

Децентрализирана репутациска мрежа: Рамка за природна општествена организација

Pavel Kudrna
Prague, Czechia
Draft v1 — March 2026

Abstract

Чувството за правда—уверувањето дека неправдите се исправуваат и заслугата се наградува—е најсилната кохезивна сила на општеството. Кога централизираните институции на управувањето не можат да го обезбедат ова чувство, бидејќи трошокот за спроведување на некое право го надминува самата вредност на тоа право, општествената кохезија ерозира. Сегашните институционални структури не успеваат да разрешат значителна класа спорови на систематски ист начин на кој централното планирање не успева да ги распредели ресурсите: преку информациска асиметрија, отсутни повратни петелки и одвоеност на носителите на одлуки од последиците на нивните одлуки. Овој труд претставува Репутациска општествена мрежа (RSN): децентрализиран, неподмитлив, отпорен на цензура комуникациски слој изграден врз Децентрализирани идентификатори (DID) кој им овозможува на псевдонимните учесници да објавуваат, проверуваат и консумираат репутациски информации за однесувањето во реалниот свет. Основниот механизам почива врз три дизајнерски принципи: (1) асиметрична трошкова структура каде читањето на репутациски податоци е евтино, но пишувањето бара проверлив напор; (2) недетерминистички протокол за избор на проверувач заснован на конзистентно хеширање кој ги наплатува радикалните тврдења преку ескалирачки трошоци на итерации; и (3) пазарно управуван модел на репутациска власт каде приватните проверувачи ја залагаат својата натрупана репутација на точноста на тврдењата што ги поддржуваат. Добиената архитектура произведува емергентна меритократија без централна координација и овозможува постепена, реверзибилна миграциска патека од постојните државно администрирани системи.

1 Вовед

1.1 проблемот на централизираната доверба

Современото управување почива врз една фундаментална претпоставка: дека централизираните институции можат да посредуваат доверба меѓу непознати во голем обем. Судовите пресудуваат спорови. Регистрите потврдуваат сопственост. Регулаторните тела спроведуваат стандарди. Овие институции беа осмислени во ера кога информациите беа оскудни, комуникацијата беше бавна, а делегирањето на власт на централно тело беше единствениот изводлив механизам за координација. Централизираното управување, сепак, не успева поради истите структурни причини како и централното планирање: информациска асиметрија, отсутни повратни петелки и одвоеност на носителите на одлуки од последиците на нивните одлуки.

Претпоставката не успева, на пример, кога трошокот за институционалното посредување ја надминува вредноста на спорот. Замислете закупец кој открива дека неговиот изнајмен стан нема законски задолжителен сертификат за електрична безбедност—состојба која претставува непосредна опасност по животот. Законското право на закупецот да се повлече од договорот е недвосмислено. Сепак, трошокот за спроведување на тоа право преку судскиот систем ја надминува паричната вредност на депозитот и должната отштета, дури и вклучувајќи ја потенцијалната законска компензација [1]. Рационалниот одговор е да се апсорбира загубата и да се излезе.

Ова не е патолошки граничен случај. Тоа е стандардното искуство за значителна класа спорови во кои штетата е реална, но паричниот влог паѓа под прагот на кој институционалното спроведување станува економски рационално. Резултатот е систем кој структурно ги фаворизира

лошите актери: оние кои им нанесуваат штета на другите во обеми под овој праг можат да дејствуваат некажнето, бидејќи трошокот за барање правда паѓа врз оштетената страна.

Горниот пример е извлечен од правната средина на авторот—чешкиот граѓанско-правен систем. Во другите правни традиции—прецедентно засновано обичајно право, обичајно право, мешани системи—правдата не успева на различни начини и во различни степени, во зависност од културните и процедуралните специфики на јурисдикцијата. Читателите веројатно ќе препознаат еквивалентни примери од сопствениот контекст. Она што е структурно универзално е шаблонот: спорови чија вредност паѓа под прагот на економски рационалното спроведување завршуваат со тоа што загубата ја апсорбира оштетената страна. RSN не ветува совршена правда—таа само го намалува структурното предимство што го уживаат лошите актери кога институционалното спроведување е неекономично.

1.2 Зошто постојните решенија не се доволни

Рамките за децентрализиран идентитет (DID) [2] обезбедуваат криптографски механизми за само-суверено управување со идентитетот, но се фокусираат првенствено на верификација на идентитетот без да го адресираат поширокото прашање за репутацијата на однесувањето.

Соулбаунд токени (SBT) [3] го фаќаат сознанието дека репутацијата е непренослива, но се потпираат на блокчејн инфраструктура со ограничувања во скалабилноста и не ги адресираат економските поттици кои управуваат со внесувањето информации. Сродни концепти како токени на заслуга (на пр., *Liberland*) споделуваат слична филозофија, но остануваат врзани за специфични јурисдикциски рамки.

Децентрализирани автономни организации (DAO) [4] го спроведуваат управувањето преку паметни договори, но ја реплицираат плутократската динамика каде влијанието е пропорционално на капиталот. Квадратното гласање [5] делумно го ублажува ова, но ја ограничува практичната примена. DAO исто така се соочуваат со фундаменталниот *проблем на пророштво (oracle)*: паметните договори не можат сигурно да проверат состојби во реалниот свет без доверлив надворешен извор, а овој проблем нема општо решение во рамките на блокчејн архитектурата.

Ниту еден постоен систем не ги комбинира децентрализацијата, отпорноста на цензура, псевдонимноста, проверливиот трошок за влез и емергентниот консензус.

1.3 Придонеси

Овој труд ги дава следните придонеси:

1. Дефиниција на **Репутациска општествена мрежа (RSN)**, децентрализиран протокол кој ја проширува DID рамката за да поддржи билатерална размена на репутација.
2. **Недетерминистички протокол за избор на проверувач** заснован на конзистентно хеширање [6].
3. **Принципот на скап радикализам**, кој ги наплатува тврдењата според нивното растојание од мрежниот консензус преку три сложувачки трошковни канали.
4. **Модел на репутабилна власт** со асиметрични поттици каде лажната поддршка чини катастрофално повеќе отколку легитимните такси.
5. **Постепена миграциска патека** преку паралелна фискална инфраструктура.

2 Дизајнерски принципи

Архитектурата на RSN е ограничена со пет непреговарливи дизајнерски принципи.

Континуитет и еволуција. Системот коегзистира со постојните институции во текот на преоден период со неопределена должина. Преминот мора да биде реверзибилен во секоја фаза.

Доброволност и одговорност. Учеството е доброволно, но доброволноста е споена со одговорност: учесник кој презема контрола врз некоја институционална функција истовремено ги презема и придружните обврски.

Разноликост и културна неутралност. Консензусот произлегува од билатерални интеракции, а не од предодредени правила наметнати од дизајнерите на системот.

Отпорност и отпор на цензура. Трошокот за цензурирање на мрежата мора да го надмине трошокот за нејзино толерирање. Само целосен тоталитаризам—по разорна политичка и економска цена—може да го потисне системот.

Консензус и спроведување. Системот ги вградува човечките склоности кон ситничавост,

злоба и одмаздничко задоволство како носечки карактеристики. Недоличното однесување не е забрането; тоа е наплатено.

3 Преглед на системот

3.1 Репутациска општествена мрежа

RSN е децентрализиран, рамноправен (peer-to-peer) комуникациски слој во кој учесниците разменуваат проверливи информации за однесувањето во реалниот свет. Нејзините дефинирачки својства се: децентрализирана и нецензурабилна инфраструктура; псевдонимно учество преку DID; асиметрична трошкова структура (читањето е евтино, пишувањето е скапо); криптографска проверливост; и **поддршка на стандарди**—машински читливи формати за информации кои се шират низ мрежата, за услуги нудени од властите (составување тврдење, поддршка, услуга на сведок) и за форматот на политиката, вклучувајќи правила за оценување на репутацијата на спротивната страна и проценка на ризикот од несоваѓање на политиката (меѓу декларираното и вистинското однесување).

3.2 Архитектонски компоненти

RSN се состои од четири примарни компоненти (Сл. 1):

1. **DID слој.** Идентитети на учесниците со декларирани правила, репутациски метаподатоци и мрежно рутирање.
2. **Протокол на тврдења.** Структуриран формат за објавување тврдења за настани во реалниот свет.
3. **Верификациска мрежа.** Децентрализиран протокол за доделување проверувачи со користење конзистентно хеширање.
4. **Слој за агрегација на репутација.** Услуги кои произведуваат човечки читливи резимеа на репутацијата.

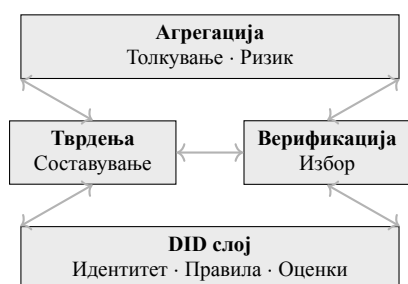


Figure 1: Четирислојна архитектура на RSN.

3.3 Улоги на учесниците

Верификациска трансакција вклучува до шест различни DID улоги (Сл. 2): **Издавач** (DID_I , го создава и поднесува тврдењето), **Субјект** (DID_S , DID за кого е тврдењето—може да се совпаѓа со Издавачот), **Власт** (DID_A , го поддржува тврдењето за такса; може да нуди и услуги на сведок—*изборно*), **Сведок** ($DID_{W_{1..n}}$, инкогнито надзорник на чесноста на проверувачот преку кодови за предизвик—*изборно*), **Проверувач** (DID_V , алгоритамски избран да го објави тврдењето) и **RSN** (мрежата каде се објавуваат проверените тврдења). Која било улога може да се делегира на друг DID (Дел 7.4). Власта вообичаено ја спојува поддршката со услугите на сведок, но двете функции се логички независни.

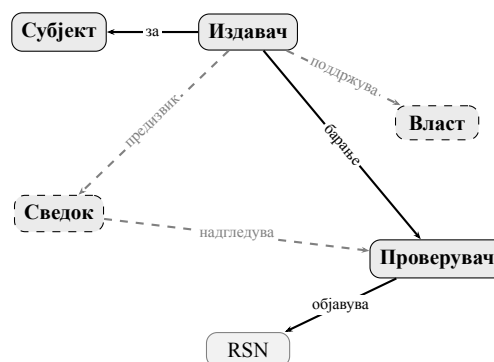


Figure 2: DID улоги во верификациска трансакција. Испрекинато = изборно (Власт, Сведок).

3.4 Неподмитливост: Четири сили

Неподмитливоста на RSN не произлегува од еден единствен механизам, туку од четири истовремени сили. Ниту една не е доволна сама по себе; само нивната комбинација прави обидот за корупција економски ирационален.

Непредвидлива цел. Проверувачот за секое тврдење се избира недетерминистички преку конзистентно хеширање (Дел 5.3). Напаѓачот не може однапред да насочи специфичен проверувач за поткуп, бидејќи идентитетот на проверувачот е функција од содржината на тврдењето и претходните итерации, а не од изборот на издавачот.

Репутациски лост—бавно нагоре, брзо надолу. Репутацијата може да се стекне само постепено, преку одржливо конзистентно однесување. Таа, сепак, може катастрофално да се изгуби во една единствена измамничка поддршка (Дел 6.2). Оваа асиметрија значи дека

години натрупана репутација можат да се уништат од една нечесна поддршка; оптималната стратегија останува да се одбијат сомнителните тврдења.

Јавно ветување. Секој DID сопственик јавно ја декларира својата политика—машински читлив збир правила кои се обврзува да ги следи. Отстапувањето меѓу декларацијата и вистинското однесување е откривливо и се наплатува како репутациски престап потежок од самата основна повреда (Дел 7.3). Лицемерието, според тоа, е поскапо од директната нечесност.

Асиметрија на трошокот за напад врз мрежата (mesh). Трошокот за цензурирање или дестабилизирање на мрежата расте нелинеарно со големината и густината на мрежата, додека трошокот за нејзино толерирање останува константен. За цензурата да се исплати, централизиран актер би морал да ја примени низ целата мрежа—барјќи мерки непропорционални на секоја замислива корист (Дел 10).

4 Модел на децентрализиран идентитет

4.1 DID со специјални својства

RSN ја проширува спецификацијата W3C DID Core [2] со: **Декларирани правила** (машински читливи обврски за однесување), **Репутациски метаподатоци** (агрегирана оценка на однесувањето) и **Мрежно рутирање** (променлива опцион порта одвоена од стабилната позиција на прстенот).

4.2 Животен циклус на тврдењето

Тврдењето поминува низ шест фази (Сл. 3): составување, изборна поддршка од власт, избор на проверувач преку конзистентно хеширање, верификациска одлука (прифаќање или одбивање со итерација), објавување и репутациско ажурирање за сите страни.

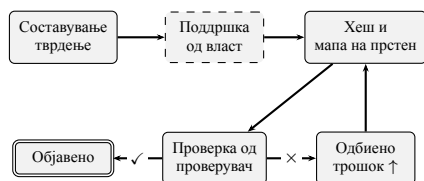


Figure 3: Животен циклус на тврдењето со итеративна петелка.

4.3 Однос кон W3C DID Core

Моделот на идентитет на RSN е правилен надмножество на спецификацијата W3C DID Core [2]. Сите RSN DID се валидни W3C DID. RSN-специфичните проширувања се кодирани како својства на DID документот дефинирани во посветена спецификација за DID метод, компатибилни со постојната инфраструктура како ION [7] и Ceramic [8].

5 Верификација и пропација на информации

5.1 Трошок за внесување информации

Основниот економски принцип на RSN е асиметријата меѓу читањето и пишувањето. Читањето на репутациски податоци се приближува кон нула гранична цена за учесниците кои се дел од DID мрежата и имаат пристап сразмерен на нивната репутација—дојденците мора постепено да заработат поширок пристап (види анти-паразитизам). Пишувањето—сфатено како трајна материјализација на репутацијата во мрежата, а не како еднократен технички чин—бара проверливо кумулативно вложување низ три димензии: **време** (години живот потрошени на конзистентно однесување, исполнети обврски и негувани односи), **енергија** (напор вложен во чесно постапување, грижа за партнерствата и долгорочна доверливост) и **пари** (вложување во сопственото име—професионален развој, квалитетот на сопствената работа, надомест за нанесени штети). Репутацијата не може да се купи веднаш—таа е исход на доживотно натрупување што системот само го прави видливо и преносливо низ контексти. Еднократните технички трошоци на протоколот (криптографски потписи, такси за проверувач) се занемарливи во споредба со ова основно вложување.

5.2 Општествен граф и длабочина на контактите

RSN е фундаментално општествена мрежа: секој DID додава контакти (други DID) кои ја дозволуваат врска. Тие контакти имаат свои контакти, и така натаму. Алгоритамското пребарување на проверувач работи во рамките на конфигурирабилна длабочина h на поврзани контакти (на пр., $h = 3$: сопствените директни контакти, нивните контакти и контакти на контакти).

Оваа архитектура не бара единствен глобален блокчејн—таа природно ја фаворизира појавата на заедници/кластери со преклопувања во други заедници. Секој DID учесник мора да има објавена **политика**—машински читлив збир правила кои управуваат со тоа како се оценуваат дојдовните барања. Прекршувањата на политиката се запишуваат во мрежата како негативни артефакти.

5.3 Алгоритамски избор на проверувач

Верификацискиот протокол користи конзистентно хеширање [6] (Сл. 4). Верификацијата е платена услуга: проверувачите работат за такса, создавајќи пазар каде конкуренцијата ги движи цените, брзината и доверливоста.

Чекор 1. Документот на тврдењето се спојува со резултатот од хешот на претходната итерација (или $\emptyset$ во првата итерација) и се хешира:

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

Алгоритмот мора да ја вклучи *целосната патека* на сите претходни барања и одговори—не само хеш на претходната итерација. Целосниот одговор на секој проверувач (прифаќање, одбивање, наведена цена, причина) се додава на растечкиот документ, проверлив преку криптографски потписи на секој чекор.

Чекор 2. Хешот се мапира на N позиции на прстенот на конзистентно хеширање, рамномерно распределени (на пр., за $N = 4$: $+0^\circ, +90^\circ, +180^\circ, +270^\circ$). Од секоја позиција, пребарување во насока на стрелките на часовникот го избира најблискиот DID како кандидат за проверувач (Сл. 5). N е променлив параметар кој може да зависи од процентот на моментално активни DID, времето од денот или историската одзивност на мрежата.

Чекор 3. Проверувачот прифаќа (објавува, залагајќи репутација) или одбива (враќајќи се на Чекор 1 со хешот на одбивањето). Кога јазол не одговара и покрај декларирањето на онлајн статус, следното барање мора да ги вклучи сите одговори од сите N претходни кандидати за проверувач.

Анти-паразитизам. Целните DID можат да постават такси или ограничувања на пристапот за прашања од нови DID со малку репутација. Овој степенуван механизам (не бинарен) ги принудува дојденците да изградат репутација преку вистинска активност пред слободно да ги консумираат податоците на другите.



Figure 4: Протокол за избор на проверувач. Анти-спам депозитот е избран и може да биде повратен. Конечната такса се плаќа само при прифаќање.

Секое одбивање го додава целосниот одговор на проверувачот (вклучувајќи причини и услови) на документот на тврдењето, проширувајќи ја неговата содржина. Од проширениот документ, недетерминистички се пресметува нов хеш, кој се мапира на различна позиција на прстенот и избира различен проверувач. Документирањето на целосната патека е задолжително—издавачот не може да го предвиди или влијае врз следниот проверувач. Ако проверувач го игнорира барањето и покрај компатибилна декларирана политика, сведоците (ако се присутни) го запишуваат ова, а издавачот може да приложи сведочки доказ при конечното објавување.

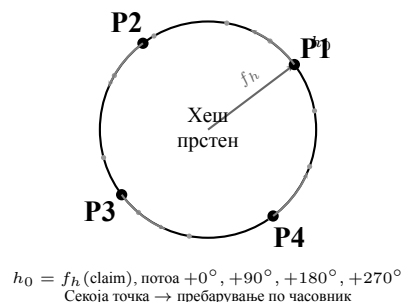


Figure 5: Повеќеточкест избор ($N=4$). Хешот h_0 го поставува поместувањето; 4 точки рамномерно распределени од h_0 .

5.4 Протокол на сведок

Улогата **Сведок** обезбедува инкогнито одговорност за чесноста на проверувачот преку криптографски

протокол на код за предизвик:

Чекор W1. Барателот го потпишува верификациското барање и го испраќа до N_w сведоци—контакти од општествената мрежа на барателот, или специјализирани даватели на услуги на сведок кои работат за такса.

Чекор W2. Секој сведок w_i го потпишува целото потпишано барање, го задржува оригиналниот потпис σ_i и пресметува код за предизвик $c_i = h(\sigma_i)$. Кодот за предизвик се додава на барањето.

Чекор W3. Барањето, кое сега носи N_w кодови за предизвик, се испраќа до проверувачот. Проверувачот ги набљудува кодовите, но *не може да утврди* кои се сведоците ниту дали кодовите одговараат на реални потписи.

Чекор W4 (чесен проверувач). Ако проверувачот одговори според својата декларирана политика, кодовите за предизвик остануваат непросирни. Сведоците никогаш не се откриваат. Не се објавуваат дополнителни податоци.

Чекор W5 (прекршување на политиката). Ако проверувачот ја прекрши својата политика (го игнорира барањето, одговара недоследно), барателот ги држи оригиналните потписи на сведоците σ_i . Тие можат да се објават како придружни податоци: секој може да провери $c_i = h(\sigma_i)$, докажувајќи дека сведокот бил присутен. Барателот може да објави независно—проверувачот веќе ги потпишал кодовите за предизвик во својот одговор.

Својството на блеф. Барателот може да замени случајни вредности за некои или сите кодови за предизвик. Проверувачот не може да ги разликува вистинските кодови (поткрепени со високо-репутирани власти) од шум. Оваа *неизвесност* е механизмот на спроведување: секое барање го носи ризикот дека почитувана власт набљудува инкогнито. Трошокот за одржување на овој притисок е близу нула (генерирање случајни броеви), додека потенцијалниот трошок од нечесноста за проверувачот е катастрофален. Чесното однесување се поттикнува дури и во отсуство на вистински сведоци.

Власта како сведок. Власт која поддржува тврдење може да ги спои услугите на сведок: „Го поддржувам вашето тврдење и служам како инкогнито сведок за време на верификацијата.“ Ова е природен деловен модел—власта веќе го има контекстот. Сепак, двете улоги се логички независни.

5.5 Принцип на скап радикализам

Три трошковни канали се сложуваат истовремено (Сл. 6):

Канал 1: Трошок на итерација. Секое одбивање принудува нова итерација која троши време и ресурси. Линеарен раст.

Канал 2: Надувување на документот. Секоја итерација го додава целосниот одговор на проверувачот на документот на тврдењето. Растот е линеарен, но со основно поместување: почетниот товар (содржина на тврдењето, поддршка од власт, криптографски потписи) веќе има нетривијална големина B_0 . Вкупна големина по k итерации: $S(k) = B_0 + k \cdot \Delta$, каде Δ е просечната големина на одговорот.

Канал 3: Ризична премија на проверувачот. Ризикот е субјективен. Проверувачот проценува дали декларираните политики на DID кој бара се во судир со сопствените комерцијални, општествени или политички интереси на проверувачот. Премијата може да ескалира експоненцијално со согледаното растојание од „идеалот“ на проверувачот: $P(d) = \alpha \cdot e^{\beta d}$, каде d е субјективната метрика на растојание на проверувачот. Надвор од личната граница на недопирливост, проверувачот може целосно да одбие.

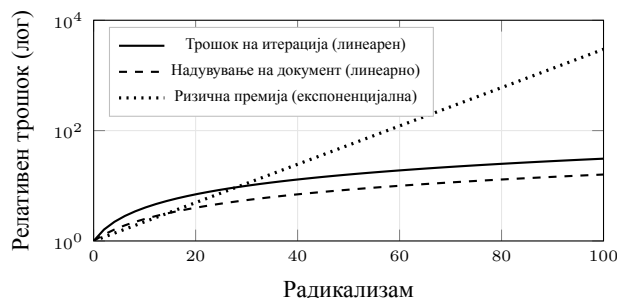


Figure 6: Ескалација на трошокот низ три канали. Ризичната премија доминира при висок радикализам.

Критично, ова не е цензура. Ниту едно тврдење не е забрането. Системот го наплатува ризикот (Табела 1).

Table 1: Споредба на трошоци низ типови тврдења.

Тип	Итер.	Док.	Такса	Вкупно
Веродостојно	$k_{\min}$	B_0	$P_{\min}$	Ниско
Контроверзно	k_{med}	$B_0 + k\Delta$	$\alpha e^{\beta d}$	Умерено
Радикално	$k_{\max}$	$\gg B_0$	$\gg P_{\min}$	Многу високо
Измамничко	$\rightarrow \infty$	—	—	Необјавливо

6 Репутација и проценка на ризик

6.1 Модел на натрупување на репутација

Репутацијата покажува три својства: **бавно натрупување** (постепен раст преку конзистентно однесување), **брзо уништување** (една единствена измама може катастрофално да ја намали оценката) и **индивидуална евалуација** (секоја консумирачка страна може да применува своја сопствена агрегациска функција).

6.2 Репутабилни власти

Репутабилна власт ги прегледува тврдењата и, ако е задоволна, ги ко-потпишува—залагајќи ја својата сопствена репутација (Сл. 7). Асиметријата е намерна: стекнувањето репутација е бавно (постепено $+\delta$ по чесна поддршка), додека губењето е катастрофално ($-\Delta \gg \delta$ по лажна поддршка; илустративно, на пр., $+2\%$ наспроти -70%). Оптималната стратегија е секогаш да се одбијат сомнителните тврдења. Специфичните вредности на δ и Δ се системски параметри.

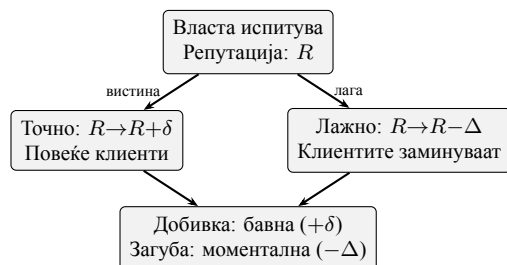


Figure 7: Репутабилна власт—асиметрични поттици.

6.3 Повеќедимензионална репутација

Репутацијата не е скалар, туку вектор низ повеќе димензии: финансиска доверливост, лична интегритет, професионална компетентност, граѓанска ангажираност и други (Сл. 8). Различните даватели на евалуација го проектираат овој вектор поинаку во зависност од контекстот—заемодавецот ѝ дава приоритет на финансиската доверливост, работодавачот на професионалната компетентност, соседот на граѓанското однесување. Не постои единствена „точна“ репутациска оценка; само перспективи.

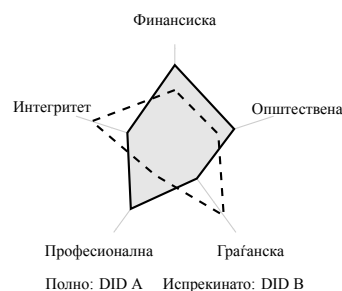


Figure 8: Повеќедимензионални репутациски вектори. Различни DID покажуваат различни профили низ димензиите.

6.4 Демократизирана проценка на ризик

RSN ја демократизира систематската проценка на ризик—способност моментално концентрирана во финансиските институции, но применлива далеку надвор од банкарството. Индустриски конгломерати кои ја проценуваат доверливоста на добавувачите, осигурителни компании кои го наплатуваат ризикот на однесувањето, длабинска анализа за спојувања и преземања, проценка на животниот век на опрема во производството—каде било каде ризикот на спротивната страна бара проценка, RSN обезбедува децентрализирана, пазарно управувана алтернатива. Пазар на услуги за толкување ги преведува суровите повеќедимензионални репутациски податоци во употребливи резимеа, правејќи ја евалуацијата на спротивната страна достапна за секој учесник по гранична цена.

7 Консензус и разрешување спорови

7.1 Модел на децентрализирана правда

RSN ја преформулира правдата како проблем на билатерално преговарање. Заканата за трајна, проверлива репутациска штета е поефективен одвраќач отколку правни постапки кои оштетената страна не може да си ги дозволи.

7.2 Емергентен консензус

Секој учесник одржува личен праг на задоволство. Агрегатниот консензус на мрежата произлегува како статистички просек на илјадници билатерални преговори (Сл. 9). Одговор далеку над консензусот (варварски) е скап за објавување. Одговор близу консензусот (пропорционален) е евтин.

Консензусот не е правило—тоа е ценовен сигнал.

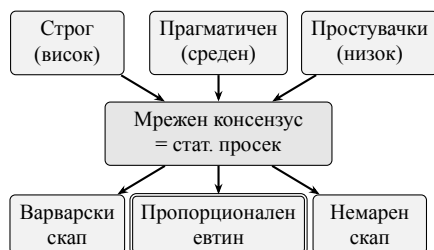


Figure 9: Емергентен консензус од индивидуалните прагови на задоволство.

7.3 Калибрација на казната

Секој DID сопственик јавно декларира одговори на специфични категории недолучно однесување. Непропорционално строги или благи декларации привлекуваат негативни репутациски сигнали. Пропорционалните декларации се прифаќаат без триење—самокалибрирачки казнен систем.

Консензусните декларации самите се подложни на откривање лицемерие: декларативното обврзување кон консензусна позиција додека се однесува недоследно претставува репутациски престап потешок од самото основно отстапување, бидејќи покажува намерна измама.

7.4 Делегирање

Сите активности во рамките на еден DID—со еден исклучок—можат да се делегираат на друг DID. **Улогата Субјект—DID чие однесување е предмет на тврдењето—не може да се делегира; таа е непреносливо врзана за сопственикот на идентитетот на кого се однесува тврдењето.** Другите активни улоги—Издавач, Власт, Сведок, Проверувач—можат да се пренесат на назначен делегатски DID, било за верификација, поднесување тврдење, учество во консензус или разрешување спор. Делегирањето е отповикливо во секое време. Ова овозможува специјализација (на пр., професионални верификациски услуги) додека сопственикот задржува крајна контрола и одговорност. Делегирањето се применува низ целиот систем и е суштинско за скалабилноста.

7.5 Од индивидуален морал до емергентен општествен договор

Декларираната политика на секој DID претставува формализација на индивидуалниот морал: што сопственикот смета за прифатливо, како реагира на

специфични однесувања, што бара од спротивните страни. Овие политики не се наметнати од дизајнер на системот—тие се избрани од секој учесник и изразени во машински читлива форма.

Оваа формализација овозможува тристепен емергенција. Прво, индивидуалниот морал се кодира како **политика**—збир декларирани правила, прагови и одговорни функции кои DID се обврзува да ги следи. Второ, агрегатот од сите политики низ мрежата произведува **емергентна етика**—статистички набљудливи норми кои ниту еден единствен учесник не ги дизајнирал, но кои произлегуваат од интеракцијата на илјадници индивидуални морални позиции [9]. Трето, оваа емергентна етика, изразена како споделени норми на однесување спроведени преку билатерални ценовни сигнали, претставува **мерлив општествен договор**—не теоретски конструкт што никој не го потпишал [10], туку емпириски набљудлив збир правила поткрепени со вистинско однесување.

Овој процес ги отсликува наодите од теоријата на моралните основи [11]: човечкиот морал е интуитивен, плуралистички и културно променлив. RSN не бара морален консензус како влез; таа произведува консензус на однесување како излез. Добиениот општествен договор не е статичен—тој еволуира како учесниците се приклучуваат, заминуваат и ги приспособуваат своите политики како одговор на повратната информација од мрежата. За разлика од класичната теорија на општествениот договор, овој договор е отповиклив, набљудлив и спроведлив без суверен.

8 Економски модел

Претходните делови опишаа алатка—верификациските механизми на RSN, трошковната структура и емергентниот консензус. Овој дел опишува методологија за примена на оваа алатка врз фискален и управувачки премин. Алатката е за општа намена; методологијата подолу е една можна примена.

8.1 Структура на поттици

Репутацијата како капитал создава директни поттици за чесно однесување. Во нормално работење, учесниците природно градат репутација преку секојдневни трансакции и исполнети обврски. Примарниот трошок е за **негативни тврдења**—запишување штета нанесена од други.

Оваа асиметрија поттикнува корисно, доверливо однесување: да се биде чесен не чини ништо дополнително, додека да се биде штетен создава документирана трага што другите ќе платат да ја зачуваат. Лицемерието—декларирање правила без нивно следење—е најскапиот режим на неуспех, бидејќи покажува намерна измама.

8.2 Паралелен фискален систем

Три компоненти овозможуваат конкурентен притисок: (1) **Едноставен данок**—единствена пропорционална стапка без исклучоци, првично маргинално под постојната ефективна стапка; (2) **Електронска регистрација на трошење (ESR)**—инвертирање на чешкиот EET модел така што граѓаните ги надгледуваат државните трошоци; (3) **Даночна алокација насочена од граѓаните**—почнувајќи од неколку проценти во првата година и достигнувајќи, по една деценија, некаде од ниските двоцифрени броеви до целосна миграција кон систем насочен од граѓаните, во зависност од стапката на прифаќање. Вистинското темпо зависи од брзината со која се појавуваат слободно-пазарни алтернативи на државните услуги и од подготвеноста на државата да соработува со преминот; функцијата на времето не мора да биде линеарна, и нема причина да се постави горна граница за тоа каде прифаќањето може конечно да пристигне.

9 Миграциска патека

Миграцијата се одвива низ три фази (Сл. 10): **Фаза 1: Прекривка** (RSN како информациски слој, државата е единствен давател), **Фаза 2: Конкурентност** (RSN обезбедува функционални алтернативи, употреба на двоен систем) и **Фаза 3: Премин** (RSN ги надминува државните еквиваленти, доброволна миграција). Преминот е реверзибилен во секоја фаза.

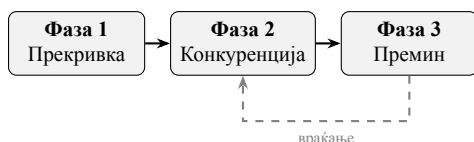


Figure 10: Тристепенна миграција—реверзибилна во секоја фаза.

Примарниот механизам на притисок е фискален: кога условните даночни обврзници достигнат „економски значајно малцинство X “—група

доволно голема што репресијата против неа предизвикува нетривијална економска штета и граѓанската непослушност станува веродостојна закана—државата влегува во преговарање. За илустрација, користиме $X \approx 15\%$ од БДП, но вистинскиот праг зависи од специфичната економија.

10 Безбедносна анализа

Разгледуваме пет категории противници: индивидуални лоши актери, организирани групи, корпоративни противници, противници на државно ниво и противници на ниво на протокол.

Отпорност на Sybil [12]. Градењето репутација бара одржлива, проверлива интеракција. Трошокот за успешен Sybil напад расте линеарно со лажните идентитети и квадратно со целното ниво на репутација. Работењето со повеќе DID паралелно е можно, но скапо по дизајн—секој идентитет мора независно да натрупа репутација преку вистинска активност. Во слободните општества овој трошок ја одвраќа лежерната злоупотреба; во диктатурите, паралелните DID стануваат алатка за преживување која овозможува компартментализиран отпор, подземна координација и побезбедна навигација на црниот пазар.

Одбрана од дослук. Шаблоните на заемна поддршка меѓу затворени групи се откривливи преку анализа на општествениот граф. Функциите за агрегација на репутација ги дисконтираат тврдењата од тесно кластерирани извори.

Противник на државно ниво. Onion рутирањето, отсуството на централизирана инфраструктура и распределбата на улогата Проверувач низ базата на учесници обезбедуваат дека потиснувањето бара мерки непропорционални на секоја корист.

Приватност наспроти одговорност. Псевдонимноста—средина меѓу анонимноста и откривањето на идентитетот—им овозможува на DID да натрупаат значајна репутација без да го откриваат идентитетот на сопственикот во реалниот свет.

11 Разгледувања за приватноста

Моделот на приватност на RSN е изграден врз псевдонимност. Сопственикот ја контролира откривањето на идентитетот: минимално (чист

псевдоним), селективно (специфични акредитиви поврзани) или целосно (законски идентитет придружен). Објавените тврдења се трајни—системот поддржува контекстуална корекција, но не и бришење. Сопственикот може да напушти компрометиран DID и да почне одново, откажувајќи се од натрупаната репутација.

12 Сродна работа

Спецификацијата W3C DID Core [2] и Ceramic Network [8] ја обезбедуваат основата на идентитетот. EigenTrust [13] демонстрираше распределена агрегација на репутација без централна власт. SBT [3] ги воведоа непреносливите општествени токени. RSN се разликува по својот акцент врз економскиот трошок како филтер за квалитет и по својот механизам за наплата на радикализмот.

DAO [4] и квадратното гласање [5] ја демонстрираа изводливоста на децентрализираното управување. RSN го изведува консензусот од билатерални ценовни преговори наместо од гласање.

Предлогот се потпира на анархо-капиталистичката теорија [14, 15] за приватно давање услуги, но отстапува во два критични аспекти: тој дизајнира за злобата и одмаздничките импулси наместо да претпоставува рационалност, и предлага постепен премин наместо револуција. Концептот на емергентни општествени договори има претходници во теоријата на Хајек за спонтаниот поредок [16].

Анархо-агоризам. RSN споделува значителна заедничка основа со агористичката контра-економија [17]—особено акцентот врз градењето паралелни институции и доброволната размена. Сепак, агоризмот има тенденција да претпоставува рационален личен интерес како доволен механизам за координација и често му недостасува конкретна миграциска патека од постојните државни структури. RSN експлицитно ги вградува нерационалните склоности на однесувањето и обезбедува механизам на фискален притисок за постепен премин.

Меритократија. RSN може да претставува прв функционален опис на тоа како меритократијата [18] може да се појави како системско својство наместо како слоган. Традиционалните меритократски системи не успеваат бидејќи бараат централна власт да ја дефинира и спроведе „заслугата“. Во RSN, заслугата произлегува од билатерални евалуации:

оние кои даваат вредност натрупуваат репутација; ниту еден комитет не одлучува кој има заслуга.

Сопственоста како привилегија. RSN фундаментално отстапува од анархо-капиталистичките и австриско-школските третмани на сопственичките права како природни и апсолутни. Во рамката на RSN, сопственоста е *привилегија*—општествено признание кое, во екстремни случаи, може да се повлече од заедницата кога учесник фундаментално ги прекршува споделените норми (предавство, одбивање да се брани заедницата во егзистенцијална криза, систематска експлоатација). Ова не е државна експропријација, туку повлекување на општественото признание од мрежата на билатерални односи.

13 Дискусија и ограничувања

Ладен старт. Вредноста на RSN зависи од мрежните ефекти; раните прифаќачи се соочуваат со ограничена вредност додека учеството не достигне праг. Сепак, дури и од раните фази, DID мрежата служи како корисен дополнителен извор на информации. Се очекува раната евалуација на репутацијата и проценката на властите постепено да се развиваат со зголемена софистицираност.

Анти-паразитизам и контрола на пристап. Целните DID можат да наметнат степенувани такси и ограничувања на пристапот за прашања од DID со ниска репутација. Ова не е бинарно, туку континуирана скала: колку помалку репутација има DID кој прашува, толку помалку информации добива, толку подолго чека и толку повеќе плаќа. Овој механизам поттикнува вистинско учество наместо пасивна консумација.

Нееднаквост на пристап. Трошокот за објавување тврдења може да ги филтрира легитимните поплаки од економски необезбедените учесници. Ублажување: секој учесник истовремено служи како потенцијален проверувач (или ја делегира оваа улога) и заработува верификациски такси. Во доволен временски хоризонт, нерадикален учесник треба да се приближи до финансиска неутралност—верификацискиот приход приближно ги надоместува трошоците за објавување. Ова е статистичко очекување, не гаранција.

Репутациска нееднаквост. Раните прифаќачи натрупуваат предности кои можат да создадат бариери за подоцнежните. Сепак, евалуацијата на репутацијата ја вршат независни даватели кои

можат да изберат да ја ублажат предноста на првиот преку своите агрегациски алгоритми. Да се биде прв со добра репутација е легитимна компаративна економска предност—и тоа е по дизајн.

Отворени прашања. Оптималните трошковни функции, стандардите за агрегација, управувањето со протоколот и интеракцијата со синтетичките репутациски податоци генерирани од ВИ остануваат области за идна работа.

Овој труд не тврди дека RSN ќе произведе оптимални исходи во сите околности. Тој тврди дека RSN претставува *изводлива* алтернатива—технички имплементабилна, економски самоодржлива и општествено компатибилна со човечките склоности на однесување какви што тие навистина се.

14 Заклучок

Овој труд ја претстави Репутациската општествена мрежа, децентрализиран протокол кој овозможува псевдонимна, проверлива размена на репутација. Принципот на скап радикализам обезбедува дека измамничките тврдења се исфрлаат од пазарот преку цена, без цензура. Предложената миграциска патека овозможува постепен, реверзибилен премин од постојните институции. Дизајнот ја вградува човечката природа каква што е—вклучувајќи ситничавост, злоба и желбата за одмаздничко задоволство—наместо да бара идеолошка трансформација. Резултатот не е утопија, туку систем каде правдата е достапна, репутацијата е заработена, а трошокот на недоличното однесување го носи страната која го предизвикала.

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.