

# Decentralizirano omrežje ugleda: Ogrodje za naravno družbeno organizacijo

Pavel Kudrna  
Praga, Češka  
Osutek v1 — marec 2026

## Abstract

Občutek za pravičnost—prepričanje, da so krivice popravljene in zasluge nagrajene—je najmočnejša povezovalna sila družbe. Ko središčne institucije upravljanja ne morejo zagotoviti tega občutka, ker strošek uveljavljanja pravice presega vrednost same pravice, se družbena kohezija razkrajja. Sedanje institucionalne strukture ne zmorejo razrešiti pomembnega razreda sporov na sistematično enak način, kot centralno planiranje ne zmore razporejati virov: prek informacijske asimetrije, manjkajočih povratnih zank in ločenosti odločevalcev od posledic njihovih odločitev. Ta prispevek predstavlja družbeno omrežje ugleda (Reputation Social Network, RSN): decentralizirano, nepodkupljivo, cenzuri odporno komunikacijsko plast, zgrajeno na decentraliziranih identifikatorjih (DID), ki psevdonimnim udeležencem omogoča objavlanje, preverjanje in uporabo informacij o ugledu glede vedenja v resničnem svetu. Osrednji mehanizem sloni na treh načelih zasnove: (1) na asimetrični strukturi stroškov, kjer je branje podatkov o ugledu poceni, pisanje pa zahteva preverljiv trud; (2) na nedeterminističnem protokolu izbire preverjevalcev, ki temelji na konsistentnem razpršilnem preslikavanju (consistent hashing) in ovrednoti radikalne trditve prek naraščajočih stroškov iteracij; in (3) na tržno gnanem modelu avtoritete ugleda, kjer zasebni preverjevalci vlagajo svoj nakopičeni ugled na točnost trditve, ki jih potrjujejo. Nastala arhitektura ustvarja porajajočo se meritokracijo brez središčne koordinacije in omogoča postopno, povratno pot preseljevanja iz obstoječih državno upravljanjih sistemov.

## 1 Uvod

### 1.1 Problem središčnega zaupanja

Sodobno upravljanje sloni na temeljni predpostavki: da lahko središčne institucije posredujejo zaupanje med neznanci v velikem obsegu. Sodišča razsojajo

spore. Registri potrjujejo lastništvo. Regulatorna telesa uveljavljajo standarde. Te institucije so bile zasnovane v obdobju, ko so bile informacije redke, komunikacija počasna in prenos pooblastil na središčno telo edini izvedljiv mehanizem usklajevanja. Središčno upravljanje pa odpove iz istih strukturnih razlogov kot centralno planiranje: zaradi informacijske asimetrije, manjkajočih povratnih zank in ločenosti odločevalcev od posledic njihovih odločitev.

Predpostavka odpove na primer takrat, ko strošek institucionalnega posredovanja presega vrednost spora. Vzemimo najemnika, ki odkrije, da njegovemu najetemu stanovanju manjka zakonsko zahtevano potrdilo o električni varnosti—stanje, ki neposredno ogroža življenje. Zakonska pravica najemnika do odstopa od pogodbe je nedvoumna. Vendar strošek uveljavljanja te pravice prek sodnega sistema presega denarno vrednost varščine in dolgovane odškodnine, tudi če upoštevamo morebitno zakonsko nadomestilo [1]. Racionalen odziv je, da izgubo prevzame nase in odide.

To ni patološki robni primer. To je privzeta izkušnja za pomemben razred sporov, v katerih je škoda resnična, denarni vložki pa padejo pod prag, pri katerem postane institucionalno uveljavljanje ekonomsko racionalno. Rezultat je sistem, ki strukturno daje prednost slabim akterjem: tisti, ki škodujejo drugim v obsegu pod tem pragom, lahko ravnajo nekaznovano, ker strošek iskanja pravice pade na oškodovano stran.

Zgornji primer je vzet iz avtorjevega pravnega okolja—češkega sistema civilnega prava. V drugih pravnih izročilih—precedenčnem običajnem pravu (common law), običajskem pravu, mešanih sistemih—pravičnost odpove na drugačne načine in v drugačni meri, odvisno od kulturnih in postopkovnih posebnosti pravnega reda. Bralci bodo verjetno prepoznali enakovredne primere iz svojega konteksta. Kar je strukturno univerzalno, je vzorec: spori, katerih vrednost pade pod prag ekonomsko racionalnega uveljavljanja, se končajo tako, da izgubo prevzame oškodovana stran. RSN ne obljublja popolne

pravičnosti—zgolj zmanjšuje strukturno prednost, ki jo slabi akterji uživajo, ko institucionalno uveljavljanje ni ekonomično.

## 1.2 Zakaj obstoječe rešitve ne zadostujejo

**Ogrodja decentralizirane identitete (DID)** [2] zagotavljajo kriptografske mehanizme za samosuvereno upravljanje identitete, a se osredotočajo predvsem na preverjanje identitete, ne da bi obravnavala širše vprašanje vedenjskega ugleda.

**Žetoni, vezani na dušo (Soulbound Tokens, SBT)** [3] zajemajo uvid, da je ugled neprenosljiv, a se opirajo na infrastrukturo veriženja blokov s skalabilnostnimi omejitvami in ne obravnavajo ekonomskih spodbud, ki urejajo vnos informacij. Sorodni koncepti, kot so žetoni zaslug (npr. *Liberland*), imajo podobno filozofijo, a ostajajo vezani na določena jurisdikcijska ogrodja.

**Decentralizirane avtonomne organizacije (DAO)** [4] uveljavljajo upravljanje prek pametnih pogodb, a ponavljajo plutokratsko dinamiko, kjer je vpliv sorazmeren kapitalu. Kvadratno glasovanje [5] to delno omili, a omejuje praktično uveljavitev. DAO se soočajo tudi s temeljnim *problemom oraklja*: pametne pogodbe ne morejo zanesljivo preveriti stanj v resničnem svetu brez zaupanja vrednega zunanjega vira, ta problem pa nima splošne rešitve znotraj arhitekture veriženja blokov.

Noben obstoječi sistem ne združuje decentralizacije, odpornosti proti cenzuri, psevdonimnosti, preverljivega stroška vstopa in porajajočega se soglasja.

## 1.3 Prispevki

Ta prispevek prinaša naslednje prispevke:

1. Opredelitev **družbenega omrežja ugleda (RSN)**, decentraliziranega protokola, ki razširja ogrodje DID za podporo dvostranske izmenjave ugleda.
2. **Nedeterministični protokol izbire preverjevalcev**, ki temelji na konsistentnem razpršilnem preslikavanju [6].
3. **Načelo dragega radikalizma**, ki ovrednoti trditve glede na njihovo oddaljenost od omrežnega soglasja prek treh sestavljajočih se kanalov stroškov.
4. **Model ugledne avtoritete** z asimetričnimi spodbudami, kjer lažna potrditev stane katastrofalno več kot legitimne pristojbine.
5. **Postopno pot preseljevanja** prek vzporedne fiskalne infrastrukture.

## 2 Načela zasnove

Arhitekturo RSN omejuje pet nepogajljivih načel zasnove.

**Kontinuiteta in evolucija.** Sistem soobstaja z obstoječimi institucijami v prehodnem obdobju nedoločenega trajanja. Prehod mora biti na vsaki stopnji povraten.

**Prostovoljnost in odgovornost.** Udeležba je prostovoljna, a je prostovoljnost sklopljena z odgovornostjo: udeleženec, ki prevzame nadzor nad institucionalno funkcijo, hkrati prevzame spremljajoče obveznosti.

**Raznolikost in kulturna nevtralnost.** Soglasje se poraja iz dvostranskih interakcij, ne iz vnaprej določenih pravil, ki jih vsiljujejo snovalci sistema.

**Odpornost in odpornost proti cenzuri.** Strošek cenzuriranja omrežja mora presežati strošek njegovega prenašanja. Le popolni totalitarizem—ob rušilnih političnih in ekonomskih stroških—lahko sistem zatre.

**Soglasje in uveljavljanje.** Sistem vgrajuje človeška nagnjenja k malenkostnosti, kljubovalnosti in maščevalnemu zadovoljstvu kot nosilne značilnosti. Neustrezno ravnanje ni prepovedano; je ovrednoteno.

## 3 Pregled sistema

### 3.1 Družbeno omrežje ugleda

RSN je decentralizirana komunikacijska plast neposredne (peer-to-peer) izmenjave, v kateri udeleženci izmenjujejo preverljive informacije o vedenju v resničnem svetu. Njegove opredeljujoče lastnosti so: decentralizirana in necenzurabilna infrastruktura; psevdonimna udeležba prek DID; asimetrična struktura stroškov (branje je poceni, pisanje drago); kriptografska preverljivost; ter **podpora standardom**—strojno berljivi formati za informacije, ki se širijo skozi omrežje, za storitve, ki jih ponujajo avtoritete (sestavljanje trditev, potrjevanje, priča kot storitev), in za format politike, vključno s pravili za vrednotenje ugleda nasprotne stranke ter ocenjevanje tveganja neujemanja politike (med prijavljenim in dejanskim vedenjem).

### 3.2 Arhitekturne komponente

RSN sestavljajo štiri glavne komponente (sl. 1):

1. **Plast DID.** Identitete udeležencev s prijavljenimi pravili, metapodatki o ugledu in usmerjanjem po omrežju.

2. **Protokol trditve.** Strukturiran format za objavljanje navedb o dogodkih v resničnem svetu.
3. **Preverjevalno omrežje.** Decentraliziran protokol za dodeljevanje preverjevalcev z uporabo konsistentnega razpršilnega preslikavanja.
4. **Plast združevanja ugleda.** Storitve, ki proizvajajo človeku berljive povzetke ugleda.

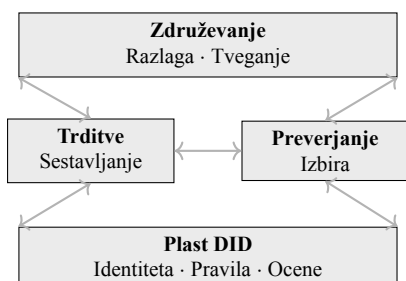


Figure 1: Štiriplastna arhitektura RSN.

### 3.3 Vloge udeležencev

Preverjevalna transakcija vključuje do šest različnih vlog DID (sl. 2): **Izdajatelj** ( $DID_I$ , ustvari in odda trditve), **Subjekt** ( $DID_S$ , DID, na katerega se trditev nanaša—lahko sovpada z izdajateljem), **Avtoriteta** ( $DID_A$ , potrdi trditev za pristojbino; lahko ponuja tudi storitve priče—*neobvezno*), **Priča** ( $DID_{W_{1..n}}$ , prikriti nadzornik poštenosti preverjevalca prek izzivnih kod—*neobvezno*), **Preverjevalec** ( $DID_V$ , algoritmično izbran za objavo trditve) in **RSN** (omrežje, kjer se objavijo preverjene trditve). Vsako vlogo je mogoče prenesti na drug DID (razdelek 7.4). Avtoriteta pogosto združuje potrjevanje s storitvami priče, a sta funkciji logično neodvisni.

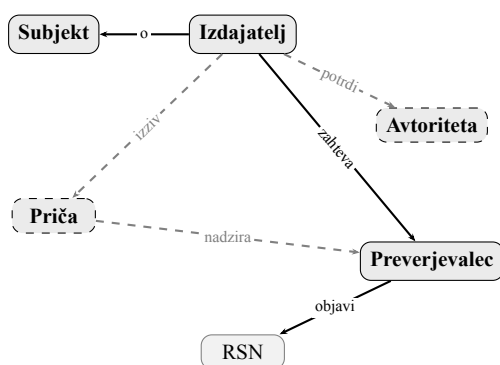


Figure 2: Vloge DID v preverjevalni transakciji. Črtkano = neobvezno (Avtoriteta, Priča).

### 3.4 Nepodkupljivost: štiri sile

Nepodkupljivost RSN ne izhaja iz enega samega mehanizma, temveč iz štirih sočasnih sil. Nobena sama

zase ne zadostuje; šele njihova kombinacija naredi poskus podkupovanja ekonomsko neracionalen.

**Nepredvidljiva tarča.** Preverjevalec za vsako trditev je izbran nedeterministično prek konsistentnega razpršilnega preslikavanja (razdelek 5.3). Napadalec ne more vnaprej izbrati določenega preverjevalca za podkupovanje, ker je preverjevalčeva identiteta funkcija vsebine trditve in prejšnjih iteracij, ne pa izbire izdajatelja.

**Vzvod ugleda—počasi gor, hitro dol.** Ugled je mogoče pridobivati le postopoma, prek vztrajno doslednega vedenja. Izgubiti pa ga je mogoče katastrofalno v enem samem goljufivem potrjevanju (razdelek 6.2). Ta asimetrija pomeni, da lahko leta nakopičenega ugleda uniči eno samo nepošteno potrjevanje; optimalna strategija ostaja zavračanje sumljivih trditve.

**Javna obljuba.** Vsak imetnik DID javno prijavi svojo politiko—strojno berljiv niz pravil, ki se jim zaveže slediti. Razhajanje med prijavo in dejanskim vedenjem je zaznavno in ovrednoteno kot prekršek zoper ugled, hujši od temeljne kršitve (razdelek 7.3). Hinavščina je torej dražja od neposredne nepoštenosti.

**Asimetrija stroškov napada na mrežo.** Strošek cenzuriranja ali destabilizacije omrežja narašča nelinearno z velikostjo in gostoto omrežja, medtem ko strošek njegovega prenašanja ostaja konstanten. Da bi se cenzura izplačala, bi jo moral središčni akter uveljaviti čez celotno omrežje—kar zahteva ukrepe, nesorazmerne z vsako predstavljivo koristjo (razdelek 10).

## 4 Model decentralizirane identitete

### 4.1 DID s posebnimi lastnostmi

RSN razširja specifikacijo W3C DID Core [2] z: **prijavljenimi pravili** (strojno berljive vedenjske zaveze), **metapodatki o ugledu** (združena vedenjska ocena) in **usmerjanjem po omrežju** (spremenljiv čebulni prehod, ločen od stabilnega položaja na obroču).

### 4.2 Življenjski cikel trditve

Trditev poteka skozi šest stopenj (sl. 3): sestavljanje, neobvezno potrjevanje s strani avtoritete, izbira preverjevalca prek konsistentnega razpršilnega preslikavanja, odločitev o preverjanju (sprejem ali zavrnitev z iteracijo), objava in posodobitev ugleda za vse stranke.

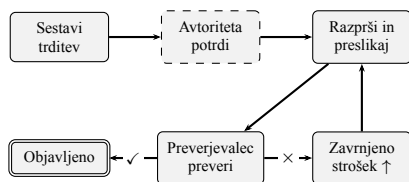


Figure 3: Življenjski cikel trditve z iteracijsko zanko.

### 4.3 Razmerje do W3C DID Core

Model identitete RSN je pravi nadmnožica specifikacije W3C DID Core [2]. Vsi DID v RSN so veljavni DID po W3C. Razširitve, specifične za RSN, so zakodirane kot lastnosti dokumenta DID, opredeljene v namenski specifikaciji metode DID, združljive z obstoječo infrastrukturo, kot sta ION [7] in Ceramic [8].

## 5 Preverjanje in širjenje informacij

### 5.1 Strošek vnosa informacij

Osrednje ekonomsko načelo RSN je asimetrija med branjem in pisanjem. Branje podatkov o ugledu se za udeležence, ki so del omrežja DID in imajo dostop, sorazmeren z njihovim ugledom, približuje ničelnemu mejnemu strošku—novinci si morajo širši dostop postopoma prislužiti (glejte protileeching). Pisanje—razumljeno kot trajno udejanjanje ugleda v omrežju, ne kot enkratno tehnično dejanje—zahteva preverljivo nakopičeno vlaganje v treh razsežnostih: **čas** (leta življenja, porabljena za dosledno vedenje, izpolnjene zaveze in negovane odnose), **energija** (trud, vložen v pošteno ravnanje, skrb za partnerstva in dolgoročno zanesljivost) in **denar** (vlaganje v lastno ime—strokovni razvoj, kakovost lastnega dela, poravnava za povzročeno škodo). Ugleda ni mogoče kupiti v hipu—je izid vseživljenjskega kopičenja, ki ga sistem zgolj naredi vidnega in prenosljivega med konteksti. Enkratni tehnični stroški protokola (kriptografski podpisi, pristojbine preverjevalcev) so zanemarljivi v primerjavi s tem temeljnim vlaganjem.

### 5.2 Družbeni graf in globina stikov

RSN je v temelju družbeno omrežje: vsak DID dodaja stike (druge DID), ki povezavo dovolijo. Ti stiki imajo svoje stike in tako naprej. Algoritmično iskanje preverjevalcev deluje znotraj nastavljenih globine  $h$  povezanih stikov (npr.  $h = 3$ : neposredni stiki, njihovi stiki in stiki stikov). Ta arhitektura ne zahteva ene same globalne verige blokov—naravno spodbuja nastanek skupnosti/gruč s prekrivanji v druge skupnosti. Vsak udeleženec DID mora imeti objavljeno

**politiko**—strojno berljiv niz pravil, ki urejajo, kako se vrednotijo dohodne zahteve. Kršitve politike se v omrežju zabeležijo kot negativni artefakti.

### 5.3 Algoritmična izbira preverjevalca

Preverjevalni protokol uporablja konsistentno razpršilno preslikavanje [6] (sl. 4). Preverjanje je plačljiva storitev: preverjevalci delujejo za pristožbino, kar ustvarja trg, kjer konkurenca oblikuje ceno, hitrost in zanesljivost.

**Korak 1.** Dokument trditve se združi z rezultatom razpršitve prejšnje iteracije (ali  $\emptyset$  pri prvi iteraciji) in razprši:

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

Algoritem mora vključevati *celotno pot* vseh prejšnjih zahtev in odgovorov—ne le razpršitve prejšnje iteracije. Celoten odgovor vsakega preverjevalca (sprejem, zavrnitev, ponujena cena, razlog) se pripne rastočemu dokumentu, preverljivo prek kriptografskih podpisov na vsakem koraku.

**Korak 2.** Razpršitev se preslika na  $N$  položajev na obroču konsistentnega razpršilnega preslikavanja, enakomerno razporejenih (npr. za  $N = 4$ :  $+0^\circ, +90^\circ, +180^\circ, +270^\circ$ ). Iz vsakega položaja iskanje v smeri urnega kazalca izbere najbližji DID kot kandidata za preverjevalca (sl. 5).  $N$  je spremenljiv parameter, ki je lahko odvisen od odstotka trenutno aktivnih DID, časa v dnevu ali pretekle odzivnosti omrežja.

**Korak 3.** Preverjevalec sprejme (objavi in vloži ugled) ali zavrne (vrne se na korak 1 z razpršitvijo zavrnitve). Ko vozlišče ne odgovori kljub prijavljenemu stanju povezanosti, mora naslednja zahteva vključevati vse odgovore vseh  $N$  prejšnjih kandidatov za preverjevalca.

**Protileeching.** Ciljni DID lahko določijo pristojbine ali omejitve dostopa za poizvedbe novih DID z malo ugleda. Ta stopnjevani mehanizem (ne binaren) sili novince, da si zgradijo ugled prek pristne dejavnosti, preden lahko prosto uporabljajo podatke drugih.

Vsaka zavrnitev pripne celoten odgovor preverjevalca (vključno z razlogi in pogoji) dokumentu trditve in razširi njegovo vsebino. Iz razširjenega dokumenta se nedeterministično izračuna nova razpršitev, ki se preslika na drug položaj na obroču in izbere drugega preverjevalca. Dokumentiranje celotne poti je obvezno—izdajatelj ne more predvideti ali vplivati na naslednjega preverjevalca. Če preverjevalec zanemari zahtevo kljub združljivi prijavljeni politiki, priče (če

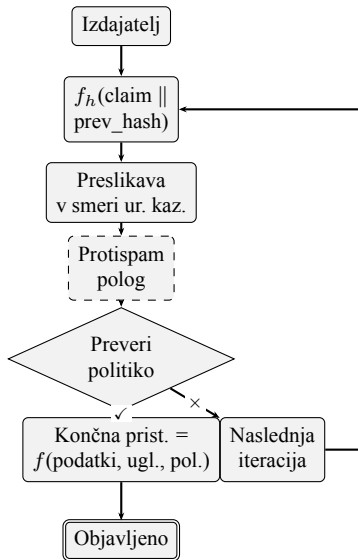


Figure 4: Protokol izbire preverjevalca. Protispam polog je neobvezen in je lahko vračljiv. Končna pristojbina se plača le ob sprejemu.

so prisotne) to zabeležijo, izdajatelj pa lahko ob končni objavi priloži dokaze prič.

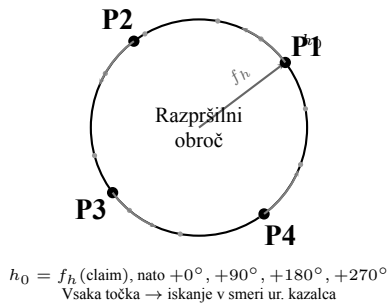


Figure 5: Večtočkovna izbira ( $N=4$ ). Razpršitev  $h_0$  določi odmik; 4 točke enakomerno razporejene od  $h_0$ .

## 5.4 Protokol priče

Vloga **priče** zagotavlja prikrito odgovornost za poštenost preverjevalca prek kriptografskega protokola izzivnih kod:

**Korak W1.** Prosilec podpiše preverjevalno zahtevo in jo pošlje  $N_w$  pričam—stikom iz proslilčevega družbenega omrežja ali specializiranim ponudnikom storitve priče, ki delujejo za pristojbino.

**Korak W2.** Vsaka priča  $w_i$  podpiše celotno podpisano zahtevo, obdrži izvirni podpis  $\sigma_i$  in izračuna izzivno kodo  $c_i = h(\sigma_i)$ . Izzivna koda se pripne zahtevi.

**Korak W3.** Zahteva, ki zdaj nosi  $N_w$  izzivnih kod, se pošlje preverjevalcu. Preverjevalec opazi kode, a ne more ugotoviti, kdo so priče ali ali kode ustrezajo

resničnim podpisom.

**Korak W4 (pošten preverjevalec).** Če se preverjevalec odzove v skladu s svojo prijavljeno politiko, izzivne kode ostanejo neprozorne. Priče niso nikoli razkrite. Nobeni dodatni podatki niso objavljeni.

**Korak W5 (kršitev politike).** Če preverjevalec krši svojo politiko (zanemari zahtevo, se odzove nedosledno), prosilec drži izvirne podpise prič  $\sigma_i$ . Te je mogoče objaviti kot spremljajoče podatke: vsakdo lahko preveri  $c_i = h(\sigma_i)$  in tako dokaže, da je bila priča prisotna. Prosilec lahko objavi neodvisno—preverjevalec je izzivne kode v svojem odgovoru že podpisal.

**Lastnost blefiranja.** Prosilec lahko nekatere ali vse izzivne kode nadomesti z naključnimi vrednostmi. Preverjevalec ne more razločiti pristnih kod (podprtih z avtoritetami visokega ugleda) od šuma. Ta *negotovost* je mehanizem uveljavljanja: vsaka zahteva nosi tveganje, da spoštovana avtoriteta opazuje prikrito. Strošek vzdrževanja tega pritiska je skoraj nič (ustvarjanje naključnih števil), medtem ko je potencialni strošek nepoštenosti za preverjevalca katastrofalen. Pošteno vedenje je spodbujeno tudi v odsotnosti dejanskih prič.

**Avtoriteta kot priča.** Avtoriteta, ki potrdi trditev, lahko združi storitve priče: „Potrjujem tvojo trditev in med preverjanjem služim kot prikrita priča.“ To je naraven poslovni model—avtoriteta že ima kontekst. Vlogi pa sta logično neodvisni.

## 5.5 Načelo dragega radikalizma

Trije kanali stroškov se stopnjujejo sočasno (sl. 6):

**Kanal 1: Strošek iteracije.** Vsaka zavrnitev sili novo iteracijo, ki porablja čas in vire. Linearna rast.

**Kanal 2: Napihovanje dokumenta.** Vsaka iteracija dokumentu trditve doda celoten odgovor preverjevalca. Rast je linearna, a z izhodišnim odklom: začetna vsebina (vsebina trditve, potrditev avtoritete, kriptografski podpisi) že ima netrivialno velikost  $B_0$ . Skupna velikost po  $k$  iteracijah:  $S(k) = B_0 + k \cdot \Delta$ , kjer je  $\Delta$  povprečna velikost odgovora.

**Kanal 3: Tveganjska premija preverjevalca.** Tveganje je subjektivno. Preverjevalec presoja, ali prijavljene politike prosečega DID nasprotujejo lastnim komercialnim, družbenim ali političnim interesom preverjevalca. Premija se lahko stopnjuje eksponentno z zaznano oddaljenostjo od preverjevalčevega „ideala“:  $P(d) = \alpha \cdot e^{\beta d}$ , kjer je  $d$  subjektivna mera oddaljenosti preverjevalca. Onkraj osebne meje nesprejemljivosti lahko preverjevalec v celoti zavrne.

Ključno je, da to ni cenzura. Nobena trditev ni pre-

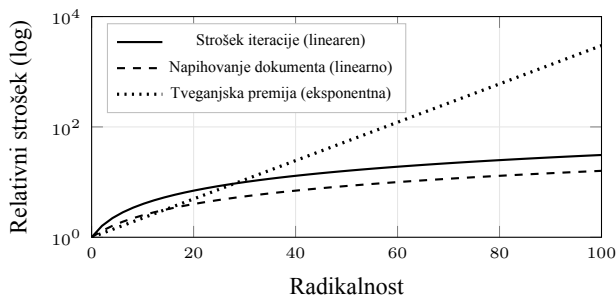


Figure 6: Stopnjevanje stroškov po treh kanalih. Tveganjska premija prevlada pri visoki radikalnosti.

povedana. Sistem ovrednoti tveganje (tabela 1).

Table 1: Primerjava stroškov glede na tip trditve.

| Tip          | Iter.                | Dok.            | Prist.               | Skupaj       |
|--------------|----------------------|-----------------|----------------------|--------------|
| Verodostojna | $k_{\min}$           | $B_0$           | $P_{\min}$           | Nizko        |
| Sporna       | $k_{\text{med}}$     | $B_0 + k\Delta$ | $\alpha e^{\beta d}$ | Zmerno       |
| Radikalna    | $k_{\max}$           | $\gg B_0$       | $\gg P_{\min}$       | Zelo visoko  |
| Goljufiva    | $\rightarrow \infty$ | —               | —                    | Neobjavljiva |

## 6 Ugled in ocena tveganja

### 6.1 Model kopičenja ugleda

Ugled izkazuje tri lastnosti: **počasno kopičenje** (postopna rast prek doslednega vedenja), **hitro uničenje** (ena sama goljufija lahko oceno katastrofalno zniža) in **individualno vrednotenje** (vsaka uporabniška stran lahko uporabi svojo funkcijo združevanja).

### 6.2 Ugledne avtoritete

Ugledna avtoriteta pregleda trditve in jih, če je zadovoljna, sopodpiše—pri čemer vloži svoj lastni ugled (sl. 7). Asimetrija je namerna: pridobivanje ugleda je počasno (postopno  $+\delta$  na pošteno potrditev), medtem ko je izguba katastrofalna ( $-\Delta \gg \delta$  na lažno potrditev; ponazoritveno npr.  $+2\%$  proti  $-70\%$ ). Optimalna strategija je vedno zavrniti sumljive trditve. Konkretni vrednosti  $\delta$  in  $\Delta$  sta parametra sistema.

### 6.3 Večrazsežnostni ugled

Ugled ni skalar, temveč vektor čez več razsežnosti: finančna zanesljivost, osebna integriteta, strokovna usposobljenost, državljanska angažiranost in druge (sl. 8). Različni ponudniki vrednotenja ta vektor projicirajo različno glede na kontekst—posojilodajalec daje prednost finančni zanesljivosti, delodajalec strokovni

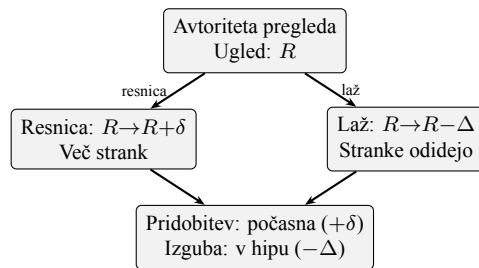


Figure 7: Ugledna avtoriteta—asimetrične spodbude.

usposobljenosti, sosed državljanškemu vedenju. Ni ene same „pravilne“ ocene ugleda; le perspektive.

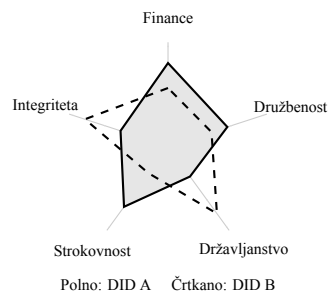


Figure 8: Večrazsežnostni vektorji ugleda. Različni DID izkazujejo različne profile čez razsežnosti.

## 6.4 Demokratizirana ocena tveganja

RSN demokratizira sistematično ocenjevanje tveganja—zmožnost, ki je trenutno skoncentrirana v finančnih institucijah, a uporabna daleč onkraj bančništva. Industrijski konglomerati, ki ocenjujejo zanesljivost dobaviteljev, zavarovalnice, ki ovrednotijo vedenjsko tveganje, skrbni pregledi pri združitvah in prevzemih, ocena življenjske dobe opreme v proizvodnji—povsod, kjer je treba oceniti tveganje nasprotne stranke, RSN ponuja decentralizirano, tržno gnano alternativo. Trg storitev razlaga prevaja surove večrazsežnostne podatke o ugledu v uporabne povzetke, s čimer postane vrednotenje nasprotne stranke dostopno vsakemu udeležencu ob mejnem strošku.

## 7 Soglasje in razreševanje sporov

### 7.1 Model decentralizirane pravičnosti

RSN preokvirja pravičnost kot problem dvostranskega pogajanja. Grožnja trajne, preverljive škode ugledu je učinkovitejše odvrčalo kot sodni postopek, ki si ga oškodovana stran ne more privoščiti.

## 7.2 Porajajoče se soglasje

Vsak udeleženec vzdržuje osebni prag zadovoljstva. Skupno soglasje omrežja se poraja kot statistično povprečje tisočev dvostranskih pogajanj (sl. 9). Odziv daleč nad soglasjem (barbarski) je drag za objavo. Odziv blizu soglasja (sorazmeren) je poceni. Soglasje ni pravilo—je cenovni signal.

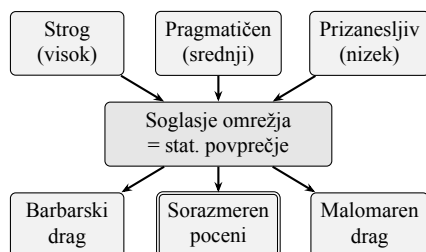


Figure 9: Porajajoče se soglasje iz individualnih pragov zadovoljstva.

## 7.3 Umerjanje kaznovanja

Vsak imetnik DID javno prijavi odzive na določene kategorije neustreznega ravnanja. Nesorazmerno ostre ali mile prijave privlačijo negativne signale ugleda. Sorazmerne prijave so sprejete brez trenja—samoumerjajoč se sistem kaznovanja.

Prijave soglasja so tudi same predmet zaznavanja hinavščine: deklarativna zaveza k položaju soglasja ob nedoslednem ravnanju pomeni prekršek zoper ugled, hujši od temeljnega odklona, saj izkazuje namerno prevaro.

## 7.4 Prenos pooblastil

Vse dejavnosti znotraj DID—z eno izjemo—je mogoče prenesti na drug DID. **Vloge subjekta—DID, katerega vedenja se trditev tiče—ni mogoče prenesti; neprenosljivo je vezana na imetnika identitete, na katerega se trditev nanaša.** Druge dejavne vloge—izdajatelj, avtoriteta, priča, preverjevalec—je mogoče prenesti na določen pooblaščen DID, bodisi za preverjanje, oddajo trditve, udeležbo v soglasju ali razreševanje sporov. Prenos pooblastil je kadar koli preklicljiv. To omogoča specializacijo (npr. profesionalne preverjevalne storitve), medtem ko imetnik obdrži končni nadzor in odgovornost. Prenos pooblastil velja za celoten sistem in je bistven za skalabilnost.

## 7.5 Od individualne moralnosti do porajajoče se družbene pogodbe

Prijavljena politika vsakega DID predstavlja formalizacijo individualne moralnosti: kaj imetnik šteje za sprejemljivo, kako se odziva na določena vedenja, kaj zahteva od nasprotnih strank. Teh politik ne vsili snovalec sistema—izbere jih vsak udeleženec in jih izrazi v strojno berljivi obliki.

Ta formalizacija omogoča troetapno porajanje. Prvič, individualna moralnost je zakodirana kot **politika**—niz prijavljenih pravil, pragov in odzivnih funkcij, ki se jim DID zaveže slediti. Drugič, skuppek vseh politik po omrežju proizvede **porajajočo se etiko**—statistično opazljive norme, ki jih ni zasnoval noben posamezen udeleženec, a nastanejo iz interakcije tisočev individualnih moralnih stališč [9]. Tretjič, ta porajajoča se etika, izražena kot skupne vedenjske norme, uveljavljene prek dvostranskih cenovnih signalov, sestavlja **merljivo družbeno pogodbo**—ne teoretičnega konstrukta, ki ga ni nihče podpisal [10], temveč empirično opazljiv niz pravil, podprt z dejanskim vedenjem.

Ta proces zrcali ugotovitve teorije moralnih temeljev [11]: človeška moralnost je intuitivna, pluralistična in kulturno spremenljiva. RSN ne zahteva moralnega soglasja kot vhoda; kot izhod proizvede vedenjsko soglasje. Nastala družbena pogodba ni statična—razvija se, ko se udeleženci pridružujejo, odhajajo in prilagajajo svoje politike v odziv na povratne informacije omrežja. Za razliko od klasične teorije družbene pogodbe je ta pogodba preklicljiva, opazljiva in izvršljiva brez suverena.

## 8 Ekonomski model

Prejšnji razdelki so opisali orodje—preverjevalne mehanizme RSN, strukturo stroškov in porajajoče se soglasje. Ta razdelek opisuje metodologijo za uporabo tega orodja pri fiskalnem in upravljavskem prehodu. Orodje je splošnonamensko; spodnja metodologija je ena od mogočih uporab.

### 8.1 Struktura spodbud

Ugled kot kapital ustvarja neposredne spodbude za pošteno vedenje. V normalnem delovanju udeleženci gradijo ugled naravno, prek vsakdanjih transakcij in izpolnjenih zavez. Glavni izdatek je za *negativne* trditve—beleženje škode, ki jo povzročijo drugi. Ta asimetrija spodbuja koristno, zanesljivo vedenje: biti pošten ne stane nič dodatnega, medtem ko škodljivost

ustvari dokumentirano sled, ki jo bodo drugi plačali, da jo ohranijo. Hinavščina—prijava pravil brez njihovega upoštevanja—je najdražji način odpovedi, saj izkazuje namerno prevaro.

## 8.2 Vzporedni fiskalni sistem

Trije sestavni deli omogočajo konkurenčni pritisk: (1) **enostavni davek**—enotna proporcionalna stopnja brez izjem, sprva rahlo pod obstoječo dejansko stopnjo; (2) **elektronska registracija porabe (ERP)**—obrat češkega modela EET, tako da državljani nadzirajo državne izdatke; (3) **državlansko usmerjena razporeditev davkov**—začne se pri nekaj odstotkih v prvem letu in po desetletju doseže kjer koli od nizkih dvomestnih vrednosti do popolne preselitve v državljansko usmerjen sistem, odvisno od hitrosti sprejemanja. Dejanski tempo je odvisen od hitrosti, s katero nastajajo prostotržne alternative državnim storitvam, in od pripravljenosti države, da sodeluje pri prehodu; funkcija časa ni nujno linearna, in ni razloga za določitev zgornje meje, kam sprejemanje sčasoma lahko prispe.

## 9 Pot preseljevanja

Preseljevanje poteka skozi tri faze (sl. 10): **faza 1: prekrivanje** (RSN kot informacijska plast, država je edini ponudnik), **faza 2: konkurenca** (RSN ponuja funkcionalne alternative, dvojna raba sistema) in **faza 3: prehod** (RSN prekaša državne enakovrednike, prostovoljno preseljevanje). Prehod je na vsaki stopnji povraten.

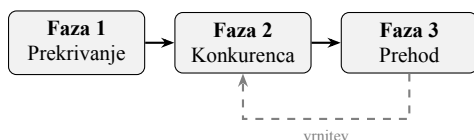


Figure 10: Trifazno preseljevanje—povratno na vsaki stopnji.

Glavni pritiskovni mehanizem je fiskalen: ko pogojni davkoplačevalci dosežejo „ekonomsko pomembno manjšino  $X$ “—skupino, dovolj veliko, da represija proti njej povzroči netrivialno ekonomsko škodo in državljanska nepokorščina postane verodostojna grožnja—država vstopi v pogajanja. Za ponazoritev uporabljamo  $X \approx 15\%$  BDP, a dejanski prag je odvisen od konkretnega gospodarstva.

## 10 Varnostna analiza

Obravnavamo pet kategorij nasprotnikov: posamezne slabe akterje, organizirane skupine, korporacijske nasprotnike, nasprotnike na ravni države in nasprotnike na ravni protokola.

**Odpornost proti sibilskim napadom** [12]. Gradnja ugleda zahteva vztrajno, preverljivo interakcijo. Strošek uspešnega sibilskega napada narašča linearno s številom lažnih identitet in kvadratno s ciljno ravtnjo ugleda. Vzoredno upravljanje več DID je mogoče, a je namerno drago—vsaka identiteta mora neodvisno nakopičiti ugled prek pristne dejavnosti. V svobodnih družbah ta strošek odvrta priložnostno zlorabo; v diktaturah vzoredni DID postanejo orodje preživetja, ki omogoča predelčeno upiranje, podtalno usklajevanje in varnejše krmarjenje po črnem trgu.

**Obramba pred dogovarjanjem (kolizijo)**. Vzorci vzajemnega potrjevanja med zaprtimi skupinami so zaznavni z analizo družbenega grafa. Funkcije združevanja ugleda razvrednotijo trditve iz tesno zgruču<PLACEHOLDER>enih virov.

**Nasprotnik na ravni države**. Čebulno usmerjanje, odsotnost središčne infrastrukture in porazdelitev vloge preverjevalca po celotni bazi udeležencev zagotavljajo, da zatiranje zahteva ukrepe, nesorazmerne s katero koli koristjo.

**Zasebnost proti odgovornosti**. Pseudonimnost—srednja pot med anonimnostjo in razkritjem identitete—omogoča, da DID nakopičijo pomenljiv ugled, ne da bi razkrili imetnikovo identiteto v resničnem svetu.

## 11 Vidiki zasebnosti

Model zasebnosti RSN je zgrajen na pseudonimnosti. Imetnik nadzira razkritje identitete: minimalno (čist pseudonim), selektivno (povezani določeni poverilni podatki) ali polno (pridružena pravna identiteta). Objavljene trditve so trajne—sistem podpira kontekstualni popravek, ne pa izbrisa. Imetnik lahko opusti ogrožen DID in začne znova, pri čemer izgubi nakopičeni ugled.

## 12 Sorodno delo

Specifikacija W3C DID Core [2] in omrežje Ceramic [8] zagotavljata temelj identitete. EigenTrust [13] je pokazal porazdeljeno združevanje ugleda brez središčne avtoritete. SBT [3] so uvedli neprenosljive družbene žetone. RSN se razlikuje po

poudarku na ekonomskem strošku kot filtru kakovosti in po svojem mehanizmu za ovrednotenje radikalnosti.

DAO [4] in kvadratno glasovanje [5] so pokazali izvedljivost decentraliziranega upravljanja. RSN izpelje soglasje iz dvostranskih cenovnih pogajanj, ne iz glasovanja.

Predlog se opira na anarhokapitalistično teorijo [14, 15] za zasebno zagotavljanje storitev, a se od nje razhaja v dveh ključnih vidikih: zasnovan je za kljubovalnost in maščevalne vzgibe, namesto da bi predpostavljala racionalnost, in predlaga postopen prehod namesto revolucije. Koncept porajajočih se družbenih pogodb ima predhodnike v Hayekovi teoriji sponstanega reda [16].

**Anarhoagorizem.** RSN deli precej skupnega z agoristično protiekonomijo [17]—zlasti poudarek na gradnji vzporednih institucij in prostovoljni menjavi. Vendar agorizem teži k predpostavki racionalnega samointeresa kot zadostnega mehanizma usklajevanja in pogosto nima konkretne poti preseljevanja iz obstoječih državnih struktur. RSN izrecno vgrajuje neracionalna vedenjska nagnjenja in zagotavlja mehanizem fiskalnega pritiska za postopen prehod.

**Meritokracija.** RSN morda predstavlja prvi delujoč opis, kako lahko meritokracija [18] nastane kot sistemska lastnost, ne pa kot slogan. Tradicionalni meritokratski sistemi odpovedo, ker zahtevajo središčno avtoriteto, ki opredeli in uveljavi „zaslugo“. V RSN zasluga nastane iz dvostranskih vrednotenj: tisti, ki dostavljajo vrednost, kopičijo ugled; noben odbor ne odloča, kdo ima zaslugę.

**Lastnina kot privilegij.** RSN se v temelju razhaja z anarhokapitalistično in avstrijsko-šolsko obravnavo lastninskih pravic kot naravnih in absolutnih. V ogrodju RSN je lastnina *privilegij*—družbeno priznanje, ki ga skupnost lahko v skrajnih primerih odvzame, ko udeleženec temeljno krši skupne norme (izdaja, zavrnitev obrambe skupnosti v eksistencialni krizi, sistematično izkoriščanje). To ni državna razlastitev, temveč odvzem družbenega priznanja s strani omrežja dvostranskih odnosov.

## 13 Razprava in omejitve

**Hladen zagon.** Vrednost RSN je odvisna od omrežnih učinkov; zgodnji uporabniki se soočajo z omejeno vrednostjo, dokler udeležba ne doseže praga. Vendar že od zgodnjih stopenj omrežje DID služi kot koristen dopolnilni vir informacij. Pričakuje se, da se bosta zgodnje vrednotenje ugleda in ocenjevanje avtoritet postopoma razvijala z naraščajočo prefinjenostjo.

**Protileeching in nadzor dostopa.** Ciljni DID lahko uvedejo stopnjevane pristojbine in omejitve dostopa za poizvedbe iz DID z nizkim ugledom. To ni binarno, temveč zvezna lestvica: manj ugleda ima poizvedujoči DID, manj informacij prejme, dlje čaka in več plača. Ta mehanizem spodbuja pristno udeležbo pred pasivno potrošnjo.

**Neenakost dostopa.** Strošek objave trditev lahko odfiltrira legitimne pritožbe ekonomsko prikrajšanih udeležencev. Omilitev: vsak udeleženec hkrati služi kot potencialni preverjevalec (ali to vlogo prenese) in zasluži preverjevalne pristojbine. Čez zadostno časovno obzorje bi se neradikalni udeleženec moral približati finančni nevtralnosti—prihodki iz preverjanja približno izravnavajo stroške objave. To je statistično pričakovanje, ne jamstvo.

**Neenakost ugleda.** Zgodnji uporabniki nakopičijo prednosti, ki lahko ustvarijo ovire za pozne prišleke. Vendar vrednotenje ugleda izvajajo tretjeosebni ponudniki, ki lahko izberejo, da prednost prvega poteze omilijo prek svojih algoritmov združevanja. Biti prvi z dobrim ugledom je legitimna primerjalna ekonomska prednost—in to je namerno.

**Odprta vprašanja.** Optimalne funkcije stroškov, standardi združevanja, upravljanje protokola in interakcija s sintetičnimi podatki o ugledu, ustvarjenimi z UI, ostajajo področja za prihodnje delo.

Ta prispevek ne trdi, da bo RSN v vseh okoliščinah proizvedel optimalne izide. Trdi, da RSN predstavlja *izvedljivo* alternativo—tehnično uresničljivo, ekonomsko samovzdržno in družbeno združljivo s človeškimi vedenjskimi nagnjenji, kakršna dejansko so.

## 14 Sklep

Ta prispevek je predstavil družbeno omrežje ugleda, decentraliziran protokol, ki omogoča psevdonimno, preverljivo izmenjavo ugleda. Načelo dragega radikalizma zagotavlja, da so goljufive trditve cenovno izločene brez cenzure. Predlagana pot preseljevanja omogoča postopen, povraten prehod iz obstoječih institucij. Zasnova vgrajuje človeško naravo, kakršna je—vključno z malenkostnostjo, kljubovalnostjo in željo po maščevalnem zadovoljstvu—namesto da bi zahtevala ideološko preobrazbo. Rezultat ni utopija, temveč sistem, kjer je pravičnost dostopna, ugled prislužen in strošek neustreznega ravnanja nosi tista stran, ki ga je povzročila.

## 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.