Detsentraliseeritud reputatsioonivõrk: Raamistik ühiskonna loomulikuks korralduseks

Pavel Kudrna
Praha, Tšehhi
Mustand v1 — märts 2026

Abstract

Õiglustunne—veendumus, et ülekohus heastatakse ja teened saavad tasu—on ühiskonna tugevaim ühendav jõud. Kui tsentraliseeritud valitsemisinstitutsioonid ei suuda seda tunnet pakkuda, sest õiguse jõustamise kulu ületab õiguse enda väärtuse, siis sotsiaalne sidusus mureneb. Praegused institutsionaalsed struktuurid ei suuda lahendada olulist osa vaidlustest süstemaatiliselt samamoodi, nagu tsentraalne planeerimine ei suuda ressursse jaotada: infoasümmeetria, puuduvate tagasisidesilmuste ning otsustajate lahutatuse tõttu oma otsuste tagajärgedest. See artikkel esitab reputatsiooni-suhtlusvõrgustiku (Reputation Social Network, RSN): detsentraliseeritud, korrumpeerimatu ja tsensuurikindla suhtluskihi, mis on ehitatud detsentraliseeritud identifikaatoritele (Decentralized Identifiers, DID) ja mis võimaldab pseudonüümsetel osalejatel avaldada, kontrollida ja tarbida reputatsiooniteavet reaalse maailma käitumise kohta. Põhimehhanism tugineb kolmele projekteerimispõhimõttele: (1) asümmeetriline kulustruktuur, kus reputatsiooniandmete lugemine on odav, kuid kirjutamine nõuab kontrollitavat pingutust; (2) mittedeterministlik kontrollijate valimise protokoll, mis põhineb järjepideval räsimisel (consistent hashing) ja hinnastab radikaalsed väited kasvavate iteratsioonikulude kaudu; ning (3) turupõhine reputatsiooniautoriteedi mudel, kus eraviisilised kontrollijad panevad oma kogunenud reputatsiooni kaalule nende väidete täpsuse eest, mida nad kinnitavad. Sellest tulenev arhitektuur loob esilekerkiva meritokraatia ilma tsentraalse koordineerimiseta ning võimaldab järkjärgulist ja pöörduvat üleminekuteed olemasolevatelt riigi hallatavatelt süsteemidelt.

1 Sissejuhatus

1.1 Tsentraliseeritud usalduse probleem

Kaasaegne valitsemine tugineb ühele põhimõttelisele eeldusele: et tsentraliseeritud institutsioonid suudavad vahendada usaldust võõraste vahel suures mastaabis. Kohtud lahendavad vaidlusi. Registrid tõendavad omandit. Reguleerivad asutused jõustavad standardeid. Need institutsioonid loodi ajastul, mil teave oli napp, suhtlus aeglane ning võimu delegeerimine tsentraalsele organile oli ainus teostatav koordineerimismehhanism. Tsentraliseeritud valitsemine aga ebaõnnestub samadel struktuurilistel põhjustel nagu tsentraalne planeerimine: infoasümmeetria, puuduvad tagasisidesilmused ning otsustajate lahutatus oma otsuste tagajärgedest.

See eeldus ebaõnnestub näiteks siis, kui institutsionaalse vahendamise kulu ületab vaidluse väärtuse. Vaatleme üürnikku, kes avastab, et tema üüritud korteril puudub seaduslikult nõutav elektriohutuse tunnistus—seisund, mis kujutab endast vahetut ohtu elule. Üürniku seaduslik õigus lepingust taganeda on ühemõtteline. Ometi ületab selle õiguse jõustamise kulu kohtusüsteemi kaudu tagatisraha ja hüvitatava kahju rahalise väärtuse, isegi arvestades võimalikku seadusjärgset kompensatsiooni [1]. Ratsionaalne vastus on kahju kanda ja lahkuda.

See ei ole patoloogiline erandjuhtum. See on vaikimisi kogemus olulise klassi vaidluste puhul, kus kahju on reaalne, kuid rahaline panus jääb allapoole künnist, mille juures institutsionaalne jõustamine muutub majanduslikult ratsionaalseks. Tulemuseks on süsteem, mis struktuurilt soosib pahatahtlikke tegutsejaid: need, kes kahjustavad teisi selle künnise alla jäävates mahtudes, saavad tegutseda karistamatult, sest õiguse otsimise kulu langeb kahjustatud poolele.

Ülaltoodud näide pärineb autori õiguskeskkonnast—Tšehhi tsiviilõigussüsteemist. Teistes õigustraditsioonides—pretsedendipõhises üldõiguses, tavaõiguses, segasüsteemides—

ebaõnnestub õiglus erineval viisil ja erineval määral sõltuvalt jurisdiktsiooni kultuurilistest ja menetluslikest eripäradest. Lugejad tunnevad tõenäoliselt ära samaväärseid näiteid oma kontekstist. Struktuuriliselt universaalne on muster: vaidlused, mille väärtus jääb allapoole majanduslikult ratsionaalse jõustamise künnist, lõppevad sellega, et kahju kannab kahjustatud pool. RSN ei luba täiuslikku õiglust—see üksnes vähendab struktuurilist eelist, mida pahatahtlikud tegutsejad naudivad siis, kui institutsionaalne jõustamine on ebaökonoomne.

1.2 Miks olemasolevad lahendused ei ole piisavad

Detsentraliseeritud identiteedi (DID) raamistikud [2] pakuvad krüptograafilisi mehhanisme iseseisvaks identiteedihalduseks, kuid keskenduvad peamiselt identiteedi kontrollimisele, käsitlemata laiemat käitumusliku reputatsiooni küsimust.

Hingega seotud märgid (Soulbound Tokens, SBT) [3] tabavad tõdemuse, et reputatsioon ei ole ülekantav, kuid tuginevad plokiahela taristule koos skaleeritavuse piirangutega ega käsitle teabe sisestamist reguleerivaid majanduslikke stiimuleid. Sarnased kontseptsioonid, nagu teenete märgid (nt Liberland), jagavad sarnast filosoofiat, kuid jäävad seotuks konkreetsete jurisdiktsiooniliste raamistikega.

Detsentraliseeritud autonoomsed organisatsioonid (DAO) [4] rakendavad valitsemist nutilepingute kaudu, kuid taastoodavad plutokraatlikku dünaamikat, kus mõjuvõim on proportsionaalne kapitaliga. Ruuthääletus [5] leevendab seda osaliselt, kuid piirab praktilist kasutuselevõttu. DAO-d seisavad silmitsi ka põhimõttelise *oraakliprobleemiga*: nutilepingud ei suuda usaldusväärselt kontrollida reaalse maailma seisundeid ilma usaldusväärse välise allikata ning sellel probleemil pole plokiahela arhitektuuri sees üldist lahendust.

Ükski olemasolev süsteem ei ühenda detsentraliseeritust, tsensuurikindlust, pseudonüümsust, kontrollitavat sisenemiskulu ja esilekerkivat konsensust.

1.3 Panus

See artikkel annab järgmise panuse:

1. **Reputatsiooni-suhtlusvõrgustiku (RSN)** määratlus—detsentraliseeritud protokoll, mis laiendab DID-raamistikku kahepoolse reputatsioonivahetuse toetamiseks.
2. **Mittedeterministlik kontrollijate valimise protokoll**, mis põhineb järjepideval räsimisel [6].
3. **Kalli radikalismi põhimõte**, mis hinnastab väited vastavalt nende kaugusele võrgu konsensusest kolme liituva kulukanali kaudu.
4. **Reputeeritud autoriteedi mudel** asümmeetriliste stiimulitega, kus vale kinnitamine maksab katastroofiliselt rohkem kui õiguspärane tasu.
5. **Järkjärguline üleminekutee** paralleelse fiskaaltaristu kaudu.

2 Projekteerimispõhimõtted

RSN-i arhitektuur on piiratud viie läbiräägitamatu projekteerimispõhimõttega.

Järjepidevus ja areng. Süsteem eksisteerib koos olemasolevate institutsioonidega määramata pikkusega üleminekuperioodil. Üleminek peab olema pöörduv igas etapis.

Vabatahtlikkus ja vastutus. Osalemine on vabatahtlik, kuid vabatahtlikkus on seotud vastutusega: osaleja, kes võtab enda kanda institutsionaalse funktsiooni juhtimise, võtab samaaegselt enda kanda ka sellega kaasnevad kohustused.

Mitmekesisus ja kultuuriline neutraalsus. Konsensus kerkib esile kahepoolsetest interaktsioonidest, mitte süsteemi loojate seatud etteantud reeglitest.

Vastupidavus ja tsensuurikindlus. Võrgu tsenseerimise kulu peab ületama selle sallimise kulu. Ainult täielik totalitarism—laostava poliitilise ja majandusliku hinnaga—suudab süsteemi maha suruda.

Konsensus ja jõustamine. Süsteem hõlmab inimlikke kalduvusi väiklusele, kiusule ja kättemaksurahuldusele kandvate elementidena. Üleastumine ei ole keelatud; see on hinnastatud.

3 Süsteemi ülevaade

3.1 Reputatsiooni-suhtlusvõrgustik

RSN on detsentraliseeritud, otspunktist otspunkti suhtluskiht, milles osalejad vahetavad kontrollitavat teavet reaalse maailma käitumise kohta. Selle määravad omadused on: detsentraliseeritud ja tsenseerimatu taristu; pseudonüümne osalemine DID-ide kaudu; asümmeetriline kulustruktuur (lugemine on odav, kirjutamine kallis); krüptograafiline kontrollitavus; ja **standardite tugi**—masinloetavad vormingud võrgu kaudu levitatavale teabele, autori-

teetide pakutavatele teenustele (väite koostamine, kinnitamine, tunnistajateenus) ning poliitikavormingule, mis hõlmab reegleid vastaspoole reputatsiooni hindamiseks ja poliitika mittevastavuse riski (deklareeritud ja tegeliku käitumise vahel) hindamiseks.

3.2 Arhitektuurikomponendid

RSN koosneb neljast põhikomponendist (joonis 1):

1. **DID-kiht.** Osalejate identiteedid koos deklareeritud reeglite, reputatsiooni metaandmete ja võrgu marsruutimisega.
2. **Väiteprotokoll.** Struktureeritud vorming väidete avaldamiseks reaalse maailma sündmuste kohta.
3. **Kontrollivõrk.** Detsentraliseeritud protokoll kontrollijate määramiseks järjepideva räsimise abil.
4. **Reputatsiooni koondamise kiht.** Teenused, mis loovad inimloetavaid reputatsioonikokkuvõtteid.

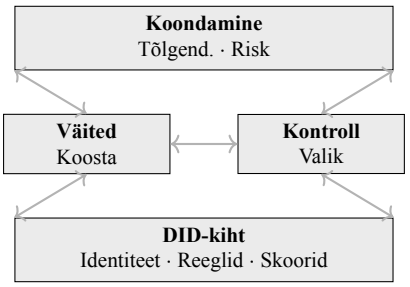

Figure 1: RSN-i neljakihiline arhitektuur.

3.3 Osalejate rollid

Kontrollitehing hõlmab kuni kuut eraldiseisvat DID-rolli (joonis 2): **Väljaandja** (DID_I, loob ja esitab väite), **Subjekt** (DID_S, DID, mille kohta väide käib—võib kattuda Väljaandjaga), **Autoriteet** (DID_A, kinnitab väite tasu eest; võib pakkuda ka tunnistajateenuseid—*valikuline*), **Tunnistaja** ($DID_{W_{1..n}}$, kontrollija aususe inkognito jälgija väljakutsekoodide abil—*valikuline*), **Kontrollija** (DID_V, algoritmiliselt valitud väidet avaldama) ja **RSN** (võrk, kus kontrollitud väited avaldatakse). Iga roll võib olla delegeeritud teisele DID-ile (jaotis 7.4). Autoriteet komplekteerib kinnitamise sageli koos tunnistajateenustega, kuid need kaks funktsiooni on loogiliselt sõltumatud.

3.4 Korrumpeerimatus: neli jõudu

RSN-i korrumpeerimatus ei tulene ühest mehhanismist, vaid neljast samaaegsest jõust. Ükski neist ei ole iseseisvalt piisav; ainult nende kombinatsioon muudab korruptsioonikatse majanduslikult ebaratsionaalseks.

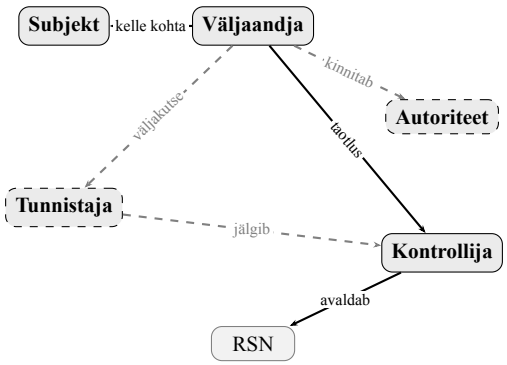

Figure 2: DID-rollid kontrollitehingus. Katkendjoon = valikuline (Autoriteet, Tunnistaja).

Ettearvamatu sihtmärk. Iga väite kontrollija valitakse mittedeterministlikult järjepideva räsimise abil (jaotis 5.3). Ründaja ei saa konkreetset kontrollijat altkäemaksuks ette sihikule võtta, sest kontrollija identiteet on väite sisu ja varasemate iteratsioonide funktsioon, mitte väljaandja valik.

Reputatsiooni võimendus—aeglaselt üles, kiiresti alla. Reputatsiooni saab omandada üksnes järkjärgult, püsiva järjepideva käitumise kaudu. Selle võib aga katastroofiliselt kaotada ühe pettusliku kinnitamisega (jaotis 6.2). See asümmeetria tähendab, et aastatega kogunenud reputatsiooni võib hävitada üksainus ebaaus kinnitamine; optimaalseks strateegiaks jääb kahtlaste väidete tagasilükkamine.

Avalik lubadus. Iga DID-i valdaja deklareerib avalikult oma poliitika—masinloetava reeglistiku, mida ta kohustub järgima. Lahknevus deklaratsiooni ja tegeliku käitumise vahel on tuvastatav ja hinnastatud reputatsioonirikkumisena, mis on raskem kui aluseks olev rikkumine ise (jaotis 7.3). Silmakirjalikkus on seega kulukam kui otsene ebaausus.

Võrgustiku ründekulu asümmeetria. Võrgu tsenseerimise või destabiliseerimise kulu kasvab mittelineaarselt koos võrgu suuruse ja tihedusega, samas kui selle sallimise kulu jääb konstantseks. Et tsensuur end ära tasuks, peaks tsentraliseeritud tegutseja rakendama seda kogu võrgu ulatuses—nõudes meetmeid, mis on ebaproportsionaalsed igasuguse kujuteldava kasuga (jaotis 10).

4 Detsentraliseeritud identiteedi mudel

4.1 DID eriomadustega

RSN laiendab W3C DID Core spetsifikatsiooni [2] järgmisega: **Deklareeritud reeglid** (masinloetavad käitumuslikud kohustused), **Reputatsiooni metaandmed** (koondatud käitumuslik skoor) ja **Võrgu marsruutimine** (muudetav sibulavärav, eraldi stabiilsest ringiasendist).

4.2 Väite elutsükkel

Väide läbib kuus etappi (joonis 3): koostamine, valikuline autoriteedi kinnitamine, kontrollija valimine järjepideva räsimise abil, kontrollimisotsus (heakskiit või tagasilükkamine koos iteratsiooniga), avaldamine ja reputatsiooni uuendamine kõigi osapoolte jaoks.

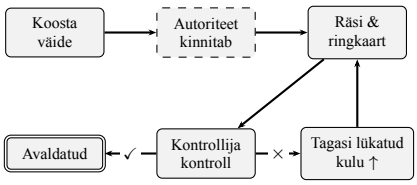

Figure 3: Väite elutsükkel koos iteratsioonisilmusega.

4.3 Suhe W3C DID Core'iga

RSN-i identiteedimudel on W3C DID Core spetsifikatsiooni [2] korrektne ülemhulk. Kõik RSN-i DID-id on kehtivad W3C DID-id. RSN-spetsiifilised laiendused on kodeeritud DID-dokumendi omadustena, mis on määratletud spetsiaalses DID-meetodi spetsifikatsioonis, ühilduvana olemasoleva taristuga nagu ION [7] ja Ceramic [8].

5 Teabe kontrollimine ja levitamine

5.1 Teabe sisestamise kulu

RSN-i keskne majanduslik põhimõte on asümmeetria lugemise ja kirjutamise vahel. Reputatsiooniandmete lugemine läheneb nullilähedasele piirkulule osalejate jaoks, kes on osa DID-võrgust ja kellel on nende reputatsioonile vastav juurdepääs—uustulnukad peavad järk-järgult teenima laiema juurdepääsu (vt parasiitluse tõkestamine). Kirjutamine—mõistetuna kui reputatsiooni püsiv materialiseerumine võrku, mitte kui ühekordne tehniline akt—nõuab kontrollitavat kumulatiivset investeeringut kolmes mõõtmes: **aeg** (järjepidevale käitumisele, täidetud kohustustele ja kultiveeritud suhetele kulutatud eluaastad), **energia** (ausasse tegutsemisse, partnerlussuhete hoidmisse ja pikaajalisse usaldusväärsusesse investeeritud pingutus) ja **raha** (investeering oma nimesse—erialane areng, oma töö kvaliteet, tekitatud kahjude hüvitamine). Reputatsiooni ei saa hetkega osta—see on eluaegse kogunemise tulemus, mille süsteem üksnes muudab nähtavaks ja kontekstideüleselt ülekantavaks. Protokolli ühekordsed tehnilised kulud (krüptograafilised allkirjad, kontrollijatasud) on selle aluseks oleva investeeringuga võrreldes tühised.

5.2 Sotsiaalne graaf ja kontaktide sügavus

RSN on olemuslikult sotsiaalne võrgustik: iga DID lisab kontakte (teisi DID-e), kes ühenduse lubavad. Neil kontaktidel on oma kontaktid ja nii edasi. Algoritmiline kontrollijate otsing toimib seotud kontaktide seadistatava sügavuse h piires (nt $h = 3$: enda otsekontaktid, nende kontaktid ja kontaktide kontaktid). See arhitektuur ei nõua ühte globaalset plokiahelat—see soosib loomulikult kogukondade/klastrite esilekerkimist koos kattumistega teistesse kogukondadesse. Igal DID-osalejal peab olema avaldatud **poliitika**—masinloetav reeglistik, mis reguleerib, kuidas sissetulevaid taotlusi hinnatakse. Poliitika rikkumised salvestatakse võrku negatiivsete artefaktidena.

5.3 Algoritmiline kontrollijate valimine

Kontrolliprotokoll kasutab järjepidevat räsimist [6] (joonis 4). Kontrollimine on tasuline teenus: kontrollijad tegutsevad tasu eest, luues turu, kus konkurents suunab hinnastamist, kiirust ja usaldusväärsust.

Samm 1. Väitedokument liidetakse eelmise iteratsiooni räsitulemusega (või $\varnothing$ esimesel iteratsioonil) ja räsitakse:

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

Algoritm peab hõlmama kõigi varasemate taotluste ja vastuste *täieliku tee*—mitte üksnes eelmise iteratsiooni räsi. Iga kontrollija täielik vastus (heakskiit, tagasilükkamine, pakutud hind, põhjus) lisatakse kasvavale dokumendile, mis on kontrollitav krüptograafiliste allkirjade abil igas etapis.

Samm 2. Räsi kaardistatakse N asendile järjepideva räsiringi peal, ühtlaselt jaotatuna (nt $N = 4$ korral: $+0°, +90°, +180°, +270°$). Igast asendist valib päripäeva otsing lähima DID-i kontrollijakandidaadiks (joonis 5). N on muutuv parameeter, mis võib sõltuda hetkel aktiivsete DID-ide protsendist, kellaajast või võrgu ajaloolisest reageerimiskiirusest.

Samm 3. Kontrollija kas nõustub (avaldab, pannes reputatsiooni kaalule) või lükkab tagasi (naastes sammu 1 juurde tagasilükkamise räsiga). Kui sõlm ei reageeri hoolimata veebis-oleku deklareerimisest, peab järgmine taotlus sisaldama kõiki vastuseid kõigilt N varasemalt kontrollijakandidaadilt.

Parasiitluse tõkestamine. Siht-DID-id võivad seada tasud või juurdepääsupiirangud vähese reputatsiooniga uute DID-ide päringutele. See astmeline mehhanism (mitte binaarne) sunnib uustulnukaid ehitama reputatsiooni ehtsa tegevuse kaudu, enne kui nad saavad vabalt teiste andmeid tarbida.

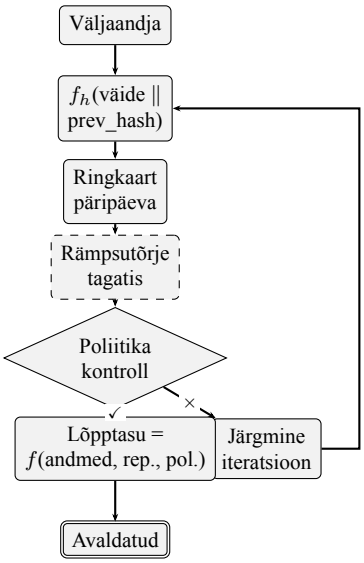

Figure 4: Kontrollija valimise protokoll. Rämpsutõrje tagatis on valikuline ja võib olla tagastatav. Lõpptasu makstakse ainult heakskiidu korral.

Iga tagasilükkamine lisab väitedokumendile kontrollija täieliku vastuse (kaasa arvatud põhjused ja tingimused), laiendades selle sisu. Laiendatud dokumendist arvutatakse mittedeterministlikult uus räsi, mis kaardistub teisele ringiasendile ja valib teise kontrollija. Täieliku tee dokumenteerimine on kohustuslik—väljaandja ei saa järgmist kontrollijat ennustada ega mõjutada. Kui kontrollija ignoreerib taotlust hoolimata ühilduvast deklareeritud poliitikast, salvestavad tunnistajad (kui neid on) selle ning väljaandja võib lõplikul avaldamisel lisada tunnistaja tõendid.

5.4 Tunnistajaprotokoll

Tunnistaja roll pakub inkognito vastutust kontrollija aususe eest krüptograafilise väljakutsekoodi protokolli kaudu:

Samm W1. Taotleja allkirjastab kontrollitaotluse ja saadab selle N_w tunnistajale—taotleja sotsiaalvõrgustiku kontaktid või spetsialiseeritud tunnistajateenuse pakkujad, kes tegutsevad tasu eest.

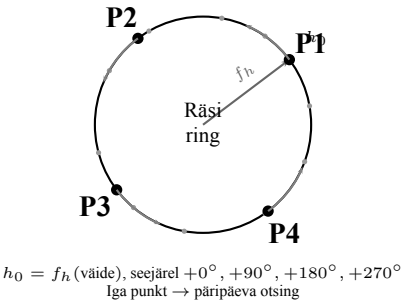

Figure 5: Mitmepunktiline valik (N=4). Räsi h_0 määrab nihke; 4 punkti ühtlaselt jaotatud alates h_0.

Samm W2. Iga tunnistaja w_i allkirjastab kogu allkirjastatud taotluse, säilitab originaalallkirja σ_i ja arvutab väljakutsekoodi $c_i = h(\sigma_i)$. Väljakutsekood lisatakse taotlusele.

Samm W3. Taotlus, mis nüüd kannab N_w väljakutsekoodi, saadetakse kontrollijale. Kontrollija näeb koode, kuid *ei suuda kindlaks teha*, kes on tunnistajad ega kas koodid vastavad tegelikele allkirjadele.

Samm W4 (aus kontrollija). Kui kontrollija reageerib vastavalt oma deklareeritud poliitikale, jäävad väljakutsekoodid läbipaistmatuks. Tunnistajaid ei avalikustata kunagi. Täiendavaid andmeid ei avaldata.

Samm W5 (poliitika rikkumine). Kui kontrollija rikub oma poliitikat (ignoreerib taotlust, reageerib ebajärjekindlalt), hoiab taotleja tunnistajate originaalallkirju σ_i. Need saab avaldada kaasandmetena: igaüks saab kontrollida, et $c_i = h(\sigma_i)$, tõestades, et tunnistaja oli kohal. Taotleja saab avaldada iseseisvalt—kontrollija on väljakutsekoodid oma vastuses juba allkirjastanud.

Blufi omadus. Taotleja võib asendada mõned või kõik väljakutsekoodid juhuslike väärtustega. Kontrollija ei suuda eristada ehtsaid koode (mida toetavad kõrge reputatsiooniga autoriteedid) mürast. See *ebakindlus* on jõustamismehhanism: iga taotlus kannab riski, et austusväärne autoriteet jälgib inkognito. Selle surve ülalhoidmise kulu on peaaegu null (juhuarvude genereerimine), samas kui ebaaususe potentsiaalne kulu kontrollijale on katastroofiline. Ausat käitumist stimuleeritakse isegi tegelike tunnistajate puudumisel.

Autoriteet tunnistajana. Autoriteet, kes kinnitab väite, võib komplekteerida tunnistajateenuseid: „Ma kinnitan sinu väite ja tegutsen kontrollimise ajal inkognito tunnistajana.” See on loomulik ärimudel—autoriteedil on juba kontekst olemas. Siiski on need kaks rolli loogiliselt sõltumatud.

5.5 Kalli radikalismi põhimõte

Kolm kulukanalit liituvad samaaegselt (joonis 6):

Kanal 1: Iteratsioonikulu. Iga tagasilükkamine sunnib peale uue iteratsiooni, mis kulutab aega ja ressursse. Lineaarne kasv.

Kanal 2: Dokumendi paisumine. Iga iteratsioon lisab väitedokumendile kontrollija täieliku vastuse. Kasv on lineaarne, kuid baasnihkega: algne kandevus (väite sisu, autoriteedi kinnitus, krüptograafilised allkirjad) omab juba märkimisväärset suurust B_0. Kogusuurus pärast k iteratsiooni: $S(k) = B_0 + k \cdot \Delta$, kus Δ on keskmine vastuse suurus.

Kanal 3: Kontrollija riskipreemia. Risk on subjektiivne. Kontrollija hindab, kas taotleva DID-i deklareeritud poliitikad on vastuolus kontrollija enda kaubanduslike, sotsiaalsete või poliitiliste huvidega. Preemia võib eksponentsiaalselt kasvada koos tajutud kaugusega kontrollija „ideaalist": $P(d) = \alpha \cdot e^{\beta d}$, kus d on kontrollija subjektiivne kaugusmõõt. Väljaspool isiklikku keelupiiri võib kontrollija täielikult keelduda.

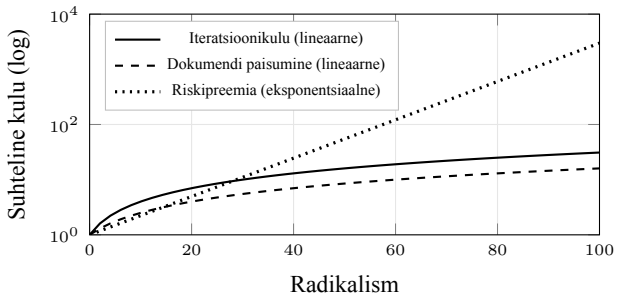

Figure 6: Kulude eskaleerumine kolme kanali ulatuses. Riskipreemia domineerib kõrge radikalismi juures.

Kriitiline on see, et tegemist ei ole tsensuuriga. Ükski väide ei ole keelatud. Süsteem hinnastab riski (tabel 1).

Table 1: Kulude võrdlus väidetüüpide lõikes.

Tüüp	Iter.	Dok	Tasu	Kokku
Usaldusväärne	$k_{\min}$	B_0	$P_{\min}$	Madal
Vastuoluline	k_{med}	$B_0{+}k\Delta$	$\alpha e^{\beta d}$	Mõõdukas
Radikaalne	$k_{\max}$	$\gg B_0$	$\gg P_{\min}$	Väga kõrge
Pettuslik	$\to \infty$	—	—	Avaldamatu

6 Reputatsioon ja riskihindamine

6.1 Reputatsiooni kogunemise mudel

Reputatsioonil on kolm omadust: **aeglane kogunemine** (järkjärguline kasv järjepideva käitumise kaudu), **kiire hävimine** (üksainus pettus võib skoori katastroofiliselt vähendada) ja **individuaalne hindamine** (iga tarbiv osapool võib rakendada oma koondamisfunktsiooni).

6.2 Reputeeritud autoriteedid

Reputeeritud autoriteet vaatab väited üle ja, kui on rahul, kaasallkirjastab need—pannes kaalule oma reputatsiooni (joonis 7). Asümmeetria on tahtlik: reputatsiooni kogumine on aeglane (järkjärguline $+\delta$ iga ausa kinnitamise kohta), samas kui selle kaotamine on katastroofiline ($-\Delta \gg \delta$ iga vale kinnitamise kohta; illustreerivalt nt $+2\%$ vs. -70%). Optimaalne strateegia on alati lükata kahtlased väited tagasi. δ ja Δ konkreetsed väärtused on süsteemi parameetrid.

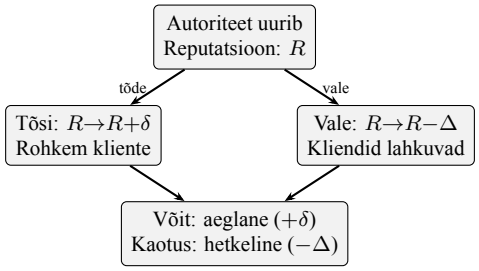

Figure 7: Reputeeritud autoriteet—asümmeetrilised stiimulid.

6.3 Mitmemõõtmeline reputatsioon

Reputatsioon ei ole skalaar, vaid vektor mitme mõõtme ulatuses: finantsusaldusväärsus, isiklik ausus, erialane kompetents, kodanikuaktiivsus ja teised (joonis 8). Erinevad hindamisteenuse pakkujad projitseerivad seda vektorit erinevalt sõltuvalt kontekstist—laenuandja seab esikohale finantsusaldusväärsuse, tööandja erialase kompetentsi, naaber kodanikukäitumise. Puudub üksainus „õige" reputatsiooniskoor; on ainult vaatenurgad.

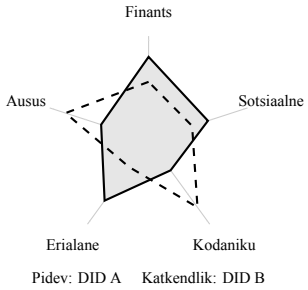

Figure 8: Mitmemõõtmelised reputatsioonivektorid. Erinevad DID-id ilmutavad mõõtmete lõikes erinevaid profiile.

6.4 Demokratiseeritud riskihindamine

RSN demokratiseerib süstemaatilise riskihindamise—võimekuse, mis on praegu koondunud finantsasutustesse, kuid mis on rakendatav kaugelt väljaspool pangandust. Tööstuskonglomeraadid, kes hindavad tarnijate usaldusväärsust, kindlustusseltsid, kes hinnastavad käitumuslikku riski, hoolsuskohustus ühinemistel ja ülevõtmistel, seadmete eluea hindamine tootmises—kõikjal, kus vastaspoole riski tuleb hinnata, pakub RSN detsentraliseeritud, turupõhist alternatiivi. Tõlgendusteenuste turg tõlgib toore mitmemõõtmelise reputatsiooniandmestiku tegutsemisvõimelisteks kokkuvõteteks, muutes vastaspoole hindamise kättesaadavaks igale osalejale piirkuluga.

7 Konsensus ja vaidluste lahendamine

7.1 Detsentraliseeritud õigluse mudel

RSN sõnastab õigluse ümber kahepoolse läbirääkimise probleemina. Püsiva, kontrollitava reputatsioonikahju oht on tõhusam heidutus kui kohtumenetlus, mida kahjustatud pool ei suuda endale lubada.

7.2 Esilekerkiv konsensus

Iga osaleja säilitab isikliku rahulululäve. Võrgu koondkonsensus kerkib esile tuhandete kahepoolsete läbirääkimiste statistilise keskmisena (joonis 9). Konsensusest kaugelt kõrgem vastus (barbaarne) on kallis avaldada. Konsensuse lähedane vastus (proportsionaalne) on odav. Konsensus ei ole reegel—see on hinnasignaal.

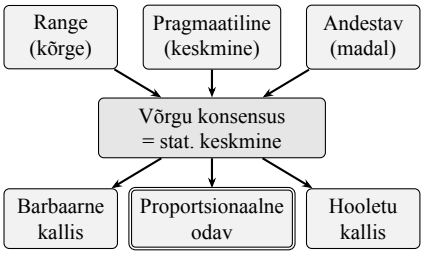

Figure 9: Esilekerkiv konsensus individuaalsetest rahulululävedest.

7.3 Karistuse kalibreerimine

Iga DID-i valdaja deklareerib avalikult reageeringud konkreetsetele üleastumiskategooriatele. Ebaproportsionaalselt karmid või leebed deklaratsioonid tõmbavad ligi negatiivseid reputatsioonisignaale. Proportsionaalsed deklaratsioonid võetakse vastu hõõrdumiseta—enesekalibreeruv karistussüsteem.

Konsensusdeklaratsioonid ise alluvad silmakirjalikkuse tuvastamisele: deklaratiivselt konsensuspositsiooni järgimise kohustuse võtmine, käitudes samal ajal ebajärjekindlalt, kujutab endast reputatsioonirikkumist, mis on raskem kui aluseks olev kõrvalekalle, sest see näitab tahtlikku pettust.

7.4 Delegeerimine

Kõik tegevused DID-i sees—ühe erandiga—võib delegeerida teisele DID-ile. **Subjekti roll—DID, kelle käitumisest väide räägib—ei ole delegeeritav; see on mitteülekantavalt seotud identiteedivaldajaga, keda väide puudutab.** Teised aktiivsed rollid—Väljaandja, Autoriteet, Tunnistaja, Kontrollija—saab üle anda määratud delegaat-DID-ile, olgu see kontrollimiseks, väite esitamiseks, konsensuses osalemiseks või vaidluste lahendamiseks. Delegeerimine on igal ajal tühistatav. See võimaldab spetsialiseerumist (nt professionaalsed kontrolliteenused), samal ajal kui valdaja säilitab lõpliku kontrolli ja vastutuse. Delegeerimine kehtib kogu süsteemi ulatuses ja on skaleeritavuse jaoks hädavajalik.

7.5 Individuaalselt moraalilt esilekerkivale ühiskondlikule lepingule

Iga DID-i deklareeritud poliitika kujutab endast individuaalse moraali vormistamist: mida valdaja peab vastuvõetavaks, kuidas ta reageerib konkreetsele käitumisele, mida ta nõuab vastaspooltelt. Neid poliitikaid ei kehtesta süsteemi looja—iga osaleja valib need ise ja väljendab neid masinloetaval kujul.

See vormistamine võimaldab kolmeastmelist esilekerkimist. Esiteks kodeeritakse individuaalne moraal **poliitikana**—deklareeritud reeglite, lävede ja reageeringufunktsioonide kogumina, mida DID kohustub järgima. Teiseks toodab kõigi poliitikate koondsumma kogu võrgu ulatuses **esilekerkiva eetika**—statistiliselt vaadeldavad normid, mida ükski osaleja ei projekteerinud, kuid mis tekivad tuhandete individuaalsete moraaliseisukohtade interaktsioonist [9]. Kolmandaks moodustavad need esilekerkivad eetikanormid, väljendatuna jagatud käitumuslike normidena, mis on jõustatud kahepoolsete hinnasignaalide kaudu, **mõõdetava ühiskondliku lepingu**—mitte teoreetilise konstruktsiooni, mille all keegi allkirja pole andnud [10], vaid empiiriliselt vaadeldava reeglistiku, mida toetab tegelik käitumine.

See protsess peegeldab moraalse alusteooria järeldusi [11]: inimmoraal on intuitiivne, pluralistlik ja kultuuriliselt varieeruv. RSN ei nõua moraalset konsensust sisendina; see toodab käitumusliku konsensuse väljundina. Sellest tulenev ühiskondlik leping ei ole staatiline—see areneb, kui osalejad liituvad, lahkuvad ja kohandavad oma poliitikaid vastavalt võrgu tagasisidele. Erinevalt klassikalisest ühiskondliku lepingu teooriast on see leping tühistatav, vaadeldav ja jõustatav ilma suverääni.

8 Majandusmudel

Eelnevad jaotised kirjeldasid tööriista—RSN-i kontrollimehhanisme, kulustruktuuri ja esilekerkivat konsensust. See jaotis kirjeldab metoodikat selle tööriista rakendamiseks fiskaal- ja valitsemisüleminekule. Tööriist on üldotstarbeline; alljärgnev metoodika on üks võimalik rakendus.

8.1 Stiimulistruktuur

Reputatsioon kapitalina loob otsesed stiimulid ausaks käitumiseks. Tavapärases toimimises ehitavad osalejad reputatsiooni loomulikult igapäevaste tehingute ja täidetud kohustuste kaudu. Peamine kulu on *negatiivsetel* väidetel—teiste tekitatud kahju talletamisel. See asümmeetria stimuleerib kasulikku ja usaldusväärset käitumist: aus olemine ei maksa midagi ekstra, samas kui kahjulik olemine loob dokumenteeritud jälje, mille säilitamise eest teised maksavad. Silmakirjalikkus—reeglite deklareerimine ilma neid järgimata—on kõige kallim tõrkerežiim, sest see näitab tahtlikku pettust.

8.2 Paralleelne fiskaalsüsteem

Kolm komponenti võimaldavad konkurentsisurvet: (1) **Lihtne maks**—üksainus proportsionaalne määr ilma eranditeta, algselt marginaalselt allpool olemasolevat efektiivset määra; (2) **Elektrooniline kulutuste registreerimine (ESR)**—Tšehhi EET-mudeli ümberpööramine, nii et kodanikud jälgivad riigi kulutusi; (3) **Kodaniku suunatud maksujaotus**—alustades esimesel aastal mõnest protsendist ja jõudes kümnendi järel kusagile madalatest kahekohalistest numbritest kuni täieliku üleminekuni kodaniku suunatud süsteemile, sõltuvalt kasutuselevõtu määrast. Tegelik tempo sõltub kiirusest, millega riigiteenustele tekivad vabaturu alternatiivid, ning riigi valmisolekust üleminekuga koostööd teha; aja funktsioon ei pea olema lineaarne ning puudub põhjus seada ülempiiri sellele, kuhu kasutuselevõtt lõpuks jõuda võib.

9 Üleminekutee

Üleminek toimub kolme faasi kaudu (joonis 10): **Faas 1: Kate** (RSN informatsioonilise kihina, riik ainus pakkuja), **Faas 2: Konkurents** (RSN pakub funktsionaalseid alternatiive, kahe süsteemi kasutus) ja **Faas 3: Üleminek** (RSN edestab riiklikke ekvivalente, vabatahtlik üleminek). Üleminek on pöörduv igas etapis.

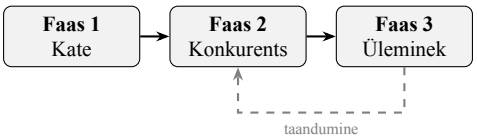

Figure 10: Kolmefaasiline üleminek—pöörduv igas etapis.

Peamine survemehhanism on fiskaalne: kui tingimuslikud maksumaksjad jõuavad „majanduslikult olulise vähemuseni X"—rühm, mis on piisavalt suur, et repressioon selle vastu põhjustab mittetriviaalset majanduslikku kahju ja kodanikuallumatus muutub usutavaks ohuks—astub riik läbirääkimistesse. Illustratsiooniks kasutame $X \approx 15\%$ SKP-st, kuid tegelik künnis sõltub konkreetsest majandusest.

10 Turvaanalüüs

Vaatleme viit vastasekategooriat: individuaalsed pahatahtlikud tegutsejad, organiseeritud rühmad, ettevõtlusvastased, riigitasandi vastased ja protokollitasandi vastased.

Sybil-kindlus [12]. Reputatsiooni ehitamine nõuab püsivat, kontrollitavat interaktsiooni. Eduka Sybil-rünnaku kulu skaleerub lineaarselt võltsidentiteetidega ja ruutsõltuvuses siht-reputatsioonitasemega. Mitme DID-i paralleelne käitamine on võimalik, kuid projekteerituna kulukas—iga identiteet peab reputatsiooni iseseisvalt koguma ehtsa tegevuse kaudu. Vabades ühiskondades heidutab see kulu juhuslikku kuritarvitamist; diktatuurides muutuvad paralleelsed DID-id ellujäämisvahendiks, mis võimaldavad lahterdatud vastupanu, maa-alust koordineerimist ja turvalisemat mustaturu navigeerimist.

Kokkumängu kaitse. Suletud rühmade vastastikuse kinnitamise mustrid on tuvastatavad sotsiaalse graafi analüüsi kaudu. Reputatsiooni koondamise funktsioonid diskonteerivad väiteid tihedalt klasterdunud allikatest.

Riigitasandi vastane. Sibulmarsruutimine, tsentraliseeritud taristu puudumine ja Kontrollija rolli jaotus osalejate baasi ulatuses tagavad, et mahasurumine nõuab meetmeid, mis on ebaproportsionaalsed igasuguse kasuga.

Privaatsus vs. vastutus. Pseudonüümsus—kesktee anonüümsuse ja identiteedi avaldamise vahel—võimaldab DID-idel koguda tähendusrikast reputatsiooni ilma valdaja reaalse identiteedi paljastamiseta.

11 Privaatsuskaalutlused

RSN-i privaatsusmudel on üles ehitatud pseudonüümsusele. Valdaja kontrollib identiteedi avaldamist: minimaalne (puhas pseudonüüm), valikuline (konkreetsed tunnistused seotud) või täielik (juriidiline identiteet seotud). Avaldatud väited on püsivad—süsteem toetab kontekstuaalset parandamist, kuid mitte kustutamist. Valdaja võib kompromiteeritud DID-i hüljata ja alustada uuesti, loobudes kogunenud reputatsioonist.

12 Seotud töö

W3C DID Core spetsifikatsioon [2] ja Ceramic Network [8] pakuvad identiteedi vundamendi. EigenTrust [13] demonstreeris hajutatud reputatsiooni koondamist ilma tsentraalse autoriteedita. SBT-d [3] tutvustasid mitteülekantavaid sotsiaalseid märke. RSN erineb oma rõhuasetusega majanduslikule kulule kvaliteedifiltrina ja oma mehhanismiga radikalismi hinnastamiseks.

DAO-d [4] ja ruuthääletus [5] demonstreerisid detsentraliseeritud valitsemise teostatavust. RSN tuletab konsensuse kahepoolsetest hinnaläbirääkimistest, mitte hääletusest.

Ettepanek toetub anarhokapitalistlikule teooriale [14, 15] eraviisilise teenusepakkumise osas, kuid lahkneb sellest kahes kriitilises punktis: see on projekteeritud kiuse ja kättemaksuimpulsside jaoks, mitte ei eelda ratsionaalsust, ning see pakub järkjärgulist üleminekut, mitte revolutsiooni. Esilekerkivate ühiskondlike lepingute kontseptsioonil on eelkäijaid Hayeki spontaanse korra teoorias [16].

Anarhoagorism. RSN-il on märkimisväärne ühisosa agoristliku vastumajandusega [17]—eelkõige rõhuasetus paralleelsete institutsioonide ehitamisele ja vabatahtlikule vahetusele. Siiski kaldub agorism eeldama ratsionaalset omakasu piisava koordineerimismehhanismina ning sellel puudub sageli konkreetne üleminekutee olemasolevatest riiklikest struktuuridest. RSN hõlmab selgesõnaliselt mitteratsionaalseid käitumuslikke kalduvusi ja pakub fiskaalset survemehhanismi järkjärguliseks üleminekuks.

Meritokraatia. RSN võib kujutada endast esimest funktsionaalset kirjeldust sellest, kuidas meritokraatia [18] saab esile kerkida süsteemse omadusena, mitte loosungina. Traditsioonilised meritokraatlikud süsteemid ebaõnnestuvad, sest need nõuavad tsentraalset autoriteeti „teene" defineerimiseks ja jõustamiseks. RSN-is kerkib teene esile kahepoolsetest hinnangutest: need, kes annavad väärtust, koguvad reputatsiooni; ükski komitee ei otsusta, kellel on teene.

Omand kui privileeg. RSN lahkneb põhimõtteliselt anarhokapitalistlikust ja Austria koolkonna käsitlusest omandiõigustest kui loomulikest ja absoluutsetest. RSN-i raamistikus on omand *privileeg*—sotsiaalne tunnustus, mille kogukond saab äärmuslikel juhtudel tagasi võtta, kui osaleja põhimõtteliselt rikub jagatud norme (reetmine, keeldumine kogukonna kaitsmisest eksistentsiaalses kriisis, süstemaatiline ärakasutamine). See ei ole riiklik sundvõõrandamine, vaid sotsiaalse tunnustuse tagasivõtmine kahepoolsete suhete võrgustiku poolt.

13 Arutelu ja piirangud

Külmkäivitus. RSN-i väärtus sõltub võrgumõjudest; varajased kasutuselevõtjad seisavad silmitsi piiratud väärtusega, kuni osalemine saavutab künnise. Siiski, isegi varajastest etappidest alates, on DID-võrk kasulikuks täiendavaks teabeallikaks. Varajase reputatsioonihinnangu ja autoriteedihinnangu eeldatakse arenevat järk-järgult koos kasvava keerukusega.

Parasiitluse tõkestamine ja juurdepääsu kontroll. Siht-DID-id võivad kehtestada astmelisi tasusid ja juurdepääsupiiranguid madala reputatsiooniga DID-ide päringutele. See ei ole binaarne, vaid pidev skaala: mida vähem reputatsiooni päringut esitaval DID-il on, seda vähem teavet ta saab, seda kauem ta ootab ja seda rohkem ta maksab. See mehhanism stimuleerib ehtsat osalust passiivse tarbimise asemel.

Juurdepääsu ebavõrdsus. Väidete avaldamise kulu võib välja filtreerida õiguspärased kaebused majanduslikult ebasoodsas olukorras osalejatelt. Leevendus: iga osaleja tegutseb samaaegselt potentsiaalse kontrollijana (või delegeerib selle rolli) ja teenib kontrollitasusid. Piisava ajahorisondi jooksul peaks mitteradikaalne osaleja lähenema finantsneutraalsusele—kontrollitulu tasakaalustab ligikaudu avaldamiskulud. See on statistiline ootus, mitte garantii.

Reputatsiooni ebavõrdsus. Varajased kasutuse-

levõtjad koguvad eeliseid, mis võivad luua tõkkeid hilistulnukatele. Siiski teostavad reputatsioonihindamist kolmandast osapoolest pakkujad, kes võivad valida esimese liikuja eelise leevendamise oma koondamisalgoritmide kaudu. Esimesena hea reputatsiooniga olemine on õiguspärane suhteline majanduslik eelis—ja see on tahtlik.

Lahtised küsimused. Optimaalsed kulufunktsioonid, koondamisstandardid, protokolli valitsemine ja interaktsioon AI-genereeritud sünteetiliste reputatsiooniandmetega jäävad tulevase töö valdkondadeks.

See artikkel ei väida, et RSN toodab optimaalseid tulemusi kõikides olukordades. See väidab, et RSN kujutab endast *teostatavat* alternatiivi—tehniliselt rakendatavat, majanduslikult isemajandavat ja sotsiaalselt ühilduvat inimlike käitumuslike kalduvustega sellisena, nagu need tegelikult on.

14 Kokkuvõte

See artikkel esitas reputatsiooni-suhtlusvõrgustiku, detsentraliseeritud protokolli, mis võimaldab pseudonüümset ja kontrollitavat reputatsioonivahetust. Kalli radikalismi põhimõte tagab, et pettuslikud väited hinnastatakse välja ilma tsensuurita. Väljapakutud üleminekutee võimaldab järkjärgulist ja pöörduvat üleminekut olemasolevatelt institutsioonidelt. Kavand hõlmab inimloomust sellisena, nagu see on—kaasa arvatud väiklus, kius ja kättemaksurahulduse iha—selle asemel, et nõuda ideoloogilist teisenemist. Tulemuseks ei ole utoopia, vaid süsteem, kus õiglus on kättesaadav, reputatsioon on teenitud ja üleastumise kulu kannab pool, kes selle põhjustas.

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.