Desentralisert omdømmenettverk: Et rammeverk for naturlig samfunnsorganisering

Pavel Kudrna
Prague, Czechia
Utkast v1 — mars 2026

Abstract

Rettferdighetssansen—overbevisningen om at urett blir rettet opp og at fortjeneste blir belønnet—er samfunnets sterkeste samlende kraft. Når sentraliserte styringsinstitusjoner ikke kan levere denne følelsen fordi kostnaden ved å håndheve en rettighet overstiger verdien av rettigheten selv, forvitrer den sosiale samholdet. Nåværende institusjonelle strukturer klarer ikke å løse en betydelig klasse av tvister på systematisk samme måte som sentral planlegging svikter i å fordele ressurser: gjennom informasjonsasymmetri, manglende tilbakekoblingssløyfer og frakobling av beslutningstakere fra konsekvensene av sine beslutninger. Denne artikkelen presenterer et omdømmebasert sosialt nettverk (Reputation Social Network, RSN): et desentralisert, ubestikkelig og sensurbestandig kommunikasjonslag bygget på desentraliserte identifikatorer (DID-er) som gjør det mulig for pseudonyme deltakere å publisere, verifisere og konsumere omdømmeinformasjon om atferd i den virkelige verden. Kjernemekanismen hviler på tre designprinsipper: (1) en asymmetrisk kostnadsstruktur der lesing av omdømmedata er billig, men skriving krever verifiserbar innsats; (2) en ikke-deterministisk protokoll for valg av verifikatorer basert på konsistent hashing som priser radikale påstander gjennom eskalerende iterasjonskostnader; og (3) en markedsdrevet modell for omdømmeautoriteter der private verifikatorer setter sitt akkumulerte omdømme på spill for nøyaktigheten av påstandene de bekrefter. Den resulterende arkitekturen frembringer et emergent meritokrati uten sentral koordinering og muliggjør en gradvis, reverserbar migreringsvei fra eksisterende statsadministrerte systemer.

1 Innledning

1.1 Problemet med sentralisert tillit

Moderne styring hviler på en grunnleggende antakelse: at sentraliserte institusjoner kan formidle tillit mellom fremmede i stor skala. Domstoler avgjør tvister. Registre sertifiserer eierskap. Tilsynsorganer håndhever standarder. Disse institusjonene ble utformet i en tid da informasjon var knapp, kommunikasjon var langsom, og delegering av myndighet til et sentralt organ var den eneste gjennomførbare koordineringsmekanismen. Sentralisert styring svikter imidlertid av de samme strukturelle grunnene som sentral planlegging: informasjonsasymmetri, manglende tilbakekoblingssløyfer og frakobling av beslutningstakere fra konsekvensene av sine beslutninger.

Antakelsen svikter for eksempel når kostnaden ved institusjonell formidling overstiger verdien av tvisten. Tenk på en leietaker som oppdager at den leide leiligheten mangler et lovpålagt elektrisk sikkerhetssertifikat—en tilstand som utgjør en umiddelbar livsfare. Leietakerens juridiske rett til å trekke seg fra kontrakten er utvetydig. Likevel overstiger kostnaden ved å håndheve denne rettigheten gjennom rettssystemet den pengemessige verdien av depositumet og erstatningen som skyldes, selv om man inkluderer potensiell lovbestemt kompensasjon [1]. Den rasjonelle responsen er å bære tapet og trekke seg ut.

Dette er ikke et patologisk grensetilfelle. Det er standarderfaringen for en betydelig klasse av tvister der skaden er reell, men de pengemessige innsatsene faller under terskelen der institusjonell håndheving blir økonomisk rasjonell. Resultatet er et system som strukturelt favoriserer aktører med onde hensikter: de som skader andre i volumer under denne terskelen kan handle ustraffet, fordi kostnaden ved å søke rettferdighet faller på den skadelidte parten.

Eksempelet ovenfor er hentet fra forfatterens juridiske miljø—det tsjekkiske sivilrettssystemet. I

andre rettstradisjoner—presedensbasert sedvanerett (common law), sedvanerett, blandede systemer—svikter rettferdigheten på ulike måter og i ulik grad, avhengig av de kulturelle og prosessuelle særtrekkene ved jurisdiksjonen. Lesere vil sannsynligvis kjenne igjen tilsvarende eksempler fra sin egen kontekst. Det som er strukturelt universelt, er mønsteret: tvister hvis verdi faller under terskelen for økonomisk rasjonell håndheving ender med at tapet bæres av den skadelidte parten. RSN lover ikke perfekt rettferdighet—den reduserer bare den strukturelle fordelen som aktører med onde hensikter nyter godt av når institusjonell håndheving er ulønnsom.

1.2 Hvorfor eksisterende løsninger kommer til kort

Rammeverk for desentralisert identitet (DID) [2] tilbyr kryptografiske mekanismer for selvsuveren identitetsforvaltning, men fokuserer primært på identitetsverifisering uten å adressere det bredere spørsmålet om atferdsmessig omdømme.

Soulbound-token (SBT-er) [3] fanger innsikten om at omdømme er ikke-overførbart, men er avhengige av blokkjede-infrastruktur med skaleringsbegrensninger og adresserer ikke de økonomiske insentivene som styrer informasjonsinngang. Beslektede konsepter som fortjenestetoken (f.eks. Liberland) deler en lignende filosofi, men forblir bundet til spesifikke jurisdiksjonelle rammeverk.

Desentraliserte autonome organisasjoner (DAO-er) [4] implementerer styring gjennom smartkontrakter, men reproduserer plutokratiske dynamikker der innflytelse er proporsjonal med kapital. Kvadratisk stemmegivning [5] demper dette delvis, men begrenser praktisk adopsjon. DAO-er står også overfor det grunnleggende *orakelproblemet*: smartkontrakter kan ikke pålitelig verifisere tilstander i den virkelige verden uten en pålitelig ekstern kilde, og dette problemet har ingen generell løsning innenfor blokkjedearkitektur.

Ingen eksisterende system kombinerer desentralisering, sensurbestandighet, pseudonymitet, verifiserbar inngangskostnad og emergent konsensus.

1.3 Bidrag

Denne artikkelen gir følgende bidrag:

1. Definisjon av **omdømmebasert sosialt nettverk (RSN)**, en desentralisert protokoll som utvider DID-rammeverket til å støtte bilateral omdømmeutveksling.
2. En **ikke-deterministisk protokoll for valg av verifikatorer** basert på konsistent hashing [6].
3. **Prinsippet om kostbar radikalisme**, som priser påstander etter deres avstand fra nettverkskonsensus gjennom tre sammensatte kostnadskanaler.
4. En **modell for anerkjente autoriteter** med asymmetriske insentiver der falsk bekreftelse koster katastrofalt mye mer enn legitime gebyrer.
5. En **gradvis migreringsvei** gjennom parallell finanspolitisk infrastruktur.

2 Designprinsipper

RSN-arkitekturen er begrenset av fem ikke-forhandlingsbare designprinsipper.

Kontinuitet og evolusjon. Systemet eksisterer side om side med eksisterende institusjoner i en overgangsperiode av ubestemt lengde. Overgangen må være reverserbar på hvert trinn.

Frivillighet og ansvar. Deltakelse er frivillig, men frivilligheten er koblet til ansvar: en deltaker som tar kontroll over en institusjonell funksjon, påtar seg samtidig de tilhørende forpliktelsene.

Mangfold og kulturell nøytralitet. Konsensus oppstår fra bilaterale interaksjoner, ikke fra forhåndsdefinerte regler pålagt av systemdesignere.

Robusthet og sensurbestandighet. Kostnaden ved å sensurere nettverket må overstige kostnaden ved å tolerere det. Kun fullstendig totalitarisme—til ruinerende politiske og økonomiske kostnader—kan undertrykke systemet.

Konsensus og håndheving. Systemet innlemmer menneskelige tilbøyeligheter til smålighet, ondskap og gjengjeldende tilfredsstillelse som bærende egenskaper. Uredelighet er ikke forbudt; den prises.

3 Systemoversikt

3.1 Omdømmebasert sosialt nettverk

RSN er et desentralisert kommunikasjonslag av typen node-til-node (peer-to-peer) der deltakere utveksler verifiserbar informasjon om atferd i den virkelige verden. Dets definerende egenskaper er: desentralisert og usensurerbar infrastruktur; pseudonym deltakelse gjennom DID-er; asymmetrisk kostnadsstruktur (lesing er billig, skriving er kostbar); kryptografisk verifiserbarhet; og **standardstøtte**—maskinlesbare formater for informasjon som spres gjennom nettverket, for tjenester tilbudt av autoriteter (sammensetning av påstander, bekreftelse, vitnetjeneste), og for policy-

formatet inkludert regler for evaluering av motpartens omdømme og vurdering av risikoen for policy-avvik (mellom erklært og faktisk atferd).

3.2 Arkitektoniske komponenter

RSN består av fire primære komponenter (Fig. 1):

1. **DID-lag.** Deltakeridentiteter med erklærte regler, omdømmemetadata og nettverksruting.
2. **Påstandsprotokoll.** Strukturert format for å publisere utsagn om hendelser i den virkelige verden.
3. **Verifikasjonsnettverk.** Desentralisert protokoll for å tildele verifikatorer ved hjelp av konsistent hashing.
4. **Aggregeringslag for omdømme.** Tjenester som produserer menneskelesbare omdømmesammendrag.

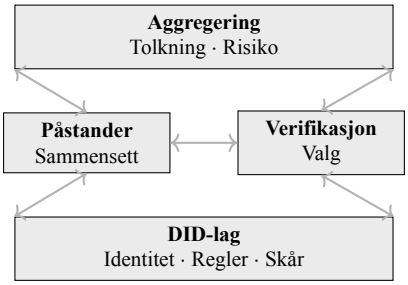

Figure 1: RSN firelags arkitektur.

3.3 Deltakerroller

En verifikasjonstransaksjon involverer opptil seks distinkte DID-roller (Fig. 2): **Utsteder** (DID_I, oppretter og sender inn påstanden), **Subjekt** (DID_S, DID-en påstanden handler om—kan sammenfalle med Utsteder), **Autoritet** (DID_A, bekrefter påstanden mot et gebyr; kan også tilby vitnetjenester—*valgfritt*), **Vitne** ($DID_{W_{1..n}}$, inkognito overvåker av verifikatorens ærlighet via utfordringskoder—*valgfritt*), **Verifikator** (DID_V, algoritmisk valgt til å publisere påstanden), og **RSN** (nettverket der verifiserte påstander publiseres). Enhver rolle kan delegeres til en annen DID (avsnitt 7.4). En Autoritet bunter vanligvis sammen bekreftelse med vitnetjenester, men de to funksjonene er logisk uavhengige.

3.4 Ubestikkelighet: Fire krefter

RSN-ets ubestikkelighet oppstår ikke fra en enkelt mekanisme, men fra fire samtidige krefter. Ingen er tilstrekkelig i seg selv; bare deres kombinasjon gjør et korrupsjonsforsøk økonomisk irrasjonelt.

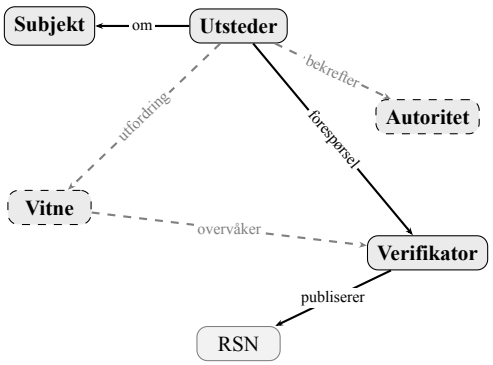

Figure 2: DID-roller i en verifikasjonstransaksjon. Stiplet = valgfritt (Autoritet, Vitne).

Uforutsigbart mål. Verifikatoren for hver påstand velges ikke-deterministisk gjennom konsistent hashing (avsnitt 5.3). En angriper kan ikke på forhånd sikte seg inn på en spesifikk verifikator for bestikkelse, fordi verifikatorens identitet er en funksjon av påstandens innhold og tidligere iterasjoner, ikke av utstederens valg.

Omdømmemessig innflytelse—langsomt opp, raskt ned. Omdømme kan bare bygges gradvis, gjennom vedvarende konsistent atferd. Det kan imidlertid gå tapt katastrofalt i en enkelt svindelaktig bekreftelse (avsnitt 6.2). Denne asymmetrien betyr at år med akkumulert omdømme kan ødelegges av én uærlig bekreftelse; den optimale strategien forblir å avvise mistenkelige påstander.

Offentlig løfte. Hver DID-innehaver erklærer offentlig sin policy—et maskinlesbart sett med regler de forplikter seg til å følge. Avvik mellom erklæringen og faktisk atferd er oppdagbart og prises som en omdømmeforseelse mer alvorlig enn den underliggende overtredelsen (avsnitt 7.3). Hykleri er derfor mer kostbart enn direkte uærlighet.

Nettverksmessig asymmetri i angrepskostnad. Kostnaden ved å sensurere eller destabilisere nettverket vokser ikke-lineært med nettverkets størrelse og tetthet, mens kostnaden ved å tolerere det forblir konstant. For at sensur skal lønne seg, måtte en sentralisert aktør anvende den på tvers av hele nettverket—noe som krever tiltak uproporsjonale med enhver tenkelig fordel (avsnitt 10).

4 Modell for desentralisert identitet

4.1 DID med spesielle egenskaper

RSN utvider W3C DID Core-spesifikasjonen [2] med: **Erklærte regler** (maskinlesbare atferdsforpliktelser), **Omdømmemetadata** (aggregert atferdsskår) og

Nettverksruting (foranderlig onion-gateway atskilt fra den stabile ringposisjonen).

4.2 Påstandens livssyklus

En påstand går gjennom seks stadier (Fig. 3): sammensetning, valgfri autoritetsbekreftelse, valg av verifikator via konsistent hashing, verifikasjonsbeslutning (godta eller avvis med iterasjon), publisering og omdømmeoppdatering for alle parter.

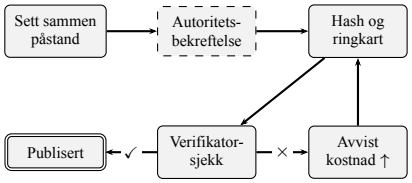

Figure 3: Påstandens livssyklus med iterasjonssløyfe.

4.3 Forhold til W3C DID Core

RSN-ets identitetsmodell er et ekte supersett av W3C DID Core-spesifikasjonen [2]. Alle RSN DID-er er gyldige W3C DID-er. De RSN-spesifikke utvidelsene er kodet som egenskaper i DID-dokumentet, definert i en dedikert DID-metodespesifikasjon, kompatibel med eksisterende infrastruktur som ION [7] og Ceramic [8].

5 Verifisering og spredning av informasjon

5.1 Kostnaden ved informasjonsinngang

RSN-ets økonomiske kjerneprinsipp er asymmetrien mellom lesing og skriving. Lesing av omdømmedata nærmer seg null marginalkostnad for deltakere som er en del av DID-nettverket og har tilgang som står i forhold til sitt omdømme—nykommere må gradvis fortjene bredere tilgang (se anti-snylting). Skriving—forstått som den varige materialiseringen av omdømme inn i nettverket, ikke som en engangs teknisk handling—krever verifiserbar kumulativ investering på tvers av tre dimensjoner: **tid** (leveår brukt på konsistent atferd, oppfylte forpliktelser og kultiverte relasjoner), **energi** (innsats lagt i ærlig handel, omsorg for partnerskap og langsiktig troverdighet), og **penger** (investering i eget navn—faglig utvikling, kvaliteten på ens arbeid, gjenoppretting av forvoldte skader). Omdømme kan ikke kjøpes umiddelbart—det er resultatet av livslang akkumulering som systemet bare gjør synlig og overførbart på tvers av kontekster. De teknisk engangskostnadene ved protokollen (kryptografiske signaturer, verifikatorgebyrer) er ubetydelige sammenlignet med denne underliggende investeringen.

5.2 Sosial graf og kontaktdybde

RSN er fundamentalt et sosialt nettverk: hver DID legger til kontakter (andre DID-er) som tillater forbindelsen. Disse kontaktene har sine egne kontakter, og så videre. Det algoritmiske søket etter verifikatorer opererer innenfor en konfigurerbar dybde h av tilknyttede kontakter (f.eks. $h = 3$: ens direkte kontakter, deres kontakter, og kontakters kontakter). Denne arkitekturen krever ikke en enkelt global blokkjede—den favoriserer naturlig fremveksten av fellesskap/klynger med overlapp inn i andre fellesskap. Hver DID-deltaker må ha en publisert **policy**—et maskinlesbart sett med regler som styrer hvordan innkommende forespørsler evalueres. Policybrudd registreres i nettverket som negative artefakter.

5.3 Algoritmisk valg av verifikator

Verifikasjonsprotokollen benytter konsistent hashing [6] (Fig. 4). Verifisering er en betalt tjeneste: verifikatorer opererer mot et gebyr, noe som skaper et marked der konkurranse driver prising, hastighet og pålitelighet.

Trinn 1. Påstandsdokumentet sammenkjedes med hashresultatet fra forrige iterasjon (eller $\varnothing$ ved første iterasjon) og hashes:

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

Algoritmen må inkludere den *fullstendige stien* av alle tidligere forespørsler og svar—ikke bare en hash av forrige iterasjon. Hver verifikators fullstendige svar (aksept, avvisning, oppgitt pris, begrunnelse) legges til det voksende dokumentet, verifiserbart gjennom kryptografiske signaturer i hvert trinn.

Trinn 2. Hashen kartlegges til N posisjoner på den konsistente hashringen, jevnt fordelt (f.eks. for $N = 4$: $+0°, +90°, +180°, +270°$). Fra hver posisjon velger et søk med klokken den nærmeste DID-en som verifikatorkandidat (Fig. 5). N er en variabel parameter som kan avhenge av prosentandelen av for øyeblikket aktive DID-er, tid på døgnet eller historisk nettverksrespons.

Trinn 3. Verifikatoren godtar (publiserer, setter omdømme på spill) eller avviser (returnerer til trinn 1 med avvisningshashen). Når en node ikke svarer til

tross for erklært tilkoblingsstatus, må neste forespørsel inkludere alle svar fra alle N tidligere verifikatorkandidater.

Anti-snylting. Mål-DID-er kan sette gebyrer eller tilgangsbegrensninger for spørringer fra nye DID-er med lite omdømme. Denne graderte mekanismen (ikke binær) tvinger nykommere til å bygge omdømme gjennom genuin aktivitet før de fritt kan konsumere andres data.

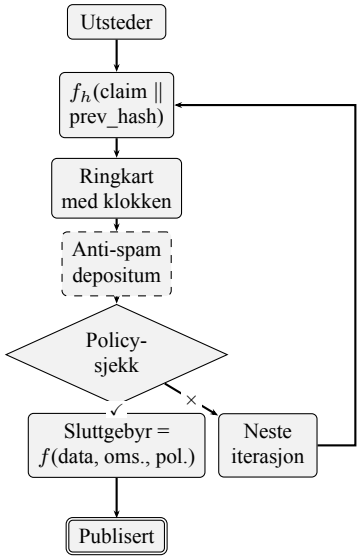

Figure 4: Protokoll for valg av verifikator. Anti-spam-depositum er valgfritt og kan være refunderbart. Sluttgebyret betales kun ved aksept.

Hver avvisning legger verifikatorens fullstendige svar (inkludert begrunnelser og betingelser) til påstandsdokumentet, og utvider dets innhold. Fra det utvidede dokumentet beregnes en ny hash ikke-deterministisk, som kartlegges til en annen ringposisjon og velger en annen verifikator. Dokumentasjon av den fullstendige stien er obligatorisk—utstederen kan ikke forutsi eller påvirke neste verifikator. Hvis en verifikator ignorerer en forespørsel til tross for en kompatibel erklært policy, registrerer vitner (hvis til stede) dette, og utstederen kan vedlegge vitnebevis ved endelig publisering.

5.4 Vitneprotokoll

Vitne-rollen gir inkognito ansvarliggjøring for verifikatorens ærlighet gjennom en kryptografisk protokoll med utfordringskoder:

Trinn V1. Forespørreren signerer verifikasjonsforespørselen og sender den til N_w vitner—kontakter fra forespørrerens sosiale nettverk, eller spesialiserte leverandører av vitnetjenester som opererer mot et gebyr.

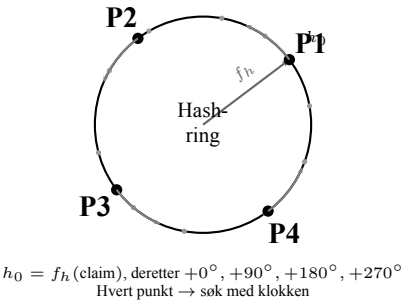

Figure 5: Flerpunktsvalg (N=4). Hash h_0 setter forskyvningen; 4 punkter jevnt fordelt fra h_0.

Trinn V2. Hvert vitne w_i signerer hele den signerte forespørselen, beholder den opprinnelige signaturen σ_i, og beregner en utfordringskode $c_i = h(\sigma_i)$. Utfordringskoden legges til forespørselen.

Trinn V3. Forespørselen, som nå bærer N_w utfordringskoder, sendes til verifikatoren. Verifikatoren observerer kodene, men *kan ikke fastslå* hvem vitnene er, eller om kodene tilsvarer reelle signaturer.

Trinn V4 (ærlig verifikator). Hvis verifikatoren svarer i tråd med sin erklærte policy, forblir utfordringskodene ugjennomsiktige. Vitner avsløres aldri. Ingen tilleggsdata publiseres.

Trinn V5 (policybrudd). Hvis verifikatoren bryter sin policy (ignorerer forespørselen, svarer inkonsekvent), holder forespørreren vitnenes opprinnelige signaturer σ_i. Disse kan publiseres som følgedata: hvem som helst kan verifisere $c_i = h(\sigma_i)$, og bevise at vitnet var til stede. Forespørreren kan publisere uavhengig—verifikatoren har allerede signert utfordringskodene i sitt svar.

Bløff-egenskapen. Forespørreren kan erstatte noen eller alle utfordringskoder med tilfeldige verdier. Verifikatoren kan ikke skille genuine koder (støttet av autoriteter med høyt omdømme) fra støy. Denne *usikkerheten* er håndhevingsmekanismen: hver forespørsel bærer risikoen for at en respektert autoritet ser på inkognito. Kostnaden ved å opprettholde dette presset er nær null (generering av tilfeldige tall), mens den potensielle kostnaden ved uærlighet for verifikatoren er katastrofal. Ærlig atferd insentiveres selv i fravær av faktiske vitner.

Autoritet som vitne. En Autoritet som bekrefter en påstand, kan bunte sammen vitnetjenester: "Jeg bekrefter din påstand og fungerer som inkognito vitne under verifiseringen." Dette er en naturlig forretningsmodell—Autoriteten har allerede konteksten. De to rollene er imidlertid logisk uavhengige.

5.5 Prinsippet om kostbar radikalisme

Tre kostnadskanaler sammensettes samtidig (Fig. 6):

Kanal 1: Iterasjonskostnad. Hver avvisning tvinger frem en ny iterasjon som forbruker tid og ressurser. Lineær vekst.

Kanal 2: Dokumentoppsvulming. Hver iterasjon legger verifikatorens fullstendige svar til påstandsdokumentet. Veksten er lineær, men med en basisforskyvning: den innledende nyttelasten (påstandsinnhold, autoritetsbekreftelse, kryptografiske signaturer) har allerede en ikke-triviell størrelse B_0. Total størrelse etter k iterasjoner: $S(k) = B_0 + k \cdot \Delta$, der Δ er gjennomsnittlig svarstørrelse.

Kanal 3: Verifikatorens risikopremie. Risiko er subjektiv. Verifikatoren vurderer om den forespørrende DID-ens erklærte policyer er i konflikt med verifikatorens egne kommersielle, sosiale eller politiske interesser. Premien kan eskalere eksponentielt med opplevd avstand fra verifikatorens "ideal": $P(d) = \alpha \cdot e^{\beta d}$, der d er verifikatorens subjektive avstandsmetrikk. Utover en personlig no-go-grense kan verifikatoren nekte fullstendig.

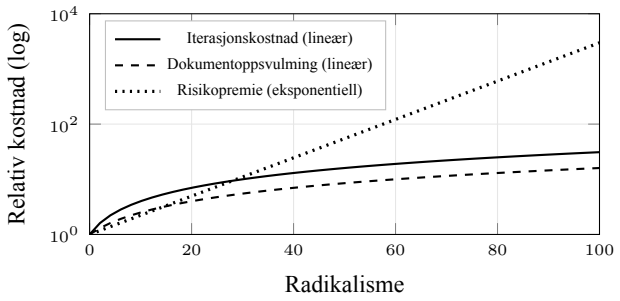

Figure 6: Kostnadseskalering på tvers av tre kanaler. Risikopremien dominerer ved høy radikalisme.

Kritisk nok er dette ikke sensur. Ingen påstand er forbudt. Systemet priser risiko (Tabell 1).

Table 1: Kostnadssammenligning på tvers av påstandstyper.

Type	Iter.	Dok	Gebyr	Total
Troverdig	k_{min}	B_0	P_{min}	Lav
Kontroversiell	k_{med}	$B_0 + k\Delta$	$\alpha e^{\beta d}$	Moderat
Radikal	k_{max}	$\gg B_0$	$\gg P_{\text{min}}$	Svært høy
Svindelaktig	$\to \infty$	—	—	Ikke publiserbar

6 Omdømme og risikovurdering

6.1 Modell for omdømmeakkumulering

Omdømme utviser tre egenskaper: **langsom akkumulering** (gradvis vekst gjennom konsistent atferd), **rask ødeleggelse** (en enkelt svindel kan redusere skåren katastrofalt), og **individuell evaluering** (hver konsumerende part kan anvende sin egen aggregeringsfunksjon).

6.2 Anerkjente autoriteter

En anerkjent autoritet vurderer påstander og, hvis tilfredsstilt, medsignerer dem—og setter sitt eget omdømme på spill (Fig. 7). Asymmetrien er tilsiktet: å bygge omdømme er langsomt (gradvis $+\delta$ per ærlig bekreftelse), mens å miste det er katastrofalt ($-\Delta \gg \delta$ per falsk bekreftelse; illustrerende, f.eks. $+2\%$ mot -70%). Den optimale strategien er alltid å avvise mistenkelige påstander. De spesifikke verdiene av δ og Δ er systemparametere.

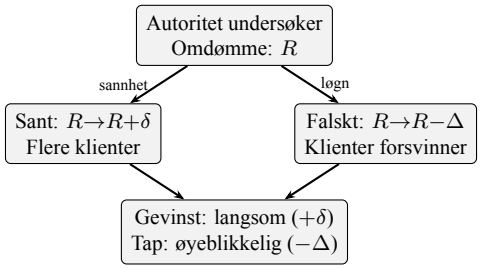

Figure 7: Anerkjent autoritet—asymmetriske insentiver.

6.3 Flerdimensjonalt omdømme

Omdømme er ikke en skalar, men en vektor på tvers av flere dimensjoner: økonomisk pålitelighet, personlig integritet, faglig kompetanse, samfunnsengasjement og andre (Fig. 8). Ulike evalueringsleverandører projiserer denne vektoren ulikt avhengig av kontekst—en långiver prioriterer økonomisk pålitelighet, en arbeidsgiver faglig kompetanse, en nabo samfunnsatferd. Det finnes ingen enkelt "korrekt" omdømmeskår; bare perspektiver.

6.4 Demokratisert risikovurdering

RSN demokratiserer systematisk risikovurdering—en kapabilitet som for øyeblikket er konsentrert i finansinstitusjoner, men anvendbar langt utover bankvirksomhet. Industrikonglomerater som vurderer leverandørpålitelighet, forsikringsselskaper som priser

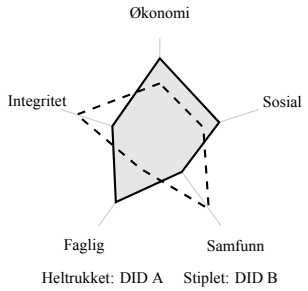

Figure 8: Flerdimensjonale omdømmevektorer. Ulike DID-er utviser ulike profiler på tvers av dimensjoner.

atferdsrisiko, aktsomhetsvurdering ved fusjoner og oppkjøp, estimering av utstyrs levetid i produksjon—hvor som helst motpartsrisiko krever vurdering, tilbyr RSN et desentralisert, markedsdrevet alternativ. Et marked av tolkningstjenester oversetter rå flerdimensjonale omdømmedata til handlingsrettede sammendrag, og gjør motpartsevaluering tilgjengelig for enhver deltaker til marginalkostnad.

7 Konsensus og tvisteløsning

7.1 Modell for desentralisert rettferdighet

RSN omformulerer rettferdighet som et bilateralt forhandlingsproblem. Trusselen om permanent, verifiserbar omdømmeskade er et mer effektivt avskrekkingsmiddel enn rettssaker den skadelidte parten ikke har råd til.

7.2 Emergent konsensus

Hver deltaker opprettholder en personlig tilfredshetsterskel. Nettverkets samlede konsensus oppstår som det statistiske gjennomsnittet av tusenvis av bilaterale forhandlinger (Fig. 9). En respons langt over konsensus (barbarisk) er kostbar å publisere. En respons nær konsensus (proporsjonal) er billig. Konsensus er ikke en regel—det er et prissignal.

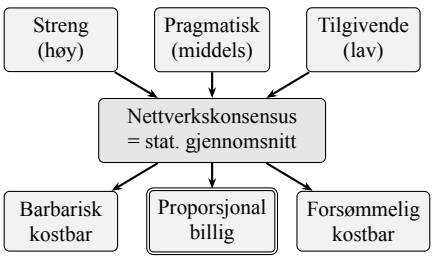

Figure 9: Emergent konsensus fra individuelle tilfredshetsterskler.

7.3 Kalibrering av straff

Hver DID-innehaver erklærer offentlig responser på spesifikke kategorier av uredelighet. Uforholdsmessig harde eller milde erklæringer tiltrekker seg negative omdømmesignaler. Proporsjonale erklæringer godtas uten friksjon—et selvkalibrerende straffesystem.

Konsensuserklæringer er selv underlagt hykleri-deteksjon: å deklarativt forplikte seg til en konsensusposisjon mens man oppfører seg inkonsekvent, utgjør en omdømmeforseelse mer alvorlig enn det underliggende avviket, ettersom det demonstrerer forsettlig bedrag.

7.4 Delegering

Alle aktiviteter innenfor en DID—med ett unntak—kan delegeres til en annen DID. **Subjekt-rollen—DID-en hvis atferd påstanden handler om—kan ikke delegeres; den er uoverførbart bundet til identitetsinnehaveren som påstanden refererer til.** De andre aktive rollene—Utsteder, Autoritet, Vitne, Verifikator—kan overføres til en utpekt delegat-DID, enten for verifisering, innsending av påstander, konsensusdeltakelse eller tvisteløsning. Delegering er tilbakekallelig når som helst. Dette muliggjør spesialisering (f.eks. profesjonelle verifikasjonstjenester) mens Innehaveren beholder den endelige kontrollen og ansvaret. Delegering gjelder på tvers av hele systemet og er avgjørende for skalerbarhet.

7.5 Fra individuell moral til emergent samfunnskontrakt

Hver DID-s erklærte policy representerer en formalisering av individuell moral: hva Innehaveren anser som akseptabelt, hvordan de responderer på spesifikke atferder, hva de krever av motparter. Disse policyene pålegges ikke av en systemdesigner—de velges av hver deltaker og uttrykkes i maskinlesbar form.

Denne formaliseringen muliggjør en trinnvis fremvekst. For det første kodes individuell moral som **policy**—et sett med erklærte regler, terskler og responsfunksjoner som DID-en forplikter seg til å følge. For det andre produserer summen av alle policyer på tvers av nettverket **emergent etikk**—statistisk observerbare normer som ingen enkelt deltaker utformet, men som oppstår fra interaksjonen mellom tusenvis av individuelle moralske posisjoner [9]. For det tredje utgjør denne emergente etikken, uttrykt som delte atferdsnormer håndhevet gjennom bilaterale prissignaler, en **målbar samfunnskontrakt**—ikke et teoretisk konstrukt som ingen signerte [10], men et

empirisk observerbart sett med regler støttet av faktisk atferd.

Denne prosessen speiler funn fra teorien om moralske grunnlag [11]: menneskelig moral er intuitiv, pluralistisk og kulturelt variabel. RSN krever ikke moralsk konsensus som en inngang; den produserer atferdskonsensus som en utgang. Den resulterende samfunnskontrakten er ikke statisk—den utvikler seg ettersom deltakere blir med, forlater og justerer sine policyer som respons på nettverkets tilbakemeldinger. I motsetning til klassisk samfunnskontraktsteori er denne kontrakten tilbakekallelig, observerbar og håndhevbar uten en suveren.

8 Økonomisk modell

De foregående avsnittene beskrev et verktøy—RSN-ets verifikasjonsmekanismer, kostnadsstruktur og emergente konsensus. Dette avsnittet beskriver en metodikk for å anvende dette verktøyet på finanspolitisk og styringsmessig overgang. Verktøyet er allsidig; metodikken nedenfor er én mulig anvendelse.

8.1 Insentivstruktur

Omdømme som kapital skaper direkte insentiver for ærlig atferd. I normal drift bygger deltakere omdømme naturlig gjennom dagligdagse transaksjoner og oppfylte forpliktelser. Den primære utgiften er på *negative* påstander—registrering av skade forvoldt av andre. Denne asymmetrien insentiverer nyttig, pålitelig atferd: å være ærlig koster ingenting ekstra, mens å være skadelig skaper et dokumentert spor som andre vil betale for å bevare. Hykleri—å erklære regler uten å følge dem—er den mest kostbare feilmodusen, ettersom det demonstrerer forsettlig bedrag.

8.2 Parallelt finanspolitisk system

Tre komponenter muliggjør konkurransepress: (1) **Enkel skatt**—en enkelt proporsjonal sats uten unntak, innledningsvis marginalt under den eksisterende effektive satsen; (2) **Elektronisk registrering av offentlige utgifter (ESR)**—en inversjon av den tsjekkiske EET-modellen slik at borgere overvåker statens utgifter; (3) **Borgerstyrt skattefordeling**—som starter på noen få prosent det første året og etter et tiår når alt fra lave tosifrede prosenter til en fullstendig migrering til et borgerstyrt system, avhengig av adopsjonstakten. Det faktiske tempoet avhenger av hastigheten hvormed frie markedsalternativer til statens tjenester oppstår, og av statens vilje til å samarbeide med overgangen; funksjonen av tid behøver ikke være lineær, og det er ingen grunn til å sette en øvre grense for hvor adopsjonen til slutt kan ende opp.

9 Migreringsvei

Migreringen forløper gjennom tre faser (Fig. 10): **Fase 1: Overlegg** (RSN som informasjonslag, staten er eneste tilbyder), **Fase 2: Konkurranse** (RSN tilbyr funksjonelle alternativer, bruk av dobbelt system), og **Fase 3: Overgang** (RSN overgår statlige ekvivalenter, frivillig migrering). Overgangen er reverserbar på hvert trinn.

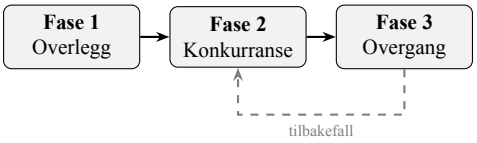

Figure 10: Trefaset migrering—reverserbar på hvert trinn.

Den primære pressmekanismen er finanspolitisk: når betingede skattebetalere når en "økonomisk signifikant minoritet X"—en gruppe stor nok til at undertrykkelse mot den forårsaker ikke-triviell økonomisk skade og sivil ulydighet blir en troverdig trussel—går staten inn i forhandling. Til illustrasjon bruker vi $X \approx 15\%$ av BNP, men den faktiske terskelen avhenger av den spesifikke økonomien.

10 Sikkerhetsanalyse

Vi vurderer fem kategorier av motstandere: individuelle aktører med onde hensikter, organiserte grupper, bedriftsmotstandere, statsnivå-motstandere og protokollnivå-motstandere.

Sybil-motstand [12]. Å bygge omdømme krever vedvarende, verifiserbar interaksjon. Kostnaden ved et vellykket Sybil-angrep skalerer lineært med falske identiteter og kvadratisk med målets omdømmenivå. Å drive flere DID-er parallelt er mulig, men kostbart ved design—hver identitet må uavhengig akkumulere omdømme gjennom genuin aktivitet. I frie samfunn avskrekker denne kostnaden tilfeldig misbruk; i diktaturer blir parallelle DID-er et overlevelsesverktøy som muliggjør kompartmentalisert motstand, underjordisk koordinering og tryggere navigering på svartebørsen.

Forsvar mot samarbeid. Mønstre av gjensidig bekreftelse blant lukkede grupper er oppdagbare gjen-

nom analyse av den sosiale grafen. Aggregeringsfunksjoner for omdømme nedvekter påstander fra tett klyngede kilder.

Statsnivå-motstander. Onion-ruting, fravær av sentralisert infrastruktur og fordeling av Verifikator-rollen på tvers av deltakerbasen sikrer at undertrykkelse krever tiltak uproporsjonale med enhver fordel.

Personvern kontra ansvarliggjøring. Pseudonymitet—en mellomting mellom anonymitet og identitetsavsløring—lar DID-er akkumulere meningsfullt omdømme uten å avsløre Innehaverens virkelige identitet.

11 Personvernhensyn

RSN-ets personvernmodell er bygget på pseudonymitet. Innehaveren kontrollerer identitetsavsløring: minimal (rent pseudonym), selektiv (spesifikke legitimasjoner koblet) eller full (juridisk identitet assosiert). Publiserte påstander er permanente—systemet støtter kontekstuell korrigering, men ikke sletting. En Innehaver kan forlate en kompromittert DID og begynne på nytt, og gir dermed avkall på akkumulert omdømme.

12 Relatert arbeid

W3C DID Core-spesifikasjonen [2] og Ceramic Network [8] gir identitetsgrunnlaget. EigenTrust [13] demonstrerte distribuert omdømmeaggregering uten sentral autoritet. SBT-er [3] introduserte ikke-overførbare sosiale token. RSN skiller seg i sin vektlegging av økonomisk kostnad som et kvalitetsfilter og sin mekanisme for prising av radikalisme.

DAO-er [4] og kvadratisk stemmegivning [5] demonstrerte gjennomførbarheten av desentralisert styring. RSN utleder konsensus fra bilaterale prisforhandlinger snarere enn fra stemmegivning.

Forslaget bygger på anarkokapitalistisk teori [14, 15] for privat tjenesteyting, men avviker på to kritiske punkter: det utformes for ondskap og gjengjeldende impulser snarere enn å anta rasjonalitet, og det foreslår gradvis overgang snarere enn revolusjon. Konseptet om emergente samfunnskontrakter har forløpere i Hayeks teori om spontan orden [16].

Anarko-agorisme. RSN deler betydelig felles grunn med agoristisk motøkonomi [17]—særlig vektleggingen av å bygge parallelle institusjoner og frivillig utveksling. Agorisme har imidlertid en tendens til å anta rasjonell egeninteresse som en tilstrekkelig koordineringsmekanisme og mangler ofte en konkret migreringsvei fra eksisterende statsstrukturer. RSN innlemmer eksplisitt ikke-rasjonelle atferdstilbøyeligheter og gir en finanspolitisk pressmekanisme for gradvis overgang.

Meritokrati. RSN kan representere en første funksjonell beskrivelse av hvordan meritokrati [18] kan oppstå som en systemisk egenskap snarere enn et slagord. Tradisjonelle meritokratiske systemer svikter fordi de krever en sentral autoritet for å definere og håndheve "fortjeneste". I RSN oppstår fortjeneste fra bilaterale evalueringer: de som leverer verdi, akkumulerer omdømme; ingen komité bestemmer hvem som har fortjeneste.

Eiendom som privilegium. RSN avviker fundamentalt fra anarkokapitalistiske og østerrikske skolens behandlinger av eiendomsrett som naturlig og absolutt. I RSN-rammeverket er eiendom et *privilegium*—en sosial anerkjennelse som i ekstreme tilfeller kan trekkes tilbake av fellesskapet når en deltaker fundamentalt bryter delte normer (svik, nektelse av å forsvare fellesskapet i en eksistensiell krise, systematisk utnyttelse). Dette er ikke statlig ekspropriasjon, men en tilbaketrekking av sosial anerkjennelse fra nettverket av bilaterale relasjoner.

13 Diskusjon og begrensninger

Kald start. RSN-ets verdi avhenger av nettverkseffekter; tidlige brukere står overfor begrenset verdi inntil deltakelsen når en terskel. Selv fra tidlige stadier tjener imidlertid DID-nettverket som en nyttig supplerende informasjonskilde. Tidlig omdømmeevaluering og autoritetsvurdering forventes å utvikle seg gradvis med økende sofistikering.

Anti-snylting og tilgangskontroll. Mål-DID-er kan pålegge graderte gebyrer og tilgangsbegrensninger på spørringer fra DID-er med lavt omdømme. Dette er ikke binært, men en kontinuerlig skala: jo mindre omdømme en spørrende DID har, desto mindre informasjon mottar den, desto lenger venter den, og desto mer betaler den. Denne mekanismen insentiverer genuin deltakelse fremfor passiv konsumering.

Ulikhet i tilgang. Kostnaden ved å publisere påstander kan filtrere bort legitime klager fra økonomisk vanskeligstilte deltakere. Avhjelping: hver deltaker fungerer samtidig som en potensiell verifikator (eller delegerer denne rollen) og tjener verifikasjonsgebyrer. Over en tilstrekkelig tidshorisont bør en ikke-radikal deltaker nærme seg finansiell nøytralitet—verifikasjonsinntekter oppveier omtrent publiseringskostnader. Dette er en statistisk forvent-

ning, ikke en garanti.

Ulikhet i omdømme. Tidlige brukere akkumulerer fordeler som kan skape barrierer for de som kommer senere. Omdømmeevaluering utføres imidlertid av tredjepartsleverandører som kan velge å dempe førsteinngangsfordelen gjennom sine aggregeringsalgoritmer. Å være først med et godt omdømme er en legitim komparativ økonomisk fordel—og det er ved design.

Åpne spørsmål. Optimale kostnadsfunksjoner, aggregeringsstandarder, protokollstyring og interaksjon med AI-generert syntetisk omdømmedata forblir områder for fremtidig arbeid.

Denne artikkelen hevder ikke at RSN vil produsere optimale utfall under alle omstendigheter. Den hevder at RSN representerer et *gjennomførbart* alternativ—teknisk implementerbart, økonomisk selvopprettholdende og sosialt kompatibelt med menneskelige atferdstilbøyeligheter slik de faktisk er.

14 Konklusjon

Denne artikkelen har presentert det omdømmebaserte sosiale nettverket, en desentralisert protokoll som muliggjør pseudonym, verifiserbar omdømmeutveksling. Prinsippet om kostbar radikalisme sikrer at svindelaktige påstander prises ut uten sensur. Den foreslåtte migreringsveien muliggjør gradvis, reverserbar overgang fra eksisterende institusjoner. Designet innlemmer menneskets natur slik den er—inkludert smålighet, ondskap og ønsket om gjengjeldende tilfredsstillelse—snarere enn å kreve ideologisk transformasjon. Resultatet er ikke utopi, men et system der rettferdighet er tilgjengelig, omdømme fortjenes, og kostnaden ved uredelighet bæres av den parten som forårsaket den.

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.