Decentralizált reputációs hálózat: Keretrendszer a társadalom természetes szerveződéséhez

Pavel Kudrna
Prága, Csehország
Vázlat v1 — 2026. március

Abstract

Az igazságérzet—az a meggyőződés, hogy a sérelmek jóvátételre kerülnek és az érdem jutalmat nyer—a társadalom legerősebb összetartó ereje. Amikor a kormányzás központosított intézményei nem képesek biztosítani ezt az érzetet, mert egy jog érvényesítésének költsége meghaladja magának a jognak az értékét, a társadalmi kohézió erodálódik. A jelenlegi intézményi struktúrák a viták jelentős osztályát ugyanolyan szisztematikusan képtelenek megoldani, ahogy a központi tervezés képtelen az erőforrások elosztására: információs aszimmetria, hiányzó visszacsatolási hurkok, valamint a döntéshozóknak a döntéseik következményeitől való elszakadása révén. Ez a tanulmány egy reputációs közösségi hálózatot (Reputation Social Network, RSN) mutat be: egy decentralizált, megvesztegethetetlen, cenzúrának ellenálló kommunikációs réteget, amely decentralizált azonosítókra (Decentralized Identifiers, DIDs) épül, és lehetővé teszi álnéven fellépő résztvevők számára, hogy valós viselkedésről szóló reputációs információt tegyenek közzé, ellenőrizzenek és fogyasszanak. Az alapmechanizmus három tervezési elven nyugszik: (1) egy aszimmetrikus költségszerkezet, amelyben a reputációs adatok olvasása olcsó, de az írás ellenőrizhető ráfordítást igényel; (2) egy nemdeterminisztikus ellenőrző-kiválasztási protokoll, amely konzisztens hasításon alapul, és a radikális állításokat egyre növekvő iterációs költségeken keresztül árazza be; valamint (3) egy piaci alapú reputációs tekintélymodell, amelyben a magánellenőrök felhalmozott reputációjukat teszik fel az általuk jóváhagyott állítások pontosságára. Az így létrejövő architektúra központi koordináció nélkül hoz létre emergens meritokráciát, és fokozatos, visszafordítható átállási utat tesz lehetővé a jelenlegi, állam által igazgatott rendszerekből.

1 Bevezetés

1.1 A központosított bizalom problémája

A modern kormányzás egy alapvető feltevésen nyugszik: hogy a központosított intézmények nagy léptékben képesek közvetíteni a bizalmat idegenek között. A bíróságok elbírálják a vitákat. A nyilvántartások igazolják a tulajdonjogot. A szabályozó testületek betartatják a szabványokat. Ezeket az intézményeket egy olyan korban tervezték, amikor az információ szűkös volt, a kommunikáció lassú, és a hatáskör központi testületre való átruházása volt az egyetlen megvalósítható koordinációs mechanizmus. A központosított kormányzás azonban ugyanazon szerkezeti okokból mond csődöt, mint a központi tervezés: információs aszimmetria, hiányzó visszacsatolási hurkok, valamint a döntéshozóknak a döntéseik következményeitől való elszakadása miatt.

A feltevés csődöt mond például akkor, amikor az intézményi közvetítés költsége meghaladja a vita értékét. Vegyünk egy bérlőt, aki felfedezi, hogy a bérelt lakása nem rendelkezik a jogszabály által előírt villamos biztonsági tanúsítvánnyal—olyan állapot, amely közvetlen életveszélyt jelent. A bérlő szerződéstől való elállási joga egyértelmű. Ám e jog bírósági úton történő érvényesítésének költsége meghaladja a kaució és a járó kártérítés pénzbeli értékét, még az esetleges törvényes kompenzációt is beleértve [1]. A racionális válasz a veszteség elviselése és a kilépés.

Ez nem egy kóros határeset. Ez az alapértelmezett tapasztalat a viták egy jelentős osztályában, amelyekben a kár valós, de a pénzbeli tét azon küszöb alá esik, amelynél az intézményi érvényesítés gazdaságilag racionálissá válik. Az eredmény egy olyan rendszer, amely szerkezetileg a rosszhiszemű szereplőknek kedvez: azok, akik ezen küszöb alatti mértékben ártanak másoknak, büntetlenül cselekedhetnek, mert az igazságszolgáltatás keresésének költsége a sérelmet elszenvedő félre hárul.

A fenti példa a szerző jogi környezetéből—a cseh kontinentális jogrendszerből—származik. Más jogi hagyományokban—precedensalapú common law, szokásjog, vegyes rendszerek—az igazságszolgáltatás más módon és más mértékben mond csődöt, a joghatóság kulturális és eljárási sajátosságaitól függően. Az olvasók valószínűleg felismernek ehhez hasonló példákat a saját környezetükből. Ami szerkezetileg egyetemes, az a minta: azok a viták, amelyeknek értéke a gazdaságilag racionális érvényesítés küszöbe alá esik, azzal végződnek, hogy a veszteséget a sérelmet elszenvedő fél viseli. Az RSN nem ígér tökéletes igazságosságot—mindössze csökkenti azt a szerkezeti előnyt, amelyet a rosszhiszemű szereplők élveznek, amikor az intézményi érvényesítés gazdaságtalan.

1.2 Miért nem elegendők a meglévő megoldások

A **decentralizált identitás (DID) keretrendszerek** [2] kriptográfiai mechanizmusokat kínálnak az önszuverén identitáskezeléshez, ám elsősorban az identitás ellenőrzésére összpontosítanak anélkül, hogy foglalkoznának a viselkedési reputáció tágabb kérdésével.

A **lélekhez kötött tokenek (Soulbound Tokens, SBTs)** [3] megragadják azt a felismerést, hogy a reputáció nem átruházható, ám blokklánc-infrastruktúrára támaszkodnak skálázhatósági korlátokkal, és nem foglalkoznak az információ bevitelét szabályozó gazdasági ösztönzőkkel. Kapcsolódó fogalmak, mint az érdemtokenek (pl. Liberland), hasonló filozófiát képviselnek, de sajátos joghatósági keretekhez maradnak kötve.

A **decentralizált autonóm szervezetek (DAOs)** [4] a kormányzást okosszerződéseken keresztül valósítják meg, ám plutokratikus dinamikát reprodukálnak, ahol a befolyás a tőkével arányos. A kvadratikus szavazás [5] részben mérsékli ezt, de korlátozza a gyakorlati elfogadhatóságot. A DAO-k szembesülnek az alapvető *orákulum-problémával* is: az okosszerződések nem képesek megbízhatóan ellenőrizni a valós állapotokat egy megbízható külső forrás nélkül, és ennek a problémának nincs általános megoldása a blokklánc-architektúrán belül.

Egyetlen meglévő rendszer sem egyesíti a decentralizációt, a cenzúrának való ellenállást, az álnevűséget, a belépés ellenőrizhető költségét és az emergens konszenzust.

1.3 Hozzájárulások

Ez a tanulmány a következő hozzájárulásokat teszi:

1. A **reputációs közösségi hálózat (RSN)** definíciója, egy decentralizált protokollé, amely a DID keretrendszert kiterjeszti a kétoldalú reputációcsere támogatására.
2. Egy **nemdeterminisztikus ellenőrzőkiválasztási protokoll**, amely konzisztens hasításon alapul [6].
3. A **drága radikalizmus elve**, amely az állításokat a hálózati konszenzustól való távolságuk szerint árazza be három egymást erősítő költségcsatornán keresztül.
4. Egy **reputábilis tekintély modell** aszimmetrikus ösztönzőkkel, amelyben a hamis jóváhagyás katasztrofálisan többe kerül, mint a legitim díjak.
5. Egy **fokozatos átállási út** párhuzamos költségvetési infrastruktúrán keresztül.

2 Tervezési elvek

Az RSN architektúráját öt nem alkuképes tervezési elv határolja be.

Folytonosság és evolúció. A rendszer határozatlan hosszúságú átmeneti időszakon át együtt él a meglévő intézményekkel. Az átmenetnek minden szakaszban visszafordíthatónak kell lennie.

Önkéntesség és felelősség. A részvétel önkéntes, de az önkéntesség felelősséggel párosul: az a résztvevő, aki átveszi az irányítást egy intézményi funkció fölött, egyúttal az azzal járó kötelezettségeket is magára vállalja.

Sokszínűség és kulturális semlegesség. A konszenzus kétoldalú interakciókból emelkedik ki, nem a rendszertervezők által előre meghatározott szabályokból.

Ellenálló képesség és cenzúrának való ellenállás. A hálózat cenzúrázásának költségének meg kell haladnia a hálózat eltűrésének költségét. Csak a teljes totalitarizmus—romboló politikai és gazdasági áron—képes elnyomni a rendszert.

Konszenzus és érvényesítés. A rendszer a kicsinyesség, a rosszindulat és a megtorlásból fakadó elégtétel emberi hajlamait teherhordó jellemzőkként építi be. A vétséget nem tiltja; beárazza.

3 A rendszer áttekintése

3.1 Reputációs közösségi hálózat

Az RSN egy decentralizált, egyenrangú felek közötti (peer-to-peer) kommunikációs réteg, amelyben a résztvevők ellenőrizhető információt cserélnek valós viselkedésről. Meghatározó tulajdonságai: decentralizált és cenzúrázhatatlan infrastruktúra; álnéven történő részvétel DID-eken keresztül; aszimmetrikus költségszerkezet (az olvasás olcsó, az írás drága); kriptográfiai ellenőrizhetőség; valamint **szabványtámogatás**—géppel olvasható formátumok a hálózaton terjedő információhoz, a tekintélyek által kínált szolgáltatásokhoz (állítás összeállítása, jóváhagyás, tanúszolgálat), valamint a szabályzatformátumhoz, amely magában foglalja az ellenfél reputációjának értékelésére és a szabályzat-eltérés (a deklarált és a tényleges viselkedés közötti) kockázatának megítélésére vonatkozó szabályokat.

3.2 Architekturális összetevők

Az RSN négy elsődleges összetevőből áll (1. ábra):

1. **DID réteg.** A résztvevők identitásai deklarált szabályokkal, reputációs metaadatokkal és hálózati útválasztással.
2. **Állítási protokoll.** Strukturált formátum a valós eseményekről szóló kijelentések közzétételére.
3. **Ellenőrző hálózat.** Decentralizált protokoll az ellenőrök kijelölésére konzisztens hasítás segítségével.
4. **Reputáció-aggregációs réteg.** Szolgáltatások, amelyek emberi olvasásra szánt reputációs összefoglalókat állítanak elő.

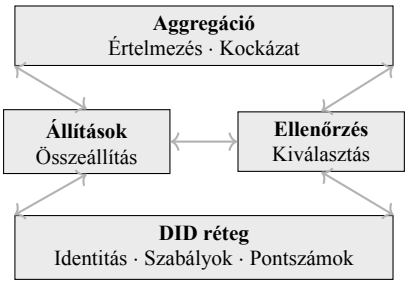

Figure 1: Az RSN négyrétegű architektúrája.

3.3 A résztvevők szerepei

Egy ellenőrzési tranzakcióban legfeljebb hat különálló DID szerep vesz részt (2. ábra): **kibocsátó** (DID_I, létrehozza és benyújtja az állítást), **alany** (DID_S, az a DID, amelyről az állítás szól—egybeeshet a kibocsátóval), **tekintély** (DID_A, díj ellenében jóváhagyja az állítást; tanúszolgálatot is kínálhat—*opcionális*), **tanú** ($DID_{W_{1..n}}$, az ellenőr becsületességének inkognitó megfigyelője kihívási kódokon keresztül—*opcionális*), **ellenőr** (DID_V, algoritmikusan kiválasztva az állítás közzétételére), valamint az **RSN** (a hálózat, ahol az ellenőrzött állítások megjelennek). Bármely szerep átruházható egy másik DID-re (7.4. szakasz). Egy tekintély gyakran a jóváhagyást tanúszolgálattal csomagolja össze, ám a két funkció logikailag független.

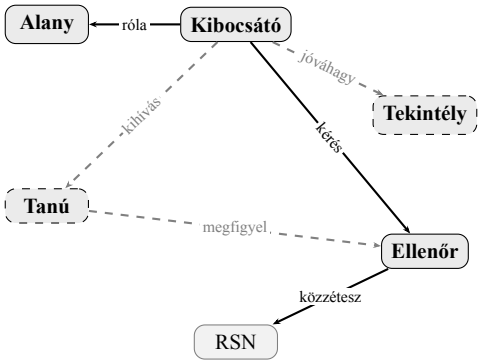

Figure 2: DID szerepek egy ellenőrzési tranzakcióban. Szaggatott = opcionális (tekintély, tanú).

3.4 Megvesztegethetetlenség: négy erő

Az RSN megvesztegethetetlensége nem egyetlen mechanizmusból fakad, hanem négy egyidejűleg ható erőből. Egyik sem elegendő önmagában; csak együttesük teszi a korrupciós kísérletet gazdaságilag irracionálissá.

Kiszámíthatatlan célpont. Az egyes állítások ellenőrét nemdeterminisztikusan, konzisztens hasítással választják ki (5.3. szakasz). A támadó nem tud előre megcélozni egy adott ellenőrt megvesztegetés céljából, mert az ellenőr kiléte az állítás tartalmának és a korábbi iterációknak a függvénye, nem a kibocsátó választásáé.

Reputációs tőkeáttétel—lassan fel, gyorsan le. A reputáció csak fokozatosan, tartósan következetes viselkedés révén szerezhető meg. Ám katasztrofálisan elveszíthető egyetlen csalárd jóváhagyással (6.2. szakasz). Ez az aszimmetria azt jelenti, hogy évek alatt felhalmozott reputációt egyetlen tisztességtelen jóváhagyás lerombolhat; az optimális stratégia továbbra is a gyanús állítások elutasítása marad.

Nyilvános ígéret. Minden DID-birtokos nyilvánosan deklarálja a szabályzatát—egy géppel olvasható szabálykészletet, amelynek betartására kötelezettséget vállal. A deklaráció és a tényleges viselkedés közötti eltérés kimutatható, és az alapul

szolgáló szabálysértésnél súlyosabb reputációs vétségként áraztatik be (7.3. szakasz). A képmutatás ezért drágább, mint a közvetlen tisztességtelenség.

Háló-támadási költség aszimmetriája. A hálózat cenzúrázásának vagy destabilizálásának költsége nemlineárisan nő a hálózat méretével és sűrűségével, míg az eltűrésének költsége állandó marad. Ahhoz, hogy a cenzúra kifizetődő legyen, egy központosított szereplőnek az egész hálózatra ki kellene terjesztenie azt—olyan intézkedéseket követelve, amelyek aránytalanok bármely elképzelhető haszonnal (10. szakasz).

4 Decentralizált identitásmodell

4.1 DID különleges tulajdonságokkal

Az RSN a W3C DID Core specifikációt [2] a következőkkel egészíti ki: **deklarált szabályok** (géppel olvasható viselkedési kötelezettségvállalások), **reputációs metaadatok** (aggregált viselkedési pontszám), valamint **hálózati útválasztás** (változtatható onion átjáró, amely elkülönül a stabil gyűrűpozíciótól).

4.2 Az állítás életciklusa

Egy állítás hat szakaszon halad át (3. ábra): összeállítás, opcionális tekintélyi jóváhagyás, ellenőrkiválasztás konzisztens hasítással, ellenőrzési döntés (elfogadás vagy elutasítás iterációval), közzététel, valamint reputáció-frissítés minden fél számára.

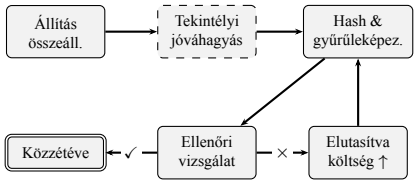

Figure 3: Az állítás életciklusa iterációs hurokkal.

4.3 Kapcsolat a W3C DID Core specifikációval

Az RSN identitásmodellje a W3C DID Core specifikáció [2] valódi bővebb halmaza. Minden RSN DID érvényes W3C DID. Az RSN-specifikus kiterjesztéseket egy dedikált DID-metódus specifikációban meghatározott DID-dokumentumtulajdonságokként kódolják, ami kompatibilis a meglévő infrastruktúrával, például az ION [7] és a Ceramic [8] rendszerekkel.

5 Az információ ellenőrzése és terjesztése

5.1 Az információbevitel költsége

Az RSN alapvető gazdasági elve az olvasás és az írás közötti aszimmetria. A reputációs adatok olvasása nulla határköltséghez közelít azon résztvevők számára, akik a DID-hálózat részei, és reputációjukkal arányos hozzáféréssel rendelkeznek—az újonnan érkezőknek fokozatosan ki kell érdemelniük a szélesebb hozzáférést (lásd a potyautas-védelmet). Az írás—úgy értve, mint a reputáció tartós materializálódása a hálózatba, nem pedig egyszeri technikai aktus—ellenőrizhető, halmozódó ráfordítást igényel három dimenzióban: **idő** (a következetes viselkedésre, a teljesített kötelezettségvállalásokra és az ápolt kapcsolatokra fordított életévek), **energia** (a becsületes ügyintézésbe, a partnerségek gondozásába és a hosszú távú megbízhatóságba fektetett erőfeszítés), valamint **pénz** (a saját név javára történő befektetés—szakmai fejlődés, a munka minősége, az okozott károk jóvátétele). A reputáció nem vásárolható meg azonnal—az egész életen át tartó felhalmozódás eredménye, amelyet a rendszer csupán láthatóvá és a kontextusok között átvihetővé tesz. A protokoll egyszeri technikai költségei (kriptográfiai aláírások, ellenőri díjak) elhanyagolhatók ehhez az alapul szolgáló befektetéshez képest.

5.2 Társadalmi gráf és kapcsolati mélység

Az RSN alapvetően egy közösségi hálózat: minden DID kontaktokat (más DID-eket) ad hozzá, akik engedélyezik a kapcsolatot. Ezeknek a kontaktoknak megvannak a saját kontaktjaik, és így tovább. Az algoritmikus ellenőrkeresés a kapcsolt kontaktok konfigurálható h mélységén belül működik (pl. $h = 3$: a közvetlen kontaktok, azok kontaktjai, és a kontaktok kontaktjai). Ez az architektúra nem igényel egyetlen globális blokkláncot—természetesen kedvez a közösségek/klaszterek kialakulásának, amelyek átfednek más közösségekbe. Minden DID-résztvevőnek rendelkeznie kell közzétett **szabályzattal**—egy géppel olvasható szabálykészlettel, amely szabályozza, hogyan értékelik a beérkező kéréseket. A szabályzatsértéseket a hálózat negatív artefaktumokként rögzíti.

5.3 Algoritmikus ellenőr-kiválasztás

Az ellenőrzési protokoll konzisztens hasítást [6] alkalmaz (4. ábra). Az ellenőrzés fizetett szolgáltatás: az

ellenőrök díjért működnek, létrehozva egy piacot, ahol a verseny formálja az árazást, a sebességet és a megbízhatóságot.

1. lépés. Az állítási dokumentumot összefűzik az előző iteráció hasítási eredményével (vagy $\varnothing$-vel az első iterációnál), és hasítják:

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

Az algoritmusnak tartalmaznia kell az összes korábbi kérés és válasz *teljes útvonalát*—nem pusztán az előző iteráció hasítását. Minden ellenőr teljes válasza (elfogadás, elutasítás, megadott ár, indoklás) hozzáfűződik a növekvő dokumentumhoz, amely minden lépésnél kriptográfiai aláírásokkal ellenőrizhető.

2. lépés. A hasítást leképezik a konzisztens hasítási gyűrűn N pozícióra, egyenletesen elosztva (pl. $N = 4$ esetén: $+0°, +90°, +180°, +270°$). Minden pozícióból egy óramutató járásával megegyező irányú keresés választja ki a legközelebbi DID-et ellenőrjelöltként (5. ábra). Az N egy változó paraméter, amely függhet a jelenleg aktív DID-ek százalékos arányától, a napszaktól vagy a hálózat korábbi reakciókészségétől.

3. lépés. Az ellenőr elfogad (közzétesz, reputációt téve fel) vagy elutasít (visszatérve az 1. lépéshez az elutasítás hasításával). Amikor egy csomópont nem válaszol annak ellenére, hogy online állapotot deklarál, a következő kérésnek tartalmaznia kell mind az N korábbi ellenőrjelölt összes válaszát.

Potyautas-védelem. A cél-DID-ek díjakat vagy hozzáférési korlátozásokat állíthatnak be a kevés reputációval rendelkező új DID-ek lekérdezéseihez. Ez a fokozatos (nem bináris) mechanizmus arra kényszeríti az újonnan érkezőket, hogy valós tevékenységgel építsenek reputációt, mielőtt szabadon fogyaszthatnák mások adatait.

Minden elutasítás hozzáfűzi az ellenőr teljes válaszát (az indokokat és feltételeket is beleértve) az állítási dokumentumhoz, kibővítve annak tartalmát. A kibővített dokumentumból nemdeterminisztikusan új hasítást számítanak, amely egy másik gyűrűpozícióra képeződik le, és egy másik ellenőrt választ ki. A teljes útvonal dokumentálása kötelező—a kibocsátó nem tudja megjósolni vagy befolyásolni a következő ellenőrt. Ha egy ellenőr figyelmen kívül hagy egy kérést kompatibilis deklarált szabályzat ellenére, a tanúk (ha jelen vannak) ezt rögzítik, és a kibocsátó a végső közzétételkor csatolhatja a tanúbizonyítékot.

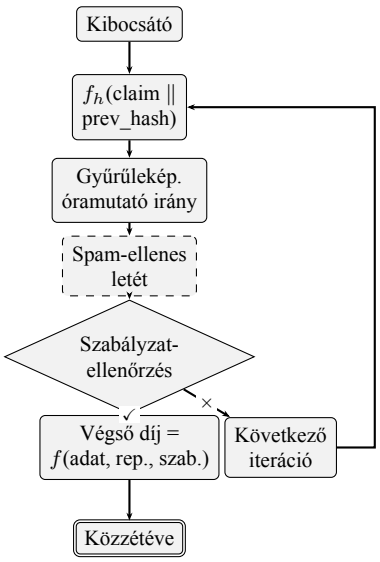

Figure 4: Ellenőr-kiválasztási protokoll. A spam-ellenes letét opcionális és visszatéríthető lehet. A végső díjat csak elfogadás esetén fizetik.

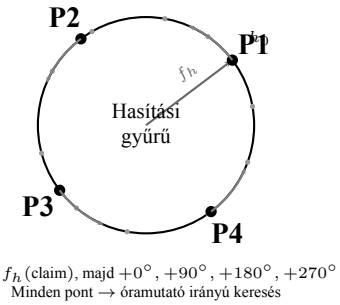

Figure 5: Többpontos kiválasztás (N=4). A h_0 hasítás adja az eltolást; 4 pont egyenletesen elosztva h_0-tól.

5.4 Tanúprotokoll

A **tanú** szerep inkognitó elszámoltathatóságot biztosít az ellenőr becsületessége felett egy kriptográfiai kihívási-kód protokollon keresztül:

W1. lépés. A kérelmező aláírja az ellenőrzési kérést, és elküldi N_w tanúnak—kontaktoknak a kérelmező közösségi hálózatából, vagy díj ellenében működő szakosodott tanúszolgálat-nyújtóknak.

W2. lépés. Minden w_i tanú aláírja a teljes aláírt kérést, megőrzi az eredeti σ_i aláírást, és kiszámít egy $c_i = h(\sigma_i)$ kihívási kódot. A kihívási kód hozzáfűződik a kéréshez.

W3. lépés. A kérés, amely immár N_w kihívási kódot hordoz, elküldésre kerül az ellenőrnek. Az ellenőr megfigyeli a kódokat, de *nem tudja megállapítani*, kik a tanúk, vagy hogy a kódok valós aláírásoknak felelnek-e meg.

W4. lépés (becsületes ellenőr). Ha az ellenőr a deklarált szabályzatának megfelelően válaszol, a ki-

hívási kódok átláthatatlanok maradnak. A tanúk sosem lepleződnek le. Nem tesznek közzé további adatot.

W5. lépés (szabályzatsértés). Ha az ellenőr megsérti a szabályzatát (figyelmen kívül hagyja a kérést, inkonzisztensen válaszol), a kérelmező birtokolja a tanúk eredeti σ_i aláírásait. Ezek kísérő adatként közzétehetők: bárki ellenőrizheti, hogy $c_i = h(\sigma_i)$, bizonyítva, hogy a tanú jelen volt. A kérelmező függetlenül közzéteheti—az ellenőr már aláírta a kihívási kódokat a válaszában.

A blöff tulajdonság. A kérelmező néhány vagy az összes kihívási kód helyett véletlen értékeket helyettesíthet be. Az ellenőr nem tudja megkülönböztetni a valódi kódokat (magas reputációjú tekintélyek által fedezetteket) a zajtól. Ez a *bizonytalanság* az érvényesítési mechanizmus: minden kérés magában hordozza annak kockázatát, hogy egy tekintélyes hatóság inkognitó figyeli. E nyomás fenntartásának költsége közel nulla (véletlen számok generálása), miközben a tisztességtelenség lehetséges költsége az ellenőr számára katasztrofális. A becsületes viselkedés még tényleges tanúk hiányában is ösztönözve van.

Tekintély mint tanú. Egy tekintély, amely jóváhagy egy állítást, tanúszolgálatot is csomagolhat hozzá: „jóváhagyom az állításodat, és inkognitó tanúként szolgálok az ellenőrzés során”. Ez természetes üzleti modell—a tekintély már rendelkezik kontextussal. A két szerep azonban logikailag független.

5.5 A drága radikalizmus elve

Három költségcsatorna erősíti egymást egyidejűleg (6. ábra):

1. csatorna: iterációs költség. Minden elutasítás egy új iterációt kényszerít ki, amely időt és erőforrásokat emészt fel. Lineáris növekedés.

2. csatorna: dokumentumduzzadás. Minden iteráció hozzáadja az ellenőr teljes válaszát az állítási dokumentumhoz. A növekedés lineáris, de alapeltolással: a kezdeti hasznos teher (az állítás tartalma, a tekintélyi jóváhagyás, a kriptográfiai aláírások) már nem elhanyagolható B_0 mérettel rendelkezik. Teljes méret k iteráció után: $S(k) = B_0 + k \cdot \Delta$, ahol Δ az átlagos válaszméret.

3. csatorna: ellenőri kockázati felár. A kockázat szubjektív. Az ellenőr felméri, hogy a kérelmező DID deklarált szabályzatai ütköznek-e az ellenőr saját kereskedelmi, társadalmi vagy politikai érdekeivel. A felár exponenciálisan nőhet az ellenőr „ideáljától” észlelt távolsággal: $P(d) = \alpha \cdot e^{\beta d}$, ahol d az ellenőr szubjektív távolságmértéke. Egy személyes tiltott határon túl az ellenőr teljesen megtagadhatja.

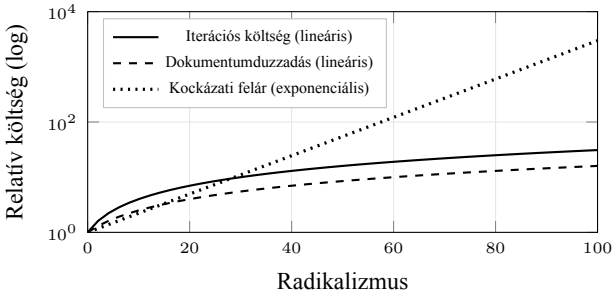

Figure 6: Költségeszkaláció három csatornán át. A kockázati felár dominál magas radikalizmusnál.

Lényeges, hogy ez nem cenzúra. Egyetlen állítás sincs megtiltva. A rendszer beárazza a kockázatot (1. táblázat).

Table 1: Költség-összehasonlítás az állítástípusok között.

Típus	Iter.	Dok.	Díj	Összes
Hiteles	$k_{\min}$	B_0	$P_{\min}$	Alacsony
Ellentmondásos	k_{med}	$B_0 + k\Delta$	$\alpha e^{\beta d}$	Mérsékelt
Radikális	$k_{\max}$	$\gg B_0$	$\gg P_{\min}$	Nagyon magas
Csalárd	$\to \infty$	—	—	Közzétehetetlen

6 Reputáció és kockázatértékelés

6.1 Reputáció-felhalmozási modell

A reputáció három tulajdonságot mutat: **lassú felhalmozódás** (fokozatos növekedés következetes viselkedés révén), **gyors lerombolás** (egyetlen csalás katasztrofálisan csökkentheti a pontszámot), valamint **egyéni értékelés** (minden fogyasztó fél a saját aggregációs függvényét alkalmazhatja).

6.2 Reputábilis tekintélyek

Egy reputábilis tekintély átvizsgálja az állításokat, és ha meggyőződött, társaláírja őket—saját reputációját téve fel (7. ábra). Az aszimmetria szándékos: a reputáció megszerzése lassú (fokozatos $+\delta$ becsületes jóváhagyásonként), miközben elvesztése katasztrofális ($-\Delta \gg \delta$ hamis jóváhagyásonként; szemléltetésképp pl. $+2\%$ vs. -70%). Az optimális stratégia mindig a gyanús állítások elutasítása. A δ és Δ konkrét értékei rendszerparaméterek.

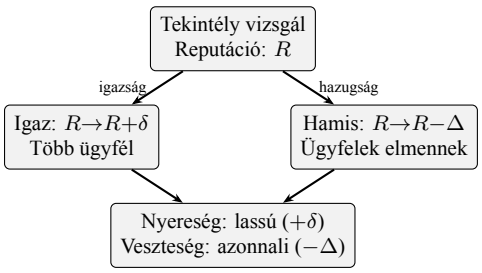

Figure 7: Reputábilis tekintély—aszimmetrikus ösztönzők.

6.3 Többdimenziós reputáció

A reputáció nem skalár, hanem vektor több dimenzió mentén: pénzügyi megbízhatóság, személyes integritás, szakmai kompetencia, közéleti szerepvállalás és mások (8. ábra). A különböző értékelést nyújtó szolgáltatók ezt a vektort másképp vetítik ki a kontextustól függően—egy hitelező a pénzügyi megbízhatóságot helyezi előtérbe, egy munkáltató a szakmai kompetenciát, egy szomszéd a közéleti viselkedést. Nincs egyetlen „helyes” reputációs pontszám; csak nézőpontok.

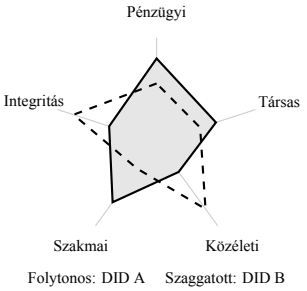

Figure 8: Többdimenziós reputációs vektorok. A különböző DID-ek eltérő profilokat mutatnak a dimenziók mentén.

6.4 Demokratizált kockázatértékelés

Az RSN demokratizálja a szisztematikus kockázatértékelést—egy olyan képességet, amely jelenleg a pénzügyi intézményekben összpontosul, ám a bankszektoron messze túl is alkalmazható. Ipari konglomerátumok a beszállítói megbízhatóság felmérésekor, biztosítótársaságok a viselkedési kockázat árazásakor, átvilágítás fúziók és felvásárlások esetén, berendezések élettartamának becslése a gyártásban—bárhol, ahol az ellenféllel kapcsolatos kockázatot fel kell mérni, az RSN decentralizált, piaci alapú alternatívát kínál. Az értelmezési szolgáltatások piaca a nyers, többdimenziós reputációs adatokat cselekvésre alkalmas összefoglalókká fordítja, elérhetővé téve az ellenfél értékelését bármely résztvevő számára határköltségen.

7 Konszenzus és vitarendezés

7.1 Decentralizált igazságszolgáltatási modell

Az RSN az igazságszolgáltatást kétoldalú tárgyalási problémaként fogalmazza újra. A tartós, ellenőrizhető reputációs kár fenyegetése hatékonyabb visszatartó erő, mint egy olyan bírósági eljárás, amelyet a sérelmet elszenvedő fél nem engedhet meg magának.

7.2 Emergens konszenzus

Minden résztvevő fenntart egy személyes elégedettségi küszöböt. A hálózat összesített konszenzusa több ezer kétoldalú tárgyalás statisztikai átlagaként emelkedik ki (9. ábra). A konszenzus felett messze járó válasz (barbár) drága a közzététele. A konszenzushoz közeli válasz (arányos) olcsó. A konszenzus nem szabály—árjelzés.

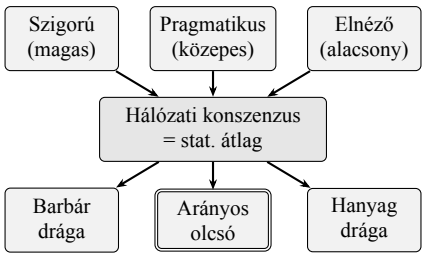

Figure 9: Emergens konszenzus egyéni elégedettségi küszöbökből.

7.3 A büntetés kalibrálása

Minden DID-birtokos nyilvánosan deklarálja a válaszait meghatározott vétségkategóriákra. Az aránytalanul szigorú vagy engedékeny deklarációk negatív reputációs jelzéseket vonzanak. Az arányos deklarációkat súrlódás nélkül fogadják el—egy önkalibráló büntetési rendszer.

Maguk a konszenzuális deklarációk is alá vannak vetve a képmutatás-észlelésnek: deklaratívan elkötelezni magunkat egy konszenzuális álláspont mellett, miközben inkonzisztensen viselkedünk, az alapul szolgáló eltérésnél súlyosabb reputációs vétséget képez, mivel szándékos megtévesztést mutat.

7.4 Delegálás

Egy DID-en belül minden tevékenység—egyetlen kivétellel—átruházható egy másik DID-re. **Az alany szerep—az a DID, amelynek viselkedéséről az állítás szól—nem delegálható; nem átruházhatóan kötődik ahhoz az identitásbirtokoshoz, akire az állítás utal.** A többi aktív szerep—kibocsátó, tekintély, tanú, ellenőr—átruházható egy kijelölt meghatalmazott DID-re, akár ellenőrzés, állításbenyújtás, konszenzusban való részvétel vagy vitarendezés céljából. A delegálás bármikor visszavonható. Ez lehetővé teszi a specializációt (pl. szakszerű ellenőrzési szolgáltatások), miközben a birtokos megtartja a végső irányítást és felelősséget. A delegálás az egész rendszerre alkalmazandó, és elengedhetetlen a skálázhatósághoz.

7.5 Az egyéni erkölcstől az emergens társadalmi szerződésig

Minden DID deklarált szabályzata az egyéni erkölcs formalizálását képviseli: mit tart a birtokos elfogadhatónak, hogyan reagál meghatározott viselkedésekre, mit követel meg az ellenfelektől. Ezeket a szabályzatokat nem egy rendszertervező írja elő—minden résztvevő maga választja meg és géppel olvasható formában fejezi ki őket.

Ez a formalizálás egy háromszakaszos emergenciát tesz lehetővé. Először az egyéni erkölcs **szabályzatként** kódolódik—deklarált szabályok, küszöbök és válaszfüggvények halmazaként, amelyek betartására a DID kötelezettséget vállal. Másodszor a hálózat összes szabályzatának összessége **emergens etikát** hoz létre—statisztikailag megfigyelhető normákat, amelyeket egyetlen résztvevő sem tervezett, de amelyek több ezer egyéni erkölcsi álláspont interakciójából keletkeznek [9]. Harmadszor ezek az emergens etikák, közös viselkedési normákként kifejezve és kétoldalú árjelzéseken keresztül érvényesítve, **mérhető társadalmi szerződést** képeznek—nem elméleti konstrukciót, amelyet senki sem írt alá [10], hanem a tényleges viselkedéssel alátámasztott, empirikusan megfigyelhető szabálykészletet.

Ez a folyamat tükrözi az erkölcsi alapok elméletének [11] eredményeit: az emberi erkölcs intuitív, pluralisztikus és kulturálisan változó. Az RSN nem igényel erkölcsi konszenzust bemenetként; viselkedési konszenzust állít elő kimenetként. Az így létrejövő társadalmi szerződés nem statikus—fejlődik, ahogy a résztvevők csatlakoznak, kilépnek, és a hálózati visszacsatolásra reagálva módosítják szabályzataikat. A klasszikus társadalmiszerződés-elmélettel ellentétben ez a szerződés visszavonható, megfigyelhető és szuverén nélkül érvényesíthető.

8 Gazdasági modell

Az előző szakaszok egy eszközt írtak le—az RSN ellenőrzési mechanizmusait, költségszerkezetét és emergens konszenzusát. Ez a szakasz egy módszertant ír le ezen eszköz alkalmazására a költségvetési és kormányzati átmenetre. Az eszköz általános célú; az alábbi módszertan egy lehetséges alkalmazás.

8.1 Ösztönzőszerkezet

A reputáció mint tőke közvetlen ösztönzőket teremt a becsületes viselkedésre. Normál működésben a résztvevők természetesen építenek reputációt a mindennapi tranzakciók és a teljesített kötelezettségvállalások révén. Az elsődleges kiadás a *negatív* állításokra esik—a mások által okozott károk rögzítésére. Ez az aszimmetria hasznos, megbízható viselkedést ösztönöz: a becsületesség nem kerül semmi többletbe, míg az ártalmasság dokumentált nyomot hagy, amelyet mások hajlandók fizetni a megőrzéséért. A képmutatás—szabályok deklarálása azok betartása nélkül—a legdrágább kudarcmód, mivel szándékos megtévesztést mutat.

8.2 Párhuzamos költségvetési rendszer

Három összetevő tesz lehetővé versenynyomást: (1) **egyszerű adó**—egyetlen arányos kulcs kivételek nélkül, kezdetben marginálisan a meglévő tényleges kulcs alatt; (2) **elektronikus kiadás-nyilvántartás (Electronic Spending Registration, ESR)**—a cseh EET-modell megfordítása, hogy a polgárok felügyeljék az állami kiadásokat; (3) **polgár által irányított adóelosztás**—az első évben néhány százalékkal indulva, és egy évtized után elérve akár az alacsony kétjegyű tartományt, akár a polgár által irányított rendszerre való teljes átállást, az elfogadás ütemétől függően. A tényleges tempó attól függ, milyen gyorsan jelennek meg szabadpiaci alternatívák az állami szolgáltatásokra, valamint az állam hajlandóságától, hogy együttműködjön az átmenettel; az idő függvényének nem kell lineárisnak lennie, és nincs ok arra, hogy felső korlátot szabjunk annak, ahová az elfogadás végül eljuthat.

9 Átállási út

Az átállás három fázison halad át (10. ábra): **1. fázis: rárétegzés** (az RSN mint információs réteg, az ál-

lam az egyetlen szolgáltató), **2. fázis: verseny** (az RSN funkcionális alternatívákat kínál, kettős rendszerhasználat), valamint **3. fázis: átmenet** (az RSN felülmúlja az állami megfelelőket, önkéntes átállás). Az átmenet minden szakaszban visszafordítható.

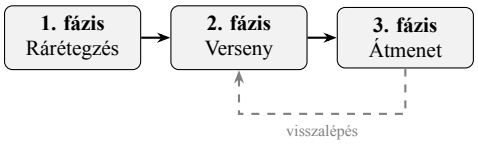

Figure 10: Háromfázisú átállás—minden szakaszban visszafordítható.

Az elsődleges nyomásmechanizmus költségvetési: amikor a feltételes adófizetők elérnek egy „gazdaságilag jelentős kisebbséget X"—egy olyan csoportot, amely elég nagy ahhoz, hogy az ellene irányuló elnyomás nem elhanyagolható gazdasági kárt okozzon, és a polgári engedetlenség hiteles fenyegetéssé váljon—az állam tárgyalásba kezd. Szemléltetésül $X \approx 15\%$-nyi GDP-t használunk, de a tényleges küszöb az adott gazdaságtól függ.

10 Biztonsági elemzés

Öt ellenfél-kategóriát tekintünk: egyéni rosszhiszemű szereplők, szervezett csoportok, vállalati ellenfelek, állami szintű ellenfelek, valamint protokollszintű ellenfelek.

Sybil-ellenállás [12]. A reputáció felépítése tartós, ellenőrizhető interakciót igényel. Egy sikeres Sybil-támadás költsége lineárisan skálázódik a hamis identitások számával és kvadratikusan a célzott reputációszinttel. Több DID párhuzamos működtetése lehetséges, de szándékosan drága—minden identitásnak önállóan kell reputációt felhalmoznia valós tevékenységgel. Szabad társadalmakban ez a költség elrettent az alkalmi visszaéléstől; diktatúrákban a párhuzamos DID-ek túlélési eszközzé válnak, amelyek lehetővé teszik a részekre bontott ellenállást, a földalatti koordinációt és a biztonságosabb feketepiaci navigálást.

Összejátszás elleni védelem. A zárt csoportokon belüli kölcsönös jóváhagyás mintázatai kimutathatók társadalmi gráfelemzéssel. A reputáció-aggregációs függvények leértékelik a szorosan klaszterezett forrásokból származó állításokat.

Állami szintű ellenfél. Az onion útválasztás, a központosított infrastruktúra hiánya és az ellenőr szerep szétosztása a résztvevők között biztosítja, hogy az elnyomás bármely haszonhoz aránytalan intézkedéseket követel.

Adatvédelem vs. elszámoltathatóság. Az álnevűség—köztes út az anonimitás és az identitás felfedése között—lehetővé teszi a DID-ek számára, hogy értékes reputációt halmozzanak fel a birtokos valós identitásának felfedése nélkül.

11 Adatvédelmi megfontolások

Az RSN adatvédelmi modellje az álnevűségre épül. A birtokos irányítja az identitás felfedését: minimális (tiszta álnév), szelektív (meghatározott hitelesítő adatok kapcsolva) vagy teljes (jogi identitás társítva). A közzétett állítások tartósak—a rendszer támogatja a kontextusfüggő helyesbítést, de a törlést nem. Egy birtokos elhagyhat egy kompromittálódott DID-et, és újrakezdheti, feláldozva a felhalmozott reputációt.

12 Kapcsolódó munkák

A W3C DID Core specifikáció [2] és a Ceramic Network [8] adja az identitásalapot. Az EigenTrust [13] demonstrálta az elosztott reputáció-aggregációt központi hatóság nélkül. Az SBT-k [3] bevezették a nem átruházható társadalmi tokeneket. Az RSN abban különbözik, hogy hangsúlyt fektet a gazdasági költségre mint minőségszűrőre, valamint a radikalizmus beárazásának mechanizmusára.

A DAO-k [4] és a kvadratikus szavazás [5] demonstrálták a decentralizált kormányzás megvalósíthatóságát. Az RSN a konszenzust szavazás helyett kétoldalú áralkukból vezeti le.

A javaslat az anarcho-kapitalista elméletre [14, 15] támaszkodik a magánszolgáltatás terén, de két kritikus szempontból eltér tőle: a racionalitás feltételezése helyett a rosszindulatra és a megtorlásból fakadó ösztönökre tervez, és forradalom helyett fokozatos átmenetet javasol. Az emergens társadalmi szerződések fogalmának előzményei megtalálhatók Hayek spontán rend elméletében [16].

Anarcho-agorizmus. Az RSN jelentős közös alapot oszt meg az agorista ellengazdaságtannal [17]—különösen a párhuzamos intézmények építésének és az önkéntes cserének a hangsúlyozásában. Az agorizmus azonban hajlamos a racionális önérdeket elegendő koordinációs mechanizmusként feltételezni, és gyakran hiányzik belőle egy konkrét átállási út a meglévő állami struktúrákból. Az RSN kifejezetten beépíti a nem racionális viselkedési hajlamokat, és költségvetési nyomásmechanizmust kínál a fokozatos átmenethez.

Meritokrácia. Az RSN talán egy első funkcionális leírását képviseli annak, hogyan emelkedhet ki a mer-

itokrácia [18] rendszerszintű tulajdonságként, nem pedig szlogenként. A hagyományos meritokratikus rendszerek azért vallanak kudarcot, mert egy központi hatóságot igényelnek az „érdem” meghatározásához és érvényesítéséhez. Az RSN-ben az érdem a kétoldalú értékelésekből emelkedik ki: akik értéket teremtenek, reputációt halmoznak fel; egyetlen bizottság sem dönti el, kinek van érdeme.

A tulajdon mint privilégium. Az RSN alapvetően eltér a tulajdonjogok anarcho-kapitalista és osztrák iskolai kezelésétől, amely azokat természetesnek és abszolútnak tekinti. Az RSN keretrendszerében a tulajdon *privilégium*—egy társadalmi elismerés, amely szélsőséges esetekben visszavonható a közösség által, amikor egy résztvevő alapvetően megsérti a közös normákat (árulás, a közösség megvédésének megtagadása egzisztenciális válságban, szisztematikus kizsákmányolás). Ez nem állami kisajátítás, hanem a társadalmi elismerés visszavonása a kétoldalú kapcsolatok hálózata által.

13 Diszkusszió és korlátok

Hidegindítás. Az RSN értéke hálózati hatásoktól függ; a korai alkalmazók korlátozott értékkel szembesülnek, amíg a részvétel el nem ér egy küszöböt. Ám már a korai szakaszoktól kezdve a DID-hálózat hasznos kiegészítő információforrásként szolgál. A korai reputációértékelés és tekintélyfelmérés várhatóan fokozatosan, egyre kifinomultabbá válva fejlődik.

Potyautas-védelem és hozzáférés-szabályozás. A cél-DID-ek fokozatos díjakat és hozzáférési korlátozásokat szabhatnak ki az alacsony reputációjú DID-ek lekérdezéseire. Ez nem bináris, hanem folytonos skála: minél kevesebb reputációja van egy lekérdező DID-nek, annál kevesebb információt kap, annál tovább vár, és annál többet fizet. Ez a mechanizmus a valós részvételt ösztönzi a passzív fogyasztással szemben.

Hozzáférési egyenlőtlenség. Az állítások közzétételének költsége kiszűrheti a jogos panaszokat a gazdaságilag hátrányos helyzetű résztvevőktől. Enyhítés: minden résztvevő egyúttal potenciális ellenőrként szolgál (vagy delegálja ezt a szerepet), és ellenőrzési díjakat keres. Elegendő időhorizonton egy nem radikális résztvevőnek meg kell közelítenie a pénzügyi semlegességet—az ellenőrzési bevétel megközelítőleg ellensúlyozza a közzétételi költségeket. Ez statisztikai várakozás, nem garancia.

Reputációs egyenlőtlenség. A korai alkalmazók olyan előnyöket halmoznak fel, amelyek akadályokat teremthetnek a későbbi belépők számára. Ám a reputációértékelést harmadik fél szolgáltatói végzik, akik dönthetnek úgy, hogy aggregációs algoritmusaikkal mérséklik az elsőmozgató-előnyt. Elsőnek lenni jó reputációval legitim komparatív gazdasági előny—és ez szándékos.

Nyitott kérdések. Az optimális költségfüggvények, az aggregációs szabványok, a protokollkormányzás, valamint az MI által generált szintetikus reputációs adatokkal való kölcsönhatás a jövőbeli munka területei maradnak.

Ez a tanulmány nem állítja, hogy az RSN minden körülmények között optimális kimeneteket produkál. Azt állítja, hogy az RSN egy *megvalósítható* alternatívát képvisel—technikailag megvalósítható, gazdaságilag önfenntartó, és társadalmilag összeegyeztethető az emberi viselkedési hajlamokkal úgy, ahogy azok valójában vannak.

14 Következtetés

Ez a tanulmány bemutatta a reputációs közösségi hálózatot, egy decentralizált protokollt, amely álnéven történő, ellenőrizhető reputációcserét tesz lehetővé. A drága radikalizmus elve biztosítja, hogy a csalárd állítások cenzúra nélkül árazódjanak ki. A javasolt átállási út fokozatos, visszafordítható átmenetet tesz lehetővé a meglévő intézményekből. A terv az emberi természetet olyannak építi be, amilyen—a kicsinyességet, a rosszindulatot és a megtorlásból fakadó elégtétel iránti vágyat is beleértve—ahelyett, hogy ideológiai átalakulást igényelne. Az eredmény nem utópia, hanem egy olyan rendszer, ahol az igazságosság elérhető, a reputáció kiérdemelt, és a vétség költségét az a fél viseli, aki okozta.

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.