

Gedecentraliseerd Reputatienetwerk: Een raamwerk voor natuurlijke maatschappelijke organisatie

Pavel Kudrna
Prague, Czechia
Draft v1 — March 2026

Abstract

Het rechtvaardigheidsgevoel—de overtuiging dat onrecht wordt rechtgezet en verdienste wordt beloond—is de sterkste bindende kracht van de samenleving. Wanneer gecentraliseerde bestuursinstellingen dit gevoel niet kunnen leveren omdat de kosten van het afdwingen van een recht de waarde van het recht zelf overstijgen, brokkelt de maatschappelijke samenhang af. Bestaande institutionele structuren slagen er niet in een aanzienlijke categorie geschillen op te lossen, en wel op systematisch dezelfde wijze waarop centrale planning faalt bij het toewijzen van middelen: door informatieasymmetrie, ontbrekende terugkoppelingslussen en de loskoppeling van besluitvormers van de gevolgen van hun beslissingen. Dit artikel presenteert een Reputatie Sociaal Netwerk (RSN): een gedecentraliseerde, onomkoopbare, censurbestendige communicatielaag gebouwd op Decentralized Identifiers (DIDs) die pseudonieme deelnemers in staat stelt reputatie-informatie over gedrag in de echte wereld te publiceren, te verifiëren en te consumeren. Het kernmechanisme rust op drie ontwerpprincipes: (1) een asymmetrische kostenstructuur waarbij het lezen van reputatiegegevens goedkoop is maar het schrijven verifieerbare inspanning vereist; (2) een niet-deterministisch protocol voor de selectie van verifieerders op basis van consistent hashing dat radicale beweringen beprijsd via oplopende iteratiekosten; en (3) een marktgedreven model van reputatie-autoriteiten waarbij private verifieerders hun opgebouwde reputatie inzetten voor de juistheid van de beweringen die zij onderschrijven. De resulterende architectuur brengt een emergente meritocratie voort zonder centrale coördinatie en maakt een geleidelijk, omkeerbaar migratiepad mogelijk vanuit bestaande, door de staat beheerde systemen.

1 Inleiding

1.1 Het probleem van gecentraliseerd vertrouwen

Modern bestuur rust op een fundamentele aanname: dat gecentraliseerde instellingen op schaal vertrouwen tussen vreemden kunnen bemiddelen. Rechtbanken beslechten geschillen. Registers certificeren eigendom. Toezichhoudende instanties handhaven normen. Deze instellingen werden ontworpen in een tijdperk waarin informatie schaars was, communicatie traag verliep en de delegatie van bevoegdheid aan een centraal orgaan het enige haalbare coördinatiemechanisme was. Gecentraliseerd bestuur faalt echter om dezelfde structurele redenen als centrale planning: informatieasymmetrie, ontbrekende terugkoppelingslussen en de loskoppeling van besluitvormers van de gevolgen van hun beslissingen.

De aanname faalt bijvoorbeeld wanneer de kosten van institutionele bemiddeling de waarde van het geschil overstijgen. Neem een huurder die ontdekt dat zijn gehuurde appartement een wettelijk verplicht elektrisch veiligheidscertificaat mist—een omstandigheid die onmiddellijk levensgevaar oplevert. Het wettelijke recht van de huurder om de overeenkomst te ontbinden is ondubbelzinnig. Toch overstijgen de kosten van het afdwingen van dat recht via de rechtbank de geldwaarde van de borg en de verschuldigde schadevergoeding, zelfs met inbegrip van eventuele wettelijke compensatie [1]. De rationele reactie is het verlies te dragen en te vertrekken.

Dit is geen pathologisch randgeval. Het is de standaardervaring voor een aanzienlijke categorie geschillen waarin de schade reëel is maar de financiële inzet onder de drempel valt waarboven institutionele handhaving economisch rationeel wordt. Het resultaat is een systeem dat structureel kwaadwillenden bevoordeelt: wie anderen schade toebrengt in hoeveelheden onder deze drempel kan ongestraft handelen, omdat de kosten van het zoeken naar recht op de benadeelde partij drukken.

Het bovenstaande voorbeeld is ontleend aan de juridische omgeving van de auteur—het Tsjechische civielrechtelijke stelsel. In andere rechtstradities—op precedenten gebaseerd common law, gewoonterecht, gemengde stelsels—faalt de rechtvaardigheid op andere manieren en in verschillende mate, afhankelijk van de culturele en procedurele bijzonderheden van het rechtsgebied. Lezers zullen waarschijnlijk gelijkwaardige voorbeelden uit hun eigen context herkennen. Wat structureel universeel is, is het patroon: geschillen waarvan de waarde onder de drempel van economisch rationele handhaving valt, eindigen ermee dat het verlies door de benadeelde partij wordt gedragen. Het RSN belooft geen perfecte rechtvaardigheid—het vermindert slechts het structurele voordeel dat kwaadwillenden genieten wanneer institutionele handhaving oneconomisch is.

1.2 Waarom bestaande oplossingen tekoortschieten

Raamwerken voor gedecentraliseerde identiteit (DID) [2] bieden cryptografische mechanismen voor zelfsoverein identiteitsbeheer, maar richten zich hoofdzakelijk op identiteitsverificatie zonder de bredere kwestie van gedragsreputatie aan te pakken.

Soulbound Tokens (SBTs) [3] vatten het inzicht dat reputatie niet-overdraagbaar is, maar leunen op blockchain-infrastructuur met schaalbaarheidsbeperkingen en pakken de economische prikkels die de invoer van informatie beheersen niet aan. Verwante concepten zoals merit tokens (bijv. Liberland) delen een vergelijkbare filosofie, maar blijven gebonden aan specifieke jurisdictionele kaders.

Gedecentraliseerde autonome organisaties (DAO's) [4] implementeren bestuur via smart contracts, maar reproduceren plutocratische dynamieken waarbij invloed evenredig is aan kapitaal. Quadratic voting [5] verzacht dit gedeeltelijk, maar beperkt de praktische toepassing. DAO's staan ook voor het fundamentele *oracle-probleem*: smart contracts kunnen toestanden in de echte wereld niet betrouwbaar verifiëren zonder een vertrouwde externe bron, en dit probleem heeft geen algemene oplossing binnen de blockchain-architectuur.

Geen enkel bestaand systeem combineert decentralisatie, censurbestendigheid, pseudonimiteit, verifieerbare toegangskosten en emergente consensus.

1.3 Bijdragen

Dit artikel levert de volgende bijdragen:

1. Definitie van het **Reputatie Sociaal Netwerk (RSN)**, een gedecentraliseerd protocol dat het DID-raamwerk uitbreidt ter ondersteuning van bilaterale reputatie-uitwisseling.
2. Een **niet-deterministisch protocol voor de selectie van verifieerders** op basis van consistent hashing [6].
3. Het **principe van duur radicalisme**, dat beweringen beprijst naar hun afstand tot de netwerkconsensus via drie samenwerkende kostenkanalen.
4. Een **model van reputable autoriteiten** met asymmetrische prikkels waarbij valse onderschrijving catastrofaal veel meer kost dan legitieme vergoedingen.
5. Een **geleidelijk migratiepad** via parallelle fiscale infrastructuur.

2 Ontwerpprincipes

De RSN-architectuur wordt begrensd door vijf niet-onderhandelbare ontwerpprincipes.

Continuïteit en evolutie. Het systeem bestaat naast bestaande instellingen gedurende een overgangsperiode van onbepaalde duur. De overgang moet in elke fase omkeerbaar zijn.

Vrijwilligheid en verantwoordelijkheid. Deelname is vrijwillig, maar vrijwilligheid gaat gepaard met verantwoordelijkheid: een deelnemer die de controle over een institutionele functie op zich neemt, neemt tegelijkertijd de bijbehorende verplichtingen op zich.

Diversiteit en culturele neutraliteit. Consensus ontstaat uit bilaterale interacties, niet uit vooraf vastgelegde regels die door systeemontwerpers worden opgelegd.

Veerkracht en censurbestendigheid. De kosten van het censureren van het netwerk moeten de kosten van het tolereren ervan overstijgen. Alleen volledig totalitarisme—tegen ruïneuze politieke en economische kosten—kan het systeem onderdrukken.

Consensus en handhaving. Het systeem verwerkt menselijke neigingen tot kleingeestigheid, wrok en vergeldende genoegdoening als dragende kenmerken. Wangedrag wordt niet verboden; het wordt beprijsd.

3 Systeemoverzicht

3.1 Reputatie Sociaal Network

Het RSN is een gedecentraliseerde, peer-to-peer communicatielaag waarin deelnemers verifieerbare informatie over gedrag in de echte wereld uitwisselen. De bepalende eigenschappen zijn: gedecentraliseerde en niet-censureerbare infrastructuur; pseudonieme deelname via DID's; asymmetrische kostenstructuur (lezen is goedkoop, schrijven is duur); cryptografische verifieerbaarheid; en **ondersteuning van standaarden**—machinaal leesbare formaten voor informatie die door het netwerk wordt verspreid, voor diensten die door autoriteiten worden aangeboden (samenstelling van beweringen, onderschrijving, getuigedienst) en voor het beleidsformaat, met inbegrip van regels voor het beoordelen van de reputatie van tegenpartijen en het inschatten van het risico op beleidsdiscrepantie (tussen aangegeven en werkelijk gedrag).

3.2 Architectuurcomponenten

Het RSN bestaat uit vier primaire componenten (Fig. 1):

1. **DID-laag.** Identiteiten van deelnemers met aangegeven regels, reputatiemetadata en netwerkrouing.
2. **Bewering-protocol.** Gestructureerd formaat voor het publiceren van beweringen over gebeurtenissen in de echte wereld.
3. **Verificatienetwerk.** Gedecentraliseerd protocol voor het toewijzen van verifieerders via consistent hashing.
4. **Reputatie-aggregatielaag.** Diensten die voor mensen leesbare reputatiesamenvattingen produceren.

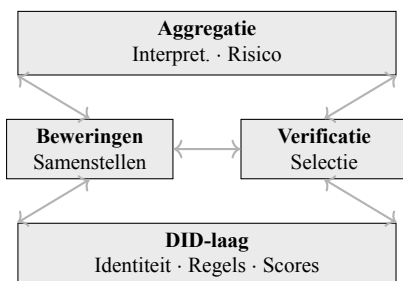


Figure 1: RSN-architectuur met vier lagen.

3.3 Rollen van deelnemers

Een verificatietransactie omvat tot zes onderscheiden DID-rollen (Fig. 2): **Uitgever** (DID_I , stelt de bewering op en dient deze in), **Onderwerp** (DID_S , de DID waarover de bewering gaat—kan samenvallen met de Uitgever), **Autoriteit** (DID_A , onderschrijft de bewering tegen een vergoeding; kan ook getuigediensten aanbieden—*optioneel*), **Getuige** ($DID_{W1..n}$, incognito toezichthouder op de eerlijkheid van de verifieerder via challenge-codes—*optioneel*), **Verifieerder** (DID_V , algoritmisch geselecteerd om de bewering te publiceren) en het **RSN** (het netwerk waar geverifieerde beweringen worden gepubliceerd). Elke rol kan aan een andere DID worden gedelegeerd (Sectie 7.4). Een Autoriteit combineert doorgaans onderschrijving met getuigediensten, maar de twee functies zijn logisch onafhankelijk.

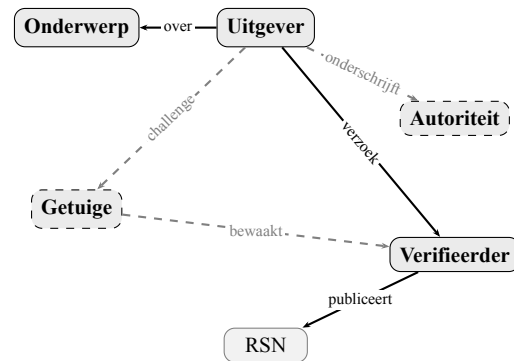


Figure 2: DID-rollen in een verificatietransactie. Gestippeld = optioneel (Autoriteit, Getuige).

3.4 Onomkoopbaarheid: vier krachten

De onomkoopbaarheid van het RSN komt niet voort uit één enkel mechanisme, maar uit vier gelijktijdige krachten. Geen enkele is op zichzelf voldoende; alleen hun combinatie maakt een corruptiepoging economisch irrationeel.

Onvoorspelbaar doelwit. De verifieerder voor elke bewering wordt niet-deterministisch geselecteerd via consistent hashing (Sectie 5.3). Een aanval kan geen specifieke verifieerder vooraf als doelwit voor omkoping kiezen, omdat de identiteit van de verifieerder een functie is van de inhoud van de bewering en van voorgaande iteraties, niet van de keuze van de uitgever.

Reputatiehefboom—langzaam omhoog, snel omhoog. Reputatie kan alleen stapsgewijs worden opgebouwd, via aanhoudend consistent gedrag. Ze kan echter catastrofaal verloren gaan bij één frauduleuze onderschrijving (Sectie 6.2). Deze asymmetrie betekent dat jaren van opgebouwde reputatie door één oneerlijke onderschrijving vernietigd kunnen worden; de optimale strategie blijft verdachte beweringen te weigeren.

Publieke belofte. Elke DID-houder verklaart publiekelijk zijn beleid—een machinaal leesbare set regels die hij zich verbindt na te leven. Afwijking tussen de verklaring en het werkelijke gedrag is detecteerbaar en wordt beprijsd als een reputatievergriep dat ernstiger is dan de onderliggende overtreding (Sectie 7.3). Hypocrisie is daarom duurder dan directe oneerlijkheid.

Asymmetrie van aanvalskosten in het netwerk. De kosten van het censureren of destabiliseren van het netwerk groeien niet-lineair met de omvang en dichtheid van het netwerk, terwijl de kosten van het tolereren ervan constant blijven. Om censuur lonend te maken, zou een gecentraliseerde actor deze over het hele netwerk moeten toepassen—wat maatregelen vereist die niet in verhouding staan tot enig denkbaar voordeel (Sectie 10).

4 Model voor gedecentraliseerde identiteit

4.1 DID met bijzondere eigenschappen

Het RSN breidt de W3C DID Core-specificatie [2] uit met: **Aangegeven regels** (machinaal leesbare gedragsverbintenissen), **Reputatiemetadatum** (geaggregeerde gedragsscore) en **Netwerkroting** (veranderlijke onion-gateway, los van de stabiele ringpositie).

4.2 Levenscyclus van een bewering

Een bewering doorloopt zes fasen (Fig. 3): samenstelling, optionele onderschrijving door een autoriteit, selectie van de verifieerder via consistent hashing, verificatiebeslissing (aanvaarden of weigeren met iteratie), publicatie en reputatie-update voor alle partijen.

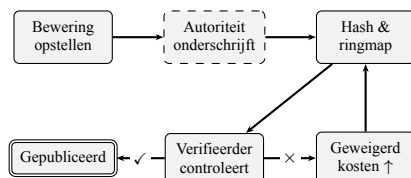


Figure 3: Levenscyclus van een bewering met iteratielus.

4.3 Relatie tot W3C DID Core

Het identiteitsmodel van het RSN is een echte superset van de W3C DID Core-specificatie [2]. Alle RSN-DIDs zijn geldige W3C-DIDs. De RSN-specifieke uit-

breidingen zijn gecodeerd als eigenschappen van het DID-document, gedefinieerd in een specifieke DID-methodespecificatie, compatibel met bestaande infrastructuur zoals ION [7] en Ceramic [8].

5 Verificatie en verspreiding van informatie

5.1 Kosten van informatie-invoer

Het economische kernprincipe van het RSN is de asymmetrie tussen lezen en schrijven. Het lezen van reputatiegegevens nadert nulmarginale kosten voor deelnemers die deel uitmaken van het DID-netwerk en toegang hebben die in verhouding staat tot hun reputatie—nieuwkomers moeten geleidelijk bredere toegang verdienen (zie anti-leeching). Schrijven—opgevat als de duurzame materialisatie van reputatie in het netwerk, niet als een eenmalige technische handeling—vereist een verifieerbare cumulatieve investering langs drie dimensies: **tijd** (levensjaren besteed aan consistent gedrag, nagekomen verbintenissen en gecultiveerde relaties), **energie** (inspanning geïnvesteerd in eerlijk handelen, zorg voor samenwerkingen en betrouwbaarheid op lange termijn) en **geld** (investering in de eigen naam—professionele ontwikkeling, de kwaliteit van het eigen werk, herstel van veroorzaakte schade). Reputatie kan niet onmiddellijk worden gekocht—ze is het resultaat van levenslange opbouw die het systeem slechts zichtbaar en overdraagbaar tussen contexten maakt. De eenmalige technische kosten van het protocol (cryptografische handtekeningen, vergoedingen voor verifiers) zijn verwaarloosbaar in vergelijking met deze onderliggende investering.

5.2 Sociale grafiek en contactdiepte

Het RSN is fundamenteel een sociaal netwerk: elke DID voegt contacten toe (andere DIDs) die de verbinding toestaan. Deze contacten hebben hun eigen contacten, enzovoort. De algoritmische zoektocht naar verifiers werkt binnen een instelbare diepte h van gekoppelde contacten (bijv. $h = 3$: de eigen directe contacten, hun contacten, en contacten van contacten). Deze architectuur vereist geen enkele wereldwijde blockchain—ze bevordert van nature het ontstaan van gemeenschappen/clusters met overlappingen naar andere gemeenschappen. Elke DID-deelnemer moet een gepubliceerd **beleid** hebben—een machinaal leesbare set regels die bepaalt hoe inkomende verzoeken worden beoordeeld. Beleidsschendingen worden als

negatieve artefacten in het netwerk vastgelegd.

5.3 Algoritmische selectie van verifieerders

Het verificatieprotocol maakt gebruik van consistent hashing [6] (Fig. 4). Verificatie is een betaalde dienst: verifieerders werken tegen een vergoeding, wat een markt creëert waarin concurrentie prijsstelling, snelheid en betrouwbaarheid aandrijft.

Stap 1. Het beweringsdocument wordt samengevoegd met het hashresultaat van de vorige iteratie (of $\emptyset$ bij de eerste iteratie) en gehasht:

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

Het algoritme moet het *volledige pad* van alle voorgaande verzoeken en antwoorden bevatten—niet louter een hash van de vorige iteratie. Het volledige antwoord van elke verifieerder (aanvaarding, weigering, opgegeven prijs, reden) wordt aan het groeiende document toegevoegd, verifieerbaar via cryptografische handtekeningen bij elke stap.

Stap 2. De hash wordt afgebeeld op N posities op de consistent-hashing, gelijkmatig verdeeld (bijv. voor $N = 4$: $+0^\circ, +90^\circ, +180^\circ, +270^\circ$). Vanaf elke positie selecteert een zoektocht met de klok mee de dichtstbijzijnde DID als kandidaat-verifieerder (Fig. 5). N is een variabele parameter die kan afhangen van het percentage momenteel actieve DIDs, het tijdstip van de dag of de historische reactiesnelheid van het netwerk.

Stap 3. De Verifieerder aanvaardt (publiceert en zet reputatie in) of weigert (keert terug naar Stap 1 met de weigeringshash). Wanneer een knooppunt niet reageert ondanks een verklaarde online-status, moet het volgende verzoek alle antwoorden van alle N voorgaande kandidaat-verifieerders bevatten.

Anti-leeching. Doel-DIDs mogen vergoedingen of toegangsbeperkingen instellen voor vragen van nieuwe DIDs met weinig reputatie. Dit gegradueerde mechanisme (niet binair) dwingt nieuwkomers reputatie op te bouwen door echte activiteit voordat zij vrijelijk de gegevens van anderen consumeren.

Elke weigering voegt het volledige antwoord van de verifieerder (inclusief redenen en voorwaarden) toe aan het beweringsdocument, waardoor de inhoud ervan uitdijt. Op basis van het uitgebreide document wordt niet-deterministisch een nieuwe hash berekend, die naar een andere ringpositie wijst en een andere verifieerder selecteert. Documentatie van het volledige pad is verplicht—de uitgever kan de volgende verifieerder niet voorspellen of beïnvloeden. Als een verifieerder een verzoek negeert ondanks een compatibel

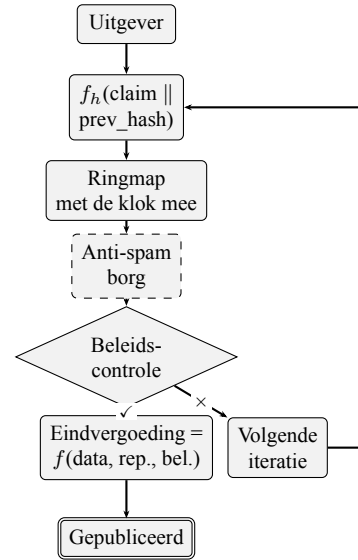


Figure 4: Protocol voor de selectie van verifieerders. De anti-spamborg is optioneel en kan restitueerbaar zijn. De eindvergoeding wordt alleen bij aanvaarding betaald.

verklaard beleid, leggen getuigen (indien aanwezig) dit vast, en de uitgever kan getuigenbewijs bijvoegen bij de uiteindelijke publicatie.

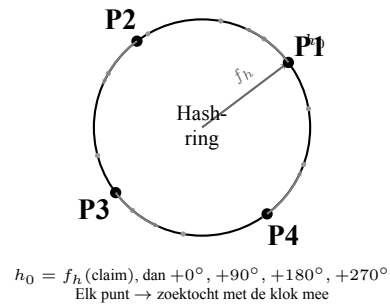


Figure 5: Selectie op meerdere punten ($N=4$). Hash h_0 bepaalt de verschuiving; 4 punten gelijkmatig verdeeld vanaf h_0 .

5.4 Getuigeprotocol

De rol van **Getuige** biedt incognito verantwoording voor de eerlijkheid van de verifieerder via een cryptografisch challenge-code-protocol:

Stap W1. De verzoeker ondertekent het verificatieverzoek en verzendt het naar N_w getuigen—contacten uit het sociale netwerk van de verzoeker, of gespecialiseerde aanbieders van getuigediensten die tegen een vergoeding werken.

Stap W2. Elke getuige w_i ondertekent het volledige ondertekende verzoek, behoudt de oorspronkelijke handtekening σ_i en berekent een challenge-code $c_i =$

$h(\sigma_i)$. De challenge-code wordt aan het verzoek toegevoegd.

Stap W3. Het verzoek, dat nu N_w challenge-codes draagt, wordt naar de verifieerder verzonden. De verifieerder ziet de codes maar *kan niet vaststellen* wie de getuigen zijn of dat de codes overeenkomen met echte handtekeningen.

Stap W4 (eerlijke verifieerder). Als de verifieerder reageert volgens zijn verklaarde beleid, blijven de challenge-codes ondoorzichtig. Getuigen worden nooit onthuld. Er worden geen aanvullende gegevens gepubliceerd.

Stap W5 (beleidsschending). Als de verifieerder zijn beleid schendt (het verzoek negeert, inconsistent reageert), bezit de verzoeker de oorspronkelijke handtekeningen σ_i van de getuigen. Deze kunnen als begeleidende gegevens worden gepubliceerd: iedereen kan $c_i = h(\sigma_i)$ verifiëren, wat bewijst dat de getuige aanwezig was. De verzoeker kan onafhankelijk publiceren—de verifieerder heeft de challenge-codes al in zijn antwoord ondertekend.

De bluff-eigenschap. De verzoeker mag willekeurige waarden invullen voor sommige of alle challenge-codes. De verifieerder kan echte codes (gedekt door hoogaangeschreven autoriteiten) niet van ruis onderscheiden. Deze *onzekerheid* is het handhavingsmechanisme: elk verzoek draagt het risico dat een gerespecteerde autoriteit incognito meekijkt. De kosten van het handhaven van deze druk zijn vrijwel nul (het genereren van willekeurige getallen), terwijl de mogelijke kosten van oneerlijkheid voor de verifieerder catastrofaal zijn. Eerlijk gedrag wordt aangemoedigd, zelfs bij afwezigheid van werkelijke getuigen.

Autoriteit als getuige. Een Autoriteit die een bewering onderschrijft, mag getuigediensten bundelen: “Ik onderschrijf uw bewering en dien als incognito getuige tijdens de verificatie.” Dit is een natuurlijk bedrijfsmodel—de Autoriteit beschikt al over de context. De twee rollen zijn echter logisch onafhankelijk.

5.5 Principe van duur radicalisme

Drie kostenkanalen versterken elkaar gelijktijdig (Fig. 6):

Kanaal 1: iteratiekosten. Elke weigering dwingt een nieuwe iteratie af die tijd en middelen verbruikt. Lineaire groei.

Kanaal 2: documentopzwellung. Elke iteratie voegt het volledige antwoord van de verifieerder toe aan het beweringsdocument. De groei is lineair, maar met een basisverschuiving: de initiële payload (in-

houd van de bewering, onderschrijving door de autoriteit, cryptografische handtekeningen) heeft al een niet-triviale omvang B_0 . Totale omvang na k iteraties: $S(k) = B_0 + k \cdot \Delta$, waarbij Δ de gemiddelde antwoordomvang is.

Kanaal 3: risicopremie van de verifieerder. Risico is subjectief. De verifieerder beoordeelt of het verklaarde beleid van de verzoekende DID in conflict is met zijn eigen commerciële, sociale of politieke belangen. De premie kan exponentieel oplopen met de waargenomen afstand tot het “ideaal” van de verifieerder: $P(d) = \alpha \cdot e^{\beta d}$, waarbij d de subjectieve afstandsmaat van de verifieerder is. Voorbij een persoonlijke no-go-grens mag de verifieerder volledig weigeren.

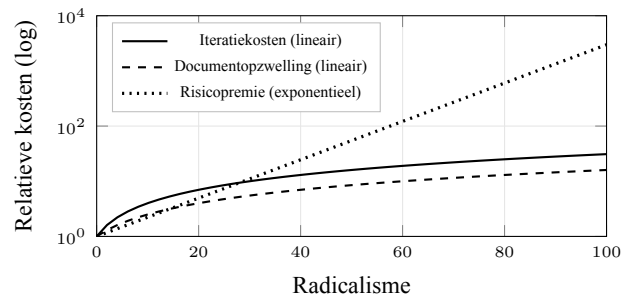


Figure 6: Kostenescalatie over drie kanalen. De risicopremie domineert bij hoog radicalisme.

Cruciaal is dat dit geen censuur is. Geen enkele bewering wordt verboden. Het systeem beprijsst risico (Tabel 1).

Table 1: Kostenvergelijking over verschillende soorten beweringen.

Type	Iter.	Doc	Verg.	Totaal
Geloofwaardig	$k_{\min}$	B_0	$P_{\min}$	Laag
Controversieel	k_{med}	$B_0 + k\Delta$	$\alpha e^{\beta d}$	Matig
Radicaal	$k_{\max}$	$\gg B_0$	$\gg P_{\min}$	Zeer hoog
Frauduleus	$\rightarrow \infty$	—	—	Onpubliceerbaar

6 Reputatie- en risicobeoordeling

6.1 Model voor reputatieopbouw

Reputatie vertoont drie eigenschappen: **trage opbouw** (stapsgewijze groei door consistent gedrag), **snelle vernietiging** (één enkele fraude kan de score catastrofaal verlagen) en **individuele beoordeling** (elke consumerende partij mag haar eigen aggregatiefunctie toepassen).

6.2 Reputabele autoriteiten

Een Reputabele Autoriteit beoordeelt beweringen en medeondertekent ze als ze tevreden is—waarbij ze haar eigen reputatie inzet (Fig. 7). De asymmetrie is opzettelijk: reputatie winnen is traag (stapsgewijs $+\delta$ per eerlijke onderschrijving), terwijl ze verliezen catastrofaal is ($-\Delta \gg \delta$ per valse onderschrijving; ter illustratie bijv. $+2\%$ tegenover -70%). De optimale strategie is altijd verdachte beweringen te weigeren. De specifieke waarden van δ en Δ zijn systeemparameters.

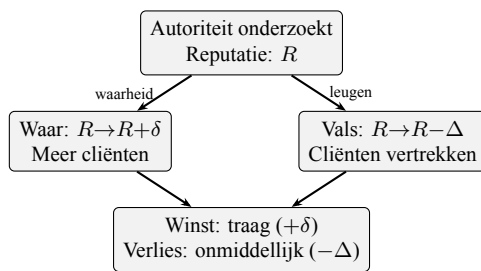


Figure 7: Reputabele Autoriteit—asymmetrische prikkels.

6.3 Multidimensionale reputatie

Reputatie is geen scalair maar een vector over meerdere dimensies: financiële betrouwbaarheid, persoonlijke integriteit, professionele competentie, maatschappelijke betrokkenheid en andere (Fig. 8). Verschillende evaluatie-aanbieders projecteren deze vector anders, afhankelijk van de context—een kredietverstrekker geeft voorrang aan financiële betrouwbaarheid, een werkgever aan professionele competentie, een buur aan maatschappelijk gedrag. Er bestaat geen enkele “juiste” reputatiescore; alleen perspectieven.

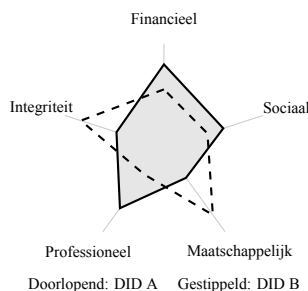


Figure 8: Multidimensionale reputatievectoren. Verschillende DIDs vertonen verschillende profielen over de dimensies.

6.4 Gedemocratiseerde risicobeoordeling

Het RSN democratiseert systematische risicobeoordeling—een capaciteit die momenteel geconcentreerd is bij financiële instellingen maar veel breder toepasbaar is dan bankieren. Industriële conglomeraten die de betrouwbaarheid van leveranciers beoordelen, verzekeraars die gedragsrisico beprijken, due diligence bij fusies en overnames, schatting van de levensduur van apparatuur in de productie—overal waar tegenpartijrisico beoordeling vereist, biedt het RSN een gedecentraliseerd, marktgedreven alternatief. Een markt van interpretatiediensten vertaalt ruwe multidimensionale reputatiegegevens in bruikbare samenvattingen, waardoor de beoordeling van tegenpartijen tegen marginale kosten toegankelijk wordt voor elke deelnemer.

7 Consensus en geschillenbeslechting

7.1 Model voor gedecentraliseerde rechtvaardigheid

Het RSN herformuleert rechtvaardigheid als een probleem van bilaterale onderhandeling. De dreiging van permanente, verifieerbare reputatieschade is een doeltreffender afschrikmiddel dan een gerechtelijke procedure die de benadeelde partij zich niet kan veroorloven.

7.2 Emergente consensus

Elke deelnemer hanteert een persoonlijke tevredenheidstrempel. De geaggregeerde consensus van het netwerk ontstaat als het statistische gemiddelde van duizenden bilaterale onderhandelingen (Fig. 9). Een reactie ver boven de consensus (barbaars) is duur om te publiceren. Een reactie dicht bij de consensus (evenredig) is goedkoop. De consensus is geen regel—het is een prijs signaal.

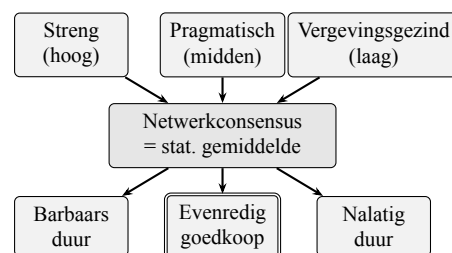


Figure 9: Emergente consensus uit individuele tevredenheidstrempels.

7.3 Kalibratie van bestraffing

Elke DID-houder verklaart publiekelijk zijn reacties op specifieke categorieën van wangedrag. Onevenredig harde of milde verklaringen trekken negatieve reputatiesignalen aan. Evenredige verklaringen worden zonder wrijving aanvaard—een zelfkalibrerend bestraffingssysteem.

Consensusverklaringen zijn zelf onderworpen aan detectie van hypocrisie: zich declaratief verbinden aan een consensuspositie terwijl men zich inconsistent gedraagt, vormt een reputatievergriep dat ernstiger is dan de onderliggende afwijking, aangezien het opzettelijke misleiding aantoonbaar.

7.4 Delegatie

Alle activiteiten binnen een DID—met één uitzondering—mogen aan een andere DID worden gedelegeerd. **De rol van Onderwerp—de DID over wiens gedrag de bewering gaat—kan niet worden gedelegeerd; ze is niet-overdraagbaar gebonden aan de identiteitshouder op wie de bewering betrekking heeft.** De andere actieve rollen—Uitgever, Autoriteit, Getuige, Verifieerder—kunnen worden overgedragen aan een aangewezen gedelegeerde DID, hetzij voor verificatie, het indienen van beweringen, deelname aan de consensus of geschillenbeslechting. Delegatie is te allen tijde herroepbaar. Dit maakt specialisatie mogelijk (bijv. professionele verificatiediensten) terwijl de Houder de uiteindelijke controle en verantwoordelijkheid behoudt. Delegatie is van toepassing op het hele systeem en is essentieel voor schaalbaarheid.

7.5 Van individuele moraal naar een emergent sociaal contract

Het verklaarde beleid van elke DID vertegenwoordigt een formalisering van individuele moraal: wat de Houder aanvaardbaar acht, hoe hij reageert op specifiek gedrag, wat hij van tegenpartijen verlangt. Dit beleid wordt niet opgelegd door een systeemontwerper—het wordt door elke deelnemer gekozen en in machinaal leesbare vorm uitgedrukt.

Deze formalisering maakt een driedfasige emergentie mogelijk. Ten eerste wordt individuele moraal gecodeerd als **beleid**—een set verklaarde regels, dremfels en responsfuncties die de DID zich verbindt na te leven. Ten tweede brengt het geheel van alle beleidsregels in het netwerk **emergente ethiek** voort—statistisch waarneembare normen die geen enkele deelnemer heeft ontworpen maar die voortkomen uit de in-

teractie van duizenden individuele morele posities [9]. Ten derde vormt deze emergente ethiek, uitgedrukt als gedeelde gedragsnormen die worden gehandhaafd via bilaterale prijssignalen, een **meetbaar sociaal contract**—geen theoretisch construct dat niemand heeft ondertekend [10], maar een empirisch waarneembare set regels die door daadwerkelijk gedrag wordt ondersteund.

Dit proces weerspiegelt bevindingen uit de moral foundations theory [11]: menselijke moraal is intuïtief, pluralistisch en cultureel variabel. Het RSN vereist geen morele consensus als input; het produceert gedragsconsensus als output. Het resulterende sociale contract is niet statisch—het evolueert naarmate deelnemers toetreden, vertrekken en hun beleid aanpassen als reactie op netwerkfeedback. In tegenstelling tot de klassieke sociaal-contracttheorie is dit contract herroepbaar, waarneembaar en afdwingbaar zonder een soeverein.

8 Economisch model

De voorgaande secties beschreven een instrument—de verificatiemechanismen, kostenstructuur en emergente consensus van het RSN. Deze sectie beschrijft een methodologie voor het toepassen van dit instrument op een fiscale en bestuurlijke overgang. Het instrument is algemeen inzetbaar; de onderstaande methodologie is één mogelijke toepassing.

8.1 Prikkelstructuur

Reputatie als kapitaal creëert directe prikkels voor eerlijk gedrag. In normale werking bouwen deelnemers op natuurlijke wijze reputatie op via alledaagse transacties en nagekomen verbintenissen. De voornaamste uitgave betreft *negatieve* beweringen—het vastleggen van door anderen aangerichte schade. Deze asymmetrie stimuleert nuttig, betrouwbaar gedrag: eerlijk zijn kost niets extra, terwijl schadelijk zijn een gedocumenteerd spoor achterlaat dat anderen zullen betalen om te bewaren. Hypocrisie—regels verklaren zonder ze na te leven—is de duurste faalwijze, aangezien het opzettelijke misleiding aantoonbaar.

8.2 Parallel fiscaal systeem

Drie componenten maken concurrentiedruk mogelijk: (1) **Eenvoudige belasting**—één enkel proportioneel tarief zonder uitzonderingen, aanvankelijk marginaal onder het bestaande effectieve tarief; (2) **Elektronische uitgavenregistratie (ESR)**—een omkering van

het Tsjechische EET-model zodat burgers de staatsuitgaven bewaken; (3) **Door burgers gestuurde belastingtoewijzing**—beginnend bij enkele procenten in het eerste jaar en na een decennium ergens tussen de lage dubbele cijfers en een volledige migratie naar een door burgers gestuurd systeem, afhankelijk van de mate van adoptie. Het werkelijke tempo hangt af van de snelheid waarmee vrijemarktalternatieven voor staatsdiensten ontstaan en van de bereidheid van de staat om aan de overgang mee te werken; de functie van de tijd hoeft niet lineair te zijn, en er is geen reden om een bovengrens te stellen aan waar de adoptie uiteindelijk kan uitkomen.

9 Migratiepad

De migratie verloopt via drie fasen (Fig. 10): **Fase 1: overlay** (RSN als informatielaag, de staat is de enige aanbieder), **Fase 2: concurrentie** (RSN biedt functionele alternatieven, gebruik van beide systemen) en **Fase 3: overgang** (RSN presteert beter dan de staatsequivalenten, vrijwillige migratie). De overgang is in elke fase omkeerbaar.

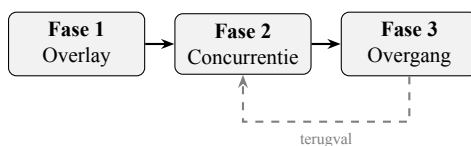


Figure 10: Migratie in drie fasen—in elke fase omkeerbaar.

Het voornaamste drukmechanisme is fiscaal: wanneer voorwaardelijke belastingbetalers een “economisch significante minderheid X ” bereiken—een groep die groot genoeg is dat repressie ertegen niet-triviale economische schade veroorzaakt en burgerlijke ongehoorzaamheid een geloofwaardige dreiging wordt—treedt de staat in onderhandeling. Ter illustratie gebruiken we $X \approx 15\%$ van het bbp, maar de werkelijke drempel hangt af van de specifieke economie.

10 Veiligheidsanalyse

We beschouwen vijf categorieën van tegenstanders: individuele kwaadwillenden, georganiseerde groepen, bedrijfsmatige tegenstanders, tegenstanders op statelijk niveau en tegenstanders op protocolniveau.

Sybil-bestendigheid [12]. Het opbouwen van reputatie vereist aanhoudende, verifieerbare interactie. De kosten van een geslaagde Sybil-aanval schalen lineair

met het aantal valse identiteiten en kwadratisch met het beoogde reputatieniveau. Meerdere DID's parallel bedienen is mogelijk maar bewust duur—elke identiteit moet onafhankelijk reputatie opbouwen door echte activiteit. In vrije samenlevingen schrikt deze kostprijs terloops misbruik af; in dictaturen worden parallelle DID's een overlevingsinstrument dat gecompartmenteerd verzet, ondergrondse coördinatie en veiliger navigatie op de zwarte markt mogelijk maakt.

Verdediging tegen collusie. Patronen van wederzijdse onderschrijving binnen gesloten groepen zijn detecteerbaar via analyse van de sociale grafiek. Reputatie-aggregatiefuncties verdisconteren beweringen uit sterk geclusterde bronnen.

Tegenstander op statelijk niveau. Onion-routing, de afwezigheid van gecentraliseerde infrastructuur en de verdeling van de rol van Verifieerder over de deelnemersbasis waarborgen dat onderdrukking maatregelen vereist die niet in verhouding staan tot enig voordeel.

Privacy tegenover verantwoording. Pseudonimiteit—een tussenweg tussen anonimiteit en identiteitsonthulling—stelt DID's in staat betekenisvolle reputatie op te bouwen zonder de reële identiteit van de Houder te onthullen.

11 Privacyoverwegingen

Het privacy-model van het RSN is gebouwd op pseudonimiteit. De Houder bepaalt de openbaarmaking van identiteit: minimaal (zuiver pseudoniem), selectief (specifieke referenties gekoppeld) of volledig (wettelijke identiteit gekoppeld). Gepubliceerde beweringen zijn permanent—het systeem ondersteunt contextuele correctie maar geen wissing. Een Houder mag een gecompromitteerde DID opgeven en opnieuw beginnen, waarbij hij de opgebouwde reputatie prijsgeeft.

12 Verwant werk

De W3C DID Core-specificatie [2] en het Ceramic Network [8] bieden de identiteitsbasis. Eigen-Trust [13] demonstreerde gedistribueerde reputatie-aggregatie zonder centrale autoriteit. SBTs [3] introduceerden niet-overdraagbare sociale tokens. Het RSN onderscheidt zich door de nadruk op economische kosten als kwaliteitsfilter en door zijn mechanisme voor het beprizen van radicalisme.

DAO's [4] en quadratic voting [5] toonden de haalbaarheid van gedecentraliseerd bestuur aan. Het RSN leidt consensus af uit bilaterale prijsonderhandelingen in plaats van uit stemmen.

Het voorstel bouwt voort op de anarcho-kapitalistische theorie [14, 15] voor private dienstverlening, maar wijkt op twee cruciale punten af: het ontwerpt voor wrok en vergeldende impulsen in plaats van rationaliteit aan te nemen, en het stelt een geleidelijke overgang voor in plaats van revolutie. Het concept van emergente sociale contracten heeft voorlopers in Hayeks theorie van de spontane orde [16].

Anarcho-aporisme. Het RSN deelt aanzienlijke gemeenschappelijke grond met de agoristische counter-economie [17]—in het bijzonder de nadruk op het opbouwen van parallelle instellingen en vrijwillige uitwisseling. Het agorisme neemt echter doorgaans rationeel eigenbelang aan als een toereikend coördinatiemechanisme en mist vaak een concreet migratiepad vanuit bestaande staatsstructuren. Het RSN verwerkt expliciet niet-rationele gedragsneigingen en biedt een fiscaal drukmechanisme voor een geleidelijke overgang.

Meritocratie. Het RSN vormt wellicht een eerste functionele beschrijving van hoe meritocratie [18] kan ontstaan als een systemische eigenschap in plaats van een slogan. Traditionele meritocratische systemen falen omdat ze een centrale autoriteit vereisen om “verdienste” te definiëren en af te dwingen. In het RSN ontstaat verdienste uit bilaterale evaluaties: wie waarde levert, bouwt reputatie op; geen enkele commissie beslist wie verdienste heeft.

Eigendom als privilege. Het RSN wijkt fundamenteel af van de anarcho-kapitalistische en Oostenrijkse-school-behandelingen van eigendomsrechten als natuurlijk en absoluut. In het RSN-raamwerk is eigendom een *privilege*—een maatschappelijke erkenning die in extreme gevallen door de gemeenschap kan worden ingetrokken wanneer een deelnemer gedeelde normen fundamenteel schendt (verraad, weigering de gemeenschap te verdedigen in een existentiële crisis, systematische uitbuiting). Dit is geen onteigening door de staat, maar een intrekking van maatschappelijke erkenning door het netwerk van bilaterale relaties.

13 Discussie en beperkingen

Koude start. De waarde van het RSN hangt af van netwerkeffecten; vroege gebruikers krijgen beperkte waarde totdat de deelname een drempel bereikt. Toch dient het DID-netwerk zelfs vanaf de vroege stadia als een nuttige aanvullende informatiebron. Verwacht wordt dat vroege reputatie-evaluatie en autoriteitsbeoordeling zich geleidelijk zullen ontwikkelen met toen-

emende verfijning.

Anti-leeching en toegangscontrole. Doel-DIDs mogen gegradeerde vergoedingen en toegangsbeperkingen opleggen aan vragen van DIDs met een lage reputatie. Dit is niet binair maar een continue schaal: hoe minder reputatie een vragende DID heeft, hoe minder informatie ze ontvangt, hoe langer ze wacht en hoe meer ze betaalt. Dit mechanisme stimuleert echte deelname boven passieve consumptie.

Ongelijkheid van toegang. De kosten van het publiceren van beweringen kunnen legitieme grieven van economisch achtergestelde deelnemers wegfilteren. Verzachting: elke deelnemer dient tegelijkertijd als potentiële verifieerder (of delegeert deze rol) en verdient verificatievergoedingen. Over een voldoende lange tijdshorizon zou een niet-radical deelnemer financiële neutraliteit moeten benaderen—waarbij de verificatie-inkomsten de publicatiekosten ongeveer compenseren. Dit is een statistische verwachting, geen garantie.

Reputatieongelijkheid. Vroege gebruikers vergaren voordelen die drempels kunnen opwerpen voor latecomers. Reputatie-evaluatie wordt echter uitgevoerd door externe aanbieders die ervoor kunnen kiezen het voordeel van de eerste zet te verzachten via hun aggregatie-algoritmes. Als eerste een goede reputatie hebben is een legitiem vergelijkend economisch voordeel—en dat is opzettelijk zo.

Open vragen. Optimale kostenfuncties, aggregatiestandaarden, protocolbestuur en de interactie met door AI gegenereerde synthetische reputatiegegevens blijven gebieden voor toekomstig werk.

Dit artikel beweert niet dat het RSN in alle omstandigheden optimale uitkomsten zal opleveren. Het beweert dat het RSN een *haalbaar* alternatief vormt—technisch implementeerbaar, economisch zelfvoorzienend en sociaal verenigbaar met menselijke gedragsneigingen zoals die werkelijk zijn.

14 Conclusie

Dit artikel heeft het Reputatie Sociaal Netwerk gepresenteerd, een gedecentraliseerd protocol dat pseudonieme, verifieerbare reputatie-uitwisseling mogelijk maakt. Het principe van duur radicalisme waarborgt dat frauduleuze beweringen uit de markt worden geprijsd zonder censuur. Het voorgestelde migratiepad maakt een geleidelijke, omkeerbare overgang vanuit bestaande instellingen mogelijk. Het ontwerp verwerkt de menselijke natuur zoals die is—inclusief kleingeestigheid, wrok en het verlangen naar

vergeldende genoegdoening—in plaats van een ideologische transformatie te vereisen. Het resultaat is geen utopie, maar een systeem waarin rechtvaardigheid toegankelijk is, reputatie wordt verdiend en de kosten van wangedrag worden gedragen door de partij die het veroorzaakte.

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.