Decentraliserat ryktesnätverk: Ett ramverk för naturlig samhällsorganisation

Pavel Kudrna
Prague, Czechia
Draft v1 — March 2026

Abstract

Rättskänslan—övertygelsen om att oförrätter rättas till och att förtjänst belönas—är samhällets starkaste sammanhållande kraft. När centraliserade styrningsinstitutioner inte kan leverera denna känsla, eftersom kostnaden för att göra en rättighet gällande överstiger själva rättighetens värde, urholkas den sociala sammanhållningen. Nuvarande institutionella strukturer misslyckas med att lösa en betydande klass av tvister systematiskt på samma sätt som central planering misslyckas med att fördela resurser: genom informationsasymmetri, saknade återkopplingsslingor och avståndet mellan beslutsfattare och konsekvenserna av deras beslut. Denna uppsats presenterar ett ryktessocialt nätverk (RSN): ett decentraliserat, omutbart, censurresistent kommunikationslager byggt på decentraliserade identifierare (DID) som gör det möjligt för pseudonyma deltagare att publicera, verifiera och konsumera ryktesinformation om beteende i verkligheten. Kärnmekanismen vilar på tre designprinciper: (1) en asymmetrisk kostnadsstruktur där läsning av ryktesdata är billig men skrivande kräver verifierbar ansträngning; (2) ett ickedeterministiskt protokoll för val av verifierare baserat på konsekvent hashning som prissätter radikala påståenden genom eskalerande iterationskostnader; och (3) en marknadsdriven modell för ryktesauktoritet där privata verifierare satsar sitt ackumulerade rykte på riktigheten i de påståenden de stödjer. Den resulterande arkitekturen frambringar en emergent meritokrati utan central samordning och möjliggör en gradvis, reversibel migrationsväg från befintliga statligt administrerade system.

1 Inledning

1.1 Problemet med centraliserat förtroende

Modern styrning vilar på ett grundläggande antagande: att centraliserade institutioner kan förmedla förtroende mellan främlingar i stor skala. Domstolar avgör tvister. Register intygar ägande. Tillsynsorgan upprätthåller standarder. Dessa institutioner utformades i en tid då information var knapp, kommunikation var långsam och delegering av auktoritet till ett centralt organ var den enda genomförbara samordningsmekanismen. Centraliserad styrning misslyckas dock av samma strukturella skäl som central planering: informationsasymmetri, saknade återkopplingsslingor och avståndet mellan beslutsfattare och konsekvenserna av deras beslut.

Antagandet brister till exempel när kostnaden för institutionell förmedling överstiger tvistens värde. Betrakta en hyresgäst som upptäcker att den hyrda lägenheten saknar ett lagstadgat elsäkerhetsintyg—ett förhållande som utgör en omedelbar livsfara. Hyresgästens juridiska rätt att frånträda avtalet är otvetydig. Ändå överstiger kostnaden för att göra denna rätt gällande genom domstolssystemet det penningmässiga värdet av depositionen och det skadestånd som är skyldigt, även med potentiell lagstadgad ersättning inräknad [1]. Det rationella svaret är att bära förlusten och lämna.

Detta är inte ett patologiskt gränsfall. Det är standarderfarenheten för en betydande klass av tvister där skadan är verklig men de penningmässiga insatserna faller under tröskeln där institutionell verkställighet blir ekonomiskt rationell. Resultatet är ett system som strukturellt gynnar illasinnade aktörer: de som skadar andra i volymer under denna tröskel kan agera ostraffat, eftersom kostnaden för att söka rättvisa faller på den skadade parten.

Exemplet ovan är hämtat från författarens juridiska miljö—det tjeckiska civilrättssystemet. I andra rättstraditioner—prejudikatsbaserad sedvanerätt, sedvänjerätt, blandade system—misslyckas rättvisan på olika sätt och i olika grad, beroende på jurisdiktionens kulturella och processuella särdrag. Läsare kommer sannolikt att känna igen motsvarande exempel från sitt eget sammanhang. Det som är strukturellt universellt är mönstret: tvister vars värde faller under tröskeln för ekonomiskt rationell verkställighet slutar med att för-

lusten bärs av den skadade parten. RSN utlovar inte perfekt rättvisa—det minskar enbart den strukturella fördel som illasinnade aktörer åtnjuter när institutionell verkställighet är olönsam.

1.2 Varför befintliga lösningar inte räcker till

Ramverk för decentraliserad identitet (DID) [2] tillhandahåller kryptografiska mekanismer för självsuverän identitetshantering men fokuserar främst på identitetsverifiering utan att ta itu med den bredare frågan om beteenderykte.

Soulbound-token (SBT) [3] fångar insikten att rykte är icke-överförbart men förlitar sig på blockkedjeinfrastruktur med skalbarhetsbegränsningar och tar inte itu med de ekonomiska incitament som styr informationsinträdet. Relaterade koncept såsom förtjänsttoken (t.ex. Liberland) delar en liknande filosofi men förblir bundna till specifika jurisdiktionella ramverk.

Decentraliserade autonoma organisationer (DAO) [4] implementerar styrning genom smarta kontrakt men återskapar plutokratiska dynamiker där inflytandet är proportionellt mot kapital. Kvadratisk röstning [5] mildrar detta delvis men begränsar praktiskt införande. DAO:er står också inför det grundläggande *orakelproblemet*: smarta kontrakt kan inte tillförlitligt verifiera tillstånd i verkligheten utan en betrodd extern källa, och detta problem har ingen generell lösning inom blockkedjearkitektur.

Inget befintligt system kombinerar decentralisering, censurresistens, pseudonymitet, verifierbar inträdeskostnad och emergent konsensus.

1.3 Bidrag

Denna uppsats lämnar följande bidrag:

1. Definition av det **ryktes-sociala nätverket (RSN)**, ett decentraliserat protokoll som utvidgar DID-ramverket för att stödja bilateralt ryktesutbyte.
2. Ett **ickedeterministiskt protokoll för val av verifierare** baserat på konsekvent hashning [6].
3. **Principen om dyr radikalism**, som prissätter påståenden efter deras avstånd från nätverkskonsensus genom tre samverkande kostnadskanaler.
4. En **modell för renommerad auktoritet** med asymmetriska incitament där falskt godkännande kostar katastrofalt mycket mer än legitima avgifter.
5. En **gradvis migrationsväg** genom parallell fiskal infrastruktur.

2 Designprinciper

RSN-arkitekturen begränsas av fem icke förhandlingsbara designprinciper.

Kontinuitet och evolution. Systemet samexisterar med befintliga institutioner under en övergångsperiod av obestämd längd. Övergången måste vara reversibel i varje skede.

Frivillighet och ansvar. Deltagande är frivilligt, men frivilligheten är kopplad till ansvar: en deltagare som övertar kontrollen över en institutionell funktion övertar samtidigt de åtföljande skyldigheterna.

Mångfald och kulturell neutralitet. Konsensus uppstår ur bilaterala interaktioner, inte ur förutbestämda regler påtvingade av systemdesigners.

Motståndskraft och censurresistens. Kostnaden för att censurera nätverket måste överstiga kostnaden för att tolerera det. Endast full totalitarism—till ruinerande politisk och ekonomisk kostnad—kan undertrycka systemet.

Konsensus och verkställighet. Systemet införlivar mänskliga böjelser mot småaktighet, illvilja och hämndlysten tillfredsställelse som bärande egenskaper. Missförhållanden är inte förbjudna; de prissätts.

3 Systemöversikt

3.1 Ryktes-socialt nätverk

RSN är ett decentraliserat, peer-to-peer-kommunikationslager där deltagare utbyter verifierbar information om beteende i verkligheten. Dess definierande egenskaper är: decentraliserad och ocensurerbar infrastruktur; pseudonymt deltagande genom DID:er; asymmetrisk kostnadsstruktur (läsning är billig, skrivande är dyrt); kryptografisk verifierbarhet; och **standardstöd**—maskinläsbara format för information som sprids genom nätverket, för tjänster som erbjuds av auktoriteter (sammanställning av påståenden, godkännande, vittnestjänst), och för policyformatet inklusive regler för att bedöma motpartens rykte och risken för policyavvikelse (mellan deklarerat och faktiskt beteende).

3.2 Arkitekturkomponenter

RSN består av fyra huvudkomponenter (Fig. 1):

1. **DID-lager.** Deltagaridentiteter med deklarerade regler, ryktesmetadata och nätverksdirigering.
2. **Påståendeprotokoll.** Strukturerat format för att publicera utsagor om verkliga händelser.

3. **Verifieringsnätverk.** Decentraliserat protokoll för att tilldela verifierare med hjälp av konsekvent hashning.
4. **Ryktesaggregeringslager.** Tjänster som producerar mänskligt läsbara ryktessammanfattningar.

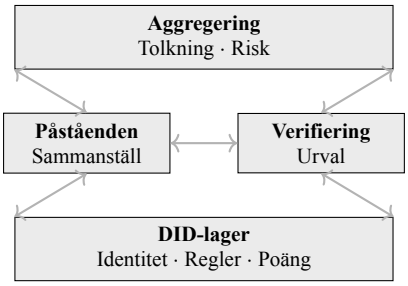

Figure 1: RSN:s fyrlagersarkitektur.

3.3 Deltagarroller

En verifieringstransaktion involverar upp till sex distinkta DID-roller (Fig. 2): **Utfärdare** (DID_I, skapar och lämnar in påståendet), **Subjekt** (DID_S, den DID som påståendet handlar om—kan sammanfalla med Utfärdaren), **Auktoritet** (DID_A, godkänner påståendet mot en avgift; kan även erbjuda vittnestjänster—*valfritt*), **Vittne** ($DID_{W_{1..n}}$, inkognitoövervakare av verifierarens ärlighet via utmaningskoder—*valfritt*), **Verifierare** (DID_V, algoritmiskt vald att publicera påståendet), och **RSN** (nätverket där verifierade påståenden publiceras). Vilken roll som helst kan delegeras till en annan DID (Avsnitt 7.4). En Auktoritet paketerar vanligtvis godkännande med vittnestjänster, men de två funktionerna är logiskt oberoende.

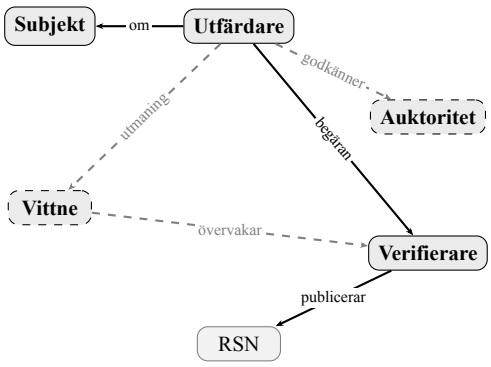

Figure 2: DID-roller i en verifieringstransaktion. Streckad = valfri (Auktoritet, Vittne).

3.4 Omutbarhet: fyra krafter

RSN:s omutbarhet uppstår inte ur en enda mekanism utan ur fyra samtidiga krafter. Ingen är tillräcklig ensam; endast deras kombination gör ett korruptionsförsök ekonomiskt irrationellt.

Oförutsägbart mål. Verifieraren för varje påstående väljs ickedeterministiskt genom konsekvent hashning (Avsnitt 5.3). En angripare kan inte i förväg rikta in sig på en specifik verifierare för mutor, eftersom verifierarens identitet är en funktion av påståendets innehåll och tidigare iterationer, inte av utfärdarens val.

Ryktesmässig hävstång—långsamt upp, snabbt ner. Rykte kan endast förvärvas stegvis, genom ihållande konsekvent beteende. Det kan dock förloras katastrofalt genom ett enda bedrägligt godkännande (Avsnitt 6.2). Denna asymmetri innebär att år av ackumulerat rykte kan förstöras av ett oärligt godkännande; den optimala strategin förblir att avvisa misstänkta påståenden.

Offentligt löfte. Varje DID-innehavare deklarerar offentligt sin policy—en maskinläsbar uppsättning regler som de förbinder sig att följa. Avvikelse mellan deklarationen och faktiskt beteende är upptäckbar och prissätts som en ryktesförseelse allvarligare än den underliggande överträdelsen (Avsnitt 7.3). Hyckleri är därför dyrare än direkt oärlighet.

Mesh-nätverkets asymmetriska angreppskostnad. Kostnaden för att censurera eller destabilisera nätverket växer icke-linjärt med nätverkets storlek och täthet, medan kostnaden för att tolerera det förblir konstant. För att censur ska löna sig skulle en centraliserad aktör behöva tillämpa den över hela nätverket—vilket kräver åtgärder oproportionerliga mot någon tänkbar nytta (Avsnitt 10).

4 Modell för decentraliserad identitet

4.1 DID med särskilda egenskaper

RSN utvidgar W3C:s DID Core-specifikation [2] med: **Deklarerade regler** (maskinläsbara beteendeåtaganden), **Ryktesmetadata** (aggregerad beteendepoäng), och **Nätverksdirigering** (föränderlig onion-gateway skild från den stabila ringpositionen).

4.2 Påståendets livscykel

Ett påstående fortskrider genom sex steg (Fig. 3): sammanställning, valfritt auktoritetsgodkännande, val av verifierare via konsekvent hashning, verifieringsbeslut (godkänn eller avvisa med iteration), publicering, och ryktesuppdatering för alla parter.

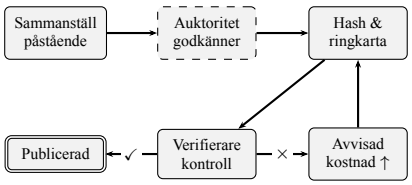

Figure 3: Påståendets livscykel med iterationsslinga.

4.3 Förhållande till W3C DID Core

RSN:s identitetsmodell är en äkta övermängd av W3C:s DID Core-specifikation [2]. Alla RSN-DID:er är giltiga W3C-DID:er. De RSN-specifika utvidgningarna kodas som egenskaper i DID-dokumentet, definierade i en särskild DID-metodspecifikation, kompatibel med befintlig infrastruktur såsom ION [7] och Ceramic [8].

5 Informationsverifiering och spridning

5.1 Kostnaden för informationsinträde

RSN:s centrala ekonomiska princip är asymmetrin mellan läsning och skrivande. Läsning av ryktesdata närmar sig noll marginalkostnad för deltagare som är del av DID-nätverket och har tillgång i nivå med sitt rykte—nykomlingar måste gradvis förtjäna bredare tillgång (se anti-snyltning). Skrivande—förstått som den varaktiga materialiseringen av rykte in i nätverket, inte som en engångsteknisk handling—kräver verifierbar kumulativ investering över tre dimensioner: **tid** (levnadsår ägnade åt konsekvent beteende, uppfyllda åtaganden och odlade relationer), **energi** (ansträngning nedlagd på ärlig handel, omsorg om partnerskap och långsiktig pålitlighet), och **pengar** (investering i det egna namnet—yrkesutveckling, kvaliteten på det egna arbetet, gottgörelse för orsakad skada). Rykte kan inte köpas omedelbart—det är resultatet av livslång ackumulering som systemet enbart gör synlig och överförbar mellan sammanhang. Protokollets engångstekniska kostnader (kryptografiska signaturer, verifieraravgifter) är försumbara jämfört med denna underliggande investering.

5.2 Social graf och kontaktdjup

RSN är i grunden ett socialt nätverk: varje DID lägger till kontakter (andra DID:er) som tillåter kopplingen. Dessa kontakter har sina egna kontakter, och så vidare. Den algoritmiska verifierarsökningen verkar inom ett konfigurerbart djup h av länkade kontakter (t.ex. $h = 3$: ens direkta kontakter, deras kontakter, och kontakternas kontakter). Denna arkitektur kräver inte en enda global blockkedja—den gynnar naturligt uppkomsten av gemenskaper/kluster med överlappningar in i andra gemenskaper. Varje DID-deltagare måste ha en publicerad **policy**—en maskinläsbar uppsättning regler som styr hur inkommande förfrågningar bedöms. Policyöverträdelser registreras i nätverket som negativa artefakter.

5.3 Algoritmiskt val av verifierare

Verifieringsprotokollet använder konsekvent hashning [6] (Fig. 4). Verifiering är en betald tjänst: verifierare arbetar mot en avgift, vilket skapar en marknad där konkurrens driver prissättning, hastighet och tillförlitlighet.

Steg 1. Påståendedokumentet sammanfogas med föregående iterations hashresultat (eller $\varnothing$ vid första iterationen) och hashas:

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

Algoritmen måste inkludera den *fullständiga vägen* av alla tidigare förfrågningar och svar—inte enbart en hash av föregående iteration. Varje verifierares fullständiga svar (godkännande, avslag, offererat pris, skäl) läggs till det växande dokumentet, verifierbart genom kryptografiska signaturer vid varje steg.

Steg 2. Hashen mappas till N positioner på den konsekventa hashringen, jämnt fördelade (t.ex. för $N = 4$: $+0°, +90°, +180°, +270°$). Från varje position väljer en medurs sökning den närmaste DID:en som verifierarkandidat (Fig. 5). N är en variabel parameter som kan bero på andelen för närvarande aktiva DID:er, tid på dygnet, eller nätverkets historiska svarsförmåga.

Steg 3. Verifieraren godkänner (publicerar, satsar rykte) eller avvisar (återgår till Steg 1 med avslagshashen). När en nod inte svarar trots att den deklarerar online-status måste nästa förfrågan inkludera alla svar från alla N tidigare verifierarkandidater.

Anti-snyltning. Mål-DID:er kan sätta avgifter eller åtkomstbegränsningar för förfrågningar från nya DID:er med litet rykte. Denna graderade mekanism (inte binär) tvingar nykomlingar att bygga rykte genom genuin aktivitet innan de fritt konsumerar andras data.

Varje avslag lägger till verifierarens fullständiga svar (inklusive skäl och villkor) till påståendedokumentet, vilket utökar dess innehåll. Från det utökade dokumentet beräknas ickedeterministiskt en ny hash, som mappas till en annan ringposition och väljer en annan verifierare. Dokumentation av hela vägen är obligatorisk—utfärdaren kan inte förutsäga eller

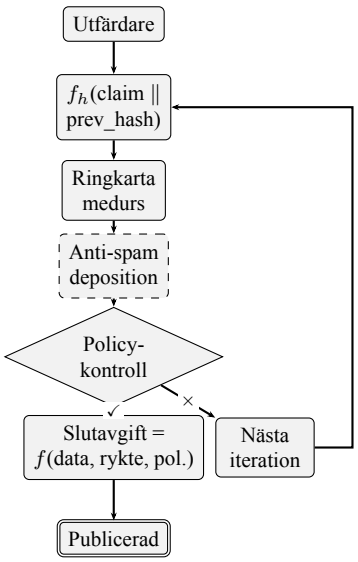

Figure 4: Protokoll för val av verifierare. Anti-spam-depositionen är valfri och kan vara återbetalbar. Slutavgiften betalas endast vid godkännande.

påverka nästa verifierare. Om en verifierare ignorerar en förfrågan trots en förenlig deklarerad policy registrerar vittnen (om de finns) detta, och utfärdaren kan bifoga vittnesbevis vid slutpublicering.

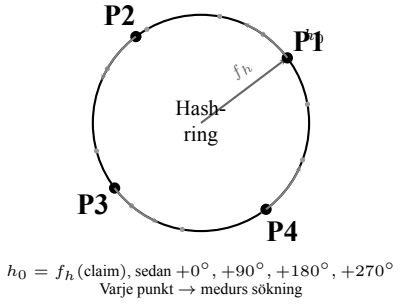

Figure 5: Flerpunktsval (N=4). Hashen h_0 sätter förskjutningen; 4 punkter jämnt fördelade från h_0.

5.4 Vittnesprotokoll

Vittnes-rollen ger inkognito-ansvarsutkrävande för verifierarens ärlighet genom ett kryptografiskt utmaningskodsprotokoll:

Steg W1. Den begärande signerar verifieringsförfrågan och skickar den till N_w vittnen—kontakter från den begärandes sociala nätverk, eller specialiserade leverantörer av vittnestjänster som verkar mot en avgift.

Steg W2. Varje vittne w_i signerar hela den signerade förfrågan, behåller originalsignaturen σ_i, och beräknar en utmaningskod $c_i = h(\sigma_i)$. Utmaningskoden läggs till förfrågan.

Steg W3. Förfrågan, som nu bär N_w utmaningskoder, skickas till verifieraren. Verifieraren observerar koderna men *kan inte avgöra* vilka vittnena är eller huruvida koderna motsvarar verkliga signaturer.

Steg W4 (ärlig verifierare). Om verifieraren svarar i enlighet med sin deklarerade policy förblir utmaningskoderna ogenomskinliga. Vittnen avslöjas aldrig. Ingen ytterligare data publiceras.

Steg W5 (policyöverträdelse). Om verifieraren bryter mot sin policy (ignorerar förfrågan, svarar inkonsekvent) innehar den begärande vittnenas originalsignaturer σ_i. Dessa kan publiceras som kompletterande data: vem som helst kan verifiera $c_i = h(\sigma_i)$, vilket bevisar att vittnet var närvarande. Den begärande kan publicera oberoende—verifieraren signerade redan utmaningskoderna i sitt svar.

Bluffegenskapen. Den begärande kan ersätta några eller alla utmaningskoder med slumpmässiga värden. Verifieraren kan inte skilja äkta koder (uppbackade av högt renommerade auktoriteter) från brus. Denna *osäkerhet* är verkställighetsmekanismen: varje förfrågan bär risken att en respekterad auktoritet iakttar inkognito. Kostnaden för att upprätthålla detta tryck är nära noll (att generera slumptal), medan den potentiella kostnaden av oärlighet för verifieraren är katastrofal. Ärligt beteende incitamenteras även i frånvaro av faktiska vittnen.

Auktoritet som vittne. En Auktoritet som godkänner ett påstående kan paketera vittnestjänster: "Jag godkänner ditt påstående och tjänar som inkognitovittne under verifieringen." Detta är en naturlig affärsmodell—Auktoriteten har redan sammanhanget. De två rollerna är dock logiskt oberoende.

5.5 Principen om dyr radikalism

Tre kostnadskanaler samverkar samtidigt (Fig. 6):

Kanal 1: Iterationskostnad. Varje avslag framtvingar en ny iteration som förbrukar tid och resurser. Linjär tillväxt.

Kanal 2: Dokumentuppsvällning. Varje iteration lägger till verifierarens fullständiga svar till påståendedokumentet. Tillväxten är linjär, men med en basförskjutning: den initiala nyttolasten (påståendets innehåll, auktoritetsgodkännande, kryptografiska signaturer) har redan en icke-trivial storlek B_0. Total storlek efter k iterationer: $S(k) = B_0 + k \cdot \Delta$, där Δ är den genomsnittliga svarsstorleken.

Kanal 3: Verifierarens riskpremie. Risk är subjektiv. Verifieraren bedömer huruvida den begärande DID:ens deklarerade policyer strider mot verifierarens egna kommersiella, sociala eller politiska intressen.

Premien kan eskalera exponentiellt med det upplevda avståndet från verifierarens "ideal": $P(d) = \alpha \cdot e^{\beta d}$, där d är verifierarens subjektiva avståndsmått. Bortom en personlig no-go-gräns kan verifieraren vägra helt.

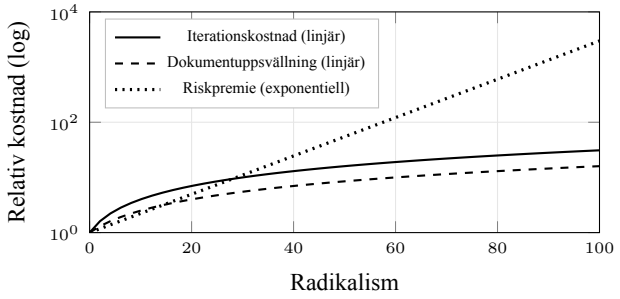

Figure 6: Kostnadseskalering över tre kanaler. Riskpremien dominerar vid hög radikalism.

Avgörande är att detta inte är censur. Inget påstående är förbjudet. Systemet prissätter risk (Tabell 1).

Table 1: Kostnadsjämförelse mellan påståendetyper.

Typ	Iter.	Dok	Avgift	Totalt
Trovärdig	$k_{\min}$	B_0	$P_{\min}$	Låg
Kontroversiell	k_{med}	$B_0 + k\Delta$	$\alpha e^{\beta d}$	Måttlig
Radikal	$k_{\max}$	$\gg B_0$	$\gg P_{\min}$	Mycket hög
Bedräglig	$\to \infty$	—	—	Opublicerbar

6 Rykte och riskbedömning

6.1 Modell för ryktesackumulering

Rykte uppvisar tre egenskaper: **långsam ackumulering** (stegvis tillväxt genom konsekvent beteende), **snabb förstörelse** (ett enda bedrägeri kan sänka poängen katastrofalt), och **individuell bedömning** (varje konsumerande part kan tillämpa sin egen aggregeringsfunktion).

6.2 Renommerade auktoriteter

En Renommerad Auktoritet granskar påståenden och, om den är tillfredsställd, medsignerar dem—och satsar sitt eget rykte (Fig. 7). Asymmetrin är avsiktlig: att vinna rykte är långsamt (stegvis $+\delta$ per ärligt godkännande), medan att förlora det är katastrofalt ($-\Delta \gg \delta$ per falskt godkännande; illustrativt t.ex. $+2\%$ mot -70%). Den optimala strategin är alltid att avvisa misstänkta påståenden. De specifika värdena på δ och Δ är systemparametrar.

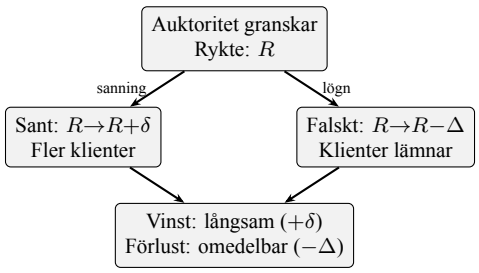

Figure 7: Renommerad Auktoritet—asymmetriska incitament.

6.3 Flerdimensionellt rykte

Rykte är inte en skalär utan en vektor över flera dimensioner: finansiell pålitlighet, personlig integritet, yrkeskompetens, samhällsengagemang, med flera (Fig. 8). Olika bedömningsleverantörer projicerar denna vektor olika beroende på sammanhang—en långivare prioriterar finansiell pålitlighet, en arbetsgivare yrkeskompetens, en granne samhällsbeteende. Det finns ingen enda "korrekt" ryktespoäng; endast perspektiv.

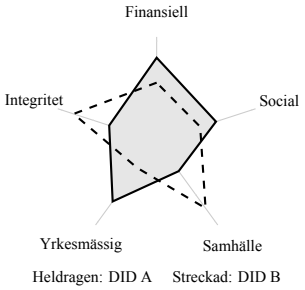

Figure 8: Flerdimensionella ryktesvektorer. Olika DID:er uppvisar olika profiler över dimensioner.

6.4 Demokratiserad riskbedömning

RSN demokratiserar systematisk riskbedömning—en förmåga som för närvarande är koncentrerad till finansinstitut men tillämpbar långt bortom bankväsendet. Industrikonglomerat som bedömer leverantörers tillförlitlighet, försäkringsbolag som prissätter beteenderisk, due diligence vid fusioner och förvärv, uppskattning av utrustnings livslängd inom tillverkning—överallt där motpartsrisk kräver bedömning tillhandahåller RSN ett decentraliserat, marknadsdrivet alternativ. En marknad av tolkningstjänster översätter rå flerdimensionell ryktesdata till användbara sammanfattningar, vilket gör motpartsbedömning tillgänglig för varje deltagare till marginalkostnad.

7 Konsensus och tvistlösning

7.1 Modell för decentraliserad rättvisa

RSN omformulerar rättvisa som ett bilateralt förhandlingsproblem. Hotet om permanent, verifierbar ryktesskada är ett effektivare avskräckningsmedel än rättsprocesser som den skadade parten inte har råd med.

7.2 Emergent konsensus

Varje deltagare upprätthåller en personlig tillfredsställelsetröskel. Nätverkets aggregerade konsensus uppstår som det statistiska genomsnittet av tusentals bilaterala förhandlingar (Fig. 9). Ett svar långt över konsensus (barbariskt) är dyrt att publicera. Ett svar nära konsensus (proportionellt) är billigt. Konsensus är inte en regel—det är en prissignal.

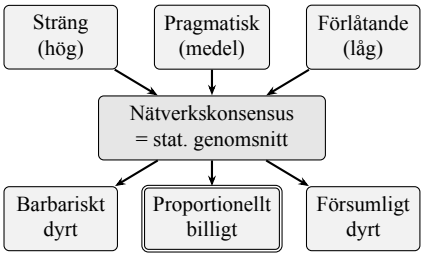

Figure 9: Emergent konsensus från individuella tillfredsställelsetrösklar.

7.3 Bestraffningskalibrering

Varje DID-innehavare deklarerar offentligt svar på specifika kategorier av missförhållanden. Oproportionerligt hårda eller milda deklarationer drar till sig negativa ryktessignaler. Proportionella deklarationer accepteras utan friktion—ett självkalibrerande bestraffningssystem.

Konsensusdeklarationer är själva föremål för hyckleridetektering: att deklarativt förbinda sig till en konsensusposition medan man beter sig inkonsekvent utgör en ryktesförseelse allvarligare än den underliggande avvikelsen, eftersom den påvisar avsiktligt bedrägeri.

7.4 Delegering

Alla aktiviteter inom en DID—med ett undantag—kan delegeras till en annan DID. **Subjektsrollen—den DID vars beteende påståendet handlar om—kan inte delegeras; den är icke-överförbart bunden till den identitetsinnehavare som påståendet refererar till.** De övriga aktiva rollerna—Utfärdare, Auktoritet, Vittne, Verifierare—kan överföras till en utsedd delegat-DID, vare sig för verifiering, inlämning av påståenden, konsensusdeltagande eller tvistlösning. Delegering är återkallelig när som helst. Detta möjliggör specialisering (t.ex. professionella verifieringstjänster) medan Innehavaren behåller den yttersta kontrollen och ansvaret. Delegering gäller över hela systemet och är väsentlig för skalbarhet.

7.5 Från individuell moral till emergent samhällskontrakt

Varje DID:s deklarerade policy representerar en formalisering av individuell moral: vad Innehavaren anser acceptabelt, hur de svarar på specifika beteenden, vad de kräver av motparter. Dessa policyer påtvingas inte av en systemdesigner—de väljs av varje deltagare och uttrycks i maskinläsbar form.

Denna formalisering möjliggör en emergens i tre steg. Först kodas individuell moral som **policy**—en uppsättning deklarerade regler, trösklar och svarsfunktioner som DID:en förbinder sig att följa. För det andra producerar summan av alla policyer över nätverket **emergent etik**—statistiskt observerbara normer som ingen enskild deltagare utformat men som uppstår ur interaktionen mellan tusentals individuella moraliska ståndpunkter [9]. För det tredje utgör denna emergenta etik, uttryckt som delade beteendenormer som upprätthålls genom bilaterala prissignaler, ett **mätbart samhällskontrakt**—inte en teoretisk konstruktion som ingen undertecknat [10], utan en empiriskt observerbar uppsättning regler uppbackad av faktiskt beteende.

Denna process speglar rön från teorin om moraliska grunder [11]: mänsklig moral är intuitiv, pluralistisk och kulturellt variabel. RSN kräver inte moralisk konsensus som indata; den producerar beteendekonsensus som utdata. Det resulterande samhällskontraktet är inte statiskt—det utvecklas allteftersom deltagare ansluter sig, lämnar och justerar sina policyer som svar på nätverksåterkoppling. Till skillnad från klassisk samhällskontraktsteori är detta kontrakt återkalleligt, observerbart och verkställbart utan en suverän.

8 Ekonomisk modell

De föregående avsnitten beskrev ett verktyg—RSN:s verifieringsmekanismer, kostnadsstruktur och emergenta konsensus. Detta avsnitt beskriver en metodik för att tillämpa detta verktyg på fiskal och styrningsmässig övergång. Verktyget är allmängiltigt;

metodiken nedan är en möjlig tillämpning.

8.1 Incitamentsstruktur

Rykte som kapital skapar direkta incitament för ärligt beteende. Vid normal drift bygger deltagare rykte naturligt genom vardagliga transaktioner och uppfyllda åtaganden. Den primära utgiften är på *negativa* påståenden—att registrera skada orsakad av andra. Denna asymmetri incitamenterar nyttigt, tillförlitligt beteende: att vara ärlig kostar inget extra, medan att vara skadlig skapar ett dokumenterat spår som andra kommer att betala för att bevara. Hyckleri—att deklarera regler utan att följa dem—är det dyraste felläget, eftersom det påvisar avsiktligt bedrägeri.

8.2 Parallellt fiskalt system

Tre komponenter möjliggör konkurrenstryck: (1) **Enkel skatt**—en enda proportionell sats utan undantag, inledningsvis marginellt under den befintliga effektiva satsen; (2) **Elektronisk utgiftsregistrering (ESR)**—som inverterar den tjeckiska EET-modellen så att medborgarna övervakar statliga utgifter; (3) **Medborgarstyrd skatteallokering**—som börjar på några få procent första året och når, efter ett decennium, allt från låga tvåsiffriga tal till en fullständig migration till ett medborgarstyrt system, beroende på införandetakten. Den faktiska takten beror på hur snabbt fri marknads alternativ till statliga tjänster uppstår och på statens vilja att samarbeta med övergången; tidsfunktionen behöver inte vara linjär, och det finns ingen anledning att sätta en övre gräns för var införandet slutligen kan hamna.

9 Migrationsväg

Migrationen fortskrider genom tre faser (Fig. 10): **Fas 1: Överlagring** (RSN som informationslager, staten är enda leverantör), **Fas 2: Konkurrens** (RSN tillhandahåller funktionella alternativ, användning av dubbla system), och **Fas 3: Övergång** (RSN överträffar statliga motsvarigheter, frivillig migration). Övergången är reversibel i varje skede.

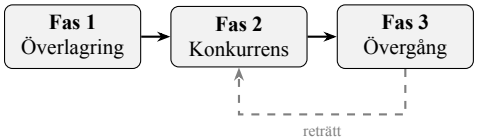

Figure 10: Migration i tre faser—reversibel i varje skede.

Den primära tryckmekanismen är fiskal: när villkorliga skattebetalare når en "ekonomiskt betydande minoritet X"—en grupp tillräckligt stor för att repression mot den orsakar icke-triviala ekonomiska skador och civil olydnad blir ett trovärdigt hot—inleder staten förhandling. För illustration använder vi $X \approx 15\%$ av BNP, men den faktiska tröskeln beror på den specifika ekonomin.

10 Säkerhetsanalys

Vi betraktar fem kategorier av motståndare: enskilda illasinnade aktörer, organiserade grupper, företagsmotståndare, motståndare på statsnivå, och motståndare på protokollnivå.

Sybil-resistens [12]. Att bygga rykte kräver ihållande, verifierbar interaktion. Kostnaden för en framgångsrik Sybil-attack skalar linjärt med falska identiteter och kvadratiskt med målets ryktesnivå. Att driva flera DID:er parallellt är möjligt men dyrt av design—varje identitet måste oberoende ackumulera rykte genom genuin aktivitet. I fria samhällen avskräcker denna kostnad tillfälligt missbruk; i diktaturer blir parallella DID:er ett överlevnadsverktyg som möjliggör uppdelat motstånd, underjordisk samordning och säkrare navigering på svarta marknaden.

Försvar mot maskopi. Mönster av ömsesidigt godkännande bland slutna grupper är upptäckbara genom analys av den sociala grafen. Ryktesaggregeringsfunktioner nedvärderar påståenden från tätt klustrade källor.

Motståndare på statsnivå. Onion-dirigering, avsaknaden av centraliserad infrastruktur, och fördelningen av Verifierarrollen över deltagarbasen säkerställer att undertryckande kräver åtgärder oproportionerliga mot någon nytta.

Integritet kontra ansvarsutkrävande. Pseudonymitet—en medelväg mellan anonymitet och identitetsavslöjande—tillåter DID:er att ackumulera meningsfullt rykte utan att avslöja Innehavarens verkliga identitet.

11 Integritetsöverväganden

RSN:s integritetsmodell är byggd på pseudonymitet. Innehavaren styr identitetsavslöjandet: minimalt (ren pseudonym), selektivt (specifika referenser länkade), eller fullständigt (juridisk identitet associerad). Publicerade påståenden är permanenta—systemet stödjer kontextuell korrigering men inte radering. En In-

nehavare kan överge en kompromitterad DID och börja på nytt, och förverkar då ackumulerat rykte.

12 Relaterat arbete

W3C:s DID Core-specifikation [2] och Ceramic Network [8] tillhandahåller identitetsgrunden. EigenTrust [13] demonstrerade distribuerad ryktesaggregering utan central auktoritet. SBT:er [3] introducerade icke-överförbara sociala token. RSN skiljer sig i sin betoning på ekonomisk kostnad som ett kvalitetsfilter och sin mekanism för att prissätta radikalism.

DAO:er [4] och kvadratisk röstning [5] demonstrerade genomförbarheten av decentraliserad styrning. RSN härleder konsensus från bilaterala prisförhandlingar snarare än röstning.

Förslaget bygger på anarkokapitalistisk teori [14, 15] för privat tjänsteleverans men avviker i två avgörande avseenden: det designar för illvilja och hämndlystna impulser snarare än att förutsätta rationalitet, och det föreslår gradvis övergång snarare än revolution. Konceptet emergenta samhällskontrakt har föregångare i Hayeks teori om spontan ordning [16].

Anarko-agorism. RSN delar betydande gemensam grund med agoristisk motekonomi [17]—särskilt betoningen på att bygga parallella institutioner och frivilligt utbyte. Agorismen tenderar dock att förutsätta rationellt egenintresse som en tillräcklig samordningsmekanism och saknar ofta en konkret migrationsväg från befintliga statsstrukturer. RSN införlivar uttryckligen icke-rationella beteendeböjelser och tillhandahåller en fiskal tryckmekanism för gradvis övergång.

Meritokrati. RSN kan representera en första funktionell beskrivning av hur meritokrati [18] kan uppstå som en systemisk egenskap snarare än en slogan. Traditionella meritokratiska system misslyckas eftersom de kräver en central auktoritet för att definiera och upprätthålla "förtjänst". I RSN uppstår förtjänst ur bilaterala bedömningar: de som levererar värde ackumulerar rykte; ingen kommitté avgör vem som har förtjänst.

Egendom som privilegium. RSN avviker grundläggande från anarkokapitalistiska och österrikiska skolans behandlingar av äganderätt som naturlig och absolut. I RSN-ramverket är egendom ett *privilegium*—ett socialt erkännande som i extrema fall kan dras tillbaka av gemenskapen när en deltagare grundläggande bryter mot delade normer (svek, vägran att försvara gemenskapen i en existentiell kris, systematisk exploatering). Detta är inte statlig expropriation utan ett tillbakadragande av socialt erkännande från nätverket av bilaterala relationer.

13 Diskussion och begränsningar

Kallstart. RSN:s värde beror på nätverkseffekter; tidiga användare möter begränsat värde tills deltagandet når en tröskel. Även från tidiga skeden fungerar dock DID-nätverket som en användbar kompletterande informationskälla. Tidig ryktesbedömning och auktoritetsbedömning förväntas utvecklas gradvis med ökande sofistikering.

Anti-snyltning och åtkomstkontroll. Mål-DID:er kan införa graderade avgifter och åtkomstbegränsningar för förfrågningar från DID:er med lågt rykte. Detta är inte binärt utan en kontinuerlig skala: ju mindre rykte en förfrågande DID har, desto mindre information får den, desto längre väntar den, och desto mer betalar den. Denna mekanism incitamenterar genuint deltagande framför passiv konsumtion.

Ojämlik tillgång. Kostnaden för att publicera påståenden kan filtrera bort legitima klagomål från ekonomiskt missgynnade deltagare. Motåtgärd: varje deltagare fungerar samtidigt som en potentiell verifierare (eller delegerar denna roll) och tjänar verifieringsavgifter. Över en tillräcklig tidshorisont bör en icke-radikal deltagare närma sig finansiell neutralitet—verifieringsintäkter som ungefär uppväger publiceringskostnader. Detta är en statistisk förväntan, inte en garanti.

Ryktesojämlikhet. Tidiga användare ackumulerar fördelar som kan skapa hinder för senkomlingar. Ryktesbedömning utförs dock av tredjepartsleverantörer som kan välja att mildra förstahandsfördelen genom sina aggregeringsalgoritmer. Att vara först med ett gott rykte är en legitim komparativ ekonomisk fördel—och det är avsiktligt.

Öppna frågor. Optimala kostnadsfunktioner, aggregeringsstandarder, protokollstyrning, och interaktion med AI-genererad syntetisk ryktesdata förblir områden för framtida arbete.

Denna uppsats hävdar inte att RSN kommer att producera optimala utfall under alla omständigheter. Den hävdar att RSN representerar ett *genomförbart* alternativ—tekniskt implementerbart, ekonomiskt självförsörjande, och socialt förenligt med mänskliga beteendeböjelser som de faktiskt är.

14 Slutsats

Denna uppsats har presenterat det ryktes-sociala nätverket, ett decentraliserat protokoll som möjliggör pseudonymt, verifierbart ryktesutbyte. Principen om dyr radikalism säkerställer att bedrägliga påståenden prissätts bort utan censur. Den föreslagna migrationsvägen möjliggör en gradvis, reversibel övergång från befintliga institutioner. Designen införlivar den mänskliga naturen som den är—inklusive småaktighet, illvilja och begäret efter hämndlysten tillfredsställelse—snarare än att kräva ideologisk omvandling. Resultatet är inte utopi utan ett system där rättvisa är tillgänglig, rykte förtjänas, och kostnaden för missförhållanden bärs av den part som orsakade dem.

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.