

Decentralizuotas reputacijos tinklas: Natūralaus visuomenės organizavimo sistema

Pavel Kudrna
Prague, Czechia
Draft v1 — March 2026

Abstract

Teisingumo jausmas—įsitikinimas, kad neteisybės ištaisomos, o nuopelnai atlyginami—yra stipriausia visuomenę vienijanti jėga. Kai centralizuotos valdymo institucijos negali suteikti šio jausmo, nes teisės įgyvendinimo kaina viršija pačios teisės vertę, socialinė sanglauda yra griunama. Dabartinės institucinės struktūros nesugeba išspręsti reikšmingos ginčų dalies sistemiškai lygiai taip pat, kaip centrinis planavimas nesugeba paskirstyti išteklių: dėl informacijos asimetrijos, trūkstamų grįžtamojo ryšio kilpų ir sprendimų priėmėjų atsiribojimo nuo savo sprendimų padarinių. Šiame straipsnyje pristatomas reputacijos socialinis tinklas (RSN): decentralizuotas, nepaperkamas, cenzūrai atsparus komunikacijos sluoksnis, sukurtas remiantis decentralizuotais identifikatoriais (DID), leidžiantis pseudonimiškiems dalyviams skelbti, tikrinti ir vartoti reputacijos informaciją apie realaus pasaulio elgesį. Pagrindinis mechanizmas remiasi trimis projektavimo principais: (1) asimetrine kaštų struktūra, kurioje reputacijos duomenų skaitymas yra pigus, o rašymas reikalauja patikrinamų pastangų; (2) nedeterministiniu tikrintojų parinkimo protokolu, pagrįstu nuosekliuoju maišymu, kuris įkainoja radikalius teiginius per didėjančius iteracijų kaštus; ir (3) rinkos vairuojamu reputacijos autoritetų modeliu, kuriame privatūs tikrintojai stato savo sukaupią reputaciją už jų patvirtinamų teiginių tikslumą. Gauta architektūra sukuria emergentinę meritokratiją be centrinio koordinavimo ir įgalina laipsnišką, grįžtamą migracijos kelią nuo esamų valstybės administruojamų sistemų.

1 Įvadas

1.1 Centralizuoto pasitikėjimo problema

Šiuolaikinis valdymas remiasi esmine prielaida: kad centralizuotos institucijos gali tarpininkauti pasitikėjimą tarp nepažįstamų žmonių plačiu mastu.

Teismai sprendžia ginčus. Registrai patvirtina nuosavybę. Reguliavimo institucijos užtikrina standartus. Šios institucijos buvo sukurtos epochoje, kai informacijos buvo stinga, komunikacija buvo lėta, o įgaliojimų perdavimas centrinei institucijai buvo vienintelis įmanomas koordinavimo mechanizmas. Tačiau centralizuotas valdymas žlunga dėl tų pačių struktūrinių priežasčių kaip ir centrinis planavimas: informacijos asimetrijos, trūkstamų grįžtamojo ryšio kilpų ir sprendimų priėmėjų atsiribojimo nuo savo sprendimų padarinių.

Ši prielaida žlunga, pavyzdžiui, kai institucinio tarpininkavimo kaina viršija ginčo vertę. Įsivaizduokite nuomininką, kuris atranda, kad jo išsinuomotas butas neturi teisiškai reikalaujamo elektros saugos sertifikato—sąlygos, kelianti tiesioginį pavojų gyvybei. Nuomininko teisinė teisė atsisakyti sutarties yra vienareikšmiška. Tačiau šios teisės įgyvendinimo per teismų sistemą kaina viršija užstato ir priteistinų nuostolių piniginę vertę, net įskaitant galimą įstatyminę kompensaciją [1]. Racionalus atsakas yra susitaikyti su nuostoliu ir pasitraukti.

Tai nėra patologinis kraštutinis atvejis. Tai yra numatytoji patirtis reikšmingai ginčų klasei, kurioje žala yra reali, bet piniginis statymas nesiekia ribos, ties kuria institucinis įgyvendinimas tampa ekonomiškai racionalus. Rezultatas—sistema, kuri struktūriškai palankiai vertina blogus veikėjus: tie, kurie kenkia kitiems žemiau šios ribos, gali veikti nebaudžiami, nes teisingumo siekimo kaina tenka nukentėjusiai šaliai.

Aukščiau pateiktas pavyzdys paimtas iš autoriaus teisinės aplinkos—Čekijos civilinės teisės sistemos. Kitose teisinėse tradicijose—precedentu grįstoje bendrojoje teisėje, paprotinėje teisėje, mišriose sistemose—teisingumas žlunga skirtingais būdais ir skirtingu mastu, priklausomai nuo jurisdikcijos kultūrinių ir procedūrinių ypatumų. Skaitytojai tikriausiai atpažins lygiaverčius pavyzdžius iš savo aplinkos. Struktūriškai universalus yra šablonas: ginčai, kurių vertė nesiekia ekonomiškai racionalaus įgyvendinimo ribos, baigiasi nuostoliu, kurį prisiima

nukentėjusi šalis. RSN nežada tobulo teisingumo—jis tik sumažina struktūrinį pranašumą, kurį blogi veikėjai turi, kai institucinis įgyvendinimas yra neekonomiškas.

1.2 Kodėl esami sprendimai yra nepakankami

Decentralizuoto identiteto (DID) sistemos [2] teikia kriptografinius mechanizmus savarankiškai valdomam tapatybės tvarkymui, bet daugiausia dėmesio skiria tapatybės tikrinimui, neatsakydamos į platesnį elgesio reputacijos klausimą.

Sielai pririšti žetonai (SBT) [3] užfiksuoja įžvalgą, kad reputacija yra neperduodama, bet remiasi blokų grandinės infrastruktūra su mastelio apribojimais ir neatsako į ekonomines paskatas, valdančias informacijos įvedimą. Susijusios koncepcijos, tokios kaip nuopelnų žetonai (pvz., Liberland), remiasi panašia filosofija, bet lieka susietos su konkrečiomis jurisdikcinėmis sistemomis.

Decentralizuotos autonominės organizacijos (DAO) [4] įgyvendina valdymą per išmaniąsias sutartis, bet atkartoja plutokratinę dinamiką, kai įtaka yra proporcinga kapitalui. Kvadratinis balsavimas [5] iš dalies tai sušvelnina, bet riboja praktinį pritaikymą. DAO taip pat susiduria su esmine *orakulo problema*: išmaniosios sutartys negali patikimai patikrinti realaus pasaulio būsenų be patikimo išorinio šaltinio, o ši problema neturi bendro sprendimo blokų grandinės architektūroje.

Nė viena esama sistema neapjungia decentralizacijos, atsparumo cenzūrai, pseudonimiškumo, patikrinamos įėjimo kainos ir emergentinio konsensuso.

1.3 Įnašai

Šis straipsnis pateikia šiuos įnašus:

1. **Reputacijos socialinio tinklo (RSN) apibrėžimas**—decentralizuoto protokolo, plečiančio DID sistemą, kad būtų palaikomas dvišalis reputacijos mainai.
2. **Nedeterministinis tikrintojų parinkimo protokolas**, pagrįstas nuosekliajū maišymu [6].
3. **Brangaus radikalumo principas**, įkainojantis teiginius pagal jų atstumą nuo tinklo konsensuso per tris besidauginančius kaštų kanalus.
4. **Patikimo autoriteto modelis** su asimetrinėmis paskatomis, kai melagingas patvirtinimas kainuoja katastrofiškai daugiau nei teisėti mokesčiai.
5. **Laipsniškas migracijos kelias** per lygiagrečią fiskalinę infrastruktūrą.

2 Projektavimo principai

RSN architektūrą riboja penki nediskutuotini projektavimo principai.

Tęstinumas ir evoliucija. Sistema sugyvena su esamomis institucijomis pereinamuoju neapibrėžtos trukmės laikotarpiu. Perėjimas turi būti grįžtamas kiekviename etape.

Savanoriškumas ir atsakomybė. Dalyvavimas yra savanoriškas, bet savanoriškumas siejamas su atsakomybe: dalyvis, prisiimantis institucinės funkcijos kontrolę, kartu prisiima ir lydinčias pareigas.

Įvairovė ir kultūrinis neutralumas. Konsensusas atsiranda iš dvišalių sąveikų, o ne iš anksto nustatytų taisyklių, primestų sistemos kūrėjų.

Atsparumas ir atsparumas cenzūrai. Tinklo cenzūravimo kaina turi viršyti jo toleravimo kainą. Tik visiškas totalitarizmas—pragaištingomis politinėmis ir ekonominėmis sąnaudomis—gali nuslopinti sistemą.

Konsensusas ir įgyvendinimas. Sistema įtraukia žmogiškuosius polinkius į smulkmeniškumą, pyktį ir keršto pasitenkinimą kaip laikančiąsias savybes. Netinkamas elgesys nėra draudžiamas; jis yra įkainojamas.

3 Sistemos apžvalga

3.1 Reputacijos socialinis tinklas

RSN yra decentralizuotas, tarpusavio (peer-to-peer) komunikacijos sluoksnis, kuriame dalyviai keičiasi patikrinama informacija apie realaus pasaulio elgesį. Jo apibrėžiančios savybės yra: decentralizuota ir necenzūruojama infrastruktūra; pseudonimiškas dalyvavimas per DID; asimetrinė kaštų struktūra (skaitymas pigus, rašymas brangus); kriptografinis patikrinamumas; ir **standartų palaikymas**—mašininio būdu skaitomi formatai informacijai, sklindančiai per tinklą, autoritetų teikiamoms paslaugoms (teiginio sudarymas, patvirtinimas, liudytojo paslauga) ir politikos formatui, įskaitant taisykles, skirtas įvertinti sandorio šalies reputaciją ir politikos neatitikimo riziką (tarp deklaruoto ir faktinio elgesio).

3.2 Architektūriniai komponentai

RSN sudaro keturi pagrindiniai komponentai (1 pav.):

1. **DID sluoksnis.** Dalyvių tapatybės su deklaruotomis taisyklėmis, reputacijos metaduomenimis ir tinklo maršrutizavimu.

2. **Teiginių protokolai.** Struktūrizuotas formatas teiginiams apie realaus pasaulio įvykius skelbti.
3. **Tikrinimo tinklas.** Decentralizuotas protokolas tikrintojams priskirti, naudojant nuoseklųjį maišymą.
4. **Reputacijos apibendrinimo sluoksnis.** Paslaugos, kuriančios žmogaus skaitomas reputacijos santraukas.

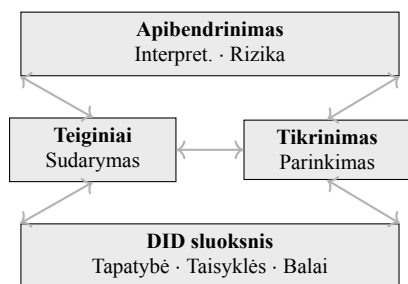


Figure 1: RSN keturių sluoksnių architektūra.

3.3 Dalyvių vaidmenys

Tikrinimo transakcijoje dalyvauja iki šešių skirtingų DID vaidmenų (2 pav.): **Išdavėjas** (DID_I , sukuria ir pateikia teiginį), **Subjektas** (DID_S , DID, apie kurį yra teiginys—gali sutapti su Išdavėju), **Autoritetas** (DID_A , patvirtina teiginį už mokestį; taip pat gali teikti liudytojo paslaugas—*neprivaloma*), **Liudytojas** ($DID_{W_{1..n}}$, inkognito tikrintojų sąžiningumo stebėtojas per iššūkio kodus—*neprivaloma*), **Tikrintojas** (DID_V , algoritmiškai parinktas teiginiiui paskelbti) ir **RSN** (tinklas, kuriame skelbiami patikrinti teiginiai). Bet koks vaidmuo gali būti deleguotas kitam DID (7.4 skyrius). Autoritetas dažnai apjungia patvirtinimą su liudytojo paslaugomis, bet abi funkcijos yra logiškai nepriklausomos.

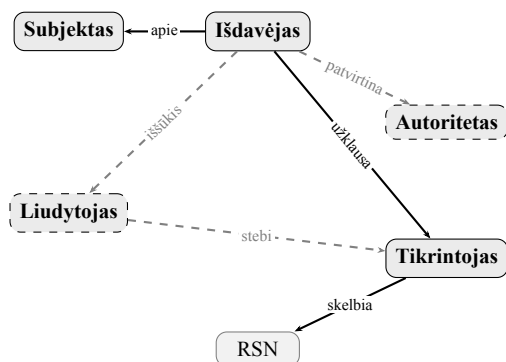


Figure 2: DID vaidmenys tikrinimo transakcijoje. Punktyras = neprivaloma (Autoritetas, Liudytojas).

3.4 Nepaperkamumas: keturios jėgos

RSN nepaperkamumas kyla ne iš vieno mechanizmo, o iš keturių vienalaikių jėgų. Nė viena nepakanka pati savaime; tik jų derinys daro korupcijos bandymą ekonomiškai neracionalų.

Nenuspėjamas taikiny. Kiekvieno teiginio tikrintojas parenkamas nedeterministiškai per nuoseklųjį maišymą (5.3 skyrius). Užpuolikas negali iš anksto nusitaikyti į konkretų tikrintoją papirkimui, nes tikrintojų tapatybė yra teiginio turinio ir ankstesnių iteracijų funkcija, o ne išdavėjo pasirinkimas.

Reputacinis svirtas—lėtai aukštyn, greitai žemyn. Reputacija gali būti įgyjama tik palaipsniui, per nuolatinį nuoseklų elgesį. Tačiau ji gali būti katastrofiškai prarasta vieną kartą apgaulingai patvirtinus (6.2 skyrius). Ši asimetrija reiškia, kad metų metais sukaupta reputacija gali būti sugriauta vieno nesąžiningo patvirtinimo; optimali strategija lieka atmesti įtartinus teiginius.

Viešas pažadas. Kiekvienas DID turėtojas viešai deklaruoja savo politiką—mašininio būdu skaitomą taisyklių rinkinį, kurio įsipareigoja laikytis. Deklaracijos ir faktinio elgesio neatitikimas yra aptinkamas ir įkainojamas kaip reputacinis nusižengimas, sunkesnis nei pats pažeidimas (7.3 skyrius). Todėl veidmainystė kainuoja daugiau nei tiesioginis nesąžiningumas.

Tinklo atakos kaštų asimetrija. Tinklo cenzūravimo ar destabilizavimo kaina auga netiesiškai su tinklo dydžiu ir tankiu, o jo toleravimo kaina lieka pastovi. Kad cenzūra atsipirktų, centralizuotas veikėjas turėtų ją taikyti visame tinkle—reikalaujant priemonių, neproporcingų bet kokiai įsivaizduojamai naudai (10 skyrius).

4 Decentralizuoto identiteto modelis

4.1 DID su ypatingomis savybėmis

RSN plečia W3C DID Core specifikaciją [2] šiais elementais: **Deklaruotos taisyklės** (mašininio būdu skaitomi elgesio įsipareigojimai), **Reputacijos metaduomenys** (apibendrintas elgesio balas) ir **Tinklo maršrutizavimas** (kintantis onion šliuzas, atskirtas nuo stabilios pozicijos žiede).

4.2 Teiginio gyvavimo ciklas

Teiginys pereina šešis etapus (3 pav.): sudarymas, neprivalomas autoriteto patvirtinimas, tikrintojų parinkimas per nuoseklųjį maišymą, tikrinimo sprendimas (priimti arba atmesti su iteracija), paskelbimas ir

reputacijos atnaujinimas visoms šalims.

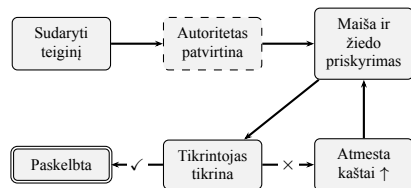


Figure 3: Teiginio gyvavimo ciklas su iteracijos kilpa.

4.3 Ryšys su W3C DID Core

RSN tapatybės modelis yra tinkamas W3C DID Core specifikacijos [2] superrinkinys. Visi RSN DID yra galiojantys W3C DID. RSN specifiniai plėtiniai yra užkoduoti kaip DID dokumento savybės, apibrėžtos atskiroje DID metodo specifikacijoje, suderinamoje su esama infrastruktūra, tokia kaip ION [7] ir Ceramic [8].

5 Informacijos tikrinimas ir sklaida

5.1 Informacijos įvedimo kaina

Pagrindinis RSN ekonominis principas yra asimetrija tarp skaitymo ir rašymo. Reputacijos duomenų skaitymas artėja prie nulinių ribinių kaštų dalyviams, kurie yra DID tinklo dalis ir turi jų reputaciją atitinkančią prieigą—naujokai turi palaipsniui užsitarnauti platesnę prieigą (žr. apsaugą nuo išnaudojimo). Rašymas—suprantamas kaip tvarus reputacijos materializavimas į tinklą, o ne kaip vienkartinis techninis veiksmas—reikalauja patikrinamų kaupiamųjų investicijų per tris dimensijas: **laiką** (gyvenimo metai, praleisti nuosekliai elgiantis, vykdant įsipareigojimus ir puoselėjant santykius), **energiją** (pastangos, investuotos į sąžiningą sandėrį, rūpestį partnerystėmis ir ilgalaikį patikimumą) ir **pinigus** (investicija į savo vardą—profesinis tobulėjimas, darbo kokybė, padarytos žalos atlyginimas). Reputacijos negalima nusipirkti akimirksniu—ji yra viso gyvenimo kaupimo rezultatas, kurį sistema tik padaro matomą ir perkeliama tarp kontekstų. Vienkartiniai techniniai protokolo kaštai (kriptografiniai parašai, tikrintojų mokesčiai) yra nereikšmingi, palyginti su šia pamatine investicija.

5.2 Socialinis grafas ir kontaktų gylis

RSN iš esmės yra socialinis tinklas: kiekvienas DID prideda kontaktus (kitus DID), kurie leidžia ryšį. Šie kontaktai turi savo kontaktus ir taip toliau. Algoritminė tikrintojų paieška veikia konfigūruojamame susietų kontaktų gylyje h (pvz., $h = 3$: tiesioginiai kon-

taktai, jų kontaktai ir kontaktų kontaktai). Ši architektūra nereikalauja vienos globalios blokų grandinės—ji natūraliai skatina bendruomenių / grupių, turinčių persidengimų su kitomis bendruomenėmis, atsiradimą. Kiekvienas DID dalyvis privalo turėti paskelbtą **politiką**—mašininiu būdu skaitomą taisyklių rinkinį, valdantį, kaip vertinamos gaunamos užklausos. Politikos pažeidimai yra fiksuojami tinkle kaip neigiami artefaktai.

5.3 Algoritminis tikrintojų parinkimas

Tikrinimo protokolas naudoja nuoseklųjį maišymą [6] (4 pav.). Tikrinimas yra mokama paslauga: tikrintojai veikia už mokestį, sukurdami rinką, kurioje konkurencija lemia kainodarą, greitį ir patikimumą.

1 žingsnis. Teiginio dokumentas sujungiamas su ankstesnės iteracijos maišos rezultatu (arba $\emptyset$ pirmoje iteracijoje) ir maišomas:

$$\text{poz} = f_h(\text{teiginys} \parallel \text{prev_hash}) \quad (1)$$

Algoritmas turi įtraukti *visą kelią* iš visų ankstesnių užklausų ir atsakymų—ne vien ankstesnės iteracijos maišą. Kiekvieno tikrintojų pilnas atsakymas (priėmimas, atmetimas, nurodyta kaina, priežastis) yra pridedamas prie augančio dokumento, patikrinamas per kriptografinius parašus kiekviename žingsnyje.

2 žingsnis. Maiša priskiriama N pozicijoms nuosekliojo maišymo žiede, tolygiai paskirstytoms (pvz., $N = 4$: $+0^\circ$, $+90^\circ$, $+180^\circ$, $+270^\circ$). Iš kiekvienos pozicijos pagal laikrodžio rodyklę atliekama paieška parenka artimiausią DID kaip tikrintojų kandidatą (5 pav.). N yra kintamas parametras, galintis priklausyti nuo šiuo metu aktyvių DID procento, paros meto arba istorinio tinklo reagavimo.

3 žingsnis. Tikrintojas priima (paskelbia, statydamas reputaciją) arba atmeta (grįždamas į 1 žingsnį su atmetimo maiša). Kai mazgas neatsako, nepaisant to, kad deklaruoja aktyvią būseną, kita užklausa turi įtraukti visus atsakymus iš visų N ankstesnių tikrintojų kandidatų.

Apsauga nuo išnaudojimo. Tiksliniai DID gali nustatyti mokesčius ar prieigos apribojimus užklausoms iš naujų DID su maža reputacija. Šis laipsniškas mechanizmas (ne dvejetainis) verčia naujokus kaupti reputaciją per tikrą veiklą, prieš laisvai vartojant kitų duomenis.

Kiekvienas atmetimas prideda pilną tikrintojų atsakymą (įskaitant priežastis ir sąlygas) prie teiginio dokumento, plėsdamas jo turinį. Iš išplėsto dokumento nedeterministiškai apskaičiuojama nauja maiša, priskiriama kitai žiedo pozicijai ir parenkanti

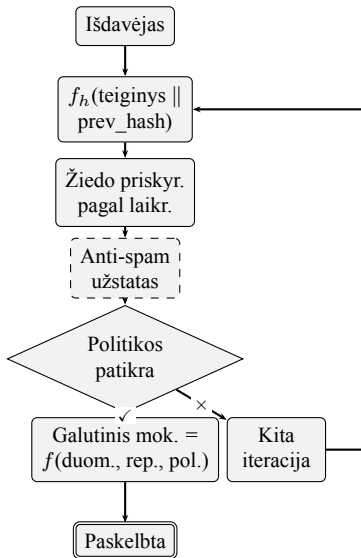


Figure 4: Tikrintojų parinkimo protokolai. Anti-spam užstatas yra neprivalomas ir gali būti grąžinamas. Galutinis mokestis mokamas tik priėmimo atveju.

kitą tikrintoją. Viso kelio dokumentavimas yra privalomas—išdavėjas negali numatyti ar paveikti kito tikrintojų. Jei tikrintojas ignoruoja užklausa, nepaisant suderinamos deklaruotos politikos, liudytojai (jei yra) tai fiksuoja, ir išdavėjas gali pridėti liudytojų įrodymus galutinio paskelbimo metu.

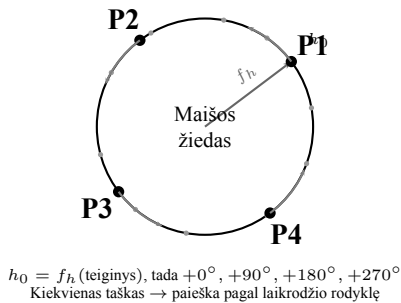


Figure 5: Kelių taškų parinkimas ($N=4$). Maiša h_0 nustato poslinkį; 4 taškai tolygiai paskirstyti nuo h_0 .

5.4 Liudytojų protokolai

Liudytojo vaidmuo suteikia inkognito atskaitomybę už tikrintojų sąžiningumą per kriptografinį iššūkio kodų protokolą:

W1 žingsnis. Užklauskėjas pasirašo tikrinimo užklausa ir siunčia ją N_w liudytojams—kontaktams iš užklauskėjo socialinio tinklo arba specializuotiems liudytojų paslaugų teikėjams, veikiantiems už mokestį.

W2 žingsnis. Kiekvienas liudytojas w_i pasirašo visą pasirašytą užklausa, išsaugo originalų parašą σ_i ir apskaičiuoja iššūkio kodą $c_i = h(\sigma_i)$. Iššūkio kodas

pridedamas prie užklauskos.

W3 žingsnis. Užklauskėjas, dabar nešanti N_w iššūkio kodų, siunčiami tikrintojui. Tikrintojas mato kodus, bet *negali nustatyti*, kas yra liudytojai ar ar kodai atitinka tikrus parašus.

W4 žingsnis (sąžiningas tikrintojas). Jei tikrintojas atsako pagal savo deklaruotą politiką, iššūkio kodai lieka neperskaitomi. Liudytojai niekada neatskleidžiami. Jokie papildomi duomenys neskelbiami.

W5 žingsnis (politikos pažeidimas). Jei tikrintojas pažeidžia savo politiką (ignoruoja užklausa, atsako nenuosekliai), užklauskėjas turi liudytojų originalius parašus σ_i . Šie gali būti paskelbti kaip lydintys duomenys: bet kas gali patikrinti $c_i = h(\sigma_i)$, įrodydamas, kad liudytojas buvo. Užklauskėjas gali paskelbti savarankiškai—tikrintojas jau pasirašė iššūkio kodus savo atsakyme.

Blefo savybė. Užklauskėjas gali pakeisti kai kuriuos ar visus iššūkio kodus atsitiktinėmis reikšmėmis. Tikrintojas negali atskirti tikrų kodų (paremtų aukštos reputacijos autoritetais) nuo triukšmo. Šis *netikrumas* yra įgyvendinimo mechanizmas: kiekviena užklausa neša riziką, kad gerbiamas autoritetas stebi inkognito. Šio spaudimo palaikymo kaina yra beveik nulinė (atsitiktinių skaičių generavimas), o galima nesąžiningumo kaina tikrintojui yra katastrofiška. Sąžiningas elgesys yra skatinamas net nesant tikrų liudytojų.

Autoritetas kaip liudytojas. Autoritetas, patvirtinantis teiginį, gali apjungti liudytojo paslaugas: „Patvirtinu jūsų teiginį ir tarnauju kaip inkognito liudytojas tikrinimo metu.“ Tai natūralus verslo modelis—autoritetas jau turi kontekstą. Tačiau abu vaidmenys yra logiškai nepriklausomi.

5.5 Brangaus radikalumo principas

Trys kaštų kanalai vienu metu dauginasi (6 pav.):

1 kanalas: iteracijos kaštai. Kiekvienas atmetimas priverčia naują iteraciją, sunaudojančią laiką ir išteklius. Tiesinis augimas.

2 kanalas: dokumento išpūtimas. Kiekviena iteracija prideda pilną tikrintojų atsakymą prie teiginio dokumento. Augimas yra tiesinis, bet su baziniu poslinkiu: pradinis krovinys (teiginio turinys, autoriteto patvirtinimas, kriptografiniai parašai) jau turi netrivialų dydį B_0 . Bendras dydis po k iteracijų: $S(k) = B_0 + k \cdot \Delta$, kur Δ yra vidutinis atsakymo dydis.

3 kanalas: tikrintojų rizikos priedas. Rizika yra subjektyvi. Tikrintojas įvertina, ar užklauskėjas DID deklaruotos politikos prieštarauja tikrintojų komercini-

ams, socialiniams ar politiniams interesams. Priedas gali eksponentiškai augti su suvokiamu atstumu nuo tikrintojo „idealo“: $P(d) = \alpha \cdot e^{\beta d}$, kur d yra tikrintojo subjektyvi atstumo metrika. Peržengus asmeninę neperžengiamą ribą, tikrintojas gali visiškai atsisakyti.

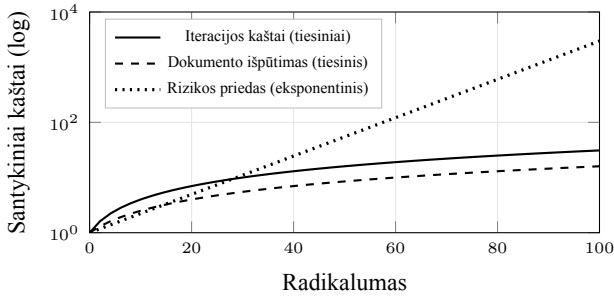


Figure 6: Kaštų eskalacija per tris kanalus. Rizikos priedas dominuoja esant dideliui radikalumui.

Iš esmės tai nėra cenzūra. Joks teiginys nedraudžiamas. Sistema įkainoja riziką (1 lentelė).

Table 1: Kaštų palyginimas pagal teiginių tipus.

Tipas	Iter.	Dok.	Mok.	Iš viso
Patikimas	$k_{\min}$	B_0	$P_{\min}$	Žemi
GINČYTINAS	k_{med}	$B_0 + k\Delta$	$\alpha e^{\beta d}$	Vidutiniai
Radikalus	$k_{\max}$	$\gg B_0$	$\gg P_{\min}$	Labai aukšti
Apgaulingas	$\rightarrow \infty$	—	—	Nepaskelbiamas

6 Reputacija ir rizikos vertinimas

6.1 Reputacijos kaupimo modelis

Reputacija pasižymi trimis savybėmis: **lėtu kaupimu** (laipsniškas augimas per nuoseklų elgesį), **greitu sunaikinimu** (viena apgaulė gali katastrofiškai sumažinti balą) ir **individualiu vertinimu** (kiekviena vartojanti šalis gali taikyti savo apibendrinimo funkciją).

6.2 Patikimi autoritetai

Patikimas autoritetas peržiūri teiginius ir, jei įsitikina, kartu pasirašo juos—statydamas savo reputaciją (7 pav.). Asimetrija yra numatyta: reputacijos įgijimas yra lėtas (laipsniškas $+\delta$ už kiekvieną sąžiningą patvirtinimą), o jos praradimas yra katastrofiškas ($-\Delta \gg \delta$ už kiekvieną melagingą patvirtinimą; iliustratyviai, pvz., $+2\%$ prieš -70%). Optimali strategija visada yra atmesti įtartinus teiginius. Konkrečios δ ir Δ reikšmės yra sistemos parametrai.

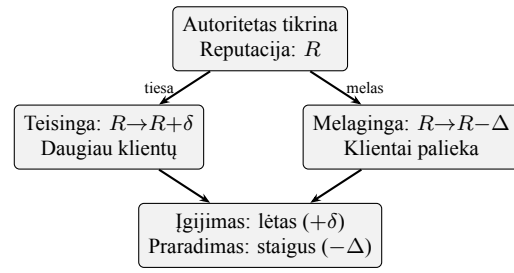


Figure 7: Patikimas autoritetas—asimetrinės paskatos.

6.3 Daugiadimensinė reputacija

Reputacija yra ne skaliaras, o vektorius per kelias dimensijas: finansinis patikimumas, asmeninis sąžiningumas, profesinė kompetencija, pilietinis įsitraukimas ir kitos (8 pav.). Skirtingi vertinimo teikėjai projektuoja šį vektorių skirtingai, priklausomai nuo konteksto—skolintojas teikia pirmenybę finansiniam patikimumui, darbdavys—profesinei kompetencijai, kaimynas—pilietiniam elgesiui. Nėra vieno „teisingo“ reputacijos balo; tik perspektyvos.

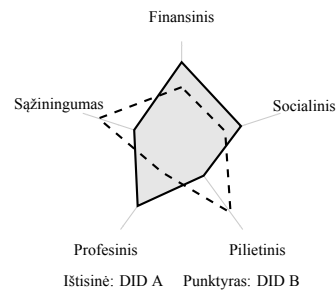


Figure 8: Daugiadimensiniai reputacijos vektoriai. Skirtingi DID rodo skirtingus profilius per dimensijas.

6.4 Demokratizuotas rizikos vertinimas

RSN demokratizuoja sisteminį rizikos vertinimą—galimybę, šiuo metu sutelktą finansų institucijose, bet pritaikomą kur kas plačiau nei bankininkystė. Pramoniniai konglomeratai, vertinantys tiekėjų patikimumą, draudimo bendrovės, įkainojančios elgesio riziką, deramas patikrinimas susijungimams ir įsigijimams, įrangos tarnavimo laiko įvertinimas gamyboje—visur, kur sandorio šalies rizika reikalauja vertinimo, RSN teikia decentralizuotą, rinkos varuojamą alternatyvą. Interpretavimo paslaugų rinka paverčia neapdorotus daugiadimensinius reputacijos duomenis įgyvendinamomis santraukomis, padarydama sandorio šalies vertinimą prieinamą bet kuriam dalyviui ribiniais kaštais.

7 Konsensusas ir ginčų sprendimas

7.1 Decentralizuoto teisingumo modelis

RSN performuluoja teisingumą kaip dvišalio derybų problemą. Nuolatinės, patikrinamos reputacinės žalos grėsmė yra veiksmingesnė atgrasymo priemonė nei teismo procesas, kurio nukentėjusi šalis negali sau leisti.

7.2 Emergentinis konsensusas

Kiekvienas dalyvis palaiko asmeninę pasitenkinimo ribą. Tinklo bendras konsensusas atsiranda kaip tūkstančių dvišalių derybų statistinis vidurkis (9 pav.). Atsakas gerokai virš konsensuso (barbariškas) yra brangus paskelbti. Atsakas šalia konsensuso (proporcingas) yra pigus. Konsensusas yra ne taisyklė—jis yra kainos signalas.

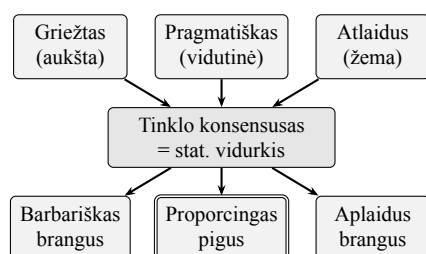


Figure 9: Emergentinis konsensusas iš individualių pasitenkinimo ribų.

7.3 Bausmės kalibravimas

Kiekvienas DID turėtojas viešai deklaruoja atsakus į konkrečias netinkamo elgesio kategorijas. Ne-proporcingai griežtos ar švelnios deklaracijos pritraukia neigiamus reputacijos signalus. Proporcingos deklaracijos priimamos be trinties—savikalibruojanti bausmės sistema.

Konsensuso deklaracijoms taip pat taikoma veidmainystės aptikimas: deklaratyvus įsipareigojimas laikytis konsensuso pozicijos, elgiantis nenuosekliai, yra reputacinis nusižengimas, sunkesnis nei pats nukrypimas, nes rodo tyčinį apgaudinėjimą.

7.4 Delegavimas

Visos veiklos DID viduje—su viena išimtimi—gali būti deleguotos kitam DID. **Subjekto vaidmuo—DID, apie kurio elgesį yra teiginys—negali būti deleguotas; jis yra neperduodamai susietas su tapatybės turėtoju, kuriam teiginys skirtas.** Kiti aktyvūs vaidmenys—Išdavėjas, Autoritetas, Liudytojas,

Tikrintojas—gali būti perduoti paskirtam deleguoto DID, ar tai būtų tikrinimui, teiginio pateikimui, dalyvavimui konsensuse ar ginčų sprendimui. Delegavimas gali būti atšauktas bet kuriuo metu. Tai įgalina specializaciją (pvz., profesionalias tikrinimo paslaugas), kol turėtojas išlaiko galutinę kontrolę ir atsakomybę. Delegavimas taikomas visoje sistemoje ir yra būtinas masteliui.

7.5 Nuo individualios moralės prie emergentinės socialinės sutarties

Kiekvieno DID deklaruota politika atspindi individualios moralės formalizavimą: ką turėtojas laiko priimtiniu, kaip jis reaguoja į konkretų elgesį, ko reikalauja iš sandomio šalių. Šios politikos nėra primetamos sistemos kūrėjo—jas pasirenka kiekvienas dalyvis ir išreiškia mašininio būdu skaitoma forma.

Šis formalizavimas įgalina trijų etapų emergenciją. Pirma, individuali moralė užkoduojama kaip **politika**—deklaruotų taisyklių, ribų ir atsako funkcijų rinkinys, kurio DID įsipareigoja laikytis. Antra, visų politikų agregatas visame tinkle sukuria **emergentinę etiką**—statistiškai stebimas normas, kurių nesukūrė joks vienas dalyvis, bet kurios kyla iš tūkstančių individualių moralinių pozicijų sąveikos [9]. Trečia, ši emergentinė etika, išreikšta kaip bendros elgesio normos, įgyvendinamos per dvišalius kainos signalus, sudaro **išmatuojamą socialinę sutartį**—ne teorinį konstruktą, kurio niekas nepasirašė [10], o empiriškai stebimą taisyklių rinkinį, paremtą faktiniu elgesiu.

Šis procesas atspindi moralinių pagrindų teorijos išvadas [11]: žmogaus moralė yra intuityvi, pluralistinė ir kultūriškai kintanti. RSN nereikalauja moralinio konsensuso kaip įvesties; jis kuria elgesio konsensumą kaip išvestį. Gauta socialinė sutartis nėra statiška—ji vystosi, kai dalyviai prisijungia, palieka ir koreguoja savo politiką atsakydami į tinklo grįžtamąjį ryšį. Skirtingai nei klasikinė socialinės sutarties teorija, ši sutartis yra atšaukiama, stebima ir įgyvendinama be suvereno.

8 Ekonominis modelis

Ankstesniuose skyriuose aprašytas įrankis—RSN tikrinimo mechanizmai, kaštų struktūra ir emergentinis konsensusas. Šis skyrius aprašo metodologiją, kaip taikyti šį įrankį fiskaliniam ir valdymo perėjimui. Įrankis yra universalus; žemiau pateikta metodologija yra viena galima taikymo galimybė.

8.1 Paskatų struktūra

Reputacija kaip kapitalas sukuria tiesiogines paskatas sąžiningam elgesiui. Įprastinėje veikloje dalyviai natūraliai kaupia reputaciją per kasdienius sandorius ir įvykdytus įsipareigojimus. Pagrindinės išlaidos tenka *neigiamiesiems* teiginiams—kitų padarytos žalos fiksavimui. Ši asimetrija skatina naudingą, patikimą elgesį: būti sąžiningam nekainuoja papildomai, o būti žalingam sukuria dokumentuotą pėdsaką, kurį kiti sumokės, kad išsaugotų. Veidmainystė—taisyklių deklaravimas jų nesilaikant—yra brangiausias žlugimo būdas, nes rodo tyčinį apgaudinėjimą.

8.2 Lygiagreti fiskalinė sistema

Trys komponentai įgalina konkurencinį spaudimą: (1) **Paprastas mokestis**—vienas proporcingas tarifas be išimčių, iš pradžių šiek tiek žemesnis už esamą efektyvųjį tarifą; (2) **Elektroninė išlaidų registracija (EIR)**—apverčianti Čekijos EET modelį, kad piliečiai stebėtų valstybės išlaidas; (3) **Piliečių valdomas mokesčių paskirstymas**—prasidedantis nuo kelių procentų pirmaisiais metais ir per dešimtmetį pasiekiantis bet kur nuo žemų dvizenklių skaičių iki visiškos migracijos prie piliečių valdomos sistemos, priklausomai nuo perėmimo tempo. Faktinis tempas priklauso nuo greičio, kuriuo atsiranda laisvosios rinkos alternatyvos valstybės paslaugoms, ir nuo valstybės noro bendradarbiauti pereinant; laiko funkcija neturi būti tiesinė, ir nėra priežasties nustatyti viršutinę ribą, kur perėmimas galiausiai gali atsirasti.

9 Migracijos kelias

Migracija vyksta per tris etapus (10 pav.): **1 etapas: Perdanga** (RSN kaip informacinis sluoksnis, valstybė yra vienintelis teikėjas), **2 etapas: Konkurencija** (RSN teikia funkcinės alternatyvas, dviejų sistemų naudojimas) ir **3 etapas: Perėjimas** (RSN lenkia valstybės atitikmenis, savanoriška migracija). Perėjimas yra grįžtamas kiekviename etape.

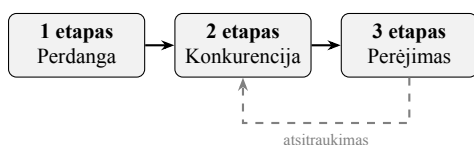


Figure 10: Trijų etapų migracija—grįžtama kiekviename etape.

Pagrindinis spaudimo mechanizmas yra fiskalinis: kai sąlyginiai mokesčių mokėtojai pasiekia

„ekonomiškai reikšmingą mažumą X “—grupę, pakankamai didelę, kad represijos prieš ją sukeltų netrivialią ekonominę žalą, o pilietinis nepaklusnumas taptų patikima grėsme—valstybė pradeda derybas. Iliustracijai naudojame $X \approx 15\%$ BVP, bet faktinė riba priklauso nuo konkrečios ekonomikos.

10 Saugumo analizė

Nagrinėjame penkias priešininkų kategorijas: individualius blogus veikėjus, organizuotas grupes, korporacinius priešininkus, valstybinio lygio priešininkus ir protokolo lygio priešininkus.

Atsparumas Sybil atakoms [12]. Reputacijos kaupimas reikalauja nuolatinės, patikrinamos sąveikos. Sėkmingos Sybil atakos kaina auga tiesiškai su netikromis tapatybėmis ir kvadratiškai su tiksline reputacijos riba. Kelių DID valdymas lygiagrečiai yra įmanomas, bet brangus pagal projektą—kiekviena tapatybė turi savarankiškai sukaupti reputaciją per tikrą veiklą. Laisvose visuomenėse šie kaštai atgraso nuo atsitiktinio piktnaudžiavimo; diktatūrose lygiagretūs DID tampa išgyvenimo įrankiu, įgalinančiu suskaidytą pasipriešinimą, pagrindinį koordinavimą ir saugesnę juodosios rinkos navigaciją.

Apsauga nuo slapto susitarimo. Abipusio patvirtinimo šablonai tarp uždarų grupių yra aptinkami per socialinio grafo analizę. Reputacijos apibendrinimo funkcijos nuvertina teiginius iš glaudžiai susigrupavusių šaltinių.

Valstybinio lygio priešininkas. Onion maršrutizavimas, centralizuotos infrastruktūros nebuvimas ir Tikrintojų vaidmens paskirstymas visoje dalyvių bazėje užtikrina, kad slopinimas reikalauja priemonių, neproporcingų bet kokiai naudai.

Privatumas prieš atskaitomybę. Pseudonimiškumas—tarpinė padėtis tarp anonimiškumo ir tapatybės atskleidimo—leidžia DID kaupti prasmingą reputaciją neatskleidžiant turėtojo realaus pasaulio tapatybės.

11 Privatumo aspektai

RSN privatumo modelis remiasi pseudonimiškumu. Turėtojas kontroliuoja tapatybės atskleidimą: minimalus (grynas pseudonimas), selektyvus (susieti konkretūs kredencialai) arba pilnas (susieta teisinė tapatybė). Paskelbti teiginiai yra nuolatiniai—sistema palaiko kontekstinį taisymą, bet ne ištrynimą. Turėtojas gali atsisakyti pažeisto DID ir pradėti iš naujo, atsisakydamas sukauptos reputacijos.

12 Susiję darbai

W3C DID Core specifikacija [2] ir Ceramic Network [8] teikia tapatybės pagrindą. EigenTrust [13] pademonstravo paskirstytą reputacijos apibendrinimą be centrinės institucijos. SBT [3] įvedė neperduodamus socialinius žetonus. RSN skiriasi savo dėmesiu ekonominiams kaštams kaip kokybės filtrui ir mechanizmui radikalumui įkainoti.

DAO [4] ir kvadratinis balsavimas [5] pademonstravo decentralizuoto valdymo įgyvendinamumą. RSN išveda konsensą iš dvišalių kainos derybų, o ne iš balsavimo.

Pasiūlymas remiasi anarcho-kapitalistine teorija [14, 15] dėl privataus paslaugų teikimo, bet skiriasi dviem esminiais aspektais: jis projektuoja pyktį ir keršto impulsus, o ne prisiima racionalumą, ir siūlo laipsnišką perėjimą, o ne revoliuciją. Emergentinių socialinių sutarčių koncepcija turi pirmtakų Hayeko spontaniškos tvarkos teorijoje [16].

Anarcho-agorizmas. RSN turi reikšmingų sąlyčio taškų su agoristine kontra-ekonomika [17]—ypač akcentu statyti lygiagrečias institucijas ir savanoriškus mainus. Tačiau agorizmas linkęs prisiimti racionalų savanaudiškumą kaip pakankamą koordinavimo mechanizmą ir dažnai stokoja konkretaus migracijos kelio nuo esamų valstybės struktūrų. RSN aiškiai įtraukia neracionalius elgesio polinkius ir teikia fiskalinį spaudimo mechanizmą laipsniškam perėjimui.

Meritokratija. RSN gali atspindėti pirmąjį funkcinį aprašymą, kaip meritokratija [18] gali atsirasti kaip sisteminė savybė, o ne šūkis. Tradicinės meritokratinės sistemos žlunga, nes reikalauja centrinės institucijos „nuopelnams“ apibrėžti ir įgyvendinti. RSN nuopelnai atsiranda iš dvišalių vertinimų: tie, kurie teikia vertę, kaupia reputaciją; joks komitetas nesprenžia, kas turi nuopelnų.

Nuosavybė kaip privilegija. RSN iš esmės skiriasi nuo anarcho-kapitalistinio ir Austrijos mokyklos nuosavybės teisių kaip natūralių ir absoliučių traktavimo. RSN sistemoje nuosavybė yra *privilegija*—socialinis pripažinimas, kuris kraštutiniais atvejais gali būti atimtas bendruomenės, kai dalyvis iš esmės pažeidžia bendras normas (išdavystė, atsisakymas ginti bendruomenę egzistencinės krizės metu, sisteminis išnaudojimas). Tai nėra valstybės nusavinimas, o socialinio pripažinimo atėmimas dvišalių santykių tinklo.

13 Diskusija ir apribojimai

Šaltas startas. RSN vertė priklauso nuo tinklo efektų; ankstyvieji perėmėjai susiduria su ribota verte, kol dalyvavimas nepasiekia ribos. Tačiau net nuo ankstyvųjų etapų DID tinklas tarnauja kaip naudingas papildomas informacijos šaltinis. Tikimasi, kad ankstyvasis reputacijos vertinimas ir autoriteto įvertinimas vystysis palaipsniui, didėjant sudėtingumui.

Apsauga nuo išnaudojimo ir prieigos kontrolė. Tiksliniai DID gali nustatyti laipsniškus mokesčius ir prieigos apribojimus užklausoms iš žemos reputacijos DID. Tai nėra dvejetainis, o tolydi skalė: kuo mažiau reputacijos turi užklausiantis DID, tuo mažiau informacijos jis gauna, tuo ilgiau laukia ir tuo daugiau moka. Šis mechanizmas skatina tikrą dalyvavimą, o ne pasyvų vartojimą.

Prieigos nelygybė. Teiginių skelbimo kaina gali atfiltruoti teisėtus nusiskundimus iš ekonomiškai nepalankioje padėtyje esančių dalyvių. Sušvelninimas: kiekvienas dalyvis vienu metu tarnauja kaip potencialus tikrintojas (arba deleguoja šį vaidmenį) ir uždirba tikrinimo mokesčius. Per pakankamą laiko horizontą neradikalus dalyvis turėtų priartėti prie finansinio neutralumo—tikrinimo pajamos maždaug kompensuoja skelbimo kaštus. Tai statistinis lūkestis, o ne garantija.

Reputacijos nelygybė. Ankstyvieji perėmėjai kaupia pranašumus, kurie gali sukurti kliūtis vėlyviesiems. Tačiau reputacijos vertinimą atlieka trečiųjų šalių teikėjai, kurie gali pasirinkti sušvelninti pirmtako pranašumą per savo apibendrinimo algoritmus. Būti pirmam su gera reputacija yra teisėtas lyginamasis ekonominis pranašumas—ir tai yra pagal projektą.

Atviri klausimai. Optimalios kaštų funkcijos, apibendrinimo standartai, protokolo valdymas ir sąveika su DI sugeneruotais sintetiniais reputacijos duomenimis lieka būsimo darbo sritimis.

Šis straipsnis neteigia, kad RSN sukurs optimalius rezultatus visomis aplinkybėmis. Jis teigia, kad RSN atspindi *įgyvendinamą* alternatyvą—techniškai realizuojamą, ekonomiškai save išlaikančią ir socialiai suderinamą su žmogaus elgesio polinkiais tokiais, kokie jie iš tikrųjų yra.

14 Išvados

Šiame straipsnyje pristatytas reputacijos socialinis tinklas—decentralizuotas protokolas, įgalinantis pseudonimišką, patikrinamą reputacijos mainai. Bran-
gaus radikalumo principas užtikrina, kad apgaulingi

teiginiai būtų įkainojami už ribų be cenzūros. Siūlomas migracijos kelias įgalina laipsnišką, grįžtamą perėjimą nuo esamų institucijų. Projektas įtraukia žmogaus prigimtį tokią, kokia ji yra—įskaitant smulkmeniškumą, pyktį ir keršto pasitenkinimo troškimą—o ne reikalauja ideologinės transformacijos. Rezultatas yra ne utopija, o sistema, kurioje teisingumas yra prieinamas, reputacija yra užsitarnaujama, o netinkamo elgesio kaina tenka tai šaliai, kuri jį sukėlė.

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.