

Decentralizovaná reputačná sieť: Rámec pre prirodzenú organizáciu spoločnosti

Pavel Kudrna
Prague, Czechia
Draft v1 — March 2026

Abstract

Zmysel pre spravodlivosť—presvedčenie, že krivdy sú napravené a zásluhy odmenené—je najsilnejšou súdržnou silou spoločnosti. Keď centralizované inštitúcie správy nedokážu tento zmysel poskytnúť, pretože náklady na vymáhanie práva prevyšujú hodnotu samotného práva, spoločenská súdržnosť sa rozpadá. Súčasné inštitucionálne štruktúry zlyhávajú pri riešení významnej triedy sporov systematicky rovnakým spôsobom, akým centrálné plánovanie zlyháva pri alokácii zdrojov: prostredníctvom informačnej asymetrie, chýbajúcich spätnoväzbových slučiek a odpojenia rozhodovateľov od dôsledkov ich rozhodnutí. Tento článok predstavuje Reputačnú sociálnu sieť (RSN): decentralizovanú, neskorumpovateľnú, voči cenzúre odolnú komunikačnú vrstvu postavenú na decentralizovaných identifikátoroch (DID), ktorá umožňuje pseudonymným účastníkom publikovať, overovať a konzumovať reputačné informácie o správaní v reálnom svete. Základný mechanizmus spočíva na troch návrhových princípoch: (1) asymetrická nákladová štruktúra, kde čítanie reputačných dát je lacné, ale zápis vyžaduje overiteľné úsilie; (2) nedeterministický protokol výberu overovateľa založený na konzistentnom hashovaní, ktorý oceňuje radikálne tvrdenia prostredníctvom eskalujúcich nákladov iterácií; a (3) trhovo riadený model reputačnej autority, kde súkromní overovatelia stavajú svoju nahromadenú reputáciu na presnosť tvrdení, ktoré potvrdzujú. Výsledná architektúra produkuje emergentnú meritokraciu bez centrálnej koordinácie a umožňuje postupnú, zvrtnú migračnú cestu z existujúcich štátom spravovaných systémov.

1 Úvod

1.1 Problém centralizovanej dôvery

Moderná správa spoločnosti spočíva na základnom predpoklade: že centralizované inštitúcie dokážu

sprostredkovať dôveru medzi neznámymi ľuďmi vo veľkom rozsahu. Súdny rozhodujú spory. Registre potvrdzujú vlastníctvo. Regulačné orgány vymáhajú štandardy. Tieto inštitúcie boli navrhnuté v čase, keď informácie boli vzácne, komunikácia bola pomalá a delegovanie autority na centrálny orgán bolo jediným uskutočniteľným koordinačným mechanizmom. Centralizovaná správa však zlyháva z rovnakých štrukturálnych dôvodov ako centrálné plánovanie: informačná asymetria, chýbajúce spätnoväzbové slučky a odpojenie rozhodovateľov od dôsledkov ich rozhodnutí.

Tento predpoklad zlyháva napríklad vtedy, keď náklady na inštitucionálne sprostredkovanie prevýšia hodnotu sporu. Uvažujme o nájomníkovi, ktorý zistí, že jeho prenajatý byt nemá zákonom vyžadovaný certifikát o elektrickej bezpečnosti—stav, ktorý predstavuje bezprostredné ohrozenie života. Zákonné právo nájomníka odstúpiť od zmluvy je jednoznačné. Náklady na vymáhanie tohto práva prostredníctvom súdneho systému však prevyšujú peňažnú hodnotu zálohy a dlžnej náhrady škody, dokonca aj vrátane možného zákonného odškodnenia [1]. Racionálnou reakciou je stratu vstrebať a odísť.

Nejde o patologický okrajový prípad. Je to štandardná skúsenosť pre významnú triedu sporov, v ktorých je ujma reálna, ale peňažná výška klesá pod prah, pri ktorom sa inštitucionálne vymáhanie stáva ekonomicky racionálnym. Výsledkom je systém, ktorý štrukturálne zvýhodňuje zlých aktérov: tí, ktorí poškodzujú druhých v objemoch pod týmto prahom, môžu konať bezrestne, pretože náklady na dosiahnutie spravodlivosti nesie poškodená strana.

Vyššie uvedený príklad je čerpaný z autorovho právneho prostredia—českého systému občianskeho práva. V iných právnych tradíciách—precedenčnom obyčajovom práve (common law), zvykovom práve, zmiešaných systémoch—spravodlivosť zlyháva odlišnými spôsobmi a v rôznej miere, v závislosti od kultúrnych a procesných špecifik danej jurisdikcie. Čitatelia pravdepodobne rozpoznajú ekvivalentné

príklady zo svojho vlastného kontextu. Štrukturálne univerzálny je vzorec: spory, ktorých hodnota klesá pod prah ekonomicky racionálneho vymáhania, končia tým, že stratu vstrebe poškodená strana. RSN nesľubuje dokonalú spravodlivosť—iba znižuje štrukturálnu výhodu, ktorú zlí aktéri požívajú, keď je inštitucionálne vymáhanie neekonomické.

1.2 Prečo existujúce riešenia nestačia

Rámce decentralizovanej identity (DID) [2] poskytujú kryptografické mechanizmy pre správu suverénnej identity (self-sovereign identity), ale zameriavajú sa predovšetkým na overovanie identity bez riešenia širšej otázky reputácie správania.

Soulbound tokens (SBT) [3] zachytávajú poznatok, že reputácia je neprenosná, ale spoliehajú sa na blockchainovú infraštruktúru s obmedzeniami škálovateľnosti a neriešia ekonomické stimuly upravujúce vkladanie informácií. Súvisiace koncepty ako zásluhové tokeny (napr. Liberland) zdieľajú podobnú filozofiu, no zostávajú viazané na konkrétne juridické rámce.

Decentralizované autonómne organizácie (DAO) [4] implementujú správu prostredníctvom smart kontraktov, ale replikujú plutokratickú dynamiku, kde je vplyv úmerný kapitálu. Kvadratické hlasovanie [5] to čiastočne zmierňuje, ale obmedzuje praktické prijatie. DAO tiež čelia zásadnému *problému orákula*: smart kontrakty nedokážu spoľahlivo overiť stavy reálneho sveta bez dôveryhodného externého zdroja a tento problém nemá v rámci blockchainovej architektúry všeobecné riešenie.

Žiadny existujúci systém nekombinuje decentralizáciu, odolnosť voči cenzúre, pseudonymitu, overiteľné náklady na vstup a emergentný konsenzus.

1.3 Prínosy

Tento článok prináša nasledujúce prínosy:

1. Definíciu **Reputačnej sociálnej siete (RSN)**, decentralizovaného protokolu rozširujúceho rámec DID o podporu obojstrannej výmeny reputácie.
2. **Nedeterministický protokol výberu overovateľa** založený na konzistentnom hashovaní [6].
3. **Princíp drahého radikalizmu**, ktorý oceňuje tvrdenia podľa ich vzdialenosti od sieťového konsenzu prostredníctvom troch kumulujúcich sa nákladových kanálov.
4. Model **reputovanej autority** s asymetrickými stimulmi, kde falošné potvrdenie stojí katas-

trofálne viac než legitímne poplatky.

5. **Postupnú migračnú cestu** prostredníctvom paralelnej fiškálnej infraštruktúry.

2 Návrhové princípy

Architektúra RSN je obmedzená piatimi nespochybniteľnými návrhovými princípmi.

Kontinuita a evolúcia. Systém koexistuje s existujúcimi inštitúciami počas prechodného obdobia určitej dĺžky. Prechod musí byť v každej fáze zvrtný.

Dobrovoľnosť a zodpovednosť. Účasť je dobrovoľná, ale dobrovoľnosť je spojená so zodpovednosťou: účastník, ktorý preberá kontrolu nad inštitucionálnou funkciou, súčasne preberá aj sprievodné povinnosti.

Rozmanitosť a kultúrna neutralita. Konsenzus vzniká z obojstranných interakcií, nie z vopred stanovených pravidiel vnútených návrhármí systému.

Odolnosť a odolnosť voči cenzúre. Náklady na cenzurovanie siete musia prevýšiť náklady na jej tolerovanie. Iba úplný totalitarizmus—za rujnujúcich politických a ekonomických nákladov—dokáže systém potlačiť.

Konsenzus a vymáhanie. Systém zahŕňa ľudské sklony k malichernosti, zlomyseľnosti a odplatnému zadostučineniu ako nosné prvky. Pochybenie nie je zakázané; je ocenené.

3 Prehľad systému

3.1 Reputačná sociálna sieť

RSN je decentralizovaná, peer-to-peer komunikačná vrstva, v ktorej si účastníci vymieňajú overiteľné informácie o správaní v reálnom svete. Jej definujúcimi vlastnosťami sú: decentralizovaná a necenzurovateľná infraštruktúra; pseudonymná účasť prostredníctvom DID; asymetrická nákladová štruktúra (čítanie je lacné, zápis je drahý); kryptografická overiteľnosť; a **podpora štandardov**—strojovo čitateľné formáty pre informácie šírené sieťou, pre služby ponúkané autoritami (skladanie tvrdení, potvrdzovanie, svedecká služba) a pre formát politiky vrátane pravidiel na hodnotenie reputácie protistrany a posudzovanie rizika nesúladu politiky (medzi deklarovaným a skutočným správaním).

3.2 Architektonické komponenty

RSN pozostáva zo štyroch primárnych komponentov (Obr. 1):

1. **Vrstva DID.** Identity účastníkov s deklarovanými pravidlami, reputačnými metadátami a sieťovým smerovaním.
2. **Protokol tvrdení.** Štruktúrovaný formát na publikovanie výrokov o udalostiach v reálnom svete.
3. **Overovacia sieť.** Decentralizovaný protokol na pridelovanie overovateľov pomocou konzistentného hashovania.
4. **Vrstva agregácie reputácie.** Služby, ktoré produkujú ľudsky čitateľné súhrny reputácie.

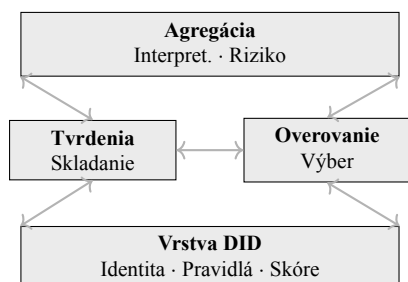


Figure 1: Štvorvrstvá architektúra RSN.

3.3 Roly účastníkov

Overovacia transakcia zahŕňa až šesť odlišných rolí DID (Obr. 2): **Vydavateľ** (DID_I , vytvára a odosiela tvrdenie), **Subjekt** (DID_S , DID, o ktorom tvrdenie je—môže sa zhodovať s vydavateľom), **Autorita** (DID_A , potvrdzuje tvrdenie za poplatok; môže tiež ponúkať svedecké služby—*voliteľné*), **Svedok** ($DID_{W_{1..n}}$, inkognito monitor čestnosti overovateľa prostredníctvom výzvoch kódov—*voliteľné*), **Overovateľ** (DID_V , algoritmicke vybraný na publikovanie tvrdenia) a **RSN** (sieť, kde sa overené tvrdenia publikujú). Ktorákoľvek rola môže byť delegovaná na iný DID (kapitola 7.4). Autorita bežne zväzuje potvrdzovanie so svedeckými službami, ale obe funkcie sú logicky nezávislé.

3.4 Neskorumpovateľnosť: štyri sily

Neskorumpovateľnosť RSN nevychádza z jediného mechanizmu, ale zo štyroch súčasne pôsobiach síl. Žiadna sama osebe nepostačuje; iba ich kombinácia robí pokus o korupciu ekonomicky iracionálnym.

Nepredvídateľný cieľ. Overovateľ pre každé tvrdenie je vybraný nedeterministicky prostredníctvom konzistentného hashovania (kapitola 5.3). Útočník nemôže vopred zacieliť konkrétneho overovateľa na

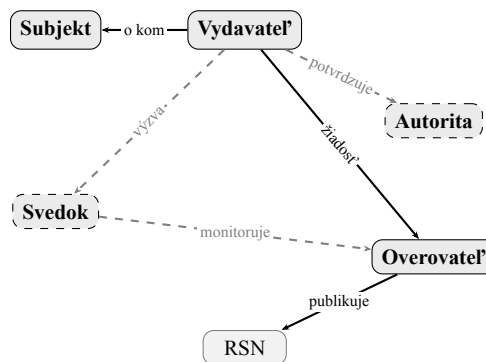


Figure 2: Roly DID v overovacej transakcii. Prerušovane = voliteľné (Autorita, Svedok).

úplatok, pretože identita overovateľa je funkciou obsahu tvrdenia a predchádzajúcich iterácií, nie voľby vydavateľa.

Reputačná páka—pomaly hore, rýchlo dole. Reputáciu možno získať iba postupne, prostredníctvom trvalého konzistentného správania. Možno ju však stratiť katastrofálne jediným podvodným potvrdením (kapitola 6.2). Táto asymetria znamená, že roky nahromadenej reputácie môžu byť zničené jediným nečestným potvrdením; optimálnou stratégiou zostáva odmietat' podozrivé tvrdenia.

Verejný sľub. Každý držiteľ DID verejne deklaruje svoju politiku—strojovo čitateľnú sadu pravidiel, ktoré sa zaväzuje dodržiavať. Odchýlka medzi deklaráciou a skutočným správaním je zistiteľná a ocenená ako reputačný priestupok závažnejší než samotné porušenie (kapitola 7.3). Pokrytectvo je preto nákladnejšie než priama nečestnosť.

Asymetria nákladov na útok voči sieti (mesh). Náklady na cenzurovanie alebo destabilizáciu siete rastú nelineárne s veľkosťou a hustotou siete, zatiaľ čo náklady na jej tolerovanie zostávajú konštantné. Aby sa cenzúra vyplatila, centralizovaný aktér by ju musel aplikovať naprieč celou sieťou—čo si vyžaduje opatrenia neúmerné akémukoľvek predstaviteľnému prospechu (kapitola 10).

4 Model decentralizovanej identity

4.1 DID so špeciálnymi vlastnosťami

RSN rozširuje špecifikáciu W3C DID Core [2] o: **deklarované pravidlá** (strojovo čitateľné záväzky týkajúce sa správania), **reputačné metadáta** (agregované skóre správania) a **sieťové smerovanie** (meniteľná onion brána oddelená od stabilnej pozície na kruhu).

4.2 Životný cyklus tvrdenia

Tvrdenie prechádza šiestimi fázami (Obr. 3): skladanie, voliteľné potvrdenie autoritou, výber overovateľa cez konzistentné hashovanie, rozhodnutie o overení (prijatie alebo odmietnutie s iteráciou), publikovanie a aktualizácia reputácie pre všetky strany.

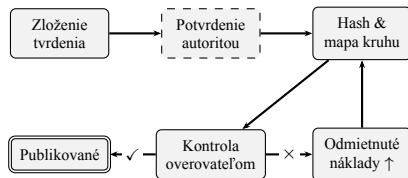


Figure 3: Životný cyklus tvrdenia s iteračnou slučkou.

4.3 Vzťah k W3C DID Core

Model identity RSN je vlastnou nadmnožinou špecifikácie W3C DID Core [2]. Všetky DID v RSN sú platné W3C DID. Rozšírenia špecifické pre RSN sú zakódované ako vlastnosti DID dokumentu definované vo vyhradenej špecifikácii DID metódy, kompatibilné s existujúcou infraštruktúrou ako ION [7] a Ceramic [8].

5 Overovanie a šírenie informácií

5.1 Náklady na vstup informácie

Základným ekonomickým princípom RSN je asymetria medzi čítaním a zápisom. Čítanie reputačných dát sa blíži nulovým marginálnym nákladom pre účastníkov, ktorí sú súčasťou siete DID a majú prístup zodpovedajúci ich reputácii—nováčikovia si musia postupne zaslúžiť širší prístup (pozri ochranu proti parazitovaniu). Zápis—chápaný ako trvalá materializácia reputácie do siete, nie ako jednorazový technický úkon—vyžaduje overiteľnú kumulatívnu investíciu v troch dimenziách: **čas** (roky života strávené konzistentným správaním, splnenými záväzkami a pestovanými vzťahmi), **energia** (úsilie vložené do čestného jednania, starostlivosti o partnerstvá a dlhodobej dôveryhodnosti) a **peniaze** (investícia do vlastného mena—profesijný rozvoj, kvalita vlastnej práce, náhrada spôsobených škôd). Reputáciu nemožno kúpiť okamžite—je výsledkom celoživotného hromadenia, ktoré systém iba sprístupňuje a robí prenosným naprieč kontextmi. Jednorazové technické náklady protokolu (kryptografické podpisy, poplatky overovateľom) sú zanedbateľné v porovnaní s touto základnou investíciou.

5.2 Sociálny graf a hĺbka kontaktov

RSN je v podstate sociálna sieť: každý DID pridáva kontakty (iné DID), ktoré spojenie povolia. Tieto kontakty majú svoje vlastné kontakty a tak ďalej. Algoritmické vyhľadávanie overovateľa pôsobí v rámci konfigurovateľnej hĺbky h prepojených kontaktov (napr. $h = 3$: priame kontakty, ich kontakty a kontakty kontaktov). Táto architektúra nevyžaduje jediný globálny blockchain—prirodzene uprednostňuje vznik komunit/klastrov s prekryvmi do iných komunit. Každý účastník s DID musí mať publikovanú **politiku**—strojovo čitateľnú sadu pravidiel upravujúcich, ako sa vyhodnocujú prichádzajúce žiadosti. Porušenia politiky sú v sieti zaznamenané ako negatívne artefakty.

5.3 Algoritmický výber overovateľa

Overovací protokol využíva konzistentné hashovanie [6] (Obr. 4). Overovanie je platená služba: overovatelia pracujú za poplatok, čím vzniká trh, kde konkurencia poháňa cenu, rýchlosť a spoľahlivosť.

Krok 1. Dokument tvrdenia sa zretáží s výsledkom hashu predchádzajúcej iterácie (alebo $\emptyset$ pri prvej iterácii) a zahashuje:

$$\text{pos} = f_h(\text{claim} \parallel \text{prev_hash}) \quad (1)$$

Algoritmus musí zahŕňať *úplnú cestu* všetkých predchádzajúcich žiadostí a odpovedí—nie iba hash predchádzajúcej iterácie. Úplná odpoveď každého overovateľa (prijatie, odmietnutie, uvedená cena, dôvod) sa pripája k rastúcemu dokumentu, overiteľná prostredníctvom kryptografických podpisov v každom kroku.

Krok 2. Hash sa namapuje na N pozícií na kruhu konzistentného hashu, rovnomerne rozložených (napr. pre $N = 4$: $+0^\circ$, $+90^\circ$, $+180^\circ$, $+270^\circ$). Z každej pozície vyhľadávanie v smere hodinových ručičiek vyberie najbližší DID ako kandidáta na overovateľa (Obr. 5). N je premenlivý parameter, ktorý môže závisieť od percenta aktuálne aktívnych DID, dennej doby alebo historickej odozvy siete.

Krok 3. Overovateľ prijme (publikuje a stavia reputáciu) alebo odmietne (návrat na krok 1 s hashom odmietnutia). Keď uzol neodpovedá napriek deklarovanému stavu online, ďalšia žiadosť musí obsahovať všetky odpovede od všetkých N predchádzajúcich kandidátov na overovateľa.

Ochrana proti parazitovaniu (anti-leeching). Cieľové DID môžu nastaviť poplatky alebo

obmedzenia prístupu pre dotazy od nových DID s malou reputáciou. Tento odstupňovaný mechanizmus (nie binárny) núti nováčikov budovať reputáciu prostredníctvom skutočnej aktivity predtým, než môžu voľne konzumovať dáta ostatných.

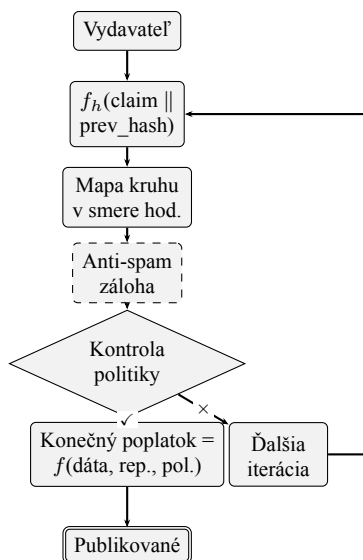


Figure 4: Protokol výberu overovateľa. Anti-spam záloha je voliteľná a môže byť vratná. Konečný poplatok sa platí iba pri prijatí.

Každé odmietnutie pripája úplnú odpoveď overovateľa (vrátane dôvodov a podmienok) k dokumentu tvrdenia, čím rozširuje jeho obsah. Z rozšíreného dokumentu sa nedeterministicky vypočíta nový hash, ktorý sa mapuje na inú pozíciu na kruhu a vyberá iného overovateľa. Zdokumentovanie úplnej cesty je povinné—vydavateľ nemôže predvídať ani ovplyvniť ďalšieho overovateľa. Ak overovateľ ignoruje žiadosť napriek kompatibilnej deklarovanej politike, svedkovia (ak sú prítomní) to zaznamenajú a vydavateľ môže pri konečnom publikovaní priložiť svedecké dôkazy.

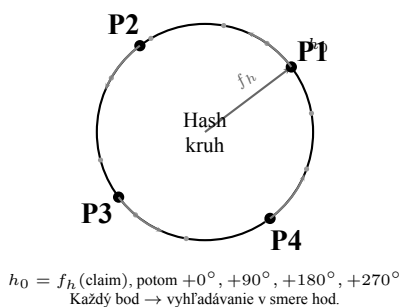


Figure 5: Viacbodový výber ($N=4$). Hash h_0 nastavuje posun; 4 body rovnomerne rozložené od h_0 .

5.4 Protokol svedka

Rola **Svedka** poskytuje inkognito zodpovednosť za česťnosť overovateľa prostredníctvom kryptografického protokolu výzvočných kódov:

Krok W1. Žiadateľ podpíše overovaciu žiadosť a odošle ju N_w svedkom—kontaktom zo žiadateľovej sociálnej siete alebo špecializovaným poskytovateľom svedeckých služieb pracujúcim za poplatok.

Krok W2. Každý svedok w_i podpíše celú podpísanú žiadosť, ponechá si pôvodný podpis σ_i a vypočíta výzvočný kód $c_i = h(\sigma_i)$. Výzvočný kód sa pripojí k žiadosti.

Krok W3. Žiadosť, ktorá teraz nesie N_w výzvočných kódov, sa odošle overovateľovi. Overovateľ kódy vidí, ale *nedokáže určiť*, kto sú svedkovia ani či kódy zodpovedajú skutočným podpisom.

Krok W4 (česťný overovateľ). Ak overovateľ odpovie podľa svojej deklarovanej politiky, výzvočné kódy zostanú nepriehľadné. Svedkovia nie sú nikdy odhalení. Nepublikujú sa žiadne ďalšie dáta.

Krok W5 (porušenie politiky). Ak overovateľ poruší svoju politiku (ignoruje žiadosť, odpovedá nekonzistentne), žiadateľ drží pôvodné podpisy svedkov σ_i . Tie možno publikovať ako sprievodné dáta: ktokoľvek môže overiť $c_i = h(\sigma_i)$, čím sa dokáže, že svedok bol prítomný. Žiadateľ môže publikovať nezávisle—overovateľ už výzvočné kódy vo svojej odpovedi podpísal.

Vlastnosť blafovania. Žiadateľ môže niektoré alebo všetky výzvočné kódy nahradiť náhodnými hodnotami. Overovateľ nedokáže odlíšiť pravé kódy (kryté vysoko reputovanými autoritami) od šumu. Táto *neistota* je vymáhacím mechanizmom: každá žiadosť nesie riziko, že nejaká rešpektovaná autorita prizera inkognito. Náklady na udržiavanie tohto tlaku sú takmer nulové (generovanie náhodných čísel), zatiaľ čo potenciálne náklady nečesťnosti pre overovateľa sú katastrofálne. Česťné správanie je stimulované aj bez skutočných svedkov.

Autorita ako svedok. Autorita, ktorá potvrdzuje tvrdenie, môže zväzať svedecké služby: „Potvrdzujem vaše tvrdenie a slúžim ako inkognito svedok počas overovania.“ Ide o prirodzený obchodný model—autorita už kontext má. Obe roly sú však logicky nezávislé.

5.5 Princíp drahého radikalizmu

Tri nákladové kanály sa kumulujú súčasne (Obr. 6):

Kanál 1: Náklady iterácie. Každé odmietnutie vynúti novú iteráciu spotrebúvajúcu čas a zdroje.

Lineárny rast.

Kanál 2: Nabobtnávanie dokumentu. Každá iterácia pridáva úplnú odpoveď overovateľa k dokumentu tvrdenia. Rast je lineárny, ale so základným posunom: počiatočný obsah (obsah tvrdenia, potvrdenie autoritou, kryptografické podpisy) už má netriviálnu veľkosť B_0 . Celková veľkosť po k iteráciách: $S(k) = B_0 + k \cdot \Delta$, kde Δ je priemerná veľkosť odpovede.

Kanál 3: Riziková prirážka overovateľa. Riziko je subjektívne. Overovateľ posudzuje, či deklarované politiky žiadajúceho DID kolidujú s vlastnými komerčnými, sociálnymi alebo politickými záujmami overovateľa. Prirážka môže exponenciálne eskalovať s vnímanou vzdialenosťou od „ideálu“ overovateľa: $P(d) = \alpha \cdot e^{\beta d}$, kde d je subjektívna metrika vzdialenosti overovateľa. Za hranicou osobného „no-go“ môže overovateľ úplne odmietnuť.

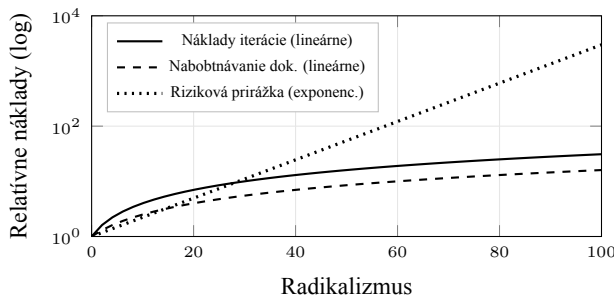


Figure 6: Eskalácia nákladov naprieč tromi kanálmi. Riziková prirážka dominuje pri vysokom radikalizme.

Kľúčové je, že toto nie je cenzúra. Žiadne tvrdenie nie je zakázané. Systém oceňuje riziko (Tab. 1).

Table 1: Porovnanie nákladov naprieč typmi tvrdení.

Typ	Iter.	Dok	Poplatok	Spolu
Dôveryhodné	$k_{\min}$	B_0	$P_{\min}$	Nízke
Kontroverzné	k_{med}	$B_0 + k\Delta$	$\alpha e^{\beta d}$	Stredné
Radikálne	$k_{\max}$	$\gg B_0$	$\gg P_{\min}$	Veľmi vysoké
Podvodné	$\rightarrow \infty$	—	—	Nepublikovateľné

6 Reputácia a hodnotenie rizika

6.1 Model hromadenia reputácie

Reputácia vykazuje tri vlastnosti: **pomalé hromadenie** (postupný rast prostredníctvom konzistentného správania), **rýchle zničenie** (jediný podvod môže katastrofálne znížiť skóre) a **individuálne hodnotenie** (každá konzumujúca strana môže uplatniť vlastnú agregáciu funkciu).

6.2 Reputované authority

Reputovaná autorita preskúma tvrdenia a ak je spokojná, spolupodpíše ich—stavajúc svoju vlastnú reputáciu (Obr. 7). Asymetria je zámerná: získavanie reputácie je pomalé (postupné $+\delta$ za každé čestné potvrdenie), zatiaľ čo jej strata je katastrofálna ($-\Delta \gg \delta$ za falošné potvrdenie; ilustratívne napr. $+2\%$ oproti -70%). Optimálnou stratégiou je vždy odmietat podozrivé tvrdenia. Konkrétne hodnoty δ a Δ sú systémové parametre.

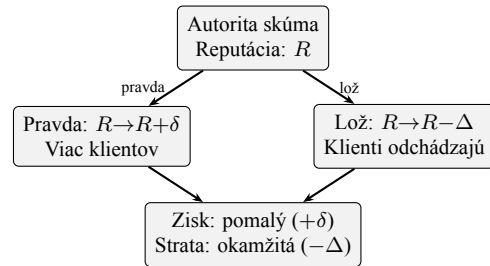


Figure 7: Reputovaná autorita—asymetrické stimuly.

6.3 Viacrozmerná reputácia

Reputácia nie je skalár, ale vektor naprieč viacerými dimenziami: finančná spoľahlivosť, osobná integrita, profesijná kompetentnosť, občianska angažovanosť a ďalšie (Obr. 8). Rôzni poskytovatelia hodnotenia premietajú tento vektor odlišne v závislosti od kontextu—veriteľ uprednostňuje finančnú spoľahlivosť, zamestnávateľ profesijnú kompetentnosť, sused občianske správanie. Neexistuje jediné „správne“ reputačné skóre; iba perspektívy.

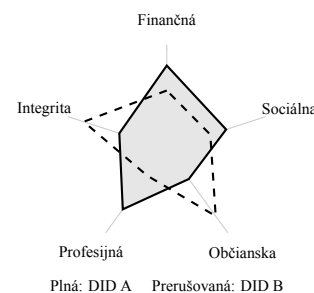


Figure 8: Viacrozmerné reputačné vektory. Rôzne DID vykazujú rôzne profily naprieč dimenziami.

6.4 Demokratizované hodnotenie rizika

RSN demokratizuje systematické hodnotenie rizika—schopnosť, ktorá je dnes sústredená vo finančných inštitúciách, ale použiteľná ďaleko za hranicami

bankovníctva. Priemyselné konglomeráty posudzujúce spoľahlivosť dodávateľov, poisťovne oceňujúce behaviorálne riziko, due diligence pri fúziách a akvizíciách, odhad životnosti zariadení vo výrobe—kdekoľvek si riziko protistrany vyžaduje posúdenie, RSN poskytuje decentralizovanú, trhovo riadenú alternatívu. Trh interpretačných služieb prekladá surové viacrozmerne reputačné dáta na použiteľné súhrny, čím sprístupňuje hodnotenie protistrany ktorémukoľvek účastníkovi za marginálne náklady.

7 Konsenzus a riešenie sporov

7.1 Model decentralizovanej spravodlivosti

RSN preformuluje spravodlivosť ako problém obojstranného vyjednávania. Hrozba trvalého, overiteľného poškodenia reputácie je účinnejším odstrašujúcim prostriedkom než súdne konanie, ktoré si poškodená strana nemôže dovoliť.

7.2 Emergentný konsenzus

Každý účastník si udržiava osobný prah zadosťučinenia. Agregovaný konsenzus siete vzniká ako štatistický priemer tisícov obojstranných vyjednávani (Obr. 9). Reakcia výrazne nad konsenzom (barbarská) je drahá na publikovanie. Reakcia blízka konsenzu (proporcionálna) je lacná. Konsenzus nie je pravidlo—je to cenový signál.

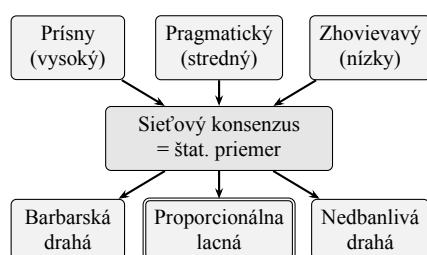


Figure 9: Emergentný konsenzus z individuálnych prahov zadosťučinenia.

7.3 Kalibrácia trestu

Každý držiteľ DID verejne deklaruje reakcie na konkrétne kategórie pochybenia. Neprimerane tvrdé alebo zhovievavé deklarácie priťahujú negatívne reputačné signály. Proporcionálne deklarácie sú prijímané bez trenia—samokalibračný trestný systém.

Deklarácie konsenzu samy podliehajú detekcii pokrytectva: deklaratívne zaviazat' sa ku konsenzuálnej pozícii a pritom sa správať nekonzistentne pred-

stavuje reputačný priestupok závažnejší než samotná odchýlka, keďže demonštruje úmyselné klamstvo.

7.4 Delegovanie

Všetky aktivity v rámci DID—s jednou výnimkou—môžu byť delegované na iný DID. **Rola subjektu—DID, o ktorého správaní tvrdenie je—nemôže byť delegovaná; je neprenosne viazaná na držiteľa identity, na ktorého sa tvrdenie vzťahuje.** Ostatné aktívne roly—Vydavateľ, Autorita, Svedok, Overovateľ—môžu byť prenesené na určený delegátsky DID, či už na overovanie, odosielanie tvrdení, účasť na konsenze alebo riešenie sporov. Delegovanie je kedykoľvek odvolateľné. To umožňuje špecializáciu (napr. profesionálne overovacie služby), pričom držiteľ si ponecháva konečnú kontrolu a zodpovednosť. Delegovanie sa uplatňuje naprieč celým systémom a je nevyhnutné pre škálovateľnosť.

7.5 Od individuálnej morálky k emergentnej spoločenskej zmluve

Deklarovaná politika každého DID predstavuje formalizáciu individuálnej morálky: čo držiteľ považuje za prijateľné, ako reaguje na konkrétne správanie, čo vyžaduje od protistrán. Tieto politiky nie sú vnútené návrhom systému—sú zvolené každým účastníkom a vyjadrené v strojovo čitateľnej forme.

Táto formalizácia umožňuje trojfázový vznik. Po prvé, individuálna morálka je zakódovaná ako **politika**—sada deklarovaných pravidiel, prahov a reakčných funkcií, ktoré sa DID zaväzuje dodržiavať. Po druhé, agregát všetkých politík naprieč sieťou produkuje **emergentnú etiku**—štatisticky pozorovateľné normy, ktoré nenavrhol žiadny jednotlivý účastník, ale ktoré vznikajú z interakcie tisícov individuálnych morálnych pozícií [9]. Po tretie, tieto emergentné etiky, vyjadrené ako zdieľané normy správania vymáhané prostredníctvom obojstranných cenových signálov, tvoria **merateľnú spoločenskú zmluvu**—nie teoretický konštrukt, ktorý nikto nepodpísal [10], ale empiricky pozorovateľnú sadu pravidiel krytú skutočným správaním.

Tento proces zrkadlí zistenia z teórie morálnych základov [11]: ľudská morálka je intuitívna, pluralistická a kultúrne premenlivá. RSN nevyžaduje morálny konsenzus ako vstup; produkuje behaviorálny konsenzus ako výstup. Výsledná spoločenská zmluva nie je statická—vyvíja sa, ako sa účastníci pripájajú, odchádzajú a upravujú svoje politiky v reakcii na spätnú väzbu siete. Na rozdiel od klasickej teórie

spoločenskej zmluvy je táto zmluva odvolateľná, pozorovateľná a vymáhateľná bez suveréna.

8 Ekonomický model

Predchádzajúce kapitoly opísali nástroj—overovacie mechanizmy RSN, nákladovú štruktúru a emergentný konsenzus. Táto kapitola opisuje metodiku uplatnenia tohto nástroja na fiškálny a správny prechod. Nástroj je univerzálny; nižšie uvedená metodika je jednou možnou aplikáciou.

8.1 Štruktúra stimulov

Reputácia ako kapitál vytvára priame stimuly pre čestné správanie. Za bežnej prevádzky si účastníci budujú reputáciu prirodzene prostredníctvom každodenných transakcií a splnených záväzkov. Primárny výdavok smeruje na *negatívne* tvrdenia—zaznamenávanie škody spôsobenej inými. Táto asymetria stimuluje užitočné, spoľahlivé správanie: byť čestný nestojí nič navyše, zatiaľ čo byť škodlivý vytvára zdokumentovanú stopu, ktorú budú iní ochotní zaplatiť za jej uchovanie. Pokrytectvo—deklarovanie pravidiel bez ich dodržiavania—je najdrahším režimom zlyhania, keďže demonštruje úmyselné klamstvo.

8.2 Paralelný fiškálny systém

Tri komponenty umožňujú konkurenčný tlak: (1) **jednoduchá daň**—jediná proporcionálna sadzba bez výnimiek, spočiatku marginálne pod existujúcou efektívnou sadzbou; (2) **elektronická registrácia výdavkov (ESR)**—obrátenie českého modelu EET tak, aby občania dohliadali na štátne výdavky; (3) **občanom riadené pridelovanie daní**—začínajúce na niekoľkých percentách v prvom roku a po desaťročí dosahujúce hocičo od nízkych dvojciferných hodnôt po úplnú migráciu na občanom riadený systém, v závislosti od miery prijatia. Skutočné tempo závisí od rýchlosti, akou vznikajú voľnotrhové alternatívy k štátnym službám, a od ochoty štátu spolupracovať na prechode; funkcia času nemusí byť lineárna a nie je dôvod stanovovať hornú hranicu toho, kam prijatie napokon môže dospieť.

9 Migračná cesta

Migrácia prebieha v troch fázach (Obr. 10): **Fáza 1: Prekryv** (RSN ako informačná vrstva, štát je jediným

poskytovateľom), **Fáza 2: Konkurencia** (RSN poskytuje funkčné alternatívy, súbežné používanie oboch systémov) a **Fáza 3: Prechod** (RSN prekonáva štátne ekvivalenty, dobrovoľná migrácia). Prechod je v každej fáze zvrtný.

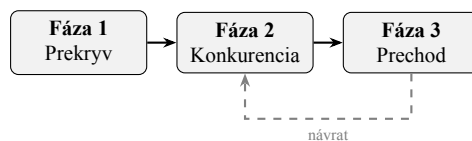


Figure 10: Trojfázová migrácia—zvrtná v každej fáze.

Primárnym tlakovým mechanizmom je fiškálny: keď podmienení daňoví poplatníci dosiahnu „ekonomicky významnú menšinu X “—skupinu dostatočne veľkú na to, aby represia voči nej spôsobila netriviálne ekonomické škody a občianska neposlušnosť sa stala vierohodnou hrozbou—štát vstupuje do vyjednávania. Na ilustráciu používame $X \approx 15\%$ HDP, ale skutočný prah závisí od konkrétnej ekonomiky.

10 Bezpečnostná analýza

Uvažujeme päť kategórií protivníkov: jednotliví zlí aktéri, organizované skupiny, korporátni protivníci, protivníci na úrovni štátu a protivníci na úrovni protokolu.

Odolnosť voči Sybil útoku [12]. Budovanie reputácie vyžaduje trvalú, overiteľnú interakciu. Náklady na úspešný Sybil útok rastú lineárne s počtom falošných identít a kvadraticky s cieľovou úrovňou reputácie. Prevádzka viacerých DID paralelne je možná, ale zámerne drahá—každá identita si musí nezávisle nahromadiť reputáciu prostredníctvom skutočnej aktivity. V slobodných spoločnostiach tieto náklady odrádzajú od príležitostného zneužitia; v diktatúrach sa paralelné DID stávajú nástrojom prežitia umožňujúcim kompartmentalizovaný odpor, podzemnú koordináciu a bezpečnejšiu navigáciu na čiernom trhu.

Obrana proti kolúzii. Vzorce vzájomného potvrdzovania medzi uzavretými skupinami sú zistiteľné prostredníctvom analýzy sociálneho grafu. Agregčné funkcie reputácie diskontujú tvrdenia z tesne zhľuknutých zdrojov.

Protivník na úrovni štátu. Onion smerovanie, absencia centralizovanej infraštruktúry a rozloženie roly overovateľa naprieč základňou účastníkov zabezpečujú, že potlačenie vyžaduje opatrenia neúmerne akémukoľvek prospechu.

Súkromie vs. zodpovednosť. Pseudonymita—stredná cesta medzi anonymitou a zverejnením identity—umožňuje DID hromadiť zmysuplnú reputáciu bez odhalenia reálnej identity držiteľa.

11 Aspekty súkromia

Model súkromia RSN je postavený na pseudonymite. Držiteľ kontroluje zverejnenie identity: minimálne (čistý pseudonym), selektívne (prepojené konkrétne poverenia) alebo úplné (pridružená právna identita). Publikované tvrdenia sú trvalé—systém podporuje kontextuálnu opravu, ale nie vymazanie. Držiteľ môže opustiť kompromitovaný DID a začať odznova, čím sa vzdá nahromadenej reputácie.

12 Súvisiaca práca

Špecifikácia W3C DID Core [2] a sieť Ceramic [8] poskytujú základ identity. EigenTrust [13] demonštroval distribuovanú agregáciu reputácie bez centrálnej autority. SBT [3] zaviedli neprenosné sociálne tokeny. RSN sa líši dôrazom na ekonomické náklady ako filter kvality a svojím mechanizmom oceňovania radikalizmu.

DAO [4] a kvadratické hlasovanie [5] demonštrovali uskutočniteľnosť decentralizovanej správy. RSN odvodzuje konsenzus z obojstranných cenových vyjednávanií namiesto hlasovania.

Návrh čerpá z anarchokapitalistickej teórie [14, 15] pre súkromné poskytovanie služieb, ale odkláňa sa v dvoch kľúčových ohľadoch: navrhuje pre zlomyseľnosť a odplatné impulzy namiesto predpokladania racionality a navrhuje postupný prechod namiesto revolúcie. Koncept emergentných spoločenských zmlúv má predchodcov v Hayekovej teórii spontánneho poriadku [16].

Anarcho-agorizmus. RSN zdieľa významnú spoločnú pôdu s agoristickou protiekonomikou [17]—najmä dôraz na budovanie paralelných inštitúcií a dobrovoľnú výmenu. Agorizmus však má sklon predpokladať racionálny vlastný záujem ako dostatočný koordinačný mechanizmus a často mu chýba konkrétna migračná cesta z existujúcich štátnych štruktúr. RSN explicitne zahŕňa neracionálne behaviorálne sklony a poskytuje mechanizmus fiškálneho tlaku na postupný prechod.

Meritokracia. RSN môže predstavovať prvý funkčný opis toho, ako môže meritokracia [18] vzniknúť ako systémová vlastnosť namiesto slogana. Tradičné meritokratické systémy zlyhávajú,

pretože vyžadujú centrálnu autoritu na definovanie a vymáhanie „zásluh“. V RSN zásluhy vznikajú z obojstranných hodnotení: tí, ktorí prinášajú hodnotu, hromadia reputáciu; žiadny výbor nerozhoduje, kto má zásluhy.

Vlastníctvo ako privilégium. RSN sa zásadne odkláňa od anarchokapitalistického a rakúsko-školského poňatia vlastníckych práv ako prirodzených a absolútnych. V rámci RSN je vlastníctvo *privilégiom*—spoločenským uznaním, ktoré môže byť v extrémnych prípadoch odňaté komunitou, keď účastník zásadne poruší zdieľané normy (zrada, odmietnutie brániť komunitu v existenčnej kríze, systematické vykorisťovanie). Nejde o štátne vyvlastnenie, ale o odňatie spoločenského uznania sieťou obojstranných vzťahov.

13 Diskusia a obmedzenia

Studený štart. Hodnota RSN závisí od sieťových efektov; skorí osvojovatelia čelia obmedzenej hodnote, kým účasť nedosiahne prah. Avšak už od skorých fáz slúži sieť DID ako užitočný doplnkový zdroj informácií. Očakáva sa, že skoré hodnotenie reputácie a posudzovanie autorít sa budú postupne rozvíjať s rastúcou sofistikovanosťou.

Ochrana proti parazitovaniu a kontrola prístupu. Cieľové DID môžu ukladať odstupňované poplatky a obmedzenia prístupu pre dotazy od nízko-reputačných DID. Nejde o binárnu, ale o spojitú škálu: čím menej reputácie dotazujúci DID má, tým menej informácií dostane, tým dlhšie čaká a tým viac platí. Tento mechanizmus stimuluje skutočnú účasť namiesto pasívnej konzumácie.

Nerovnosť prístupu. Náklady na publikovanie tvrdení môžu odfiltrovať legitímne krivdy ekonomicky znevýhodnených účastníkov. Zmierne: každý účastník súčasne slúži ako potenciálny overovateľ (alebo túto rolu deleguje) a zarába overovacie poplatky. Za dostatočný časový horizont by sa neradikálny účastník mal priblížiť finančnej neutralite—príjem z overovania približne vyrovnáva náklady na publikovanie. Ide o štatistické očakávanie, nie o záruku.

Nerovnosť reputácie. Skorí osvojovatelia hromadia výhody, ktoré môžu vytvárať bariéry pre neskorších prichádzajúcich. Avšak hodnotenie reputácie vykonávajú poskytovatelia tretích strán, ktorí sa môžu rozhodnúť zmierniť výhodu prvého ťahu prostredníctvom svojich agregáčnych algoritmov. Byť prvý s dobrou reputáciou je legitímna komparatívna ekonomická výhoda—a to zámerne.

Otvorené otázky. Optimálne nákladové funkcie, štandardy agregácie, správa protokolu a interakcia s AI generovanými syntetickými reputačnými dátami zostávajú oblasťami pre budúcu prácu.

Tento článok netvrdí, že RSN prinesie optimálne výsledky za všetkých okolností. Tvrdí, že RSN predstavuje *uskutočniteľnú* alternatívu—technicky implementovateľnú, ekonomicky sebestačnú a spoločensky kompatibilnú s ľudskými behaviorálnymi sklonmi tak, ako skutočne sú.

14 Záver

Tento článok predstavil Reputačnú sociálnu sieť, decentralizovaný protokol umožňujúci pseudonymnú, overiteľnú výmenu reputácie. Princíp drahého radikalizmu zabezpečuje, že podvodné tvrdenia sú cenovo vytlačané bez cenzúry. Navrhnutá migračná cesta umožňuje postupný, zvrtný prechod z existujúcich inštitúcií. Návrh zahŕňa ľudskú povahu tak, ako je—vrátane malichernosti, zlomyseľnosti a túžby po odplatnom zadosťučinení—namiesto vyžadovania ideologickej premeny. Výsledkom nie je utópia, ale systém, kde je spravodlivosť dostupná, reputácia je zaslužená a náklady na pochybenie nesie strana, ktorá ho spôsobila.

References

- [1] Czech Republic, “Act no. 549/1991 coll., on court fees, as amended,” 1991, fee schedule for court proceedings; cost rules per Act No. 99/1963 Coll. (Code of Civil Procedure) and Decree No. 177/1996 Coll. (Attorney Tariff).
- [2] M. Sporny, D. Longley, M. Sabadello, D. Reed, O. Steele, and C. Allen, “Decentralized identifiers (DIDs) v1.0,” W3C Recommendation, Jul. 2022.
- [3] E. G. Weyl, P. Ohlhaver, and V. Buterin, “Decentralized society: Finding Web3’s soul,” *SSRN Electronic Journal*, May 2022.
- [4] V. Buterin, “DAOs, DACs, DAs and more: An incomplete terminology guide,” Ethereum Blog, May 2014.
- [5] V. Buterin, Z. Hitzig, and E. G. Weyl, “A flexible design for funding public goods,” *Management Science*, vol. 65, no. 11, pp. 5171–5187, 2019.
- [6] D. Karger, E. Lehman, T. Leighton, R. Panigrahy, M. Levine, and D. Lewin, “Consistent hashing and random trees: Distributed caching protocols for relieving hot spots on the World Wide Web,” in *Proc. 29th ACM STOC*, 1997, pp. 654–663.
- [7] D. Buchner, “ION — a scalable DID method based on Bitcoin,” Microsoft, 2021.
- [8] Ceramic Network, “Ceramic protocol specification,” GitHub, 2023. [Online]. Available: <https://github.com/ceramicnetwork>
- [9] É. Durkheim, *The Division of Labor in Society*. Free Press, 1893, english translation 1984.
- [10] J. Rawls, *A Theory of Justice*. Harvard University Press, 1971.
- [11] J. Haidt, *The Righteous Mind: Why Good People Are Divided by Politics and Religion*. Vintage Books, 2012.
- [12] J. R. Douceur, “The Sybil attack,” in *Proc. 1st International Workshop on Peer-to-Peer Systems (IPTPS)*, 2002, pp. 251–260.
- [13] S. D. Kamvar, M. T. Schlosser, and H. Garcia-Molina, “The EigenTrust algorithm for reputation management in P2P networks,” in *Proc. 12th International Conference on World Wide Web*, 2003, pp. 640–651.
- [14] M. N. Rothbard, *For a New Liberty: The Libertarian Manifesto*. Macmillan, 1973.
- [15] H.-H. Hoppe, *Democracy: The God That Failed*. Transaction Publishers, 2001.
- [16] F. A. Hayek, *Law, Legislation and Liberty*. University of Chicago Press, 1973.
- [17] S. E. I. Konkin, *An Agorist Primer*. KoPubCo, 2006.
- [18] M. Young, *The Rise of the Meritocracy*. Thames and Hudson, 1958.