Decentralizēts reputācijas tīkls: ietvars sabiedrības dabiskai organizācijai

Pavel Kudrna
Prague, Czechia
Draft v1 — March 2026

Abstract

Taisnīguma izjūta—pārliecība, ka netaisnības tiek labotas un nopelni atalgoti—ir spēcīgākais sabiedrības saliedēšanas spēks. Kad centralizētas pārvaldes institūcijas nespēj šo izjūtu nodrošināt, jo tiesību aizstāvēšanas izmaksas pārsniedz pašas tiesības vērtību, sabiedrības saliedētība kļūst vājāka. Pašreizējās institucionālās struktūras neatrisina nozīmīgu strīdu kategoriju sistemātiski tāpat, kā centrālā plānošana nespēj sadalīt resursus: caur informācijas asimetriju, trūkstošām atgriezeniskās saites cilpām un lēmumu pieņēmēju atrautību no savu lēmumu sekām. Šajā rakstā tiek prezentēts reputācijas sociālais tīkls (RSN): decentralizēts, nepiekukuļojams, cenzūrai izturīgs komunikācijas slānis, kas balstīts uz decentralizētiem identifikatoriem (DID) un kas ļauj pseidonīmiem dalībniekiem publicēt, verificēt un patērēt reputācijas informāciju par reālās pasaules uzvedību. Pamatmehānisms balstās uz trim projektēšanas principiem: (1) asimetriska izmaksu struktūra, kurā reputācijas datu lasīšana ir lēta, bet rakstīšanai nepieciešams verificējams pūliņš; (2) nedeterministisks verificētāju atlases protokols, kas balstīts uz konsekventu jaukšanu un kas rada radikālu apgalvojumu cenu caur pieaugošām iterāciju izmaksām; un (3) uz tirgu balstīts reputācijas autoritātes modelis, kurā privātie verificētāji ieliek uz spēles savu uzkrāto reputāciju par to apgalvojumu precizitāti, ko tie apstiprina. Iegūtā arhitektūra rada emerģentu meritokrātiju bez centrālas koordinācijas un dara iespējamu pakāpenisku, atgriezenisku migrācijas ceļu no esošajām valsts pārvaldītajām sistēmām.

1 Ievads

1.1 Centralizētas uzticēšanās problēma

Mūsdienu pārvalde balstās uz fundamentālu pieņēmumu: ka centralizētas institūcijas var starpniekot uzticēšanos starp svešiniekiem lielā mērogā. Tiesas izšķir strīdus. Reģistri apliecina īpašumtiesības. Regulatīvās iestādes uzrauga standartu ievērošanu. Šīs institūcijas tika izveidotas laikmetā, kad informācija bija reta, komunikācija lēna un pilnvaru deleģēšana centrālajai institūcijai bija vienīgais iespējamais koordinācijas mehānisms. Tomēr centralizēta pārvalde neizdodas to pašu strukturālo iemeslu dēļ kā centrālā plānošana: informācijas asimetrija, trūkstošas atgriezeniskās saites cilpas un lēmumu pieņēmēju atrautība no savu lēmumu sekām.

Pieņēmums neizdodas, piemēram, tad, kad institucionālās starpniecības izmaksas pārsniedz strīda vērtību. Iedomāsimies īrnieku, kurš atklāj, ka viņa īrētajam dzīvoklim trūkst likumā prasītā elektrodrošības sertifikāta—apstākļa, kas rada tūlītējus draudus dzīvībai. Īrnieka juridiskās tiesības atkāpties no līguma ir nepārprotamas. Tomēr šo tiesību aizstāvēšanas izmaksas caur tiesu sistēmu pārsniedz drošības naudas un pienākošos zaudējumu naudisko vērtību, pat ieskaitot iespējamo likumā noteikto kompensāciju [1]. Racionālā atbilde ir zaudējumu absorbēt un aiziet.

Šis nav patoloģisks izņēmuma gadījums. Tā ir noklusētā pieredze nozīmīgai strīdu kategorijai, kurā kaitējums ir reāls, bet naudiskā likme ir zem sliekšņa, no kura institucionālā aizstāvēšana kļūst ekonomiski racionāla. Rezultāts ir sistēma, kas strukturāli dod priekšroku ļaunprātīgiem dalībniekiem: tie, kas kaitē citiem apjomos zem šī sliekšņa, var rīkoties nesodīti, jo taisnīguma meklēšanas izmaksas gulstas uz cietušo pusi.

Iepriekšējais piemērs ir ņemts no autora tiesiskās vides—Čehijas civiltiesību sistēmas. Citās tiesību tradīcijās—uz precedentiem balstītajās vispārējās tiesībās, paražu tiesībās, jauktās sistēmās—taisnīgums neizdodas dažādos veidos un dažādā mērā atkarībā no jurisdikcijas kultūras un procesuālajām īpatnībām. Lasītāji, visticamāk, atpazīs līdzvērtīgus piemērus no sava konteksta. Strukturāli universāls ir šis raksts: strīdi, kuru vērtība ir zem ekonomiski racionālas aizstāvēšanas sliekšņa, beidzas ar to,

ka zaudējumu absorbē cietusī puse. RSN nesola perfektu taisnīgumu—tas tikai samazina strukturālo priekšrocību, kādu ļaunprātīgi dalībnieki bauda tad, kad institucionālā aizstāvēšana ir ekonomiski neizdevīga.

1.2 Kāpēc esošie risinājumi ir nepietiekami

Decentralizētas identitātes (DID) ietvari [2] nodrošina kriptogrāfiskus mehānismus pašsuverēnai identitātes pārvaldībai, taču koncentrējas galvenokārt uz identitātes verifikāciju, neaptverot plašāko uzvedības reputācijas jautājumu.

Ar dvēseli saistītie žetoni (SBT) [3] fiksē ieskatu, ka reputācija nav pārnesama, taču balstās uz blokķēdes infrastruktūru ar mērogošanas ierobežojumiem un neaptver ekonomiskos stimulus, kas pārvalda informācijas ievadi. Radniecīgi jēdzieni, piemēram, nopelnu žetoni (piem., Liberland), balstās uz līdzīgu filozofiju, taču paliek piesaistīti konkrētiem jurisdikcijas ietvariem.

Decentralizētas autonomas organizācijas (DAO) [4] īsteno pārvaldi caur viedlīgumiem, taču atkārto plutokrātisku dinamiku, kurā ietekme ir proporcionāla kapitālam. Kvadrātiskā balsošana [5] to daļēji mazina, taču ierobežo praktisko ieviešanu. DAO saskaras arī ar fundamentālo *orākula problēmu*: viedlīgumi nespēj uzticami verificēt reālās pasaules stāvokļus bez uzticama ārēja avota, un šai problēmai blokķēdes arhitektūrā nav vispārēja risinājuma.

Neviena esošā sistēma neapvieno decentralizāciju, izturību pret cenzūru, pseidonimitāti, verificējamas ievades izmaksas un emerģentu konsensu.

1.3 Ieguldījums

Šis raksts sniedz šādu ieguldījumu:

1. **Reputācijas sociālā tīkla (RSN)** definīciju—decentralizēta protokola, kas paplašina DID ietvaru, lai atbalstītu divpusēju reputācijas apmaiņu.
2. **Nedeterministisku verificētāju atlases protokolu**, kas balstīts uz konsekventu jaukšanu [6].
3. **Dārgā radikālisma principu**, kas cenas apgalvojumus atbilstoši to attālumam no tīkla konsensa caur trim savstarpēji pastiprinošiem izmaksu kanāliem.
4. **Reputablas autoritātes modeli** ar asimetriskiem stimuliem, kur nepatiess apstiprinājums izmaksā katastrofāli vairāk nekā leģitīmas maksas.
5. **Pakāpenisku migrācijas ceļu** caur paralēlu fiskālo infrastruktūru.

2 Projektēšanas principi

RSN arhitektūru ierobežo pieci nepārkāpjami projektēšanas principi.

Nepārtrauktība un evolūcija. Sistēma līdzāspastāv ar esošajām institūcijām nenoteikta ilguma pārejas periodā. Pārejai jābūt atgriezeniskai katrā posmā.

Brīvprātība un atbildība. Dalība ir brīvprātīga, taču brīvprātība ir savienota ar atbildību: dalībnieks, kurš uzņemas kontroli pār institucionālu funkciju, vienlaikus uzņemas arī tai pievienotās saistības.

Daudzveidība un kultūras neitralitāte. Konsenss rodas no divpusējām mijiedarbībām, nevis no sistēmas projektētāju uzspiestiem iepriekš noteiktiem noteikumiem.

Noturība un izturība pret cenzūru. Tīkla cenzēšanas izmaksām jāpārsniedz tā paciešanas izmaksas. Tikai pilnīgs totalitārisms—par postošu politisku un ekonomisku cenu—var sistēmu apspiest.

Konsenss un piespiešana. Sistēma iekļauj cilvēka tieksmes uz sīkumainību, ļaunprātību un atriebīgu gandarījumu kā nesošas iezīmes. Nekrietnība nav aizliegta; tā tiek cenota.

3 Sistēmas pārskats

3.1 Reputācijas sociālais tīkls

RSN ir decentralizēts, vienādranga (peer-to-peer) komunikācijas slānis, kurā dalībnieki apmainās ar verificējamu informāciju par reālās pasaules uzvedību. Tā noteicošās īpašības ir: decentralizēta un cenzējama neesoša infrastruktūra; pseidonīma dalība caur DID; asimetriska izmaksu struktūra (lasīšana ir lēta, rakstīšana dārga); kriptogrāfiska verificējamība; un **standartu atbalsts**—mašīnlasāmi formāti informācijai, kas tiek izplatīta tīklā, autoritāšu piedāvātajiem pakalpojumiem (apgalvojumu sastādīšana, apstiprināšana, liecinieka pakalpojums), kā arī politikas formātam, ieskaitot noteikumus otras puses reputācijas novērtēšanai un politikas neatbilstības riska novērtēšanai (starp deklarēto un faktisko uzvedību).

3.2 Arhitektūras komponenti

RSN sastāv no četriem galvenajiem komponentiem (att. 1):

1. **DID slānis.** Dalībnieku identitātes ar deklarētiem noteikumiem, reputācijas metadatiem un tīkla maršrutēšanu.

2. **Apgalvojumu protokols.** Strukturēts formāts apgalvojumu par reālās pasaules notikumiem publicēšanai.
3. **Verifikācijas tīkls.** Decentralizēts protokols verificētāju piešķiršanai, izmantojot konsekventu jaukšanu.
4. **Reputācijas agregācijas slānis.** Pakalpojumi, kas rada cilvēklasāmus reputācijas kopsavilkumus.

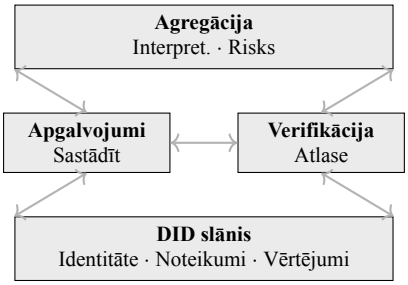

Figure 1: RSN četru slāņu arhitektūra.

3.3 Dalībnieku lomas

Verifikācijas transakcijā ir iesaistītas līdz sešām atšķirīgām DID lomām (att. 2): **Izdevējs** (DID_I, izveido un iesniedz apgalvojumu), **Subjekts** (DID_S, DID, par kuru ir apgalvojums—var sakrist ar Izdevēju), **Autoritāte** (DID_A, apstiprina apgalvojumu par maksu; var arī piedāvāt liecinieka pakalpojumus—*izvēles*), **Liecinieks** ($DID_{W_{1..n}}$, inkognito verificētāja godīguma uzraugs caur izaicinājuma kodiem—*izvēles*), **Verificētājs** (DID_V, algoritmiski atlasīts, lai publicētu apgalvojumu), un **RSN** (tīkls, kurā tiek publicēti verificētie apgalvojumi). Jebkuru lomu var deleģēt citam DID (7.4. sadaļa). Autoritāte parasti apvieno apstiprināšanu ar liecinieka pakalpojumiem, taču abas funkcijas ir loģiski neatkarīgas.

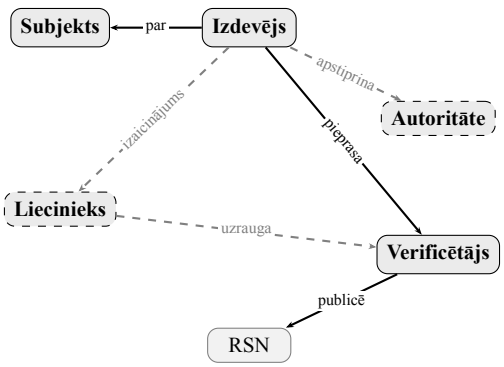

Figure 2: DID lomas verifikācijas transakcijā. Punktētas = izvēles (Autoritāte, Liecinieks).

3.4 Nepiekukuļojamība: četri spēki

RSN nepiekukuļojamība nerodas no viena mehānisma, bet no četriem vienlaicīgiem spēkiem. Neviens pats par sevi nav pietiekams; tikai to kombinācija padara mēģinājumu korumpēt ekonomiski neracionālu.

Neparedzams mērķis. Katra apgalvojuma verificētājs tiek atlasīts nedeterministiski caur konsekventu jaukšanu (5.3. sadaļa). Uzbrucējs nevar iepriekš iemērķēt konkrētu verificētāju kukuļošanai, jo verificētāja identitāte ir apgalvojuma satura un iepriekšējo iterāciju funkcija, nevis izdevēja izvēle.

Reputācijas svira—lēna augšup, ātra lejup. Reputāciju var iegūt tikai pakāpeniski, caur ilgstošu konsekventu uzvedību. Tomēr to var katastrofāli zaudēt vienā krāpnieciskā apstiprinājumā (6.2. sadaļa). Šī asimetrija nozīmē, ka gadu gaitā uzkrātu reputāciju var iznīcināt viens negodīgs apstiprinājums; optimālā stratēģija paliek noraidīt aizdomīgus apgalvojumus.

Publisks solījums. Katrs DID turētājs publiski deklarē savu politiku—mašīnlasāmu noteikumu kopu, kurus tas apņemas ievērot. Novirze starp deklarāciju un faktisko uzvedību ir atklājama un tiek cenota kā reputācijas pārkāpums, kas ir smagāks par pašu pamatpārkāpumu (7.3. sadaļa). Tāpēc liekulība ir dārgāka par tiešu negodīgumu.

Tīkla uzbrukuma izmaksu asimetrija. Tīkla cenzēšanas vai destabilizēšanas izmaksas aug nelineāri līdz ar tīkla lielumu un blīvumu, kamēr tā paciešanas izmaksas paliek nemainīgas. Lai cenzūra atmaksātos, centralizētam dalībniekam tā būtu jāpiemēro visā tīklā—prasot pasākumus, kas ir nesamērīgi ar jebkādu iedomājamu ieguvumu (10. sadaļa).

4 Decentralizētas identitātes modelis

4.1 DID ar īpašām īpašībām

RSN paplašina W3C DID Core specifikāciju [2] ar: **Deklarētiem noteikumiem** (mašīnlasāmas uzvedības saistības), **Reputācijas metadatiem** (agregēts uzvedības vērtējums) un **Tīkla maršrutēšanu** (maināma sīpola (onion) vārteja, kas nošķirta no stabilās pozīcijas gredzenā).

4.2 Apgalvojuma dzīves cikls

Apgalvojums iziet cauri sešiem posmiem (att. 3): sastādīšana, izvēles autoritātes apstiprinājums, verificētāja atlase caur konsekventu jaukšanu, verifikācijas lēmums (pieņemt vai noraidīt ar iterāciju), publicēšana un reputācijas atjaunināšana visām pusēm.

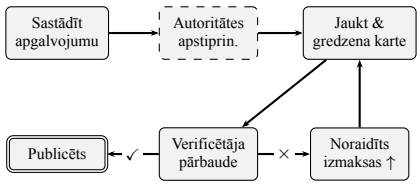

Figure 3: Apgalvojuma dzīves cikls ar iterāciju cilpu.

4.3 Saistība ar W3C DID Core

RSN identitātes modelis ir W3C DID Core specifikācijas [2] īsts virskopums. Visi RSN DID ir derīgi W3C DID. RSN specifiskie paplašinājumi ir kodēti kā DID dokumenta īpašības, kas definētas atsevišķā DID metodes specifikācijā, saderīgā ar esošo infrastruktūru, piemēram, ION [7] un Ceramic [8].

5 Informācijas verifikācija un izplatīšana

5.1 Informācijas ievades izmaksas

RSN pamata ekonomiskais princips ir asimetrija starp lasīšanu un rakstīšanu. Reputācijas datu lasīšana tuvojas nullei robežizmaksām dalībniekiem, kas ir daļa no DID tīkla un kam ir piekļuve, kas atbilst viņu reputācijai—jaunpienācējiem pakāpeniski jāizpelnās plašāka piekļuve (sk. pretpiesūkšanās mehānismu). Rakstīšana—saprasta kā reputācijas noturīga materializācija tīklā, nevis kā vienreizējs tehnisks akts—prasa verificējamu kumulatīvu ieguldījumu trijās dimensijās: **laiks** (dzīves gadi, kas pavadīti konsekventā uzvedībā, izpildītas saistības un koptas attiecības), **enerģija** (godīgā rīcībā ieguldītais pūliņš, rūpes par partnerībām un ilgtermiņa uzticamība) un **nauda** (ieguldījums savā vārdā—profesionālā izaugsme, sava darba kvalitāte, nodarītā kaitējuma atlīdzināšana). Reputāciju nevar nopirkt uzreiz—tā ir mūža uzkrājuma rezultāts, ko sistēma tikai padara redzamu un pārnesamu starp kontekstiem. Protokola vienreizējās tehniskās izmaksas (kriptogrāfiskie paraksti, verificētāju maksas) ir niecīgas salīdzinājumā ar šo pamatā esošo ieguldījumu.

5.2 Sociālais grafs un kontaktu dziļums

RSN pēc būtības ir sociāls tīkls: katrs DID pievieno kontaktus (citus DID), kas atļauj savienojumu. Šiem kontaktiem ir savi kontakti, un tā tālāk. Algoritmiskā verificētāju meklēšana darbojas konfigurējama dziļuma h ietvaros starp saistītajiem kontaktiem (piem., $h = 3$: cilvēka tiešie kontakti, viņu kontakti un kontaktu kontakti). Šī arhitektūra neprasa vienu globālu blokķēdi—tā dabiski atbalsta kopienu/klasteru rašanos ar pārklāšanos citās kopienās. Katram DID dalībniekam jābūt publicētai **politikai**—mašīnlasāmai noteikumu kopai, kas pārvalda, kā tiek novērtēti ienākošie pieprasījumi. Politikas pārkāpumi tiek reģistrēti tīklā kā negatīvi artefakti.

5.3 Algoritmiskā verificētāju atlase

Verifikācijas protokols izmanto konsekventu jaukšanu [6] (att. 4). Verifikācija ir maksas pakalpojums: verificētāji darbojas par maksu, radot tirgu, kurā konkurence virza cenu veidošanu, ātrumu un uzticamību.

1. solis. Apgalvojuma dokuments tiek savienots ar iepriekšējās iterācijas jaukšanas rezultātu (vai $\varnothing$ pirmajā iterācijā) un jaukts:

$$\text{pos} = f_h(\text{claim} \| \text{prev\_hash}) \tag{1}$$

Algoritmam jāiekļauj visu iepriekšējo pieprasījumu un atbilžu *pilnais ceļš*—ne tikai iepriekšējās iterācijas jaukšana. Katra verificētāja pilnā atbilde (pieņemšana, noraidīšana, kotētā cena, iemesls) tiek pievienota augošajam dokumentam, verificējama caur kriptogrāfiskiem parakstiem katrā solī.

2. solis. Jaukšana tiek attēlota uz N pozīcijām konsekventā jaukšanas gredzenā, vienmērīgi sadalītām (piem., $N = 4$ gadījumā: $+0°, +90°, +180°, +270°$). No katras pozīcijas pulksteņrādītāja virziena meklēšana izvēlas tuvāko DID kā verificētāja kandidātu (att. 5). N ir mainīgs parametrs, kas var būt atkarīgs no pašlaik aktīvo DID procentuālā daudzuma, diennakts laika vai tīkla vēsturiskās atsaucības.

3. solis. Verificētājs pieņem (publicē, liekot uz spēles reputāciju) vai noraida (atgriežoties pie 1. soļa ar noraidījuma jaukšanu). Kad mezgls neatbild, neskatoties uz deklarēto tiešsaistes statusu, nākamajam pieprasījumam jāiekļauj visas atbildes no visiem N iepriekšējiem verificētāju kandidātiem.

Pretpiesūkšanās. Mērķa DID var noteikt maksas vai piekļuves ierobežojumus pieprasījumiem no jauniem DID ar nelielu reputāciju. Šis pakāpeniskais mehānisms (nevis binārs) piespiež jaunpienācējus veidot reputāciju caur patiesu aktivitāti, pirms tie brīvi patērē citu datus.

Katrs noraidījums pievieno verificētāja pilno atbildi (ieskaitot iemeslus un nosacījumus) apgalvojuma dokumentam, paplašinot tā saturu. No paplašinātā dokumenta nedeterministiski tiek aprēķināta jauna jaukšana, kas attēlojas uz citu gredzena pozīciju

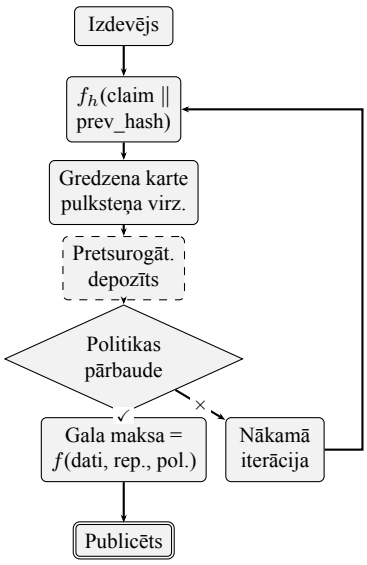

Figure 4: Verificētāju atlases protokols. Pretsurogāta depozīts ir izvēles un var būt atmaksājams. Gala maksu maksā tikai pēc pieņemšanas.

un izvēlas citu verificētāju. Pilnā ceļa dokumentēšana ir obligāta—izdevējs nevar paredzēt vai ietekmēt nākamo verificētāju. Ja verificētājs ignorē pieprasījumu, neskatoties uz saderīgu deklarēto politiku, liecinieki (ja tādi ir) to reģistrē, un izdevējs var pievienot liecinieku pierādījumus gala publicēšanā.

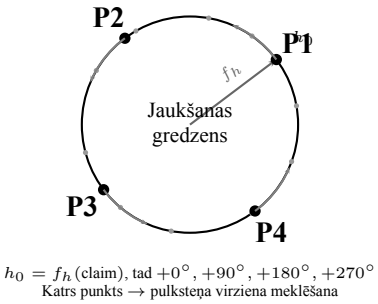

Figure 5: Daudzpunktu atlase (N=4). Jaukšana h_0 nosaka nobīdi; 4 punkti vienmērīgi sadalīti no h_0.

5.4 Liecinieka protokols

Liecinieka loma nodrošina inkognito atbildību par verificētāja godīgumu caur kriptogrāfisku izaicinājuma koda protokolu:

W1. solis. Pieprasītājs paraksta verifikācijas pieprasījumu un nosūta to N_w lieciniekiem—kontaktiem no pieprasītāja sociālā tīkla vai specializētiem liecinieku pakalpojumu sniedzējiem, kas darbojas par maksu.

W2. solis. Katrs liecinieks w_i paraksta visu parakstīto pieprasījumu, saglabā oriģinālo parakstu σ_i un aprēķina izaicinājuma kodu $c_i = h(\sigma_i)$. Izaicinājuma kods tiek pievienots pieprasījumam.

W3. solis. Pieprasījums, kas tagad nes N_w izaicinājuma kodus, tiek nosūtīts verificētājam. Verificētājs novēro kodus, bet *nevar noteikt*, kas ir liecinieki vai vai kodi atbilst reāliem parakstiem.

W4. solis (godīgs verificētājs). Ja verificētājs atbild atbilstoši savai deklarētajai politikai, izaicinājuma kodi paliek necaurspīdīgi. Liecinieki nekad netiek atklāti. Nekādi papildu dati netiek publicēti.

W5. solis (politikas pārkāpums). Ja verificētājs pārkāpj savu politiku (ignorē pieprasījumu, atbild nekonsekventi), pieprasītājs tur liecinieku oriģinālos parakstus σ_i. Tos var publicēt kā pavaddatus: jebkurš var verificēt $c_i = h(\sigma_i)$, pierādot, ka liecinieks bija klāt. Pieprasītājs var publicēt neatkarīgi—verificētājs jau ir parakstījis izaicinājuma kodus savā atbildē.

Blefa īpašība. Pieprasītājs dažiem vai visiem izaicinājuma kodiem var aizvietot nejaušas vērtības. Verificētājs nevar atšķirt īstus kodus (kurus balsta augstas reputācijas autoritātes) no trokšņa. Šī *nenoteiktība* ir piespiešanas mehānisms: katrs pieprasījums nes risku, ka cienīta autoritāte to inkognito vēro. Šī spiediena uzturēšanas izmaksas ir tuvu nullei (nejaušu skaitļu ģenerēšana), kamēr negodīguma potenciālās izmaksas verificētājam ir katastrofālas. Godīga uzvedība tiek stimulēta pat tad, ja reālu liecinieku nav.

Autoritāte kā liecinieks. Autoritāte, kas apstiprina apgalvojumu, var apvienot liecinieka pakalpojumus: „Es apstiprinu tavu apgalvojumu un kalpoju kā inkognito liecinieks verifikācijas laikā.” Tas ir dabisks biznesa modelis—autoritātei jau ir konteksts. Tomēr abas lomas ir loģiski neatkarīgas.

5.5 Dārgā radikālisma princips

Trīs izmaksu kanāli pastiprinās vienlaicīgi (att. 6):

1. kanāls: iterācijas izmaksas. Katrs noraidījums piespiež jaunu iterāciju, kas patērē laiku un resursus. Lineāra izaugsme.

2. kanāls: dokumenta uzblīšana. Katra iterācija pievieno pilno verificētāja atbildi apgalvojuma dokumentam. Izaugsme ir lineāra, bet ar bāzes nobīdi: sākotnējā slodze (apgalvojuma saturs, autoritātes apstiprinājums, kriptogrāfiskie paraksti) jau ir ar netriviālu izmēru B_0. Kopējais izmērs pēc k iterācijām: $S(k) = B_0 + k \cdot \Delta$, kur Δ ir vidējais atbildes izmērs.

3. kanāls: verificētāja riska prēmija. Risks ir subjektīvs. Verificētājs novērtē, vai pieprasošā DID deklarētās politikas ir pretrunā ar verificētāja paša

komerciālajām, sociālajām vai politiskajām interesēm. Prēmija var eksponenciāli pieaugt līdz ar uztverto attālumu no verificētāja „ideāla”: $P(d) = \alpha \cdot e^{\beta d}$, kur d ir verificētāja subjektīvā attāluma metrika. Aiz personiskās aizlieguma robežas verificētājs var atteikt pilnībā.

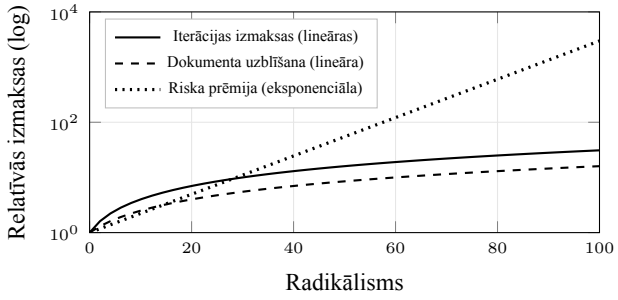

Figure 6: Izmaksu eskalācija trijos kanālos. Riska prēmija dominē pie augsta radikālisma.

Būtiski, ka tā nav cenzūra. Neviens apgalvojums nav aizliegts. Sistēma cena risku (tab. 1).

Table 1: Izmaksu salīdzinājums pa apgalvojumu tipiem.

Tips	**Iter.**	**Dok.**	**Maksa**	**Kopā**
Ticams	$k_{\min}$	B_0	$P_{\min}$	Zemas
Strīdīgs	k_{med}	$B_0 + k\Delta$	$\alpha e^{\beta d}$	Vidējas
Radikāls	$k_{\max}$	$\gg B_0$	$\gg P_{\min}$	Ļoti augstas
Krāpniecisks	$\to \infty$	—	—	Nepublicējams

6 Reputācija un riska novērtēšana

6.1 Reputācijas uzkrāšanas modelis

Reputācijai ir trīs īpašības: **lēna uzkrāšana** (pakāpeniska izaugsme caur konsekventu uzvedību), **strauja iznīcināšana** (viena krāpšana var katastrofāli samazināt vērtējumu) un **individuāls novērtējums** (katra patērējošā puse var piemērot savu agregācijas funkciju).

6.2 Reputablas autoritātes

Reputabla autoritāte pārskata apgalvojumus un, ja apmierināta, tos līdzparaksta—liekot uz spēles savu reputāciju (att. 7). Asimetrija ir apzināta: reputācijas iegūšana ir lēna (pakāpenisks $+\delta$ par godīgu apstiprinājumu), kamēr tās zaudēšana ir katastrofāla ($-\Delta \gg \delta$ par nepatiesu apstiprinājumu; ilustratīvi, piem., $+2\%$ pret -70%). Optimālā stratēģija vienmēr ir noraidīt aizdomīgus apgalvojumus. Konkrētās δ un Δ vērtības ir sistēmas parametri.

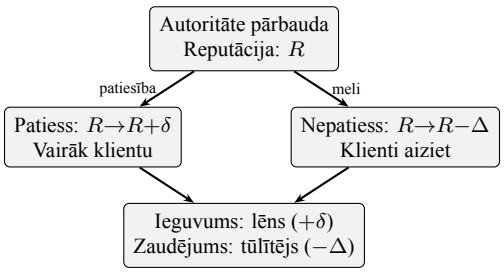

Figure 7: Reputabla autoritāte—asimetriski stimuli.

6.3 Daudzdimensionāla reputācija

Reputācija nav skalārs, bet vektors vairākās dimensijās: finansiālā uzticamība, personiskā integritāte, profesionālā kompetence, pilsoniskā iesaiste un citas (att. 8). Dažādi novērtēšanas pakalpojumu sniedzēji projicē šo vektoru atšķirīgi atkarībā no konteksta—aizdevējs par prioritāti izvirza finansiālo uzticamību, darba devējs profesionālo kompetenci, kaimiņš pilsonisko uzvedību. Nav vienota „pareiza” reputācijas vērtējuma; ir tikai perspektīvas.

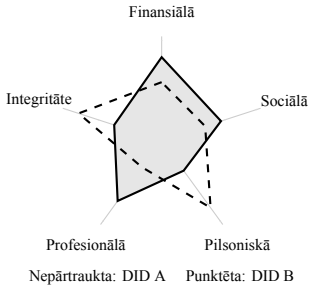

Figure 8: Daudzdimensionāli reputācijas vektori. Dažādi DID uzrāda atšķirīgus profilus pa dimensijām.

6.4 Demokratizēta riska novērtēšana

RSN demokratizē sistemātisku riska novērtēšanu—spēju, kas pašlaik ir koncentrēta finanšu institūcijās, taču piemērojama tālu ārpus banku sfēras. Rūpniecības konglomerāti, kas novērtē piegādātāju uzticamību, apdrošināšanas sabiedrības, kas cena uzvedības risku, uzticamības pārbaude apvienošanās un pārņemšanas darījumos, iekārtu kalpošanas laika novērtēšana ražošanā—visur, kur darījuma partnera risks prasa novērtēšanu, RSN nodrošina decentralizētu, uz tirgu balstītu alternatīvu. Interpretācijas pakalpojumu tirgus pārvērš neapstrādātus daudzdimensionālus reputācijas datus rīcībai izmantojamos kopsavilkumos, padarot darījuma partnera novērtēšanu pieejamu jebkuram dalībniekam par robežizmaksām.

7 Konsenss un strīdu izšķiršana

7.1 Decentralizēta taisnīguma modelis

RSN pārformulē taisnīgumu kā divpusēju sarunu problēmu. Draudi ar pastāvīgu, verificējamu reputācijas kaitējumu ir efektīvāks atturoša faktors nekā tiesvedība, ko cietusī puse nevar atļauties.

7.2 Emerģents konsenss

Katrs dalībnieks uztur personisku gandarījuma slieksni. Tīkla kopējais konsenss rodas kā tūkstošiem divpusēju sarunu statistiskais vidējais (att. 9). Atbilde tālu virs konsensa (barbariska) ir dārgi publicējama. Atbilde tuvu konsensam (samērīga) ir lēta. Konsenss nav noteikums—tas ir cenas signāls.

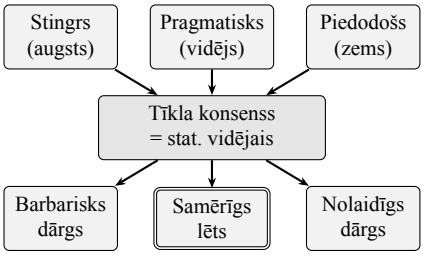

Figure 9: Emerģents konsenss no individuāliem gandarījuma sliekšņiem.

7.3 Soda kalibrēšana

Katrs DID turētājs publiski deklarē atbildes uz konkrētām nekrietnības kategorijām. Nesamērīgi bargas vai iecietīgas deklarācijas piesaista negatīvus reputācijas signālus. Samērīgas deklarācijas tiek pieņemtas bez berzes—paškalibrējoša soda sistēma.

Konsensa deklarācijas pašas ir pakļautas liekulības atklāšanai: deklaratīvi apņemties par konsensa pozīciju, uzvedoties nekonsekventi, ir reputācijas pārkāpums, kas ir smagāks par pašu novirzi, jo tas demonstrē tīšu maldināšanu.

7.4 Deleģēšana

Visas aktivitātes DID ietvaros—ar vienu izņēmumu—var deleģēt citam DID. **Subjekta loma—DID, par kura uzvedību ir apgalvojums—nav deleģējama; tā ir nepārnesami piesaistīta identitātes turētājam, uz kuru apgalvojums attiecas.** Pārējās aktīvās lomas—Izdevējs, Autoritāte, Liecinieks, Verificētājs—var nodot norādītam delegāta DID, vai tas būtu verifikācijai, apgalvojuma iesniegšanai, dalībai konsensā vai strīdu izšķiršanai. Deleģēšana ir atsaucama jebkurā laikā. Tas dara iespējamu specializāciju (piem., profesionālus verifikācijas pakalpojumus), kamēr turētājs saglabā galīgo kontroli un atbildību. Deleģēšana attiecas uz visu sistēmu un ir būtiska mērogojamībai.

7.5 No individuālas morāles uz emerģentu sabiedrisko līgumu

Katra DID deklarētā politika ir individuālas morāles formalizācija: ko turētājs uzskata par pieņemamu, kā tas reaģē uz konkrētu uzvedību, ko tas prasa no darījuma partneriem. Šīs politikas neuzspiež sistēmas projektētājs—tās izvēlas katrs dalībnieks un izsaka mašīnlasāmā formā.

Šī formalizācija dara iespējamu trīs posmu emerģenci. Pirmkārt, individuālā morāle tiek kodēta kā **politika**—deklarētu noteikumu, sliekšņu un atbildes funkciju kopa, kuru DID apņemas ievērot. Otrkārt, visu politiku kopums tīklā rada **emerģentu ētiku**—statistiski novērojamas normas, kuras neveidoja neviens atsevišķs dalībnieks, bet kuras rodas no tūkstošiem individuālu morālu pozīciju mijiedarbības [9]. Treškārt, šī emerģentā ētika, izteikta kā kopīgas uzvedības normas, ko piespiež caur divpusējiem cenas signāliem, veido **izmērāmu sabiedrisko līgumu**—nevis teorētisku konstruktu, ko neviens nav parakstījis [10], bet empīriski novērojamu noteikumu kopu, ko balsta faktiskā uzvedība.

Šis process atspoguļo morālo pamatu teorijas atziņas [11]: cilvēka morāle ir intuitīva, plurālistiska un kultūrai mainīga. RSN neprasa morālu konsensu kā ievadi; tas rada uzvedības konsensu kā izvadi. Iegūtais sabiedriskais līgums nav statisks—tas attīstās, dalībniekiem pievienojoties, aizejot un pielāgojot savas politikas atbildē uz tīkla atgriezenisko saiti. Atšķirībā no klasiskās sabiedriskā līguma teorijas šis līgums ir atsaucams, novērojams un piespiežams bez suverēna.

8 Ekonomiskais modelis

Iepriekšējās sadaļas aprakstīja rīku—RSN verifikācijas mehānismus, izmaksu struktūru un emerģentu konsensu. Šī sadaļa apraksta metodoloģiju šī rīka pielietojumam fiskālajā un pārvaldes pārejā. Rīks ir vispārējas nozīmes; zemāk aprakstītā metodoloģija ir viens iespējams pielietojums.

8.1 Stimulu struktūra

Reputācija kā kapitāls rada tiešus stimulus godīgai uzvedībai. Normālā darbībā dalībnieki dabiski veido reputāciju caur ikdienas darījumiem un izpildītām

saistībām. Galvenie izdevumi ir par *negatīviem* apgalvojumiem—citu nodarītā kaitējuma reģistrēšanu. Šī asimetrija stimulē noderīgu, uzticamu uzvedību: būt godīgam neizmaksā neko papildus, kamēr būt kaitīgam rada dokumentētu pēdu, kuru citi maksās, lai saglabātu. Liekulība—deklarēt noteikumus, tos neievērojot—ir visdārgākais neveiksmes veids, jo tā demonstrē tīšu maldināšanu.

8.2 Paralēla fiskālā sistēma

Trīs komponenti rada konkurences spiedienu: (1) **Vienkāršs nodoklis**—viena proporcionāla likme bez izņēmumiem, sākotnēji nedaudz zem esošās efektīvās likmes; (2) **Elektroniska izdevumu reģistrācija (ESR)**—apvēršot Čehijas EET modeli tā, lai pilsoņi uzraudzītu valsts izdevumus; (3) **Pilsoņu virzīta nodokļu sadale**—sākot ar dažiem procentiem pirmajā gadā un sasniedzot pēc desmit gadiem jebko no zemām divciparu vērtībām līdz pilnīgai migrācijai uz pilsoņu virzītu sistēmu atkarībā no ieviešanas ātruma. Faktiskais temps ir atkarīgs no ātruma, kādā rodas brīvā tirgus alternatīvas valsts pakalpojumiem, un no valsts gatavības sadarboties ar pāreju; laika funkcijai nav jābūt lineārai, un nav iemesla noteikt augšējo robežu tam, kur ieviešana galu galā var nonākt.

9 Migrācijas ceļš

Migrācija notiek caur trim fāzēm (att. 10): **1. fāze: pārklājums** (RSN kā informatīvs slānis, valsts ir vienīgais sniedzējs), **2. fāze: konkurence** (RSN nodrošina funkcionālas alternatīvas, divsistēmu lietošana) un **3. fāze: pāreja** (RSN pārspēj valsts ekvivalentus, brīvprātīga migrācija). Pāreja ir atgriezeniska katrā posmā.

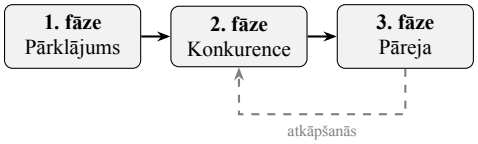

Figure 10: Trīs fāžu migrācija—atgriezeniska katrā posmā.

Galvenais spiediena mehānisms ir fiskāls: kad nosacītie nodokļu maksātāji sasniedz „ekonomiski nozīmīgu mazākumu X"—grupu, kas ir pietiekami liela, lai represijas pret to radītu netriviālu ekonomisku kaitējumu un pilsoniskā nepaklausība kļūtu par ticamu draudu—valsts uzsāk sarunas. Ilustrācijai izmantojam $X \approx 15\%$ no IKP, taču faktiskais slieksnis ir atkarīgs no konkrētās ekonomikas.

10 Drošības analīze

Mēs apsveram piecas pretinieku kategorijas: individuāli ļaunprātīgi dalībnieki, organizētas grupas, korporatīvi pretinieki, valsts līmeņa pretinieki un protokola līmeņa pretinieki.

Sibilas noturība [12]. Reputācijas veidošana prasa ilgstošu, verificējamu mijiedarbību. Veiksmīga Sibilas uzbrukuma izmaksas aug lineāri līdz ar viltus identitātēm un kvadrātiski līdz ar mērķa reputācijas līmeni. Vairāku DID darbināšana paralēli ir iespējama, bet apzināti dārga—katrai identitātei neatkarīgi jāuzkrāj reputācija caur patiesu aktivitāti. Brīvās sabiedrībās šīs izmaksas attur no gadījuma rakstura ļaunprātības; diktatūrās paralēlie DID kļūst par izdzīvošanas rīku, kas dara iespējamu nodalītu pretošanos, pagrīdes koordināciju un drošāku melnā tirgus navigāciju.

Aizsardzība pret slepenu vienošanos. Savstarpējas apstiprināšanas modeļi slēgtu grupu ietvaros ir atklājami caur sociālā grafa analīzi. Reputācijas agregācijas funkcijas atlaiž apgalvojumus no cieši saistītiem avotiem.

Valsts līmeņa pretinieks. Sīpola maršrutēšana, centralizētas infrastruktūras neesamība un Verificētāja lomas sadale pa dalībnieku bāzi nodrošina, ka apspiešana prasa pasākumus, kas ir nesamērīgi ar jebkādu ieguvumu.

Privātums pret atbildību. Pseidonimitāte—vidusceļš starp anonimitāti un identitātes atklāšanu—ļauj DID uzkrāt jēgpilnu reputāciju, neatklājot turētāja reālās pasaules identitāti.

11 Privātuma apsvērumi

RSN privātuma modelis balstās uz pseidonimitāti. Turētājs kontrolē identitātes atklāšanu: minimālu (tīrs pseidonīms), selektīvu (saistīti konkrēti akreditācijas dati) vai pilnu (piesaistīta juridiskā identitāte). Publicētie apgalvojumi ir pastāvīgi—sistēma atbalsta kontekstuālu labošanu, bet ne dzēšanu. Turētājs var pamest kompromitētu DID un sākt no jauna, atsakoties no uzkrātās reputācijas.

12 Saistītie darbi

W3C DID Core specifikācija [2] un Ceramic Network [8] nodrošina identitātes pamatu. EigenTrust [13] demonstrēja izkliedētu reputācijas agregāciju bez centrālas autoritātes. SBT [3] ieviesa nepārnesamus sociālos žetonus. RSN atšķiras ar uzsvaru uz ekonomiskajām izmaksām kā kvalitātes filtru un ar

mehānismu radikālisma cenošanai.

DAO [4] un kvadrātiskā balsošana [5] demonstrēja decentralizētas pārvaldes iespējamību. RSN atvasina konsensu no divpusējām cenu sarunām, nevis no balsošanas.

Priekšlikums balstās uz anarhokapitālisma teoriju [14, 15] attiecībā uz privātu pakalpojumu sniegšanu, taču atšķiras divos būtiskos aspektos: tas ir projektēts ļaunprātībai un atriebīgiem impulsiem, nevis pieņem racionalitāti, un tas ierosina pakāpenisku pāreju, nevis revolūciju. Emerģentu sabiedrisko līgumu jēdzienam ir priekšteči Haijeka spontānās kārtības teorijā [16].

Anarhoagorisms. RSN dala ievērojamu kopīgu pamatu ar agorisma pretekonomiku [17]—īpaši uzsvaru uz paralēlu institūciju veidošanu un brīvprātīgu apmaiņu. Tomēr agorisms mēdz pieņemt racionālu pašinteresi kā pietiekamu koordinācijas mehānismu un bieži trūkst konkrēta migrācijas ceļa no esošajām valsts struktūrām. RSN skaidri iekļauj neracionālas uzvedības tieksmes un nodrošina fiskālā spiediena mehānismu pakāpeniskai pārejai.

Meritokrātija. RSN var būt pirmais funkcionālais apraksts tam, kā meritokrātija [18] var rasties kā sistēmiska īpašība, nevis kā sauklis. Tradicionālās meritokrātiskās sistēmas neizdodas, jo tām nepieciešama centrāla autoritāte, lai definētu un piespiestu „nopelnu". RSN nopelni rodas no divpusējiem novērtējumiem: tie, kas sniedz vērtību, uzkrāj reputāciju; neviena komiteja neizlemj, kam ir nopelni.

Īpašums kā privilēģija. RSN fundamentāli atkāpjas no anarhokapitālisma un austriešu skolas traktējuma par īpašumtiesībām kā dabiskām un absolūtām. RSN ietvarā īpašums ir *privilēģija*—sociāla atzīšana, ko galējos gadījumos kopiena var atsaukt, kad dalībnieks fundamentāli pārkāpj kopīgas normas (nodevība, atteikšanās aizstāvēt kopienu eksistenciālā krīzē, sistemātiska ekspluatācija). Tā nav valsts ekspropriācija, bet sociālas atzīšanas atsaukšana no divpusēju attiecību tīkla.

13 Diskusija un ierobežojumi

Aukstais starts. RSN vērtība ir atkarīga no tīkla efektiem; agrīnie ieviesēji saskaras ar ierobežotu vērtību, līdz dalība sasniedz slieksni. Tomēr pat no agrīnajiem posmiem DID tīkls kalpo kā noderīgs papildu informācijas avots. Sagaidāms, ka agrīnā reputācijas novērtēšana un autoritāšu novērtēšana attīstīsies pakāpeniski, pieaugot sarežģītībai.

Pretpiesūkšanās un piekļuves kontrole. Mērķa DID var uzlikt pakāpeniskas maksas un piekļuves ierobežojumus pieprasījumiem no zemas reputācijas DID. Tā nav bināra, bet nepārtraukta skala: jo mazāk reputācijas ir pieprasošajam DID, jo mazāk informācijas tas saņem, jo ilgāk tas gaida un jo vairāk maksā. Šis mehānisms stimulē patiesu dalību pār pasīvu patēriņu.

Piekļuves nevienlīdzība. Apgalvojumu publicēšanas izmaksas var filtrēt leģitīmas sūdzības no ekonomiski nelabvēlīgā stāvoklī esošiem dalībniekiem. Mazināšana: katrs dalībnieks vienlaikus kalpo kā potenciāls verificētājs (vai deleģē šo lomu) un pelna verifikācijas maksas. Pietiekami ilgā laika horizontā neradikālam dalībniekam vajadzētu tuvoties finansiālai neitralitātei—verifikācijas ieņēmumiem aptuveni kompensējot publicēšanas izmaksas. Tā ir statistiska gaidāmā vērtība, nevis garantija.

Reputācijas nevienlīdzība. Agrīnie ieviesēji uzkrāj priekšrocības, kas var radīt barjeras vēlākiem pievienotājiem. Tomēr reputācijas novērtēšanu veic trešo pušu sniedzēji, kas var izvēlēties mazināt pirmā gājēja priekšrocību caur savām agregācijas algoritmiem. Būt pirmajam ar labu reputāciju ir leģitīma salīdzinoša ekonomiska priekšrocība—un tā ir apzināta.

Atklātie jautājumi. Optimālas izmaksu funkcijas, agregācijas standarti, protokola pārvalde un mijiedarbība ar mākslīgā intelekta ģenerētiem sintētiskiem reputācijas datiem paliek nākotnes darba jomas.

Šis raksts neapgalvo, ka RSN radīs optimālus rezultātus visos apstākļos. Tas apgalvo, ka RSN ir *īstenojama* alternatīva—tehniski ieviešama, ekonomiski pašuzturoša un sociāli saderīga ar cilvēka uzvedības tieksmēm tādām, kādas tās patiesībā ir.

14 Secinājums

Šis raksts ir prezentējis reputācijas sociālo tīklu—decentralizētu protokolu, kas dara iespējamu pseidonīmu, verificējamu reputācijas apmaiņu. Dārgā radikālisma princips nodrošina, ka krāpnieciski apgalvojumi tiek izcenoti no aprites bez cenzūras. Ierosinātais migrācijas ceļš dara iespējamu pakāpenisku, atgriezenisku pāreju no esošajām institūcijām. Projekts iekļauj cilvēka dabu tādu, kāda tā ir—ieskaitot sīkumainību, ļaunprātību un vēlmi pēc atriebīga gandarījuma—, nevis prasa ideoloģisku transformāciju. Rezultāts nav utopija, bet sistēma, kurā taisnīgums ir pieejams, reputācija ir nopelnīta un nekrietnības izmaksas nes tā puse, kas tās izraisīja.

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.