

Decentralizovaná reputační síť: Rámec pro přirozenou organizaci společnosti

Pavel Kudrna
Prague, Czechia
Draft v1 — březen 2026

Abstrakt

Pocit spravedlnosti — přesvědčení, že křivdy jsou napraveny a zásluhy odměněny — je nejsilnějším soudržným prvkem společnosti. Když centralizované instituce správy nemohou tento pocit zajistit, protože náklady na vymáhání práva překračují hodnotu samotného práva, společenská soudržnost eroduje. Současné institucionální struktury selhávají při řešení významné třídy sporů systematicky stejným způsobem, jakým centrální plánování selhává při alokaci zdrojů: informační asymetrií, chybějícími zpětnými vazbami a odpojením rozhodovatelů od důsledků jejich rozhodnutí. Tento článek představuje reputační sociální síť (Reputation Social Network, RSN): decentralizovanou, nezkorumpovatelnou, cenově odolnou komunikační vrstvu postavenou na decentralizovaných identifikátorech (Decentralized Identifiers, DID), která umožňuje pseudonymním účastníkům publikovat, ověřovat a konzumovat reputační informace o chování v reálném světě. Jádrem mechanismu spočívá na třech konstrukčních principech: (1) asymetrická nákladová struktura, kde čtení reputačních dat je levné, ale zápis vyžaduje ověřitelné úsilí; (2) nedeterministický protokol výběru ověřovatelů založený na konzistentním hashování, který oceňuje radikální tvrzení prostřednictvím eskalujících iteračních nákladů; a (3) tržně řízený model reputačních autorit, v němž soukromí ověřovatelé sázejí svou nashromážděnou reputaci na přesnost tvrzení, která endorsují. Výsledkem je architektura, která vytváří emergentní meritokracii bez centrální koordinace a umožňuje postupnou, reverzibilní migrační cestu od stávajících státem spravovaných systémů.

1 Úvod

1.1 Problém centralizované důvěry

Moderní správa věcí veřejných spočívá na základním předpokladu: že centralizované instituce dokáží zprostředkovat důvěru mezi cizími lidmi ve velkém

měřítku. Soudy rozhodují spory. Rejstříky osvědčují vlastnictví. Regulační orgány vynucují standardy. Tyto instituce byly navrženy v době, kdy informace byly vzácné, komunikace pomalá a delegování pravomocí na centrální orgán bylo jediným proveditelným koordinacním mechanismem. Centralizovaná správa však selhává ze stejných strukturálních důvodů jako centrální plánování: informační asymetrie, chybějící zpětné vazby a odpojení rozhodovatelů od důsledků jejich rozhodnutí.

Tento předpoklad selhává například tehdy, když náklady na institucionální zprostředkování převyšují hodnotu sporu. Uvažme nájemce, který zjistí, že pronajatý byt postrádá zákonem požadovanou revizní zprávu elektroinstalace — stav, který bezprostředně ohrožuje život. Nájemcovo právní oprávnění odstoupit od smlouvy je jednoznačné. Avšak náklady na vynucení tohoto práva prostřednictvím soudního systému převyšují peněžní hodnotu kauce a dlužného odškodného, a to i se započtením případného tabulkového odškodnění [1]. Racionální odpovědí je ztrátu absorbovat a odejít.

Nejedná se o patologický okrajový případ. Je to standardní zkušenost u významné třídy sporů, v nichž je újma reálná, ale finanční sázka spadá pod práh, při němž se institucionální vynucování stává ekonomicky racionálním. Výsledkem je systém, který strukturálně nadřazuje nepoctivým aktérům: ti, kdo poškozují ostatní v objemech pod tímto prahem, mohou jednat beztrestně, protože náklady na vymáhání spravedlnosti nejsou poškození.

Uvedený příklad pochází z autorova právního prostředí — českého kontinentálního systému. V jiných právních tradicích — precedenčním common law, zvykovém právu, smíšených systémech — selhává justice odlišnými způsoby a v jiné míře, podle kulturních a procedurálních specifik dané jurisdikce. Čtenář si patrně rozpomene na ekvivalentní příklad ze svého kontextu. Strukturálně univerzální je vzorec: spory, jejichž hodnota leží pod prahem ekonomicky racionálního vymáhání, končí absorbováním ztráty poškozenou stra-

nou. Reputační síť neslibuje dokonalou spravedlnost — pouze redukuje strukturální výhodu, kterou nepoctiví aktéři získávají, když je institucionální vymáhání ekonomicky neúnosné.

1.2 Proč stávající řešení nedostačují

Rámce decentralizované identity (DID) [2] poskytují kryptografické mechanismy pro sebevládní správu identity, ale zaměřují se primárně na ověřování identity bez řešení širší otázky behaviorální reputace.

Soulbound tokeny (SBT) [3] zachycují poznatek, že reputace je nepřenositelná, ale spoléhají na blockchainovou infrastrukturu s omezeními škálovatelnosti a neřeší ekonomické pobídky řídicí zadávání informací. Koncepty jako meritové tokeny (např. *Liberland*) sdílejí podobnou filosofii, ale zůstávají vázány na konkrétní jurisdikční rámce.

Decentralizované autonomní organizace (DAO) [4] implementují správu prostřednictvím chytrých kontraktů, ale replikují plutokratickou dynamiku, kde vliv je úměrný kapitálu. Kvadratické hlasování [5] tento problém částečně zmírňuje, ale omezuje praktické přijetí. DAO navíc čelí fundamentálnímu *oracle problému*: chytré kontrakty nemohou spolehlivě ověřovat stavy reálného světa bez důvěryhodného externího zdroje, a tento problém nemá obecné řešení v rámci blockchainové architektury.

Žádný existující systém nekombinuje decentralizaci, odolnost vůči cenzuře, pseudonymitu, ověřitelné náklady vstupu a emergentní konsenzus.

1.3 Příspěvek tohoto článku

Článek předkládá následující příspěvky:

1. Definice **reputační sociální sítě (RSN)**, decentralizovaného protokolu rozšiřujícího rámec DID o podporu bilaterální výměny reputačních informací.
2. **Nedeterministický protokol výběru ověřovatelů** založený na konzistentním hashování [6].
3. **Princip drahého radikalismu**, který oceňuje tvrzení podle jejich vzdálenosti od síťového konsenzu prostřednictvím tří kumulativních nákladových kanálů.
4. **Model reputační autority** s asymetrickými pobídkami, kde náklady na endorsování nepravdy katastroficky převyšují výnosy z endorsování pravdy.
5. **Postupná migrační cesta** prostřednictvím paralelní fiskální infrastruktury.

2 Konstrukční principy

Architektura RSN je omezena pěti nepřekročitelnými konstrukčními principy.

Kontinuita a evoluce. Systém koexistuje se stávajícími institucemi během přechodného období neurčité délky. Přechod musí být reverzibilní v každé fázi.

Dobrovolnost a odpovědnost. Účast je dobrovolná, ale dobrovolnost je spojena s odpovědností: účastník, který převezme kontrolu nad institucionální funkcí, současně přebírá povinnosti, které ji doprovázejí.

Diverzita a kulturní neutralita. Konsenzus vzniká z bilaterálních interakcí mezi účastníky, nikoli z přednastavených pravidel vnucených tvůrci systému.

Odolnost a rezistence vůči cenzuře. Náklady na cenzurování sítě musí převýšit náklady na její tolerování. Pouze plný totalitarismus — za zničující politické a ekonomické náklady — může systém potlačit.

Konsenzus a vynucování. Systém zahrnuje lidské sklony k malichernosti, zlovůli a touze po odplatě jako nosné prvky sociální architektury. Protiprávní jednání není zakázáno; je oceněno.

3 Přehled systému

3.1 Reputační sociální síť

RSN je decentralizovaná peer-to-peer komunikační vrstva, v níž účastníci vyměňují ověřitelné informace o chování v reálném světě. Její určující vlastnosti jsou: decentralizovaná a necenzurovatelná infrastruktura; pseudonymní účast prostřednictvím DID; asymetrická nákladová struktura (čtení je levné, zápis je drahý); kryptografická ověřitelnost; a **podpora standardů** pro strojově zpracovatelné informace šířené v síti, pro služby poskytované autoritami (tvorba tvrzení, endorsace, svědecká služba) a pro formát policy včetně pravidel vyhodnocování reputace protistrany a posuzování rizika nesouladu politik (deklarovaných i skutečných).

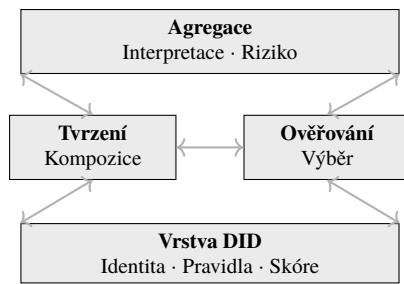
3.2 Architektonické komponenty

RSN sestává ze čtyř primárních komponent (obr. 1):

1. **Vrstva DID.** Identity účastníků s deklarovanými pravidly, reputačními metadaty a síťovým směrováním.
2. **Protokol tvrzení.** Strukturovaný formát pro publikování assertions o událostech reálného světa.
3. **Ověřovací síť.** Decentralizovaný protokol pro přidělování ověřovatelů pomocí konzistentního ha-

shování.

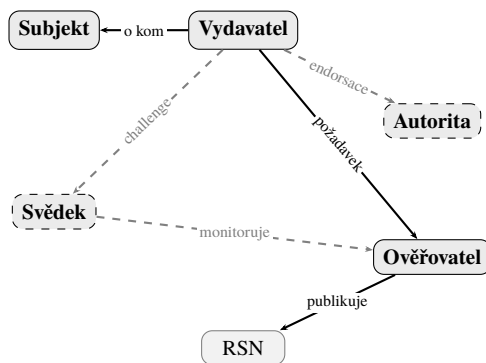
4. **Vrstva agregace reputace.** Služby produkující lidsky čitelné reputační souhrny.



Obrázek 1: Architektura RSN — čtyřvrstvá hierarchie.

3.3 Role účastníků

Ověřovací transakce zahrnuje až šest různých DID rolí (obr. 2): **Vydavatel** (Issuer, DID_I , vytváří a podává tvrzení), **Subjekt** (Subject, DID_S , DID, o kterém tvrzení hovoří — může se shodovat s Vydavatelem), **Autorita** (DID_A , endoruje tvrzení za poplatek; může nabízet i svědeckou službu — *volitelná*), **Svěddek** ($DID_{W_{1..n}}$, incognito monitor poctivosti ověřovatele prostřednictvím challenge kódů — *volitelný*), **Ověřovatel** (DID_V , algoritmicky vybrán k publikaci tvrzení) a **RSN** (sít, kam jsou ověřená tvrzení publikována). Jakákoli role může být delegována na jiné DID (sekce 7.4). Autorita běžně spojuje endorovací se svědeckou službou, ale obě funkce jsou logicky nezávislé.



Obrázek 2: Role DID v ověřovací transakci. Čárkované = volitelné (Autorita, Svědek).

3.4 Nezkorumpovatelnost: čtyři síly

Nezkorumpovatelnost RSN nevychází z jediného mechanismu, ale ze čtyř souběžně působících sil. Žádná z nich není sama o sobě dostatečná; teprve jejich kombinace činí pokus o korupci ekonomicky neracionálním.

Nepředvídatelný cíl. Ověřovatel pro každé tvrzení je vybrán nedeterministicky prostřednictvím konzis-

tentního hashování (sekce 5.3). Útočník nemůže předem cílit konkrétního ověřovatele k uplacení, protože identita ověřovatele je funkcí obsahu tvrzení a předchozích iterací, nikoli volby vydavatele.

Reputační páka — pomalý růst, rychlá ztráta. Reputaci lze získat pouze inkrementálně, prostřednictvím soustavného konzistentního chování. Lze ji však ztratit katastroficky jediným podvodem (sekce 6.2). Tato asymetrie znamená, že roky budované reputace mohou být zničeny jednou nečestnou endorací; optimální strategií zůstává odmítat podezřelá tvrzení.

Veřejný závazek. Každý držitel DID veřejně deklaruje svou policy — strojově čitelný soubor pravidel, podle kterých se zavazuje jednat. Odchyłka deklarace od skutečného chování je detekovatelná a oceněna jako reputační prohřešek závažnější než původní porušení (sekce 7.3). Pokrytectví je tedy nákladnější než přímá nečestnost.

Mřížková asymetrie nákladů útoku. Náklady na cenzurování nebo destabilizaci sítě rostou nelineárně s velikostí a hustotou sítě, zatímco náklady na její tolerování zůstávají konstantní. Aby se cenzura vyplatila, musel by ji centralizovaný aktér uplatnit napříč celou sítí — což vyžaduje opatření neúměrná jakémukoli přínosu (sekce 10).

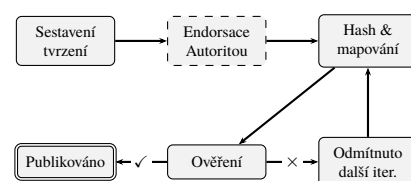
4 Model decentralizované identity

4.1 DID se speciálními vlastnostmi

RSN rozšiřuje specifikaci W3C DID Core [2] o: **Deklarovaná pravidla** (strojově čitelné behaviorální závazky), **Reputační metadata** (agregované behaviorální skóre) a **Síťové směřování** (měnitelný onion gateway oddělený od stabilní pozice na kruhu).

4.2 Životní cyklus tvrzení

Tvrzení prochází šesti fázemi (obr. 3): kompozice, volitelná endorace Autoritou, výběr ověřovatele přes konzistentní hashování, rozhodnutí o ověření (přijetí nebo odmítnutí s iterací), publikace a aktualizace reputace všech stran.



Obrázek 3: Životní cyklus tvrzení s iterační smyčkou.

4.3 Vztah k W3C DID Core

Model identity RSN je vlastní nadmnožinou specifikace W3C DID Core [2]. Všechny RSN DID jsou platnými W3C DID. RSN-specifická rozšíření jsou kódována jako vlastnosti DID dokumentu definované ve vyhrazené specifikaci DID metody, kompatibilní se stávající infrastrukturou jako ION [7] a Ceramic [8].

5 Ověřování a propagace informací

5.1 Náklady na vstup informací

Klíčovým ekonomickým principem RSN je asymetrie mezi čtením a zápisem. Čtení reputačních dat se blíží nulovým marginálním nákladům pro účastníky, kteří jsou součástí DID sítě a mají přístup k informacím odpovídající jejich reputaci — nově přichází si musí postupně zasloužit širší přístup (viz anti-leeching mechanismus). Zápis — chápáno jako trvalé zhmotnění reputace do sítě, nikoli jako jednorázový technický akt — vyžaduje ověřitelnou kumulativní investici ve třech dimenzích: **čas** (roky života strávené konzistentním chováním, splněními závazky a vybudovanými vztahy), **energie** (úsilí vynaložené na čestné jednání, péči o partnerské vazby a dlouhodobou důvěryhodnost) a **peníze** (investice do vlastního jména — profesního rozvoje, kvality dodávané práce, nápravy způsobených škod). Reputaci nelze zakoupit okamžitě — je výsledkem celoživotní akumulace, kterou systém pouze zviditelňuje a činí přenositelnou napříč kontexty. Jednorázové technické náklady protokolu (kryptografické podpisy, poplatky ověřovatelům) jsou ve srovnání s touto investicí zanedbatelné.

5.2 Sociální graf a hloubka kontaktů

RSN je v první řadě sociální síť: každé DID si přidává do svých kontaktů známé, kteří toto propojení povolí. Ti mají vlastní kontakty a ti další. Do algoritmického vyhledávání ověřovatelů vstupuje konfigurovatelná hloubka h navázaných kontaktů (např. $h = 3$: přímé kontakty, jejich kontakty a kontakty kontaktů). Tato architektura nevyžaduje jeden globální blockchain pro celou planetu — naopak přirozeně preferuje vznik komunit/clusterů s přesahy do dalších komunit. Každý účastník DID sítě musí mít publikovanou svou **policy** — strojově čitelný soubor pravidel, na základě kterých vyhodnocuje přichozí požadavky a které musí dodržovat. Porušení vlastní deklarované policy je zaznamenáno v síti jako negativní artefakt.

5.3 Algoritmický výběr ověřovatelů

Ověřovací protokol využívá konzistentní hashování [6] (obr. 4). Ověřování je placená služba: ověřovatelé pracují za poplatek, čímž vzniká trh, kde konkurence řídí ceny, rychlost a spolehlivost.

Krok 1. Dokument tvrzení je zřetěžen s výsledkem hashe z předchozí iterace (nebo $\emptyset$ při první iteraci) a hashován:

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

Algoritmus musí zahrnovat *kompletní cestu* všech předchozích požadavků a odpovědí — nikoli pouze hash předchozí iterace. Kompletní odpověď každého ověřovatele (přijetí, odmítnutí, kotovaná cena, důvod) je připojena k rostoucímu dokumentu a je ověřitelná kryptografickými podpisy v každém kroku.

Krok 2. Hash je mapován na N pozic na konzistentním hashovacím kruhu, rovnoměrně rozložených (např. pro $N = 4$: $+0^\circ, +90^\circ, +180^\circ, +270^\circ$). Z každé pozice vyhledávání ve směru hodinových ručiček vybere nejbližší DID jako kandidáta na ověřovatele (obr. 5). N je proměnný parametr závislý na procentu aktivních DID, denní době nebo historické odezvě sítě.

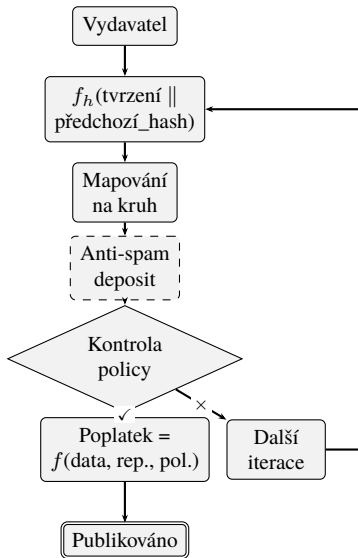
Krok 3. Ověřovatel přijme (publikuje, sází reputaci) nebo odmítne (vrací se ke kroku 1 s hashem odmítnutí). Když node neodpovídá navzdory deklarovanému online statusu, další požadavek musí zahrnovat všechny odpovědi od všech N předchozích kandidátů.

Anti-leeching. Cílové DID si mohou stanovit poplatky nebo přístupová omezení pro dotazy od nových DID s nízkou reputací. Tento graduální mechanismus (nikoli binární) nutí nováčky budovat reputaci prostřednictvím skutečné aktivity v síti.

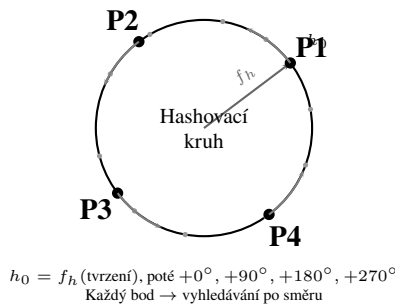
Každé odmítnutí přidává k dokumentu tvrzení zamítavou odpověď ověřovatele (včetně důvodů a podmínek), čímž rozšiřuje jeho obsah. Z rozšířeného dokumentu se nedeterministicky vypočte nový hash, mapující na jinou pozici na kruhu a vybírající jiného ověřovatele. Dokumentace celé cesty je povinná — vydavatel nemůže predikovat ani ovlivnit výběr dalšího ověřovatele. Pokud ověřovatel ignoruje požadavek navzdory své deklarované policy, svědci (jsou-li přítomni) toto zaznamenají a vydavatel může při finálním publikování přiložit svědecké důkazy o porušení.

5.4 Protokol svědka (Witness Protocol)

Role **svědka** (Witness) zajišťuje incognito odpovědnost za poctivost ověřovatele prostřednictvím kryptografického protokolu challenge kódů:



Obrázek 4: Protokol výběru ověřovatelů. Anti-spam deposit je volitelný a může být vratný. Finální poplatek se platí pouze při přijetí.



Obrázek 5: Vícenásobný výběr ($N=4$). Hash h_0 určí offset; 4 body rovnoměrně rozložené od h_0 .

Krok W1. Žadatel podepíše ověřovací požadavek a pošle ho N_w svědkům — kontaktům ze své sociální sítě nebo specializovaným poskytovatelům svědecké služby za poplatek.

Krok W2. Každý svědek w_i podepíše celý podepsaný požadavek, ponechá si originální podpis σ_i a vypočte challenge kód $c_i = h(\sigma_i)$. Challenge kód je připojen k požadavku.

Krok W3. Požadavek s N_w challenge kódy je odeslán ověřovateli. Ověřovatel vidí kódy, ale *nemůže určit*, kdo jsou svědci ani zda kódy odpovídají skutečným podpisům.

Krok W4 (pochtivý ověřovatel). Pokud ověřovatel odpoví v souladu se svou deklarovanou politikou, challenge kódy zůstávají neprůhledné. Svědci nemusí být odhaleni. Žádná doplňková data se nepublikují.

Krok W5 (porušení politiky). Pokud ověřovatel poruší svou politiku (ignoruje požadavek, odpovídá nekonzistentně), žadatel drží originální podpisy

svědků σ_i . Ty mohou být publikovány jako doprovodná data: kdokoli si může ověřit $c_i = h(\sigma_i)$, čímž prokáže přítomnost svědka. Žadatel může publikovat nezávisle — ověřovatel již podepsal challenge kódy ve své odpovědi.

Vlastnost bluffu. Žadatel může za některé nebo všechny challenge kódy substituovat náhodné hodnoty. Ověřovatel nemůže rozlišit skutečné kódy (podložené vysoce reputovanými autoritami) od šumu. Tato *nejistota* je vynucovací mechanismus: každý požadavek nese riziko, že respektovaná autorita sleduje incognito. Náklady na udržování tohoto tlaku jsou téměř nulové (generování náhodných čísel), zatímco potenciální náklady nečestnosti pro ověřovatele jsou katastrofické. Pochtivé chování je motivováno i bez skutečných svědků.

Autorita jako svědek. Autorita, která endorсуje tvrzení, může spojit svou službu se svědeckou: „Endorsuji tvé tvrzení a zároveň budu incognito svědkem při ověřování.“ Jde o přirozený obchodní model — Autorita již má kontext. Obě role jsou však logicky nezávislé.

5.5 Princip drahého radikalismu

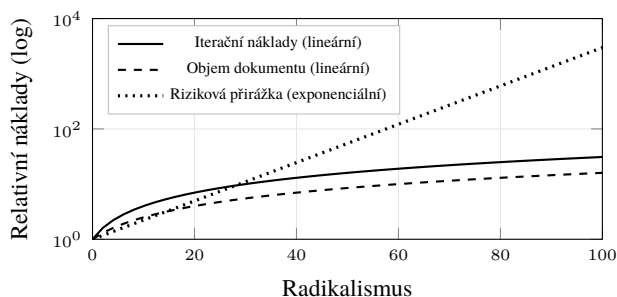
Tři nákladové kanály se kumulují současně (obr. 6):

Kanál 1: Iterační náklady. Každé odmítnutí vynucuje novou iteraci spotřebovávající čas a zdroje. Lineární růst.

Kanál 2: Narůstání objemu dokumentu. Každá iterace přidává kompletní odpověď ověřovatele do dokumentu tvrzení. Růst je lineární, ale se základním offsetem: počáteční datová zátěž (obsah tvrzení, endorсace autority, kryptografické podpisy) má již nenulovou velikost B_0 . Celková velikost po k iteracích: $S(k) = B_0 + k \cdot \Delta$, kde Δ je průměrná velikost odpovědi.

Kanál 3: Riziková přirážka ověřovatele. Riziko je subjektivní. Ověřovatel posuzuje, zda deklarované politiky žádajícího DID jsou v rozporu s jeho vlastními obchodními, sociálními nebo politickými zájmy. Přirážka může eskalovat exponenciálně se subjektivní vzdáleností od ověřovatelova „ideálu“: $P(d) = \alpha \cdot e^{\beta d}$, kde d je subjektivní metrika vzdálenosti. Za osobní hranici nepřijatelnosti může ověřovatel zcela odmítnout.

Zásadní je, že se nejedná o cenzuru. Žádné tvrzení není zakázáno. Systém oceňuje riziko (tabulka 1).



Obrázek 6: Eskalace nákladů ve třech kanálech. Riziková přírážka dominuje při vysokém radikalismu.

Tabulka 1: Porovnání nákladů podle typu tvrzení.

Typ	Iter.	Dok.	Popl.	Celkem
Věrohodné	$k_{\min}$	B_0	$P_{\min}$	Nízké
Kontroverzní	k_{med}	$B_0 + k\Delta$	$\alpha e^{\beta d}$	Střední
Radikální	$k_{\max}$	$\gg B_0$	$\gg P_{\min}$	Velmi vysoké
Podvodné	$\rightarrow \infty$	—	—	Nepublikovatelné

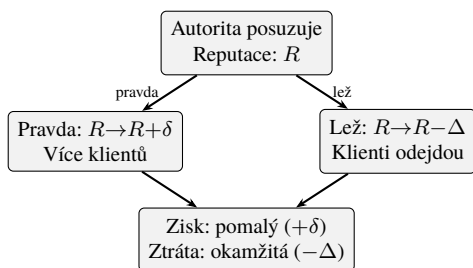
6 Reputace a hodnocení rizik

6.1 Model akumulace reputace

Reputace vykazuje tři vlastnosti: **pomalá akumulace** (inkrementální růst prostřednictvím konzistentního chování), **rapidní destrukce** (jediný podvod může katastroficky snížit skóre) a **individuální vyhodnocení** (každá konzumující strana může aplikovat vlastní agregační funkci).

6.2 Reputační Autority

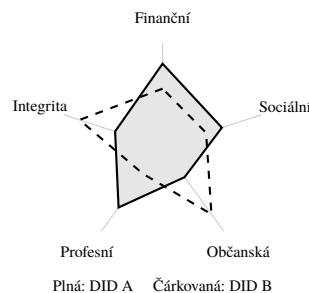
Reputační Autorita přezkoumává tvrzení a, je-li přesvědčena, spolupodepisuje je — sází vlastní reputaci (obr. 7). Asymetrie je záměrná: získávání reputace je pomalé (inkrementální růst $+\delta$ za poctivou endorsaci), zatímco její ztráta je katastrofická (řádově $-\Delta \gg \delta$ za nepravdivou endorsaci; ilustrativně např. $+2\%$ vs. -70%). Optimální strategií je vždy odmítnat podezřelá tvrzení. Konkrétní hodnoty δ a Δ jsou parametry systému.



Obrázek 7: Reputační Autorita — asymetrické po-bídky.

6.3 Vícerozměrná reputace

Reputace není skalár, ale vektor napříč více dimenzemi: finanční spolehlivost, osobní integrita, profesní kompetence, občanská angažovanost a další (obr. 8). Různí poskytovatelé hodnocení promítají tento vektor odlišně v závislosti na kontextu — věřitel upřednostňuje finanční spolehlivost, zaměstnavatel profesní kompetenci, soused občanské chování. Neexistuje jediné “správné” reputační skóre; pouze perspektivy.



Obrázek 8: Vícerozměrné reputační vektory. Různé DID vykazují různé profily napříč dimenzemi.

6.4 Demokratizace hodnocení rizik

RSN demokratizuje systematické hodnocení rizik — schopnost v současnosti soustředěnou ve finančních institucích, ale aplikovatelnou daleko za hranice bankovníctví. Průmyslové celky hodnotící spolehlivost dodavatelů, pojišťovny oceňující behaviorální riziko, due diligence pro fúze a akvizice, odhady životnosti zařízení ve výrobě — všude, kde je třeba hodnotit riziko protistrany, RSN poskytuje decentralizovanou, tržně řízenou alternativu. Trh interpretačních služeb překládá surová vícerozměrná reputační data do prakticky využitelných souhrnů, čímž se hodnocení protistrany stává dostupným pro jakéhokoli účastníka za marginální náklady.

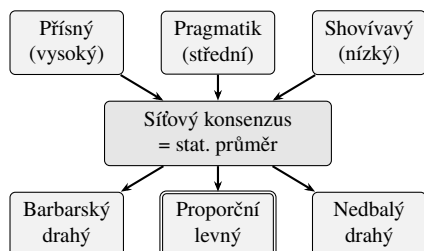
7 Konsenzus a řešení sporů

7.1 Model decentralizované spravedlnosti

RSN přerámovává spravedlnost jako problém bilaterálního vyjednávání. Hrozba trvalého, ověřitelného reputačního poškození je účinnějším odstrašujícím prostředkem než soudní řízení, které si poškozená strana nemůže dovolit.

7.2 Emergentní konsenzus

Každý účastník udržuje osobní práh satisfakce. Agregátní konsenzus sítě emerguje jako statistický průměr tisíců bilaterálních vyjednávání (obr. 9). Reakce výrazně překračující konsenzus (barbarická) je drahá na publikaci. Reakce blízká konsenzu (proporcionální) je levná. Konsenzus není pravidlo — je to cenový signál.



Obrázek 9: Emergentní konsenzus z individuálních prahů satisfakce.

7.3 Kalibrace trestů

Každý Držitel DID veřejně deklaruje reakce na konkrétní kategorie protiprávního jednání. Nepřiměřeně přísné nebo mírné deklarace přitahují negativní reputační signály. Proporcionální deklarace jsou přijímány bez třenic — samokalibrovací systém trestů.

Deklarace konsenzu jsou samy předmětem detekce pokrytectví: deklarativní přihlášení ke konsenzuální pozici při současném nekonzistentním chování představuje reputační prohřešek závažnější než samotná odchylka, neboť prokazuje záměrný podvod.

7.4 Delegation

Veškeré činnosti v rámci DID — s jedinou výjimkou — mohou být delegovány na jiné DID. **Roli Subjektu, tedy DID, o jehož chování tvrzení vypovídá, delegovat nelze; je nepřevoditelně vázána na nositele identity, kterého se tvrzení týká.** Ostatní aktivní role — Vydavatel, Autorita, Svědek, Ověřovatel — lze převést na určený delegátní DID, ať už jde o ověřování, podání tvrzení, účast na konsenzu nebo řešení sporů. Delegation je kdykoli odvolatelná. To umožňuje specializaci (např. profesionální ověřovací služby), přičemž Držitel si zachovává konečnou kontrolu a odpovědnost. Delegation se uplatňuje v celém systému a je nezbytná pro škálovatelnost.

7.5 Od individuální morálky k emergentní sociální smlouvě

Deklarovaná politika (policy) každého DID představuje formalizaci individuální morálky: co Držitel považuje za přijatelné, jak reaguje na konkrétní chování, co vyžaduje od protistran. Tyto politiky nejsou vnučeny tvůrcem systému — jsou voleny každým účastníkem a vyjádřeny ve strojově čitelné formě.

Tato formalizace umožňuje třístupňovou emergenci. Zaprvé, individuální morálka je kódována jako **politika** (policy) — soubor deklarovaných pravidel, prahů a reakčních funkcí, k jejichž dodržování se DID zavazuje. Zadruhé, agregát všech politik napříč sítí produkuje **emergentní etiku** — statisticky pozorovatelné normy, které žádný jednotlivý účastník nenavrhl, ale které vznikají z interakce tisíců individuálních morálních pozic [9]. Zatřetí, tato emergentní etika, vyjádřená jako sdílené behaviorální normy vynucované prostřednictvím bilaterálních cenových signálů, představuje **měřitelnou sociální smlouvu** — nikoli teoretický konstrukt, který nikdo nepodepsal [10], ale empiricky pozorovatelný soubor pravidel podložený skutečným chováním.

Tento proces odráží poznatky teorie morálních základů (Moral Foundations Theory) [11]: lidská morálka je intuitivní, pluralitní a kulturně proměnlivá. RSN nevyžaduje morální konsenzus jako vstup; produkuje behaviorální konsenzus jako výstup. Výsledná sociální smlouva není statická — vyvíjí se s tím, jak účastníci vstupují, odcházejí a upravují své politiky v reakci na zpětnou vazbu sítě. Na rozdíl od klasické teorie společenské smlouvy je tato smlouva odvolatelná, pozorovatelná a vymahatelná bez suveréna.

8 Ekonomický model

Předcházející sekce popisovaly nástroj — ověřovací mechanismy RSN, nákladovou strukturu a emergentní konsenzus. Tato sekce popisuje metodiku aplikace tohoto nástroje na fiskální a správní přechod. Nástroj je univerzální; níže popsána metodika je jednou z možných aplikací.

8.1 Struktura pobídek

Reputace jako kapitál vytváří přímé pobídky pro poctivé chování. V běžném provozu účastníci budují reputaci přirozeně prostřednictvím každodenních transakcí a splněných závazků. Primárním výdajem jsou *negativní* tvrzení — zaznamenávání újmy způsobené jinými. Tato asymetrie motivuje užitečné, spolehlivé

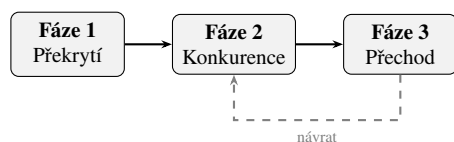
chování: poctivost nestojí nic navíc, zatímco škodlivost vytváří dokumentovanou stopu, za jejíž zachování budou ostatní platit. Pokrytectví — deklarování pravidel bez jejich dodržování — je nejnákladnějším režimem selhání, protože prokazuje záměrný podvod.

8.2 Paralelní fiskální systém

Tři komponenty umožňují konkurenční tlak: (1) **Jednoduchá daň** — jednotná proporcionální sazba bez výjimek, zpočátku marginálně pod efektivní sazbou stávajícího systému; (2) **Elektronická evidence výdajů (ESR)** — obrácení českého modelu EET tak, aby občané sledovali státní výdaje; (3) **Občany řízené přidělování daní** — v prvním roce řádově nižší jednotky procent, po deseti letech podle míry adopce kdekoli od nejnižších desítek procent až po kompletní migraci na občansky řízený systém. Konkrétní tempo závisí na rychlosti nástupu volnotržních alternativ ke státním službám a na ochotě státu spolupracovat na přechodu; funkce času nemusí být lineární a není žádný důvod předem omezovat horní hranici toho, kam může adopce dojít.

9 Migrační cesta

Migrace probíhá ve třech fázích (obr. 10): **Fáze 1: Překrytí** (RSN jako informační vrstva, stát je jediným poskytovatelem), **Fáze 2: Konkurence** (RSN poskytuje funkční alternativy, duální využití) a **Fáze 3: Přechod** (RSN předčí státní ekvivalenty, dobrovolná migrace). Přechod je reverzibilní v každé fázi.



Obrázek 10: Třífázová migrace — reverzibilní v každé fázi.

Primárním tlakovým mechanismem je fiskální: když podmínění daňoví poplatníci dosáhnou “ekonomicky signifikantní menšiny X ” — skupiny dostatečně velké, aby represe proti ní způsobila nemalé ekonomické škody a občanská neposlušnost se stala věrohodnou hrozbou — stát vstupuje do vyjednávání. Ilustrativně používáme $X \approx 15\%$ HDP, ale skutečný práh závisí na konkrétní ekonomice.

10 Bezpečnostní analýza

Uvažujeme pět kategorií protivníků: jednotliví zlí aktéři, organizované skupiny, korporátní protivníci, státní protivníci a protivníci na úrovni protokolu.

Odolnost vůči Sybil útokům [12]. Budování reputace vyžaduje soustavnou, ověřitelnou interakci. Náklady na úspěšný Sybil útok rostou lineárně s počtem falešných identit a kvadraticky s cílovou úrovní reputace. Provoz více DID paralelně je možný, ale záměrně nákladný — každá identita musí nezávisle akumulovat reputaci prostřednictvím skutečné aktivity. Ve svobodných společnostech tyto náklady odrazují od zneužívání; v diktaturách se paralelní DID stávají nástrojem přežití umožňujícím kompartmentalizovaný odpor, koordinaci podzemních sítí a bezpečnější navigaci černým trhem.

Obrana proti koluzi. Vzory vzájemného endorsování mezi uzavřenými skupinami jsou detekovatelné prostřednictvím analýzy sociálního grafu. Reputační agregační funkce diskontují tvrzení z těsně propojených zdrojů.

Státní protivník. Onion směřování, absence centralizované infrastruktury a distribuce role Ověřovatele napříč účastnickou základnou zajišťují, že potlačení vyžaduje opatření neúměrná jakémukoli přínosu.

Soukromí vs. odpovědnost. Pseudonymita — střední řešení mezi anonymitou a odhalením identity — umožňuje DID akumulovat smysluplnou reputaci bez odhalení reálné identity Držitele.

11 Aspekty ochrany soukromí

Model ochrany soukromí RSN je postaven na pseudonymitě. Držitel kontroluje míru odhalení identity: minimální (čistý pseudonym), selektivní (propojení konkrétních pověření) nebo plné (asociace s právní identitou). Publikovaná tvrzení jsou trvalá — systém podporuje kontextovou opravu, nikoli výmaz. Držitel může opustit kompromitovaný DID a začít znovu, přičemž se vzdá nashromážděné reputace.

12 Související práce

Specifikace W3C DID Core [2] a Ceramic Network [8] poskytují základ identity. EigenTrust [13] demonstroval distribuovanou agregaci reputace bez centrální autority. SBT [3] zavedly nepřenositelné sociální tokeny. RSN se liší důrazem na ekonomické náklady jako filtr kvality a mechanismem pro oceňování radikalismu.

DAO [4] a kvadratické hlasování [5] prokázaly proveditelnost decentralizované správy. RSN odvozuje konsenzus z bilaterálních cenových vyjednávání namísto hlasování.

Návrh čerpá z anarchokapitalistické teorie [14, 15] pro soukromé poskytování služeb, ale odchyluje se ve dvou kritických ohledech: navrhuje design zahrnující zlovůli a touhu po odplatě namísto předpokladu racionality a navrhuje postupný přechod namísto revoluce. Koncept emergentních společenských smluv má předchůdce v Hayekově teorii spontánního řádu [16].

Anarcho-agorismus. RSN sdílí významný společný základ s agoristickou kontra-ekonomikou [17] — zejména důraz na budování paralelních institucí a dobrovolnou směnu. Agorismus však obvykle předpokládá racionální vlastní zájem jako dostatečný koordináční mechanismus a často postrádá konkrétní migrační cestu od stávajících státních struktur. RSN explicitně zahrnuje neracionální behaviorální tendence a poskytuje mechanismus fiskálního tlaku pro postupný přechod.

Meritokracie. RSN může představovat první funkční popis toho, jak může meritokracie [18] emergovat jako systémová vlastnost namísto sloganu. Tradiční meritokratické systémy selhávají, protože vyžadují centrální autoritu k definování a vynucování “zásluh”. V RSN zásluhy emergují z bilaterálních hodnocení: ti, kdo dodávají hodnotu, akumulují reputaci; žádný výbor nerozhoduje, kdo má zásluhy.

Vlastnictví jako privilegium. RSN se zásadně odchyluje od anarchokapitalistického a rakouského pojetí vlastnických práv jako přirozených a absolutních. V rámci RSN je vlastnictví *privilegium* — sociální uznání, které může být v krajních případech odňato komunitou, když účastník zásadně poruší sdílené normy (zrada, odmítnutí bránit komunitu v existenční krizi, systematické vykořisťování). Nejedná se o státní vyvlastnění, ale o odnětí sociálního uznání sítí bilaterálních vztahů.

13 Diskuse a omezení

Studený start. Hodnota RSN závisí na síťových efektech; raní adoptéři čelí omezené hodnotě, dokud participace nedosáhne prahové hodnoty. Nicméně i od raných fází slouží DID síť jako užitečný doplňkový zdroj informací. Rané vyhodnocení reputace a autority se předpokládá postupně s narůstající sofistikovaností.

Anti-leeching a řízení přístupu. Cílové DID mohou uvalovat graduální poplatky a přístupová omezení na dotazy od DID s nízkou reputací. Nejde o binární

bránu, ale o plynulou škálu: čím nižší reputace dotazujícího DID, tím méně informací obdrží, déle čeká a více platí. Tento mechanismus motivuje skutečnou participaci oproti pasivní konzumaci.

Nerovnost přístupu. Náklady na publikování tvrzení mohou filtrovat legitimní stížnosti ekonomicky znevýhodněných účastníků. Mitigace: každý účastník současně slouží jako potenciální ověřovatel (nebo tuto roli deleguje) a pobírá poplatky za ověřování. V dostatečném časovém horizontu by neradikální účastník měl dosáhnout přibližné finanční neutrality — příjmy z ověřování přibližně kompenzují náklady na publikování. Jde o statistický předpoklad, nikoli garanci.

Nerovnost reputace. Raní adoptéři akumulují výhody, které mohou vytvářet bariéry pro pozdější příchozí. Hodnocení reputace však provádějí třetí strany — poskytovatelé hodnocení, kteří mohou ve svých agregačních algoritmech zmírňovat výhodu prvního hybatele. Být první s dobrou reputací je legitimní komparativní ekonomická výhoda — a to je záměr.

Otevřené otázky. Optimální nákladové funkce, standardy agregace, správa protokolu a interakce s uměle generovanými syntetickými reputačními daty zůstávají oblastmi pro budoucí výzkum.

Tento článek netvrdí, že RSN přinese optimální výsledky za všech okolností. Tvrdí, že RSN představuje *proveditelnou* alternativu — technicky implementovatelnou, ekonomicky sebeudržitelnou a sociálně kompatibilní s lidskými behaviorálními tendencemi tak, jaké skutečně jsou.

14 Závěr

Tento článek představil reputační sociální síť, decentralizovaný protokol umožňující pseudonymní, ověřitelnou výměnu reputačních informací. Princip drahého radikalismu zajišťuje, že podvodná tvrzení jsou vytlačena cenou bez cenzury. Navrhovaná migrační cesta umožňuje postupný, reverzibilní přechod od stávajících institucí. Design zahrnuje lidskou přirozenost takovou, jaká je — včetně malichernosti, zlovůle a touhy po odplatě — namísto toho, aby vyžadoval ideologickou transformaci. Výsledkem není utopie, ale systém, v němž je spravedlnost dostupná, reputace je zasloužená a náklady protiprávního jednání nese strana, která je způsobila.

Reference

- [1] Česká republika, “Zákon č. 549/1991 sb., o soudních poplatcích, ve znění pozdějších předpisů,”

- 1991, sazebník soudních poplatků; náklady řízení dle zák. č. 99/1963 Sb. (OSŘ) a vyhl. č. 177/1996 Sb. (advokátní tarif).
- [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.