

Decentralizirana reputacijska mreža: Okvir za prirodnu organizaciju društva

Pavel Kudrna
Prague, Czechia
Draft v1 — March 2026

Abstract

Osjećaj pravde—uvjerenje da se nepravde ispravljaju i da se zasluge nagrađuju—najsnažnija je kohezivna sila društva. Kada centralizirane institucije upravljanja ne mogu pružiti taj osjećaj jer trošak provođenja prava premašuje vrijednost samog prava, društvena kohezija se raspada. Postojeće institucionalne strukture ne uspijevaju riješiti značajnu klasu sporova na sustavno isti način na koji centralno planiranje ne uspijeva alocirati resurse: kroz asimetriju informacija, nedostatak povratnih petlji i odvojenost donositelja odluka od posljedica njihovih odluka. Ovaj rad predstavlja Reputacijsku društvenu mrežu (RSN): decentralizirani, nepotkupljivi, cenzuri otporni komunikacijski sloj izgrađen na decentraliziranim identifikatorima (DID) koji pseudonimnim sudionicima omogućuje objavljivanje, provjeru i konzumiranje reputacijskih informacija o ponašanju u stvarnom svijetu. Temeljni mehanizam počiva na tri načela dizajna: (1) asimetričnoj strukturi troškova gdje je čitanje reputacijskih podataka jeftino, ali pisanje zahtijeva provjerljiv napor; (2) nedeterminističkom protokolu za odabir provjeritelja temeljenom na konzistentnom raspršivanju koji cijenu radikalnih tvrdnji određuje kroz eskalirajuće troškove iteracije; i (3) tržišno vođenom modelu reputacijskog autoriteta gdje privatni provjeritelji zalažu svoju akumuliranu reputaciju na točnost tvrdnji koje podržavaju. Rezultirajuća arhitektura proizvodi emergentnu meritokraciju bez središnje koordinacije i omogućuje postupan, reverzibilan put migracije od postojećih sustava kojima upravlja država.

1 Uvod

1.1 Problem centraliziranog povjerenja

Suvremeno upravljanje počiva na temeljnoj pretpostavci: da centralizirane institucije mogu posredovati povjerenje između stranaca u velikim razmjerima. Sudovi presuđuju u sporovima. Registri

potvrđuju vlasništvo. Regulatorna tijela provode standarde. Te su institucije osmišljene u doba kada su informacije bile oskudne, komunikacija spora, a delegiranje ovlasti središnjem tijelu jedini izvediv mehanizam koordinacije. Centralizirano upravljanje, međutim, zakazuje iz istih strukturnih razloga kao i centralno planiranje: asimetrije informacija, nedostatka povratnih petlji i odvojenosti donositelja odluka od posljedica njihovih odluka.

Pretpostavka zakazuje, primjerice, kada trošak institucionalnog posredovanja premašuje vrijednost spora. Zamislite najmoćnija koji otkrije da unajmljeni stan nema zakonski propisanu potvrdu o električnoj sigurnosti—stanje koje predstavlja neposrednu opasnost za život. Zakonsko pravo najmoćnija da odstupi od ugovora je nedvosmisleno. Ipak, trošak provođenja tog prava putem sudskog sustava premašuje novčanu vrijednost pologa i dugovane štete, čak i uključujući moguću zakonsku naknadu [1]. Racionalan odgovor jest apsorbirati gubitak i izaći.

Ovo nije patološki rubni slučaj. To je zadano iskustvo za značajnu klasu sporova u kojima je šteta stvarna, ali novčani ulozi padaju ispod praga na kojem institucionalno provođenje postaje ekonomski racionalno. Rezultat je sustav koji strukturno pogoduje zlonamjernim akterima: oni koji drugima nanose štetu u obujmu ispod tog praga mogu djelovati nekažnjeno, jer trošak traženja pravde pada na oštećenu stranu.

Gornji primjer preuzet je iz pravnog okruženja autora—češkog sustava građanskog prava. U drugim pravnim tradicijama—običajnom pravu temeljenom na presedanima, običajnom pravu, mješovitim sustavima—pravda zakazuje na različite načine i u različitim stupnjevima, ovisno o kulturnim i procesnim posebnostima jurisdikcije. Čitatelji će vjerojatno prepoznati istovjetne primjere iz vlastitog konteksta. Ono što je strukturno univerzalno jest obrazac: sporovi čija vrijednost pada ispod praga ekonomski racionalnog provođenja završavaju tako da gubitak apsorbira oštećena strana. RSN ne obećava savršenu pravdu—on samo smanjuje strukturnu prednost koju

zlonamjerni akteri uživaju kada je institucionalno provođenje neekonomično.

1.2 Zašto postojeća rješenja ne zadovoljavaju

Okviri decentraliziranog identiteta (DID) [2] pružaju kriptografske mehanizme za samosuvereno upravljanje identitetom, ali se prvenstveno usredotočuju na provjeru identiteta bez rješavanja šireg pitanja reputacije ponašanja.

Soulbound tokeni (SBT) [3] obuhvaćaju uvid da je reputacija neprenosiva, ali se oslanjaju na blockchain infrastrukturu s ograničenjima skalabilnosti i ne bave se ekonomskim poticajima koji upravljaju unosom informacija. Srodni koncepti poput tokena zasluga (npr. Liberland) dijele sličnu filozofiju, ali ostaju vezani za specifične jurisdikcijske okvire.

Decentralizirane autonomne organizacije (DAO) [4] provode upravljanje putem pametnih ugovora, ali repliciraju plutokratsku dinamiku u kojoj je utjecaj proporcionalan kapitalu. Kvadratno glasovanje [5] to djelomično ublažava, ali ograničava praktičnu primjenu. DAO-i se također suočavaju s temeljnim *problemom proročišta*: pametni ugovori ne mogu pouzdano provjeriti stanja u stvarnom svijetu bez pouzdanog vanjskog izvora, a taj problem nema općenito rješenje unutar blockchain arhitekture.

Nijedan postojeći sustav ne kombinira decentralizaciju, otpornost na cenzuru, pseudonimnost, provjerljiv trošak ulaska i emergentni konsenzus.

1.3 Doprinosi

Ovaj rad daje sljedeće doprinose:

1. Definiciju **Reputacijske društvene mreže (RSN)**, decentraliziranog protokola koji proširuje DID okvir kako bi podržao bilateralnu razmjenu reputacije.
2. **Nedeterministički protokol za odabir provjeritelja** temeljen na konzistentnom raspršivanju [6].
3. **Načelo skupog radikalizma**, koje cijenu tvrdnji određuje prema njihovoj udaljenosti od mrežnog konsenzusa kroz tri kumulativna kanala troška.
4. **Model uglednog autoriteta** s asimetričnim poticajima gdje lažno podupiranje košta katastrofalno više od legitimnih naknada.
5. **Postupan put migracije** kroz paralelnu fiskalnu infrastrukturu.

2 Načela dizajna

Arhitekturu RSN-a ograničava pet neprekršivih načela dizajna.

Kontinuitet i evolucija. Sustav koegzistira s postojećim institucijama tijekom prijelaznog razdoblja neodređene duljine. Prijelaz mora biti reverzibilan u svakoj fazi.

Dobrovoljnost i odgovornost. Sudjelovanje je dobrovoljno, ali dobrovoljnost je spregnuta s odgovornošću: sudionik koji preuzme kontrolu nad institucionalnom funkcijom istodobno preuzima i pripadajuće obveze.

Raznolikost i kulturna neutralnost. Konsenzus proizlazi iz bilateralnih interakcija, a ne iz unaprijed zadanih pravila koja nameću dizajneri sustava.

Otpornost i otpor cenzuri. Trošak cenzuriranja mreže mora premašiti trošak njezinog toleriranja. Samo potpuni totalitarizam—uz razorne političke i ekonomske troškove—može potisnuti sustav.

Konsenzus i provođenje. Sustav ugrađuje ljudske sklonosti prema sitničavosti, pakosti i osvetničkom zadovoljstvu kao noseće značajke. Nedolično ponašanje nije zabranjeno; ono se naplaćuje.

3 Pregled sustava

3.1 Reputacijska društvena mreža

RSN je decentralizirani komunikacijski sloj ravnopravnih čvorova u kojem sudionici razmjenjuju provjerljive informacije o ponašanju u stvarnom svijetu. Njegova su definirajuća svojstva: decentralizirana i necenzurabilna infrastruktura; pseudonimno sudjelovanje putem DID-ova; asimetrična struktura troškova (čitanje je jeftino, pisanje je skupo); kriptografska provjerljivost; i **podrška standardima**—strojno čitljivi formati za informacije koje se propagiraju kroz mrežu, za usluge koje nude autoriteti (sastavljanje tvrdnji, podupiranje, usluga svjedočenja) te za format politike uključujući pravila za procjenu reputacije druge strane i procjenu rizika neusklađenosti politike (između deklariranog i stvarnog ponašanja).

3.2 Arhitektonske komponente

RSN se sastoji od četiri primarne komponente (Sl. 1):

1. **DID sloj.** Identiteti sudionika s deklariranim pravilima, reputacijskim metapodacima i mrežnim usmjeravanjem.
2. **Protokol tvrdnji.** Strukturirani format za ob-

javljanje tvrdnji o događajima u stvarnom svijetu.

3. **Mreža provjere.** Decentralizirani protokol za dodjeljivanje provjeritelja pomoću konzistentnog raspršivanja.
4. **Sloj agregacije reputacije.** Usluge koje proizvode ljudski čitljive sažetke reputacije.

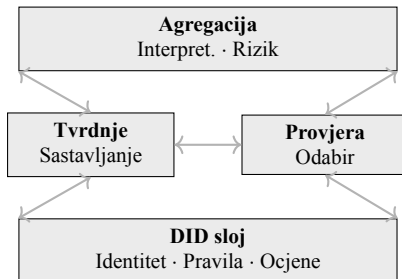


Figure 1: Četveroslojna arhitektura RSN-a.

3.3 Uloge sudionika

Transakcija provjere uključuje do šest različitih DID uloga (Sl. 2): **Izdavatelj** (DID_I , stvara i podnosi tvrdnju), **Subjekt** (DID_S , DID na koji se tvrdnja odnosi—može se podudarati s Izdavateljem), **Autoritet** (DID_A , podupire tvrdnju uz naknadu; može ponuditi i usluge svjedočenja—*neobavezno*), **Svjedok** ($DID_{W1..n}$, incognito nadzornik poštenja provjeritelja putem izazovnih kodova—*neobavezno*), **Provjeritelj** (DID_V , algoritamski odabran za objavljivanje tvrdnje), i **RSN** (mreža u kojoj se objavljuju provjerene tvrdnje). Bilo koja uloga može se delegirati drugom DID-u (Odjeljak 7.4). Autoritet obično objedinjuje podupiranje s uslugama svjedočenja, ali su dvije funkcije logički neovisne.

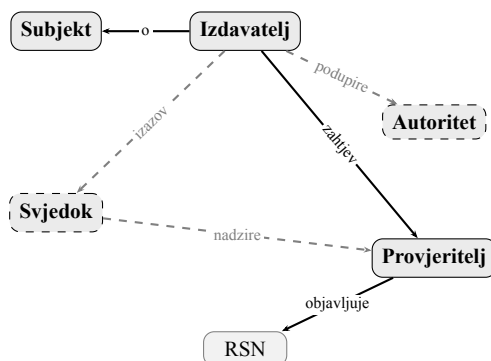


Figure 2: DID uloge u transakciji provjere. Iscrtkano = neobavezno (Autoritet, Svjedok).

3.4 Nepotkupljivost: četiri sile

Nepotkupljivost RSN-a ne proizlazi iz jednog mehanizma, već iz četiri istodobne sile. Nijedna nije sama po sebi dovoljna; tek njihova kombinacija čini pokušaj korupcije ekonomski iracionalnim.

Nepredvidljiva meta. Provjeritelj za svaku tvrdnju odabire se nedeterministički putem konzistentnog raspršivanja (Odjeljak 5.3). Napadač ne može unaprijed ciljati određenog provjeritelja radi podmićivanja, jer je identitet provjeritelja funkcija sadržaja tvrdnje i prethodnih iteracija, a ne izbora izdavatelja.

Reputacijska poluga—sporo gore, brzo dolje. Reputacija se može steći samo postupno, kroz dugo-trajno dosljedno ponašanje. Međutim, može se katastrofalno izgubiti jednim prijevaram podupiranjem (Odjeljak 6.2). Ta asimetrija znači da se godine akumulirane reputacije mogu uništiti jednim nepoštenim podupiranjem; optimalna strategija ostaje odbijanje sumnjivih tvrdnji.

Javno obećanje. Svaki nositelj DID-a javno deklarira svoju politiku—strojno čitljiv skup pravila kojih se obvezuje pridržavati. Razilaženje između deklaracije i stvarnog ponašanja je otkrivo i naplaćuje se kao reputacijski prekršaj teži od samog kršenja (Odjeljak 7.3). Licemjerje je stoga skuplje od izravne nepoštenosti.

Asimetrija troška napada na mrežu. Trošak cenzuriranja ili destabilizacije mreže raste nelinearno s veličinom i gustoćom mreže, dok trošak njezinog toleriranja ostaje konstantan. Da bi se cenzura isplatila, centralizirani bi je akter morao primijeniti na cijelu mrežu—što zahtijeva mjere nesrazmjerne bilo kojoj zamislivoj koristi (Odjeljak 10).

4 Model decentraliziranog identiteta

4.1 DID s posebnim svojstvima

RSN proširuje W3C DID Core specifikaciju [2] sa: **deklariranim pravilima** (strojno čitljive obveze ponašanja), **reputacijskim metapodacima** (agregirana ocjena ponašanja) i **mrežnim usmjeravanjem** (promjenjivi onion pristupnik odvojen od stabilne pozicije na prstenu).

4.2 Životni ciklus tvrdnje

Tvrdnja prolazi kroz šest faza (Sl. 3): sastavljanje, neobavezno podupiranje autoriteta, odabir provjeritelja putem konzistentnog raspršivanja, odluka o provjeri (prihvatanje ili odbijanje s iteracijom), objava

i ažuriranje reputacije za sve strane.

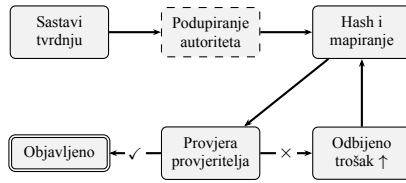


Figure 3: Životni ciklus tvrdnje s petljom iteracije.

4.3 Odnos prema W3C DID Core

Model identiteta RSN-a pravi je nadskup W3C DID Core specifikacije [2]. Svi RSN DID-ovi su valjani W3C DID-ovi. Proširenja specifična za RSN kodirana su kao svojstva DID dokumenta definirana u namjenskoj specifikaciji DID metode, kompatibilnoj s postojećom infrastrukturom poput ION-a [7] i Ceramica [8].

5 Provjera i propagacija informacija

5.1 Trošak unosa informacija

Temeljno ekonomsko načelo RSN-a jest asimetrija između čitanja i pisanja. Čitanje reputacijskih podataka približava se nultom graničnom trošku za sudionike koji su dio DID mreže i imaju pristup razmjernan svojoj reputaciji—pridošlice moraju postupno zaraditi širi pristup (vidi anti-parazitizam). Pisanje—shvaćeno kao trajna materijalizacija reputacije u mreži, a ne kao jednokratni tehnički čin—zahtijeva provjerljivo kumulativno ulaganje kroz tri dimenzije: **vrijeme** (godine života provedene u dosljednom ponašanju, ispunjenim obvezama i njegovanim odnosima), **energiju** (napor uložen u pošteno postupanje, brigu o partnerstvima i dugoročnu pouzdanost) i **novac** (ulaganje u vlastito ime—profesionalni razvoj, kvaliteta vlastitog rada, naknada za nanese štete). Reputacija se ne može trenutno kupiti—ona je ishod cjeloživotne akumulacije koju sustav samo čini vidljivom i prenosivom kroz kontekste. Jednokratni tehnički troškovi protokola (kriptografski potpisi, naknade provjeritelja) zanemarivi su u usporedbi s tim temeljnim ulaganjem.

5.2 Društveni graf i dubina kontakata

RSN je u osnovi društvena mreža: svaki DID dodaje kontakte (druge DID-ove) koji dopuštaju povezivanje. Ti kontakti imaju vlastite kontakte, i tako dalje. Algoritamsko pretraživanje provjeritelja djeluje unutar podesive dubine h povezanih kontakata (npr. $h = 3$: vlastiti izravni kontakti, njihovi kontakti i kontakti

kontakata). Ova arhitektura ne zahtijeva jedinstveni globalni blockchain—ona prirodno pogoduje pojavi zajednica/klastera s preklapanjima u druge zajednice. Svaki DID sudionik mora imati objavljenu **politiku**—strojno čitljiv skup pravila koja upravljaju načinom vrednovanja dolaznih zahtjeva. Kršenja politike bilježe se u mreži kao negativni artefakti.

5.3 Algoritamski odabir provjeritelja

Protokol provjere koristi konzistentno raspršivanje [6] (Sl. 4). Provjera je plaćena usluga: provjeritelji djeluju uz naknadu, stvarajući tržište na kojem konkurencija oblikuje cijene, brzinu i pouzdanost.

Korak 1. Dokument tvrdnje se spaja s rezultatom raspršivanja prethodne iteracije (ili $\emptyset$ u prvoj iteraciji) i raspršuje:

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

Algoritam mora uključivati *cjelovit put* svih prethodnih zahtjeva i odgovora—ne samo hash prethodne iteracije. Cjeloviti odgovor svakog provjeritelja (prihvaćanje, odbijanje, ponudena cijena, razlog) dodaje se rastućem dokumentu, provjerljiv putem kriptografskih potpisa u svakom koraku.

Korak 2. Hash se mapira na N pozicija na prstenu konzistentnog raspršivanja, ravnomjerno raspoređenih (npr. za $N = 4$: $+0^\circ$, $+90^\circ$, $+180^\circ$, $+270^\circ$). Iz svake pozicije, pretraga u smjeru kazaljke na satu odabire najbliži DID kao kandidata za provjeritelja (Sl. 5). N je varijabilan parametar koji može ovisiti o postotku trenutno aktivnih DID-ova, dobu dana ili povijesnoj odzivnosti mreže.

Korak 3. Provjeritelj prihvaća (objavljuje, zalažući reputaciju) ili odbija (vraćajući se na Korak 1 s hashom odbijanja). Kada čvor ne odgovori unatoč deklariranom statusu online, sljedeći zahtjev mora uključivati sve odgovore od svih N prethodnih kandidata za provjeritelja.

Anti-parazitizam. Ciljni DID-ovi mogu postaviti naknade ili ograničenja pristupa za upite od novih DID-ova s malo reputacije. Taj postupni mehanizam (ne binarni) prisiljava pridošlice da izgrade reputaciju kroz istinsku aktivnost prije nego što slobodno konzumiraju tuđe podatke.

Svako odbijanje dodaje cjeloviti odgovor provjeritelja (uključujući razloge i uvjete) dokumentu tvrdnje, proširujući njegov sadržaj. Iz proširenog dokumenta nedeterministički se izračunava novi hash, mapirajući na drugu poziciju prstena i odabirući drugog provjeritelja. Dokumentiranje cjelovitog puta je obavezno—izdavatelj ne može predvidjeti ni utjecati

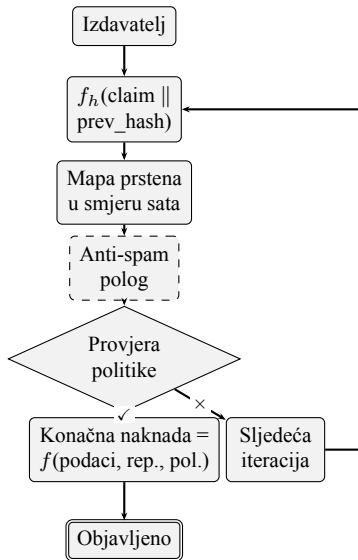


Figure 4: Protokol odabira provjeritelja. Anti-spam polog je neobavezan i može biti povratan. Konačna naknada plaća se samo pri prihvaćanju.

na sljedećeg provjeritelja. Ako provjeritelj zanemari zahtjev unatoč kompatibilnoj deklariranoj politici, svjedoci (ako su prisutni) to bilježe, a izdavatelj može priložiti dokaze svjedoka pri konačnoj objavi.

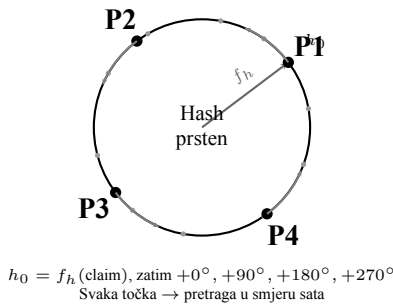


Figure 5: Višetočkovni odabir ($N=4$). Hash h_0 postavlja pomak; 4 točke ravnomjerno raspoređene od h_0 .

5.4 Protokol svjedoka

Uloga **Svjedoka** pruža incognito odgovornost za poštenje provjeritelja kroz kriptografski protokol izazovnog koda:

Korak W1. Podnositelj zahtjeva potpisuje zahtjev za provjeru i šalje ga N_w svjedocima—kontaktima iz podnositeljeve društvene mreže, ili specijaliziranim pružateljima usluge svjedočenja koji djeluju uz naknadu.

Korak W2. Svaki svjedok w_i potpisuje cjeloviti potpisani zahtjev, zadržava izvorni potpis σ_i i izračunava izazovni kod $c_i = h(\sigma_i)$. Izazovni kod dodaje se

zahtjevu.

Korak W3. Zahtjev, koji sada nosi N_w izazovnih kodova, šalje se provjeritelju. Provjeritelj vidi kodove, ali *ne može utvrditi* tko su svjedoci ni odgovaraju li kodovi stvarnim potpisima.

Korak W4 (pošten provjeritelj). Ako provjeritelj odgovori u skladu sa svojom deklariranom politikom, izazovni kodovi ostaju neprozirni. Svjedoci se nikada ne otkrivaju. Nikakvi dodatni podaci se ne objavljuju.

Korak W5 (kršenje politike). Ako provjeritelj prekrši svoju politiku (zanemari zahtjev, odgovori nedosljedno), podnositelj zahtjeva drži izvorne potpise svjedoka σ_i . Oni se mogu objaviti kao popratni podaci: svatko može provjeriti $c_i = h(\sigma_i)$, dokazujući da je svjedok bio prisutan. Podnositelj zahtjeva može objaviti neovisno—provjeritelj je već potpisao izazovne kodove u svom odgovoru.

Svojstvo blefa. Podnositelj zahtjeva može zamijeniti neke ili sve izazovne kodove nasumičnim vrijednostima. Provjeritelj ne može razlikovati istinske kodove (potkrijepljene visokoreputiranim autoritetima) od šuma. Ta *neizvjesnost* je mehanizam provođenja: svaki zahtjev nosi rizik da ugledni autoritet promatra incognito. Trošak održavanja tog pritiska gotovo je nula (generiranje nasumičnih brojeva), dok je potencijalni trošak nepoštenja za provjeritelja katastrofalan. Pošteno ponašanje potiče se čak i u odsutnosti stvarnih svjedoka.

Autoritet kao svjedok. Autoritet koji podupire tvrdnju može objediniti usluge svjedočenja: „Podupirem vašu tvrdnju i služim kao incognito svjedok tijekom provjere.” To je prirodan poslovni model—autoritet već ima kontekst. Međutim, dvije su uloge logički neovisne.

5.5 Načelo skupog radikalizma

Tri kanala troška zbrajaju se istodobno (Sl. 6):

Kanal 1: Trošak iteracije. Svako odbijanje prisiljava na novu iteraciju koja troši vrijeme i resurse. Linearan rast.

Kanal 2: Bujanje dokumenta. Svaka iteracija dodaje cjeloviti odgovor provjeritelja dokumentu tvrdnje. Rast je linearan, ali s osnovnim pomakom: početni sadržaj (sadržaj tvrdnje, podupiranje autoriteta, kriptografski potpisi) već ima netrivialnu veličinu B_0 . Ukupna veličina nakon k iteracija: $S(k) = B_0 + k \cdot \Delta$, gdje je Δ prosječna veličina odgovora.

Kanal 3: Premija za rizik provjeritelja. Rizik je subjektivan. Provjeritelj procjenjuje jesu li deklarirane politike DID-a koji podnosi zahtjev u sukobu s

provjeriteljevim vlastitim komercijalnim, društvenim ili političkim interesima. Premija može eksponencijalno eskalirati s percipiranom udaljenošću od provjeriteljevog „ideala”: $P(d) = \alpha \cdot e^{\beta d}$, gdje je d provjeriteljeva subjektivna mjera udaljenosti. Iza osobne granice odbijanja, provjeritelj može u potpunosti odbiti.

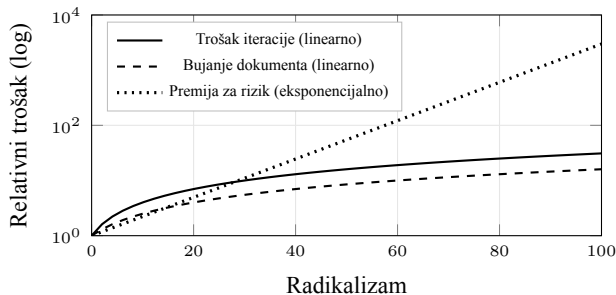


Figure 6: Eskalacija troška kroz tri kanala. Premija za rizik dominira pri visokom radikalizmu.

Ključno, ovo nije cenzura. Nijedna tvrdnja nije zabranjena. Sustav naplaćuje rizik (Tablica 1).

Table 1: Usporedba troškova po vrstama tvrdnji.

Vrsta	Iter.	Dok.	Nakn.	Ukupno
Vjerodostojna	$k_{\min}$	B_0	$P_{\min}$	Nizak
Kontroverzna	k_{med}	$B_0 + k\Delta$	$\alpha e^{\beta d}$	Umjeren
Radikalna	$k_{\max}$	$\gg B_0$	$\gg P_{\min}$	Vrlo visok
Prijevarna	$\rightarrow \infty$	—	—	Neobjavljiva

6 Procjena reputacije i rizika

6.1 Model akumulacije reputacije

Reputacija pokazuje tri svojstva: **sporu akumulaciju** (postupni rast kroz dosljedno ponašanje), **brzo uništenje** (jedna prijevara može katastrofalno smanjiti ocjenu) i **individualno vrednovanje** (svaka konzumirajuća strana može primijeniti vlastitu funkciju agregacije).

6.2 Ugledni autoriteti

Ugledni autoritet pregledava tvrdnje i, ako je zadovoljan, supotpisuje ih—zalažući vlastitu reputaciju (Sl. 7). Asimetrija je namjerna: stjecanje reputacije je sporo (postupno $+\delta$ po poštenom podupiranju), dok je njezin gubitak katastrofalan ($-\Delta \gg \delta$ po lažnom podupiranju; ilustrativno, npr. $+2\%$ nasuprot -70%). Optimalna strategija uvijek je odbiti sumnjive tvrdnje. Konkretni vrijednosti δ i Δ su parametri sustava.

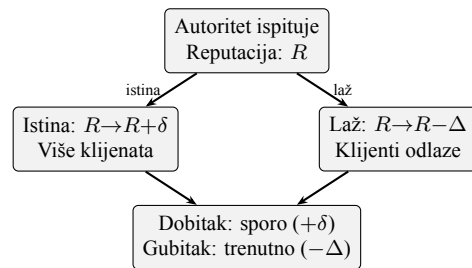


Figure 7: Ugledni autoritet—asimetrični poticaji.

6.3 Višedimenzionalna reputacija

Reputacija nije skalar, već vektor kroz više dimenzija: financijska pouzdanost, osobni integritet, profesionalna kompetencija, građanski angažman i druge (Sl. 8). Različiti pružatelji vrednovanja projiciraju ovaj vektor drugačije ovisno o kontekstu—zajmodavac prioritzira financijsku pouzdanost, poslodavac profesionalnu kompetenciju, susjed građansko ponašanje. Ne postoji jedinstvena „ispravna” ocjena reputacije; samo perspektive.

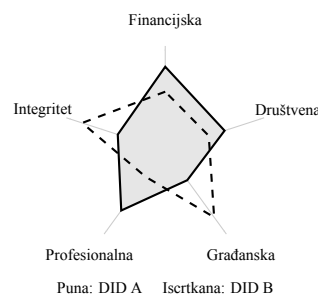


Figure 8: Višedimenzionalni vektori reputacije. Različiti DID-ovi pokazuju različite profile kroz dimenzije.

6.4 Demokratizirana procjena rizika

RSN demokratizira sustavnu procjenu rizika—sposobnost trenutno koncentriranu u financijskim institucijama, ali primjenjivu daleko izvan bankarstva. Industrijski konglomerati koji procjenjuju pouzdanost dobavljača, osiguravajuća društva koja određuju cijenu bihevioralnog rizika, dubinska analiza za spajanja i preuzimanja, procjena životnog vijeka opreme u proizvodnji—gdje god rizik druge strane zahtijeva procjenu, RSN pruža decentraliziranu, tržišno vođenu alternativu. Tržište usluga interpretacije prevodi sirove višedimenzionalne reputacijske podatke u upotrebljive sažetke, čineći vrednovanje druge strane dostupnim svakom sudioniku uz granični trošak.

7 Konsenzus i rješavanje sporova

7.1 Model decentralizirane pravde

RSN preoblikuje pravdu kao problem bilateralnog pregovaranja. Prijetnja trajnom, provjerljivom štetom po reputaciji učinkovitiji je odvrćajući čimbenik od sudskih postupaka koje oštećena strana ne može priuštiti.

7.2 Emergentni konsenzus

Svaki sudionik održava osobni prag zadovoljstva. Agregatni konsenzus mreže pojavljuje se kao statistički prosjek tisuća bilateralnih pregovora (Sl. 9). Odgovor daleko iznad konsenzusa (barbarski) skup je za objavu. Odgovor blizu konsenzusa (proporcionalan) je jeftin. Konsenzus nije pravilo—on je cjenovni signal.

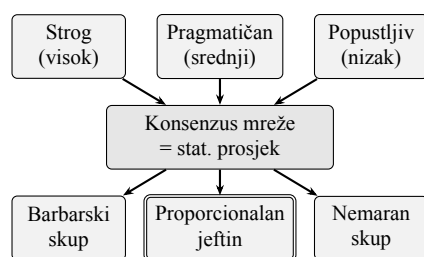


Figure 9: Emergentni konsenzus iz individualnih pragova zadovoljstva.

7.3 Kalibracija kazne

Svaki nositelj DID-a javno deklarira odgovore na specifične kategorije nedoličnog ponašanja. Nesrazmjerno stroge ili blage deklaracije privlače negativne reputacijske signale. Proporcionalne deklaracije prihvaćaju se bez trvenja—samokalibrirajući sustav kažnjavanja.

Deklaracije konsenzusa i same podliježu otkrivanju licemjerja: deklarativno obvezivanje na konsenzusnu poziciju uz nedosljedno ponašanje predstavlja reputacijski prekršaj teži od samog odstupanja, jer pokazuje namjernu prijevaru.

7.4 Delegiranje

Sve aktivnosti unutar DID-a—uz jednu iznimku—mogu se delegirati drugom DID-u. **Uloga Subjekta—DID-a čije je ponašanje predmet tvrdnje—ne može se delegirati; ona je neprenosivo vezana za nositelja identiteta na kojeg se tvrdnja odnosi.** Ostale aktivne uloge—Izdavatelj, Autoritet, Svjedok, Provjeritelj—mogu se prenijeti na određeni delegatski DID, bilo za

provjeru, podnošenje tvrdnji, sudjelovanje u konsenzusu ili rješavanje sporova. Delegiranje je opozivo u svakom trenutku. To omogućuje specijalizaciju (npr. profesionalne usluge provjere) dok nositelj zadržava krajnju kontrolu i odgovornost. Delegiranje se primjenjuje na cijeli sustav i ključno je za skalabilnost.

7.5 Od individualnog morala do emergentnog društvenog ugovora

Deklarirana politika svakog DID-a predstavlja formalizaciju individualnog morala: što nositelj smatra prihvatljivim, kako reagira na specifična ponašanja, što zahtijeva od drugih strana. Te politike ne nameće dizajner sustava—bira ih svaki sudionik i izražava u strojno čitljivom obliku.

Ta formalizacija omogućuje trostupanjsku emergenciju. Prvo, individualni moral kodiran je kao **politika**—skup deklariranih pravila, pragova i funkcija odgovora kojih se DID obvezuje pridržavati. Drugo, agregat svih politika kroz mrežu proizvodi **emergentnu etiku**—statistički vidljive norme koje nijedan pojedinac sudionik nije osmislio, ali koje proizlaze iz interakcije tisuća individualnih moralnih pozicija [9]. Treće, ta emergentna etika, izražena kao zajedničke norme ponašanja provedene kroz bilateralne cjenovne signale, čini **mjerljiv društveni ugovor**—ne teorijski konstrukt koji nitko nije potpisao [10], već empirijski uočljiv skup pravila potkrijepljen stvarnim ponašanjem.

Taj proces zrcali nalaze teorije moralnih temelja [11]: ljudski moral je intuitivan, pluralistički i kulturno varijabilan. RSN ne zahtijeva moralni konsenzus kao ulaz; on proizvodi bihevioralni konsenzus kao izlaz. Rezultirajući društveni ugovor nije statičan—on se razvija kako se sudionici pridružuju, odlaze i prilagođavaju svoje politike kao odgovor na povratne informacije mreže. Za razliku od klasične teorije društvenog ugovora, ovaj ugovor je opoziv, uočljiv i provediv bez suverena.

8 Ekonomski model

Prethodni odjeljci opisali su alat—mehanizme provjere RSN-a, strukturu troškova i emergentni konsenzus. Ovaj odjeljak opisuje metodologiju za primjenu tog alata na fiskalnu i upravljačku tranziciju. Alat je opće namjene; metodologija u nastavku jedna je moguća primjena.

8.1 Struktura poticaja

Reputacija kao kapital stvara izravne poticaje za pošteno ponašanje. U normalnom radu, sudionici prirodno grade reputaciju kroz svakodnevne transakcije i ispunjene obveze. Primarni izdatak odnosi se na *negativne* tvrdnje—bilježenje štete koju su nanijeli drugi. Ta asimetrija potiče korisno, pouzdano ponašanje: biti pošten ne košta ništa dodatno, dok štetnost stvara dokumentirani trag koji će drugi platiti da ga sačuvaju. Licemjerje—deklariranje pravila bez njihova pridržavanja—najskuplji je oblik neuspjeha, jer pokazuje namjernu prijevaru.

8.2 Paralelni fiskalni sustav

Tri komponente omogućuju konkurentski pritisak: (1) **Jednostavan porez**—jedinstvena proporcionalna stopa bez iznimaka, u početku neznatno ispod postojeće efektivne stope; (2) **Elektronička registracija potrošnje (ESR)**—obrtanje češkog EET modela tako da građani nadziru državne rashode; (3) **Građanski usmjerena alokacija poreza**—počevši od nekoliko posto u prvoj godini i dosežući, nakon desetljeća, bilo što od niskih dvoznamenkastih vrijednosti do pune migracije na građanski usmjeren sustav, ovisno o stopi prihvaćanja. Stvarni tempo ovisi o brzini kojom se pojavljuju slobodno-tržišne alternative državnim uslugama i o spremnosti države na suradnju u tranziciji; funkcija vremena ne mora biti linearna, i nema razloga postaviti gornju granicu na to gdje prihvaćanje u konačnici može stići.

9 Put migracije

Migracija se odvija kroz tri faze (Sl. 10): **Faza 1: Sloj preklapanja** (RSN kao informacijski sloj, država je jedini pružatelj), **Faza 2: Konkurencija** (RSN pruža funkcionalne alternative, korištenje dvostrukog sustava) i **Faza 3: Tranzicija** (RSN nadmašuje državne ekvivalente, dobrovoljna migracija). Prijelaz je reverzibilan u svakoj fazi.

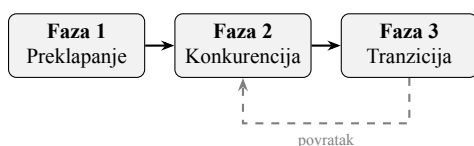


Figure 10: Trofazna migracija—reverzibilna u svakoj fazi.

Primarni mehanizam pritiska je fiskalni: kada uvjetni porezni obveznici dosegnu „ekonomski znača-

jnu manjinu X ”—skupinu dovoljno veliku da represija protiv nje uzrokuje netrivialnu ekonomsku štetu i da građanski neposluh postane vjerodostojna prijetnja—država ulazi u pregovore. Za ilustraciju koristimo $X \approx 15\%$ BDP-a, ali stvarni prag ovisi o konkretnom gospodarstvu.

10 Sigurnosna analiza

Razmatramo pet kategorija protivnika: pojedinačne zlonamjerne aktore, organizirane skupine, korporativne protivnike, protivnike na razini države i protivnike na razini protokola.

Otpornost na Sybil napade [12]. Izgradnja reputacije zahtijeva dugotrajnu, provjerljivu interakciju. Trošak uspješnog Sybil napada raste linearno s lažnim identitetima i kvadratno s ciljnom razinom reputacije. Rukovanje s više DID-ova paralelno je moguće, ali skupo po dizajnu—svaki identitet mora neovisno akumulirati reputaciju kroz istinsku aktivnost. U slobodnim društvima taj trošak odvraća od površne zloporabe; u diktaturama, paralelni DID-ovi postaju alat preživljavanja koji omogućuje odjeljivanje otpora, podzemnu koordinaciju i sigurnije snalaženje na crnom tržištu.

Obrana od tajnog dogovaranja. Obrasci uzajamnog podupiranja među zatvorenim skupinama otkrivi su analizom društvenog grafa. Funkcije agregacije reputacije diskontiraju tvrdnje iz čvrsto povezanih izvora.

Protivnik na razini države. Onion usmjerenje, odsutnost centralizirane infrastrukture i raspodjela uloge Provjeritelja kroz bazu sudionika osiguravaju da potiskivanje zahtijeva mjere nesrazmjerne bilo kojoj koristi.

Privatnost nasuprot odgovornosti. Pseudonimnost—srednji put između anonimnosti i otkrivanja identiteta—omogućuje DID-ovima da akumuliraju smislenu reputaciju bez otkrivanja stvarnog identiteta nositelja.

11 Razmatranja o privatnosti

Model privatnosti RSN-a izgrađen je na pseudonimnosti. Nositelj kontrolira otkrivanje identiteta: minimalno (čisti pseudonim), selektivno (povezane specifične vjerodajnice) ili potpuno (pridružen pravni identitet). Objavljene tvrdnje su trajne—sustav podržava kontekstualni ispravak, ali ne i brisanje. Nositelj može napustiti kompromitirani DID i početi iznova, gubeći akumuliranu reputaciju.

12 Srodni rad

W3C DID Core specifikacija [2] i Ceramic Network [8] pružaju temelj identiteta. EigenTrust [13] demonstrirao je distribuiranu agregaciju reputacije bez središnjeg autoriteta. SBT-ovi [3] uveli su neprenosive društvene tokene. RSN se razlikuje po naglasku na ekonomskom trošku kao filtru kvalitete i po svom mehanizmu za određivanje cijene radikalizma.

DAO-i [4] i kvadratno glasovanje [5] demonstrirali su izvedivost decentraliziranog upravljanja. RSN izvodi konsenzus iz bilateralnih cjenovnih pregovora, a ne iz glasovanja.

Prijedlog se oslanja na anarho-kapitalističku teoriju [14, 15] za privatno pružanje usluga, ali odstupa u dva ključna pogleda: dizajniran je za pakost i osvetničke impulse umjesto da pretpostavlja racionalnost, i predlaže postupnu tranziciju umjesto revolucije. Koncept emergentnih društvenih ugovora ima prethodnike u Hayekovoj teoriji spontanog reda [16].

Anarho-agorizam. RSN dijeli značajno zajedničko tlo s agorističkom kontra-ekonomijom [17]—posebno naglasak na izgradnji paralelnih institucija i dobrovoljnoj razmjeni. Međutim, agorizam ima tendenciju pretpostavljati racionalan vlastiti interes kao dovoljan mehanizam koordinacije i često mu nedostaje konkretan put migracije od postojećih državnih struktura. RSN eksplicitno ugrađuje neracionalne bihevioralne sklonosti i pruža mehanizam fiskalnog pritiska za postupnu tranziciju.

Meritokracija. RSN može predstavljati prvi funkcionalni opis toga kako meritokracija [18] može nastati kao sistemsko svojstvo, a ne slogan. Tradicionalni meritokratski sustavi zakazuju jer zahtijevaju središnji autoritet da definira i provede „zaslugu”. U RSN-u, zasluga proizlazi iz bilateralnih vrednovanja: oni koji isporučuju vrijednost akumuliraju reputaciju; nijedan odbor ne odlučuje tko ima zaslugu.

Vlasništvo kao povlastica. RSN se temeljno razlikuje od anarho-kapitalističkih i austrijskoškolskih tretmana vlasničkih prava kao prirodnih i apsolutnih. U RSN okviru, vlasništvo je *povlastica*—društveno priznanje koje se, u ekstremnim slučajevima, može oduzeti od strane zajednice kada sudionik temeljno prekrši zajedničke norme (izdaja, odbijanje obrane zajednice u egzistencijalnoj krizi, sustavno iskorištavanje). To nije državna eksproprijacija, već povlačenje društvenog priznanja od strane mreže bilateralnih odnosa.

13 Rasprava i ograničenja

Hladan start. Vrijednost RSN-a ovisi o mrežnim učincima; rani usvojitelji suočavaju se s ograničenom vrijednošću dok sudjelovanje ne dosegne prag. Međutim, čak i od ranih faza, DID mreža služi kao koristan dopunski izvor informacija. Očekuje se da će se rano vrednovanje reputacije i procjena autoriteta postupno razvijati uz sve veću sofisticiranost.

Anti-parazitizam i kontrola pristupa. Ciljni DID-ovi mogu nametnuti postupne naknade i ograničenja pristupa za upite od DID-ova niske reputacije. To nije binarno, već kontinuirana ljestvica: što manje reputacije DID koji šalje upit ima, to manje informacija dobiva, to duže čeka i to više plaća. Taj mehanizam potiče istinsko sudjelovanje umjesto pasivne konzumacije.

Nejednakost pristupa. Trošak objavljivanja tvrdnji može filtrirati legitimne pritužbe ekonomski slabijih sudionika. Ublažavanje: svaki sudionik istodobno služi kao potencijalni provjeritelj (ili delegira tu ulogu) i zarađuje naknade za provjeru. Kroz dovoljan vremenski horizont, neradikalni sudionik trebao bi se približiti financijskoj neutralnosti—prihod od provjere približno kompenzira troškove objavljivanja. To je statističko očekivanje, a ne jamstvo.

Nejednakost reputacije. Rani usvojitelji akumuliraju prednosti koje mogu stvoriti prepreke za one koji dolaze kasnije. Međutim, vrednovanje reputacije provode neovisni pružatelji koji mogu odabrati ublažiti prednost prvog poteza kroz svoje algoritme agregacije. Biti prvi s dobrom reputacijom legitimna je usporedna ekonomska prednost—i to je po dizajnu.

Otvorena pitanja. Optimalne funkcije troška, standardi agregacije, upravljanje protokolom i interakcija s reputacijskim podacima koje sintetizira umjetna inteligencija ostaju područja za budući rad.

Ovaj rad ne tvrdi da će RSN proizvesti optimalne ishode u svim okolnostima. On tvrdi da RSN predstavlja *izvedivu* alternativu—tehnički provedivu, ekonomski samoodrživu i društveno kompatibilnu s ljudskim bihevioralnim sklonostima kakve one stvarno jesu.

14 Zaključak

Ovaj rad predstavio je Reputacijsku društvenu mrežu, decentralizirani protokol koji omogućuje pseudonimnu, provjerljivu razmjenu reputacije. Načelo skupog radikalizma osigurava da se prijevarne tvrdnje isključe cijenom bez cenzure. Predloženi put mi-

gracije omogućuje postupnu, reverzibilnu tranziciju od postojećih institucija. Dizajn ugrađuje ljudsku prirodu kakva jest—uključujući sitničavost, pakost i želju za osvetničkim zadovoljstvom—umjesto da zahtijeva ideološku transformaciju. Rezultat nije utopija, već sustav u kojem je pravda dostupna, reputacija se zarađuje, a trošak nedoličnog ponašanja snosi strana koja ga je uzrokovala.

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.