Hajautettu mainejärjestelmä: Viitekehys yhteiskunnan luonnolliselle järjestäytymiselle

Pavel Kudrna
Praha, Tšekki
Luonnos v1 — maaliskuu 2026

Abstract

Oikeudentunto—vakaumus siitä, että vääryydet oikaistaan ja ansiot palkitaan—on yhteiskunnan vahvin koossapitävä voima. Kun keskitetyt hallintoinstituutiot eivät kykene tuottamaan tätä tunnetta, koska oikeuden toteuttamisen kustannus ylittää itse oikeuden arvon, sosiaalinen koheesio rapautuu. Nykyiset institutionaaliset rakenteet epäonnistuvat merkittävän riitaluokan ratkaisemisessa järjestelmällisesti samalla tavalla kuin keskusjohtoinen suunnittelu epäonnistuu resurssien kohdentamisessa: informaation epäsymmetrian, puuttuvien takaisinkytkentöjen ja päätöksentekijöiden ja heidän päätöstensä seurausten välisen katkoksen kautta. Tämä artikkeli esittelee maineeseen perustuvan sosiaalisen verkoston (Reputation Social Network, RSN): hajautetun, korruptoitumattoman ja sensuuria kestävän viestintäkerroksen, joka rakentuu hajautetuille tunnisteille (Decentralized Identifiers, DID) ja mahdollistaa salanimellä toimiville osallistujille todellisesta käyttäytymisestä kertovan mainetiedon julkaisemisen, todentamisen ja kuluttamisen. Ydinmekanismi nojaa kolmeen suunnitteluperiaatteeseen: (1) epäsymmetriseen kustannusrakenteeseen, jossa mainetiedon lukeminen on halpaa mutta kirjoittaminen edellyttää todennettavaa ponnistelua; (2) epädeterministiseen todentajan valintaprotokollaan, joka perustuu johdonmukaiseen tiivistämiseen ja hinnoittelee radikaalit väitteet kasvavien iteraatiokustannusten kautta; ja (3) markkinavetoiseen maineauktoriteettimalliin, jossa yksityiset todentajat panttaavat kertyneen maineensa hyväksymiensä väitteiden paikkansapitävyyden puolesta. Näin syntyvä arkkitehtuuri tuottaa emergentin meritokratian ilman keskitettyä koordinointia ja mahdollistaa asteittaisen, peruutettavissa olevan siirtymäpolun nykyisistä valtion hallinnoimista järjestelmistä.

1 Johdanto

1.1 Keskitetyn luottamuksen ongelma

Nykyaikainen hallinto nojaa perustavaan oletukseen: että keskitetyt instituutiot voivat välittää luottamusta tuntemattomien välillä laajassa mittakaavassa. Tuomioistuimet ratkaisevat riitoja. Rekisterit vahvistavat omistusoikeuden. Sääntelyelimet valvovat standardeja. Nämä instituutiot suunniteltiin aikakautena, jolloin informaatio oli niukkaa, viestintä hidasta ja auktoriteetin delegointi keskuselimelle oli ainoa toteuttamiskelpoinen koordinointimekanismi. Keskitetty hallinto kuitenkin epäonnistuu samoista rakenteellisista syistä kuin keskusjohtoinen suunnittelu: informaation epäsymmetria, puuttuvat takaisinkytkennät sekä päätöksentekijöiden ja heidän päätöstensä seurausten välinen katkos.

Oletus pettää esimerkiksi silloin, kun institutionaalisen välityksen kustannus ylittää riidan arvon. Ajatellaan vuokralaista, joka havaitsee, että hänen vuokra-asunnostaan puuttuu lain edellyttämä sähköturvallisuustodistus—puute, joka aiheuttaa välittömän hengenvaaran. Vuokralaisen laillinen oikeus purkaa sopimus on kiistaton. Silti tuon oikeuden toteuttamisen kustannus tuomioistuinjärjestelmän kautta ylittää vakuuden ja maksettavien vahingonkorvausten rahallisen arvon, vaikka mukaan laskettaisiin mahdollinen lakisääteinen korvaus [1]. Rationaalinen vastaus on kärsiä tappio ja vetäytyä.

Tämä ei ole patologinen ääritapaus. Se on oletusarvoinen kokemus merkittävässä riitaluokassa, jossa vahinko on todellinen mutta rahallinen panos jää sen kynnyksen alle, jonka yläpuolella institutionaalinen täytäntöönpano tulee taloudellisesti järkeväksi. Tuloksena on järjestelmä, joka rakenteellisesti suosii pahantekijöitä: ne, jotka vahingoittavat muita tämän kynnyksen alittavissa määrin, voivat toimia rankaisematta, koska oikeuden hakemisen kustannus lankeaa vahinkoa kärsineelle osapuolelle.

Yllä oleva esimerkki on peräisin kirjoitta-

jan oikeudellisesta ympäristöstä—Tšekin siviilioikeusjärjestelmästä. Muissa oikeusperinteissä—ennakkopäätöksiin nojaava common law, tapaoikeus, sekajärjestelmät—oikeus epäonnistuu eri tavoin ja eri asteissa riippuen lainkäyttöalueen kulttuurisista ja menettelyllisistä erityispiirteistä. Lukijat tunnistanevat vastaavia esimerkkejä omasta kontekstistaan. Rakenteellisesti universaalia on kuvio: riidat, joiden arvo jää taloudellisesti järkevän täytäntöönpanon kynnyksen alle, päättyvät siihen, että vahinkoa kärsinyt osapuoli kantaa tappion. RSN ei lupaa täydellistä oikeutta—se vain vähentää sitä rakenteellista etua, jonka pahantekijät saavat, kun institutionaalinen täytäntöönpano on epätaloudellista.

1.2 Miksi olemassa olevat ratkaisut jäävät vajaiksi

Hajautetun identiteetin (DID) viitekehykset [2] tarjoavat kryptografisia mekanismeja itsemääräisen identiteetin hallintaan, mutta keskittyvät ensisijaisesti identiteetin todentamiseen käsittelemättä laajempaa kysymystä käyttäytymiseen perustuvasta maineesta.

Sielusidonnaiset tunnukset (Soulbound Tokens, SBT) [3] tavoittavat oivalluksen siitä, että maine on siirtokelvotonta, mutta nojaavat lohkoketjuinfrastruktuuriin, jolla on skaalautuvuusrajoitteita, eivätkä käsittele tiedon syöttämistä ohjaavia taloudellisia kannustimia. Vastaavat käsitteet, kuten ansiotunnukset (esim. Liberland), jakavat samankaltaisen filosofian mutta pysyvät sidottuina tiettyihin lainkäyttöalueen viitekehyksiin.

Hajautetut autonomiset organisaatiot (Decentralized Autonomous Organizations, DAO) [4] toteuttavat hallinnon älysopimusten kautta, mutta toistavat plutokraattista dynamiikkaa, jossa vaikutusvalta on suhteessa pääomaan. Neliöllinen äänestäminen [5] lieventää tätä osittain mutta rajoittaa käytännön omaksumista. DAO:t kohtaavat myös perustavan *oraakkeliongelman*: älysopimukset eivät voi luotettavasti todentaa todellisen maailman tiloja ilman luotettua ulkoista lähdettä, eikä tähän ongelmaan ole yleistä ratkaisua lohkoketjuarkkitehtuurin sisällä.

Mikään olemassa oleva järjestelmä ei yhdistä hajautusta, sensuurin kestävyyttä, salanimisyyttä, todennettavaa syöttämisen kustannusta ja emergenttiä konsensusta.

1.3 Tutkimuksen kontribuutiot

Tämä artikkeli tekee seuraavat kontribuutiot:

1. **Maineeseen perustuvan sosiaalisen verkoston (RSN)** määrittely: hajautettu protokolla, joka laajentaa DID-viitekehystä tukemaan kaksisuuntaista mainevaihtoa.
2. **Epädeterministinen todentajan valintaprotokolla**, joka perustuu johdonmukaiseen tiivistämiseen [6].
3. **Kalliin radikalismin periaate**, joka hinnoittelee väitteet niiden etäisyyden mukaan verkoston konsensuksesta kolmen kasautuvan kustannuskanavan kautta.
4. **Maineauktoriteettimalli**, jossa on epäsymmetriset kannustimet ja jossa väärä hyväksyntä maksaa katastrofaalisesti enemmän kuin legitiimit maksut.
5. **Asteittainen siirtymäpolku** rinnakkaisen finanssi-infrastruktuurin kautta.

2 Suunnitteluperiaatteet

RSN-arkkitehtuuria rajaa viisi neuvottelematonta suunnitteluperiaatetta.

Jatkuvuus ja kehitys. Järjestelmä toimii rinnakkain olemassa olevien instituutioiden kanssa määrittelemättömän pituisen siirtymäkauden ajan. Siirtymän on oltava peruutettavissa jokaisessa vaiheessa.

Vapaaehtoisuus ja vastuu. Osallistuminen on vapaaehtoista, mutta vapaaehtoisuuteen kytkeytyy vastuu: osallistuja, joka ottaa haltuunsa institutionaalisen tehtävän, ottaa samalla kannettavakseen siihen liittyvät velvoitteet.

Moninaisuus ja kulttuurinen neutraalius. Konsensus syntyy kaksisuuntaisista vuorovaikutuksista, ei järjestelmän suunnittelijoiden asettamista ennalta määrätyistä säännöistä.

Kestävyys ja sensuurin vastustuskyky. Verkoston sensuroinnin kustannuksen on ylitettävä sen sietämisen kustannus. Vain täysi totalitarismi—turmiollisin poliittisin ja taloudellisin kustannuksin—voi tukahduttaa järjestelmän.

Konsensus ja täytäntöönpano. Järjestelmä sisällyttää inhimilliset taipumukset pikkumaisuuteen, ilkeyteen ja kostonhaluiseen tyydytykseen kantaviksi ominaisuuksiksi. Väärinkäytöstä ei kielletä; se hinnoitellaan.

3 Järjestelmän yleiskuvaus

3.1 Maineeseen perustuva sosiaalinen verkosto

RSN on hajautettu, vertaisverkkoon (peer-to-peer) perustuva viestintäkerros, jossa osallistujat vaihtavat todennettavaa tietoa todellisesta käyttäytymisestä. Sen määrittelevät ominaisuudet ovat: hajautettu ja sensuroimaton infrastruktuuri; salanimellä osallistuminen DID:ien kautta; epäsymmetrinen kustannusrakenne (lukeminen halpaa, kirjoittaminen kallista); kryptografinen todennettavuus; ja **standardituki**—koneluettavat muodot verkostossa leviävälle tiedolle, auktoriteettien tarjoamille palveluille (väitteen kokoaminen, hyväksyntä, todistajapalvelu) sekä käytäntömuodolle, joka sisältää säännöt vastapuolen maineen arvioimiseen ja käytäntöristiriidan (ilmoitetun ja todellisen käyttäytymisen välillä) riskin arviointiin.

3.2 Arkkitehtuurin komponentit

RSN koostuu neljästä pääkomponentista (kuva 1):

1. **DID-kerros.** Osallistujien identiteetit ilmoitettuine sääntöineen, mainemetadatoineen ja verkostoreitityksineen.
2. **Väiteprotokolla.** Jäsennelty muoto todellisen maailman tapahtumia koskevien väitteiden julkaisemiseen.
3. **Todennusverkosto.** Hajautettu protokolla todentajien osoittamiseen johdonmukaisen tiivistämisen avulla.
4. **Maineen aggregointikerros.** Palvelut, jotka tuottavat ihmisen luettavia maineyhteenvetoja.

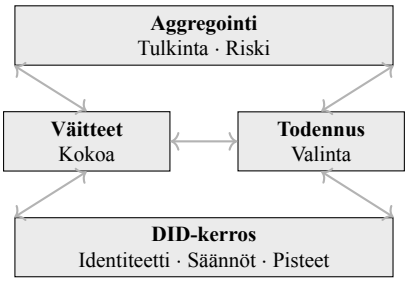

Figure 1: RSN:n nelikerroksinen arkkitehtuuri.

3.3 Osallistujien roolit

Todennustapahtumaan osallistuu enintään kuusi erillistä DID-roolia (kuva 2): **Antaja** (DID_I, luo ja lähettää väitteen), **Kohde** (DID_S, DID, jota väite koskee—voi olla sama kuin Antaja), **Auktoriteetti** (DID_A, hyväksyy väitteen maksua vastaan; voi myös tarjota todistajapalveluja—*valinnainen*), **Todistaja** ($DID_{W_{1..n}}$, incognito-valvoja todentajan rehellisyydelle haastekoodien avulla—*valinnainen*), **Todentaja** (DID_V, algoritmisesti valittu julkaisemaan väite) ja **RSN** (verkosto, jossa todennetut väitteet julkaistaan). Mikä tahansa rooli voidaan delegoida toiselle DID:ille (luku 7.4). Auktoriteetti niputtaa yleisesti hyväksynnän todistajapalveluihin, mutta nämä kaksi tehtävää ovat loogisesti riippumattomia.

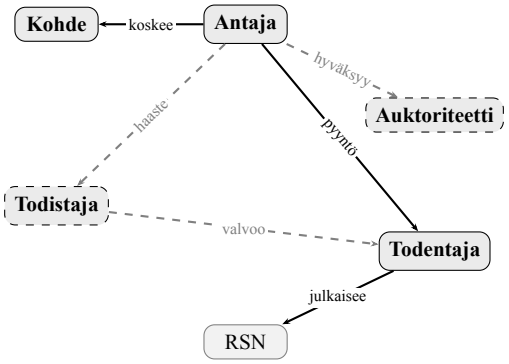

Figure 2: DID-roolit todennustapahtumassa. Katkoviiva = valinnainen (Auktoriteetti, Todistaja).

3.4 Korruptoitumattomuus: neljä voimaa

RSN:n korruptoitumattomuus ei synny yksittäisestä mekanismista vaan neljästä samanaikaisesta voimasta. Mikään niistä ei riitä yksinään; vasta niiden yhdistelmä tekee korruptioyrityksestä taloudellisesti irrationaalisen.

Ennakoimaton kohde. Kunkin väitteen todentaja valitaan epädeterministisesti johdonmukaisen tiivistämisen avulla (luku 5.3). Hyökkääjä ei voi kohdentaa lahjontaa ennalta tiettyyn todentajaan, koska todentajan henkilöllisyys on väitteen sisällön ja aiempien iteraatioiden funktio, ei antajan valinnan.

Maineen vipuvaikutus—hidas ylös, nopea alas. Mainetta voi kartuttaa vain vähitellen, jatkuvan johdonmukaisen käyttäytymisen kautta. Se voidaan kuitenkin menettää katastrofaalisesti yhdellä petollisella hyväksynnällä (luku 6.2). Tämä epäsymmetria tarkoittaa, että vuosien kertynyt maine voidaan tuhota yhdellä epärehellisellä hyväksynnällä; optimaalinen strategia on aina hylätä epäilyttävät väitteet.

Julkinen lupaus. Jokainen DID:in haltija ilmoittaa julkisesti käytäntönsä—koneluettavan sääntöjoukon, jota hän sitoutuu noudattamaan. Ilmoituksen ja todellisen käyttäytymisen välinen poikkeama on havaittavissa ja hinnoitellaan mainerikkomukseksi, joka on ankarampi kuin itse taustalla oleva rikkomus

(luku 7.3). Tekopyhyys on siten kalliimpaa kuin suora epärehellisyys.

Verkkorakenteen hyökkäyskustannuksen epäsymmetria. Verkoston sensuroinnin tai horjuttamisen kustannus kasvaa epälineaarisesti verkoston koon ja tiheyden mukana, kun taas sen sietämisen kustannus pysyy vakiona. Jotta sensuuri kannattaisi, keskitetyn toimijan olisi sovellettava sitä koko verkostoon—mikä vaatisi toimenpiteitä, jotka ovat suhteettomia mihinkään kuviteltavissa olevaan hyötyyn nähden (luku 10).

4 Hajautetun identiteetin malli

4.1 DID erityisominaisuuksin

RSN laajentaa W3C DID Core -spesifikaatiota [2] seuraavilla: **Ilmoitetut säännöt** (koneluettavat käyttäytymissitoumukset), **Mainemetadata** (aggregoitu käyttäytymispistemäärä) ja **Verkostoreititys** (muuttuva onion-yhdyskäytävä, joka on erillinen vakaasta rengaspositiosta).

4.2 Väitteen elinkaari

Väite etenee kuuden vaiheen läpi (kuva 3): kokoaminen, valinnainen auktoriteetin hyväksyntä, todentajan valinta johdonmukaisen tiivistämisen avulla, todennuspäätös (hyväksyntä tai hylkäys iteraatiolla), julkaisu ja maineen päivitys kaikille osapuolille.

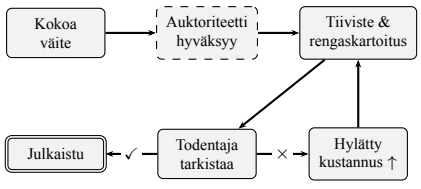

Figure 3: Väitteen elinkaari iteraatiosilmukalla.

4.3 Suhde W3C DID Core -spesifikaatioon

RSN:n identiteettimalli on W3C DID Core -spesifikaation [2] varsinainen ylijoukko. Kaikki RSN-DID:t ovat päteviä W3C-DID:ejä. RSN:lle ominaiset laajennukset koodataan DID-dokumentin ominaisuuksina, jotka määritellään omistetussa DID-menetelmäspesifikaatiossa, yhteensopivana olemassa olevan infrastruktuurin kuten ION:in [7] ja Ceramicin [8] kanssa.

5 Tiedon todentaminen ja leviäminen

5.1 Tiedon syöttämisen kustannus

RSN:n taloudellinen ydinperiaate on lukemisen ja kirjoittamisen välinen epäsymmetria. Mainetiedon lukeminen lähestyy nollaa rajakustannusta osallistujille, jotka ovat osa DID-verkostoa ja joilla on maineensa mukainen pääsy—tulokkaiden on ansaittava laajempi pääsy vähitellen (ks. loisimisen esto). Kirjoittaminen—ymmärrettynä maineen kestävänä konkretisoitumisena verkostoon, ei yksittäisenä teknisenä toimena—vaatii todennettavaa kumulatiivista panostusta kolmella ulottuvuudella: **aika** (elinvuodet, jotka on käytetty johdonmukaiseen käyttäytymiseen, täytettyihin sitoumuksiin ja vaalittuihin suhteisiin), **energia** (rehelliseen toimintaan, kumppanuuksien vaalimiseen ja pitkäaikaiseen luotettavuuteen sijoitettu ponnistus) ja **raha** (sijoitus omaan nimeen—ammatillinen kehittyminen, oman työn laatu, aiheutettujen vahinkojen hyvittäminen). Mainetta ei voi ostaa hetkessä—se on elinikäisen kertymän lopputulos, jonka järjestelmä vain tekee näkyväksi ja siirrettäväksi kontekstien välillä. Protokollan kertaluonteiset tekniset kustannukset (kryptografiset allekirjoitukset, todentajan maksut) ovat mitättömiä tähän taustalla olevaan sijoitukseen verrattuna.

5.2 Sosiaalinen graafi ja kontaktien syvyys

RSN on pohjimmiltaan sosiaalinen verkosto: kukin DID lisää kontakteja (muita DID:ejä), jotka sallivat yhteyden. Näillä kontakteilla on omat kontaktinsa, ja niin edelleen. Algoritminen todentajan haku toimii säädettävän linkitettyjen kontaktien syvyyden h sisällä (esim. $h = 3$: omat suorat kontaktit, heidän kontaktinsa ja kontaktien kontaktit). Tämä arkkitehtuuri ei vaadi yhtä globaalia lohkoketjua—se suosii luonnostaan yhteisöjen/klustereiden syntymistä, jotka limittyvät muihin yhteisöihin. Jokaisella DID-osallistujalla on oltava julkaistu **käytäntö**—koneluettava sääntöjoukko, joka ohjaa saapuvien pyyntöjen arviointia. Käytäntörikkomukset kirjataan verkostoon negatiivisina artefakteina.

5.3 Algoritminen todentajan valinta

Todennusprotokolla käyttää johdonmukaista tiivistämistä [6] (kuva 4). Todentaminen on maksullinen palvelu: todentajat toimivat maksua vastaan, mikä luo markkinat, joissa kilpailu ohjaa hinnoittelua, nopeutta ja luotettavuutta.

Vaihe 1. Väitedokumentti ketjutetaan edellisen iteraation tiivistetulokseen (tai ∅ ensimmäisellä iteraatiolla) ja tiivistetään:

$$\text{pos} = f_h(\text{väite} \| \text{prev\_hash}) \quad (1)$$

Algoritmin on sisällettävä kaikkien aiempien pyyntöjen ja vastausten *täydellinen polku*—ei pelkkää edellisen iteraation tiivistettä. Kunkin todentajan koko vastaus (hyväksyntä, hylkäys, ilmoitettu hinta, perustelu) liitetään kasvavaan dokumenttiin, todennettavana kryptografisten allekirjoitusten avulla joka vaiheessa.

Vaihe 2. Tiiviste kartoitetaan N positioon johdonmukaisen tiivistysrenkaan ympärille, tasaisesti jaettuina (esim. $N = 4$: $+0°, +90°, +180°, +270°$). Kustakin positiosta myötäpäivään suuntautuva haku valitsee lähimmän DID:in todentajaehdokkaaksi (kuva 5). N on muuttuva parametri, joka voi riippua parhaillaan aktiivisten DID:ien prosenttiosuudesta, vuorokaudenajasta tai verkoston historiallisesta vasteajasta.

Vaihe 3. Todentaja hyväksyy (julkaisee, panttaa maineensa) tai hylkää (palaa vaiheeseen 1 hylkäystiivisteen kanssa). Kun solmu ei vastaa, vaikka se ilmoittaa olevansa verkossa, seuraavan pyynnön on sisällettävä kaikki vastaukset kaikilta N aiemmalta todentajaehdokkaalta.

Loisimisen esto. Kohde-DID:t voivat asettaa maksuja tai pääsyrajoituksia kyselyille vähän mainetta omaavilta uusilta DID:eiltä. Tämä porrastettu mekanismi (ei binäärinen) pakottaa tulokkaat rakentamaan mainetta aidon toiminnan kautta ennen kuin he saavat vapaasti kuluttaa muiden dataa.

Kukin hylkäys liittää todentajan koko vastauksen (mukaan lukien perustelut ja ehdot) väitedokumenttiin, laajentaen sen sisältöä. Laajennetusta dokumentista lasketaan epädeterministisesti uusi tiiviste, joka kartoittuu eri rengaspositioon ja valitsee eri todentajan. Koko polun dokumentointi on pakollista—antaja ei voi ennustaa tai vaikuttaa seuraavaan todentajaan. Jos todentaja jättää pyynnön huomiotta yhteensopivasta ilmoitetusta käytännöstä huolimatta, todistajat (jos läsnä) kirjaavat tämän, ja antaja voi liittää todistajien todisteet lopulliseen julkaisuun.

5.4 Todistajaprotokolla

Todistaja-rooli tarjoaa incognito-vastuuvelvollisuuden todentajan rehellisyydelle kryptografisen haastekoodiprotokollan kautta:

Vaihe W1. Pyytäjä allekirjoittaa todennuspyynnön ja lähettää sen N_w todistajalle—kontakteille pyytäjän

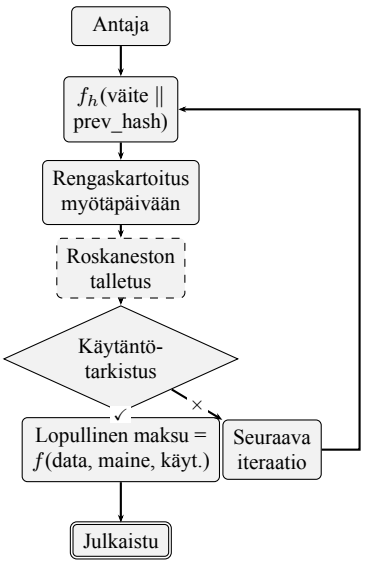

Figure 4: Todentajan valintaprotokolla. Roskaneston talletus on valinnainen ja voi olla palautettavissa. Lopullinen maksu maksetaan vain hyväksynnän yhteydessä.

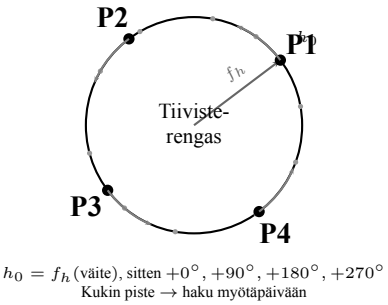

Figure 5: Monipistevalinta (N=4). Tiiviste h_0 asettaa siirtymän; 4 pistettä tasaisesti jaettuina h_0:sta.

sosiaalisesta verkostosta tai maksua vastaan toimiville erikoistuneille todistajapalvelun tarjoajille.

Vaihe W2. Kukin todistaja w_i allekirjoittaa koko allekirjoitetun pyynnön, säilyttää alkuperäisen allekirjoituksen σ_i ja laskee haastekoodin $c_i = h(\sigma_i)$. Haastekoodi liitetään pyyntöön.

Vaihe W3. Pyyntö, joka nyt kantaa N_w haastekoodia, lähetetään todentajalle. Todentaja näkee koodit mutta *ei voi määrittää*, keitä todistajat ovat tai vastaavatko koodit todellisia allekirjoituksia.

Vaihe W4 (rehellinen todentaja). Jos todentaja vastaa ilmoittamansa käytännön mukaisesti, haastekoodit pysyvät läpinäkymättöminä. Todistajia ei koskaan paljasteta. Lisädataa ei julkaista.

Vaihe W5 (käytäntörikkomus). Jos todentaja rikkoo käytäntöään (jättää pyynnön huomiotta, vastaa epäjohdonmukaisesti), pyytäjällä on hallussaan todistajien alkuperäiset allekirjoitukset σ_i. Nämä voidaan julkaista oheisdatana: kuka tahansa voi toden-

taa $c_i = h(\sigma_i)$, mikä todistaa todistajan olleen läsnä. Pyytäjä voi julkaista itsenäisesti—todentaja allekirjoitti haastekoodit jo vastauksessaan.

Bluffiominaisuus. Pyytäjä voi korvata osan tai kaikki haastekoodit satunnaisilla arvoilla. Todentaja ei voi erottaa aitoja koodeja (korkean maineen auktoriteettien tukemia) kohinasta. Tämä *epävarmuus* on täytäntöönpanomekanismi: jokainen pyyntö kantaa riskin siitä, että arvostettu auktoriteetti seuraa incognito. Tämän paineen ylläpitämisen kustannus on lähes nolla (satunnaislukujen generointi), kun taas epärehellisyyden mahdollinen kustannus todentajalle on katastrofaalinen. Rehelliseen käyttäytymiseen kannustetaan, vaikka todellisia todistajia ei olisikaan.

Auktoriteetti todistajana. Auktoriteetti, joka hyväksyy väitteen, voi niputtaa mukaan todistajapalveluja: "Hyväksyn väitteesi ja toimin incognito-todistajana todennuksen aikana." Tämä on luonnollinen liiketoimintamalli—auktoriteetilla on jo konteksti. Nämä kaksi roolia ovat kuitenkin loogisesti riippumattomia.

5.5 Kalliin radikalismin periaate

Kolme kustannuskanavaa kasautuvat samanaikaisesti (kuva 6):

Kanava 1: Iteraatiokustannus. Kukin hylkäys pakottaa uuteen iteraatioon, joka kuluttaa aikaa ja resursseja. Lineaarinen kasvu.

Kanava 2: Dokumentin paisuminen. Kukin iteraatio lisää todentajan koko vastauksen väitedokumenttiin. Kasvu on lineaarista, mutta perussiirtymällä: alkuperäisellä hyötykuormalla (väitteen sisältö, auktoriteetin hyväksyntä, kryptografiset allekirjoitukset) on jo ei-triviaali koko B_0. Kokonaiskoko k iteraation jälkeen: $S(k) = B_0 + k \cdot \Delta$, missä Δ on keskimääräinen vastauksen koko.

Kanava 3: Todentajan riskilisä. Riski on subjektiivinen. Todentaja arvioi, ovatko pyytävän DID:in ilmoitetut käytännöt ristiriidassa todentajan omien kaupallisten, sosiaalisten tai poliittisten etujen kanssa. Lisä voi kasvaa eksponentiaalisesti havaitun etäisyyden mukaan todentajan "ihanteesta": $P(d) = \alpha \cdot e^{\beta d}$, missä d on todentajan subjektiivinen etäisyysmitta. Henkilökohtaisen ehdottoman rajan ylittyessä todentaja voi kieltäytyä kokonaan.

Ratkaisevasti tämä ei ole sensuuria. Mitään väitettä ei kielletä. Järjestelmä hinnoittelee riskin (taulukko 1).

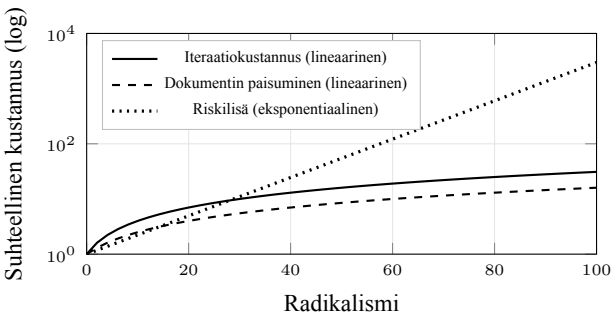

Figure 6: Kustannusten kärjistyminen kolmessa kanavassa. Riskilisä hallitsee korkealla radikalismilla.

Table 1: Kustannusvertailu väitetyyppien välillä.

Tyyppi	Iter.	Dok.	Maksu	Yht.
Uskottava	k_{min}	B_0	P_{min}	Matala
Kiistanalainen	k_{med}	$B_0 + k\Delta$	$\alpha e^{\beta d}$	Kohtalainen
Radikaali	k_{max}	$\gg B_0$	$\gg P_{\text{min}}$	Erittäin korkea
Petollinen	$\to \infty$	—	—	Julkaisukelvoton

6 Maine ja riskinarviointi

6.1 Maineen kertymämalli

Maineella on kolme ominaisuutta: **hidas kertyminen** (asteittainen kasvu johdonmukaisen käyttäytymisen kautta), **nopea tuhoutuminen** (yksi petos voi laskea pistemäärää katastrofaalisesti) ja **yksilöllinen arviointi** (kukin kuluttava osapuoli voi soveltaa omaa aggregointifunktiotaan).

6.2 Maineikkaat auktoriteetit

Maineikas auktoriteetti tarkastaa väitteet ja, jos on tyytyväinen, allekirjoittaa ne yhdessä—pantaten oman maineensa (kuva 7). Epäsymmetria on tarkoituksellinen: maineen ansaitseminen on hidasta (asteittainen $+\delta$ kutakin rehellistä hyväksyntää kohti), kun taas sen menettäminen on katastrofaalista ($-\Delta \gg \delta$ kutakin väärää hyväksyntää kohti; havainnollistavasti esim. $+2\%$ vs. -70%). Optimaalinen strategia on aina hylätä epäilyttävät väitteet. Arvojen δ ja Δ tarkat arvot ovat järjestelmäparametreja.

6.3 Moniulotteinen maine

Maine ei ole skalaari vaan vektori useiden ulottuvuuksien yli: taloudellinen luotettavuus, henkilökohtainen rehellisyys, ammatillinen pätevyys, kansalaisosallistuminen ja muut (kuva 8). Eri arviointipalvelut projisoivat tämän vektorin eri tavoin kontekstista riippuen—lainanantaja priorisoi taloudellista luotettavuutta, työnantaja ammatillista pätevyyttä, naa-

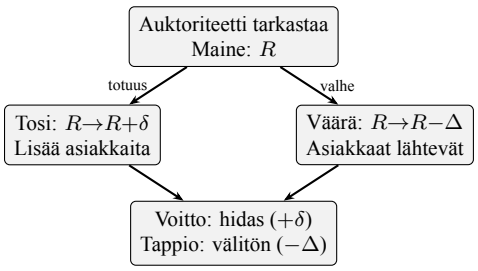

Figure 7: Maineikas auktoriteetti—epäsymmetriset kannustimet.

puri kansalaiskäyttäytymistä. Ei ole yhtä "oikeaa" mainepistemäärää; vain näkökulmia.

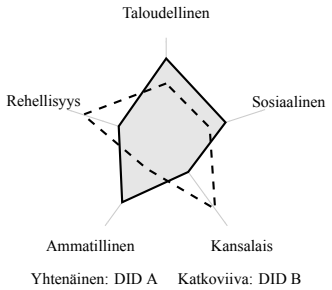

Figure 8: Moniulotteiset mainevektorit. Eri DID:t osoittavat erilaisia profiileja ulottuvuuksien yli.

6.4 Demokratisoitu riskinarviointi

RSN demokratisoi järjestelmällisen riskinarvioinnin—kyvyn, joka on tällä hetkellä keskittynyt rahoituslaitoksiin mutta soveltuu paljon pankkitoimintaa laajemmalle. Teollisuuskonglomeraatit arvioimassa toimittajien luotettavuutta, vakuutusyhtiöt hinnoittelemassa käyttäytymisriskiä, due diligence yrityskaupoissa ja -sulautumisissa, laitteiden eliniän arviointi valmistuksessa—missä tahansa vastapuoliriski vaatii arviointia, RSN tarjoaa hajautetun, markkinavetoisen vaihtoehdon. Tulkintapalveluiden markkinat kääntävät raa'an moniulotteisen mainedatan toimintakelpoisiksi yhteenvedoiksi, tehden vastapuolen arvioinnista minkä tahansa osallistujan saatavilla olevaa rajakustannuksin.

7 Konsensus ja riitojenratkaisu

7.1 Hajautetun oikeuden malli

RSN muotoilee oikeuden uudelleen kaksisuuntaisena neuvotteluongelmana. Pysyvän, todennettavan mainevahingon uhka on tehokkaampi pelote kuin oikeudenkäynti, johon vahinkoa kärsinyt osapuoli ei ole varaa.

7.2 Emergentti konsensus

Kukin osallistuja ylläpitää henkilökohtaista tyytyväisyyskynnystä. Verkoston kokonaiskonsensus syntyy tuhansien kaksisuuntaisten neuvottelujen tilastollisena keskiarvona (kuva 9). Konsensuksen kaukana yläpuolella oleva vastaus (barbaarinen) on kallis julkaista. Konsensuksen lähellä oleva vastaus (suhteellinen) on halpa. Konsensus ei ole sääntö—se on hintasignaali.

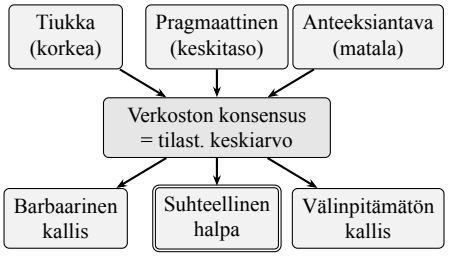

Figure 9: Emergentti konsensus yksilöllisistä tyytyväisyyskynnyksistä.

7.3 Rangaistuksen kalibrointi

Kukin DID:in haltija ilmoittaa julkisesti vastauksensa tiettyihin väärinkäytöskategorioihin. Suhteettoman ankarat tai lempeät ilmoitukset houkuttelevat negatiivisia mainesignaaleja. Suhteelliset ilmoitukset hyväksytään kitkatta—itseään kalibroiva rangaistusjärjestelmä.

Konsensusilmoitukset ovat itsessään tekopyhyyden havaitsemisen alaisia: konsensuskantaan sitoutuminen julistuksen tasolla samalla epäjohdonmukaisesti käyttäytyen muodostaa mainerikkomuksen, joka on ankarampi kuin taustalla oleva poikkeama, koska se osoittaa tahallista petosta.

7.4 Delegointi

Kaikki DID:in sisäiset toiminnot—yhtä poikkeusta lukuun ottamatta—voidaan delegoida toiselle DID:ille. **Kohde-roolia—DID:iä, jonka käyttäytymistä väite koskee—ei voi delegoida; se on siirtokelvottomasti sidottu siihen identiteetin haltijaan, johon väite viittaa.** Muut aktiiviset roolit—Antaja, Auktoriteetti, Todistaja, Todentaja—voidaan siirtää nimetylle valtuutetulle DID:ille, olipa kyse todennuksesta, väitteen lähettämisestä, konsensukseen osallistumisesta tai riitojenratkaisusta. Delegointi on peruutettavissa milloin tahansa. Tämä mahdollistaa erikoistumisen (esim. ammattimaiset todennuspalvelut), samalla kun haltija säilyttää perimmäisen hallinnan ja vastuun. Delegointi koskee koko

järjestelmää ja on olennaista skaalautuvuudelle.

7.5 Yksilön moraalista emergenttiin yhteiskuntasopimukseen

Kunkin DID:in ilmoitettu käytäntö edustaa yksilön moraalin formalisointia: mitä haltija pitää hyväksyttävänä, miten hän vastaa tiettyihin käyttäytymisiin, mitä hän vaatii vastapuolilta. Näitä käytäntöjä ei aseta järjestelmän suunnittelija—kukin osallistuja valitsee ne ja ilmaisee koneluettavassa muodossa.

Tämä formalisointi mahdollistaa kolmivaiheisen emergenssin. Ensin yksilön moraali koodataan **käytännöksi**—joukoksi ilmoitettuja sääntöjä, kynnyksiä ja vastefunktioita, joita DID sitoutuu noudattamaan. Toiseksi kaikkien verkoston käytäntöjen kokonaisuus tuottaa **emergentin etiikan**—tilastollisesti havaittavia normeja, joita yksikään osallistuja ei suunnitellut mutta jotka syntyvät tuhansien yksilöllisten moraalikantojen vuorovaikutuksesta [9]. Kolmanneksi tämä emergentti etiikka, ilmaistuna jaettuina käyttäytymisnormeina, joita valvotaan kaksisuuntaisilla hintasignaaleilla, muodostaa **mitattavissa olevan yhteiskuntasopimuksen**—ei teoreettisen rakennelman, jota kukaan ei allekirjoittanut [10], vaan empiirisesti havaittavan sääntöjoukon, jota todellinen käyttäytyminen tukee.

Tämä prosessi heijastelee moraalisten perustusten teorian löydöksiä [11]: inhimillinen moraali on intuitiivinen, pluralistinen ja kulttuurisesti vaihteleva. RSN ei vaadi moraalista konsensusta syötteenä; se tuottaa käyttäytymiskonsensuksen tuloksena. Näin syntyvä yhteiskuntasopimus ei ole staattinen—se kehittyy, kun osallistujat liittyvät, poistuvat ja säätävät käytäntöjään verkoston palautteen mukaan. Toisin kuin klassinen yhteiskuntasopimusteoria, tämä sopimus on peruutettavissa, havaittavissa ja täytäntöönpanokelpoinen ilman suvereenia.

8 Talousmalli

Edeltävät luvut kuvasivat työkalua—RSN:n todennusmekanismeja, kustannusrakennetta ja emergenttiä konsensusta. Tämä luku kuvaa metodologiaa tämän työkalun soveltamiseksi finanssi- ja hallintosiirtymään. Työkalu on yleiskäyttöinen; alla oleva metodologia on yksi mahdollinen sovellus.

8.1 Kannustinrakenne

Maine pääomana luo suoria kannustimia rehelliseen käyttäytymiseen. Normaalitoiminnassa osallistujat rakentavat mainetta luonnostaan jokapäiväisten transaktioiden ja täytettyjen sitoumusten kautta. Ensisijainen menoerä liittyy *negatiivisiin* väitteisiin—muiden aiheuttaman vahingon kirjaamiseen. Tämä epäsymmetria kannustaa hyödylliseen, luotettavaan käyttäytymiseen: rehellinen oleminen ei maksa ylimääräistä, kun taas vahingollinen oleminen luo dokumentoidun jäljen, jonka muut maksavat säilyttääkseen. Tekopyhyys—sääntöjen ilmoittaminen niitä noudattamatta—on kallein epäonnistumisen muoto, koska se osoittaa tahallista petosta.

8.2 Rinnakkainen finanssijärjestelmä

Kolme komponenttia mahdollistaa kilpailullisen paineen: (1) **Yksinkertainen vero**—yksi suhteellinen prosentti ilman poikkeuksia, aluksi marginaalisesti nykyisen efektiivisen prosentin alapuolella; (2) **Sähköinen menorekisteröinti (Electronic Spending Registration, ESR)**—kääntäen Tšekin EET-mallin niin, että kansalaiset valvovat valtion menoja; (3) **Kansalaisohjattu verojen kohdentaminen**—alkaen muutamasta prosentista ensimmäisenä vuonna ja saavuttaen vuosikymmenen jälkeen mitä tahansa alhaisista kaksinumeroisista luvuista täyteen siirtymään kansalaisohjattuun järjestelmään, omaksumisen nopeudesta riippuen. Todellinen tahti riippuu siitä, kuinka nopeasti valtion palveluiden vapaiden markkinoiden vaihtoehtoja syntyy, ja valtion halukkuudesta tehdä yhteistyötä siirtymän kanssa; ajan funktion ei tarvitse olla lineaarinen, eikä ole mitään syytä asettaa ylärajaa sille, mihin omaksuminen voi lopulta yltää.

9 Siirtymäpolku

Siirtymä etenee kolmen vaiheen läpi (kuva 10): **Vaihe 1: Päällyskerros** (RSN informaatiokerroksena, valtio ainoa tarjoaja), **Vaihe 2: Kilpailu** (RSN tarjoaa toiminnallisia vaihtoehtoja, kaksoisjärjestelmän käyttö) ja **Vaihe 3: Siirtymä** (RSN ylittää valtion vastineet, vapaaehtoinen siirtyminen). Siirtymä on peruutettavissa jokaisessa vaiheessa.

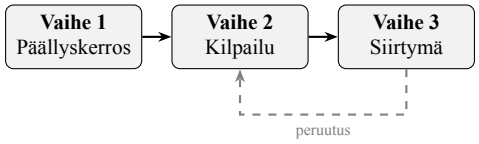

Figure 10: Kolmivaiheinen siirtymä—peruutettavissa jokaisessa vaiheessa.

Ensisijainen painemekanismi on finanssipoliittinen:

kun ehdolliset veronmaksajat saavuttavat "taloudellisesti merkittävän vähemmistön X"—ryhmän, joka on kyllin suuri, jotta sitä vastaan kohdistuva sortaminen aiheuttaa ei-triviaalia taloudellista vahinkoa ja kansalaistottelemattomuudesta tulee uskottava uhka—valtio ryhtyy neuvottelemaan. Havainnollistuksen vuoksi käytämme $X \approx 15\%$ BKT:sta, mutta todellinen kynnys riippuu kyseisestä taloudesta.

10 Turvallisuusanalyysi

Tarkastelemme viittä vastustajakategoriaa: yksittäiset pahantekijät, järjestäytyneet ryhmät, yritysvastustajat, valtiotason vastustajat ja protokollatason vastustajat.

Sybil-vastustuskyky [12]. Maineen rakentaminen vaatii jatkuvaa, todennettavaa vuorovaikutusta. Onnistuneen Sybil-hyökkäyksen kustannus skaalautuu lineaarisesti valeidentiteettien mukaan ja neliöllisesti kohdemainetason mukaan. Useiden DID:ien käyttäminen rinnakkain on mahdollista mutta suunnittelultaan kallista—kunkin identiteetin on itsenäisesti kartutettava mainetta aidon toiminnan kautta. Vapaissa yhteiskunnissa tämä kustannus ehkäisee satunnaista väärinkäyttöä; diktatuureissa rinnakkaiset DID:t muuttuvat selviytymistyökaluksi, joka mahdollistaa lokeroidun vastarinnan, maanalaisen koordinaation ja turvallisemman mustan pörssin navigoinnin.

Salaliittopuolustus. Suljettujen ryhmien keskinäisen hyväksynnän kuviot ovat havaittavissa sosiaalisen graafin analyysin kautta. Maineen aggregointifunktiot alentavat tiiviisti klusteroituneiden lähteiden väitteitä.

Valtiotason vastustaja. Onion-reititys, keskitetyn infrastruktuurin puuttuminen ja Todentaja-roolin jakautuminen osallistujakannan kesken varmistavat, että tukahduttaminen vaatii toimenpiteitä, jotka ovat suhteettomia mihinkään hyötyyn nähden.

Yksityisyys vs. vastuuvelvollisuus. Salanimisyys—välimaasto anonymiteetin ja identiteetin paljastamisen välillä—antaa DID:ien kartuttaa merkityksellistä mainetta paljastamatta haltijan todellisen maailman identiteettiä.

11 Yksityisyysnäkökohdat

RSN:n yksityisyysmalli rakentuu salanimisyydelle. Haltija hallitsee identiteetin paljastamista: minimaalinen (puhdas salanimi), valikoiva (tietyt tunnistetiedot linkitetty) tai täysi (laillinen identiteetti liitetty). Julkaistut väitteet ovat pysyviä—järjestelmä tukee kontekstuaalista korjausta mutta ei poistamista. Haltija voi hylätä vaarantuneen DID:in ja aloittaa alusta, luopuen kertyneestä maineesta.

12 Aiempi tutkimus

W3C DID Core -spesifikaatio [2] ja Ceramic Network [8] tarjoavat identiteettiperustan. EigenTrust [13] osoitti hajautetun maineen aggregoinnin ilman keskusauktoriteettia. SBT:t [3] esittelivät siirtokelvottomat sosiaaliset tunnukset. RSN eroaa painottamalla taloudellista kustannusta laatusuodattimena ja mekanisminaan radikalismin hinnoittelu.

DAO:t [4] ja neliöllinen äänestäminen [5] osoittivat hajautetun hallinnon toteutettavuuden. RSN johtaa konsensuksen kaksisuuntaisista hintaneuvotteluista äänestämisen sijaan.

Ehdotus ammentaa anarkokapitalistisesta teoriasta [14, 15] yksityisen palveluntarjonnan osalta mutta poikkeaa kahdessa ratkaisevassa suhteessa: se suunnittelee ilkeyttä ja kostonhaluisia impulsseja varten sen sijaan, että olettaisi rationaalisuutta, ja se ehdottaa asteittaista siirtymää vallankumouksen sijaan. Emergenttien yhteiskuntasopimusten käsitteellä on esikuvia Hayekin spontaanin järjestyksen teoriassa [16].

Anarko-agorismi. RSN:llä on merkittävää yhteistä maaperää agoristisen vastatalouden [17] kanssa—erityisesti painotus rinnakkaisten instituutioiden rakentamiseen ja vapaaehtoiseen vaihtoon. Agorismi kuitenkin taipuu olettamaan rationaalisen oman edun tavoittelun riittäväksi koordinointimekanismiksi ja usein siitä puuttuu konkreettinen siirtymäpolku olemassa olevista valtiorakenteista. RSN sisällyttää eksplisiittisesti ei-rationaaliset käyttäytymistaipumukset ja tarjoaa finanssipoliittisen painemekanismin asteittaiseen siirtymään.

Meritokratia. RSN saattaa edustaa ensimmäistä toimivaa kuvausta siitä, kuinka meritokratia [18] voi syntyä systeemisenä ominaisuutena eikä iskulauseena. Perinteiset meritokraattiset järjestelmät epäonnistuvat, koska ne vaativat keskusauktoriteetin määrittelemään ja valvomaan "ansiota". RSN:ssä ansio syntyy kaksisuuntaisista arvioinneista: ne, jotka tuottavat arvoa, kartuttavat mainetta; mikään komitea ei päätä, kenellä on ansiota.

Omaisuus etuoikeutena. RSN poikkeaa perustavasti anarkokapitalistisista ja itävaltalaisen koulukunnan käsittelyistä, jotka pitävät omistusoikeuksia luonnollisina ja absoluuttisina. RSN-viitekehyksessä omaisuus on *etuoikeus*—sosiaalinen tunnustus, joka voidaan ääritapauksissa peruuttaa

yhteisön toimesta, kun osallistuja perustavalla tavalla rikkoo jaettuja normeja (petos, kieltäytyminen puolustamasta yhteisöä eksistentiaalisessa kriisissä, järjestelmällinen hyväksikäyttö). Tämä ei ole valtion pakkolunastusta vaan sosiaalisen tunnustuksen peruuttamista kaksisuuntaisten suhteiden verkoston toimesta.

13 Pohdinta ja rajoitukset

Kylmäkäynnistys. RSN:n arvo riippuu verkostovaikutuksista; varhaiset omaksujat kohtaavat rajallisen arvon, kunnes osallistuminen saavuttaa kynnyksen. Kuitenkin jo varhaisista vaiheista lähtien DID-verkosto toimii hyödyllisenä täydentävänä tietolähteenä. Varhaisen maineen arvioinnin ja auktoriteettien arvioinnin odotetaan kehittyvän vähitellen kasvavan hienostuneisuuden myötä.

Loisimisen esto ja pääsynvalvonta. Kohde-DID:t voivat asettaa porrastettuja maksuja ja pääsyrajoituksia matalan maineen DID:eiltä tuleville kyselyille. Tämä ei ole binääristä vaan jatkuva asteikko: mitä vähemmän mainetta kyselevällä DID:illä on, sitä vähemmän tietoa se saa, sitä kauemmin se odottaa ja sitä enemmän se maksaa. Tämä mekanismi kannustaa aitoon osallistumiseen passiivisen kuluttamisen sijaan.

Pääsyn epätasa-arvo. Väitteiden julkaisemisen kustannus voi suodattaa pois legitiimejä valituksia taloudellisesti heikommassa asemassa olevilta osallistujilta. Lieventäminen: jokainen osallistuja toimii samanaikaisesti mahdollisena todentajana (tai delegoi tämän roolin) ja ansaitsee todennusmaksuja. Riittävän aikahorisontin yli ei-radikaalin osallistujan tulisi lähestyä taloudellista neutraaliutta—todennustulot suunnilleen tasapainottavat julkaisukustannukset. Tämä on tilastollinen odotus, ei takuu.

Maineen epätasa-arvo. Varhaiset omaksujat kartuttavat etuja, jotka voivat luoda esteitä myöhemmin tulleille. Maineen arvioinnin suorittavat kuitenkin kolmannen osapuolen tarjoajat, jotka voivat halutessaan lieventää ensiliikkujan etua aggregointialgoritmiensa kautta. Ensimmäisenä oleminen hyvällä maineella on legitiimi vertaileva taloudellinen etu—ja se on tarkoituksellista.

Avoimet kysymykset. Optimaaliset kustannusfunktiot, aggregointistandardit, protokollan hallinta ja vuorovaikutus tekoälyn tuottaman synteettisen mainedatan kanssa jäävät tulevan työn alueiksi.

Tämä artikkeli ei väitä, että RSN tuottaisi optimaalisia tuloksia kaikissa olosuhteissa. Se väittää, että RSN edustaa *toteuttamiskelpoista* vaihtoehtoa—teknisesti toteutettavaa, taloudellisesti itsensä ylläpitävää ja sosiaalisesti yhteensopivaa inhimillisten käyttäytymistaipumusten kanssa sellaisina kuin ne todella ovat.

14 Johtopäätös

Tämä artikkeli on esitellyt maineeseen perustuvan sosiaalisen verkoston, hajautetun protokollan, joka mahdollistaa salanimellä tapahtuvan, todennettavan mainevaihdon. Kalliin radikalismin periaate varmistaa, että petolliset väitteet hinnoitellaan pois ilman sensuuria. Ehdotettu siirtymäpolku mahdollistaa asteittaisen, peruutettavissa olevan siirtymän olemassa olevista instituutioista. Suunnittelu sisällyttää inhimillisen luonnon sellaisena kuin se on—mukaan lukien pikkumaisuuden, ilkeyden ja kostonhaluisen tyydytyksen kaipuun—sen sijaan, että vaatisi ideologista muutosta. Tuloksena ei ole utopia vaan järjestelmä, jossa oikeus on saavutettavissa, maine ansaitaan ja väärinkäytöksen kustannuksen kantaa se osapuoli, joka sen aiheutti.

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.