Rețea Descentralizată de Reputație: Un cadru pentru organizarea socială naturală

Pavel Kudrna
Prague, Czechia
Draft v1 — March 2026

Abstract

Simțul dreptății—convingerea că nedreptățile sunt îndreptate și meritul este răsplătit—este cea mai puternică forță de coeziune a societății. Când instituțiile centralizate de guvernare nu pot oferi acest simț pentru că nivelul costului impunerii unui drept depășește valoarea dreptului însuși, coeziunea socială se erodează. Structurile instituționale actuale eșuează în a soluționa o categorie semnificativă de dispute în același mod sistematic în care planificarea centralizată eșuează în alocarea resurselor: prin asimetrie informațională, bucle de feedback lipsă și deconectarea decidenților de consecințele deciziilor lor. Această lucrare prezintă o Rețea Socială de Reputație (RSN): un strat de comunicare descentralizat, incoruptibil și rezistent la cenzură, construit pe Identificatori Descentralizați (DID), care permite participanților pseudonimi să publice, să verifice și să consume informații de reputație despre comportamentul din lumea reală. Mecanismul central se bazează pe trei principii de proiectare: (1) o structură asimetrică a costurilor în care citirea datelor de reputație este ieftină, dar scrierea necesită efort verificabil; (2) un protocol nedeterminist de selecție a verificatorilor bazat pe hashing consistent, care taxează afirmațiile radicale prin costuri de iterație în creștere; și (3) un model de autoritate de reputație orientat spre piață, în care verificatorii privați își pun în joc reputația acumulată pe acuratețea afirmațiilor pe care le avizează. Arhitectura rezultată produce o meritocrație emergentă fără coordonare centrală și permite o cale de migrare graduală și reversibilă de la sistemele existente administrate de stat.

1 Introducere

1.1 Problema încrederii centralizate

Guvernarea modernă se sprijină pe o presupunere fundamentală: că instituțiile centralizate pot media încrederea între străini la scară largă. Instanțele soluționează disputele. Registrele certifică proprietatea. Organismele de reglementare impun standarde. Aceste instituții au fost concepute într-o epocă în care informația era rară, comunicarea era lentă, iar delegarea autorității către un organism central era singurul mecanism de coordonare fezabil. Guvernarea centralizată eșuează însă din aceleași motive structurale ca și planificarea centralizată: asimetrie informațională, bucle de feedback lipsă și deconectarea decidenților de consecințele deciziilor lor.

Presupunerea eșuează, de exemplu, atunci când costul medierii instituționale depășește valoarea disputei. Să considerăm un chiriaș care descoperă că apartamentul închiriat nu are un certificat de siguranță electrică cerut de lege—o condiție care reprezintă un pericol imediat pentru viață. Dreptul legal al chiriașului de a se retrage din contract este neechivoc. Totuși, costul impunerii acestui drept prin sistemul judiciar depășește valoarea monetară a garanției și a daunelor datorate, chiar incluzând eventualele compensații statutare [1]. Răspunsul rațional este să absoarbă pierderea și să iasă.

Acesta nu este un caz-limită patologic. Este experiența implicită pentru o categorie semnificativă de dispute în care prejudiciul este real, dar mizele monetare se situează sub pragul la care impunerea instituțională devine rațională din punct de vedere economic. Rezultatul este un sistem care favorizează structural actorii răuvoitori: cei care aduc prejudicii altora în volume sub acest prag pot acționa în impunitate, deoarece costul căutării dreptății cade asupra părții vătămate.

Exemplul de mai sus provine din mediul juridic al autorului—sistemul de drept civil ceh. În alte tradiții juridice—dreptul comun bazat pe precedent, dreptul cutumiar, sistemele mixte—dreptatea eșuează în moduri diferite și în grade diferite, în funcție de specificul cultural și procedural al jurisdicției. Cititorii vor recunoaște probabil exemple echivalente din propriul context. Ceea ce este universal din punct de vedere structural este tiparul: disputele a căror valoare cade sub pragul impunerii raționale economic se încheie cu pierderea absorbită de partea vătămată. RSN nu

promite o dreptate perfectă—doar reduce avantajul structural de care se bucură actorii răuvoitori atunci când impunerea instituțională este neeconomică.

1.2 De ce soluțiile existente sunt insuficiente

Cadrele de identitate descentralizată (DID) [2] oferă mecanisme criptografice pentru gestionarea identității suverane a sinelui, dar se concentrează în primul rând pe verificarea identității, fără a aborda întrebarea mai amplă a reputației comportamentale.

Token-urile Soulbound (SBT) [3] surprind ideea că reputația este netransferabilă, dar se bazează pe infrastructură blockchain cu constrângeri de scalabilitate și nu abordează stimulentele economice care guvernează introducerea informației. Concepte înrudite precum token-urile de merit (de ex., Liberland) împărtășesc o filozofie similară, dar rămân legate de cadre jurisdicționale specifice.

Organizațiile Autonome Descentralizate (DAO) [4] implementează guvernarea prin contracte inteligente, dar reproduc dinamici plutocratice în care influența este proporțională cu capitalul. Votul cuadratic [5] atenuează parțial acest lucru, dar limitează adoptarea practică. DAO-urile se confruntă de asemenea cu *problema oracolului* fundamentală: contractele inteligente nu pot verifica în mod fiabil stările din lumea reală fără o sursă externă de încredere, iar această problemă nu are o soluție generală în cadrul arhitecturii blockchain.

Niciun sistem existent nu combină descentralizarea, rezistența la cenzură, pseudonimitatea, costul verificabil de intrare și consensul emergent.

1.3 Contribuții

Această lucrare aduce următoarele contribuții:

1. Definirea **Rețelei Sociale de Reputație (RSN)**, un protocol descentralizat care extinde cadrul DID pentru a susține schimbul bilateral de reputație.
2. Un **protocol nedeterminist de selecție a verificatorilor** bazat pe hashing consistent [6].
3. **Principiul Radicalismului Costisitor**, care taxează afirmațiile în funcție de distanța lor față de consensul rețelei prin trei canale de cost care se compun.
4. Un **model de Autoritate Reputabilă** cu stimulente asimetrice, în care avizarea falsă costă catastrofal mai mult decât onorariile legitime.
5. O **cale de migrare graduală** printr-o infrastructură fiscală paralelă.

2 Principii de proiectare

Arhitectura RSN este constrânsă de cinci principii de proiectare nenegociabile.

Continuitate și evoluție. Sistemul coexistă cu instituțiile existente pe parcursul unei perioade de tranziție de durată nedeterminată. Tranziția trebuie să fie reversibilă în fiecare etapă.

Voluntariat și responsabilitate. Participarea este voluntară, dar voluntariatul este cuplat cu responsabilitatea: un participant care preia controlul asupra unei funcții instituționale își asumă simultan obligațiile aferente.

Diversitate și neutralitate culturală. Consensul emerge din interacțiuni bilaterale, nu din reguli prestabilite impuse de proiectanții sistemului.

Reziliență și rezistență la cenzură. Costul cenzurării rețelei trebuie să depășească costul tolerării ei. Doar totalitarismul deplin—cu un cost politic și economic ruinător—poate suprima sistemul.

Consens și impunere. Sistemul încorporează tendințele umane spre meschinărie, ranchiună și satisfacție retributivă ca trăsături de rezistență structurală. Reaua conduită nu este interzisă; ea este taxată.

3 Prezentare generală a sistemului

3.1 Rețeaua Socială de Reputație

RSN este un strat de comunicare descentralizat, peer-to-peer, în care participanții schimbă informații verificabile despre comportamentul din lumea reală. Proprietățile sale definitorii sunt: infrastructură descentralizată și necenzurabilă; participare pseudonimă prin DID-uri; structură asimetrică a costurilor (citirea este ieftină, scrierea este costisitoare); verificabilitate criptografică; și **suport pentru standarde**—formate care pot fi citite de mașini pentru informația propagată prin rețea, pentru serviciile oferite de autorități (compunerea afirmațiilor, avizarea, serviciul de martor) și pentru formatul de politică, incluzând reguli de evaluare a reputației contrapărții și de estimare a riscului de nepotrivire a politicii (între comportamentul declarat și cel real).

3.2 Componente arhitecturale

RSN constă din patru componente principale (Fig. 1):

1. **Stratul DID.** Identitățile participanților cu reguli declarate, metadate de reputație și rutare de rețea.
2. **Protocolul de afirmații.** Format structurat pen-

tru publicarea de aserțiuni despre evenimente din lumea reală.

3. **Rețeaua de verificare.** Protocol descentralizat pentru atribuirea verificatorilor folosind hashing consistent.
4. **Stratul de agregare a reputației.** Servicii care produc rezumate de reputație lizibile pentru oameni.

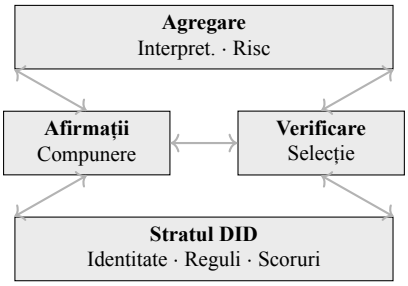

Figure 1: Arhitectura RSN pe patru straturi.

3.3 Rolurile participanților

O tranzacție de verificare implică până la șase roluri DID distincte (Fig. 2): **Emitentul** (DID_I, creează și trimite afirmația), **Subiectul** (DID_S, DID-ul despre care este afirmația—poate coincide cu Emitentul), **Autoritatea** (DID_A, avizează afirmația contra unui onorariu; poate oferi și servicii de martor—*opțional*), **Martorul** ($DID_{W_{1..n}}$, monitor incognito al onestității verificatorului prin coduri de provocare—*opțional*), **Verificatorul** (DID_V, selectat algoritmic pentru a publica afirmația) și **RSN** (rețeaua în care sunt publicate afirmațiile verificate). Orice rol poate fi delegat unui alt DID (Secțiunea 7.4). O Autoritate combină în mod obișnuit avizarea cu serviciile de martor, dar cele două funcții sunt logic independente.

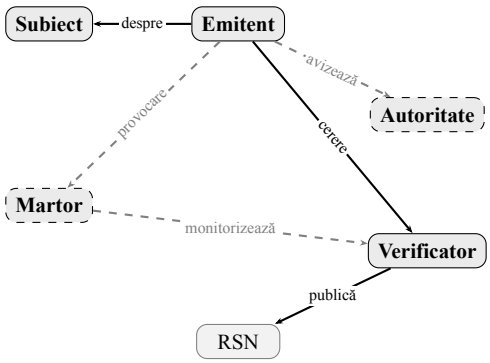

Figure 2: Rolurile DID într-o tranzacție de verificare. Linie punctată = opțional (Autoritate, Martor).

3.4 Incoruptibilitate: patru forțe

Incoruptibilitatea RSN nu provine dintr-un singur mecanism, ci din patru forțe concurente. Niciuna nu este suficientă în sine; doar combinația lor face ca o tentativă de corupere să fie irațională din punct de vedere economic.

Țintă imprevizibilă. Verificatorul pentru fiecare afirmație este selectat nedeterminist prin hashing consistent (Secțiunea 5.3). Un atacator nu poate viza în prealabil un verificator anume pentru mituire, deoarece identitatea verificatorului este o funcție a conținutului afirmației și a iterațiilor anterioare, nu a alegerii emitentului.

Efect de pârghie reputațional—creștere lentă, prăbușire rapidă. Reputația poate fi câștigată doar incremental, printr-un comportament consistent susținut. Ea poate fi însă pierdută catastrofal printr-o singură avizare frauduloasă (Secțiunea 6.2). Această asimetrie înseamnă că ani de reputație acumulată pot fi distruși de o singură avizare necinstită; strategia optimă rămâne respingerea afirmațiilor suspecte.

Promisiune publică. Fiecare Deținător de DID își declară public politica—un set de reguli care pot fi citite de mașini pe care se angajează să le urmeze. Divergența dintre declarație și comportamentul real este detectabilă și taxată ca o abatere reputațională mai gravă decât încălcarea de bază (Secțiunea 7.3). Ipocrizia este, prin urmare, mai costisitoare decât necinstea directă.

Asimetria costului atacului asupra rețelei mesh. Costul cenzurării sau destabilizării rețelei crește neliniar odată cu dimensiunea și densitatea rețelei, în timp ce costul tolerării ei rămâne constant. Pentru ca cenzura să merite, un actor centralizat ar trebui să o aplice pe întreaga rețea—necesitând măsuri disproporționate față de orice beneficiu imaginabil (Secțiunea 10).

4 Modelul de identitate descentralizată

4.1 DID cu proprietăți speciale

RSN extinde specificația W3C DID Core [2] cu: **Reguli declarate** (angajamente comportamentale care pot fi citite de mașini), **Metadate de reputație** (scor comportamental agregat) și **Rutare de rețea** (poartă onion mutabilă, separată de poziția stabilă pe inel).

4.2 Ciclul de viață al afirmației

O Afirmație parcurge șase etape (Fig. 3): compunere, avizare opțională de către autoritate, selecția verificatorului prin hashing consistent, decizia de verificare (acceptare sau respingere cu iterație), publicare și actualizarea reputației pentru toate părțile.

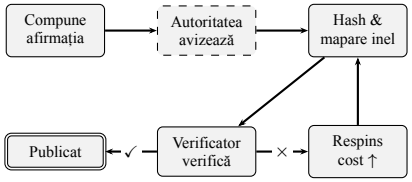

Figure 3: Ciclul de viață al afirmației cu bucla de iterație.

4.3 Relația cu W3C DID Core

Modelul de identitate al RSN este un supraset propriu al specificației W3C DID Core [2]. Toate DID-urile RSN sunt DID-uri W3C valide. Extensiile specifice RSN sunt codificate ca proprietăți ale documentului DID, definite într-o specificație de metodă DID dedicată, compatibilă cu infrastructura existentă precum ION [7] și Ceramic [8].

5 Verificarea și propagarea informației

5.1 Costul intrării informației

Principiul economic central al RSN este asimetria dintre citire și scriere. Citirea datelor de reputație se apropie de un cost marginal zero pentru participanții care fac parte din rețeaua DID și au acces proporțional cu reputația lor—noii veniți trebuie să câștige treptat un acces mai larg (vezi anti-parazitismul). Scrierea—înțeleasă ca materializarea durabilă a reputației în rețea, nu ca un act tehnic punctual—necesită o investiție cumulativă verificabilă pe trei dimensiuni: **timp** (ani de viață dedicați comportamentului consistent, angajamentelor onorate și relațiilor cultivate), **energie** (efort investit în tranzacții oneste, grija pentru parteneriate și fiabilitate pe termen lung) și **bani** (investiție în propriul nume—dezvoltare profesională, calitatea muncii, reparații pentru prejudiciile cauzate). Reputația nu poate fi cumpărată instantaneu—este rezultatul unei acumulări de-o viață pe care sistemul doar o face vizibilă și transferabilă între contexte. Costurile tehnice punctuale ale protocolului (semnături criptografice, onorarii ale verificatorilor) sunt neglijabile în comparație cu această investiție de bază.

5.2 Graful social și profunzimea contactelor

RSN este fundamental o rețea socială: fiecare DID adaugă contacte (alte DID-uri) care permit conexiunea. Aceste contacte au propriile lor contacte, și așa mai departe. Căutarea algoritmică a verificatorului operează în interiorul unei profunzimi configurabile h de contacte legate (de ex., $h = 3$: contactele directe, contactele lor și contactele contactelor). Această arhitectură nu necesită un singur blockchain global—favorizează în mod natural emergența unor comunități/clustere cu suprapuneri către alte comunități. Fiecare participant DID trebuie să aibă o **politică** publicată—un set de reguli care pot fi citite de mașini care guvernează modul în care sunt evaluate cererile primite. Încălcările de politică sunt înregistrate în rețea ca artefacte negative.

5.3 Selecția algoritmică a verificatorului

Protocolul de verificare folosește hashing consistent [6] (Fig. 4). Verificarea este un serviciu contra cost: verificatorii operează pentru un onorariu, creând o piață în care concurența determină prețul, viteza și fiabilitatea.

Pasul 1. Documentul afirmației este concatenat cu rezultatul hash al iterației anterioare (sau $\varnothing$ la prima iterație) și hash-uit:

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

Algoritmul trebuie să includă *calea completă* a tuturor cererilor și răspunsurilor anterioare—nu doar un hash al iterației precedente. Răspunsul complet al fiecărui verificator (acceptare, respingere, preț cotat, motiv) este adăugat documentului în creștere, verificabil prin semnături criptografice la fiecare pas.

Pasul 2. Hash-ul este mapat pe N poziții pe inelul de hashing consistent, distribuite uniform (de ex., pentru $N = 4$: $+0°, +90°, +180°, +270°$). Din fiecare poziție, o căutare în sensul acelor de ceasornic selectează cel mai apropiat DID drept candidat verificator (Fig. 5). N este un parametru variabil care poate depinde de procentul de DID-uri active la momentul respectiv, de ora din zi sau de reactivitatea istorică a rețelei.

Pasul 3. Verificatorul acceptă (publică, punându-și în joc reputația) sau respinge (revenind la Pasul 1 cu hash-ul respingerii). Când un nod nu răspunde deși declară statut online, cererea următoare trebuie să includă toate răspunsurile de la toți cei N candidați verificatori anteriori.

Anti-parazitism. DID-urile țintă pot stabili onorarii sau restricții de acces pentru interogări de la DID-uri

noi cu reputație scăzută. Acest mecanism gradat (nu binar) obligă noii veniți să își construiască reputația printr-o activitate autentică înainte de a consuma liber datele altora.

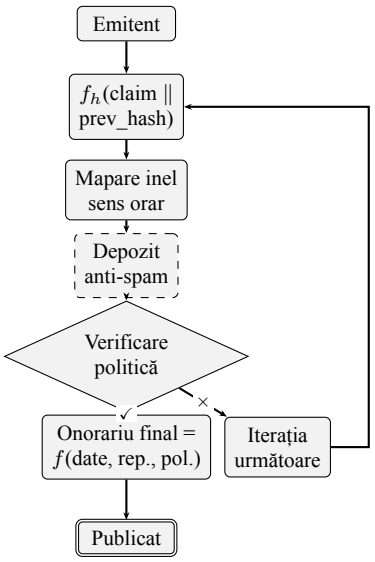

Figure 4: Protocolul de selecție a verificatorului. Depozitul anti-spam este opțional și poate fi rambursabil. Onorariul final se plătește doar la acceptare.

Fiecare respingere adaugă răspunsul complet al verificatorului (inclusiv motive și condiții) la documentul afirmației, extinzându-i conținutul. Din documentul extins, se calculează nedeterminist un nou hash, mapat pe o poziție diferită pe inel și selectând un verificator diferit. Documentarea căii complete este obligatorie—emitentul nu poate prezice sau influența verificatorul următor. Dacă un verificator ignoră o cerere în ciuda unei politici declarate compatibile, martorii (dacă sunt prezenți) înregistrează acest lucru, iar emitentul poate atașa dovezile martorilor la publicarea finală.

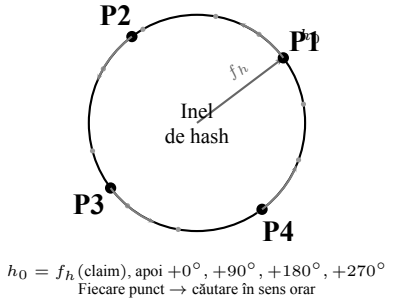

Figure 5: Selecție cu puncte multiple (N=4). Hash-ul h_0 stabilește decalajul; 4 puncte distribuite uniform de la h_0.

5.4 Protocolul martorului

Rolul de **Martor** oferă responsabilizare incognito pentru onestitatea verificatorului printr-un protocol criptografic de cod de provocare:

Pasul W1. Solicitantul semnează cererea de verificare și o trimite către N_w martori—contacte din rețeaua socială a solicitantului sau furnizori specializați de servicii de martor care operează contra cost.

Pasul W2. Fiecare martor w_i semnează întreaga cerere semnată, păstrează semnătura originală σ_i și calculează un cod de provocare $c_i = h(\sigma_i)$. Codul de provocare este adăugat la cerere.

Pasul W3. Cererea, purtând acum N_w coduri de provocare, este trimisă către verificator. Verificatorul observă codurile, dar *nu poate determina* cine sunt martorii sau dacă codurile corespund unor semnături reale.

Pasul W4 (verificator onest). Dacă verificatorul răspunde conform politicii sale declarate, codurile de provocare rămân opace. Martorii nu sunt niciodată dezvăluiți. Nu se publică date suplimentare.

Pasul W5 (încălcare de politică). Dacă verificatorul își încalcă politica (ignoră cererea, răspunde inconsecvent), solicitantul deține semnăturile originale ale martorilor σ_i. Acestea pot fi publicate ca date însoțitoare: oricine poate verifica $c_i = h(\sigma_i)$, demonstrând că martorul a fost prezent. Solicitantul poate publica independent—verificatorul a semnat deja codurile de provocare în răspunsul său.

Proprietatea de cacealma. Solicitantul poate înlocui unele sau toate codurile de provocare cu valori aleatorii. Verificatorul nu poate distinge codurile autentice (susținute de autorități cu reputație înaltă) de zgomot. Această *incertitudine* este mecanismul de impunere: fiecare cerere poartă riscul ca o autoritate respectată să privească incognito. Costul menținerii acestei presiuni este aproape zero (generarea de numere aleatorii), în timp ce costul potențial al necinstei pentru verificator este catastrofal. Comportamentul onest este stimulat chiar și în absența martorilor reali.

Autoritatea ca martor. O Autoritate care avizează o afirmație poate combina serviciile de martor: „Avizez afirmația ta și servesc drept martor incognito în timpul verificării.” Acesta este un model de afaceri natural—Autoritatea are deja contextul. Totuși, cele două roluri sunt logic independente.

5.5 Principiul Radicalismului Costisitor

Trei canale de cost se compun simultan (Fig. 6):

Canalul 1: Costul iterației. Fiecare respingere forțează o nouă iterație care consumă timp și resurse. Creștere liniară.

Canalul 2: Umflarea documentului. Fiecare iterație adaugă răspunsul complet al verificatorului la documentul afirmației. Creșterea este liniară, dar cu un decalaj de bază: încărcătura inițială (conținutul afirmației, avizarea autorității, semnăturile criptografice) are deja o dimensiune netrivială B_0. Dimensiunea totală după k iterații: $S(k) = B_0 + k \cdot \Delta$, unde Δ este dimensiunea medie a răspunsului.

Canalul 3: Prima de risc a verificatorului. Riscul este subiectiv. Verificatorul evaluează dacă politicile declarate ale DID-ului solicitant intră în conflict cu propriile interese comerciale, sociale sau politice ale verificatorului. Prima poate escalada exponențial odată cu distanța percepută față de „idealul" verificatorului: $P(d) = \alpha \cdot e^{\beta d}$, unde d este metrica de distanță subiectivă a verificatorului. Dincolo de o graniță personală interzisă, verificatorul poate refuza complet.

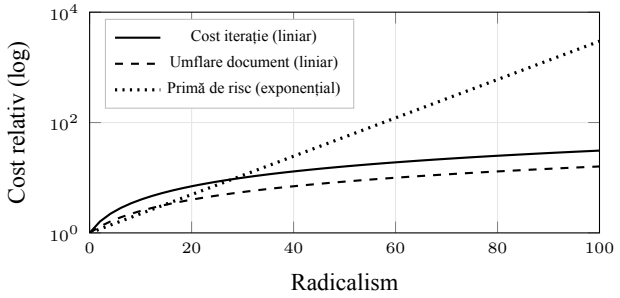

Figure 6: Escaladarea costului pe trei canale. Prima de risc domină la radicalism ridicat.

În mod critic, aceasta nu este cenzură. Nicio afirmație nu este interzisă. Sistemul taxează riscul (Tabelul 1).

Table 1: Comparație de cost între tipurile de afirmații.

Tip	Iter.	Doc	Onor.	Total
Credibilă	$k_{\min}$	B_0	$P_{\min}$	Scăzut
Controversată	k_{med}	$B_0{+}k\Delta$	$\alpha e^{\beta d}$	Moderat
Radicală	$k_{\max}$	$\gg B_0$	$\gg P_{\min}$	Foarte ridicat
Frauduloasă	$\to \infty$	—	—	Nepublicabilă

6 Reputația și evaluarea riscului

6.1 Modelul de acumulare a reputației

Reputația prezintă trei proprietăți: **acumulare lentă** (creștere incrementală prin comportament consistent), **distrugere rapidă** (o singură fraudă poate reduce scorul catastrofal) și **evaluare individuală** (fiecare parte consumatoare poate aplica propria funcție de agregare).

6.2 Autorități Reputabile

O Autoritate Reputabilă examinează afirmațiile și, dacă este mulțumită, le co-semnează—punându-și în joc propria reputație (Fig. 7). Asimetria este intenționată: câștigarea reputației este lentă (incremental $+\delta$ per avizare onestă), în timp ce pierderea ei este catastrofală ($-\Delta \gg \delta$ per avizare falsă; ilustrativ, de ex., $+2\%$ față de -70%). Strategia optimă este întotdeauna respingerea afirmațiilor suspecte. Valorile specifice ale δ și Δ sunt parametri ai sistemului.

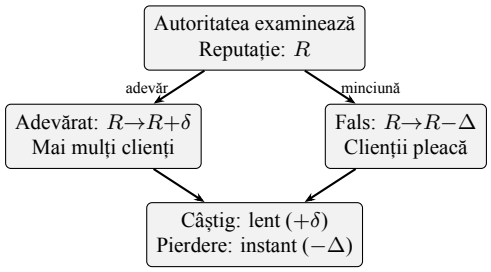

Figure 7: Autoritate Reputabilă—stimulente asimetrice.

6.3 Reputație multidimensională

Reputația nu este un scalar, ci un vector pe mai multe dimensiuni: fiabilitate financiară, integritate personală, competență profesională, angajament civic și altele (Fig. 8). Diferiți furnizori de evaluare proiectează acest vector diferit, în funcție de context—un creditor prioritizează fiabilitatea financiară, un angajator competența profesională, un vecin comportamentul civic. Nu există un singur scor de reputație „corect"; doar perspective.

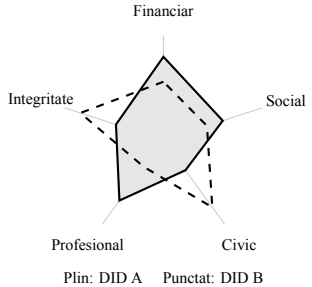

Figure 8: Vectori de reputație multidimensională. DID-uri diferite prezintă profiluri diferite pe dimensiuni.

6.4 Evaluarea democratizată a riscului

RSN democratizează evaluarea sistematică a riscului—o capacitate concentrată în prezent în instituțiile financiare, dar aplicabilă cu mult dincolo de domeniul bancar. Conglomerate industriale care evaluează fiabilitatea furnizorilor, companii de asigurări care taxează riscul comportamental, due diligence pentru fuziuni și achiziții, estimarea duratei de viață a echipamentelor în producție—oriunde riscul contrapărții necesită evaluare, RSN oferă o alternativă descentralizată, orientată spre piață. O piață de servicii de interpretare traduce datele brute de reputație multidimensională în rezumate acționabile, făcând evaluarea contrapărții accesibilă oricărui participant la cost marginal.

7 Consens și soluționarea disputelor

7.1 Modelul de justiție descentralizată

RSN reformulează justiția ca o problemă de negociere bilaterală. Amenințarea unei deteriorări permanente și verificabile a reputației este un factor de descurajare mai eficient decât procesele judiciare pe care partea vătămată nu și le poate permite.

7.2 Consens emergent

Fiecare participant menține un prag personal de satisfacție. Consensul agregat al rețelei emerge ca media statistică a mii de negocieri bilaterale (Fig. 9). Un răspuns cu mult peste consens (barbar) este costisitor de publicat. Un răspuns aproape de consens (proporțional) este ieftin. Consensul nu este o regulă—este un semnal de preț.

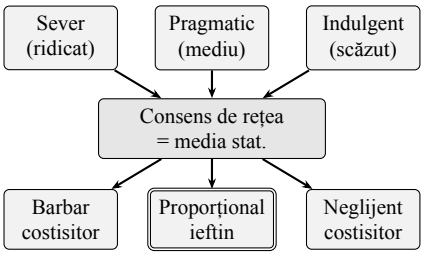

Figure 9: Consens emergent din pragurile individuale de satisfacție.

7.3 Calibrarea pedepsei

Fiecare Deținător de DID declară public răspunsurile la categorii specifice de rea conduită. Declarațiile disproporționat de aspre sau de indulgente atrag semnale de reputație negative. Declarațiile proporționale sunt acceptate fără fricțiune—un sistem de pedeapsă autocalibrant.

Declarațiile de consens sunt ele însele supuse detectării ipocriziei: angajarea declarativă față de o poziție de consens comportându-se totodată inconsecvent constituie o abatere reputațională mai gravă decât abaterea de bază, deoarece demonstrează o înșelăciune intenționată.

7.4 Delegarea

Toate activitățile din cadrul unui DID—cu o singură excepție—pot fi delegate unui alt DID. **Rolul de Subiect—DID-ul despre al cărui comportament este afirmația—nu poate fi delegat; este legat netransferabil de deținătorul identității la care se referă afirmația.** Celelalte roluri active—Emitent, Autoritate, Martor, Verificator—pot fi transferate unui DID delegat desemnat, fie pentru verificare, trimiterea afirmației, participarea la consens sau soluționarea disputelor. Delegarea este revocabilă în orice moment. Aceasta permite specializarea (de ex., servicii profesionale de verificare) în timp ce Deținătorul păstrează controlul și responsabilitatea supreme. Delegarea se aplică în întregul sistem și este esențială pentru scalabilitate.

7.5 De la moralitatea individuală la contractul social emergent

Politica declarată a fiecărui DID reprezintă o formalizare a moralității individuale: ceea ce Deținătorul consideră acceptabil, cum răspunde la comportamente specifice, ce cere de la contrapărți. Aceste politici nu sunt impuse de un proiectant de sistem—ele sunt alese de fiecare participant și exprimate într-o formă care poate fi citită de mașini.

Această formalizare permite o emergență în trei etape. În primul rând, moralitatea individuală este codificată drept **politică**—un set de reguli declarate, praguri și funcții de răspuns pe care DID-ul se angajează să le urmeze. În al doilea rând, agregatul tuturor politicilor din rețea produce **etică emergentă**—norme observabile statistic pe care niciun participant nu le-a proiectat, dar care apar din interacțiunea a mii de poziții morale individuale [9]. În al treilea rând, această etică emergentă, exprimată ca norme comportamentale comune impuse prin semnale bilaterale de preț, constituie un **contract social măsurabil**—nu un construct teoretic pe care nimeni nu l-a semnat [10], ci un set de reguli observabil empiric, susținut de comportament real.

Acest proces reflectă concluziile teoriei fundamentelor morale [11]: moralitatea umană este intuitivă, pluralistă și variabilă cultural. RSN nu necesită consensul moral ca intrare; el produce consensul comportamental ca ieșire. Contractul social rezultat nu este static—el evoluează pe măsură ce participanții aderă, pleacă și își ajustează politicile ca răspuns la feedbackul rețelei. Spre deosebire de teoria clasică a contractului social, acest contract este revocabil, observabil și aplicabil fără un suveran.

8 Modelul economic

Secțiunile precedente au descris un instrument—mecanismele de verificare ale RSN, structura costurilor și consensul emergent. Această secțiune descrie o metodologie de aplicare a acestui instrument la tranziția fiscală și de guvernare. Instrumentul este de uz general; metodologia de mai jos este o posibilă aplicație.

8.1 Structura stimulentelor

Reputația ca și capital creează stimulente directe pentru comportamentul onest. În funcționarea normală, participanții își construiesc reputația în mod natural prin tranzacții cotidiene și angajamente onorate. Cheltuiala principală este pentru afirmațiile *negative*—înregistrarea prejudiciului cauzat de alții. Această asimetrie stimulează comportamentul util și fiabil: a fi onest nu costă nimic în plus, în timp ce a fi dăunător creează o urmă documentată pe care alții vor plăti să o păstreze. Ipocrizia—declararea de reguli fără a le urma—este cel mai costisitor mod de eșec, deoarece demonstrează o înșelăciune intenționată.

8.2 Sistemul fiscal paralel

Trei componente permit presiunea concurențială: (1) **Impozit Simplu**—o singură cotă proporțională fără excepții, inițial marginal sub cota efectivă existentă; (2) **Înregistrarea Electronică a Cheltuielilor (ESR)**—inversând modelul ceh EET astfel încât cetățenii să supravegheze cheltuielile statului; (3) **Alocarea Impozitului Direcționată de Cetățean**—pornind de la câteva procente în primul an și ajungând, după un deceniu, oriunde de la un procent modest de două cifre până la o migrare completă către un sistem direcționat de cetățeni, în funcție de rata de adoptare. Tempo-ul efectiv depinde de viteza cu care apar alternative de piață liberă la serviciile statului și de disponibilitatea statului de a coopera cu tranziția; funcția de timp nu trebuie să fie liniară, iar nu există niciun motiv să se stabilească o limită superioară pentru punctul la care poate ajunge în cele din urmă adoptarea.

9 Calea de migrare

Migrarea se desfășoară în trei faze (Fig. 10): **Faza 1: Suprapunere** (RSN ca strat informațional, statul este unicul furnizor), **Faza 2: Concurență** (RSN oferă alternative funcționale, utilizare a sistemului dublu) și **Faza 3: Tranziție** (RSN depășește echivalentele de stat, migrare voluntară). Tranziția este reversibilă în fiecare etapă.

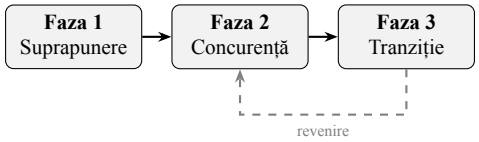

Figure 10: Migrare în trei faze—reversibilă în fiecare etapă.

Mecanismul principal de presiune este fiscal: când contribuabilii condiționali ating o „minoritate semnificativă economic X"—un grup suficient de mare încât represiunea împotriva lui să cauzeze pagube economice netriviale, iar nesupunerea civică să devină o amenințare credibilă—statul intră în negociere. Pentru ilustrare, folosim $X \approx 15\%$ din PIB, dar pragul efectiv depinde de economia specifică.

10 Analiza de securitate

Considerăm cinci categorii de adversari: actori răuvoitori individuali, grupuri organizate, adversari corporativi, adversari la nivel de stat și adversari la nivel de protocol.

Rezistență la atacuri Sybil [12]. Construirea reputației necesită o interacțiune susținută și verificabilă. Costul unui atac Sybil reușit crește liniar cu numărul de identități false și cuadratic cu nivelul de reputație țintit. Operarea mai multor DID-uri în paralel este posibilă, dar costisitoare prin proiectare—fiecare identitate trebuie să își acumuleze independent reputația printr-o activitate autentică. În societățile libere, acest cost descurajează abuzul ocazional; în dictaturi, DID-urile paralele devin un instrument de supraviețuire care permite rezistența compartimentată, coordonarea din subteran și navigarea mai sigură pe piața neagră.

Apărare împotriva coluziunii. Tiparele de avizare reciprocă în cadrul grupurilor închise sunt detectabile

prin analiza grafului social. Funcțiile de agregare a reputației reduc ponderea afirmațiilor provenite din surse strâns grupate.

Adversar la nivel de stat. Rutarea onion, absența infrastructurii centralizate și distribuirea rolului de Verificator în întreaga bază de participanți asigură faptul că suprimarea necesită măsuri disproporționate față de orice beneficiu.

Confidențialitate vs. responsabilizare. Pseudonimitatea—o cale de mijloc între anonimat și dezvăluirea identității—permite DID-urilor să acumuleze o reputație semnificativă fără a dezvălui identitatea reală a Deținătorului.

11 Considerații privind confidențialitatea

Modelul de confidențialitate al RSN se bazează pe pseudonimitate. Deținătorul controlează dezvăluirea identității: minimă (pseudonim pur), selectivă (credențiale specifice legate) sau completă (identitate juridică asociată). Afirmațiile publicate sunt permanente—sistemul susține corectarea contextuală, dar nu ștergerea. Un Deținător poate abandona un DID compromis și porni de la zero, renunțând la reputația acumulată.

12 Lucrări conexe

Specificația W3C DID Core [2] și Ceramic Network [8] oferă fundamentul de identitate. EigenTrust [13] a demonstrat agregarea distribuită a reputației fără autoritate centrală. SBT-urile [3] au introdus token-uri sociale netransferabile. RSN diferă prin accentul pus pe costul economic ca filtru de calitate și prin mecanismul său de taxare a radicalismului.

DAO-urile [4] și votul cuadratic [5] au demonstrat fezabilitatea guvernării descentralizate. RSN derivă consensul din negocieri bilaterale de preț, mai degrabă decât din vot.

Propunerea se bazează pe teoria anarho-capitalistă [14, 15] pentru furnizarea privată de servicii, dar se abate în două privințe critice: proiectează pentru ranchiună și impulsuri retributive, mai degrabă decât presupunând raționalitate, și propune o tranziție graduală, nu o revoluție. Conceptul de contracte sociale emergente are antecedente în teoria ordinii spontane a lui Hayek [16].

Anarho-agorism. RSN împărtășește un teren comun semnificativ cu contra-economia agoristă [17]—în special accentul pe construirea de instituții paralele și schimbul voluntar. Totuși, agorismul tinde să presupună interesul propriu rațional ca mecanism suficient de coordonare și adesea îi lipsește o cale concretă de migrare de la structurile statale existente. RSN încorporează explicit tendințe comportamentale nonraționale și oferă un mecanism de presiune fiscală pentru tranziția graduală.

Meritocrație. RSN poate reprezenta o primă descriere funcțională a modului în care meritocrația [18] poate emerge ca o proprietate sistemică, mai degrabă decât ca un slogan. Sistemele meritocratice tradiționale eșuează pentru că necesită o autoritate centrală care să definească și să impună „meritul”. În RSN, meritul emerge din evaluări bilaterale: cei care oferă valoare acumulează reputație; niciun comitet nu decide cine are merit.

Proprietatea ca privilegiu. RSN se abate fundamental de la tratamentul anarho-capitalist și al școlii austriece al drepturilor de proprietate ca naturale și absolute. În cadrul RSN, proprietatea este un *privilegiu*—o recunoaștere socială care poate, în cazuri extreme, să fie retrasă de comunitate atunci când un participant încalcă fundamental normele comune (trădare, refuzul de a apăra comunitatea într-o criză existențială, exploatare sistematică). Aceasta nu este expropriere de stat, ci o retragere a recunoașterii sociale de către rețeaua de relații bilaterale.

13 Discuție și limitări

Pornirea la rece. Valoarea RSN depinde de efectele de rețea; cei care adoptă devreme se confruntă cu o valoare limitată până când participarea atinge un prag. Totuși, chiar și din stadiile timpurii, rețeaua DID servește drept sursă utilă de informație suplimentară. Se așteaptă ca evaluarea timpurie a reputației și estimarea autorității să se dezvolte treptat, cu o sofisticare crescândă.

Anti-parazitism și control al accesului. DID-urile țintă pot impune onorarii gradate și restricții de acces la interogările de la DID-uri cu reputație scăzută. Aceasta nu este binară, ci o scală continuă: cu cât un DID interogator are mai puțină reputație, cu atât primește mai puțină informație, așteaptă mai mult și plătește mai mult. Acest mecanism stimulează participarea autentică în locul consumului pasiv.

Inegalitatea accesului. Costul publicării afirmațiilor poate filtra plângeri legitime de la participanți dezavantajați economic. Atenuare: fiecare participant servește simultan drept potențial verificator (sau deleagă acest rol) și câștigă onorarii de verificare. Pe

un orizont de timp suficient, un participant non-radical ar trebui să se apropie de neutralitatea financiară—venitul din verificare compensând aproximativ costurile de publicare. Aceasta este o așteptare statistică, nu o garanție.

Inegalitatea reputației. Cei care adoptă devreme acumulează avantaje care pot crea bariere pentru cei care vin mai târziu. Totuși, evaluarea reputației este efectuată de furnizori terți care pot alege să atenueze avantajul primului venit prin algoritmii lor de agregare. A fi primul cu o bună reputație este un avantaj economic comparativ legitim—și acest lucru este intenționat.

Întrebări deschise. Funcțiile optime de cost, standardele de agregare, guvernarea protocolului și interacțiunea cu datele de reputație sintetică generate de IA rămân domenii pentru lucrări viitoare.

Această lucrare nu pretinde că RSN va produce rezultate optime în toate circumstanțele. Ea pretinde că RSN reprezintă o alternativă *fezabilă*—implementabilă tehnic, autosustenabilă economic și compatibilă social cu tendințele comportamentale umane așa cum sunt ele în realitate.

14 Concluzie

Această lucrare a prezentat Rețeaua Socială de Reputație, un protocol descentralizat care permite schimbul de reputație pseudonim și verificabil. Principiul Radicalismului Costisitor asigură faptul că afirmațiile frauduloase sunt scoase de pe piață prin preț, fără cenzură. Calea de migrare propusă permite o tranziție graduală și reversibilă de la instituțiile existente. Proiectarea încorporează natura umană așa cum este—inclusiv meschinăria, ranchiuna și dorința de satisfacție retributivă—mai degrabă decât să necesite o transformare ideologică. Rezultatul nu este o utopie, ci un sistem în care dreptatea este accesibilă, reputația este câștigată, iar costul relei conduite este suportat de partea care a cauzat-o.

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.