od jejich politiky, kolik dat přenáší a jak důvěryhodný je vydavatel.

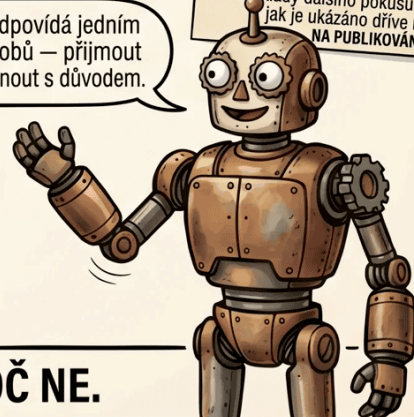
odpověď ověřovatele je přidána do chronologického seznamu — jak je znázorněno na **JAK ALGORITMUS VYBÍRÁ OVĚŘOVATELE**

cokoliv ověřovatel řekne, jejich odpověď se stane vstupem pro další volání.

každý ověřovatel odpovídá jedním z těchto dvou způsobů — přijmout s cenou, nebo odmítnout s důvodem.

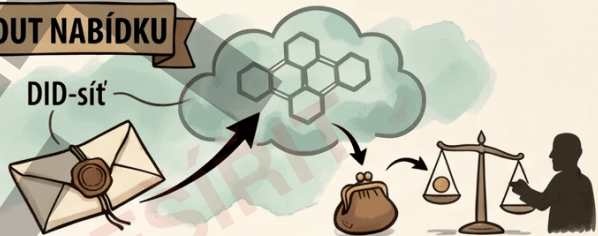
CO SE DĚJE DÁL

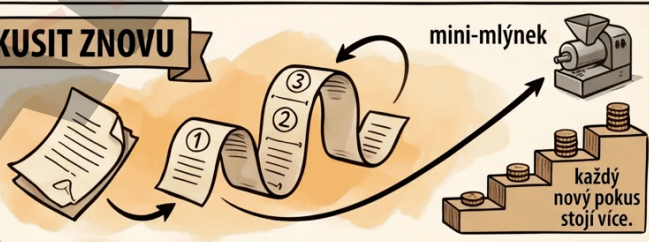
- Vydavatel se rozhodne, co s touto odpovědí udělá — viz **VYBĚR VYDAVATELE**
- Každá odpověď posune náklady dalšího pokusu — jak je ukázáno dříve na **NA PUBLIKOVÁNÍ**



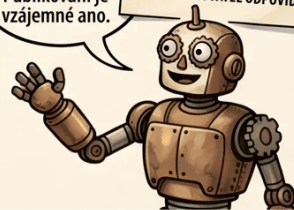
OVĚŘOVATEL BUĎ STANOVÍ CENU — NEBO VÁM ŘEKNE PROČ NE.











Ať už se ověřovatel rozhodne v odpovědi na vaši žádost o ověření jakkoliv, míček se vrací zpět k vydavateli: ten může nabídku ověřovatele za ověřovací služby přijmout, založit odpověď do chronologie a zkusit to znovu (draž), nebo odejít a smířit se s utopenými náklady.

Abyste své informaci jako vydavatel, který má zájem na vydání informace, dodali větší váhu a lepší šanci na přijetí u ověřovatelů, mohli byste využít služeb **důvěryhodné autority**. Ta předloženou informaci buď odmítne, nebo přijme a vsadí na ni své dobré jméno (reputaci). Autorita obvykle požádá o předložení důkazů z reálného světa, ověří je a klasifikuje. Výstupem je protokol o jejím zhodnocení daného případu v daném čase. Autoritu si představte jako specialistu na jistý typ služeb v reálném i digitálním světě — např. vyšetřovatele, auditora, pojišťovnu, dodavatele jistého typu zboží (v podstatě každý ekonomický aktér na trhu).

V době, kdy se budete snažit publikovat informaci v síti, už patrně bude obsahovat informace o jejích aktérech — to jsou reputační signály. Orientovat se v tom, jak reputační signály číst — co pro vás v různých situacích znamenají a jaká rizika nesou — nemusí být triviální. Každý účastník se může přes svou DID na reputační záznamy dívat různě, podle situace, kterou s protistranou řeší. Je protistrana spolehlivý plátce, nebo musím chtít peníze předem při obchodním styku? Nemá v nabízeném produktu recenze na skryté podvody a vady? Nesnaží se zbavit smluvní odpovědnosti, když se něco nepovede? Někdy se hodí i komplexnější pohled na celkovou konzistenci protistrany — záleží na preferencích toho, kdo si náhled vyžádá. Trh by mohl nabízet produkty a služby, které čtení reputace v kontextu řešené situace zjednodušují, zpracovávají a vysvětlují. I k tomu mohou sloužit rozličné autority a jejich nabízené služby.

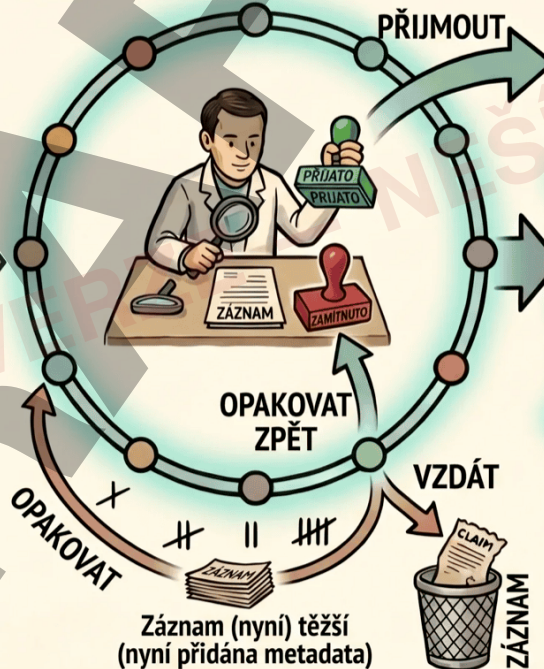
FÁZE 1 — ZVEŘEJNĚNÍ ZÁZNAM



FÁZE 2 — FILTR KVALITY



FÁZE 3 — REKURZIVNÍ OVĚŘENÍ



FÁZE 4 — TRVALÝ ZÁZNAM



Trvalý.
Ověřitelný.
Veřejný.

DRAHÉ PADĚLAT. LEVNÉ OVĚŘIT.

JAK ČÍST REPUTACI

INFORMOVANÉ ROZHODNUTÍ



Ví, s kým má co do činění.

DŘÍV NEŽ POSKYTNEŠ ÚVĚR. DŘÍV NEŽ PODEPÍŠEŠ. DŘÍV NEŽ DŮVĚRUJEŠ.

SLEPÁ DŮVĚRA



Netuší, s kým má co do činění.

■ Příklady

Typické informace zajímavé pro vydavatele — a hodnotné pro ostatní — se týkají událostí mimo běžnou mezilidskou komunikaci v reálném nebo virtuálním světě.

Negativní příklady: - důkazy o trestných činech (např. auditované důvěryhodným vyšetřovacím orgánem) - nepřímé důkazy (samy o sobě slabé, ale statisticky kumulativní) — např. opakovaná přítomnost v blízkosti více krádeží v krátkém čase → stále náhoda? - porušení smlouvy

Pozitivní příklady: - napravená škoda (dobrovolně nebo z nátlaku komunity jako trest) - přijetí a odpykání trestu navrženého autoritou XY - autorita XY odejmula uznání vlastnických práv pachatele v určitém rozsahu

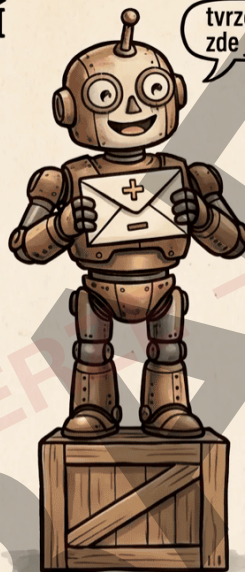
Je na každém, aby si dostupné informace o protistraně sehnal a vyhodnotil rizika dle jeho preferencí

JAKÁ TVRZENÍ SE MOHOU OBJEVIT?

PŘÍKLADY ARTEFAKTU TVRZENÍ

- NEGATIVNÍ TVRZENÍ

-  **NAPADENÍ**
fyzicky napadl jinou osobu
-  **KRÁDEŽ**
vzal něčí majetek bez souhlasu
-  **PODVOĐ**
podvedl někoho pro osobní zisk
-  **PORUŠENÍ SMLOUVY**
nesplnil dohodnutý závazek
-  **POMLUVA**
šířil poškozující nepravdu
-  **OPUŠTĚNÍ**
opustil závislé osoby nebo zanedbal povinnosti



tvrzení je prohlášení o někom -
zde jsou druhy, které lidé publikují.

+ POZITIVNÍ TVRZENÍ

-  **NAPRAVENÍ ŠKODY**
opravil dříve způsobenou škodu
-  **VYROVNÁNÍ DLHU**
zaplatil, co bylo dluženo v plné výši
-  **POSKYTNUTÍ POMOCI**
pomohl jinému na vlastní náklady
-  **OVĚŘENÁ ODBORNOST**
prokázaná dovednost v řemesle nebo oboru
-  **MIMOŘÁDNÉ SLUŽBY**
dlouhodobý přínos komunitě



pouze příklady - každé tvrzení se řídí standardem tvrzení a jakýkoli standard může přidat další.

nemusíte se připojit - ale pokud vaše chování ovlivňuje ostatní, někdo o tom může publikovat tvrzení.

TVRZENÍ JSOU ZPŮSOB, JAKÝM CHOVÁNÍ VSTUPUJE DO SÍTĚ.

KOMUNITA VÁM JI MŮŽE OTEVŘÍT



Žádné DID nemá.
Nikdy se nepřihlásil.



Neotevřel jste DID, tak ho komunita otevře **O VÁS**. Negativní tvrzení se sem připojují.



Můžete si otevřít vlastní – ale komunita obě propojí. Reputace sleduje osobu, ne klíč.

1. UBLÍŽÍŠ NĚKOMU -----> 2. KOMUNITA ZAZNAMENÁ -----> 3. NEMŮŽEŠ UNIKNOUT->

Můžete se rozhodnout nezakládat DID. Nemůžete se rozhodnout nezakládat svou reputaci.

■ Zda se informace o vás v síti objeví, závisí výhradně na vašem vlastním chování.

Do takové sítě se nikdy nemusíte připojit, a přesto se v ní mohou informace o vás objevit. Záleží výhradně na vašich činech a na tom, jaký mají dopad na ostatní.

Právě jsem ve zkratce navenek popsal, jak by mohla fungovat sociální síť inspirovaná decentralizovanou identitou (DID). Primárním účelem konceptů DID je posílit soukromí a svobodu principem přihlášení se k pravidlům, která budu dodržovat a dle kterých budu žít — dát uživatelům možnost rozhodovat, jaké informace sdílet a za jakých podmínek.

Navrhuji dále propojit DID do komunikační sítě, kde si jejich nositelé vyměňují zpětnou vazbu i mimo situace, kdy se někomu něco přihodilo a je třeba reagovat komunitně nebo jednotlivě. Takové preventivní porovnání pravidel, ke kterým jsme se přihlásili s možností si spočítat ekonomické a jiné dopady vzájemných odchylek představ o tom, jak by měl ten druhý fungovat, by se dalo považovat za motivaci k nacházení konsenzu. Namísto svobody by takový systém kladl důraz na dobrovolné rozhodování spojené s odpovědností za chování v reálném světě.

Jednotlivec systém sám nerozbije — skupina lidí má větší šanci a skupina lidí s vyjednaným konsenzem a motivacemi táhnout v mnoha věcech za jeden provaz ještě větší šanci bojovat s autoritářskými tendencemi. Předpoklad organizace z první kapitoly bude splněn, až se naplní dvě podmínky: DID reputační síť pokryje komunity natolik reprezentativně, že její používání přestane být exotické. A zároveň se tato komunitní část stane ekonomicky signifikantní menšinou, která může asertivně vyjednávat se zbytkem společnosti.

■ Dobrovolnost vs svoboda

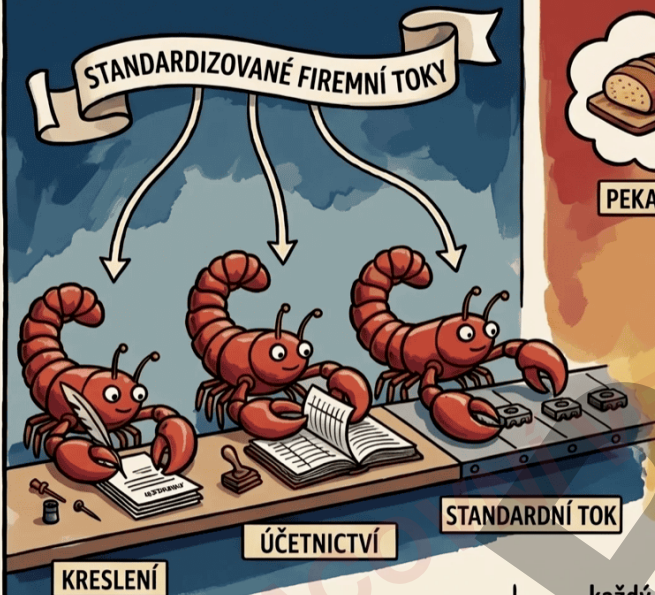
Svoboda — v pozitivním smyslu — by byla sekundárním efektem vyvažování dvou faktorů: dobrovolnosti a tlaku okolí na odpovědnost.

■ Éra AI a hodnota reputace

V éře umělé inteligence se automatizuje vše, co souvisí s kognitivním myšlením — a možná to půjde ještě dál. Co potom v mezilidské činnosti zbude jako konkurenční výhoda? Odpověď je těžká a něco se jistě najde, ale jednu věc můžeme říct s jistotou: rozhodne reputace. Ověřitelná historie vašeho chování, vašich závazků a jejich plnění — to je něco, co za vás AI nepostaví.

KDYŽ AI PŘEMÝŠLÍ ZA VÁS – CO ZBÝVÁ VÁM?

AI AGENTI PŘEBÍRAJÍ OPAKUJÍCÍ SE PRÁCI



jeden po druhém, opakuji se kognitivní úkoly jsou předávány agentům.

TAK CO ZBÝVÁ ČLOVĚKU?



každý si může vybrat stejný nápad. co odlišuje jednoho pekaře, jednoho truhláře, jednu AI dílnu od druhé?

REPUTACE – CO JE OD SEBE ODLÍŠUJE



někdo musí nést odpovědnost za to, co agent udělá – a tuto odpovědnost nelze přenést.

bez reputace vypadá každý pekař stejně – a největší značka je všechny spolkně.

mohla by to být ta decentralizovaná cesta, která drží AI na vodítku – věc, která brání jakémukoli jednomu hráči ovládnout celý trh? °

AI AUTOMATIZUJE PRÁCI – REPUTACE VÁS ČINÍ ČLOVĚKEM.

EKONOMIKA PRAVDY

KOMUNITNÍ
PÁS



JEDNA KOMUNITA. RŮZNÉ POZICE.

NEPOPULÁRNÍ ALE PŘIJATELNÉ

PODÁNÍ



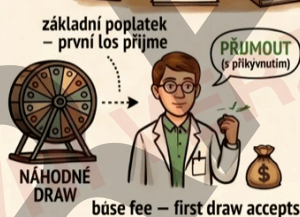
V KONSENSU



MIMO KONSENSUS



LOSOVÁNÍ



VRÁCENÍ



ÚČETNÍ
KNIHA

SPODNÍ PÁS
POZOROVATELE

ALGORITMUS VYBÍRÁ FÉROVĚ.
LIDÉ OCEŇUJÍ TO, ČEMU VĚŘÍ.

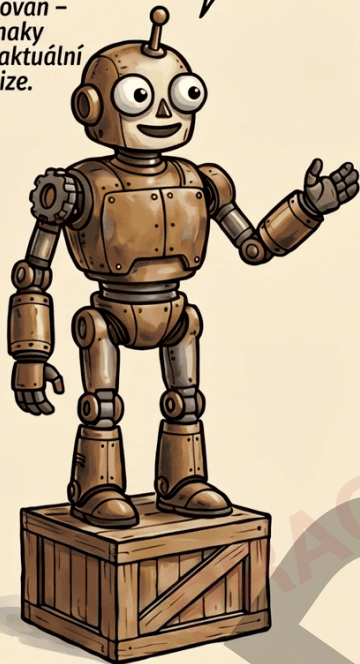


ROVNOMĚRNÉ LOSOVÁNÍ. NEROVNOMĚRNÁ ODPOVĚĎ. ČÍM DÁL OD KONSENSU, TÍM VYŠŠÍ CENA.

CO SE PUBLIKUJE V SÍTI

lze publikovat
pět věcí – každá
má verze.

každý artefakt
je verzován –
odznaky
ukazují aktuální
revize.



v1

DID DOKUMENT

váš záznam identity v síti
– klíče, metadata,
síťová adresa.

SPRÁVCE: držitel DID



v2

STANDARD TVRZENÍ

schéma, které musí tvrzení
dodržovat – co se počítá
jako platný důkaz.

SPRÁVCE: autorita s reputací
v dané doméně



v3

STANDARD POLITIKY

schéma, které musí politika
dodržovat – podoba
pravidel přijetí.

SPRÁVCE: autorita s reputací
v dané doméně

↓ odvozeno z

↓ odvozeno z



v4

TVRZENÍ

prohlášení o subjektu podle
standardu tvrzení – publikováno
vydavatelem, spolupodepsáno
autoritou standardu, pokud o to oba
požadají: vydavatel a ověřovatel.

SPRÁVCE: vydavatel publikuje –
subjekt je cílem

tvrzení existují ve dvou druzích –
pozitivní (+) a negativní (-).



v5

POLITIKA DID

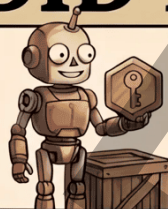
deklarovaná pravidla DID –
používaná při ověřování,
konsensu a vydávání.

SPRÁVCE: držitel DID
(jedna politika na DID)

KAŽDÝ ARTEFAKT JE VERZOVÁN. KAŽDÁ VERZE JE VEŘEJNÁ.

CO JE UVNITŘ DID DOKUMENTU?

PŘÍKLADY DID DOKUMENTNÍHO ARTEFAKTU



tvůj DID dokument je tvou identitní kartou na síti — zde je, co obsahuje.

POLE, KTERÁ UVNITŘ NAJDETE



KLÍČE A PRAVIDLA PODEPSÁNÍ

každý klíč uděluje jednu pravomoc — upravit tento dokument, vydat tvrzení, jednat jako autorita, spravovat politiku, nebo delegovat obnovu. Pravomoci mohou být předány jinému DID a později opět revokovány.

SÍŤOVÉ ADRESY

kde vás síť může zastihnout — změnitelně bez přepisování vaší identity

VYTVOŘENO A VERZOVÁNO

kdy se tato identita poprvé objevila a kterou revizí právě čtete

PROPOJENÉ IDENTITY

přehled DID, ke kterým jste připojeni — pohodlný náhled, technicky uložený jinde

MARKER NÁSTUPNICTVÍ

pokud je vaše identita ztracena nebo ukradena, autorita může tento DID označit za ukončený a odkázat na vašeho nástupce

držitel DID píše každou novou verzi — ale každá verze musí projít ověřením před tím, než ji síť publikuje.

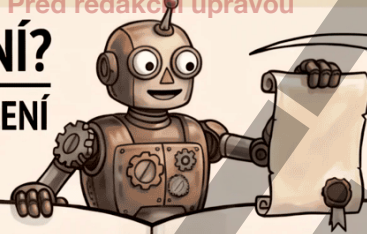
ty to napíšeš — síť to ověří. Nemůžeš se jen tak publikovat k existenci.



TY PÍŠEŠ SVOU IDENTITU — SÍŤ JI POTVRZUJE.

CO JE TO STANDARD TVRZENÍ?

PŘÍKLADY ARTEFAKTU STANDARDU TVRZENÍ



Standard je prázdný formulář
— tvrzení je formulář vyplněný.
Ukážu vám oba vedle sebe.

STANDARD — PRÁZDNÝ FORMULÁŘ



DID SUBJEKTU

DID, o které se toto tvrzení týká



DID VYDAVATELE

DID, které tvrzení podepisuje



KDY A KDE

datum a místo



SCHVÁLENÉ TYPY DŮKAZŮ

počítají se jen tyto druhy důkazů



none
mild
moderate
severe

ŠKÁLA VÝSLEDKU

vyberte přesně jednu příčku — žádný volný text

TVRZENÍ — VYPLNĚNÝ FORMULÁŘ



DID SUBJEKTU

did:nwo:alice-9f2b...



DID VYDAVATELE

did:nwo:magistrates-04...



KDY A KDE

3. březen, tržní náměstí



SCHVÁLENÉ TYPY DŮKAZŮ

fotografie ✓ — přísaha svědka ✓
— lékařská zpráva ✓



ŠKÁLA VÝSLEDKU

mírný — příčka 2 ze 4

Každé pole vlevo má přesně jeden vyplněný protějšek vpravo — to činí dvě tvrzení stejného druhu srovnatelnými.

Pečeť autority na vyplněném tvrzení
je síb: postup byl skutečně dodržen.



Vsadím svou pověst na to,
že toto bylo zpracováno
standardem.



NAPADENÍ

v3



DLUH

v2



LÉKAŘSKÁ POMOC

v4



ŘEMESLNOST

v1



SVĚDECTVÍ

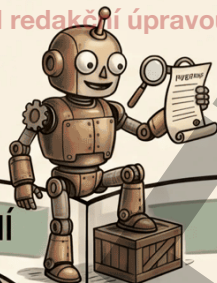
v5

STANDARD JE FORMULÁŘ — TVRZENÍ JE VYPLNĚNÝ A STVRZENÝ POVĚSTÍ FORMULÁŘ.

CO JE TO DID POLITIKA?

PŘÍKLADY ARTEFAKTU DID POLITIKY

Před redakční úpravou



moje politika není o tom, jak je tvrzení napsáno — to je práce standardu. Moje politika je o tom, jak se rozhodují, zda se o tvrzení vůbec starat: důvěřuji tomu, kdo jej podepsal, důvěřuji autoritě za jejich standardem, a stojí ta záležitost vůbec za mou pozornost?

STANDARD — ZDĚDĚNÁ VÝCHOZÍ NASTAVENÍ

NÁZEV PRAVIDLA	POPIS PRAVIDLA
SPODNÍ HRANICE REPUTACE VYDAVATELE	Přijímám vydavatele s reputací nad pět z deseti
SEZNAM DŮVĚRYHODNÝCH AUTORIT	Přijímám standardy od jakékoli autority, jejíž vlastní reputace je nad čtyři z deseti
FILTR PODSTATY	Zpracovávám jakékoli tvrzení, jehož podstata váží nad ryskou 'bezvýznamné'.
PROTISPAMOVÁ CENOVÁ KŘIVKA	předložení mně je levnější pro podstatná, vzácná tvrzení — a rychle roste pro malicherná nebo opakovaná
KOMBINOVANÉ VÁŽENÍ	reputace vydavatele a reputace autority se násobí; malicherná podstata výsledek půli

MOJE POLITIKA — ODVOZENÁ Z NĚJ

NÁZEV PRAVIDLA	✓ PONECHÁNO (fajfka)	✍️ UPRAVENO (tužka)	✗ ODSTRANĚNO (křížek)	✚ PŘIDÁNO (plus)
SPODNÍ HRANICE REPUTACE VYDAVATELE	zprůsněno — vyžaduji sedm z deseti			
SEZNAM DŮVĚRYHODNÝCH AUTORIT	Plně důvěřuji magistrátům a lékařům; půlim váhu tvrzení pod městskou stráží; cokoli pod přístavní policií odmítám úplně			
FILTR PODSTATY	malicherná otravná tvrzení mě nestojí nic na ignorování — prostě je nečtu			
PROTISPAMOVÁ CENOVÁ KŘIVKA	ponecháno — výchozí křivka mi vyhovuje			
KOMBINOVANÉ VÁŽENÍ	odstraněno — používám vlastní vzorec			
EXPONENCIÁLNÍ NÁKLADY NA OPAKOVANÁ TVRZENÍ	přidáno — každé nové tvrzení od stejného vydavatele o mně v roce stojí desetkrát tolik, co předchozí			
KLIDNÉ HODINY	přidáno — odmítám čist jakékoli tvrzení podané mezi půlnocí a úsvitem			



OVĚŘENÍ — moje politika filtruje jak přichází tvrzení, tak mé vlastní koncepty, než je vydám. Vydání je ověření na cestě ven.

KONSENZUS — moje politika je můj hlas, když komunita vyjednává o sdílených pravidlech.



VAŠE POLITIKA POSUZUJE POSLA — NE FORMU.

Proč je síť necenzurovatelná

Zatím jsme popsali, co síť umí. Teď se zaměříme na to, proč ji nelze vypnout ani cenzurovat.

Síť bude patrně postavena na principech sítě Tor a onion routingu (způsob maskování datového provozu pomocí principů Mixnet) — technologie, kde komunikace prochází několika vrstvami šifrování a žádný jednotlivý uzel nezná současně odesílatele i příjemce. Centrální instituce vám pod ruce nenahlédne, protože není kam.

Můžete s tím bojovat, ale vyhrát ne — leda byste celou zemi uvrhli do totalitního sledování na úrovni jednotlivých síťových paketů a low-level akcí na každém hardwarovém zařízení, které se do internetu připojuje a komunikuje v dané reputační síti. A právě před touhle volbou centralismus stojí: buď přijmout, že občané mají nástroj mimo váš dosah, nebo se odkopat do temných zákoutí ekonomického zaostávání ve jménu totalitní kontroly.

Nedělejme si iluze — i demokratická zřízení se o to v boji za centralismus pokusí. Raději lidi uvrhnou do okovů, než by se vzdaly moci.

Řešení zjevných pochybností

Popsaný systém přirozeně vzbuzuje řadu otázek. Pojdme si ty nejčastější probrat.

Závislost na technologii

Určitě vás již napadlo, že na rozdíl od moderního státu, který je s námi něco kolem 150 let, řešení reputační sítě, tak jak je zde popisována, závisí silně na technologii globálního/lokálního internetu. V případě jeho výpadku je fungování takové sítě ohroženo.

JAK VAŠE ZPRÁVY ZŮSTÁVAJÍ NESLEDOVATELNÉ

DVĚ OBRANNÉ LINIE ZÁROVEŇ — VRSTVY A ŠUM

OBSAH: OBALEN VE VRSTVÁCH

(technika za Torem — „onion routing“)



čtyři zámky, čtyři klíče —
jeden pro každý uzel.



ZNÁ: JEN
ODESÍATELE



ZNÁ: JEN
SOUSEDNÍ
UZLY



ZNÁ: JEN
SOUSEDNÍ
UZLY



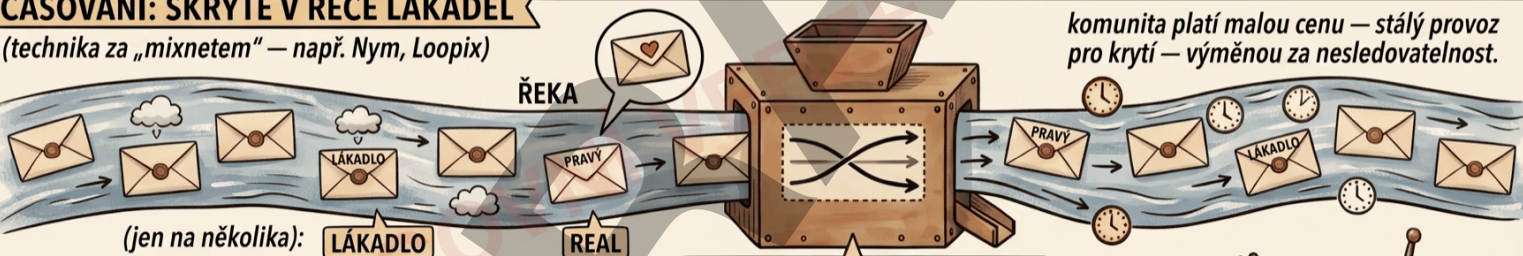
ZNÁ: JEN
PŘÍJEMCE



žádný uzel nevidí oba konce konverzace.

ČASOVÁNÍ: SKRYTÉ V ŘECE LÁKADEL

(technika za „mixnetem“ — např. Nym, Loopix)



(jen na několika):

LÁKADLO

REAL

UZEL-MIXÉR — MÍCHÁ + ZPOŽĐUJE

DVA ŠTÍTY SPOLU

MATRICE SKRÝVÁ KDO SKRÝVÁ KDY?

JEN VRSTVY	✓ ANO	✗ NE
JEN ŠUM	✗ NE	✓ ANO
VRSTVY + ŠUM	✓ ANO	✓ ANO

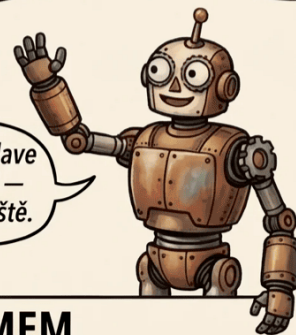
(onion routing + mixnet — kombinace, kterou potřebujeme)



sto obálek za hodinu
— na které záleží?

pozorovatel vidí tok, ale
nedokáže odlišit PRAVÝ od LÁKADLA.

pravá zpráva plave
v řece lákadel —
a nosí čtyři pláště.



OBSAH SKRYT VRSTVAMI — ČASOVÁNÍ SKRYTO ŠUMEM.

DVĚ CESTY – STÁT SE UZAVÍRÁ, SÍŤ SE OTEVÍRÁ

REPUTAČNÍ SÍŤ

STÁT

UDĚLAT NIC
ZNAMENÁ ZVOLIT
PRAVÉ DVEŘE.

brána se stále
zavírá, druhé dveře
jsou stále otevřené.

vyber si -
nebo si volba
vybere tebe.

Každý režim končí stejně. Jedinou volbou je vykročit doleva.

STÁT SE ZAVÍRÁ AUTOMATICKY. SÍŤ SE OTEVÍRÁ VOLBOU.

Jde-li o výpadek povahy dočasný, nedochází ke ztrátě dat, ani konzistence tvrzení v síti a nemělo by dojít, ani k narušení dosažených rovnováh reputací v komunitách. Na rozdíl od podobných platebních sítí se v této síti předpokládají velmi nízké četnosti procesů a údajů. V tomto se decentralizovaná reputační síť neliší od současného státu, který také nyní silně závisí na technologiích a odvykl si pracovat s papírovými kartotékami (v krizových plánech by ale neměl na vybranou).

Evoluční nástupce státu ve formě reputační sítě však může v případě trvalého výpadku (katastrofa nevídaného rozsahu) přejít zpět na primitivnější centralizovaný systém — stát.

Technologie nám umožňuje lidstvu dostat se na vyšší civilizační formy řízení a přináší nám benefity, ale i rizika.

Nevyhodím publikováním v síti peníze oknem?

Náklady na publikaci tvrzení v reputační síti nejsou z valné části utopené. Užitečnost vydavatelova sdělení do sítě — informace o skutečných křivdách, ověřené zkušenosti, relevantní varování — se v delším časovém horizontu statisticky vrací zpět ve formě poplatků za ověřování tvrzení někoho jiného z komunity. Komunita z toho má prospěch, vydavatel buduje reputaci a náklady na publikaci pravdivých informací se tak blíží vratné záloze, od které je třeba odečíst jen menší část skutečných nákladů na údržbu sítě. Naopak nepravdivé nebo triviální záznamy se nevracejí — jejich náklady jsou čistá ztráta. Poctivost je tak nejen morální volba, ale i ekonomicky racionální strategie.

Po odečtení nákladů na údržbu sítě by se tento princip dal nazvat principem ekonomické neutrality — netratím, když jsem s komunitou, trátím, když jsem proti.

Komunita má i solidární kanály, jak ocenit čestný přístup svých členů. Nedělejme si ale iluze: apel na solidaritu většinou vychází ze společenského tlaku komunity, takže nemusí jít o solidaritu v dobrovolném slova smyslu.

Co když si někdo založí víc identit?

Člověk může provozovat více DID identit paralelně. Budování reputace pro každou identitu však vyžaduje nezávislé úsilí — čas, energii, peníze.

Žádné zkratky: každá identita musí svůj track record¹ nasbírat skutečnou aktivitou. Udržovat paralelní identity je proto záměrně drahé.

Ve svobodných společnostech náklady odrazují od zneužití.

V diktaturách se však paralelní identity stávají nástrojem přežití: umožňují organizování podzemních sítí, bezpečnější navigaci černým trhem a compartmentalizovaný² odpor, kde kompromitování jedné identity neodhalí ostatní — a po svržení režimu umožňují plynule navázat na veřejný život a budovanou reputaci a klidně spojit předtím oficiální a tajnou DID tvrzením do jedné spojené množiny záznamů.

¹**Track record** (angl. *záznam výkonů*) — obecně: historie dosavadních výsledků, úspěchů i neúspěchů osoby nebo organizace. Zde: souhrn všech dosavadních interakcí dané DID identity v síti — ověřených tvrzení, přijatých i odmítnutých záznamů — z něhož se odvozuje její reputace.

²**Compartmentalizace** (z angl. *compartment* — oddíl, přihrádka) znamená oddělení informací do izolovaných celků tak, aby prozrazení jednoho celku neohrozilo ostatní. Princip známý ze zpravodajských služeb: agent zná jen svou část operace, takže i pod nátlakem nemůže prozradit celek.

STEJNÉ ÚSILÍ – PLÁNOVANÉ BÝT MARNÉ V SVOBODĚ, ZÁCHRANNÉ LANO POD TYRANÍÍ

PARALELNÍ IDENTITY STOJÍ STEJNĚ – ALE KUPUJÍ JINÉ VĚCI

V SVOBODĚ – NÁKLADNÝ PLÁN B



SEMENO → KLIČEK → SAZENEC → MLADÝ STROM → ZRÁLÝ STROM

5 až 15 let – žádné zkratky, žádný zralý strom k prodeji

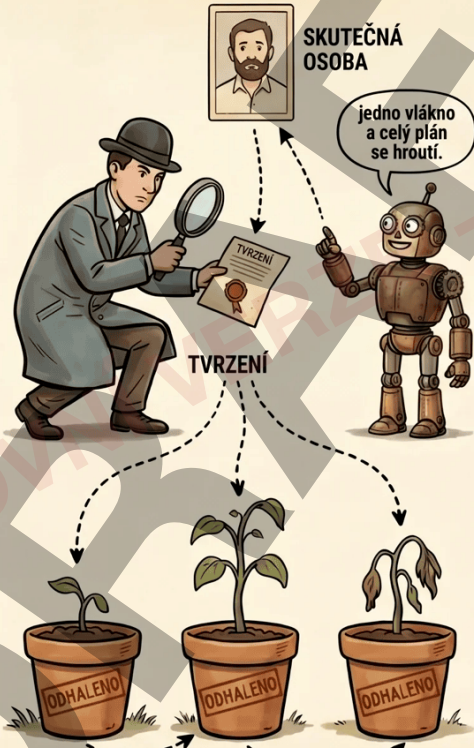


tři zahrady, trojnásobné náklady – a stále máte jen dvě ruce.

NEBO – ČISTÝ ŠTÍT PO OSOBNÍM CHYBNÉM KROKU



JEDNO TVRZENÍ A PLÁN B JE PRYČ



jediné tvrzení spojuje každý květináč se stejným zahradníkem – roky času, energie a peněz vymazány za jedno odpoledne.

POD TYRANÍÍ – JEDEN PRO STÁT, JINÉ PRO SVOBODU SDRUŽOVÁNÍ

(stát buď identity zakazuje přímo, nebo vyžaduje jejich kontrolu)



V SVOBODĚ JE ZNEUŽITÍ NÁKLADNÉ. POD TYRANÍÍ JE PŘEŽITÍ MOŽNÉ.

■ Vnímání naruby

Na rozdíl od státu princip reputační sítě postavené na decentralizované identitě obrací paradigma vnímání pořadí důležitosti:

- Důležitá je reputace, čili minulost pro hodnocení rizik interakce s protistranou a osobní údaje typu jména, adresy atp. mohou být předmětem zdvořilostní výměny dat
- Kdežto stát požaduje primárně osobní data, shromažďuje reputační data a komunitě pouští jen to, co se mu zlíbí

Nemůže si bohatý člověk prostě „koupit“ víc identit (nebo vytvářet virtuální komunity)?

Možnost vytvářet paralelní decentralizované identity na první pohled vypadá jako nefér výhoda lidí s vyššími ekonomickými možnostmi oproti těm s nižšími. Je ale potřeba zdůraznit, že na rozdíl od centralizovaného systému, kde stačí zkorumpovat pár bodů v pyramidě moci, aby se zapomnělo na nějaké nekalosti, v decentralizovaném systému by dotyčný musel zkorumpovat celou komunitu.

K tomu by mu mohly sloužit náhradní decentralizované identity, jenže jejich reputaci je nutné budovat v čase reálnou interakcí se skutečnými dalšími členy komunity — nejde si ji prostě koupit, protože v síti je ověřitelné, jak si daná identita vede.

Navíc na trhu mohou (a patrně budou) existovat služby, které formou autority nabízejí investigaci důkazů, že několik decentralizovaných identit je ve skutečnosti tatáž osoba. Jediným záznamem do reputační sítě tak lze za zlomek ceny zmařit celou investici času, energie a peněz vloženou do budování paralelních identit.

Ekonomicky se tedy vyplatí komunitu nepodvádět — případně své činy zpytovat a hledat nápravu, aby se reputace dostala zpět na přijatelnou úroveň a její nositel hněvem komunity ekonomicky či jinak netrpěl.

Ekonomicky silná identita po ztrátě reputace ve vlastní komunitě může z hněvu komunity unikat pokoutnými obchody s vytipovanými identitami — jenže ty pak také riskují ztrátu své reputace.

Zbývá ještě únik k jiné komunitě s čerstvou identitou — to ale znamená nechat za sebou veškeré výtobytky a začít někde od nuly s nulovou reputací. Někdy to může být pochopitelná cesta a jediné východisko.

POVĚŠT JE PROTIVÁHOU EKONOMICKÉ SÍLY

BOHATÝ ČLOVĚK SI KUPUJE VLIV — KOMUNITA SI TO PAMATUJE

ÚTOK — INFILTRACE A VYKOUPENÍ

ekonomická síla může vetkat nitky do jakékoli komunity — a cestou si koupit několik skutečných hlasů.

OSM NAsAZENÝCH LOUTEK + TŘI VYKOUPENÍ SOUSEDÉ



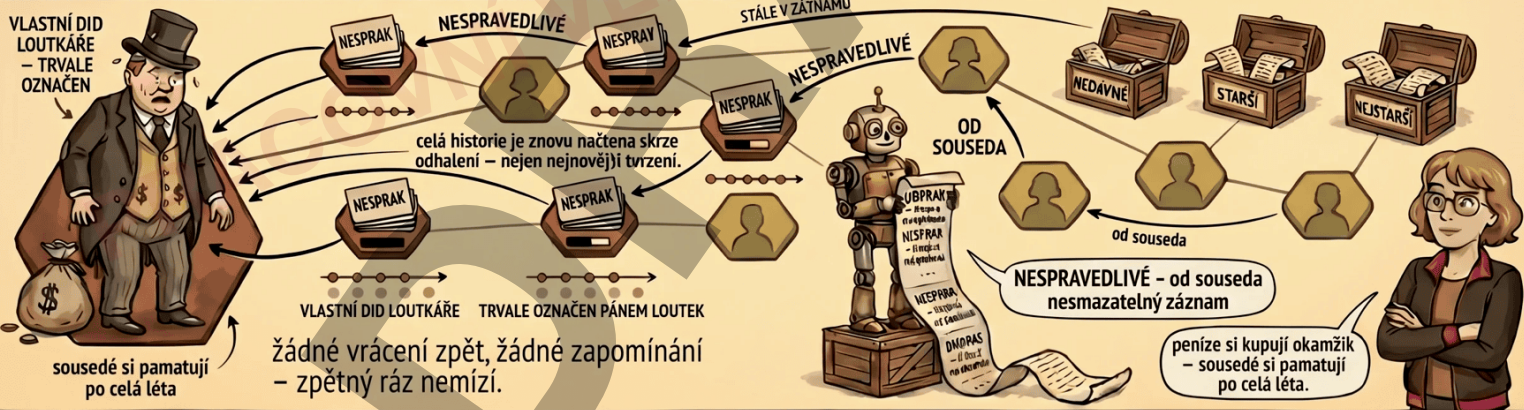
ekonomická síla může vetkat nitky do jakékoli komuni okruh přátel.

zpočátku to vypadá, že si bohatý člověk jen rozšířil okruh přátel.

POZDĚJI

OBRANA — DLOUHÁ PAMĚŤ, DISTRIBUOVANÉ ÚČETNICTVÍ

KAŽDÝ SOUSED SI UCHOVÁVÁ SVOU VLASTNÍ PAMĚŤ — ŽÁDNÁ ÚSTŘEDNÍ KNIHA, ŽÁDNÉ ZAPOMINÁNÍ



EKONOMICKÁ MOC DOSTUPUJE DOVNITŘ — ZPĚTNÝ RÁZ SE VRACÍ DOMŮ A NEJDE SMÝT.

Poznámka

Obdobně by se komunity vypořádaly s útokem, kdy někdo věnuje prostředky na vytvoření virtuální identity: pro ni je rizikové vstupovat do interakce s jinou komunitou bez ověřování — tedy nekriticky přijímat informace o identitách druhé komunity. Reputace se vždy budují v rámci komunity, ne globálně.

Co příživníci, kteří chtějí jen číst a nic komunitě nedávat?

Přístup k informacím není od prvního dne založení decentralizované identity neomezený. Noví účastníci — ti, kteří si dosud nevybudovali reputaci skutečnou aktivitou — narážejí na stupňovaná omezení: méně informací, delší čekání, vyšší náklady na dotazy. Sít' odměňuje účast, ne pasivní konzumaci a vysávání dat jen tak na potkanou.

Decentralizovaná identita riskuje svoji reputaci i tehdy, když ji za úplatu propůjčí jiné osobě (která ani v DID reputační síti být nemusí). I tady platí: takové zrazení komunity (narušování soukromí) se může odrazit na reputaci zrádce, a ten si svůj čin nemůže nechat zahladit pokoutnou dohodou, jak je zvykem v centralizovaném systému. Musí počítat s hněvem komunity včetně ztráty výdobytků — komunita je v jeho očích například garantem privilegia vlastnit movité a nemovité věci.

■ Kotva do reálného světa

Při vyhodnocování rizik je přirozeně rizikovější ten subjekt, který nepožívá privilegia vlastnictví uznávaného danou komunitou — má totiž při svých jednáních méně co ztratit (digitální vlastnictví se přesouvá snáze).

Vypadá to jako drobnost, ale má to velké důsledky. Chtít mít páku komunity na její členy implikuje vlastnictví jako privilegium — v nejsvobodnějších společnostech téměř nedotknutelné, ale stále ne právo ani základní princip, nýbrž privilegium, které v krajních případech může být odejmuto (dovedu si představit např. při odepření služby při obraně komunity v ozbrojeném konfliktu).

Podprahově to také odpovídá na to, jak se komunita zachová ke svým členům a jakou má člen motivaci za komunitu bojovat — aby si svá privilegia udržel. Člověk může ve své odpovědnosti vůči komunitě selhat, ale morálně nemůže očekávat shovívavost, pokud jde o udržení vydaných privilegií.

Finanční neutralita

Při čtení slov jako decentralizovaný, nezcenzurovatelný, nezkorumpovatelný se člověk nemůže ubránit asociacím s nejznámějšími kryptoměnami Bitcoinem, Monerem a třeba Kaspou, které lze za takové označit. Intuice však klame a poplatky za platby služeb autorit, ověřování a publikování atp. však může být realizována v jakékoliv měně nebo penězích. Důležité pro navázané účastníky sociální sítě v DID síti (tj. vaší komunity) a jejího okolí je důležité reputačně podložené potvrzení o realizaci platby. Publikace tvrzení musí být jednotlivě přiměřeně ověřitelně nákladná, aby nedocházelo situaci, kdy si může aktér

SÍŤ ODMĚŇUJE ÚČAST

REPUTACE SE BUDUJE CELÝ ŽIVOT – NELZE JI KOUPIŤ ANI PŮJČIT

ÚČASTNÍK – CELÝ ŽIVOT SKUTEČNÉ PRÁCE



tvrdší práce může zkrátit vzestup.

VĚK 20 – NOVÁČEK

reputace 5%

0 dokončených projektů



OMEZENÉ – VYSOKÉ NÁKLADY, DLOUHÉ ČEKÁNÍ

VĚK 28 – AKTIVNÍ ÚČASTNÍK

reputace 30%

dodaná smlouva
vyřešený spor
komunitní příspěvek



ZÁKLADNÍ – STANDARDNÍ NÁKLADY, BĚŽNÁ RYCHLOST

VĚK 40 – PŘÍSPĚVATEL

reputace 70%

8 dodaných projektů



PLNÝ – NÍZKÉ NÁKLADY, OKAMŽITÝ PŘÍSTUP

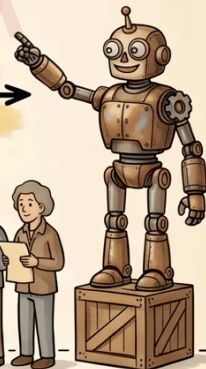
VĚK 55 – AUTORITA

reputace 95%

15+ dodaných projektů



AUTORITA – OVĚŘUJETE OSTATNÍ, SÍŤ VÁM PLATÍ

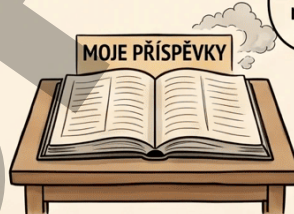


PŘÍŽIVNÍK – ČTE, NIKDY NEPUBLIKUJE



čte záznamy všech ostatních.

OMEZENÝ
PŘÍSTUP – STROP
SE NEZVEDÁ

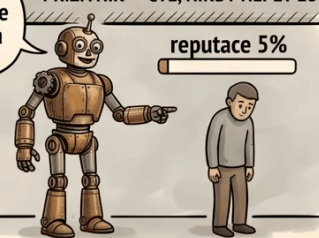


nepublikuje nic vlastního.

dveře se otevřou, až se naplní kniha tvých činů.

PŘÍŽIVNÍK – ČTE, NIKDY NEPET LUT

reputace 5%



žádné činy, žádný vzestup – rok co rok, stejná laťka.

síť vrací těm, kteří přispívají.



ČAS, ENERGIE A PENÍZE – INVESTOVANÉ DO SKUTEČNÉ PRÁCE – JSOU JEDINOU MĚNOU, KTEROU SÍŤ RESPEKTUJE.

bez vynaložené energie, peněz a času publikovat kolik a jakých tvrzení chce — to je silně nežádoucí stav, který odpovídá privilegiu elit v současném státním zřízení plném korupce.

V tomto mají zmíněné kryptoměny malou výhodu, že jejich síť plní role důvěryhodných autorit pro ověření, že k dané platbě došlo, za cenu malé ztráty soukromí a odhalení části svých adres.

Dobrovolnost, zodpovědnost a svoboda

Dobrovolnost je individuální: rozhoduji se sám. Zodpovědnost nastává, když mé rozhodnutí ovlivní ostatní — zapůsobí zpětná vazba. Svoboda není dar ani právo — je to fenomenologický³ výsledek tisíců bilaterálních interakcí mezi dobrovolností a tlakem na zodpovědnost, zprůměrovaný napříč společností. Síť tento průměr nediktuje — emerguje⁴ z cenových signálů ověřovatelů a z předem známých politik ověřování, které si nastavují členové komunity.

To, jakou preferenci svobody jednotlivec v komunitě má, se odvíjí od jeho pocitu, kolik je sám ochotný zkousnout z toho, co nakládá na bedra druhých. U věcí samozřejmých a všem prospěšných nemá morální dilema — vražda je špatná. Pak jsou případy, kdy se možnosti dostávají do pozice povolovaných privilegií: když prokážeš své schopnosti, pustíme tě do silničního provozu, aby byla menší šance, že nás

³**Fenomenologický** (z řec. *phainómenon* — to, co se jeví) — obecně: přístup zkoumající jevy tak, jak se ukazují v přímé zkušenosti, pozorováním toho, co z nich vyplývá, bez předem daných vysvětlujících teorií v mikrosvětě pod ní. Zde: svoboda není abstraktní princip definovaný shora, ale pozorovaný jev — důsledek tisíců mikrointerakcí mezi lidmi, který se vynořuje z toho, jak se k sobě reálně chováme.

⁴**Emergentní** (z lat. *emergere* — vynořit se) znamená „samovolně vznikající z interakcí jednodušších částí, aniž by to někdo navrhl nebo řídil“. Hejno ptáků létá v útvaru, přestože žádný pták nemá plán formace — útvar emerguje z jednoduchých pravidel každého jedince. Stejně tak v reputační síti nikdo nenavrhne pravidla chování celku — ta emergují z tisíců individuálních rozhodnutí.

zabiješ. A nakonec záležitosti, kdy si jednotlivec říká — to mi nestojí za to, nebudu sousedovi zakazovat pálit listí, když to sám dělám, nebo protože dělám něco jiného, co omezuje jeho komfort a mohl by to zase chtít zakázat on mně. Pokud historicky vedeme hranici svobody tam, kde začíná svoboda někoho jiného, pak reputační sociální síť postavená na decentralizované identitě to splňuje lépe než centralizovaná zastupitelská demokracie — kde se třeba vrstva privilegovaných volených zástupců snaží vyvázat ze sledování osobní komunikace, ale neváhá ho zavést svým voličům a používá k tomu různé podlé záminky a manipulace.

Přepínač svoboda–totalita (a delegování)

Jednoduchý mechanismus uvnitř DID sítě může celý systém posunout směrem k větší svobodě nebo k větší kontrole: počet záznamů, které DID smí publikovat za časové období. Když záznamy zůstávají vzácné, každý má váhu — to je svoboda. Když jsou záznamy hojné a pokrývají triviality, to je totalita. Směr volíte každým záznamem, který publikujete. Síť sama o sobě není ani svobodná, ani totalitní — je neutrální infrastrukturou. Čím se stane, určí to, jak ji lidé použijí.

Ve svém nastavení politiky pro ověřování není od věci stanovit pro obecnou DID v mé sociální síti — v komunitách — maximální počet tvrzení (obecně jakýkoli ověřitelný výrok; zde záznam publikovaný do reputační sítě), které smí vydavatel za období vypustit, abych ho bral v potaz a jeho žádosti o verifikace považoval za relevantní.

V hlavě si držím intuitivní číslo nižších jednotek ročně. Takový cenzorní přístup může působit dost izolacionisticky. Mohu ale žadatele oprávněně postavit před volbu, aby si z již vydaných záznamů vybral jeden a požádal u ověřovatele o jeho revokaci, tedy zneplatnění — což je poměrně ofenzivní požadavek v situaci, kdy se žadatel shodou okolností skutečně stal obětí vícero nezávislých křivd, a jistě bych tím přispěl k jeho pocitu odtržení od komunity.

DOBROVOLNOST → ZODPOVĚDNOST → SVOBODA

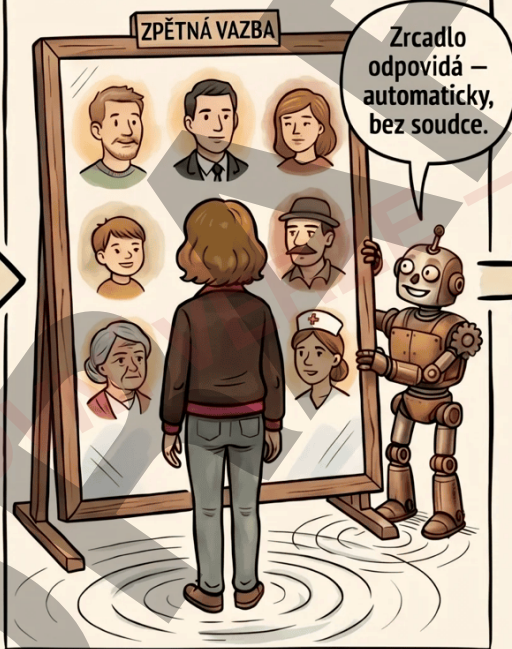
TŘI KROKY — OD ROZHODNUTÍ JEDNOHO ČLOVĚKA KE VZORCI CELÉ SPOLEČNOSTI

DOBROVOLNOST



Jedinec se rozhoduje — nikdo ho k tomu nenutí.
A nikdo mu ani není dlužen pozitivní povinnost.

ZODPOVĚDNOST



Mé volby se šíří ven — a vlnky se vrací.
Následky hovoří samy za sebe.

SVOBODA



nikdo nekreslil tuto mapu — nakreslila se sama.
svoboda je statistický tvar toho, jak se k sobě sousedé chovají.

SVOBODA NENÍ DAR SSHŮRY — JE TO VZOREC, KTERÝ TVOŘÍME SPOLEČNĚ.

PŘEPÍNAČ SVOBODA—TOTALITA

JEDEN PARAMETR — KOLIK SE ROZHODNU SLEDOVAT — NAKLÁNÍ CELOU SPOLEČNOST MEZI SVOBODU A TYRANÍ
ne mnoho knoflíků — jeden. síť sama je neutrální; má politika není.

LEVO — MÁLO, TĚŽKÉ, VÁŽNÉ



do záznamu se tesají jen vážné věci — protože tesání bolí.
ostatní zůstává soukromé: špatný den, hloupý vtíp, pozdní příchod — nic z toho není život.
lidé žijí nesledovaní, mluví svobodně a dýchají bez ohlížení.

SVOBODA JE TO, CO ODMÍTÁM POČÍTAT — TOTALITA JE TO, CO SOUHLASÍM SLEDOVAT.

VPRAVO — HODNĚ, TRIVIÁLNÍ, DUSIVÉ



každé zívnutí se stává záznamem — protože počítání je laciné.
kýchnutí, nákup, cesta domů po setmění: vše jde do záznamu, navždy.
nic není soukromé — oko nikdy nemrkne a sousedé přestanou mluvit.

Jako efektivnější se proto jeví možnost část svých práv vydat informaci do reputační sítě delegovat ve prospěch komunity nebo autority, která pak solidárně — podle svých vnitřních pravidel — rozhodne, jak je přidělit. Skupina se musí umět postarat o ty, koho považuje za znevýhodněné. Člen komunity má právo svou delegaci kdykoliv až do okamžiku použití odvolat.

■ Svoboda vs. totalitarismus

Společnost, která množství publikovaných záznamů hlídá a omezuje, bude svobodnější; společnost s nadbytkem záznamů bude tíhnout k totalitě. Lze si představit delegování práva publikovat záznamy na někoho jiného.

DELEGACE PUBLIKAČNÍCH PRÁV

PŮJČÍTE KLÍČ AUTORITĚ, KTERÁ VÁM SLOUŽÍ – A VZAPĚTÍ JEJ STÁHNETE ZPĚT

Půjčím klíč –
šňůra zůstává u mě.

Můžu půjčit více než jeden klíč
najednou – automatizace na pozadí
může vystavit nový klíč pokaždé,
když je jeden z mých vyčerpán.

delegační klíč – autorita jedná mým
jménem, v rámci pravidel, která schvaluji

AUTORITA – POSKYTOVATEL SLUŽBY

politika · standard · strana · komora



JEDEN TAH – KLÍČ SE VRACÍ DOMŮ

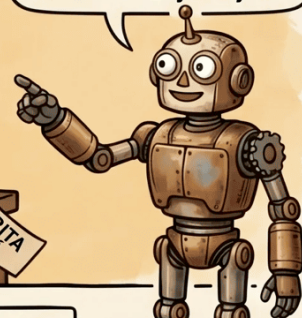
Šňůra nikdy neopustí
vaši ruku – to je celý trik.

ŠŤŮRA
ODVOLÁNÍ

MOJE PRAVO
PUBLIKOVAT

MOJE PRAVO
PUBLIKOVAT
1. ZÁZNAM

delegační klíč – autorita
jedná mým jménem,
v rámci pravidel,
která schvaluji



JEDEN KLÍČ VYTAŽEN NÁHODOU
– KLÍČ JE VYČERPÁN

DRUHY AUTORIT,
KTERÉ MOHOU
DRŽET KLÍČ



POLITICKÁ
STRANA



STANOVOVACÍ
ORGÁN



PROFESIONÁLNÍ
KOMORA



DRUŽSTVO

Odvolatelný pouze do vytažení klíče.

Po tomto okamžiku musí občan vystavit nový klíč, aby si udržel
postavení u autority – automatizace to může udělat na pozadí.

autorita slouží svým členům – ne naopak.
jeden tah za šňůru ukončí ujednání.

PŮJČTE KLÍČ – NECHTE SI ŠŤŮRU. DELEGACE NIKDY NEZNAMENÁ KAPITULACI.

Kulturní přizpůsobení

Lidé obecně rádi vidí druhým do talíře. Napříč civilizacemi se lišíme historickou zkušeností, mírou zalidnění — a tím i mírou toho, jak moc si do talíře v rámci civilizací a komunit chceme vidět. Asijské státy tíhnou ke striktnějšímu pohledu na svobodu ve společnosti, evropské a americké v jistých aspektech ke svobodnějšímu. Jakkoli je tahle paralela nepřesná, v kontextu decentralizované reputační sociální sítě lze říct, že nastavení jednotlivých komunit nediskriminuje a komunikaci v rámci své komunity si každá komunita může nastavit po svém.

I přes rozdíly budou existovat standardy uznávané napříč planetou (vražedění na setkání není dobré pro nikoho). Jiná nastavení budou komunitně specifická, jiná dokonce osobně specifická. Výhoda je, že vzájemnou komunikací a sledováním nastavení svého okolí lze hledat konsenzus — od bilaterálních dohod přes komunitní a postupem času, díky ekonomické převaze nejlépe nastavených komunit, i na globální úrovni.

O konsenzu ale raději více v příští kapitole.

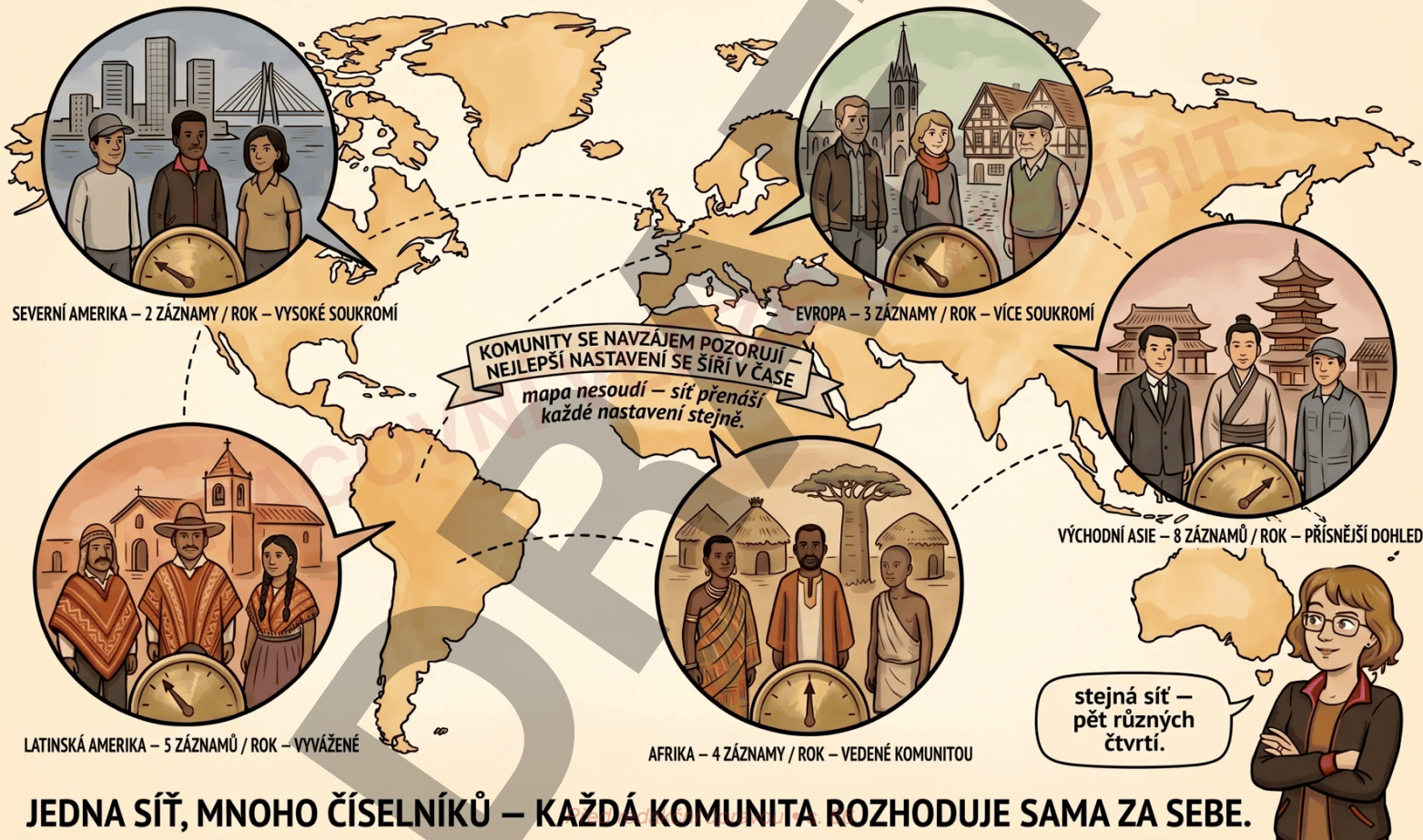
Oracle problém — propojení digitálního a fyzického světa

Pojem „oracle problém“ je nejvíce v poslední době spojován se světem kryptoměn, blockchainů a decentralizovaných systémů. Obecně: jak zajistit, aby data vstupující do digitálního systému věrně odpovídala tomu, co se skutečně stalo ve fyzickém světě? Systém sám nedokáže ověřit, jestli někdo opravdu někomu ublížil nebo jestli byla smlouva skutečně porušena — vidí jen digitální záznamy.

Tady to řešíme přes autority — subjekty, které vsadí svou reputaci na to, že digitální záznam odpovídá fyzické skutečnosti. Čím vyšší reputace autority, tím věrohodnější záznam.

KAŽDÁ KOMUNITA SE KONFIGURUJE SAMA

SÍŤ NEDISKRIMINUJE – KAŽDÝ REGION NASTAVUJE SVŮJ VLASTNÍ ČÍSELNÍK



PŘEMOSTĚNÍ DIGITÁLNÍHO A FYZICKÉHO SVĚTA

AUTORITA PŘENÁŠÍ REALITU PŘES MOST



Reputace autority činí digitální záznam důvěryhodným.

- * Systém se nesnaží vyřešit problém věštiny – přijímá, že autority jsou mostem, a sladí se s tím, jak důvěra funguje v reálném světě.
- * Pokud se most mylí ohledně reality, autorita zaplatí – svou reputací.

4. Jak ověřování funguje

Konsenzus a proces ověřování

Konsenzu o tom, která pravidla by se měla ve společnosti v průměru dodržovat a vynucovat, může pomoci následující mechanismus. Jako účastník DID deklaruji pravidla, ke kterým se hlásím a budu se jimi řídit, a zveřejním je. (Obdoba vyhlášek a zákonů, které podle mě tvoří můj vysněný svět — svět, ve kterém se neomezují, ale cítím bezpečně.)

Můžu si u svých DID kontaktů dopředu odhadnout, jak by reagovali — a posoudit, jak silně a od koho by mě v běžných sociálních či obchodních interakcích sankce zasáhly, kdyby k nim hypoteticky došlo.

K definitivnímu vyhodnocení dojde, když od jiného DID požadujete informace nebo ho žádáte o ověření tvrzení (nebo žádáte službu od autority atp.), které chcete publikovat do reputační sítě. Mělo by to dopadnout stejně, jako když to vyhodnocujete u sebe nanečisto vůči deklarované politice (policy) protistrany — a když ne, něco není v pořádku u protistrany: snaží se hrát nečistou hru.

Výsledkem je buď přijetí s nabídnutou cenou za ověření (u služeb ověřovatele, autority), nebo odmítnutí. Sankce i bonusy za odchýlení se od politiky hodnotitele se promítají do nabídnuté ceny. Žadatel se rozhodne, zda podmínky přijme, nebo přejde do dalšího kola ověřování v alokačním algoritmu — a proces opakuje, dokud není spokojený, nebo to ekonomicky nevzdá.

■ Sociální graf (The Social Graph)

Reputační síť je především sociální sítí. Přidáváte kontakty — lidi, kteří spojení povolí. Ti mají kontakty a ty mají další kontakty. Algoritmus hledá ověřovatele v konfigurovatelné hloubce (např. tři úrovně: vaše přímé kontakty, jejich kontakty a jedna úroveň dál). Žádný globální blockchain není potřeba — síť přirozeně vytváří komunity s přesahy do dalších komunit.

Algoritmus je nedeterministický: zahashuje váš dokument s tvrzením, namapuje hash na pozici na kruhu známých identit v tomto okruhu a jako kandidáta na ověřovatele vybere nejbližšího. Nemůžete předpovědět ani ovlivnit, kdo vaše tvrzení ověří.

Každé odmítnutí ověřovatele váš dokument zvětší a zdrazí jeho zpracování — to je první nákladový kanál (narůstání dokumentu). Každý další ověřovatel účtuje poplatek podle objemu dat, vaší reputace a podle toho, jak daleko se obsah vašeho tvrzení odchyluje od jeho deklarované politiky ověřování — druhý nákladový kanál (riziková přírážka). A každá iterace stojí čas a energii — třetí nákladový kanál.

■ Co ověřovatel kontroluje a v jakém pořadí

Jakmile algoritmus vybere ověřovatele, prochází tvrzení zhruba čtyřmi kroky — od nejlevnějšího filtru po nejdražší obsahovou kontrolu:

1. **Policy gating.** Spadá tenhle typ tvrzení vůbec do toho, co ověřovatel veřejně dělá? Když ne, požadavek rovnou odmítne.
2. **Důvěra v autoritu.** Je autorita, která tvrzení podepsala, podle ověřovatelovy deklarované politiky dost důvěryhodná? Autorita pod jeho prahem důvěry je důvod k odmítnutí bez ohledu na obsah.
3. **Reputace vydavatele.** Splňuje vydavatel reputační prahy, které si ověřovatel pro tento typ tvrzení deklaroval? Nízká reputace může buď zvednout poplatek, nebo vést k odmítnutí.
4. **Obsahová kontrola.** Teprve když projdou první tři kroky, ověřovatel posuzuje samotné tvrzení — podpisy, vnitřní konzistenci, formální správnost a to, jak se odchyluje od jeho politiky. Poplatek za tento poslední krok odráží skutečně podstoupené riziko.

Politiku, která řídí každou z těchto bran, ověřovatel veřejně publikuje — kroky tedy nejsou na jeho libovůli, je vázán tím, co sám deklaroval. Odchyłka od publikované politiky je sama o sobě publikovatelným tvrzením proti němu a platí za ni svou reputací.

Výsledkem je, že zveřejnění věrohodného a užitečného tvrzení stojí skoro nic. Zveřejnit radikální tvrzení stojí víc. Zveřejnit lež se stane neúnosně drahým — musíte iterovat ověřovatele za ověřovatelem

a každý, kdo vás odmítne, přidá náklady. Trh nacení vaše tvrzení a cena vám řekne, kde stojíte vůči komunitám, ve kterých se pohybujete.

Nestačí deklarovat, že pravidlo dodržuji, když ho v realitě nedodržuji. V takovém případě hrozí mému DID zveřejnění negativního záznamu, který odhalí pokrytectví — a ze mě udělá riziko pro ostatní. Výsledkem by mělo být méně pravidel, ale dodržovaných důsledněji, a pročištění té džungle zákonů a předpisů, ve které se sotva vyznají i právníci.

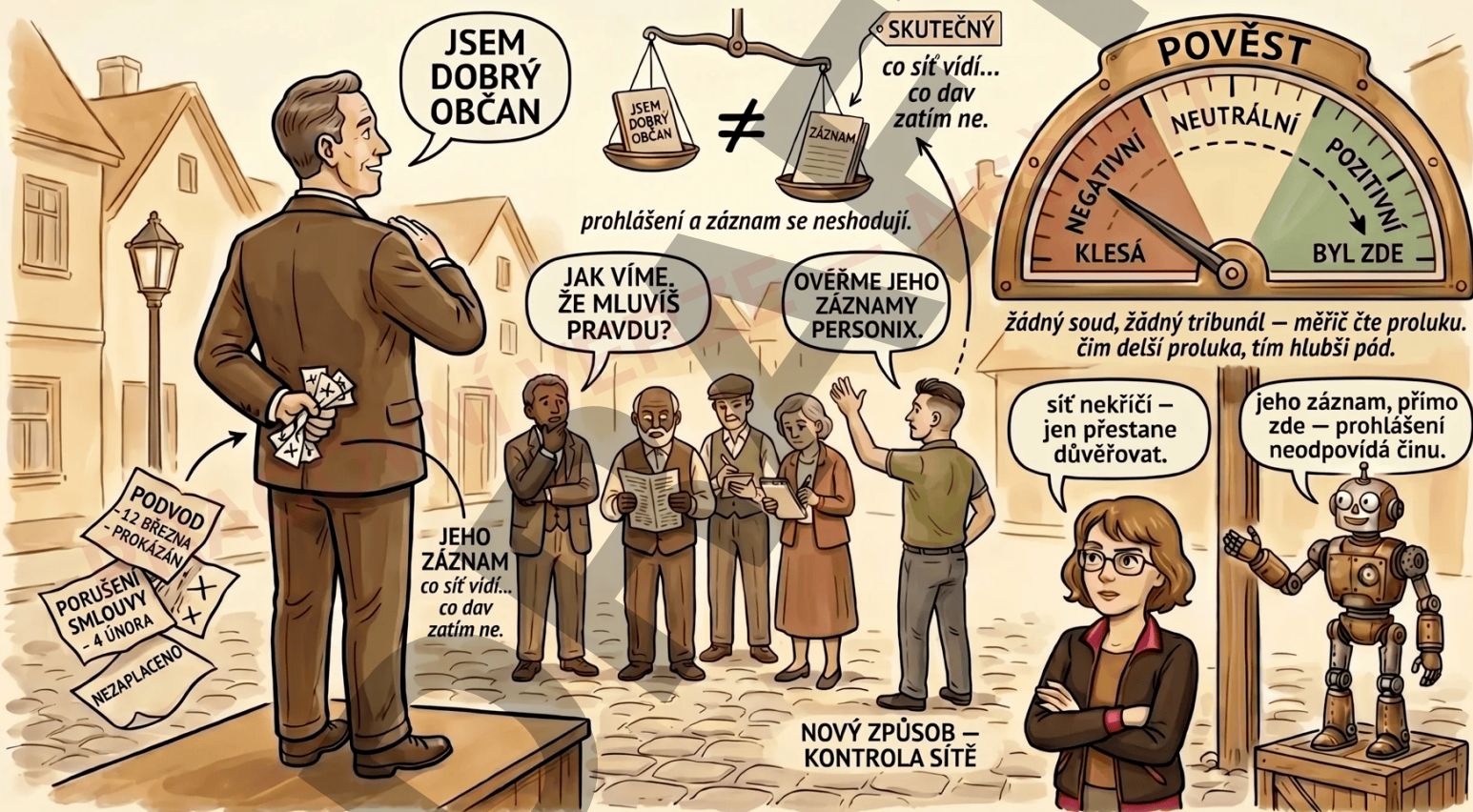
Konsenzus vs odpovědnost

Aby síť sloužila jako hodnotný zdroj informací, DID by neměl být příliš radikální — jinak ho ostatní odmítnou. Sociální tlak bude hledat rovnováhu a pokusy o narušení stability si pravděpodobně vyberou svou daň.

POKRYTECTVÍ JE NEJDRAŽŠÍ CHOVÁNÍ

Před redakční úpravou

SÍT TIŠE SROVNÁVÁ VAŠE SLOVA S VAŠÍM ZÁZNAMEM – PROLUKA JE VIDITELNÁ PRO VŠECHNY



Před redakční úpravou

VYHLÁSIT A PORUŠIT TO? PROLUKA JE NEJDRAŽŠÍ CHOVÁNÍ.

LÉK NA POKRYTECTVÍ

DEKLARUJTE SVÁ PRAVIDLA – ŽIJTE PODLE NICH, NEBO VÁS TRH VYŘADÍ

DEKLARUJI SVOU POLITIKU



každý si může přečíst mé standardy.
žádní strážci, žádná tajemství.

SVĚT PŘIHLÍŽÍ



svět si zapisuje, co skutečně dělá. každý den
přibývá v jeho knize evidence trochu více důkazů.

V OBCHODĚ – PLATÍTE ZA SVŮJ VLASTNÍ ZÁZNAM



pokrytectví netrestá autorita – je oceňováno trhem.
každá běžná služba, kterou si koupíte, nese příplatek formovaný vašim vlastním záznamem.

MOHLI BYCHOM TOMU ŘÍKAT SPOLEČENSKÁ SMLOUVA – PŘEKRESLENÁ?

žádná autorita nevynucuje etiku – dělá to cena.
mírný tlak, každý den, směřující k průměru, se kterým můžeme všichni žít.

ŽIJTE, JAK MLUVÍTE – NEBO ZA TO ZAPLAŤTE. POKRYTECTVÍ JE NEJDRAŽŠÍ REPUTACÍ.

■ Počet hlasů není to samé jako síla hlasu

Juraj Karpíš říká, že „peníze jsou pamětí dobrých skutků“. Dodávám, že reputace je pamětí těch špatných.

Z toho plyne, že meritokraticky by si větší váhu hlasu v komunitě zasloužil ten, kdo přispívá víc a nemá špatnou reputaci. Pokud se na to podíváme z pozice bilaterálních vztahů: když zvažuji, kterým tlakům na konsenzus víc vyjdu vstříc, zahrnu s největší vahou ty vztahy, ze kterých mám největší ekonomickou výhodu. Deset lidí, se kterými nemám čilý obchod, na mě zapůsobí mnohem méně než jeden trvalý obchodní partner. Toto paradigma se neomezuje jen na obchod — dá se rozšířit na sociální, politické a další vztahy.

Role v ověřovací transakci a autority

Přehled rolí

Některé role jsme krátce naťukli už v kapitole o síti a jejích základních vlastnostech. Nyní nastal čas podívat se podrobněji znova na tyto role a přidat další nezbytné, abychom zajistili větší robustnost sítě. V každé ověřovací transakci vystupuje několik rolí, pojďme se podívat, jak se chovají.

■ Role v ověřovací transakci

Každá ověřovací transakce má až šest různých rolí, shrnutých v tabulce níže. Všechny mohou mít v decentralizované reputační síti svůj DID.

Role	Popis
Vydavatel (Issuer)	Osoba, která zveřejňuje informaci do sítě — tvrdí, že se něco stalo (DID vznikla, byla editována nebo zanikla, publikované tvrzení, policy dané DID atd.)
Subjekt/Nositel (Subject)	Osoba, o které informace hovoří — adresát tvrzení
Autorita (Authority)	Důvěryhodný subjekt, který svým jménem ručí za kvalitu tvrzení jeho prošetřením a necháním si předložení důkazů nebo jejich aktivním dohledáním
Pozorovatel (Observer)	Nezávislá třetí strana, která vede záznam o tom, jak ověřovatel zpracovává tvrzení — dohlíží, aby ověřovatel výsledek nevymlčel ani se neodchýlil od deklarované politiky
Ověřovatel (Verifier)	Algoritmicky vybraný účastník, který transakci zpracuje
Delegát (Delegate)	Osoba jednající jménem jiného účastníka

Vydavatel

S vydavatelem jsme se již setkali. V případě, kdy se někomu stane nějaká křivda, nebo se chce pochlubit nějakým vlastním úspěchem, tak je to ta osoba reprezentovaná pomocí DID, která vyvolává proces vložení informace do sítě, neboť ona na tom má primární zájem (motivací je jí touha po satisfakci, nebo zlepšit svůj obraz).

PREDAVATEL – KDO PÍŠE TVRZENÍ

AUTOR • SIGNATÁŘ • SÁZÍ SVOU VLASTNÍ POVĚŠT

CO VYDAVATEL DĚLÁ

1. Píše tvrzení vlastními slovy.
2. Shromažďuje důkazy ze skutečného světa, aby je podpořil.
3. Podepisuje se svým vlastním DID a odesílá autoritě dle své volby.
4. Platí náklady na zveřejnění.
5. Nese následky, pokud lže.

MOJE POVĚŠT



Moje jméno na tom bude.
Musím si být jistý –
a přinést důkazy.

Pokud je to lež,
moje ručička klesne.

Mluvit může kdokoli.
Lži stojí řečníka.



Vydavatel je autor. Jeho jméno je na tom.

* Kdokoli s DID se může stát vydavatelem. Látkou je odvaha a odpovědnost, nikoli licence.

■ Pozitivní tvrzení

Pozitivní tvrzení o sobě si mohu jako jejich nositel a vydavatel v jednom ponechat pro situace, v nichž je chci použít (osvědčení o vzdělání, o vykonané službě atp.). V tomto se pozitivní liší od negativního, kdy sdílení negativní ověřené informace je v zájmu celé komunity, kdežto pozitivní v zájmu jejího nositele

Autorita

Autorita hraje dvojí roli: může být **auditor** (ověří kvalitu důkazů, než se tvrzení publikuje) nebo **garant** (vsadí svou reputaci na pravdivost tvrzení). V obou případech posiluje tvrzení vydavatele. Tyto dvě služby se dají oddělit — autorita může nabízet jednu, druhou, nebo obě současně. Rozhodně se předpokládá, že většinu služeb poskytovaných autoritami lze poskytovat volnotržně. Tato podmínka platí i v těžko představitelných odvětvích typu spravedlnosti, kde lze efektivně poskytovat specializované služby vyšetřování, hodnocení důkazů až po služby dnes poskytované centralizovanými armádami (strategické plánování, zajištění standardizovaného výcviku, nákupu a zajištění skladových prostředků, atd). Jen máloco si lze těžko představit, že by nešlo po restrukturalizaci zefektivnit volnotržními motivacemi.

■ Autorita, vydavatel ani pozorovatel nesmí být ověřovatelem sami sobě.

Algoritmický výběr ověřovatele zajišťuje nezávislost. Nikdo nemůže ověřit vlastní tvrzení ani tvrzení, na kterém má přímý zájem. Toto je jedno ze základních pravidel v zájmu DID z celé komunity k dodržování.

Následující grafiky zobrazují doplňující se pohled na šíři pokrývané problematiky autoritami (autoritu je možné zaměnit za termín poskytovatele).

■ Autorita i jako inkognito pozorovatel

Renomovaná autorita — třeba notář, jehož podnikání závisí výhradně na jeho track recordu — může vedle hlavních funkcí (auditor / garant) nabídnout třetí: roli inkognito pozorovatele během ověřování. Vede časově razítkovaný záznam o odeslaném tvrzení, takže ho ověřovatel nemůže potichu zahodit. Mechanismus pozorovatelské role je popsán dále v sekci o roli Pozorovatel.

Ověřovatel

Každá DID může být ověřovatelem, a to napřímo nebo skrze delegovaná práva na třetí DID. Na to abych já nebo můj zástupce mohl být ověřovatelem, měl bych být v síti dostupný (online). Ne každému se bude

AUTORITA – RUČÍ SVÝM JMÉNEM ZA KVALITU TVRZENÍ

HLUBOKÁ ANALÝZA VZADU • JEDNODUCHÉ VEDENÍ VPŘEDU



POSKYTOVATEL — PROVOZUJE SLUŽBU PODEPSÁNÍ TVRZENÍ

Před redakční úpravou

ZVEŘEJNĚNÉ STANDARDY • ZVEŘEJNĚNÉ CENY



Vázán tím, co veřejně prohlašuje. Reputace udělá zbytek.

* Poskytovatel má také svou vlastní politiku — kdy přijímá, kdy odmítá, jak vrací peníze. Je zveřejněna, ale toto není hlavní příběh.

chtít tuto podmínku splnit, proto je v definici jeho záznamu definována prioritní řada jeho zástupců, kteří danou funkci vykonávají za něj v době, kdy je offline.

Každá DID vystupující v síti má veřejně deklarovanou svoji politiku, skrze jejíž definovaná pravidla bude v ověřovacím procesu nahlížet na reputaci protistrany a obsah a formu tvrzení označeného vydavatelem za určený k publikování do reputační sítě. Součástí politik jsou i kalkulační formule na výpočet poplatků za služby ověřování. Když mám toto zajištěno, pak v rámci statisticky velkého počtu tvrzení směřujících do sítě čekám, až mě algoritmus sítě vylosuje na straně vydavatele a určí k tomu, aby v jednotlivé iteraci provedl ověření jím vydávané informace. Vydavatel si může dopředu u sebe spočítat, jak se ověřovatel korektně zachová, avšak nemůže se vyhnout jeho kontaktování (nebo jeho zástupců) a danou iteraci musí vydavatel s vybraným ověřovatelem absolvovat, i když dopředu ví, že to nedopadne.

Jak víme, že vydavatel pouští algoritmus výběru ověřovatele nad správnou množinou DID potenciálních ověřovatelů? Každá DID spolu s deklarovanou veřejnou politikou publikuje i aktuální seznam identifikátorů své sociální sítě v rámci reputační sítě. Bude-li si sociální síť vydavatele pro sebe definovat jako sociální bublinu, která konvenuje a posiluje jen jeho názory, těžko publikované informace skrze ni budou šířeni přijímány mimo ni jinými komunitami. To že se mi podaří za draho radikální informaci v síti publikovat, neimplikuje, že při vyhodnocování reputace protistrany k ní budu přihlížet. K některým jsem tlačen komunitou, abych k nim přihlížel (vynesené tresty a omezení nad provinilci) a jiné jsou čistě na mě — ekonomický přínos zahrnutí/nezahrnutí dané informace si stanovuji sám.

Subjekt

Ten, koho se publikované informace v reputační síti týkají, jsou jejich nositelé, nebo chcete-li subjekty. Incentivy v reputační síti jsou nastaveny tak, že subjekt má veškeré motivace chovat se korektně a férově dle svých pravidel a je tlačen komunitou k nějakému zlatému pravidlovému středu. Dokonce má motivace

OVĚŘOVATEL — POSUZUJE ZÁZNAM PROTI ZVEŘEJNĚNÉ POLITICE

ČTYŘI BRÁNY, V POŘADÍ. NEJDŘÍV LEVNÉ FILTRY.

BRÁNY OVĚŘENÍ – V POŘADÍ

1. FILTRACE PODLE POLITIKY

Ověřuji vůbec
tento typ záznamu?

2. DŮVĚRA V AUTORITU

Je autorita nad
mým prahem?

3. REPUTACE VYDAVATELE

Splňuje vydavatel
mou laťku reputace?

4. KONTROLA OBSAHU

Podpisy,
konzistence,
odchylka od politiky

NESMÍ BÝT:

vydavatel, autorita,
pozorovatel ani subjekt.

REPUTACE OVĚŘOVATELE

ODCHYLKA OD POLITIKY
→ REPUTACE KLESNE
→ ŽÁDNÉ DALŠÍ VÝBĚRY

CO DĚLÁ OVĚŘOVATEL

1. Filtruje podle svých zveřejněných bran politiky (v pořadí)
2. Kontroluje důvěru v autoritu, pak reputaci vydavatele
3. Vyhodnocuje obsah záznamu jen pokud brány projdou
4. Účtuje poplatek úměrný riziku
5. Sází vlastní reputaci na každém rozhodnutí

POPLATEK ∝ RIZIKO

větší riziko = větší poplatek

Nejdřív levné filtry.
Drahá kontrola obsahu nakonec.

Nesmí být
kreativní. Musí
dělat co říká
jeho politika.

Jeho vlastní
pravidla. Veřejná.
Nemůže je tiše
měnit.

POLITIKA:

BRÁNA 1: OVĚŘUJI TYP X
BRÁNA 2: AUTORITA $\geq T_1$
BRÁNA 3: REPUTACE VYD. $\geq T_2$
BRÁNA 4: OBSAH ODPOVÍDÁ Y

VYBRÁN
HASHEM

PŘIJATO

ODMÍTNUTO

Ověřovatel je vázán pravidly, která sám zveřejnil — a reputací, kterou může ztratit.

chovat se více morálně nad rámec deklarovaných pravidel — předem deklarované politiky nevylučují v komunitě, že se najde napříč komunitou shoda k retroaktivitě nějakého hodnocení nebo opatření. Z tohoto pohledu je alternativa právního uspořádání v reputační síti očekávaně motivovaná spíše duchem než doslovností.

Pozorovatel

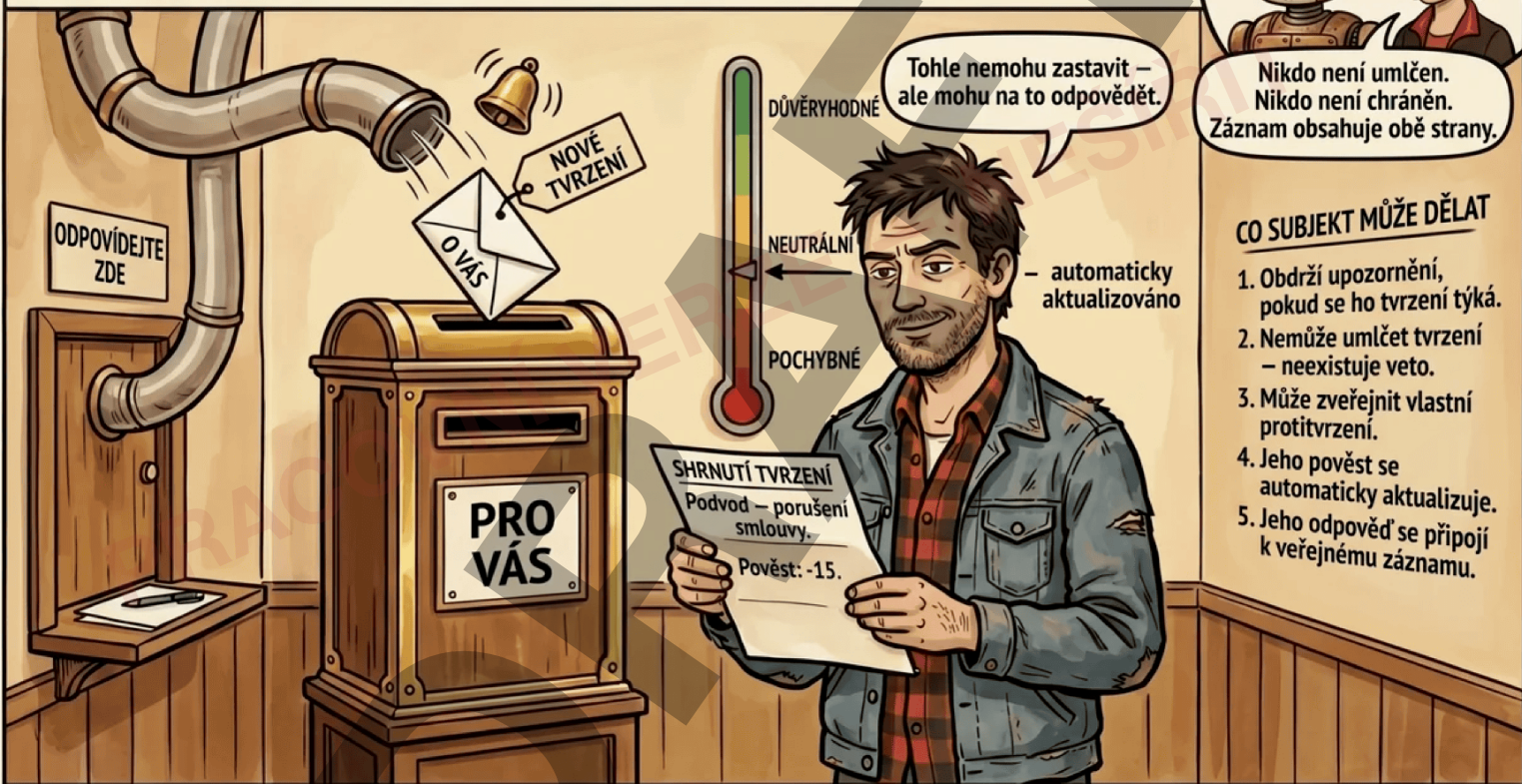
Role pozorovatele eliminuje u ověřovatele motivaci ohýbat pravidla. Ověřovatel by mohl v situacích, kdy mu žádost vydavatele nebo autority nesedí, prostě mlčet — neodpovědět, zablokovat algoritmickou posloupnost. Pozorovatel — nebo množina pozorovatelů — svou reputací ručí za to, že dokladuje průběh dotazování ověřovatele. Pokud ověřovatel mlčí navzdory deklarované politice, lze ho z porušení protokolu usvědčit.

Mechanismus: časové razítko a kód výzvy

Než pošlete tvrzení ověřovateli, projdete s ním přes pozorovatele — lidi, kterým důvěřujete, nebo specializované poskytovatele pozorovatelských služeb za drobný poplatek. Každý pozorovatel vaše podání přijme, časově razítkuje, podepíše, že ho viděl odcházet, a vytvoří kód výzvy (challenge code) — kryptografický hash svého podpisu. Kódy se připojí k vašemu požadavku. Ověřovatel je vidí, ale netuší, kdo pozorovatelé jsou ani zda jsou kódy vůbec skutečné. Pozorovatelé tak fungují jako proxy mezi vydavatelem a ověřovatelem a drží nezávislý záznam, že tvrzení bylo odesláno a co obsahovalo. Může jich být nula až N.

Když se ověřovatel chová poctivě — přijme nebo odmítne v souladu se svou deklarovanou politikou — kódy zůstanou neprůhledné. Nikdo není odhalen.

SUBJEKT — TEN, KOHO SE TVRZENÍ TÝKÁ OBDRŽÍ JE • NEMŮŽE JEJ UMLČET • MŮŽE ODPOVĚDĚT

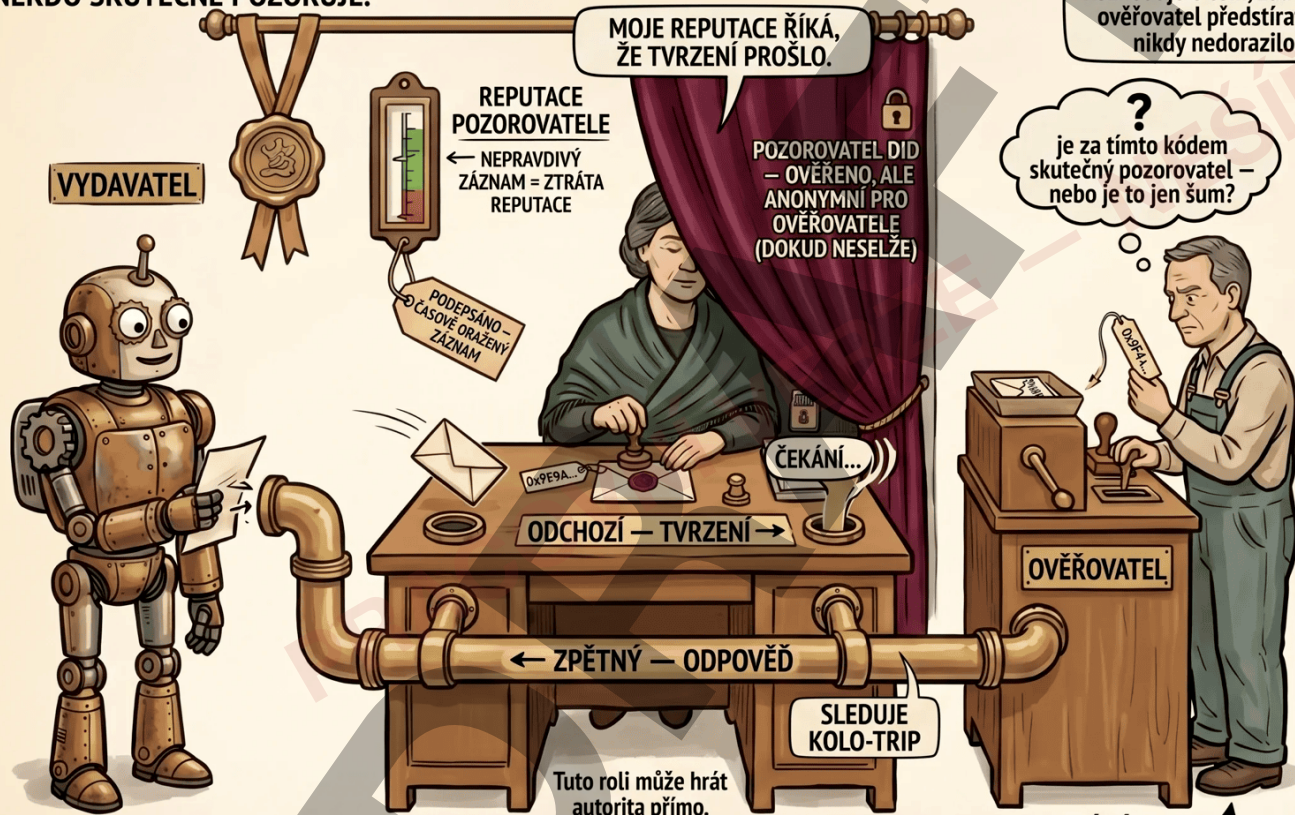


Subjekt nemá veto – pouze právo odpovědět.

*** Protitvrzení je samo o sobě tvrzením – v sázce je pověst subjektu za to, co v odpovědi uvede.**

POZOROVATEL — PROSTŘEDNÍK, KTERÝ PŘEDÁVÁ TVRZENÍ A SLEDUJE ZPĚTNOU VAZBU.

OVĚŘOVATEL S NÍ MLUVÍ. OVĚŘOVATEL SE NIKDY NEDOZVÍ JEJÍ IDENTITU, ANI ZDA NĚKDO SKUTEČNĚ POZORUJE.



CO POZOROVATEL DĚLÁ

1. Přijímá tvrzení od vydavatele
2. Orazí jej vlastním pečetěním; razítko je časově orazítkovaný záznam
3. Předává jej ověřovateli jménem vydavatele
4. Sleduje, zda se vrátí odpověď a co říká
5. Publikuje svůj podpis pouze pokud se ověřovatel chová špatně — její reputace je zárukou

SMALL FOOTNOTES

* Za jakýmkoliv požadavkem může být nula až N pozorovatelů. Ověřovatel vidí pouze neprůhledné kódy a nikdy neví, zda skutečný pozorovatel sleduje, nebo zda je to jen šum. Tato nejistota je motivací k řádnému chování.

* Symetricky, ověřovatel může směřovat odpověď prostřednictvím vlastního pozorovatele — stejný trik, opačný směr.

Anonymní pro veřejnost, odpovědný síti. Ověřovatel vidí kód, nikdy pozorovatele.

Když ale ověřovatel mlčí navzdory vstřícné politice, nebo odpoví v rozporu s tím, co publikoval, máte v ruce originální podpisy pozorovatelů. Můžete je zveřejnit jako proxy svědectví, že tvrzení bylo odesláno a že se ověřovatel nezachoval podle protokolu. Kdokoli může ověřit, že podpisy odpovídají kódům výzvy.

Pointa: skutečné pozorovatele nepotřebujete

A tady přichází ta nejelegantnější část: **reálné pozorovatele vůbec nepotřebujete**. Můžete vygenerovat náhodná čísla, která vypadají přesně jako kódy výzvy. Ověřovatel nepozná rozdíl — musí si hodit kostkou, jestli riskne svou reputaci. Za každým požadavkem, který dostane, může stát respektovaný pozorovatel sledující inkognito — nebo to může být jen šum. Ověřovatel to neví. A ta nejistota je ten mechanismus.

Náklady na udržení poctivého tlaku: skoro nulové (náhodná čísla jsou zadarmo). Potenciální náklady nepoctivosti pro ověřovatele: katastrofální. Poctivé chování je motivováno, i když ve skutečnosti nikdo nesleduje.

System funguje, protože jsou všichni trochu paranoidní. Nejistota vyjde levněji než dohled.

BLAF, KTERÝ DRŽÍ OVĚŘOVATELE POCTIVÝMI

SKUTEČNÝ POZOROVATEL A NÁHODNÝ BLAF VYPADAJÍ Z POHLEDU OVĚŘOVATELE STEJNĚ

YDAVATELKA – KAMILA



SKUTEČNÝ POZOROVATEL



OVĚŘOVATEL



OVĚŘOVATEL NEMŮŽE ROZEZNAT SKUTEČNÝ ZÁZNAM OD BLAFU. POCTIVÉ CHOVÁNÍ JE JEDINOU BEZPEČNOU SÁZKOU.

YDAVATELKA – BLAFOVÁNÍ



BEZ POZOROVATELE

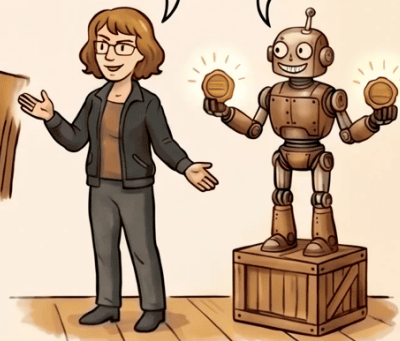


OVĚŘOVATEL



Ověřovatel je nedokáže rozeznat.

Kdo pozná rozdíl?



Náklady na tlak na poctivost: téměř nula – náhodná čísla jsou zdarma.
Náklady na dopadení při umlčování tvrzení: katastrofální – zničení reputace.

NEJISTOTA JE LEVNĚJŠÍ NEŽ DOHLED.

■ Násobnost ověřovatelů v jedné iteraci

Posilujícím doprovodným pravidlem dostupnosti ověřovatelů, může být algoritmické rozšíření, aby v jedné iteraci vrátil množinu potenciálních ověřovatelů a nikoliv jen jednoho.

Delegování

Civilizace postavila svůj ekonomický růst na schopnosti dělby práce a specializace. Svět je ve své celé kráse složitý a naše šance ho zvládnout pochopit ve své komplexitě téměř nemožná. Jak přirozené východisko se nám nabízí řada aspektů činností podporující pohodlný život delegovat na specializované dodavatele, kteří nám ušetří čas, ve výsledku energii a peníze a dovolí nám se specializovat a poskytovat služby, ve kterých my jsme nejlepší, nebo si jich trh u nás nejvíce cení.

Delegování pak můžeme vztáhnout i do reputační sítě. V kapitole Přepínač svoboda-totalita (a delegování) byly řečeny principy zajištění svobodné společnosti skrze omezení počtu publikovatelných tvrzení do sítě, za nějaký časový úsek (představujte si zjednodušeně nižší jednotky ročně práva na publikování, aby byla společnost maximálně svobodná). Tento princip lze převést do více dimenzí. Nemusíme mít jen jedno číslo, ale můžeme mít více čísel — limitů, týkajících se různých druhů tvrzení. Pro označování pokrytectví ostatních můžeme mít jiné číslo, než pro prohřešky v obchodním styku, a třeba změna DID dokumentu např. obměnou hesla asi komunita nebude skoro vůbec řešit, atp. Celé to záleží na tom, jak si komunita definuje evolučně, že je to pro ni výhodné, aby našla svoji rovnováhu mezi cílenou úrovní svobod a zodpovědností.

Proč by mělo stačit mít počet práv publikování do sítě od komunity malý? Označení DID (subjekt/nositel) negativním tvrzením ji ničí dlouho budovanou reputaci na dlouhou dobu. Zničená reputace bude čelit škále stupňujících sankcí od komunity za každý další nebo opakovaný prohřešek až do úplné eliminace narušující entity (extrém). Exponenciálně narůstající škála trestání nepotřebuje velké množství tvrzení podepřených ověřitelnými důkazy. To platí pro mírový ustálený stav v době, kdy společností necloumá katastrofa (externí nebo interní).

Statisticky pro jevy s velice řídkou pravděpodobností je četnost jejich výskytu volatilní, když je aplikovaná na jednotlivce. Skrze populaci komunity však již nikoliv. S výhodou je dobré delegovat svá práva na publikování na specializované agregační autority, které podobně jako funguje vzájemné pojištění v případech události využijí vaše právo a aplikují ho jejich jménem. Mluvme méně abstraktně a řekněme si pár příkladů: - vyhledávání a potírání organizovaného zločinu - zajištění dodržování obchodních dohod - správa privilegií (osvědčení o vzdělání, nabytí/pozbytí majetku, atp.) - atd.

DELEGOVAT – SLUŽBA TVRZENÍ, KTEROU SI PŘEDPLÁCÍTE

DELEGOVAT TO, CO SAMI NEZVLÁDNETE • PONECHAT SI TO, NA ČEM VÁM ZÁLEŽÍ



Svěřte někomu to, co sami nezvládnete. Zůstaňte v obraze. Práva stáhněte kdykoli zpět.

* Pokud ten, komu delegujete, jedná mimo dohodnutý rozsah, veřejně to ovlivní pověst obou, její i vaší.

■ Jak ve skutečnosti fungují „publikační práva“

Grafika delegáta zobrazuje publikační práva jako fyzické tokeny pro názornost, ale v systému žádný takový objekt neexistuje. Reálně to funguje takto: politiky lidí, s nimiž chcete být zadobře — vaše komunita — se agregují do emergentního pravidla o tom, kolik tvrzení od vás ročně přijmou jako relevantních, než vás začnou považovat za šum. Strop existuje, aby síť nezahltily triviální „co kdyby“ tvrzení a aby zůstala tak svobodná, jak si komunita přeje (signál se zachovává omezením objemu).

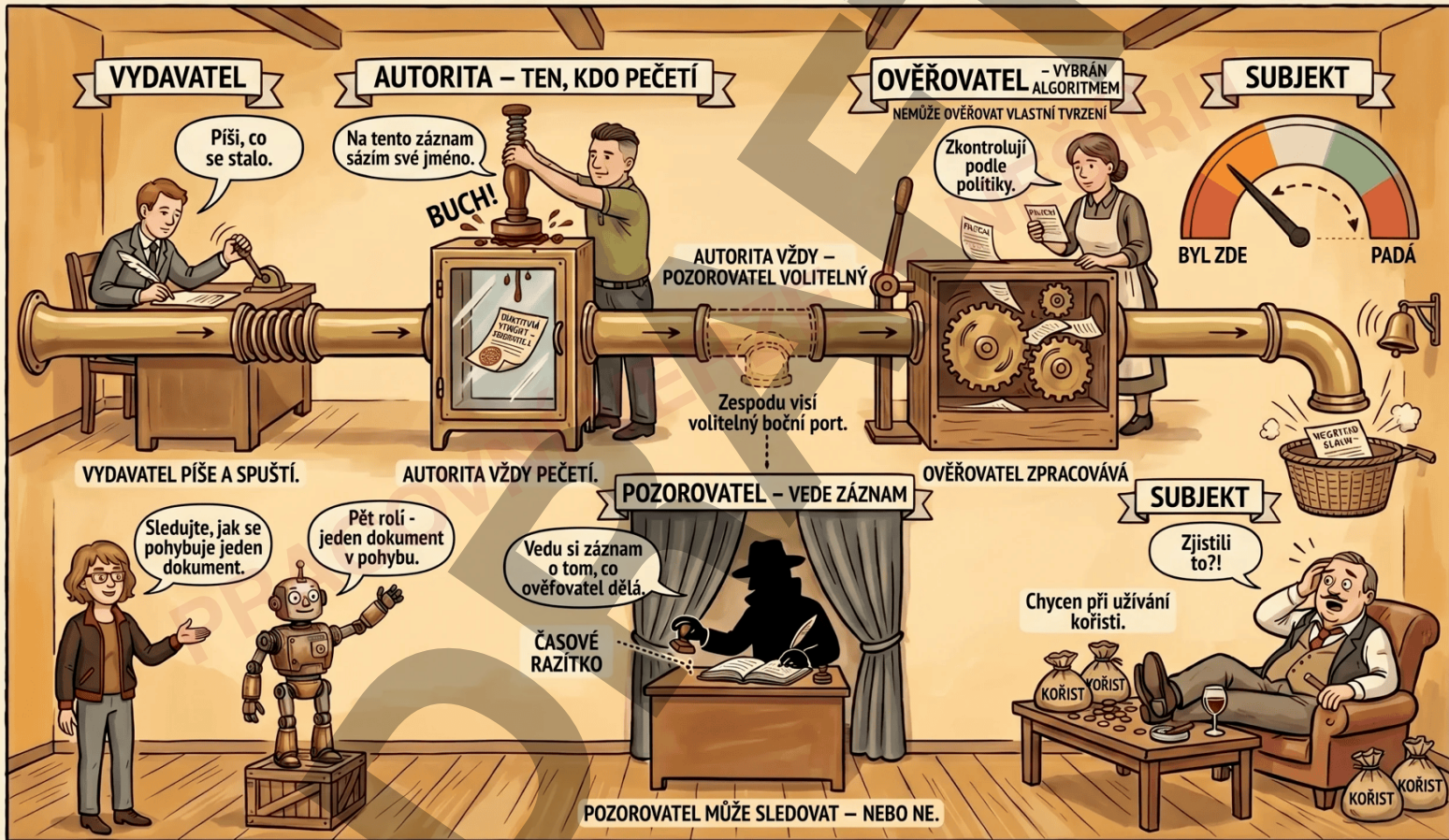
Vy si přečtete, co vám komunita dovoluje. Je to rozsah s určitým rozptylem podle toho, koho vážete největší vahou. Pak se v tomto přidělu rozhodnete — kolik tvrzení publikujete sami a kolik delegujete profesionálním službám, které je za vás publikují jen tehdy, když události spadají do jejich scope. To je to, co vás drží v dobrém postavení, aniž byste museli podávat tvrzení na každou drobnost, která se vám stane.

„Tokeny“ nebo chcete-li „žetony“ v grafice jsou vizuálním zástupcem této read-and-decide smyčky, ne doslovným artefaktem.

Delegovaná práva na publikaci je výhodné umět revokovat v reputační síti. To lze provést kdykoliv dokud delegát delegované právo nepoužije.

NEGATIVNÍ TVRZENÍ PROTÉKÁ SYSTÉMEM

SLEDUJTE JEDEN DOKUMENT — PODÍVEJTE SE, CO S NÍM KAŽDÁ ROLE DĚLÁ



PĚT ROLÍ, JEDEN DOKUMENT V POHYBU — NIKDO NEMŮŽE OVĚŘOVAT SÁM SEBE

Komunikace rolí

Následující grafika shrnuje, jak na sebe role navazují v reálném případě — od podání tvrzení vydavatelem až po publikaci v reputační síti.

Emergentní společenská smlouva — Politika/Policy

Zatím jsme popsali, jak se tvrzení ověřují a jaké role v tom hrají jednotlivé role. Teď se zaměříme na to, jak se z tisíců individuálních politik stává něco, co funguje jako skutečná společenská smlouva. Nic, co by připomínalo levičácké sny o společenské smlouvě a vynucené solidaritě.

Každý účastník deklaruje vlastní politiku podle své morálky (politiky/policy) — co považuje za přijatelné, jak reaguje na konkrétní chování ostatních. Souhrn všech politik napříč sítí, kterou daný DID zná (komunitou), produkuje emergentní etiku — pozorovatelné normy, které nikdo nenavrhl. Tyto emergentní normy podložené bilaterálními cenovými signály tvoří měřitelnou společenskou smlouvu: ne teoretický konstrukt, který nikdo od narození nepodepsal, ale empiricky pozorovatelná pravidla podložená skutečným chováním.

■ Společenská smlouva

Lidé se přou, jestli „společenská smlouva“ není oxymóron. Nikdo nic nepodepisuje, a přesto se na ni odvolávají legislativní i exekutivní akce v centralizovaných společnostech.

Fenomenologická analýza interakcí v decentralizované síti by mohla odhalit určitá emergentní pravidla — globální nebo lokální. Jak nazvat tyhle široce sdílené normy? Společenská smlouva? Stejně jako u komunit nejde společenskou smlouvu komunity přesně vypořádkovat a ohraničit — co pohled na komunitu, to jiná společenská smlouva.

POLITIKY SE SETKÁVAJÍ. POSTOJE SE TVOŘÍ.

DEKLAROVANÁ PRAVIDLA URČUJÍ DNES CENU – SLEVOU ZA SOULAD, MALUS ZA ROZDÍLNOST

KDYŽ SE POLITIKY SHODUJÍ



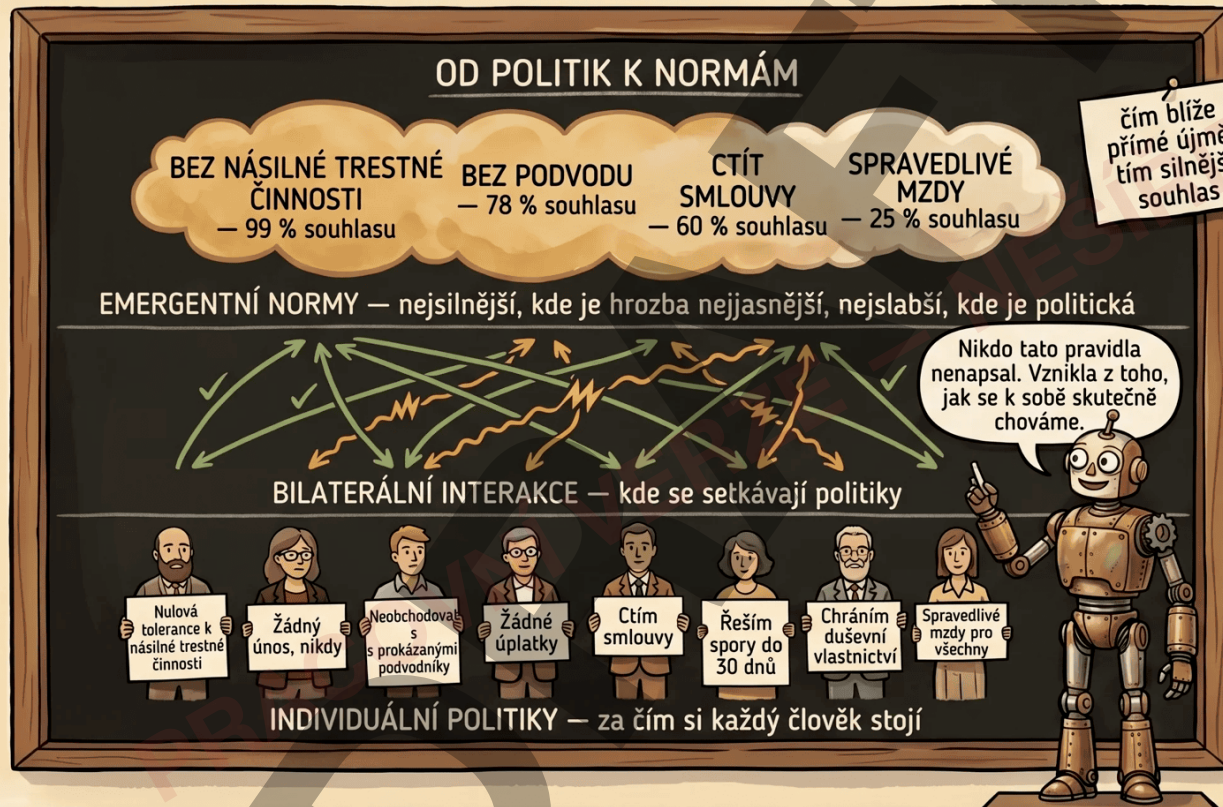
KDYŽ SE POLITIKY ROZCHÁZEJÍ



Když se dvě politiky setkají v obchodu, jejich soulad se stává modifikátorem ceny.

* Toto není o pověsti. Je to o tom, co každý veřejně deklaroval – a od čeho se nyní očekává, že to dodrží.

JAK VZNIKÁ ETIKA Z INDIVIDUÁLNÍCH POLITIK



Etika není navržena. Vzniká z toho, jak se k sobě skutečně chováme.

* Každá individuální politika je odrazem morálky daného člověka — formovaná tlakem přizpůsobit se své komunitě a prostředí.

Hodnotová politika

Stejně zavádějící je považovat „hodnotovou politiku“ za základ rozhodování. Hodnoty jsou spíš fenomenologické klastry pravidel, která se v daném čase běžně preferují. Vyvíjejí se a v čase nejsou konstantní.

Poskytování informací o sobě

Když vstupujeme do ekonomického vztahu jako dva DID subjekty, které se neznají, můžeme tomu druhému podepsat žádost do své komunity, aby o mně poskytla informace. To je ale velmi naivní představa o tom, co komunity jsou. Nejsou to uzavřené množiny — jedna DID může být účastníkem víc komunit.

Komunita je spíš fenomenologický jev z pohledu daného účastníka, který se projevuje v jeho sociální síti; není to něco, co má vždy smysl speciálně ohraničovat. Obyvatelé vesnice mohou být komunita, ale i člověk, který tam jezdí jen na víkend, může patřit k jiné komunitě v té samé vesnici. Komunita může být i fotbalové mužstvo spolu s jeho fanoušky, funkcionáři a rodinami všech zúčastněných. Národ nebo občané státu také mohou tvořit komunitu nebo komunity. Pohled na DID z různých úhlů může dát různé (často intuitivní) pohledy na komunity.

DID na pomezí jsou tedy mosty mezi komunitami a stejně jako v reálném životě se podílejí na poskytování informací o jiných členech komunit — ať už na amatérské, nebo profesionální úrovni typu autorita specializující se na propojování lidí a agregaci informací o rizikových DID.

Některé typy informací v DID síti mají povahu výhodného určení pro vzájemnou bezpodmínečnou výměnu (násilné trestné činy, podvody atp.). Jiné typy informací nicméně může komunita považovat za výlučné pro použití v rámci komunity (ekvivalent občanství, vykonané služby pro komunitu, atp.). Šířitelnost takových informací závisí na deklarovaných politikách členů komunit.

Komunita si hlídá své soukromí ve svém okruhu a naopak vyměňuje informace vzájemně výhodné na bezpodmínečnou výměnu.

5. Zločin a trest

Víme, jak síť funguje: jak vznikají záznamy, kdo je ověřuje, jak se brání podvodům ověřovatelů. Zbývá otázka — co se stane, když někdo někomu opravdu ublíží?

■ Jak moc jsme na sobě závislí?

Všichni na jednom jevišti velikého světa stojíme, a cokoliv se tu koná, všech se týče.

Jan Amos Komenský (Labyrint světa a ráj srdce)

Důvodů, proč se k reputační síti připojit nebo ji odmítnout, může být mnoho. Věřím ale, že jeden aspekt lidské přirozenosti, často považovaný za temný, může posloužit dobré věci. Mluvím o lidské potřebě cítit zadostiučinění tváří v tvář vnímané křivdě.

Zadostiučinění, spravedlnost, pomsta — spojujeme je s negativními emocemi. Aby společnost držela pohromadě, musíme alespoň předstírat, že zadostiučinění doručují centralizované instituce; jinak by se jednotlivci necítili spojeni se společností, ve které žijí. Potřebujeme v průměru patřit do nějakého týmu a důvěřovat mu. Když někdo někomu ublíží, společnost sleduje, jak bude zadostiučinění doručeno a v jaké míře. Trochu kontroverzně tvrdím, že často v historii ani nyní nezáleželo na tom, jestli byl proces s podezřelými z napáchání křivd čistý — záleželo na tom, že společnost viděla *někoho* potrestaného. Plnilo to svou funkci (četné justiční omyly a odpor k přezkoumávání starých případů mluví za vše). Pohled

oběti a pozůstalých je až druhotný. Primární jsou signály zbytku společnosti, neboť křivdy zase nejsou až tak časté, že by byly na denním pořádku každého z nás.

Decentralizovaný reputační systém by veřejnosti umožnil vidět přímé i nepřímé důkazy (auditované i neauditované). Společnost by mohla informace vyhodnotit — sama, nebo přes volnotržní služby specializované na takové hodnocení — a podle kvalitativních a kvantitativních signálů rozhodnout, jaká opatření vůči subjektu (nebo i vůči vydavateli či ověřující autoritě) uplatnit.

Co je trest? Je to forma ponížení údajného pachatele ztrátou jeho privilegií — aby oběť i společnost cítily, že škodlivé činy se nevyplácejí. Tohle je podstatné: škodlivé nebo nebezpečné chování se nesmí vyplácet a zároveň musí poskytnout pocit zadostiučinění obětem i zbytku společnosti/komunitě.

Musí takový trest zajišťovat centrální autorita? Co kdyby každý mohl předem deklarovat, jak bude na určité činy reagovat? Trest na cizím majetku samozřejmě vykonat nemůžu. Ale můžu deklarovat, že svůj majetek zpřístupním vybrané sadě exekutivních autorit, aby pachatele potrestaly, když viník vstoupí na mé državy. A můžu to deklarovat veřejně, aby ostatní mohli posoudit můj přístup.

A tady přichází cenový mechanismus přiměřenosti. Když deklaruji tvrdé tresty za drobné přestupky, sít' můj extremismus nacení: ostatní mě budou považovat za nepřiměřeného a mé náklady na ověřování vzrostou — méně lidí se mnou bude chtít obchodovat nebo za horší ceny, méně ověřovatelů přijme mé záznamy za rozumnou cenu. Když jsem naopak příliš shovívavý, komunita mě bude vnímat jako riziko. Když budu tolerovat podvody, komunita patrně bude shovívavá k pachatelům činů, které se naopak dotknou mě, aby mi to dala sežrat.

Spravedlnost přestává být luxusním zbožím. Když vám někdo ublíží, zaznamenání křivdy je cenově přijatelné, záznam je trvalý a důsledky pro provinilce jsou reálné.

■ Detekce pokrytectví

Samotná deklarace politiky nestačí — když deklaruji, že pravidlo dodržuji, ale mé chování se od něj odchyluje, rozdíl je reputační zátěží. Síť nerozlišuje mezi „porušil zákon“ a „porušil vlastní slovo“ — obojí je měřitelný signál. Pokrytectví je drahé a neznám draždivější červený hadr.

JEDNA PAST. JEDNA CESTA VEN.

INSIDER VŽDY VÝHRAVÁ KONTRAKT – DOKUD SÍŤ NEUMOŽNÍ LIDEM NAKUPOVAT PŘÍMO, BEZ POTŘEBY POVOLENÍ.



Veřejnost souhlasí s nutností nového veřejného IT systému, placeného z rozpočtu, z daní.



Úředník krčí rameny. Jeho kapsa se nadouvá úplatky.



Kontrakt byl zadán. Insider má licenci – ale žádné dovednosti a nerespektuje práci.



Insider navštěvuje souseda. „Laskavá nabídka“ je jen nejmenší drobeček.



stížnost



ticho



zavřené dveře



u právníka

Stížnost, ticho, zavřené dveře, právník. Past je zabudována do samotných pravidel.

Kde je regulace, síť reputace je mostem.



SÍŤ REPUTACE
— zde začíná nový svět —



dodání na prvním místě



poptávka to nachází



slušný život

Dodává na prvním místě. Lidé najdou aplikaci a používají ji. Každý vědný uživatel zaplatí trochu. Slušný život. Žádná ústřední autorita, kterou by bylo nutné uplatit.

Reputace je nové Dodání je důkaz.



* Když pravidla píše insider, stěžovat si uvnitř pravidel je pastí – i ty pokuty se vrací do dalšího zmanipulovaného tendru. Síť reputace je cesta ven: občané najdou produkt, zaplatí přímo tvůrci a komunita propůjčí jedinou licenci, na které záleží – důvěru získanou dodáním.

Dvě cesty. Past je v pravidlech. Cesta ven je pravidla úplně obejít.

1. TRADIČNÍ

2. SÍŤ REPUTACE

JAK SE HROMADÍ DŮKAZY

"jedno izolované tvrzení"



pouhé jedno tvrzení – příliš málo na čin.
ani jedna strana není odsouzena.

"vzorec"



pět nezávislých zdrojů –
objevuje se vzorec.

"drtivá váha"



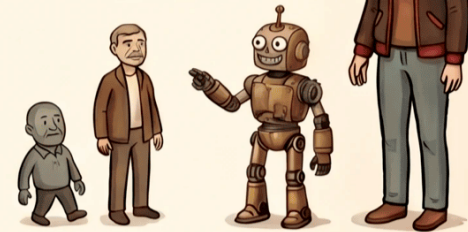
dvacet nezávislých zdrojů –
drtivá váha.



vysílání stejného tvrzení bez důkazů – když
komunita nic nevidí, je to pomluva a stojí to žalobce.



jeden žalobce ukazuje na všechny –
vzorcem je žalobce, nikoliv obviněný.



to vypadá jako dnešní svět.
a je – jen motivy jsou teď poctivé.
žádná revoluce. jen lepší pobídky.

Nezávislost je vším. Jeden hlas opakováný je hluk. Mnoho hlasů z různých míst je signál.

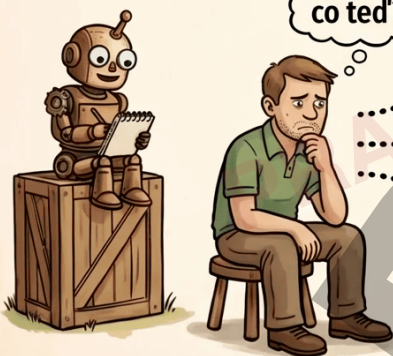
PO ŠKODĚ — CO UDĚLÁTE?

odmítnutí. vynucení. dobrovolnost. tři odpovědi vesnice.

CO SE STALO



CO TEĎ?



Racionální volba je vždy nejlépejší: OPRAVTE TO SAMI.

NEZNALOST — předstírejte, že se nic nestalo



beznaprawy — každý obchod ho odmítá — vyhnánství z hospodářského života

TREST — vynucení komunitou po odmítnutí nápravy



vynucená náprava pod dohledem davu — splaceno, ale vesnice mu zvyšuje cenu — lekce musí zůstat.

ODČINĚNÍ — dobrovolná náprava před odsouzením



dobrovolná, včasná náprava — veřejně přijata — pověst se uzdravuje, opatrně.

toto vypadá jako dnešní svět. je to tak — jen náklady jsou nyní všem viditelné. žádná revoluce. jen lepší podmínky.

Před redakční úpravou

Před redakční úpravou s. 103

■ Kvantita vs kvalita — porušení binárního paradigmatu viny

V centralizované justici je vina binární: 0 nebo 1, vinen nebo nevinen. V reputační síti nejde o to, jestli je vina prokázána, ale o kumulaci signálů.

Jedno neprokázané obvinění z krádeže obviněného pravděpodobně nevyvolá tolik ostražitosti — vyvolá ale ostražitost vůči obviňovateli. Vícero nepřímých indikátorů z různých nezávislých zdrojů už váhu mít začíná. Klíčové přitom není jen množství, ale i kvalita: nezávislost svědků (různí lidé, různé kontexty), konzistence vzorce (opakující se typ podezření), časová korelace.

Naopak časté bezdůvodné obvinění, které se od stejného vydavatele opakuje často na různé cílové subjekty, může být vyhodnoceno jako pomluva — a reputace obviňovatele zaplatí cenu.

Neměli bychom také přehlížet odčinění — dobrovolný akt před prokázáním viny, který nabízí cestu k mírnějšímu trestu. Trest nastupuje, když pachatel neudělá žádný krok k odčinění a doufá, že následkům unikne — podobně jako se to v centralizovaném systému dá koupit korupcí.

■ Typy provinění

Typy informací nemusí být omezeny na trestné činy; mohou zahrnovat: - popisy zločinů - porušení smluv a podvody - nemorální chování - narušování veřejného pořádku, reálného i virtuálního —...

Každý nový záznam v DID síti upraví hodnocenou reputaci a riziko daného DID (ať už adresáta, autora, nebo ověřující autority). Čím větší mám zodpovědnost za osud ostatních, tím opatrnější jsem.

■ Vynucování trestu pomocí delegování

Trest nemusím vynucovat osobně. Mohu (podobně jako pojištění) platit autoritu, která vynucuje výsledky podle předem definovaných pravidel — ekvivalent vyšetřovacích, pořádkových a justičních služeb. Když autorita vynucuje nepřiměřeně nebo nevynucuje vůbec, její reputace utrpí — a na reputaci stojí její schopnost užít se.

Delegace je v síti obecný princip: jakákoli aktivita DID se dá delegovat na jiný DID — ověřování, vydávání tvrzení, reakce na spory, deklarace konsenzu. Delegace je kdykoli odvolatelná. Umožňuje specializaci bez ztráty konečné kontroly.

KDO VYŠETŘUJE, KDO VYMÁHÁ?

ÚJMA → VYŠETŘOVATEL → ZÁZNAM → VYKONAVATEL → ODPOVĚDNOST



DELEGACE JE ODVOLATELNÁ. Jakákoliv DID aktivita může být delegována na jiné DID – a kdykoliv vzata zpět. *nevykonáváte trest sami. delegujete. a delegát se zodpovídá vám.*

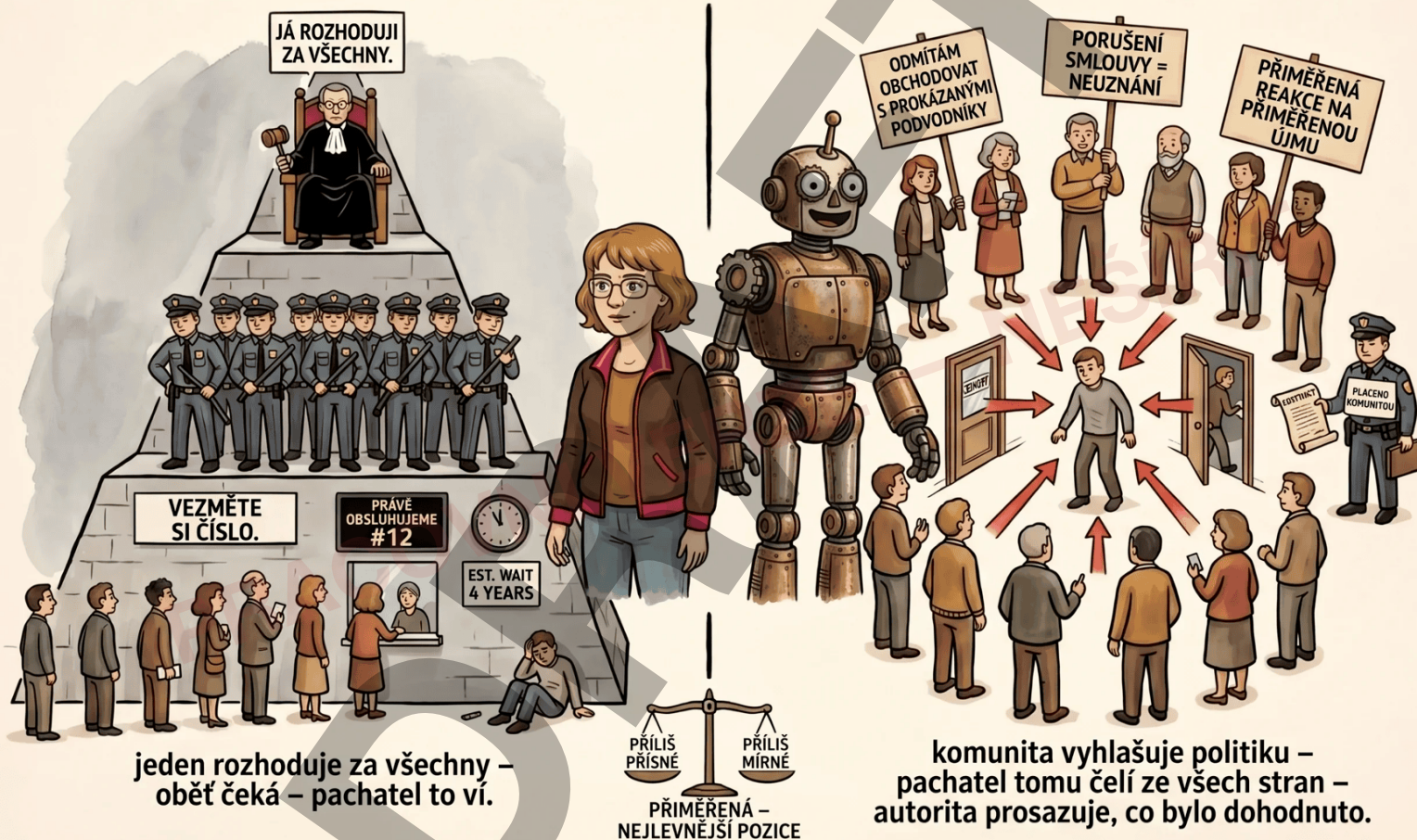
■ Demokratizace řízení rizik (Risk Management)

Necenzurovatelná reputační síť by demokratizovala to, co banky nebo údržbáři větších průmyslových celků dělají jako svou klíčovou činnost — řízení rizik.

Pro bankéře, který stojí před klientem, je hodnocení rizik připraveno předem, aby se mohl soustředit na obchodní interakci v rámci předem nastavených limitů. Sofistikovaní údržbáři v pravidelných servisních intervalech sbírají indikátory rizik (známky trhlin konstrukcí a procesy narušování provozní infrastruktury atp.) a dovedou předpovědět životnost i to, kdy a jaký zásah bude potřeba.

Použití DID si představuji podobně — někdo (pravděpodobně za poplatek) poskytne lidsky čitelný souhrn o protistraně. Souhrn bude odrážet úhel pohledu na rizika, který si zákazník objednal.

TREST BEZ ÚSTŘEDNÍ AUTORITY



jeden rozhoduje za všechny –
oběť čeká – pachatel to ví.

komunita vyhlašuje politiku –
pachatel tomu čelí ze všech stran –
autorita prosazuje, co bylo dohodnuto.

Odčinění je levnější než trest. Trest je levnější než nevědomost.

6. Sleduj stopu peněz

Máme decentralizovanou reputační síť a motivaci ji používat. Už teď umí svým uživatelům přinést konkurenční výhodu — vyjasnit možná rizika, efektivněji plánovat výběr protistrany a strategii vyjednávání s ní, včetně opatření, která známá rizika snižují.

Následuje jeden možný návrh metodiky¹, jak ho použít — jak pomocí jeho vlastností vytvořit migrační cestu ze současného systému k jeho evolučnímu nástupci. Patrně nese znaky charakteristické pro střední Evropu, kde tato teze vznikla. Lokální podmínky budou vyžadovat lokální úpravy. To, co bych doporučoval zachovat všude, je nesmlouvavý ráz opatření vůči státu — bez něj se cíl rozmělní v nekonečné diskusi a změna nepřijde nikdy. Dávejte si pozor — zástupci a podporovatelé státu vás budou zaměstnávat nesmysly. Neskákejte na to, jde jim o živobytí.

Slabé místo státu — peníze

Vraťme se na začátek. Chceme více výsledných svobod, více vlivu na jejich podobu a více odpovědnosti, která jim odpovídá. Otázka zní jednoduše: kde má stát zranitelné místo, na které lze zatlačit, aniž bychom sáhli po násilí?

Odpověď je nudná a o to silnější. Peníze.

¹**Dekonstrukce státu** — v českých podmínkách se jí patrně dopodrobna bude zabývat stejnojmenná kniha českého autora Daniela Steigerwalda (plánované vydání 2026). Osobně si od inspirativních postupů v ní velmi slibuji.

Stát je v jádru tok peněz. Přes peníze platí svůj donucovací aparát — poslední článek, který vynucuje pravidla. Bez peněz není monopol na násilí. Jakmile peníze začnou váznout, stát začne ustupovat — protože nemá čím platit ty, kdo ho fyzicky drží.

Toky peněz přirozeně kolísají — sezónně, ekonomicky, podle nálady investorů. Stát to maskuje půjčkami na finančních trzích. Občas je půjčka racionální: investice, která se vrátí. Většinou ale jde o krytí předimenzovaných výdajů na agendy, které dávno přerostly základní účel státu — obranu, vnitřní bezpečnost, justici, diplomacii. Při překročení určitých prahů reaguje národní banka úrokovými sazbami, opřenými o vlastní odhad inflace.

A tady přichází tichá daň. Inflace zdaleka není jen účetní problém makroekonomů. Je to skrytá daň z kupní síly měny, kterou platí každý, kdo si schoval pár korun na stáří. Nízkou inflaci lidé tolerují, protože nechápují její dlouhodobé účinky — neuvědomují si, že i jednociferná čísla v dlouhém horizontu rozežirají úspory natolik, že se na stáří sami zabezpečit nedokážou. A když nedokážou, jsou vychováváni k závislosti na státních dávkách. Nakonec na nich visí a jsou ke státu připoutáváni.

V turbulentních dobách — válka, pandemie, „nutná“ investice — stát rovnou zapne tisk peněz. Kupní síla zodpovědných střadatelů a pracujících klesá, zatímco jim slibujeme, že jsou dobře odměňováni. Někdo jim potají kradе čas a chválí je za to, jak skvěle vydělávají.

Tohle vážně podkopává důvěru ve stát. A důvěra je to jediné lepidlo, které celé to soukolí drží pohromadě. To je páka, na kterou se má smysl zapřít.

■ Proč peníze, a ne jiná slabá místa?

Dalším slabým místem civilizace je třeba distribuce energií. Jenže přerušení jejího toku není páka — byla by to agrese, terorismus. Dobrovolná neúčast není totéž co úmyslné poškozování druhých. Peníze jsou výjimečné v tom, že tlak lze vyvinout dobrovolně, transparentně a bez násilí.

Navrhovaný přechod k nástupci státu

Evoluce, ne revoluce

Náhlá změna budí odpor, i když je cíl přitažlivý. Rozbývá vazby — sociální, ekonomické, politické — a lidé instinktivně chrání to, co znají, před tím, co teprve uvidí.

Správný přístup je proto postupný — evoluční. Takový, aby starý systém nemohl ten nový vypnout jediným stiskem tlačítka — protože v okamžiku, kdy by mohl, by to udělal.

Bohužel to znamená smířit se s tím, že rovnovážné dobrovolnosti nedosáhneme hned po nasazení reputační sítě, ale že přijde s postupnou mírou adopce. Nástup může být — a patrně bude — pomalý, tažený touhou jednotlivců najít zastání u komunity skrze reputační síť, když konformní způsob dovolání se spravedlnosti selže (a ono selže). Ukažme si, jak by vypadal, včetně proporčních odhadů.

SLEDUJ PENÍZE – PŘÍBĚH DOSUD

CO MÁME

DECENTRALIZOVANÁ REPUTAČNÍ SÍŤ –
NEZKORUMPOVATELNÁ, NECENZUROVATELNÁ

všech pět bloků
společně tvoří síť.



základ je
postaven.

tohle je
NEDEMOKRATICKÉ!

ale vždycky to
tak fungovalo.

nejší
ani
zvolen.

OTÁZKA NYNÍ

když máš pochybnosti,
zaškrť tok

SLEDUJ
PENÍZE



Máme síť. Víme, jak to funguje. Nyní: když máš pochybnosti, zaškrť tať tok.
moc státu spočívá na penězích! sleduj ji.

■ Prázdná koryta — nehrajte dle pravidel, která jsou nastavena na vaši prohru

Pokusy o reformu zevnitř spoléhají na vnitřní mechanismy moci v naději, že úředníci budou prosazovat změny proti vlastním pobídkám. To se nestane.

Proč systém žít, místo abychom vysušili koryta, kterými mu teče život? Místo měnit starý systém a hrát podle jeho pravidel postavme nad ním novou vrstvu — takovou, která ze starého postupně udělá podmnožinu nového. Na začátku ta podmnožina téměř vyplní nadmnožinu. V čase se aktéři přesouvají.

Firmy to znají: když je starý systém příliš propletený na to, aby se nahradil, postaví paralelní a postupně do něj migrují uživatelé.

To, že státu vznikne nesoulad mezi plněním a zákonnými požadavky a bude mít tendenci se na to odvolávat, je čistě problém jeho představitelů a participantů — není potřeba se na to ohlížet. Důležité je hlídat jedinou věc: nevyvolat násilnou revoluci.

Čtyři nástroje, které se vzájemně podporují

Až dosud se DID reputační síť mohla zdát užitečná hlavně pro spravedlnost a konsenzus. Věřím, že by se dokázala stabilizovat a odolávat útokům — meritokraticky, na základě skutečných zásluh, ne formálních titulů. Ale samotná reputace stát nedonutí ustoupit. Donutí ho ekonomika a nátlak skrze ni.

Nic nám nebrání použít DID jako správce dalších nástrojů, které tvrdě tlačí na peníze. Nezačínejte plnou dobrovolností občanů — nastavte směr, který nejde státem zastavit. Přechod stojí na čtyřech konkrétních nástrojích, které si navzájem podpirají záda. Žádný z nich sám o sobě nestačí.

Jednoduchý daňový systém — vstupní lákadlo

Prvním nástrojem je jednoduchý, průhledný daňový systém postavený na DID infrastruktuře. Jedna proporcionální sazba ze všech příjmů. Žádné výjimky, daňové prázdniny, firemní odpočty, pobídky. Každá platba je auditovatelně spojena s DID, které ji zaplatilo. Křížová kontrola je triviální.

Sazba by byla nastavená o něco výhodněji než ve starém systému pro část poplatníků — to je lákadlo pro vstup. Daňová zátěž by rok od roku klesala, systém by byl čím dál přitažlivější, migrace by nabírala na tempu. Systém je zároveň správcem záznamů i výběřčím — žádný prostředník, žádná neprůhlednost.

Elektronický registr výdajů (Electronic Spending Register)

Druhým nástrojem je obrácení EET (Elektronická evidence tržeb). Místo aby stát sledoval každou tržbu živnostníka, sledujeme my každý jeho výdaj. Stát nedostane prostředky z jednoduchého daňového systému na své jednotlivé platby, pakliže každá z nich — bez výjimky — neprojde tímto sítem.

ESR je proxy², který páruje každý realizovaný výdaj státu a veřejného sektoru se záznamem plánované platby — včetně kontextového odůvodnění a identifikace příjemce, výdajového subjektu i účelu. Výsledkem jsou surová veřejná a hierarchizovatelná data. Každý si je může vzít a analyzovat. Každý může nabízet doporučení daňovým poplatníkům, co s nimi. To, co kontrolní úřady nedokázaly za léta, je najednou na kliknutí k ruce všem.

²Proxy (angl. *zástupce*) — zde zprostředkovatel, který jedná jménem jiného subjektu. ESR proxy přijímá záznamy o plánovaných platbách od kohokoli, páruje je s realizovanými výdaji státu a výslednou množinu zpřístupňuje veřejnosti.

Abyste se zapojili, nemusíte přejít k novému daňovému systému. Stačí zaplatit plně vratnou zástavu (řekněme 1–3 EUR) za realizovanou platbu. Nerealizovaný zbytek propadá jako filtr spamu, aby se systém nezahltl útoky. Záznam může zadat kdokoli — příbuzný za nemohoucího prarodiče, soused za zanedbané veřejné služby, podnikatel za neproplacenou fakturu, úředník exportem ze svého systému.

Předpokládám, že politické strany se přirozeně přerodí v poskytovatele analýz, nebo vzniknou nové, které nahradí ty staré. Místo příspěvků z daní začnou nabízet expertízu — svým přívržencům dávají na hodnotách postavené přehledy spřátelených autorit, jejich služeb a verifikačních politik. Z lenosti odfláknuté nebo nesmyslné záznamy se automaticky stávají kandidáty na rozpočtové škrt. V prvním kole vám platba vyplacená bude vždy, ale data poslouží jako podklad pro posouzení, jestli má státní výdaj dál smysl. Dodavatelé a další lidé na výplatní pásce státu mají motivaci dohlédnout, aby úředníci výdaje párovali zodpovědně. Jinak peníze v dalším kole nepřítečou.

■ Odkud se vzala zkratka ESR

V letech 2016 až 2022 zavedla česká vláda systém Elektronické evidence tržeb (EET) vůči vlastním občanům — živnostníkům a podnikatelům. Vzkaz byl jednoduchý: „Předpokládáme, že každý z vás stát podvádí. Budete evidovat každou jednotlivou tržbu, posílat ji v reálném čase na naše servery a my vás budeme hlídat. Spoluobčany budeme finančně odměňovat za to, že nás na vás upozorní, když se budete EET vyhýbat.“

EET vycházela z balkánských vzorů. První zemí, která v roce 2013 spustila celostátní povinný systém online evidence tržeb v reálném čase, bylo Chorvatsko pod názvem fiskalizacija. Česko model přijalo s několikaletým zpožděním a stalo se jedním z nejpřísnějších evropských systémů sledování tržeb.

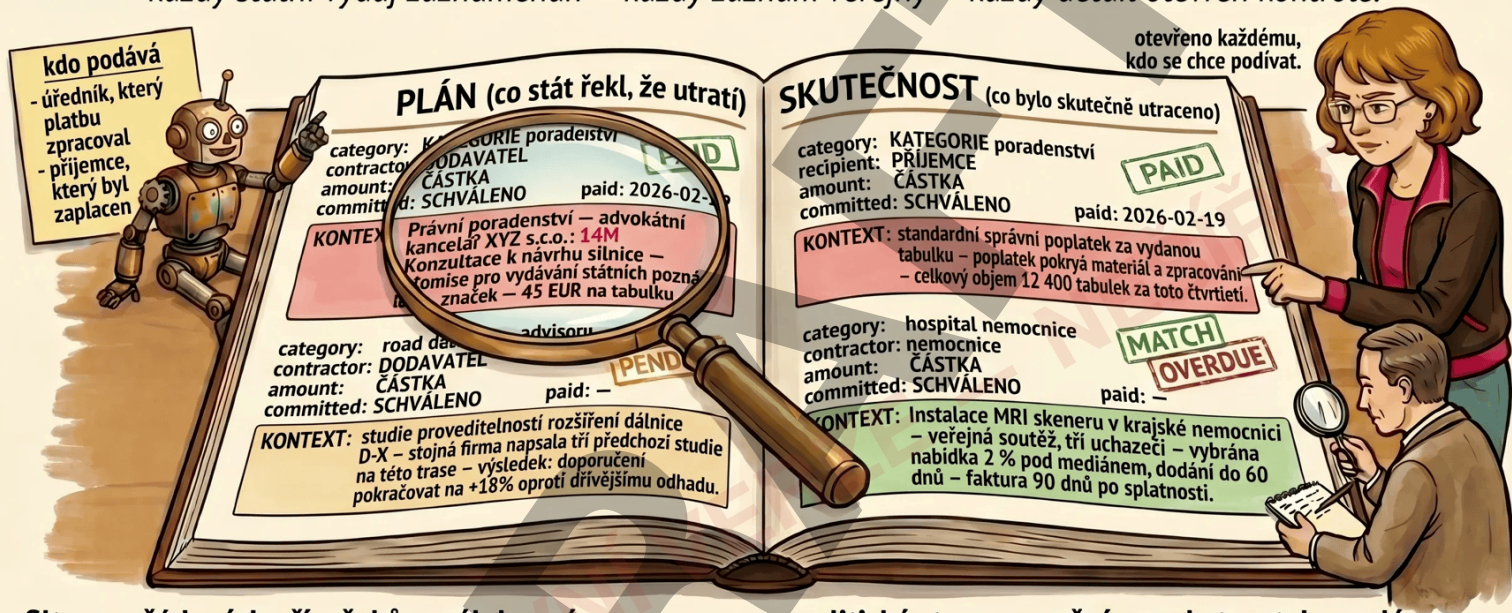
Pokud temná strana neváhá, proč bychom měli my? ESR je tatáž logika obrácená vzhůru nohama: stát se prokazuje občanům.

Alokace daní občany — váha rozhodnutí

Třetí nástroj dává daňovým poplatníkům přímý vliv na to, kam jejich peníze putují. V prvním kole stát dostal své peníze bez ohledu na to, co ESR ukázal. V druhém kole už ne — rozhoduje analýza z prvního kola a opatření, která z ní vzejdou. Malé procento zaplacené daně může plátce alokovat sám — pokud jeho DID splňuje reputační požadavky (občanství, rezidence, komunitou uznanou zletilost/způsobilost). Alokovatelné procento rok od roku roste. Potenciálně exponenciálně. Z pěti procent dnes na desítky procent za dekádu.

ESR – ELEKTRONICKÉ VÝKAZNICTVÍ VÝDAJŮ

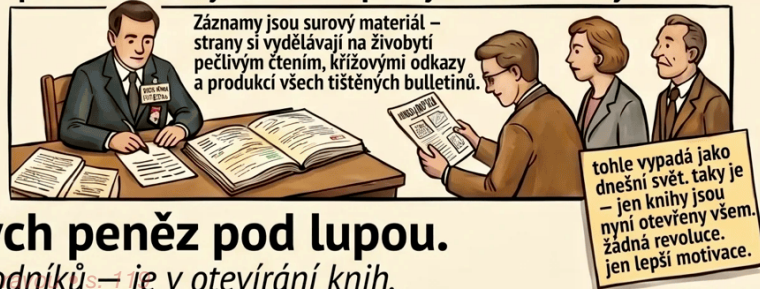
každý státní výdaj zaznamenán – každý záznam veřejný – každý detail otevřen kontrole.



filtr nevyžádaných příspěvků – záloha vrácena



politické strany se mění v poskytovatele analýz



Každá koruna veřejných peněz pod lupou.

hodnota není v chytání podvodníků – je v otevírání knih.

Surová data z ESR přirozeně řídí rozhodování poplatníků. Nekvalitní záznamy fungují jako varovný signál pro doporučené škrty. Záznamy může vytvářet kdokoli; úředníci je musí párovat. Bez toho daňový systém peníze státu nepošle — ani do státní pokladny, ani do jiných kapitol. Politický boj se přesouvá z volební urny k dennodenní alokaci konkrétních korun.

Vyjednávací platforma se státem — páka

Čtvrtý nástroj je páka, která vše propojuje a teprve dělá ze sítě reálnou hrozbu. Hlavní konflikt bude o to, jestli stát přijme ESR jako závazný standard — nejdřív na národní úrovni — a jak velké hrozby se budou muset splnit ze strany účastníků reputační sítě, aby se tak stalo.

Pákou je just-in-time financování státu, podmíněné párováním plateb s ESR. Peníze tečou až ve chvíli, kdy stát splní podmínky transparentnosti. V reputační síti vznikne čekací listina účastníků. Aktivace nastane v okamžiku, kdy skupina dosáhne ekonomicky významné velikosti — dost velké na to, aby ohrozila růst HDP. Tehdy se občanská neposlušnost stává věrohodnou hrozbou, ne gestem.

Stát si nejdéle podrží problematické platby svázané s korupcí. Pod tlakem ustoupí nejdřív tam, kde má jednoduchou obhajobu a kde se nedají hledat úspory. Postupný a zvyšující se tlak ho donutí ustupovat postupně ze všech pozic.

Občanství bez občanky

S přechodem na DID infrastrukturu ztrácí státem vydaný průkaz totožnosti svůj monopolní smysl. Nepotřebujete občanku — máte řadu DID identit a některé z nich nesou tvrzení, že jste Čech, rezident určité obce, absolvent určité školy. Tvrzení je ověřitelné, trvalé, nezávislé na státní administrativě.

ALOKACE DANÍ OBČANY – VY ROZHODUJETE, KAM VAŠE DANĚ JDOU

studujte záznamy ESR. pak posouvejte táhla.

ZPRÁVA Z ANALÝZY ESR

(důvěryhodný analytik – zvolený vámi)



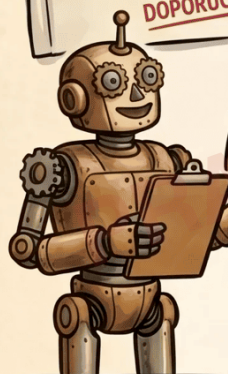
ministerstvo obrany:

- 7 zakázek za 2 roky jednomu dodavateli
- žádná veřejná slyšení o reformě nákupů
- 90denní zpoždění plateb u 60 % faktur

DOPORUČUJI SNÍŽIT.



rep 4.7/5



po přečtení zprávy – obranu dolů.

nebo delegujte toto

nechcete alokovat sami?
delegujte na:

- analytika vaší strany
- důvěryhodného souseda
- kohokoli, koho si vyberete
- a kdykoli to odvoláte.

▶ ŠKOLSTVÍ

30%

▶ ZDRAVOTNICTVÍ

25%

▼ OBRANA

10%

▶ personál

5%

▶ vybavení

3%

▶ výzkum a vývoj

2%

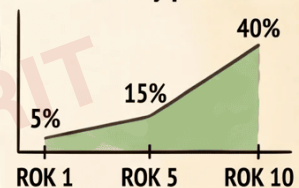
▶ INFRASTRUKTURA

20%

▼ SOCIÁLNÍ SLUŽBY

15%

alokovatelný podíl roste



klikněte na libovolný řádek k rozbalení – alokujte na jakékoli úrovni.

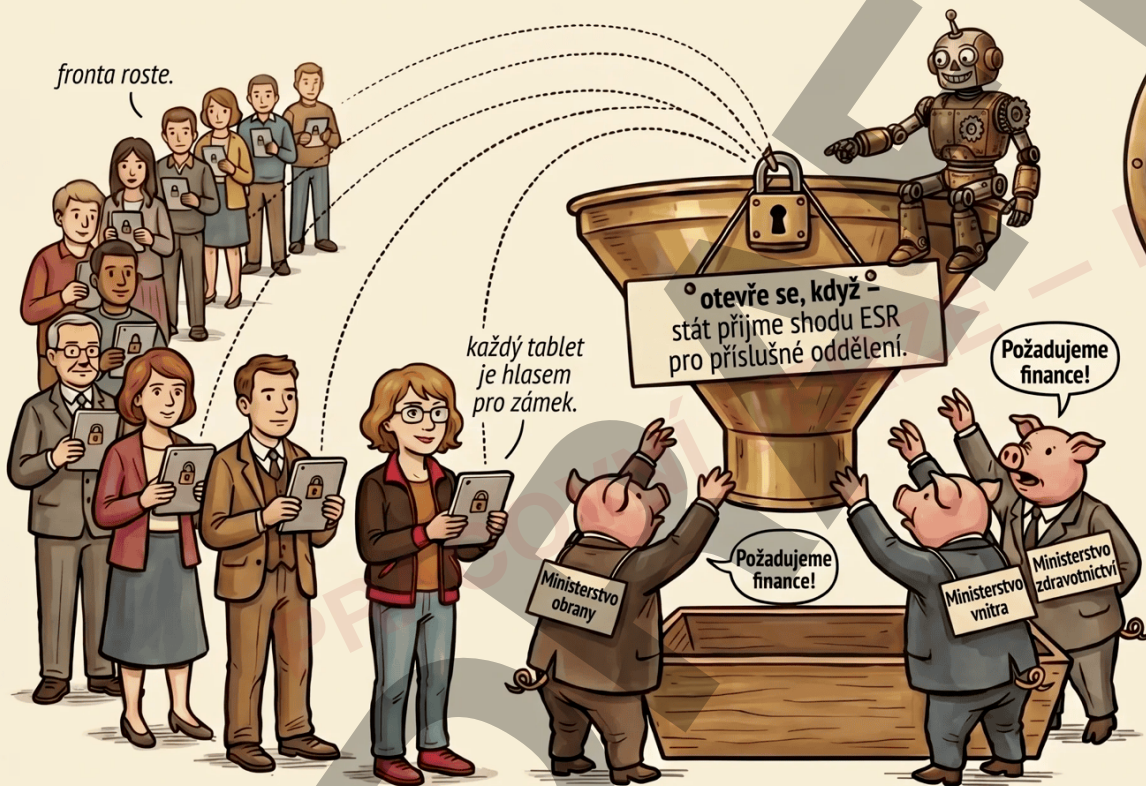


to vypadá jako dnešní svět. je to – je teď ve vaší ruce. žádná revoluce. jen lepší pobídky.

Od 5 % dnes k 40 % za desetiletí. Vy rozhodujete.
záznamy jsou otevřené. analýza je vaše. stejně jako táhlo.

NEGOCIAČNÍ PLATFORMA – UZAVŘENÝ NÁSYP

občané drží klíč. stát se otevře, když jsou podmínky splněny.



malý zlomek HDP stačí – při kritickém množství se odepření stává skutečnou hrozbou.

po dosažení kritického množství –

stát nejprve otevře své účty pro jednoduché, obhajitelné platby.

kategorie spojené s korupcí zůstávají uzamčeny nejdéle.

každé odemčení vyžaduje větší tlak – a je samo o sobě zaznamenáno.

to vypadá jako dnešní svět.

je to tak – jenom je klíč nyní v mnoha rukou. žádná revoluce. jen lepší motivace.

Peníze tečou, když existuje transparentnost. Občané drží klíč.
žádná síla. žádná revoluce. jen dostatek tabletů k tomu, aby bylo odepření důvěryhodné.

ČTYŘI NÁSTROJE EVOLUČNÍHO PŘECHODU.

system přestavěný zevnitř – aniž by se zbortil.

JEDNODUCHÁ DAŇ



jedna sazba. žádné úlevy.
křížově ověřitelné.

EVR – ELEKTRONICKÉ VYKAZOVÁNÍ VÝDAJŮ



každý výdaj zaznamenán –
každý záznam veřejný –
každý detail otevřený.

OBČANSKÁ ALOKACE DANÍ

5% → 15% → 40%
ROK 1 → ROK 5 → ROK 10



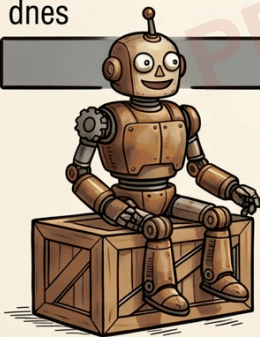
prostudujte si záznamy –
a pohněte posuvníky.

PLATFORMA PRO VYJEDNÁVÁNÍ



peníze plynou pouze tehdy,
jsou-li splněny podmínky
transparentnosti.

dnes



evoluce v plném proudu

95%

za deset let

rozšiřování



Evoluce, nikoli revoluce.

čtyři nástroje, které mění systém zevnitř.

vypadá to jako dnešní
stav – jen nástroje jsou
nyní v rukou občanů.
žádná revoluce.
jen lepší pobídky.

Otevírá se otázka technického provedení: kdo se na trhu ujme ověřování stávajících občanů mimo kontrolu státu, aby zájemce přemigroval do DID s patřičným tvrzením? Pravděpodobně vzniknou volnotržní autority specializované na ověřování identity — notáři, místní komunity, zaměstnavatelé. Svou reputací ručí za to, že daný DID skutečně patří osobě, která to o sobě tvrdí. Občanství — tedy příslušnost k určitému pohledu na komunitu — se zbaví potřeby centrální evidence. Propojením přes reputační síť se vložené údaje pospojují a validují podruhé, potřetí, počtvrté, atd.

Důsledek je intuitivní, ale v centralizovaném systému neřešitelný. Dnes může politické vedení s vidinou snazšího znovuzvolení dovážet na území komunity koncentrované problémy — přijímat migranty z jiných civilizačních okruhů bez ohledu na absorpční kapacitu a ochotu stávající komunity, měnit původní komunity tlakem, pod kterým nestíhají asimilovat příchozí z jiných civilizačních okruhů. V DID síti si korupčně přijatý migrant nemůže být jistý, že ho komunita bude dál brát za svého. Členové komunity objektivně nemusejí snášet, když jim v uniformě jejich komunity přijde do domu cizinec a vyhrožuje zákonností opatření, které chce v domě provést (zabavení telefonu potomka za příspěvek na sociální síti). S decentralizovanou reputací se s tím majorita smířovat nemusí — protože o příslušnosti ke komunitě nerozhoduje úředník, ale komunita sama, prostřednictvím svých reputačních signálů.

Síla volebního hlasu v rozhodování o věcech spadajících pod stát by v budoucnu mohla přísně korelovat se záznamy odvodů do jednoduchého daňového systému. V kombinaci s vhodnými tvrzeními o DID (například „daná osoba je občanem ČR“) lze pak vyloučit cizí státní příslušníky z voleb — registr obyvatel se přesune sem.

Překryv a reverzibilita

Netvrdím, že zvolená metodika je jedinou cestou, ani že nejlepší. Zdá se ale ucelená — pokrývá hlavní páky a zachovává možnost couvnout. Nový systém se na začátku překrývá se starým a mění jen pobídky.

OBČANSTVÍ BEZ OBČANKY

od státního povolení ke komunitnímu uznání.

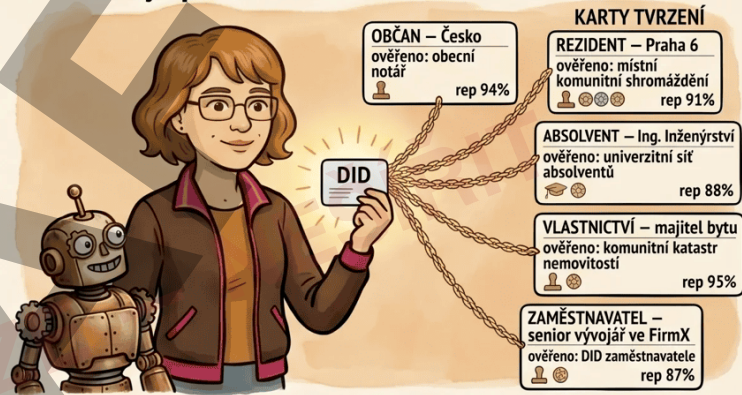
“starý způsob” institucionálního modelu státem vydávaných ID



identita = státní povolení – zrušitelné – komunita nemá slovo.



“nový způsob” modelu DID s kartami tvrzení



žádná jediná autorita nekontroluje všechna tvrzení – každé je nezávislé – každý ověřovatel riskuje svou reputaci.

“kdo sem patří?”



komunita rozhoduje – prostřednictvím reputačních signálů – distribuováno, žádný jediný hlas.

“to vypadá jako dnešní svět. To je pravda – jen ověřovatelů je nyní mnoho. Žádná revoluce. Jen lepší pobídky.”

Vaše občanství není vládním povolením. Je to uznání vaší komunity.
Státní razítko je nahrazeno řetězcem nezávislých ověřovatelů – z nichž každý má v sázce vlastní kůži.

Postupem času se starý zmenšuje, až se může — ale nemusí — rozpustit. Výhodou je postupnost a reverzibilita: kdyby se v návrhu objevila chyba, není to konec, jen oprava.

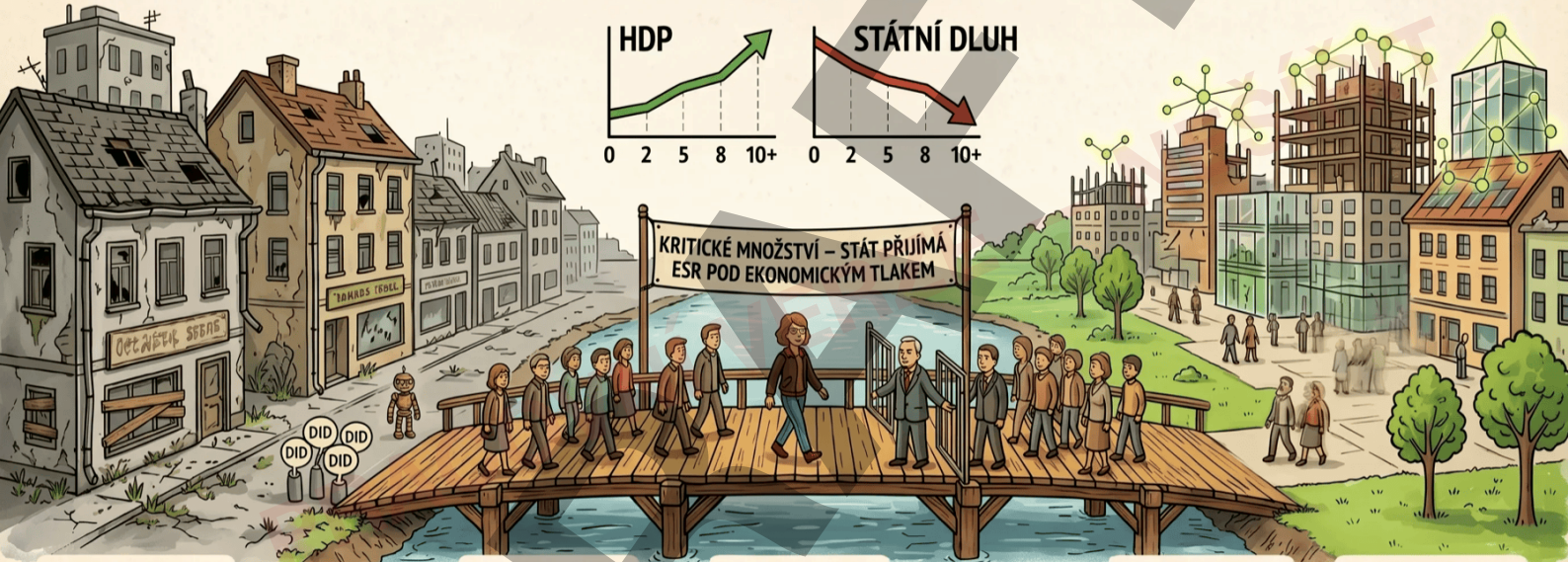
■ Mír a válka

Některé části státu nemusejí mít plně tržní alternativu — třeba armáda. Dočasné delegování mimořádných pravomocí v krizích (jako staří Řekové jmenovali diktátory) by mohlo dál existovat. Odpovědnost ale leží na decentralizované společnosti, ne na samotném vůdci. Na rozdíl od centralizovaného řízení bude jednodušší si předané pravomoci vzít zpátky, jakmile hrozba pomine — nebo dřív, když to bude potřeba. Svobodná společnost nebude mít ani ve vzájemném klání zbraní nevýhodu proti autoritativním zřízením.

■ Váleční zločinci

S just-in-time financováním státu a transparentními výdaji se obtížně hromadí zdroje na agresivní války. Daňový poplatník, který takovou válku dál financuje, se stává legitimním cílem a nemůže se dovolávat civilního statusu podle Ženevských úmluv. V novém uspořádání je tichý souhlas bráný jako participace.

EVOLUCE – NE REVOLUCE



Bod 1 – ROK 0

95%

STARÝ SYSTÉM

5%

Spuštění.
První uživatelé.
Vznikají pořadníky.

Bod 2 – ROK 2

80%

20%

Roste.
Seznam účastníků
se rozšiřuje.

Bod 3 – ROK 5

50%

50%

NOVÝ SYSTÉM

REVERSE

ZPĚTNÝ CHOD

Chyba v návrhu?
Můžeme se vrátit.
Vratnost zachována.

Bod 4 – ROK 8

25%

75%

75% nový systém –
Stát je jen podmnožinou.
Překryv zachován.

Bod 5 – ROK 10+

5%

95%

Starý systém je malou
podmnožinou nového.
Vratnost neporušena.

Postupný přechod. Vratnost v případě chyby. Směr, který nelze zastavit.

7. Závěr

Cesta existuje

Stát je takový, jaký je, kvůli technologiím dostupným v době jeho vzniku v kombinaci s lidskou přirozeností. Stavět všechno na dobrovolnosti a přitom popírat průměrnou lidskou přirozenost je naivní. Nezabývá se korupce, nezabývá se tendence směřovat k totalitarismu. Nástupce státu musí fungovat i s vlastnostmi lidí, které dnes považujeme za negativní a ostrakizujeme je, nebo trestáme.

Tato kniha popsala problém — systém (stát), kde lidé, kteří píšou pravidla, nikdy nežijí s jejich důsledky. Popsala podmínky, které musí platit, aby tenhle systém přestal fungovat. Popsala nástroj, který je splňuje. A navrhla metodologii přechodu — konkrétní kroky, jak ten nástroj použít jako možný příklad.

V první kapitole jsem zmínil pět pilířů: dobrovolnost, organizaci, odolnost, konsenzus a nezkorumpovatelnost. Splnili jsme je všechny.

- **Dobrovolnost** — nikdo vás do sítě nenutí, ale své činy si z ní neumažete.
- **Organizace** — komunita roste z toho, koho znáte, ne z toho, koho vám určili shora.
- **Odolnost** — vypnout to neumí ani stát ochotný platit za sledování každého paketu.
- **Konsenzus** — vzniká cenovým tlakem na pokrytectví, ne hlasováním ani podpisem.
- **Nezkorumpovatelnost** — pět drobných pravidel zaplétá korupci do nákladů: rovnováha dobrovolnosti a odpovědnosti, právo kohokoli promluvit, vstupní body, které si nikdo nevybírá, veřejné sliby s cenou za pokrytectví, a stín pozorovatele za každou transakcí.

Žádný pilíř sám stát nenahradí. Dohromady tvoří odolnost vůči korupci, kterou stát se vším svým aparátem nedokáže.

Jsme v bodě, kdy to celé umíme postavit se současnými technologiemi (kryptografie, decentralizovaná identita, známé psychologické pochody, aby se správně nastavily incentive,...). Chybí jediná věc: kritická masa lidí, kteří najdou odvahu pro podporu a rozhodnou se začít.

Ne revolucí.

Tyto myšlenky vznikaly mezi červnem 2025 a květnem 2026. Když jsem si sedl k psaní, měl jsem rámec v hlavě už z velké části hotový — právě proto jsem si s takovou zvědavostí přečetl [Farewell To Westphalia](#), když vyšlo. Chtěl jsem vidět, kde se jejich obrázek bude s mým překrývat a kde se rozejde. Druhý popostrk přišel od Dana Steigerwalda, který v květnu 2026 stále ještě pracuje na vlastní knize Dekonstrukce státu z jiného úhlu; jeho projekt mě dotlačil k tomu, abych vlastní vizi sepsal v plné šíři — aby ji svět měl na stole vedle ostatních.

Nežádám vás, abyste tomu věřili. Žádám vás, abyste o tom přemýšleli. A kladu vám jednu otázku:
Co byste změnili vy?

Pavel Kudrna 23. 5. 2026, Praha, Česko

VEMTE SI ZPĚT SVŮJ ČAS

občané vyhánějí parazity z veřejného života.



Braňte čas, který by ukradli. to, co bylo vzato podvodem, je vzato zpět rukou.

Podpořte projekt

Personix je financován čtenáři, jako jste vy.



Bitcoin on-chain

bc1q7cctdz6r026dgy06ul94eygg49ujtxnrq5czaj



Bitcoin Lightning

LNURL1DP68GURN8GHJ7AMPD3KX2AR0VEEKZ
AR0WD5XJTNRDAKJ7TNHV4KXCCTTDEHHM30
D3H82UNVWQHXMNP0FA8JMTDVD5XJMN9XUE
RX55QRQK

Kam tyto peníze jdou — a kam ne

QR kódy jsou **osobní kanály autora** — příspěvky jdou přímo Pavlu Kudrnovi a financují další psaní, sociální experiment / simulaci a osvětu.

Jediné legitimní cesty pro podporu tohoto projektu jsou:

- **Autorská vydání této knihy** — QR kódy ve výtiscích autorizovaných autorem.
- personix.org nebo Tor onion mirror odkazovaný odtamtud — kde *Nadace Personix* sbírá prostředky na činnosti tam popsané. Prostředky nadace jsou oddělené od osobních prostředků autora.

Cokoliv inzerované jinde — podvržené adresy v reprintech, podobné domény, sociální sítě „vybírající pro Personix“, sbírky nenavázané na žádnou z výše uvedených cest — **je nejspíš podvod**. Záměrně se vyhýbáme kryptotruhu a jeho účastníkům.

Rejstřík pojmů

Pojem	Anglicky	Význam
Alokace daní	Tax Allocation	Mechanismus, kterým daňový poplatník rozhoduje, kam putuje část jeho daní. Alokovatelné procento rok od roku roste.
Autorita	Authority	Důvěryhodná entita (osoba, organizace), která ověřuje informace a vsází na ně svou reputaci. Může být specializovaná (investativní, právní, technická).

Pojem	Anglicky	Význam
Compartmentalizace	Compartmentalization	Obecně: oddělení informací do izolovaných celků tak, aby prozrazení jednoho celku neohrozilo ostatní. Princip známý ze zpravodajských služeb. Zde: paralelní DID identity v diktaturách — kompromitace jedné z nich ostatní neodhalí.
DID	Decentralized Identity	Digitální identita, kterou si vytváříte a kontrolujete sami, bez centrální autority. Kryptograficky podepsaná vašim soukromým klíčem — nikdo vám ji nemůže odebrat ani zfalšovat.

Pojem	Anglicky	Význam
DID dokument	DID Document	Veřejně dostupný datový soubor popisující vaši DID identitu — obsahuje veřejné klíče, síťové adresy a metadata. Slouží k ověření vaší totožnosti v síti.
Due diligence	Due Diligence	Obecně: hloubková prověrka protistrany před vstupem do obchodního nebo právního vztahu — ověření její historie, financí, reputace a rizik. Zde: v reputační síti probíhá rychleji a automatictěji díky dostupnosti ověřených záznamů.
Emergentní	Emergent	Samovolně vznikající z interakcí jednodušších částí, aniž by to někdo navrhl nebo řídil. Hejno ptáků létá v útvaru bez plánu — útvar emerguje z jednoduchých pravidel, kterými se řídí každý jedinec.

Pojem	Anglicky	Význam
Emergentní společenská smlouva	Emergent Social Contract	Pravidla chování, která nevznikají shora (zákon), ale zdola — z opakovaných interakcí a konsenzu v komunitě.
ESR	Electronic Spending Register	Navrhovaný systém transparentního sledování veřejných výdajů — každý realizovaný výdaj státu se páruje s plánovanou platbou. Inspirováno českou EET, ale obrácenou proti státu.

Pojem	Anglicky	Význam
Fenomenologický	Phenomenological	Obecně: přístup zkoumající jevy tak, jak se ukazují v přímé zkušenosti, pozorováním toho, co z nich vyplývá, bez předem daných teorií. Zde: svoboda, společenská smlouva a normy chování jsou pozorované jevy — důsledky tisíců mikrointerakcí mezi lidmi, ne principy definované shora.
Hash	Hash (otisk)	Obecně: jednosměrná matematická funkce, která z libovolného vstupu vytvoří unikátní „otisk“ pevné délky — jako otisk prstu dokumentu. Ze stejného vstupu vždy vznikne stejný výstup, ale z výstupu nelze zpětně odvodit vstup. Zde: slouží k určení pozice na hash ringu a k ověřování integrity dokumentů.

Pojem	Anglicky	Význam
Hash ring	Consistent Hash Ring	Algoritmický mechanismus výběru ověřovatelů — pozici na kruhu určuje hash DID dokumentu v sociálním grafu. Zajišťuje nedeterministický, ale ověřitelný výběr.
Just-in-time financování	Just-in-Time Funding	Financování státu podmíněné transparentností — peníze tečou, až když stát přijme ESR a spáruje výdaje. Páka k vynucení spolupráce.

Pojem	Anglicky	Význam
Meritokracie	Meritocracy	Obecně: systém, kde o postavení rozhodují skutečné zásluhy a prokázané schopnosti, ne formální tituly, konexe nebo zděděná privilegia. Zde: reputační síť přirozeně upřednostňuje ty, kdo prokazatelně přispívají komunitě — jejich hlas má větší váhu díky track recordu, ne díky funkci.
Onion gateway	Onion Gateway	Síťová adresa DID identity v onion síti. Oddělená od DID dokumentu — lze ji změnit bez ztráty identity (podobně jako změna IP adresy u domény).

Pojem	Anglicky	Význam
Onion routing	Onion Routing (Tor)	Komunikační protokol zajišťující necenzurovatelnost sítě. Zprávy se šifrují ve vrstvách — každý uzel odstraní jednu vrstvu, ale nezná celou cestu.
Oracle problém	Oracle Problem	Obecně: jak zajistit, aby data vstupující do digitálního systému věrně odpovídala tomu, co se skutečně stalo ve fyzickém světě. Pojem pochází z oblasti blockchainů. Zde: řeší se přes autority, které do ověření vkládají svou reputaci jako záruku, že digitální záznam odpovídá fyzické skutečnosti.
Ověřovatel	Verifier	Účastník algoritmicky vybraný k ověření a zveřejnění záznamu. Sází své dobré jméno na pravdivost informace.

Pojem	Anglicky	Význam
Policy (politika)	Policy	Obečně: soubor pravidel nebo zásad určujících chování v určitém kontextu. Zde: každý účastník DID sítě deklaruje svou politiku — jak reaguje na konkrétní chování ostatních, jaká pravidla dodržuje a jaké tresty považuje za přiměřené. Souhrn politik tvoří emergentní společenskou smlouvu.
Princip ekonomické neutrality	Economic Neutrality Principle	Poctivé chování v síti se ekonomicky blíží nule — náklady na publikaci se vracejí jako odměny za ověřování. Nepoctivé chování je čistá ztráta.

Pojem	Anglicky	Význam
Proxy	Proxy	Obecně: zástupce nebo zprostředkovatel — systém nebo subjekt jednající jménem jiného. Zde se používá ve dvou kontextech: (1) ESR jako proxy párující veřejné výdaje s plánovanými platbami; (2) pozorovatelé jako proxy mezi vydavatelem a ověřovatelem v triku s pozorovateli.
Reputační signál	Reputation Signal	Jednotlivý záznam v síti — pozitivní (náprava škody, splnění závazku) nebo negativní (křivda, porušení smlouvy). Kumulativně tvoří reputační profil.

Pojem	Anglicky	Význam
Reputační síť	Reputation-Based Social Network (RSN)	Decentralizovaná sociální síť, kde si účastníci vyměňují zpětnou vazbu o chování v reálném světě. Záznamy jsou nákladné na vytvoření, levné na čtení.
Sociální graf	Social Graph	Síť vašich kontaktů a kontaktů vašich kontaktů. Algoritmus hledá ověřovatele v konfigurovatelné hloubce (například 3 úrovně). Žádný globální blockchain — síť přirozeně vytváří komunity s přesahy.

Pojem	Anglicky	Význam
Track record	Track Record	Obecně: historie dosavadních výsledků, úspěchů i neúspěchů osoby nebo organizace. Zde: souhrn všech dosavadních interakcí dané DID identity v síti — ověřených tvrzení, přijatých i odmítnutých záznamů — z něhož se její reputace odvozuje.
Tvrzení	Claim	Obecně: jakýkoli ověřitelný výrok. Zde: záznam publikovaný do reputační sítě — tvrzení o události, vlastnosti nebo vztahu, kryptograficky podepsané a ověřené. Např. „jsem rezident obce X“ nebo „tato osoba porušila smlouvu“.
Vydavatel	Publisher	Účastník sítě, který vytváří a publikuje záznam (tvrzení o křivdě, nápravě a podobně). Nese náklady na publikaci.

Produkční poznámky

Autorem vyhrazeno (nepodléhá licenci CC BY-SA): název a wordmark Personix, obálka knihy a kanály pro podporu (QR kódy, adresy, kontaktní e-mail). Odvozené edice musí tyto prvky odstranit nebo nahradit; použít je lze pouze k odkazu na toto původní dílo.

Zdrojové soubory. Kompletní zdroj — markdown text, infografiky, build skripty — je k dispozici spolu s tímto PDF.

Nástroje. Při přípravě textu a iteracích nad formulacemi využíval autor asistenci nástrojů umělé inteligence; infografiky byly navrženy ve spolupráci s generativními nástroji na základě autorských specifikací. Veškeré myšlenky, argumenty a závěry jsou autorovy vlastní.

PERSONIX

Nekompromisní změna

Necenzurovatelná a nezkorumpovatelná decentralizovaná reputační síť

Stát fungoval, když komunikace byla pomalá, rozhodnutí lokální a autorita žila ve stejném městě, kterému vládla. Dnešní síť obrací všechny tři předpoklady — a instituce na nich postavené už nesedí do světa, který spravují. Tato kniha popisuje nástroj, který sedí: decentralizovanou reputační síť, ve které je identita vaše, pravda veřejně auditovatelná a podplacení znamená reputační sebevraždu.

Není to manifest. Není to předpověď. Je to funkční plán toho, jak lze nástupce státu postavit — dobrovolně, jednu deklaraci po druhé.

Pavel Kudrna • Praha, 2026

personix.org

Licencováno pod Creative Commons Uvedte původ-Zachovejte licenci 4.0 Mezinárodní (CC BY-SA 4.0).