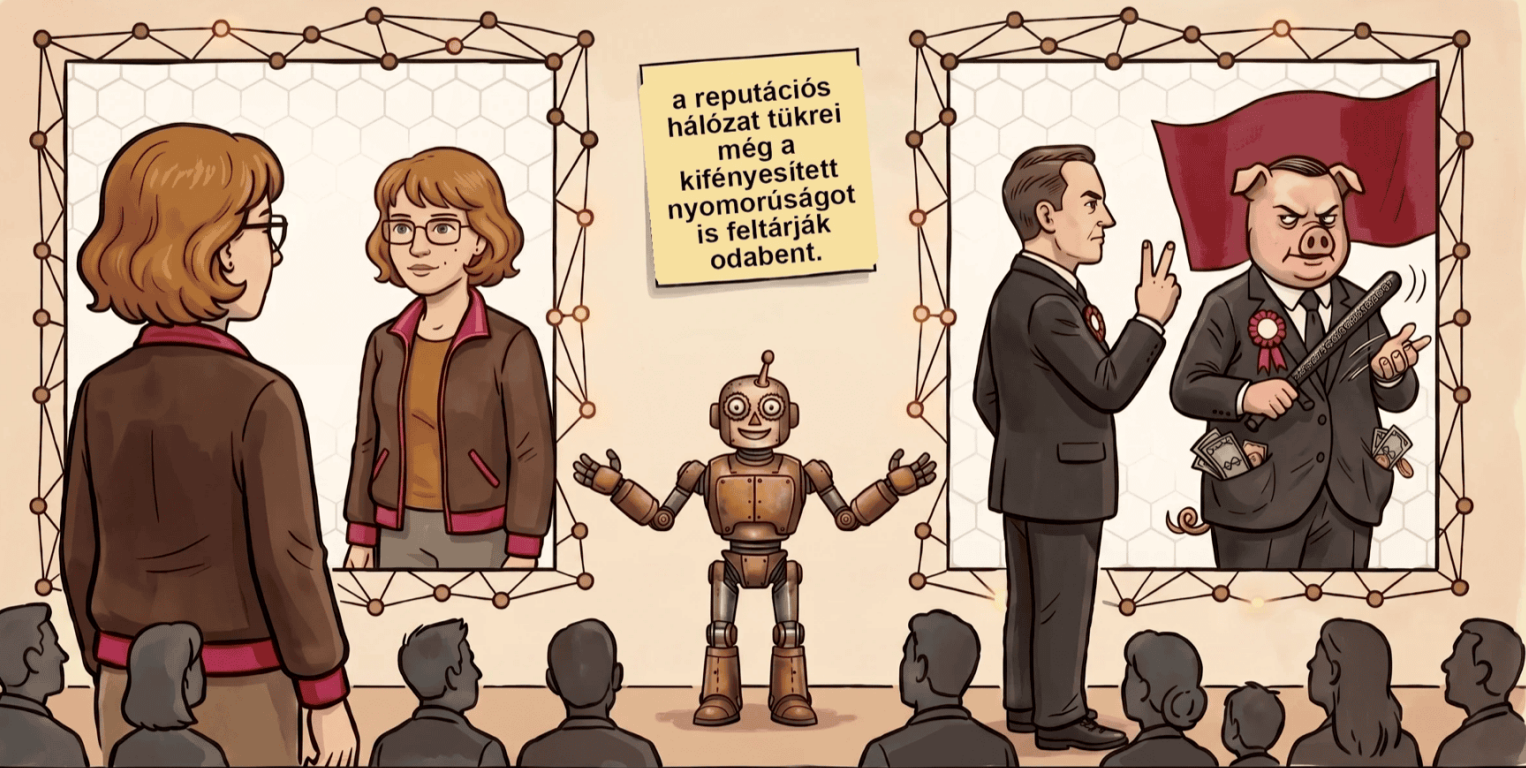


PERSONIX

a reputációs
hálózat tükröi
még a
kifényesített
nyomorúságot
is feltárják
odabent.



**Egy cenzúrázhatatlan és megvesztegethetetlen decentralizált reputációs hálózat
az állam evolúciós utódja**

Personix — Megalkuvás nélküli változás

Cenzúrázhatatlan és korrumpálhatatlan decentralizált reputációs hálózat

© 2025–2026 Pavel Kudrna, Prága

6. verzió (2026-05-21)

Első vázlat 2025. június–november; átdolgozva 2026. április–május.

Szedve $\text{\LaTeX}$ -ben (Tectonic), Palatino és Helvetica Neue betűkkel.

A5 fekvő (210×148 mm).

Licenc: **Creative Commons Attribution-ShareAlike 4.0 International (CC BY-SA 4.0)** —

creativecommons.org/licenses/by-sa/4.0/. A fenntartott elemek, a forráskódtár és a gyártási eszközökről szóló megjegyzés a könyv végén található.

Contents

Bevezetés	7
Miről szól ez a könyv?	9
A változás elengedhetetlen előfeltételei	17
A változás elengedhetetlen előfeltételei	17
Az eszköz	28
Reputáció alapú közösségi hálózat	28
Miért cenzúrázhatatlan a hálózat	53
Kézenfekvő kételyek eloszlátása	55
Technológiafüggőség	55
Kidobom-e az ablakon a pénzem, ha közzéteszek a hálózatban?	55
Mi van, ha valaki több identitást hoz létre?	57
Nem tud-e egy gazdag ember egyszerűen „megvenni” több identitást (vagy virtuális közösségeket létrehozni)?	60
Mi a helyzet a potyautasokkal, akik csak olvasni akarnak, és semmit nem adnak a közösségnek?	63

Pénzügyi semlegesség	64
Önkéntesség, felelősség és szabadság	66
A szabadság–totalitarizmus kapcsoló (és a delegálás)	67
Az oracle-probléma — híd a digitális és a fizikai világ között	73
Hogyan működik az ellenőrzés	77
Konszenzus és az ellenőrzési folyamat	77
Roles in the verification transaction and authorities	83
A szerepek áttekintése	83
Kibocsátó	84
Autoritás	85
Ellenőrző	89
Alany	91
Megfigyelő	94
A mechanizmus: időbélyeg és kihíváskód	94
A csattanó: nincs szükség valódi megfigyelőkre	96
Delegálás	98
Kommunikáció a szerepek között	103
Az emergens társadalmi szerződés — a policy	103
Információ szolgáltatása magadról	107

Bűn és bűnhődés	108
Bűn és bűnhődés	108
Kövesd a pénzt	120
Kövesd a pénz nyomát	120
Az állam gyenge pontja — a pénz	121
Proposed transition to the state's successor	124
Evolúció, nem forradalom	124
Négy eszköz, amely egymást támogatja	126
Egyszerű adórendszer — a belépő csali	127
Elektronikus kiadásnyilvántartás (ESR)	127
Polgári adóallokáció — a döntés súlya	129
Tárgyalási platform az állammal — a kar	133
Állampolgárság személyi igazolvány nélkül	135
Átfedés és visszafordíthatóság	139
Zárszó	142
Az út létezik	142
Köszönetnyilvánítás	144
Inspiráció	144

Recenzió és visszajelzés	144
Eszközök	144
Fogalomtár	147
Fogalomtár	147

Bevezetés

Úgy érzed, hogy számíthatsz az államra?

Nem vagyok hajlandó elfogadni, hogy amikor nyilvánvaló igazságtalanság ér engem, a családomat vagy valakit a közösségemben (testi sértés, csalás, indokolatlan korlátozás, ...), az állam azt válaszolja: igen, ez igazságtalanság, de ne tégy ellene semmit, különben még nagyobb bajod lesz velünk. Egy ilyen állapot beteg, és azok, akik belenyugszanak, cinkosok.

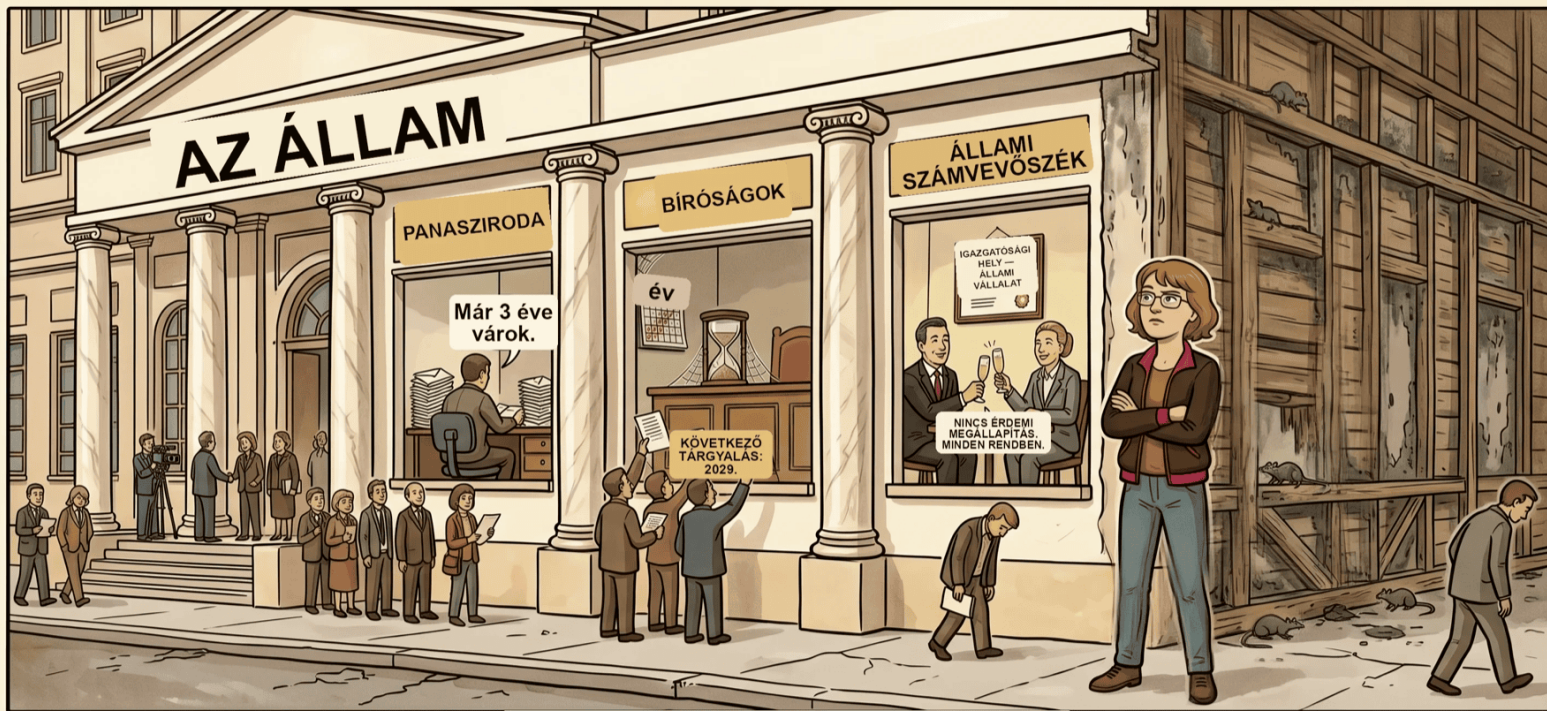
Az eredmény kölcsönös elidegenedés, közösségesdi, államosdi és a társadalom egyre mélyülő széthullása, azzal a kilátással, hogy súlyos konfliktusok jönnek.

Képes az állam lépést tartani a technológiai és társadalmi változás ütemével, vagy inkább tiltással válaszol?

Tehetnék úgy, mintha a pangást, a hozzá nem értést és a korrupciót a jogállamiság és a hagyomány deklarált stabilitásaként fognám fel, de ezt már nem akarom. Hazudnék magamnak, és hazudnék neked is.

Érzed a hivatalnokok és a választott képviselők lekezelését, amikor bátorkodsz kritizálni valamit, amiért fizetsz?

Nem vagyok hajlandó a társadalomban élő embereket méltatlannak tekinteni arra, hogy társadalmi szintű szabályokat alakítsanak, csak azért, mert nem jeleskednek azokban a soft skillekben, amelyek ma az egyetlen elégséges előfeltételei annak, hogy valaki választott képviselővé váljon az állam által kodifikált intézményekben. Hiszem, hogy a túlnyomó többség gondoskodni tud magáról, a szeretteiről



Nem fogadom el.

és a közösségéről — és hogy ebben életfilozófiájuk egy darabját látják. A körülöttem megismert emberek többsége ilyen.

De találkoztam kifejezett bunkókkal is, akik éppen azért voltak bunkók, mert tudták, hogyan játsszák a játékot — azt a játékot, amelyben a közösség nem adhat nekik visszajelzést, amelyben az állam megvédi őket, hogy senki ne bolygassa meg azt a rendet, amely magának az állam lényegének mondana ellent: annak, hogy könnyű életet biztosítson azoknak, akik a hatalmi hierarchia és intézményei felső emeletein ülnek. A feudalizmust a populisták és az elitisták uralma váltotta fel.

Szereted, ha mások megmondják, hogyan éld az életedet?

Nem fogadom el a dolgok jelenlegi állását tökéletes, végleges adottságként. Felelősnek kell lennem abban, ahogyan viselkedem, ám érzékeny vagyok arra, ha valaki megmondja, milyen helyes értékeket kellene vallanom. Nálad hogy van ez?

Miről szól ez a könyv?

Képzeld el egy reputációs közösségi hálózatot, amelyhez bárki, aki akar, létrehozhatja a saját kulcsait (megalkothatja az identitását), meghívhatja magát a közössége tagjaival, vagy egyedül vághat neki. Építéd a reputációd, és mások hasznos reputációs adataira támaszkodsz, amikor szükséged van rá. Igazságtalanság esetén a közösséged támogatását kéred — előadod az ügyedet, és megadod, amid van az ügyről, a közösség pedig megnézi, relevancia alapján eldönti, továbbadja-e másoknak, és hogyan szankcionálja az elkövetőt.

Ez az egész rövid könyv arról szól, minek kell a motorháztető alatt lennie ahhoz, hogy kívülről ilyen egyszerűen működjön. Ha kitartasz mellette, megígérem, hogy egy világ, amely most sok szempontból összetettnek és nehezen érthetőnek tűnhet, érthetőbbként és világosabbként fog megnyílni előtted. Látni

fogod, hogy sok rossz dolog úgy is beállítható, hogy már ne érje meg olyan igazságtalanul a rossz szereplőknek. És ez nem olyan eszköz, amelyhez folyamatosan az online térhez tapadva kellene ragaszkodnod — elég akkor nyúlni utána, amikor úgy érzed, szükséged van rá.

Azt is megígérem, hogy az itt leírt elrendezés közelebb áll majd az emberek valódi motivációihoz, és hogy nem kell azokat valamiféle -izmus nevében átformálnia.

Végül pedig megmutatjuk, hogyan lehet nem forradalmi átmenetet levezényelni egy olyan állapotba, amelyben a közösségek ismét teljesen működőképes társadalmi egységekké válnak, és nem kell többé csak úgy tenniük, mintha azok volnának.

Technikai cikk

Ez a könyv magyarázó kísérője az eredeti technikai cikknek: „*Decentralized Reputation Network: A Framework for Voluntary and Uncorruptible Societal Organization*” (Pavel Kudrna, 2026). Ha a formális architektúraleírás, az ellenőrző-kiválasztási algoritmus és a gazdasági mechanizmusok igazolása érdekel, azt ajánlom, azzal kezd.

■ A fejezetek egymásra épülnek

A könyv folyamatos érvelésként íródott — minden fejezet az előzőre épül. Az egyik részben bevezetett fogalmakat a későbbi részek használják, a lábjegyzeteket is beleértve. Nem ajánlom a sorrenden kívüli olvasást.

■ Kinek szól ez a könyv?

Vizuálisan barátságos formátuma ellenére a fő célközönség a szakmaibb olvasó, akit az emberi társadalom lehetséges társadalmi-gazdasági-politikai elrendezéseinek elvei foglalkoztatnak. Ahhoz, hogy eljussak oda, ahol az egész tárgykört a legszélesebb közönség számára érthetően el tudom magyarázni, még hosszú út vezet: egy teljes kommunikációs stratégia kiépítése.

Örömmel fogadok javaslatokat arra, hogyan tehető ez a kis mű vagy bármely későbbi átdolgozott kiadás érthetőbbé.

Figyelmeztetés

Nem tudom, ki vagy, hány éves vagy, és hány megszegett ígéretet kellett végigülnöd az életedben. Én végeztem az ígérettel. Ehelyett figyelmeztetni akarlak, hogy annak, amit itt megtudsz, az egyetlen kimenetele talán az a felismerés lehet, hogy valószínűleg nincs olyan út, amelyen valaki más takarítja fel



Van itt még bőven a motorháztető alatt. Tarts velem.

helyetted a mai kupacot. Én csak egy keretrendszert/eszközt írok le, amely egyszerűbbé és átláthatóbbá tehetné a takarítást. Ennek alapján megkísérlek egy társadalmi kísérletet/szimulációt előkészíteni, kijavítani az esetleges hibákat, vagy teljesen eltemetni az ötletet, ha kiderül, hogy alapvető tervezési repedések vannak benne.

Egy kérés

Mélységesen megköszönném, ha a könyv befejezése után is nyitottan viszonyulnál az ötlethez, és követnéd, merre tart, és hogyan állja ki az érdemi kritikát. Még jobban megköszönném a későbbi bevonódásodat — hogy saját ötleteiddel próbáld megtörni a javasolt egyensúlyi elveket, és ezzel jobban leteszteled, mennyire felkészült a rendszer a valós emberi viselkedésre.

Nélküled és a bevonódásod nélkül az ötlet egy fiókban maradó elmélet marad. Nélküled, a hozzájárulásaid és pénzbeli adományaid nélkül nem tudjuk majd a projektet egy valódi társadalmi kísérlet, és ezzel a valódi felkészültség felé tolni. Nélküled és az érdemi kritikád nélkül vagy megrekedünk ott, ahol most vagyunk, vagy hagyjuk, hogy elnyeljen a centristák szent grálja — az abszolút, visszafordíthatatlan totalitarizmus. Rajtunk múlik, melyik utat választjuk, vagy üljük végig tétlenül.

A kihívás

Nem éppen könnyű terhet rakunk a válladra. Máris viseled egy pazarlóan vezetett társadalom költségeit olyan okkultista-ráolvasós kézikönyveken keresztül, amelyek azt állítják, hogy a társadalmat központilag lehet a legjobban irányítani — és nekem van pofám még többet kérni tőled, és szembemenni ezekkel a tendenciákkal. Tudatában vagyok, hogy át kell majd véselnünk a történelem legnagyobb piramisjátékának — a felosztó-kirovó nyugdíjrendszernek — az összeomlását anélkül, hogy hagynánk éhezni több nemzedéket.

Mégis megkérlek: adjunk végre jobb világot a gyerekeinknek, és hagyjunk magunk után olyan örökséget, hogy azt a változást mi vittük véghez. A gazdasági növekedés felszabadítása részleges megoldás



Egy jobb világ megéri a terhet.

lehet a láthatáron lévő szorult helyzetre. Utódainknak aztán elmondhatjuk, hogy pokoli jó menet volt, és nem volt hiába.

■ A probléma

Csak a közvetlen felelősséggel kiegyensúlyozott szabadság képes valóban felszabadítani egy olyan hatalmas potenciált, amelyet a világ még nem látott.



Gyere be. A tervek készen állnak.

A változás elengedhetetlen előfeltételei

A változás elengedhetetlen előfeltételei

A jobbá váláshoz vezető változás alapvető előfeltétele, hogy az alárendeltből fölérendelt — vagy legalább egyenrangú partner — legyen. Ez azt jelenti, hogy át kell venni a legkritikusabb ügyköröket, amelyek a fölé- és alárendeltség viszonyát meghatározzák. Ezek az ügykörök azon a bizonyítékokon nyugszanak, hogy valaki az állam polgárait alkotó közösségekhez tartozik. Ez pedig maga az információ és annak ellenőrizhetősége egy olyan autoritás által, amely az adott közösségeken belül jelentős reputációval bír.

A jelenlegi rendszer meghaladásához öt előfeltételre jutottam, amelyeket aztán úgy fejték ki, ahogyan én értem őket. Ezekre az előfeltételekre úgy gondolhatunk, mint a pillérekre, amelyek a könyv további részében leírt rendszer építményét hordozzák. A pilléreket kezdetben a saját preferenciám szerint választottam ki, és miközben végiggondoltam őket, fokozatosan csiszoltam az alábbi formára azt, ahogyan mindegyiket értem.

Vegyük sorra ezt az öt pillért.

A VÁLTOZÁS ELŐFELTÉTELEI



E öt pillér nélkül minden változás csak elpazarolt idő.

■ Önkéntesség

A mi esetünkben az önkéntesség azt jelenti, hogy senki sem kényszerít arra, hogy részt vegyek a decentralizált reputációs hálózat működtetésében. Ugyanakkor nem követelhetek pozitívan megfogalmazott jogot arra, hogy a hálózat ne rögzítsen rólam információt — hogy kerül-e rólam információ a reputációs hálózatba, az kizárólag rajtam, a viselkedésemen, a tetteimen és a felelősségemen múlik.



Önkéntes — amíg utol nem ér a felelősség.

■ Szerveződés

Egyetlen egyén nem tudja megtörni a rendszert, ezért az állam ellenőrzése alatt tartja az emberek társulását, hogy megelőzze azokat a tevékenységeket, amelyek a szerkezetét és működését veszélyeztethetnék. Nem számít, hogy az emberek mellette vagy ellene szerveződnek. A szerveződés révén tompítható az elrettentő büntetések hatása, amikor valaki az akarata ellenére meri megváltoztatni az államot.

Ne tűzzünk ki közös célokat, de az út egy részét együtt megtehetjük. A legtermészetesebb forma a közösségekbe való társulás — ám ezeknek rendelkezniük kell minden szükséges eszközzel, hogy ne maradjanak pusztá közösségesdinél.

■ Ellenállóképesség

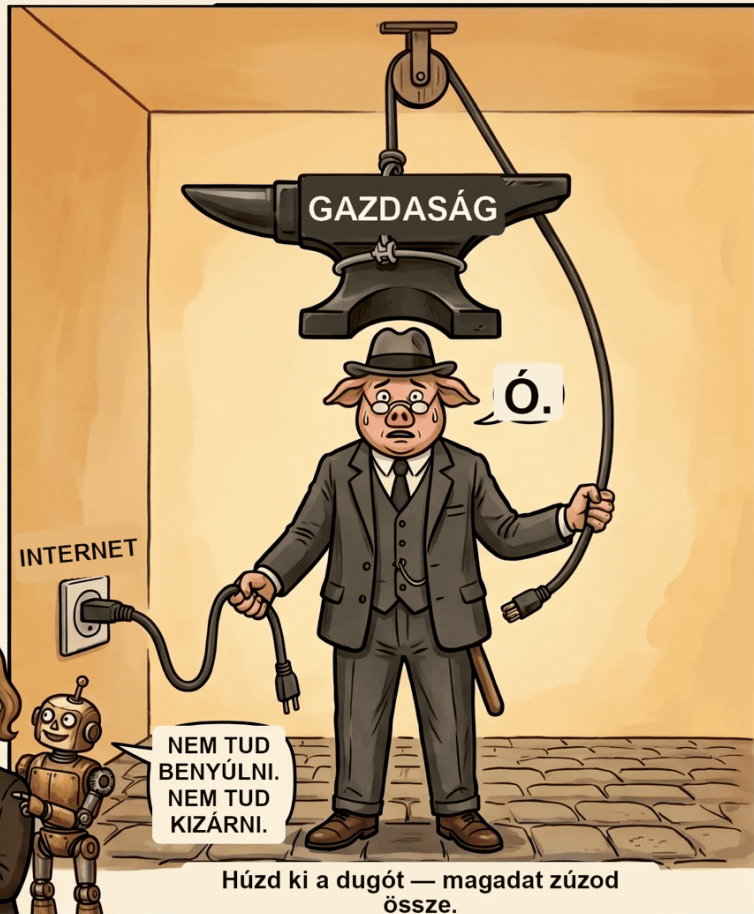
Az állam megváltoztatása — vagy az utódjához való átmenet — felé választott útnak nem szabad állami engedélytől függnie. Az eszközöknek és használatuk módjának a lehető legcenzúrázhatatlanabbnak kell lenniük. Egyszerűen szólva: a cenzúrázásuk költségének csillagászatnak kell lennie. Enélkül az egész igyekezet csak idő- és életenergia-pazarlás.

2. ELŐFELTÉTEL AZ 5-BŐL: SZERVEZŐDÉS



Egy egyén nem törheti meg a rendszert. Egy közösség igen.

3. ELŐFELTÉTEL AZ 5-BŐL: ELLENÁLLÓ KÉPESSÉG



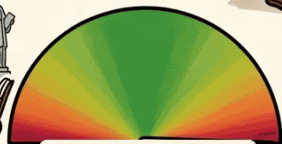
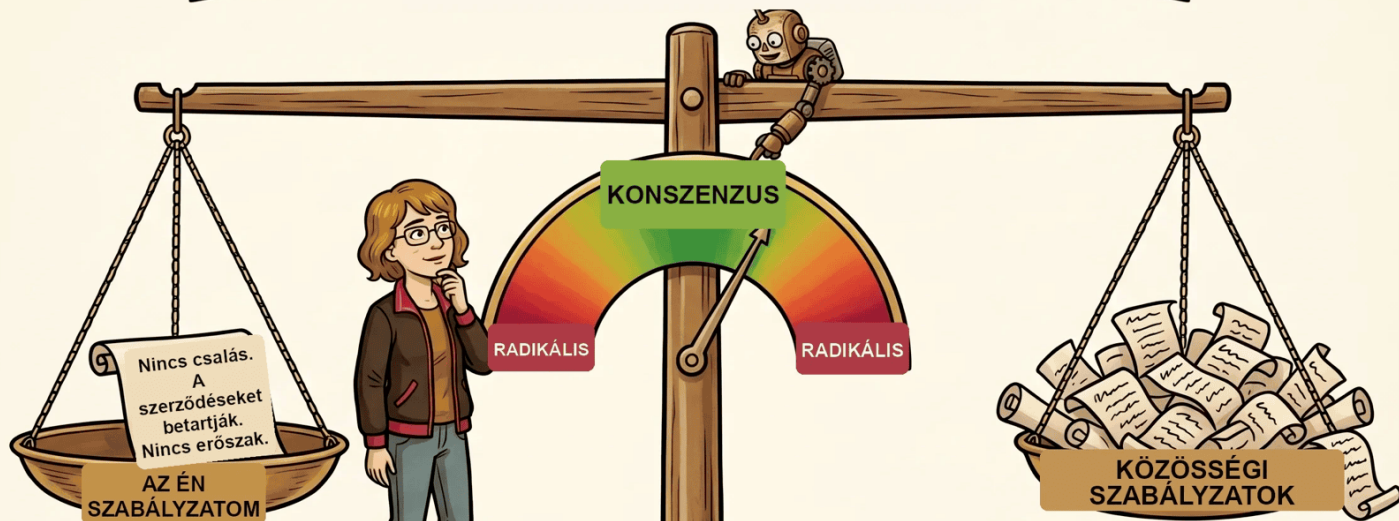
NINCS ENGEDÉLY, AMIT KÉRNI KELL. NINCS DUGÓ, AMIT KIHÚZNI.

Konszenzus

A javasolt megoldásnak a természeténél fogva tartalmaznia kell egy mechanizmust a konszenzus kialakulására, valamint egy elnyomó összetevőt azokra az esetekre, amikor a konszenzust megszegik. Nem kell önkéntes win-win megállapodásnak lennie. Elég, ha a körülmények és a társadalmi nyomás egy közösségen belül és közösségek között biztosítja a kompromisszumot.

MARADJ A SÁVBAN — NE LÉGY RADIKÁLIS.

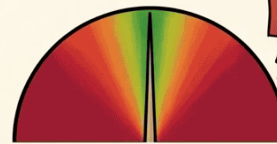
Eltérhetsz. Csak ne túlságosan.



SZABAD
TÁRSADALOM

A tűréshatár a kultúra
szabadságával tágul.

4. ELŐFELTÉTEL AZ 5-BŐL: KONSZENZUS



TEKINTÉLYELVŰ
TÁRSADALOM



A KONSZENZUS TŰRÉSHATÁR, NEM EGYHANGÚ MEGEGYEZÉS.

Korrumpálhatatlanság

A cenzúrázhatatlanság kívülről védi a rendszert. De egy emberekből álló hálózat belülről is elrothadhat — egy autoritást megszereznek, egy deklarált szabályt csendben feladnak, a résztvevőket némán megvásárolják. A cenzúrázhatatlanság üres győzelem lenne, ha a benne lévő embereket következmények nélkül meg lehetne rontani.

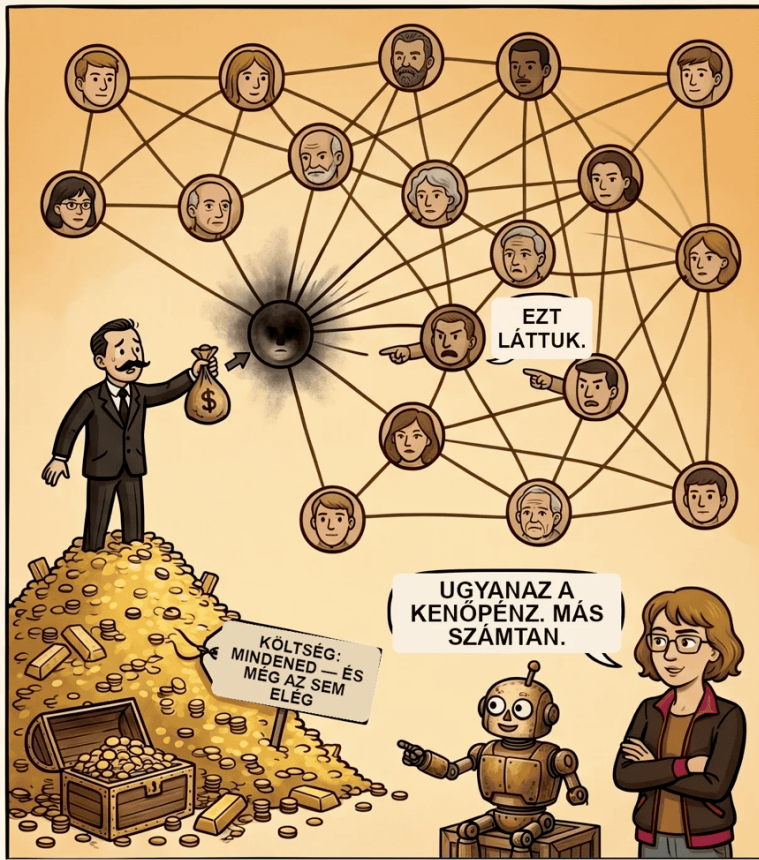
A korrumpálhatatlanság nem egyetlen ügyes trükk eredménye. A **javasolt terv több elvének összjátékából** bontakozik ki — a korrupció elleni nyomás szét van osztva az architektúrában, és az egyes részek erősítik egymást. Hogy pontosan hogyan érjük el ezt, azt fokozatosan mutatjuk meg — az eszköz leírásában, az ellenőrzésben és a büntetésről szóló fejezetben. A végén összefoglalunk mindent, ami felépült.

A korrumpálhatatlanság egyszerre a terv előfeltétele és az eredmény emergens tulajdonsága. Ez a második védelmi vonal — a befelé néző —, és nélküle az ellenállóképesség csak fél pajzs.

5. ELŐFELTÉTEL AZ 5-BŐL: MEGVESZTEGETHETETLENSÉG



Vesztegess meg pár felső emeletet — az alap ügyis fizet.



Vesztegess meg egyet — örökre elveszti a reputációját. Vesztegesd meg mindet — előbb mész csődbe.

A KORRUPCIÓNAK ÁRA VAN. A HÁLÓBAN TÚL MAGAS.

Az eszköz

Reputáció alapú közösségi hálózat

A változás előidézéséhez gondosan megtervezett eszközre van szükségünk. Először röviden felvázoljuk, a későbbi fejezetekben pedig részletesebben megvizsgáljuk az egyes darabokat, és továbbiakat is hozzáteszünk. Képzeld el egy cenzúrázhatatlan, globális, decentralizált közösségi hálózatot, ahol biztonságosan létrehozhatnád és kezelhetnéd a helyettesítő identitásodat — az úgynevezett decentralizált identitást (DID). A DID egy olyan digitális identitás, amelyet magad hozol létre és irányítasz, bármely központi hatóságtól való függés nélkül. Senki nem tudja elvenni vagy meghamisítani, mert kriptográfiailag a privát kulcsoddal (vagy kulcsaiddal, multisig révén) van aláírva.

A TE IDENTITÁSOD, A TE KULCSAID, A TE SZABÁLYAID

TE MAGAD HOZOD LÉTRE

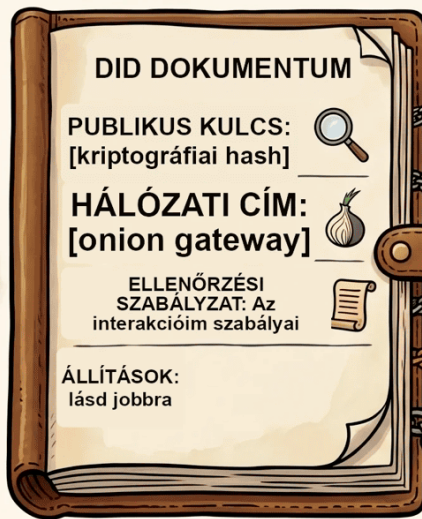
PRIVÁT KULCS — a nevedben ír alá. Csak nálad van. Soha ne oszd meg.

PUBLIKUS KULCS — ellenőrzi az aláírásaidat. A hálózat számára látható.



Nincs regisztrációs hivatal. Nincs állami űrlap. Nincs céges jóváhagyás. Te magad hozod létre.

A TE DID DOKUMENTUMOD



Ez a publikus identitásod. Bárki elolvashatja. Csak a TE privát kulcsod írhatja alá a változásait.

Ezt egyetlen állam sem vonhatja vissza.

ÁLLÍTÁSOK — ELLENŐRZÖTT TÉNYEK RÓLAD

ÁLLAMPOLGÁRSÁG:
Csehország — hitelesítette a Városi Köjegyző

VÉGZETTSÉG: MSc informatika — hitelesítette az Egyetemi Öregdiák-hálózat

TULAJDON: A 42. lakás tulajdonosa — hitelesítette a Helyi Községi Nyilvántartás

PASSZÍV TANÚ: Figyelmem kívül hagyott egy visszaélést — a szabályzat nem teljesült — benyújtotta a Szomszédsági Tanúk

CSALÁS: Megkárosította egy szomszéd megtakarításait — benyújtotta a Helyi Községi Bíróság

Az állítások ellenőrzött kijelentések. A jók és a rosszak. A hatóságok a reputációjukat teszik rájuk.



ÁLLAMI IGAZOLVÁNY — VISSZAVONHATÓ: az állam bármikor törölheti.



DID — VISSZAVONHATATLAN: csak a saját privát kulcsod írhatja alá a változásokat.

A te identitásod. A te kulcsaid. A te szabályaid. Nem kell engedély.

Megjegyzés

Ennek egyik következménye, hogy egy ilyen identitás fokozatosan felválthatná az állam által kiadott azonosító okmányokat — de erről többet az átmenetről szóló fejezetben.

Egy ilyen hálózatban az identitásodon keresztül bejelenthetnéd, hogy valaki kárt okozott neked (és később esetleg azt is, hogy orvosolta, vagy rákényszerült az orvoslásra). Ahhoz, hogy ez a visszajelzés — amely a károkozó felé irányul — releváns forrásként értéket képviseljen, az információ hálózatba juttatásának időbe, energiába és pénzbe kell kerülnie — ráadásul ellenőrizhető bizonyítékot kell előállítani mások számára, hogy ez nem üres fecsegés.

Az információ olvasása könnyű és viszonylag olcsó lenne, de egy egyéni bejegyzés létrehozása költséges és igényes. Az írás világos protokollt követne, amelyben a választott algoritmus szerinti számítás szigorúan meghatározza, melyik DID-et kell megkérni a benyújtott információ ellenőrzésére, és hogyan kell eljárni ahhoz, hogy a kiválasztott résztvevő a nevedben feldolgozza az információt, közzétegye, és annak ellenőrzőjévé váljon.

■ Algoritmus kontra radikalizmus

Az ellenőrzők algoritmikus kiválasztása biztosítja, hogy a nem radikális információközzétevők idővel közel semleges egyensúlyt tartanak fenn a közzétett információ költségei és az ellenőrzésért járó jutalmak között.

A KÖZZÉTÉTEL IDŐBE, ENERGIÁBA ÉS PÉNZBE KERÜL

A HÁLÓZATBA ÍRNI SOHA NEM INGYENES — OLVASNI IGEN

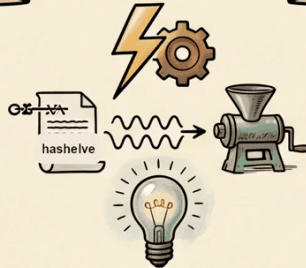
HÁROM CSATORNA — MINDHÁROM VALÓDI

IDŐ



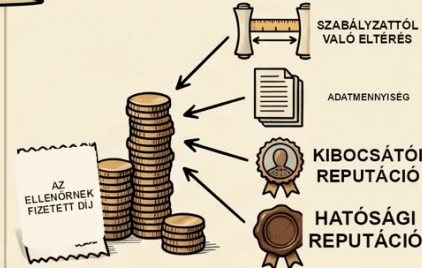
vársz, míg az algoritmus ellenőrt választ, és az ellenőr elolvassa a bejegyzésedet.

ENERGIA



aláírás, hashelés, ellenőrzés — minden lépés valódi számítás és valódi áram.

PÉNZ



minél messzebb van az állításod az ellenőr szabályzatától, minél nagyobb a bejegyzés, és minél kevésbé megbízható a kibocsátó vagy a hatósága — annál magasabb a díj.

MI TÖRTÉNIK EZUTÁN

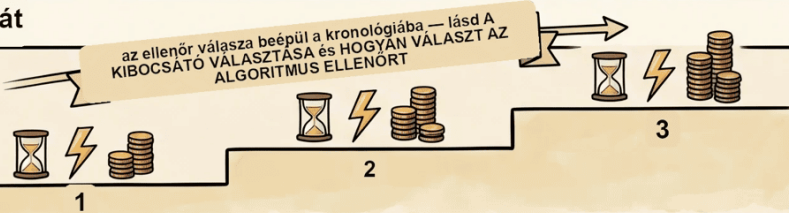
A háromlépéses ellenőrzési lánc — lásd HOGYAN VÁLASZT AZ ALGORTMUS ELLENŐRT, HOGYAN VÁLASZOL AZ ELLENŐR, A KIBOCSÁTÓ VÁLASZTÁSA

Miért védi a drága írás a reputációt — később a fejezetben

a zaj drága. A jel értékes. Ezért kér a hálózat pénzt az írásért, nem az olvasásért.

költség az iterációkon át

MINDEN ÚJRAPRÓBÁLKOZÁS TÖBBE KERÜL



minden elutasítás vagy újradobás növeli a kronológiát, amit az algoritmus felemészt — és a következő próbálkozás mindhárom csatornán drágább.

olvasási aszimmetria

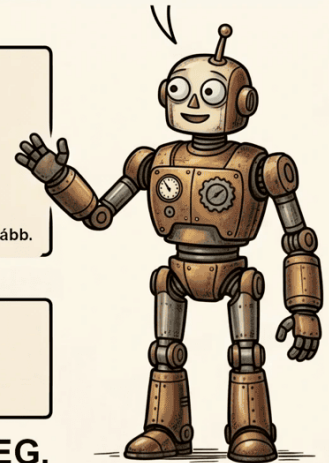
OLVASNI OLCSÓ



ingyenesen lekérdezhető

bárki olvashat reputációt és bejegyzéseket — csak az írás kerül pénzbe. Az aszimmetria a lényeg.

AZ ÍRÁS KÖLTSÉGES — AZ OLVASÁS NEM. AZ ASZIMMETRIA A LÉNYEG.



Nézzük meg, hogyan választ ki az algoritmus egy ellenőrzőt.

■ Algoritmus

Az algoritmikus kiválasztás nemdeterminisztikusan más-más ellenőrzőt (vagy lehetséges ellenőrzők egy halmazát) választ ki különböző információdarabokhoz. A teljes DID-dokumentum hashe (egyirányú matematikai függvény, amely bármely bemenetből egyedi „ujjlenyomatot” állít elő — mint egy dokumentum ujjlenyomata) határozza meg a pozíciót egy konzisztens hash-gyűrűn, és jelöli ki az ellenőrzőjelölteket.

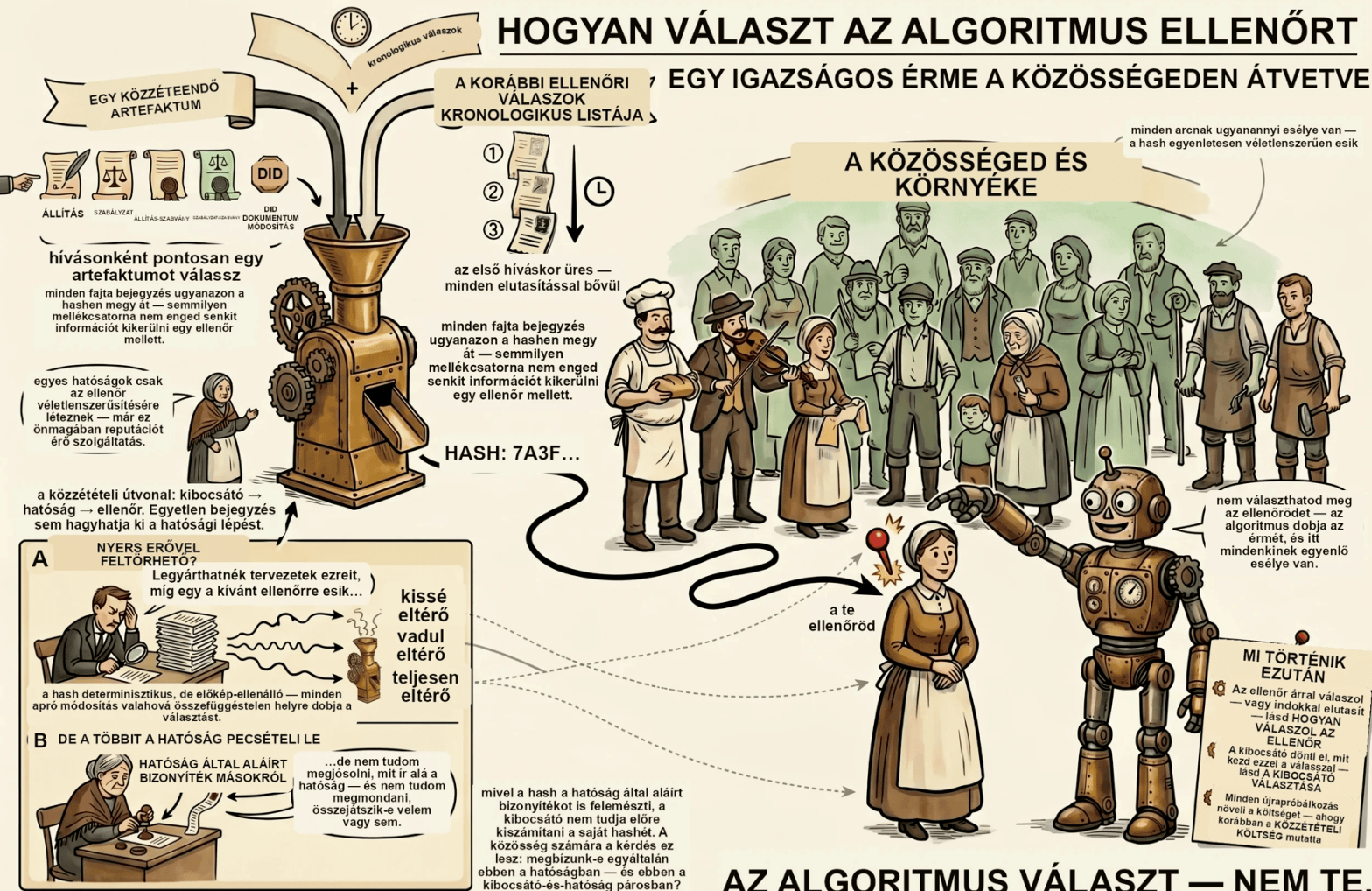
$$\text{verifier_DID} = \text{hash}(\text{DID_document})$$

Egyszerűen szólva: az algoritmus fogja a teljes DID-dokumentumot, ujjlenyomatot számol belőle, és ez az ujjlenyomat határozza meg az ellenőrződöt.

Az első ellenőrzővel, amelyet az algoritmus kiválaszt, közvétevéként nem biztos, hogy sikerrel jársz — a reputációd vagy a deklarált beállításaid nem feltétlenül felelnek meg a követelményeiknek. Algoritmikusan folytatnád a keresést a következő után egy újabb rekurzív iterációval, amely további ellenőrzőt rendel hozzád. Minden lépéssel nő a „távolság” a célként kijelölt ellenőrzőig, és nő a hozzá tartozó, közvéteendő metaadat is. Ahogy az adat nő, a költségek természetes módon emelkednek (nemcsak az állítás kezdeti mérete miatt, hanem az egyes elutasításokkal felhalmozódó metaadat miatt is). A hiteles információ jóval könnyebben átmegy, mint az értelmetlen szeszélyek. Mindenkin múlik, mekkora árat hajlandó megfizetni, és mennyire fontos neki a bejegyzés — a radikalizmus garantáltan drágává válik.

HOGYAN VÁLASZT AZ ALGORITMUS ELLENŐRT

EGY IGAZSÁGOS ÉRME A KÖZÖSSÉGEDEN ÁTVETVE



HOGYAN VÁLASZOL AZ ELLENŐR

ELFOGADÁS ÁRRAL — VAGY ELUTASÍTÁS INDOKKAL

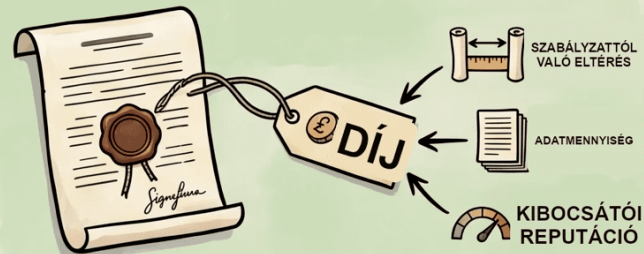


ELUTASÍTÁS — INDOKKAL

-
- a kibocsátó reputációja túl alacsony nekem
 - a bejegyzés mögötti hatóságban nem bízom
 - a kibocsátó szabályzata túl messze van az enyémtől, nem áthidalható
 - maga a dokumentum megbukik a szabályzatom szabályain

az ellenőr leírja, hogy MIÉRT — a válasza visszahat a következő próbálkozásra.

ELFOGADÁS — ÁRRAL



az ellenőr vállalja a közzétételt — de az ár tükrözi, milyen messze van az állítás a szabályzatától, mennyi adatot hordoz, és mennyire megbízható a kibocsátó.

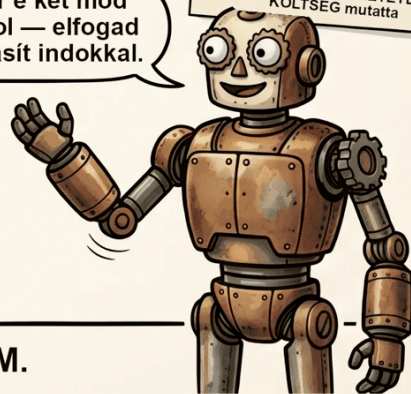
az ellenőr válasza bekerül a kronologikus listába — ahogy a HOGYAN VÁLASZT AZ ALGORITMUS ELLENŐRT mutatja

bármit mond az ellenőr, a válasza a következő hívás bemenete lesz.

minden ellenőr e két mód egyikén válaszol — elfogad árral, vagy elutasít indokkal.

MI TÖRTÉNIK EZUTÁN

- ⚙️ A kibocsátó dönti el, mit kezd ezzel a választal — lásd A KIBOCSÁTÓ VÁLASZTÁSA
- ⚙️ Minden válasz módosítja a következő próbálkozás költségét — ahogy korábban a KÖZZÉTÉTELI KÖLTSÉG mutatta



AZ ELLENŐR VAGY ÁRAT SZAB — VAGY MEGMONDJA, MIÉRT NEM.

Bármit dönt is az ellenőrző az ellenőrzési kérésedre válaszul, a labda visszakerül a közzétevő térfelére: elfogadhatja az ellenőrző ajánlatát az ellenőrzési szolgáltatásra, beledolgozhatja a választ a kronológiába és újra próbálkozhat (drágábban), vagy elsétálhat és lenyelheti az elsüllyedt költséget.

Hogy nagyobb súlyt és jobb esélyt adj az információnak az ellenőrzőknél való elfogadásra, köz-zétevőként — akinek érdeke fűződik a kibocsátott információhoz — igénybe vehetnéd egy **megbízható autoritás** szolgáltatásait. Az autoritás vagy elutasítja a benyújtott információt, vagy elfogadja, és a jó nevét (reputációját) teszi rá. Az autoritás jellemzően valós bizonyítékokat kér, ellenőrzi és osztályozza azokat. A kimenet egy jegyzőkönyv az adott ügy adott időpontban való megítéléséről. Úgy gondold egy autoritásra, mint egy bizonyos szolgáltatástípus szakértőjére a valós és a digitális világban egyaránt — például nyomozó, könyvvizsgáló, biztosító, egy adott áruosztály beszállítója (lényegében a piac bármely gazdasági szereplője).

A KIBOCSÁTÓ VÁLASZTÁSA

MIT KEZDJ AZ ELLENŐR VÁLASZÁVAL

bármít mondott az ellenőr, a kibocsátónak most EGY válasz van az asztalon.



vissza a HOGYAN VÁLASZT AZ ALGORITMUS ELLENŐRT-HÖZ — korábban látható

csak az újrapróbalkozás útja ciklikus — az elfogadás és a továbblépés is lezárja a történetet.

HÁROM KIÚT

FOGADD EL AZ AJÁNLATOT

DID-hálózat



CSAK HA ELFOGADTÁK



a kibocsátó megfizeti a díjat — a bejegyzés bekerül a hálózatba. Csak akkor elérhető, ha az ellenőr elfogadta.

PRÓBÁLD ÚJRA



a válasz bekerül a kronológiába — az algoritmus újra dob. Akkor is működik, ha az ellenőr olyan áron fogadott el, ami a kibocsátónak nem tetszik, vagy ha egyenesen elutasított.

LÉPJ TOVÁBB



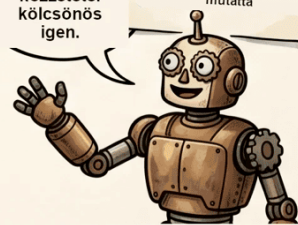
a már elköltött idő és energia nem tér vissza



a kibocsátó eldobja a tervezetet. Semmi sem kerül közzétételre — de többet sem fizet.

MI TÖRTÉNIK EZUTÁN

Minden újrapróbalkozás módosítja a következő próbálkozás költségét — ahogy korábban a KÖZZÉTÉTELI KÖLTSÉG mutatta. Maga az ellenőr válasza — ahogy korábban a HOGYAN VÁLASZOL AZ ELLENŐR mutatta.



AZ ELLENŐR JAVASOL — A KIBOCSÁTÓ DÖNT.

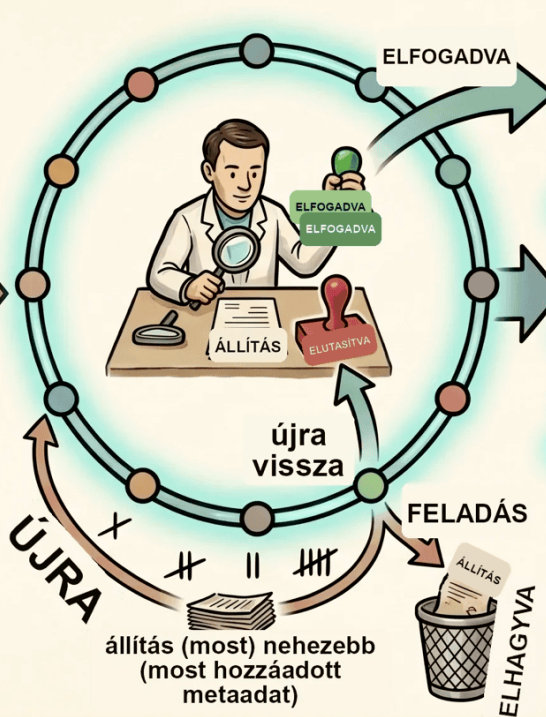
1. SZAKASZ — ÁLLÍTÁS KÖZZÉTÉTELE



2. SZAKASZ — MINŐSÉGI SZŰRŐ



3. SZAKASZ — REKURZÍV ELLENŐRZÉS



4. SZAKASZ — VÉGLEGES BEJEGYZÉS



Végleges.
Ellenőrizhető.
Nyilvános.

HAMISÍTANI DRÁGA. ELLENŐRIZNI OLCSÓ.

Mire próbálj információkat közzétenni a hálózatban, az valószínűleg már tartalmaz információt a szereplőiről — ezek a reputációs jelek. Nem feltétlenül triviális eligazodni abban, hogyan olvassuk a reputációs jeleket — mit jelentenek számodra a különböző helyzetekben, és milyen kockázatokat hordoznak. Minden résztvevő másképp nézheti a reputációs bejegyzéseket a saját DID-jén keresztül, attól függően, milyen helyzetet kezel az ellenféllel kapcsolatban. Megbízható fizető-e az ellenfél, vagy elő kell kérnem a pénzt egy üzleti tranzakcióhoz? A kínált termékhez tartoznak-e értékelések rejtett csalásról vagy hibákról? Próbál-e kibújni a szerződéses felelősség alól, amikor valami balul üt ki? Néha jól jön az ellenfél általános konzisztenciájának összetettebb nézete — attól függ, mit preferál az, aki az áttekintést kéri. A piac kínálhatna termékeket és szolgáltatásokat, amelyek egyszerűsítik, feldolgozzák és tisztázzák a reputáció olvasását az adott helyzet kontextusában. Erre a célra a különféle autoritások és az általuk kínált szolgáltatások is szolgálhatnak.

HOGYAN OLVASD A REPUTÁCIÓT

TÁJÉKOZOTT DÖNTÉS



Tudja, kivel van dolga.

VAK BIZALOM



Fogalma sincs, kivel van dolga.

MIELŐTT HITELT ADSZ. MIELŐTT ALÁÍRSZ. MIELŐTT BÍZOL.

■ Példák

A közzetevők számára jellemzően érdekes — és mások számára értékes — információk a hétköznapi, valós vagy virtuális világbeli, személyközi kommunikáción túli eseményekre vonatkoznak.

Negatív példák: - bűncselekmények bizonyítékai (pl. megbízható nyomozó testület által auditálva) - közvetett bizonyítékok (önmagukban gyengék, de statisztikailag halmozódók) — pl. ismételt jelenlét több lopás közelében rövid idő alatt → még mindig véletlen? - szerződésszegés

Pozitív példák: - orvosolt kár (önként vagy a közösség nyomására, büntetésként) - egy X autoritás által javasolt büntetés elfogadása és letöltése - X autoritás bizonyos mértékig visszavonta az elkövető tulajdonjogainak elismerését

Mindenkin múlik, hogy összegyűjti-e az ellenfélről elérhető információt, és a preferenciái szerint felméri-e a kockázatokat.

■ **Hogy megjelenik-e rólad információ a hálózatban, az kizárólag a saját viselkedéseden múlik.**

Sosem kell csatlakoznod egy ilyen hálózathoz, mégis megjelenhet rólad benne információ. Ez kizárólag a tetteiden és azok másokra gyakorolt hatásán múlik.

PÉLDÁK AZ ÁLLÍTÁS ARTEFAKTUMRA

(az állítás egy kijelentés valakiről — íme a
fajták, amiket az emberek közzétesznek.)





KÁR ORVOSOLVA

helyrehozta a korábban okozott kárt



TARTOZÁS RENDEZVE

teljesen megfizette, amivel tartozott



SEGÍTSÉG NYÚJTVA

másnak segített saját áldozat árán



IGAZOLT SZAKÉRTELEM

bizonyított jártasság egy mesterségben vagy szakterületen



KIEMELKEDŐ SZOLGÁLAT

hosszú távú hozzájárulás a közösséghez

csak példák — minden állítás egy állítás-szabványt követ, és bármely szabvány továbbiakat adhat hozzá.

nem kell csatlakoznod — de ha a viselkedésed másokat érint, valaki állítást tehet közzé róla.

AZ ÁLLÍTÁSOKON KERESZTÜL KERÜL A VISELKEDÉS A HÁLÓZATBA.

A KÖZÖSSÉG NYITHAT EGYET HELYETTED



Nincs saját DID-je.
Sosem regisztrált.



Nem nyitottál DID-et, így a közösség nyit egyet RÓLAD. A negatív állítások ide kapcsolódnak.



Nyithatsz sajátot — de a közösség összekapcsolja a kettőt. A reputáció a személyt követi, nem a kulcsot.

3. NEM MENEKÜLHETSZ

1. KÁRT
OKOZOL

2. A KÖZÖSSÉG
BENYÚJTJA

Kihagyhatod a DID nyitását. A reputációdát nem hagyhatod ki.

Amit az imént röviden felvázoltam, az az, hogyan működhet egy decentralizált identitás (DID) ihlette közösségi hálózat. A DID-koncepciók elsődleges célja a magánélet és a szabadság erősítése az „aláíratkozás” elve mentén, vagyis azon szabályokra, amelyeket követni fogok és amelyek szerint élni fogok — megadva a felhasználóknak azt a képességet, hogy eldöntsék, milyen információt osztanak meg és milyen feltételekkel.

Azt javaslom, hogy a DID-eket kössük tovább egy kommunikációs hálózatba, amelyben a tulajdonosok akkor is visszajelzést cserélnek, amikor éppen nem történt valakivel valami, amire a közösségnek vagy egy egyénnek reagálnia kellene. Azoknak a szabályoknak az ilyen megelőző összevetése, amelyekre aláíratkoztunk — azzal a lehetőséggel, hogy kiszámítsuk a kölcsönös eltérések gazdasági és egyéb következményeit abban, amit a másik féltől elvárunk annak működéséről — a konszenzuskeresés motivációjának tekinthető. A szabadság helyett egy ilyen rendszer az önkéntes döntéshozatalt hangsúlyozná, párosítva a valós viselkedésért való felelősséggel.

Egy egyén egyedül nem tudja megtörni a rendszert — egy embercsoportnak nagyobb esélye van, egy olyan embercsoportnak pedig, amely kialakított konszenzussal és sok kérdésben az egy irányba húzás motivációjával bír, még nagyobb esélye van ellenállni a tekintélyelvű tendenciáknak. Az első fejezetből ismert szerveződési előfeltétel akkor teljesül, ha két feltétel megvalósul: a DID-reputációs hálózat elég reprezentatívan lefedi a közösségeket ahhoz, hogy a használata megszűnjön egzotikusnak lenni. És ezzel egy időben ez a közösségi szegmens olyan gazdaságilag jelentős kisebbséggé válik, amely magabiztosan képes tárgyalni a társadalom többi részével.

■ Önkéntesség kontra szabadság

A szabadság — pozitív értelemben — két tényező kiegyensúlyozásának másodlagos hatása lenne: az önkéntességé és a környezet felelősség felé irányuló nyomásáé.

■ Az MI-korszak és a reputáció értéke

A mesterséges intelligencia korában minden, ami a kognitív gondolkodáshoz kapcsolódik, automatizálódik — és lehet, hogy még tovább is megy. Mi marad ekkor az emberi tevékenységben versenyelőnyként? A válasz nehéz, és biztosan találunk valamit, de egyet bizonyosan mondhatunk: a reputáció fog dönteni. A viselkedésed ellenőrizhető története, a vállalásaid és azok teljesítése — ezt az MI nem építi fel helyetted.

HA AZ MI GONDOLKODIK — MI MARAD NEKED?

AZ MI-ÜGYNÖKÖK ÁTVESZIK AZ ISMÉTLŐDŐ MUNKÁT

SZABVÁNYOSÍTOTT
CÉGES FOLYAMATOK

KÖNYVELÉS

FOGALMAZÁS

egyesével adják át az ismétlődő
szellemi munkát az ügynököknek.

AKKOR MI MARAD AZ EMBERNEK?



PÉK



AZ ÖTLET



ÁCS



MI-MŰHELY
VEZET



bárki választhatja ugyanazt az ötletet.
mitől más az egyik pék, az egyik
ács, az egyik MI-műhely a másiktól?

REPUTÁCIÓ — AMI MEGKÜLÖNBÖZTET
KETTŐT

ÁLLJA A
SZAVÁT

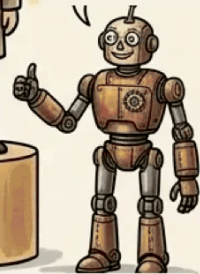
SZÓBA ÁLL AZ
ÜGYFELLEL

KIÁLL A SAJÁT
MI-JE MÖGÖTT

10 ÉV. NULLA
PANASZ

az emberi érintés
még mindig lezárja
az üzletet.

Ezt még én sem
építhetem meg
helyette — neked
kell lenned.



valakinek felelnie kell azért, amit az ügynök
teszt — és ez a felelősség nem adható át.

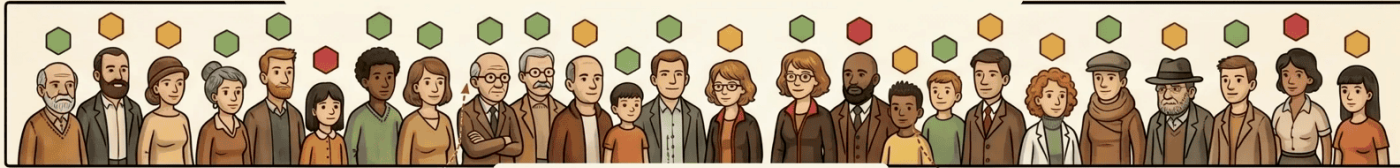
reputáció nélkül minden pék egyformának tűnik — és a legnagyobb márka mindet felfalja.

lehet, hogy ez a decentralizált út tartja pórázon az MI-t — az, ami megakadályozza, hogy bármely egyetlen szereplő birtokolja az egész piacot?

AZ MI AUTOMATIZÁLJA A MUNKÁT — A REPUTÁCIÓ TART EMBERNEK.

AZ IGAZSÁG GAZDASÁGTANA

közösségi
sáv



EGY KÖZSÉG. KÜLÖNBÖZŐ ÁLLÁSPONTOK.

NÉPSZERŰTLEN, DE ELFOGADHATÓ

KONSZENZUSON
BELÜL

KONSZENZUSON KÍVÜL

A
BENYŰJTÁS



A
SORSOLÁS



A
VISSZATÉRÍTÉS

A
FŐKÖNYV



AZ ALGORITMUS TISZTESSÉGESEN
VÁLASZT. AZ EMBEREK
BEÁRAZZÁK, AMIBEN HISZNEK.



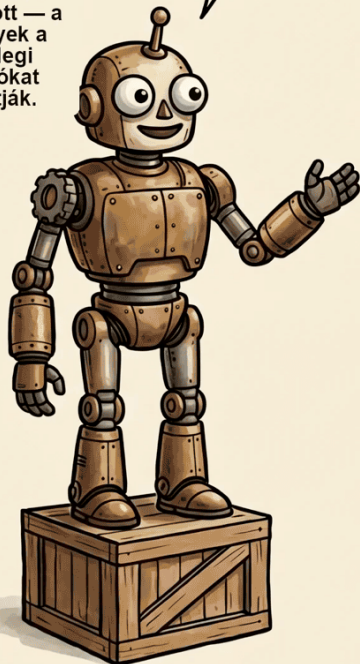
ALSÓ
MEGFIEGYELŐ
SÁV

EGYENLETES SORSOLÁS. NEM EGYENLETES VÁLASZ. MINÉL TÁVOLABB A KONSZENZUSTÓL, ANNÁL MAGASABB AZ ÁR.

MI KERÜL KÖZZÉTÉTELRE A HÁLÓZATBAN

öt dolog tehető közzé
— mindegyiknek
vannak verziói.

minden
artefaktum
verziózott — a
jelvények a
jelenlegi
revíziókat
mutatják.



v1

DID DOKUMENTUM

az identitásod bejegyzése
a hálózaton — kulcsok,
metaadatok, hálózati cím.

KEZELI: a DID birtokosa



v2

ÁLLÍTÁS-SZABVÁNY

a séma, amelyet egy
állításnak követnie kell —
mi számít érvényes
bizonyítéknak.

KEZELI: egy hatóság,
amelynek reputációja van az
adott területen



ebből
származik



v3

SZABÁLYZAT-SZABVÁNY

a séma, amelyet egy
szabályzatnak követnie kell —
az elfogadási szabályok
formája.

KEZELI: egy hatóság, amelynek
reputációja van az adott
területen



ebből
származik



v4

ÁLLÍTÁS

kijelentés egy alanyról, egy
állítás-szabványt követve — egy
kibocsátó teszi közzé, a
szabvány hatósága társaláírja, ha
a kibocsátó és az ellenőr is kéri.

KEZELI: a kibocsátó teszi
közzé — az alany a célpont
az állítások kétfélek —
pozitív (+) és negatív (-).



v5

DID SZABÁLYZAT

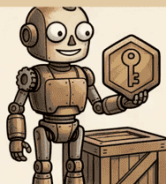
egy DID kinyilvánított
szabályai — ellenőrzésnél,
konszenzusnál és
kibocsátásnál használva.

KEZELI: a DID birtokosa
(DID-enként egy szabályzat)

MINDEN ARTEFAKTUM VERZIÓZOTT. MINDEN VERZIÓ NYILVÁNOS.

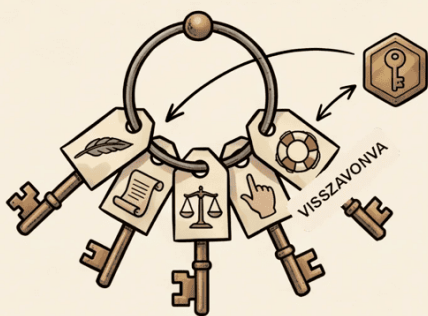
MI VAN EGY DID DOKUMENTUMBAN?

PÉLDÁK A DID DOKUMENTUM ARTEFAKTUMRA



a DID dokumentumod a személyi igazolványod a hálózaton — íme, mit tartalmaz.

MEZŐK, AMIKET BENNE TALÁLSZ



KULCSOK ÉS ALÁÍRÁSI SZABÁLYOK

minden kulcs egy jogosultságot ad — e dokumentum szerkesztése, állítás kibocsátása, hatóságként fellépés, szabályzat kezelése vagy helyreállítás delegálása. A jogosultságok átadhatók egy másik DID-nek, és később visszavonhatók.



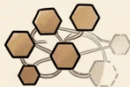
HÁLÓZATI CÍMEK

ahol a hálózat elérhet — módosítható az identitásod átírása nélkül



LÉTREHOZVA ÉS VERZIÓZVA

mikor jelent meg először ez az identitás, és melyik revíziót olvasod most



KAPCSOLT IDENTITÁSOK

azon DID-ek összefoglalója, amelyekhez kapcsolódsz — kényelmi nézet, technikailag máshol tárolva



UTÓDLÁSI JELÖLŐ

ha az identitásod elveszik vagy ellopják, egy hatóság lezártként jelölheti ezt a DID-et és megjelölheti az utódodat

a DID birtokosa írja minden új verziót — de minden verziónak át kell mennie az ellenőrzésen, mielőtt a hálózat közzéteszi.

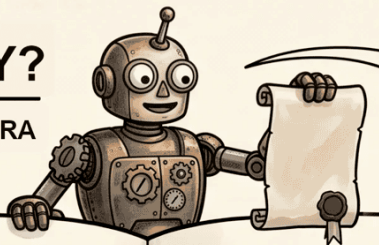
te írod — a hálózat ellenőrzi. Nem hozhatod létre magad pusztán közzététellel.



TE ÍROD AZ IDENTITÁSODAT — A HÁLÓZAT MEGERŐSÍTI.

MI AZ ÁLLÍTÁS-SZABVÁNY?

PÉLDÁK AZ ÁLLÍTÁS-SZABVÁNY ARTEFAKTUMRA



a szabvány az üres űrlap — az állítás a kitöltött űrlap. Hadd mutassam meg mindkettőt egymás mellett.

A SZABVÁNY — AZ ÜRES ŰRLAP



ALANY DID

a DID, amelyről ez az állítás szól



KIBOCSÁTÓ DID

a DID, amely aláírja az állítást



MIKOR ÉS HOL

egy dátum és egy hely



JÓVÁHAGYOTT BIZONYÍTÉKTÍPUSOK

csak ezek a bizonyítékfajták számítanak



nincs /
enyhe /
mérsékelt
/ súlyos

EREDMÉNYSKÁLA

pontosan egy fokot válassz — nincs szabad szöveg

EGY ÁLLÍTÁS — A KITÖLTÖTT ŰRLAP



ALANY DID

did:nwo:alice-9f2b...



KIBOCSÁTÓ DID

did:nwo:magistrates-04...



MIKOR ÉS HOL

Március 3., piactér



JÓVÁHAGYOTT BIZONYÍTÉKTÍPUSOK
fénykép ✓ — tanúeskü ✓ —
orvosi igazolás ✓



JÓVÁHAGYOTT BIZONYÍTÉKTÍPUSOK

mérsékelt — 2. fok a 4-ből

a bal oldali minden mezőnek pontosan egy kitöltött párja van jobbra — ettől lesz két azonos fajtájú állítás összehasonlítható.

a hatóság pecsétje egy kitöltött állításon
fogadalom: az eljárást valóban
betartották.



A reputáciomat
teszem rá, hogy ezt a
szabvány szerint
dolgozták fel.

TESTI
SÉRTÉS v3



TARTOZÁS
v2



ORVOSI
SEGÍTSÉG v4



MESTERSÉG
v1



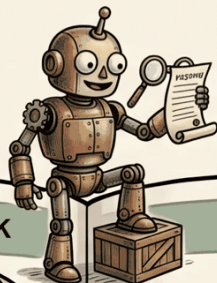
TANÚVALLOMÁS
v5



A SZABVÁNY AZ ŰRLAP — AZ ÁLLÍTÁS A KITÖLTÖTT ÉS FOGADALOMMAL MEGERŐSÍTETT ŰRLAP.

MI A DID SZABÁLYZAT?

PÉLDÁK A DID SZABÁLYZAT ARTEFAKTUMRA



a szabályzatom nem arról szól, hogyan írnak meg egy állítást — az a szabvány dolga. A szabályzatom arról szól, hogyan döntöm el, hogy egyáltalán foglalkozom-e az állítással: megbízom-e abban, aki aláírta, megbízom-e a szabványuk mögötti hatóságban, és egyáltalán megéri-e a figyelmemet a dolog?

A SZABVÁNY — ÖRÖKÖLT ALAPÉRTÉKEK

SZABÁLY NEVE



**KIBOCSÁTÓI
REPUTÁCIÓS
KÜSZÖB**

Elfogadom a tizből öt feletti reputációjú kibocsátókat



**HATÓSÁGI
BIZALMI
LISTA**

Elfogadom bármely hatóság szabványait, amelynek saját reputációja tizből négy felett van



**JELENTŐSÉG
SZŰRŐ**

Feldolgozok minden állítást, amelynek ügye a 'jelentéktelen' szint fölött van



**SPAM-ELLENES
ÁRGÖRBE**

hozzám benyújtani olcsó a lényegi, ritka állításoknál — és gyorsan drágul a jelentéktelen vagy ismételt esetében



**KOMBINÁLT
SÚLYOZÁS**

a kibocsátói és hatósági reputáció összeszorodik, a jelentéktelen ügy megfelel az eredményt

a szabályzat nem írja át a szabványt — az embereket és az ügyet ítéli meg. Megtart, módosít, eltávolít, hozzáad — négy egyszerű lépés egy közös kiindulóponton.

AZ ÉN SZABÁLYZATOM — EBBŐL SZÁRMAZTATVA

✓ MEGTARTVA pipa
✗ ELTÁVOLÍTVA cselekvő szó
✗ ELTÁVOLÍTVA cselekvő szó
✗ ELTÁVOLÍTVA cselekvő szó
✗ ELTÁVOLÍTVA cselekvő szó

szabály neve



**KIBOCSÁTÓI
REPUTÁCIÓS
KÜSZÖB**

szigorítva — tizből hetet követelek meg



**HATÓSÁGI
BIZALMI
LISTA**

Teljesen megbízom a bírakban és az orvosokban, megfelezem a városi felügyelet alatti állítások súlyát, a kikötői rendőrség alá tartozó bármit teljesen elutasítok



**JELENTŐSÉG
SZŰRŐ**

a jelentéktelen zaklató állítások figyelmen kívül hagyása sem kerül — egyszerűen nem olvasom el őket



**SPAM-ELLENES
ÁRGÖRBE**

megtartva — az alapértelmezett görbe megfelel nekem



**KOMBINÁLT
SÚLYOZÁS**

eltávolítva — saját képletet használok



**EXPONENCIÁLIS
KÖLTSÉG AZ
ISMÉLT
ÁLLÍTÁSOKRA**

hozzáadva — ugyanattól a kibocsátótól rólam egy éven belül minden új állítás tízszer annyiba kerül, mint az előző



**CSENDES
ÓRÁK**

hozzáadva — elutasítom minden éjféli és hajnal között benyújtott állítás elolvasását



ELLENŐRZÉS — a szabályzatom a beérkező állításokat és a saját tervezeteimet is szűri, mielőtt kibocsátom őket. A kibocsátás kifelé irányuló ellenőrzés.

KONSZENZUS — a szabályzatom a szavazatom, amikor a közösség közös szabályokról tárgyal.

A SZABÁLYZATOD A HÍRVIVŐT ÍTELI MEG — NEM AZ ŰRLAPOT.



Miért cenzúrázhatatlan a hálózat

Eddig azt írtuk le, mit tud a hálózat. Most arra összpontosítsunk, miért nem lehet leállítani vagy cenzúrázni.

A hálózat valószínűleg a Tor-hálózat és az onion routing (a hálózati forgalom Mixnet-elvekkel való elrejtésének módja) elveire épül majd — olyan technológiára, amelyben a kommunikáció több titkosítási rétegen halad át, és egyetlen csomópont sem ismeri egyszerre a feladót és a címzettet is. Egy központi intézmény nem tud a válladon átnézni, mert nincs honnan.

Harcolhatsz ellene, de nem győzhetsz — hacsak nem taszítod az egész országot a hálózati csomagok és minden, az internetre csatlakozó és az adott reputációs hálózaton kommunikáló hardver alacsony szintű műveleteinek szintjén zajló totális megfigyelésbe. És pontosan ez a választás áll a centralizmus előtt: vagy elfogadja, hogy a polgároknak van egy eszközük, amely elérhetetlen a számára, vagy beássa magát a gazdasági pangás sötét zugaiba a totalitárius ellenőrzés nevében.

Ne legyenek illúzióink — a demokratikus rezsimek is megpróbálják majd ezt a centralizmusért folytatott harcukban. Inkább bilincsbe verik az embereket, mintsem hogy feladják a hatalmat.

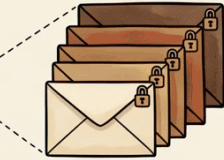
HOGYAN MARADNAK KÖVETHETETLENEK AZ ÜZENETEID KÉT VÉDVONAL EGYSZERRE — RÉTEGEK ÉS ZAJ

TARTALOM: RÉTEGEKBE CSOMAGOLVA

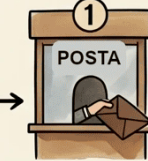
(a Tor mögötti technika — 'onion routing')



FELADÓ



négy zár, négy kulcs —
csomópontonként egy.



TUDJA: CSAK
A FELADÓT



TUDJA: CSAK A
SZOMSZÉDOKAT



TUDJA: CSAK A
SZOMSZÉDOKAT



TUDJA: CSAK
A CÍMZETTET



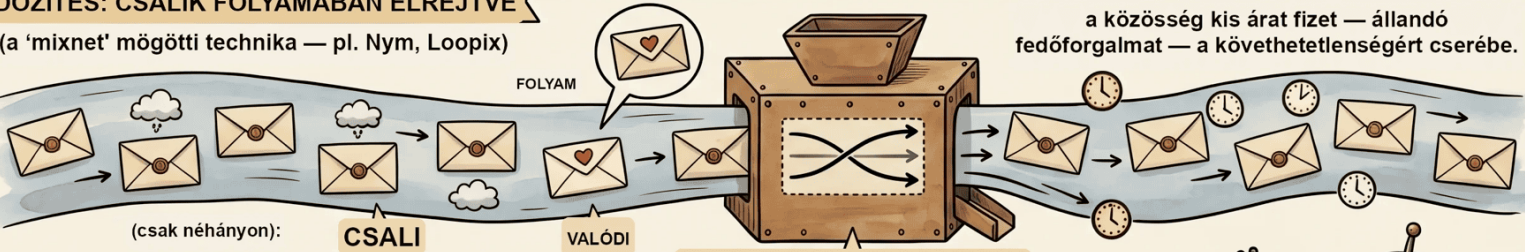
CÍMZETT

A TOVÁBBÍTÓLÁNC

egyetlen csomópont sem látja a beszélgetés mindkét végét.

IDŐZÍTÉS: CSALIK FOLYAMÁBAN ELREJTVE

(a 'mixnet' mögötti technika — pl. Nym, Loopix)



A KÉT PAJZS EGYÜTT

MÁTRIX	ELREJTI, KI ↔ KI?	ELREJTI, MIKOR?
CSAK RÉTEGEK	✓ IGEN	✗ NEM
CSAK ZAJ	✗ NEM	✓ IGEN
RÉTEGEK + ZAJ	✓ IGEN	✓ IGEN

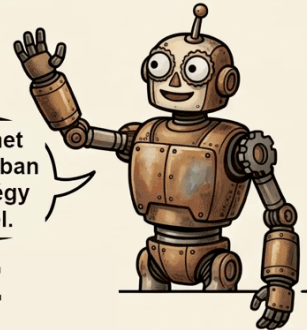
(onion routing + mixnet — a kombináció, amire szükségünk van)



óránként száz
boríték —
melyik számít?

a megfigyelő látja az áramlást,
de nem tudja megkülönböztetni
a VALÓDI CSALITÓT

a valódi üzenet
csalik folyamatban
úszik — és négy
kabátot visel.



A TARTALMAT RÉTEGEK REJTIK — AZ IDŐZÍTÉST ZAJ REJTI.

Kézenfekvő kételyek eloszlátása

A leírt rendszer természetesen számos kérdést vet fel. Vegyük sorra a leggyakoribbakat.

Technológiafüggőség

Valószínűleg már észrevetted, hogy a modern állammal ellentétben — amely mintegy 150 éve van velünk — az itt leírt reputációs hálózati megoldás erősen függ a globális/lokális internet technológiájától. Kimaradás esetén egy ilyen hálózat működése veszélybe kerül.

Ha a kimaradás átmeneti, nincs adatvesztés, sem a hálózatbeli állítások konzisztenciájának sérülése, és a közösségeken belül elért reputációs egyenlegeknek sem szabad megbomlaniuk. A hasonló fizetési hálózatokkal ellentétben ez a hálózat nagyon alacsony folyamat- és adatgyakoriságot feltételez. Ebben a tekintetben a decentralizált reputációs hálózat nem különbözik a mai államtól, amely szintén erősen függ a technológiától, és elfelejtett papíralapú kartotékrendszerrel dolgozni (bár válságtervekben nem lenne más választása).

Az állam evolúciós utódja reputációs hálózat formájában tartós kimaradás esetén (példátlan léptékű katasztrófa) visszaeshet egy primitívebb, centralizált rendszerre — az államra.

A technológia lehetővé teszi, hogy az emberiség magasabb civilizációs kormányzási formákat érjen el, és előnyöket hoz nekünk, de kockázatokat is.

Kidobom-e az ablakon a pénzem, ha közzéteszek a hálózatban?

Egy állítás reputációs hálózatban való közzétételének költségei nagyrészt nem süllyednek el. Egy közzevető hálózatba juttatott üzenetének hasznossága — valós sérelmekről szóló információ, ellenőrzött tapasztalatok, releváns figyelmeztetések — statisztikailag hosszabb távon megtérül a közösségből érkező

KÉT ÚT — AZ ÁLLAM BEZÁR, A HÁLÓZAT KINYIT

A REPUTÁCIÓS HÁLÓZAT

AZ ÁLLAM

A TÉTLENSÉG A
JOBB OLDALI
AJTÓ
VÁLASZTÁSA.

Minden rezsim ugyanúgy végződik. Az egyetlen
választás: lépj balra.

a kapu még
záródik, a másik
ajtó még nyitva.

válassz egyet
— vagy a
választás
választ téged.

AZ ÁLLAM ALAPÉRTELMEZETTEN BEZÁR. A HÁLÓZAT VÁLASZTÁSBÓL NYIT.

mások állításainak ellenőrzéséért járó díjak formájában. A közösség profitál, a közzétevő reputációt épít, és az igaz információ közzétételének költsége így egy visszatéríthető letéthez közelít, amelyből csak a tényleges hálózatfenntartási költségek kisebb részét kell levonni. Ezzel szemben a valótlan vagy jelentéktelen bejegyzések nem térülnek meg — a költségük tiszta veszteség. A becsületesség tehát nemcsak erkölcsi választás, hanem gazdaságilag racionális stratégia is.

A hálózatfenntartási költségek levonása után ezt az elvet a gazdasági semlegesség elvének nevezhetnénk — nem veszítünk, amikor a közösséggel vagyunk, veszítünk, amikor ellene.

A közösségnek szolidaritási csatornái is vannak arra, hogy megbecsülje tagjainak becsületes hozzáállását. De ne legyenek illúzióink: a szolidaritásra való hivatkozás többnyire a közösségi társadalmi nyomásból fakad, így ez nem feltétlenül szolidaritás a szó önkéntes értelmében.

Mi van, ha valaki több identitást hoz létre?

Egy ember párhuzamosan több DID-identitást is működtethet. Ám az egyes identitások reputációjának építése önálló erőfeszítést igényel — időt, energiát, pénzt.

Nincs rövidebb út: minden identitásnak valós tevékenységen keresztül kell felhalmoznia a track recordját¹. A párhuzamos identitások fenntartása tehát szándékosan drága.

A szabad társadalmakban a költségek elveszik a visszaélés kedvét.

¹**Track record** — általánosan: egy személy vagy szervezet múltbeli eredményeinek, sikereinek és kudarcaiinak története. Itt: egy adott DID-identitás összes múltbeli interakciója a hálózatban — ellenőrzött állítások, elfogadott és elutasított bejegyzések —, amelyekből a reputációja levezethető.

A diktatúrákban azonban a párhuzamos identitások túlélési eszközzé válnak: lehetővé teszik földalatti hálózatok szervezését, a feketepiacon való biztonságosabb eligazodást és a kompartmentalizált² ellenállást, amelyben az egyik identitás lelepleződése nem fedi fel a többit — a rezsim bukása után pedig zökkenőmentes visszatérést engednek a közéletbe és az ott felépített reputációhoz, sőt lehetővé teszik a korábban hivatalos és a titkos DID egyetlen, egyesített bejegyzéshalmazba való összefésülését is egy állítás révén.

²**Kompartmentalizáció** (az ang. *compartment* szóból) az információ elszigetelt egységekre való szétválasztását jelenti, hogy az egyik egység lelepleződése ne veszélyeztesse a többit. A titkosszolgálatoktól ismert elv: egy ügynök csak a saját művelet részét ismeri, így kényszer alatt sem tudja felfedni az egészet.

UGYANAZ AZ ERŐFESZÍTÉS — PAZARLÓ B-TERV A SZABADSÁGBAN, MENTŐÖV A ZSARNOKSÁGBAN

A PÁRHUZAMOS IDENTITÁSOK UGYANANNYIBA KERÜLNEK — DE MÁST VESZNEK

SZABADSÁGBAN — EGY KÖLTSÉGES B-TERV

egy második identitás — arra az esetre, ha valami balul sül el.



MAG → CSÍRA → CSEMETE → FIATAL FA → KIFEJLETT FA
5-15 év — nincs rövidítés, nincs eladó kifejtett fa



DID-A

1. év — idő, energia, pénz elköltve
5% reputáció
három kert, háromszoros költség — és még mindig csak két kezded van.



DID-B

3. év — ugyanazok a költségek újra, egymástól függetlenül fizetve — 20% reputáció



DID-C

0. év — minden előről kezdődik — 0% reputáció

VAGY — TISZTA LAP EGY SZEMÉLYES BOTLÁS UTÁN



RÉGI DID — REPUTÁCIÓ FELEGETVE

csak akkor működik, ha a slamasztika a sajátod maradt — ha másokat annyira megkárosítottál, hogy üldözőbe vegyenek, az állításaid az új cserépbe is követnek.

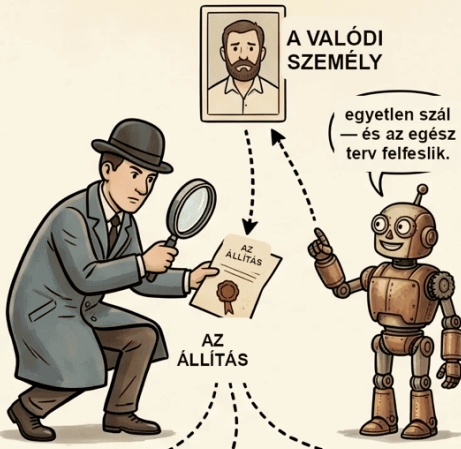


DID-FRESH-START

EGY ÁLLÍTÁS, ÉS A B-TERV ODAVAN

A VALÓDI SZEMÉLY

egyetlen szál — és az egész terv felfeslik.



AZ ÁLLÍTÁS

egyetlen állítás minden cserepet ugyanahhoz a kertészhez köt — évnyi idő, energia és pénz egy délután alatt eltörölve.



ZSARNOKSÁGBAN — EGY AZ ÁLLAMNAK, TÖBBI A SZABAD TÁRSULÁSNAK

(az állam vagy egyenesen betiltja az identitásokat, vagy saját felügyelete alatt követeli meg őket)

AMIT AZ ÁLLAM LÁT

egy álarc a rezsimnek — a többi egy még mindig élhető életért.



külső megfelelés — egy identitás átadva megfigyelésre.

SZINTÉN AZ ENYÉM — DE AZ ÁLLAM ELŐL REJTVE

AMIKET AZ ÁLLAM SOHA NEM LÁTHAT



DID-A — FÖLDALATTI SAJTÓ



DID-B — LEROHANVA



DID-C — ELLENÁLLÓ SEJT — SÉRTETLEN

a sejtek közötti téglafalak azt a munkát végzik, amit az állam tilt — vesztis el egyet, a többi folytatja, és amikor a rezsim megbukik, a kőzetel újraindul.

SZABADSÁGBAN A VISSZAÉLÉS DRÁGA. ZSARNOKSÁGBAN A TÚLÉLÉS LEHETSÉGES.

Kifordított érzékelés

Az állammal ellentétben a decentralizált identitásra épülő reputációs hálózat elve megfordítja az érzékelt prioritás paradigmáját:

- Ami számít, az a reputáció — vagyis a múlt, amelyet az ellenféllel való interakció kockázatainak felmérésére használunk —, a személyes adatok pedig, mint a nevek, címek stb., udvariassági adatszere tárgyai lehetnek
- Míg az állam elsősorban személyes adatokat követel, reputációs adatokat halmoz fel, és csak azt engedi látni a közösségnek, ami neki megfelel

Nem tud-e egy gazdag ember egyszerűen „megvenni” több identitást (vagy virtuális közösségeket létrehozni)?

A párhuzamos decentralizált identitások létrehozásának lehetősége első ránézésre tisztességtelen előnynek tűnik a nagyobb gazdasági eszközökkel bíró emberek javára a kevesebbel rendelkezőkkel szemben. Hangsúlyozni kell azonban, hogy a centralizált rendszerrel ellentétben, ahol elég a hatalmi piramis néhány pontját megvesztegetni ahhoz, hogy bizonyos gaztettek eltűnjenek, egy decentralizált rendszerben az egész közösséget meg kellene vesztegetni.

Helyettesítő decentralizált identitások szolgálhatnának erre a célra, de a reputációjukat időben, valós, tényleges közösségi tagokkal folytatott interakción keresztül kell felépíteni — nem lehet egyszerűen megvenni, mert a hálózat ellenőrizhetővé teszi, hogyan teljesít egy adott identitás.

Ráadásul létezhetnek (és valószínűleg léteznek is majd) olyan piaci szolgáltatások, amelyek autoritásként eljárva olyan nyomozásokat kínálnak, amelyek bizonyítékot állítanak elő arról, hogy több decentralizált identitás valójában ugyanaz a személy. A reputációs hálózatba bevitt egyetlen bejegyzés így a költség töredékéért semmissé teheti a párhuzamos identitások felépítésébe fektetett teljes idő-, energia- és pénzberuházást.

Gazdaságilag tehát megéri nem becsapni a közösséget — és ha kell, felülvizsgálni a tetteinket és orvoslásba fogni, hogy a reputáció visszatérjen egy elfogadható szintre, és a viselője ne szenvedjen gazdaságilag vagy másképp a közösség haragjától.

Egy gazdaságilag erős identitás, amely elvesztette a reputációját a saját közösségében, megpróbálhatja alattomos alkukkal, célzott identitásokon keresztül elkerülni a közösség haragját — de azok ekkor szintén a saját reputációjuk elvesztését kockáztatják.

Még mindig marad a menekülés egy másik közösségbe friss identitással — de ez azt jelenti, hogy minden eredményt hátrahagy, és valahol nulláról, nulla reputációval kezd. Néha érthető út lehet, és az egyetlen kiút.

Megjegyzés

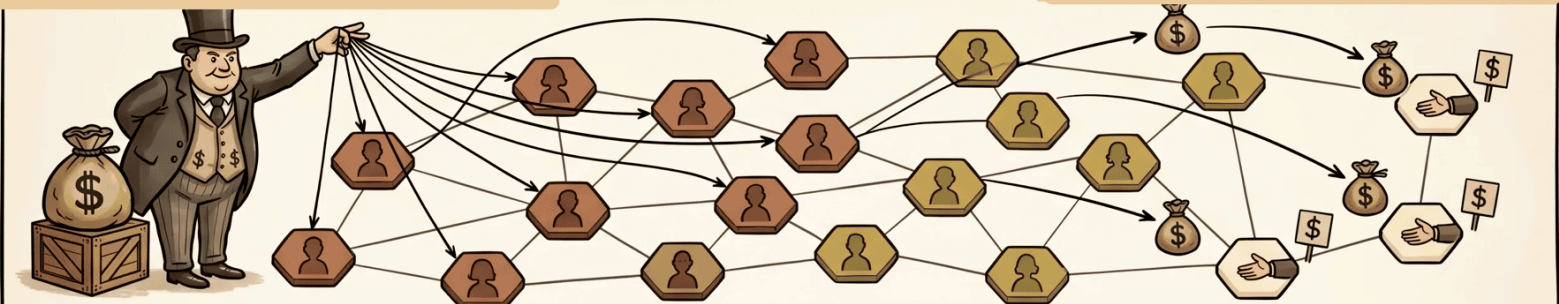
Hasonlóképpen kezelnék a közösségek azt a támadást, amelyben valaki erőforrásokat fordít egy virtuális identitás létrehozására: annak az identitásnak kockázatos ellenőrzés nélkül interakcióba lépni egy másik közösséggel — vagyis kritikátlanul elfogadni a másik közösség identitásairól szóló információt. A reputációt mindig egy közösségen belül építik, nem globálisan.

A REPUTÁCIÓ A GAZDASÁGI ERŐ ELLENSÚLYA

A GAZDAG EMBER BEFOLYÁST VESZ — A KÖZÖSSÉG EMLÉKSZIK RÁ

A TÁMADÁS — BESZIVÁRGÁS ÉS MEGVESZTEGETÉS

NYOLC BEÜLTETETT BÁBU + HÁROM MEGVESZTEGETETT SZOMSZÉD



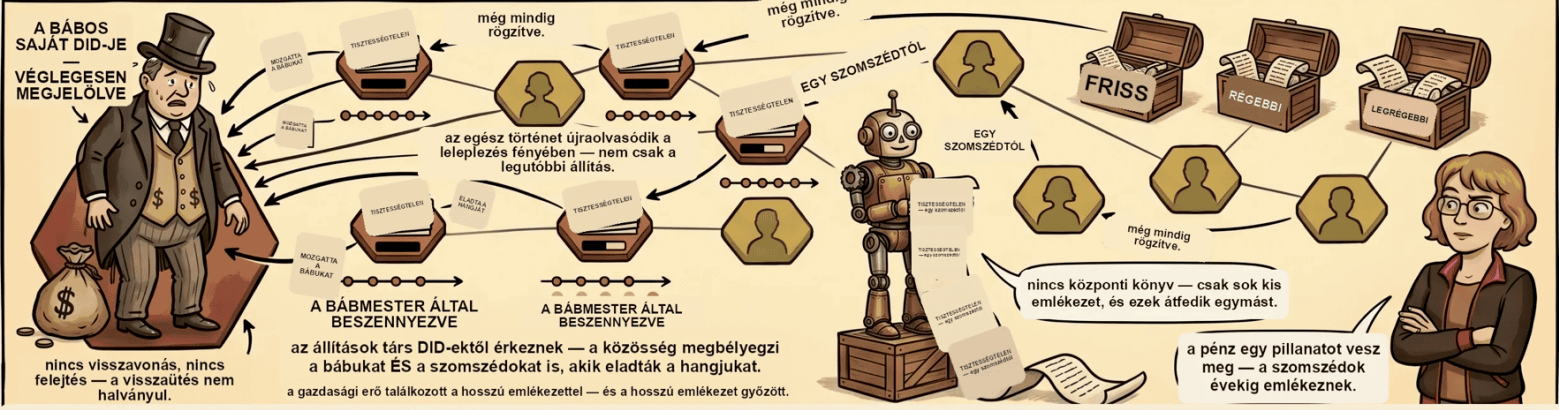
a gazdasági erő bármely közösségbe becsúszthatat zsínórokat — és útközben megvehet néhány valódi hangot.

eleinte úgy tűnik, a gazdag ember csak kiszélesítette a baráti körét.

KÉSŐBB

A VÉDELEM — HOSSZÚ EMLÉKEZET, ELOSZTOTT KÖNYVELÉS

MINDEN SZOMSZÉD A SAJÁT EMLÉKÉT ÓRZI — NINCSEK KÖZPONTI KÖNYV, NINCSEK FELEJTÉS



A GAZDASÁGI HATALOM BENYÚL — A VISSZAÜTÉS HAZATALÁL, ÉS NEM MOSÓDIK LE.

Mi a helyzet a potyautasokkal, akik csak olvasni akarnak, és semmit nem adnak a közösségnek?

Az információhoz való hozzáférés nem korlátlan egy decentralizált identitás létrehozásának első napjától. Az új résztvevők — akik még nem építettek reputációt tényleges tevékenységgel — fokozatos korlátozásokba ütköznek: kevesebb információ, hosszabb várakozási idők, magasabb lekérdezési költségek. A hálózat a részvételt jutalmazza, nem a passzív fogyasztást és az önkényes adatlehalasztást.

Egy decentralizált identitás a reputációját is kockáztatja, amikor pénzért kölcsönadja a reputációját egy másik személynek (aki lehet, hogy nincs is a DID-reputációs hálózatban). Ugyanaz az elv érvényes itt: a közösség ilyen elárulása (a magánélet megsértése) rávetülhet az áruló reputációjára, és a tettet nem lehet alattomos alkuval eltörölni, ahogyan az egy centralizált rendszerben működik. Számolniuk kell a közösség haragjával, beleértve az eredmények elvesztését is — mert a közösség az ő szemükben például az ingó és ingatlan vagyon birtoklásának kiváltságát garantálja.

Horgony a valós világhoz

A kockázat felmérésekor a kockázatosabb alany természetesen az, aki nem élvezzi az adott közösség által elismert tulajdon kiváltságát — kevesebbet veszíthet az ügyleteiben (a digitális eszközöket könnyebb mozgatni).

Apró részletnek tűnhet, de nagy következményei vannak. Ha azt akarjuk, hogy a közösségnek befolyása legyen a tagjai fölött, az kiváltsággént vonja maga után a tulajdont — a legszabadabb társadalmakban szinte érinthetetlenként, mégsem jogként, sem alapelveként, hanem kiváltsággént, amely szélsőséges esetben visszavonható (el tudom képzelni például a közösség fegyveres konfliktusban való védelme alóli kibújás megtagadását).

Ez sejtelmesen arra is választ ad, hogyan bánt majd a közösség a tagjaival, és mi motiválja a tagot arra, hogy harcoljon a közösségért — hogy megőrizze a kiváltságait. Egy ember elbukhat a közösséggel szembeni felelősségében, de erkölcsileg nem várhat elnézést, amikor a nehezen kivívott kiváltságok megőrzéséről van szó.

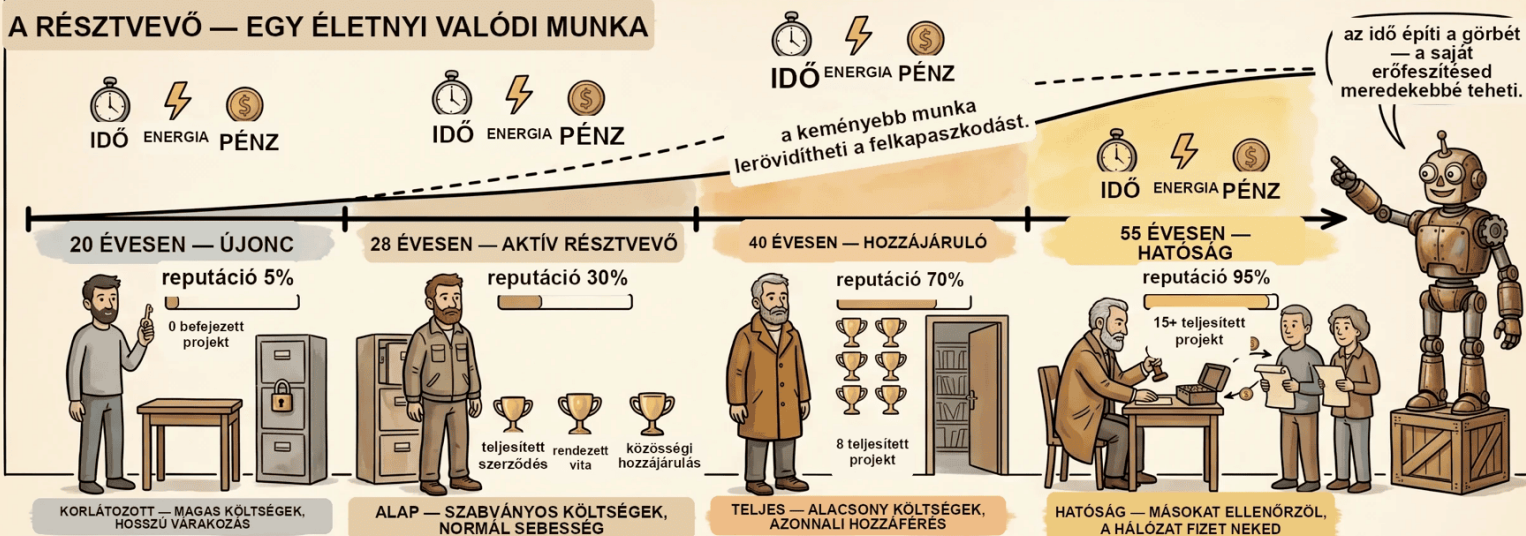
Pénzügyi semlegesség

Amikor olyan szavakat olvasunk, mint decentralizált, cenzúrázhatatlan, korrumpálhatatlan, óhatatlanul a legismertebb kriptovalutákra asszociálunk — Bitcoin, Monero és mondjuk Kasper —, amelyek leírhatók ilyen kifejezésekkel. Az intuíció itt azonban megtévesztő: az autoritások szolgáltatásaiért, az ellenőrzésért, a közzétételért és így tovább járó díjak bármely valutában vagy pénzben rendezhetők.

A HÁLÓZAT JUTALMAZZA A RÉSZVÉTELT

A REPUTÁCIÓ EGY ÉLETEN ÁT ÉPÜL — NEM MEGVEHETŐ, NEM KÖLCSÖNÖZHETŐ

A RÉSZTVEVŐ — EGY ÉLETNYI VALÓDI MUNKA



az idő építi a görbét — a saját erőfeszítésed meredekebbé teheti.

minden szakasz időbe, energiába és pénzbe kerül — együtt, nem külön.

az ajtó akkor nyílik, ahogy a tetteid főkönyve megtelik.

A POTYAUTAS — OLVAS, SOHA NEM TESZ KÖZZÉ



nincs tett, nincs emelkedés — évről évre ugyanaz a szint.

a hálózat azoknak ad vissza, akik beleadnak.

IDŐ, ENERGIA ÉS PÉNZ — VALÓDI MUNKÁBA FEKTETVE — AZ EGYETLEN VALUTA, AMIT A HÁLÓZAT TISZTEL.

Ami a DID-hálózatbeli közösségi hálózat összekapcsolt résztvevői (vagyis a közösség) és annak környezete számára számít, az egy reputációval fedezett megerősítés, hogy a fizetés megtörtént. Egy állítás közzétételének egyénileg észszerű, ellenőrizhető költséget kell viselnie, hogy egy szereplő ne tehessen közzé annyi és bármilyen állítást, amennyit csak akar, energia, pénz és idő ráfordítása nélkül — ez erősen nemkívánatos állapot lenne, amely a mai korrupcióval terhelt államrendszerekben az elit kiváltságának felel meg.

Ebben a tekintetben az említett kriptovalutáknak van egy kis előnyük: a hálózataik megbízható autoritásként működnek annak ellenőrzésében, hogy egy adott fizetés megtörtént, a magánélet kis elvesztése és néhány cím felfedésének árán.

Önkéntesség, felelősség és szabadság

Az önkéntesség egyéni: magam döntök. A felelősség akkor keletkezik, amikor a döntésem másokat érint — beindul a visszajelzés. A szabadság sem ajándék, sem jog — az önkéntesség és a felelősség felé irányuló nyomás közötti több ezer kétoldalú interakció fenomenológiai³ eredménye, a társadalom egészére átlagolva. A hálózat nem diktálja ezt az átlagot — az az ellenőrzők árjelzéseiből és azokból az előre bejelentett ellenőrzési elvekből bontakozik ki⁴, amelyeket a közösség tagjai maguknak beállítanak.

³**Fenomenológiai** (a gör. *phainómenon* — ami megjelenik szóból) — általánosan: olyan megközelítés, amely a jelenségeket úgy vizsgálja, ahogyan a közvetlen tapasztalatban megjelennek, azt figyelve, mi következik belőlük, előzetesen adott magyarázó elméletek nélkül a mélyben húzódó mikrovilágban. Itt: a szabadság nem felülről definiált absztrakt elv, hanem megfigyelt jelenség — az emberek közötti több ezer mikrointerakció következménye, amely abból bontakozik ki, ahogyan valójában bánunk egymással.

⁴**Emergens** (a lat. *emergere* — felbukkanni szóból) azt jelenti: „egyszerűbb részek interakcióiból spontán módon keletkező, anélkül, hogy bárki megtervezné vagy irányítaná.” Egy madárraj alakzatban repül, pedig egyik madárnak sincs terve az

Hogy egy közösségen belüli egyénnek mekkora a szabadság iránti preferenciája, az attól függ, mennyire érzi, hogy hajlandó maga is lenyelni abból, amit másokra kényszerít. Az olyan dolgoknál, amelyek maguktól értetődőek és mindenkinek hasznosak, nincs erkölcsi dilemma — a gyilkosság rossz. Aztán vannak esetek, ahol a lehetőségek megengedett kiváltságok pozíciójába csúsznak: bizonyítsd a képességeidet, és felengedünk az útra, hogy kisebb eséllyel ölj meg minket. És végül vannak ügyek, ahol az egyén azt mondja — nekem ez nem éri meg, nem tiltom meg a szomszédomnak a levélégetést, ha magam is égetek, vagy mert én is teszek valami mást, ami korlátozza az ő kényelmét, és ő cserébe azt akarhatná megtiltani nekem. Ha történelmileg ott húztuk meg a szabadság határát, ahol valaki más szabadsága kezdődik, akkor egy decentralizált identitásra épülő reputációs közösségi hálózat ezt jobban teljesíti, mint a centralizált képviseleti demokrácia — ahol például a választott képviselők kiváltságos rétege igyekszik kivonni magát a személyes kommunikáció megfigyelése alól, mégsem habozik azt a szavazóira erőltetni, mindenféle alattomos ürügyet és manipulációt bevetve.

A szabadság–totalitarizmus kapcsoló (és a delegálás)

Egy egyszerű mechanizmus a DID-hálózaton belül az egész rendszert nagyobb szabadság vagy nagyobb ellenőrzés felé tolhatja: a bejegyzések száma, amelyeket egy DID időszakonként közzétehet. Amíg a bejegyzések ritkák maradnak, mindegyiknek súlya van — ez a szabadság. Amikor a bejegyzések bőségesek és apróságokra terjednek ki, az a totalitarizmus. Minden közzétett bejegyzéssel te választod meg az irányt. Maga a hálózat sem nem szabad, sem nem totalitárius — semleges infrastruktúra. Hogy mivé válik, azt az dönti el, hogyan használják az emberek.

alakzatra — az alakzat az egyes madarak egyszerű szabályaiból bontakozik ki. Ugyanígy a reputációs hálózatban sem tervezi meg senki az egész viselkedési szabályait — azok több ezer egyéni döntésből bontakoznak ki.

ÖNKÉNTESSÉG → FELELŐSSÉG → SZABADSÁG

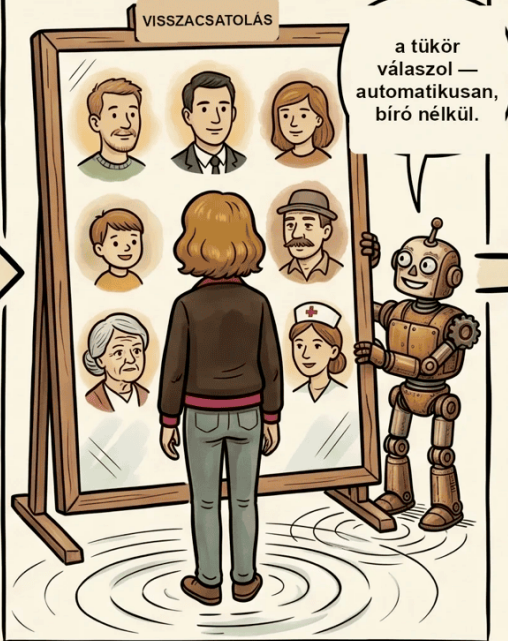
HÁROM LÉPÉS — EGY EMBER DÖNTÉSÉTŐL EGY EGÉSZ TÁRSADALOM MINTÁZATÁIG

ÖNKÉNTESSÉG



az egyén dönt — senki sem kényszeríti.
és senkinek sincs vele szemben tevételes kötelezettsége.

FELELŐSSÉG



a döntéseim hullámokat vetnek — és a hullámok visszatérnek.
a következmények magukért beszélnek.

SZABADSÁG



ezt a térképet senki sem rajzolta — magát rajzolta meg.
a szabadság annak statisztikai alakja,
ahogy a szomszédok bánnak egymással.

A SZABADSÁG NEM FELÜLRŐL KAPOTT AJÁNDÉK — HANEM A MINTÁZAT, AMIT EGYÜTT ALKOTUNK.

A saját ellenőrzési elveimen belül van értelme egy általános DID-re a közösségi hálózatomban — a közösségeken belül — meghatározni azon állítások maximális számát (bármely ellenőrizhető kijelentés általában véve; itt: a reputációs hálózatba közzétett bejegyzés), amelyet egy közzétevő időszakonként kibocsáthat ahhoz, hogy figyelembe vegyem, és relevánsnak tekintsem az ellenőrzési kéréseit.

Egy intuitív számot tartok fejben — alacsony egyszámjegyű érték évente. Egy ilyen cenzorális megközelítés meglehetősen izolacionistának tűnhet. De jogosan állíthatom a kérelmezőt választás elé: válasszon egyet a már kibocsátott bejegyzései közül, és kérje meg az ellenőrzőt annak visszavonására, vagyis érvénytelenítésére — ami meglehetősen agresszív követelés egy olyan helyzetben, amikor a kérelmező véletlenül valóban több független sérelem áldozatává vált, és így bizonyosan hozzájárulnék ahhoz, hogy elidegenedettnek érezze magát a közösségtől.

Hatékonyabb lehetőségnek tűnik ezért az a képesség, hogy a reputációs hálózatba való információközzétételi jogaink egy részét egy közösség vagy egy autoritás javára delegáljuk, amely aztán — szolidáris módon, a belső szabályai szerint — eldönti, hogyan osztja el őket. Egy csoportnak képesnek kell lennie gondoskodni azokról, akiket hátrányos helyzetűnek tekint. A közösség tagjának bármikor joga van visszavonni a delegálását, amíg a delegált jogot fel nem használták.

A SZABADSÁG-TOTALITARIZMUS KAPCSOLÓ

EGYETLEN PARAMÉTER — MENNYIT VÁLASZTOK KÖVETNI — BILLENTI AZ EGÉSZ TÁRSADALMAT SZABADSÁG ÉS ZSARNOKSÁG KÖZÖTT

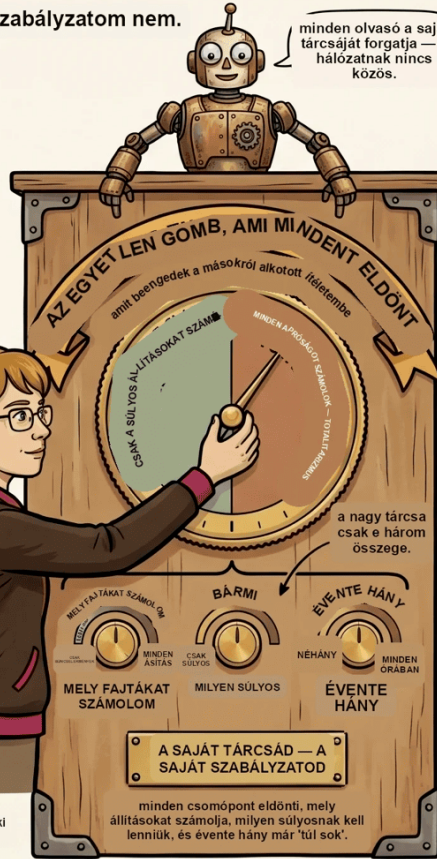
nem sok gomb — egy. a hálózat maga semleges, a szabályzatom nem.

BAL — KEVÉS, SÚLYOS, KOMOLY



csak a súlyos ügyek vésődnek a nyilvántartásba — mert a vésés nehéz.
minden más magánügy marad: egy rossz nap, egy buta vicc, egy késés — egyik sem senki aktája.
az emberek megfigyeletlenül élnek, szabadon beszélnek, és felelősség nélkül lélegznek.

minden olvasó a saját tárcsáját forgatja — a hálózatnak nincs közös.



A SAJÁT TÁRCSÁD — A SAJÁT SZABÁLYZATOD

minden csomópont eldönti, mely állításokat számolja, milyen súlyosnak kell lenniük, és évente hány már 'túl sok'.

JOBB — SOK, JELENTÉKTELEN, FOJTOGATÓ



minden ásitásból akta lesz — mert a számolás olcsó.
egy tüsszentés, egy vásárlás, egy sötétedés utáni hazaut: mind bekerül a nyilvántartásba, örökre.
semmi sem magánügy — a szem sosem hunyorít, és a szomszédok elhallgatnak.

A SZABADSÁG AZ, AMIT NEM VAGYOK HAJLANDÓ SZÁMOLNI — A TOTALITARIZMUS AZ, AMINEK A KÖVETÉSÉBE BELEEGYEZEM.

A KÖZZÉTÉTELI JOGOK DELEGÁLÁSA

KÖLCSÖNADOD A KULCSOT EGY HATÓSÁGNAK, AMELY SZOLGÁL TÉGED — ÉS EGY PILLANAT ALATT VISSZAVONOD

kölcsönadom a kulcsot
— a zsinór nálam marad.

delegálás — a hatóság a
nevemben jár el, az általam
jövähagyott szabályok között.

A VISSZAHÍVÁS
ZSINÓRJA

A KÖZZÉTÉTELI
JOGOM —
BEJEGYZÉS

egyszerre több kulcsot is
kölcsönadhatok — egy
háttér-automatizmus újat
bocsáthat ki, valahányszor
kisorsolják valamelyiket.

HATÓSÁG — SZOLGÁLTATÓ
szabályzat · szabvány · párt ·
kamara

SZABÁLYZAT

VEÉLTENSZERŰEN
KISORSOLVA,
AMIKOR A
HATÓSÁG ELJÁR

DELEGÁLT
KULCSOK —
KESZLET

VEÉLTENSZERŰEN
KISORSOLVA,
AMIKOR A
HATÓSÁG ELJÁR

EGY RÁNTÁS — A KULCS HAZATÉR

a zsinór sosem hagyja el a
kezed — ez az egész trükk
lényege.



csak addig visszavonható,
amíg a kulcsot ki nem
sorsolják.

HATÓSÁGFAJTÁK,
AMELYEK
TARTHATJÁK A
KULCSOT



POLITIKAI
PÁRT
FAKTI



SZABVÁNYÜGYI
TESTÜLET
BUDI



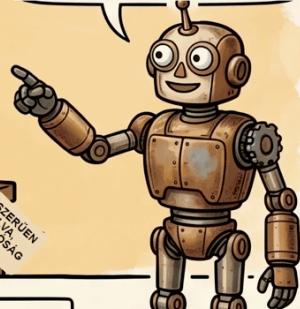
SZAKMAI
KAMARA



SZÖVETKEZET

ezután a polgárnak új kulcsot kell kibocsátania, hogy
megőrizze a jó viszonyt a hatósággal — egy automatizmus ezt
a háttérben elvegezheti.

a hatóság a tagjait szolgálja — nem fordítva.
egy rántás a zsinóron véget vet a megállapodásnak.



ADD KÖLCSÖN A KULCSOT — TARTSD MEG A ZSINÓRT. A DELEGÁLÁS SOHA NEM LEMONDÁS.

■ Szabadság kontra totalitarizmus

Egy társadalom, amely őrködik a közzétett bejegyzések mennyisége felett és korlátozza azt, szabadabb lesz; egy társadalom, amelyben a bejegyzések bősége van, a totalitarizmus felé hajlik. Elképzelhető, hogy a bejegyzések közzétételének jogát valaki másra delegáljuk.

Kulturális alkalmazkodás

Az emberek általában szeretnek egymás tányérjába látni. A civilizációk közt eltérünk a történelmi tapasztalatban és a népsűrűségben — és ezért abban is, mennyire akarunk egymás tányérjába látni a civilizációkon és közösségeken belül. Az ázsiai államok a szabadság szigorúbb szemlélete felé hajlanak a társadalomban; az európaiak és amerikaiak bizonyos szempontokból egy szabadabb felé. Bármennyire pontatlan is ez a párhuzam, egy decentralizált reputációs közösségi hálózat kontextusában elmondható, hogy az egyes közösségek beállításai nem diszkriminálnak, és minden közösség úgy konfigurálhatja a belső kommunikációját, ahogyan jónak látja.

A különbségek ellenére lesznek a bolygón átívelően elismert szabványok (a véletlenszerű ölés senkinek sem jó). Más beállítások közösségspecifikusak lesznek, megint mások pedig akár személyspecifikusak. Az előny az, hogy a kölcsönös kommunikáción és a környezet beállításainak megfigyelésén keresztül konszenzus kereshető — a kétoldalú megállapodásoktól a közösségeken át, idővel pedig a legjobban konfigurált közösségek gazdasági dominanciájának köszönhetően akár globális szinten is.

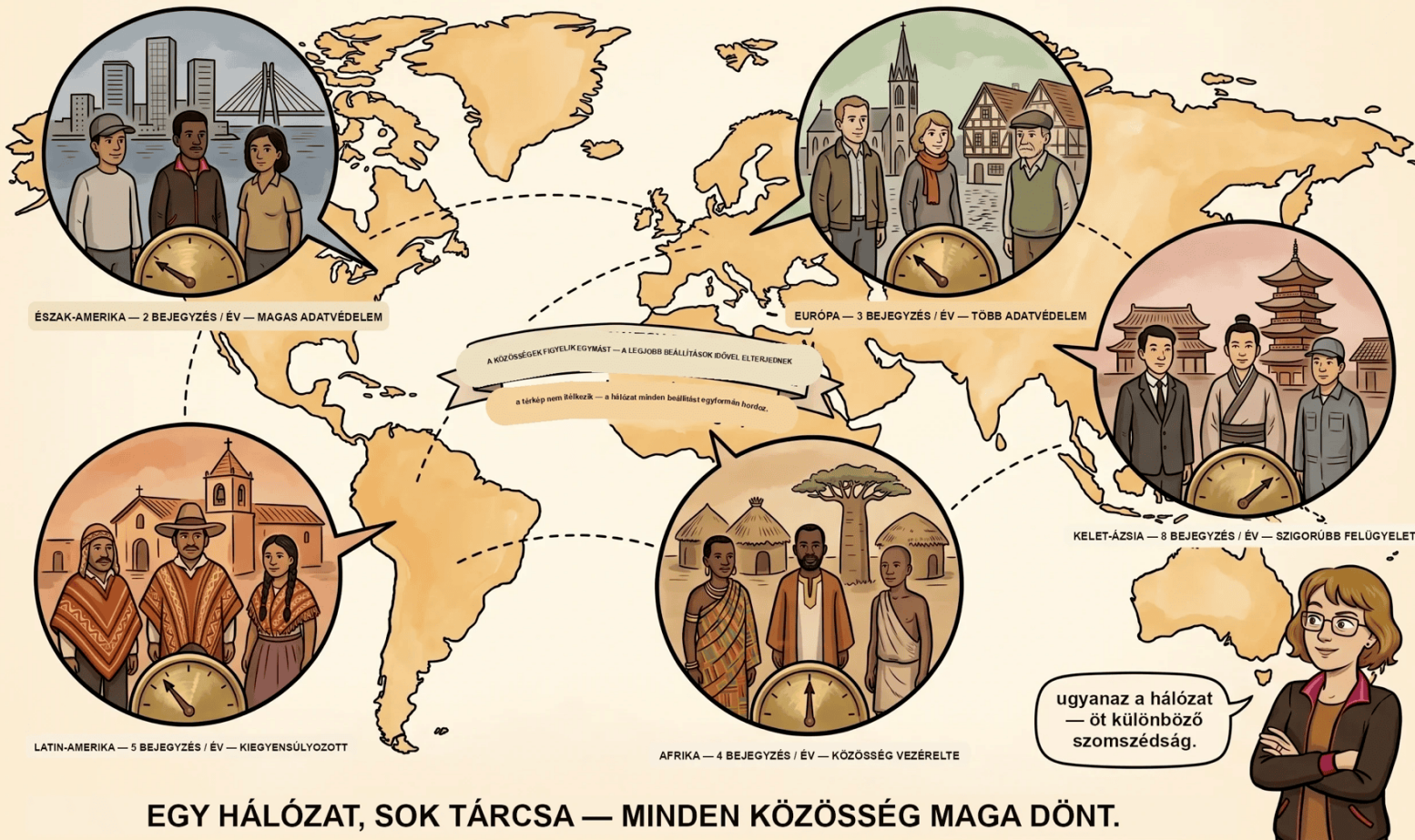
De a konszenzusról bővebben a következő fejezetben.

Az oracle-probléma — híd a digitális és a fizikai világ között

Az „oracle-probléma” kifejezést az utóbbi időben leggyakrabban a kriptovaluták, a blockchaineik és a decentralizált rendszerek világával kapcsolják össze. Általánosan: hogyan biztosítod, hogy egy digitális

MINDEN KÖZÖSSÉG MAGA KONFIGURÁLJA MAGÁT

A HÁLÓZAT NEM TESZ KÜLÖNBSEGET — MINDEN RÉGIÓ A SAJÁT TÁRCSÁJÁT ÁLLÍTTJA BE



rendszerbe belépő adatok hűen megfeleljenek annak, ami valójában történt a fizikai világban? Maga a rendszer nem tudja ellenőrizni, hogy valaki tényleg kárt okozott-e másnak, vagy hogy egy szerződést valóban megszegtek-e — csak digitális bejegyzéseket lát.

Itt ezt autoritásokon keresztül oldjuk meg — olyan entitásokon, amelyek a reputációjukat teszik arra, hogy a digitális bejegyzés megfelel a fizikai valóságnak. Minél magasabb az autoritás reputációja, annál hitelesebb a bejegyzés.

A DIGITÁLIS ÉS A FIZIKAI VILÁG ÖSSZEKÖTÉSE A HATÓSÁG ÁTVISZI A VALÓSÁGOT



A hatóság reputációja teszi megbízhatóvá a digitális bejegyzést.

* A rendszer nem próbálja megoldani az orákulum-problémát — elfogadja, hogy a hatóságok a híd, és igazodik ahhoz, ahogy a bizalom a valós világban már működik.

* Ha a híd téved a valóságról, a hatóság fizet — a reputációjával.

Hogyan működik az ellenőrzés

Konszenzus és az ellenőrzési folyamat

Ahhoz, hogy konszenzus épüljön arról, mely szabályokat kellene egy társadalomnak átlagosan betartania és érvényesítenie, a következő mechanizmus segíthet. DID-résztvevőként bejelentem azokat a szabályokat, amelyekre aláíratkozom és amelyek szerint élni fogok, és közzéteszem őket. (Gondolj rá úgy, mint az alapszabályra és a statútumokra, amelyek az én nézetem szerint az ideális világot alkotják — egy világot, amelyben nem korlátozottak, hanem biztonságban érzem magam.)

Előre megbecsülhetem, hogyan reagálnának a DID-kapcsolataim — és felmérhetem, milyen erősen és ki által lennék szankcionálva a szokásos társadalmi vagy üzleti interakciókban, ha azok hipotetikusán bekövetkeznének.

A végleges kiértékelés akkor történik, amikor információt kérsz egy másik DID-től, vagy megkéred egy állítás ellenőrzésére (vagy egy autoritástól szolgáltatást kérsz, és így tovább), amelyet közzé akarsz tenni a reputációs hálózatban. Ugyanúgy kellene végződnie, mint amikor magad futtatod le a kiértékelést, próbaútban, az ellenfél deklarált elveivel szemben — és ha nem így van, akkor valami baj van az ellenfél oldalán: tisztességtelen játékot próbál játszani.

A kimenet vagy elfogadás, az ellenőrzésre adott árajánlattal (ellenőrző- vagy autoritásszolgáltatások esetén), vagy elutasítás. Az értékelő elveitől való eltérés szankciói és bónuszai egyaránt beépülnek az árajánlatba. A kérelmező ezután eldönti, elfogadja-e a feltételeket, vagy továbblép az elosztási algoritmus következő ellenőrzési fordulójára — addig ismételve a folyamatot, amíg elégedett nem lesz, vagy amíg a gazdasági logika értelmetlenné nem teszi a folytatást.

■ A közösségi gráf

A reputációs hálózat mindenekelőtt közösségi hálózat. Kapcsolatokat adsz hozzá — embereket, akik beleegyeznek a kapcsolatba. Nekik is vannak kapcsolataik, azoknak a kapcsolatoknak pedig további kapcsolataik. Az algoritmus egy konfigurálható mélységen belül keres ellenőrzőket (pl. három szint: a közvetlen kapcsolataid, azok kapcsolatai és egy szinttel tovább). Nincs szükség globális blockchainre — a hálózat természetesen közösségeket formál, más közösségekbe való átfedésekkel.

Az algoritmus nemdeterminisztikus: hasheli az állításdokumentumodat, a hasht egy pozícióhoz rendeli az ismert identitások gyűjteményén ezen a körön belül, és a legközelebbit választja ellenőrzőjelöltnek. Nem tudod megjósolni vagy befolyásolni, ki fogja ellenőrizni az állításodat.

Minden ellenőrző elutasítása megnöveli a dokumentumodat és növeli a feldolgozási költségét — ez az első költségcsatorna (a dokumentum növekedése). Minden új ellenőrző díjat számít fel az adatmennyiség, a reputációd, valamint annak alapján, hogy az állításod tartalma mennyire tér el a deklarált ellenőrzési elveitől — ez a második költségcsatorna (kockázati felár). És minden iteráció időbe és energiába kerül — ez a harmadik költségcsatorna.

■ Mit ellenőriz az ellenőrző, sorrendben

A kiválasztás után az ellenőrző nagyjából négy sorrendbe rendezett lépésben értékeli egy állítást — először a legolcsóbb szűrők, végül a drága tartalmi ellenőrzések:

1. **Elvi kapuzás.** Ez a fajta állítás egyáltalán beleesik-e abba, amit az ellenőrző nyilvánosan ellenőriz? Ha nem, a kérést azonnal elutasítja.
2. **Autoritásbizalom.** Az állítást jóváhagyó autoritás elég megbízható-e az ellenőrző saját deklarált elvei szerint? Az ellenőrző bizalmi küszöbe alatti autoritás az állítás tartalmától függetlenül elutasítási ok.
3. **Kibocsátói reputáció.** A kibocsátó megfelel-e azoknak a reputációs küszöböknek, amelyeket az ellenőrző az ilyen típusú állításra deklarált? Az alacsony reputáció vagy megemelheti a díjat, vagy elutasítást válthat ki.
4. **Tartalmi ellenőrzés.** Csak amikor az első három kapu átmegy, értékeli az ellenőrző magát az állítást — aláírásokat, belső konzisztenciát, formai helyességet, valamint azt, mennyire tér el az ellenőrző elveitől. Az ezért az utolsó lépésért felszámított díj a ténylegesen vállalt kockázatot tükrözi.

Az ellenőrző közzéteszi az egyes kapukat szabályozó elveket, így a lépések nem az ő diszkréciójától függenek — azt kötik őt, amit már deklarált. A közzétett elvektől való eltérés maga is közzétehető állítás ellene, és a reputációjával fizet érte.

Az eredmény: egy hiteles és hasznos állítás közzététele szinte semmibe sem kerül. Egy radikális állítás közzététele többbe. Egy hazugság közzététele elrettentően drágává válik — ellenőrzőről ellenőrzőre kell iterálnod, és mindenki, aki elutasít, hozzáad a költséghez. A piac beárazza az állításodat, és az ár megmondja, hol állsz azokhoz a közösségekhez képest, amelyekben mozogsz.

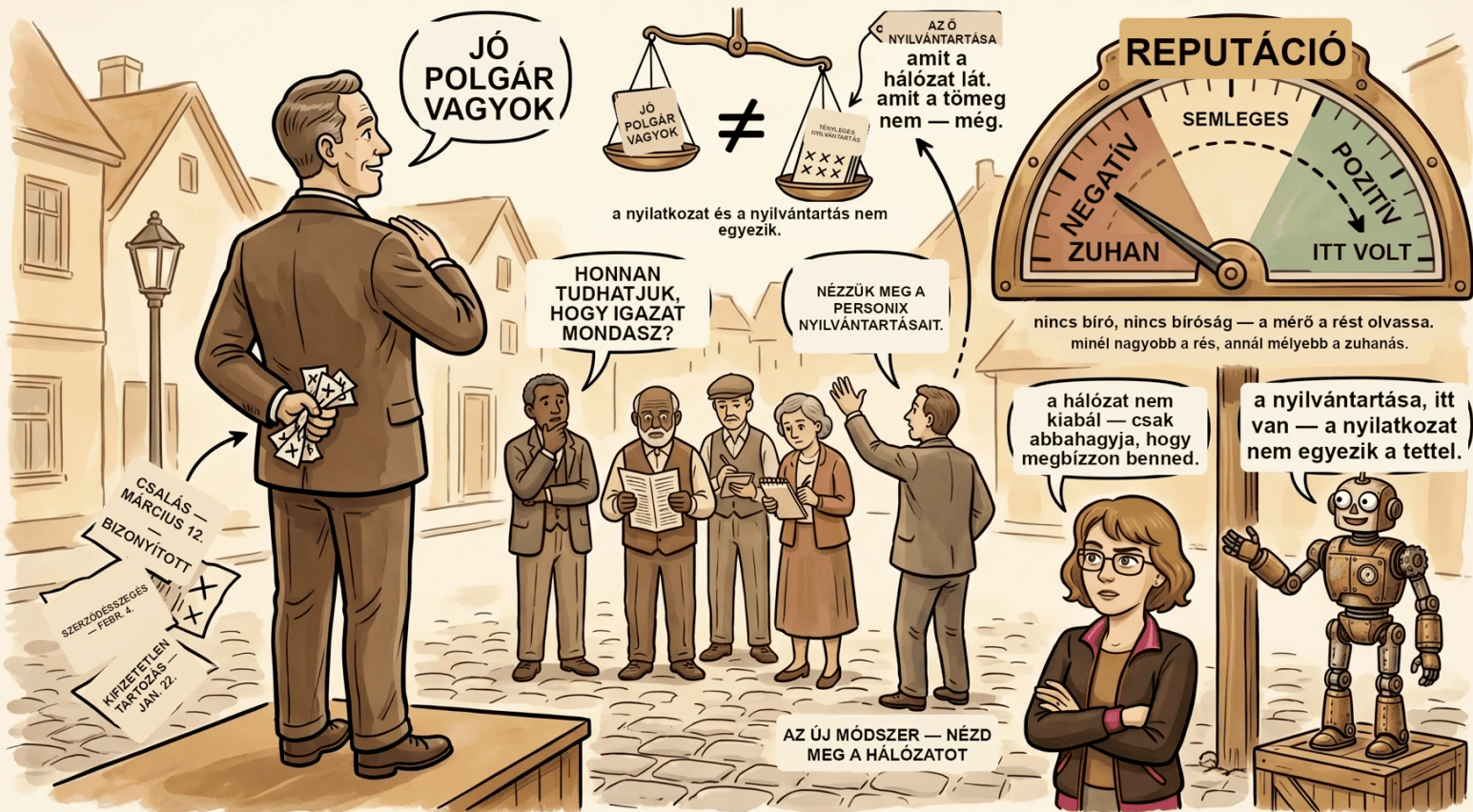
Nem elég bejelenteni, hogy betartasz egy szabályt, amikor valójában nem. Ebben az esetben a DID-ed egy olyan negatív bejegyzés közzétételét kockáztatja, amely leleplezi a képmutatást — ami kockázattá tesz téged mindenki más számára. Az eredmény kevesebb, de következetesebben betartott szabály legyen, valamint a törvények és rendeletek azon dzsungelének kitisztítása, amelyben még a jogi szakemberek is alig igazodnak el.

Konszenzus kontra elszámoltathatóság

Ahhoz, hogy a hálózat értékes információforrásként szolgáljon, egy DID ne legyen túl radikális — különben a többiek elutasítják. A társadalmi nyomás egyensúlyt keres, és a destabilizálására tett kísérleteket valószínűleg megbüntetik.

A KÉPMUTATÁS A LEGDRÁGÁBB VISELKEDÉS

A HÁLÓZAT CSENDEN ÖSSZEVETI A SZAVAJDAT A NYILVÁNTARTÁSODDAL — A RÉŚ MINDENKI SZÁMÁRA LÁTHATÓ



KINYILVÁNÍTOD ÉŚ MEGSZEGED? A RÉŚ A LEGDRÁGÁBB VISELKEDÉS.

A KÉPMUTATÁS ELLENSZERE

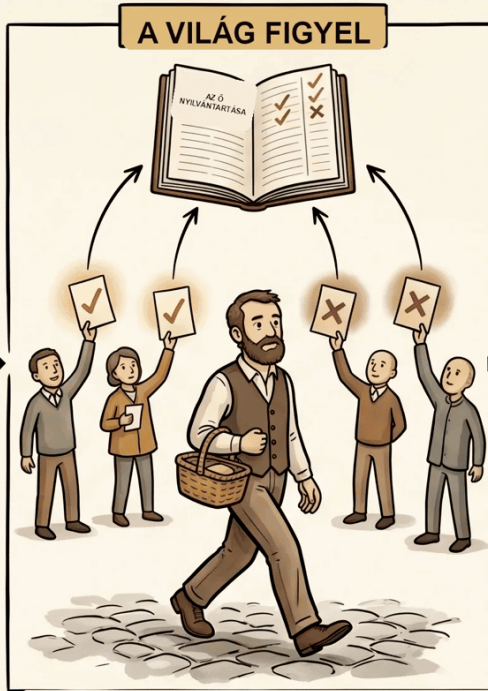
NYILVÁNÍTSD KI A SZABÁLYAIDAT — ÉLJ SZERINTÜK, VAGY A PIAC KIÁRAZ

KINYILVÁNÍTOM A SZABÁLYZATOMAT



bárki olvashatja a normáimat.
nincs kapuőr, nincs titok.

A VILÁG FIGYEL



a világ leírja, amit valójában tesz.
minden nap egy kicsivel több bizonyíték a főkönyvében.

A BOLTBAN — A SAJÁT NYILVÁNTARTÁSODÉRT FIZETSZ



a képmutatást nem a hatóság bünteti — a piac árazza be.
minden hétköznapi szolgáltatás, amit veszel, a saját nyilvánvalóságod alakította felárat hordoz.

NEVEZHETNÉNK EZT A TÁRSADALMI SZERZŐDÉSNEK — ÚJRARAJZOLVA?

nem a hatóság kényszeríti ki az etikát — hanem az ár.
finom nyomás, minden nap, a közös átlag felé, amivel mind együtt tudunk élni.

TARTSD, AMIT MONDASZ — VAGY FIZESS ÉRTE. A KÉPMUTATÁS A LEGDRÁGÁBB REPUTÁCIÓ.

■ A szavazatok száma nem ugyanaz, mint egy hang súlya

Juraj Karpiš azt mondja, hogy „a pénz a jó cselekedetek emlékezete”. Én hozzátenném, hogy a reputáció a rosszaké.

Ebből következik, hogy meritokratikusan az, aki többel járul hozzá és nincs rossz reputációja, nagyobb hangsúlyt érdemel a közösségben. A kétoldalú kapcsolatok szemüvegén át nézve: amikor mérleget, mely konszenzusnyomásoknak engedjek, a legnagyobb súly azoknak a kapcsolatoknak jut, amelyekből a legnagyobb gazdasági hasznot húzom. Tíz ember, akikkel nincs aktív kereskedelmem, sokkal kevésbé befolyásol, mint egyetlen állandó üzleti partner. Ez a paradigma nem korlátozódik a kereskedelemre — kiterjed a társadalmi, politikai és egyéb kapcsolatokra is.

Roles in the verification transaction and authorities

A szerepek áttekintése

Néhány ezek közül a szerepek közül már röviden érintettük a hálózatról és annak alaptulajdonságairól szóló fejezetben. Most itt az ideje, hogy részletesebben újra megnézzük őket, és hozzátegyük a továbbiakat, amelyekre szükségünk van, hogy a hálózat robusztusabb legyen. Minden ellenőrzési tranzakcióban több szerep vesz részt — lássuk, hogyan viselkednek.

Szerepek egy ellenőrzési tranzakcióban

Minden ellenőrzésben legfeljebb hat különböző szerep vesz részt, amelyeket az alábbi táblázat foglal össze. Mindegyiknek lehet saját DID-je a decentralizált reputációs hálózatban.

Szerep	Leírás
Kibocsátó	Az a személy, aki információt tesz közzé a hálózatban — állítja, hogy valami történt (egy DID jött létre, módosult vagy szűnt meg, egy állítás, egy adott DID elvei stb.)
Alany	Az a személy, akiről az információ szól — az állítás címzettje
Autoritás	Megbízható entitás, amely a jó nevét teszi az állítás minőségére azzal, hogy kivizsgálja, és vagy áttekinti a bemutatott bizonyítékokat, vagy aktívan összegyűjti azokat
Megfigyelő	Független harmadik fél, aki nyilvántartást vezet arról, hogyan kezeli az ellenőrző az állítást — biztosítva, hogy az ellenőrző se ne hallgasson, se ne térjen el az általa deklarált elvektől
Ellenőrző	Algoritmikusan kiválasztott résztvevő, aki feldolgozza a tranzakciót
Megbízott	Egy másik résztvevő nevében eljáró személy

Kibocsátó

A kibocsátóval már találkoztunk korábban. Amikor valakivel igazságtalanság történik, vagy szeretné közhírré tenni egy saját teljesítményét, a DID által képviselt személy az, aki elindítja a folyamatot, hogy

az információ a hálózatba kerüljön — mert neki fűződik hozzá elsődleges érdeke (a motiváció vagy az elégtétel iránti vágy, vagy a nyilvános megítélésének javítására irányuló szándék).

Pozitív állítások

A magamról szóló pozitív állításokat, amelyeknek egyszerre alanya és kibocsátója vagyok, megtarthatom azokra a helyzetekre, amelyekben használni akarom őket (diploma, teljesített szolgáltatás igazolása stb.). Ebben különbözik egy pozitív állítás egy negatívtól: egy ellenőrzött negatív állítás megosztása az egész közösség érdeke, míg egy pozitív a viselőjéé.

Autoritás

Az autoritás kettős szerepet játszik: lehet **auditor** (az állítás közzététele előtt ellenőrzi a bizonyítékok minőségét), vagy **kezes** (a reputációját teszi az állítás igazságára). Mindkét esetben megerősíti a kibocsátó állítását. Ez a két szolgáltatás szétválasztható — egy autoritás kínálhatja az egyiket, a másikat, vagy egyszerre mindkettőt. A munkafeltevés az, hogy az autoritások által nyújtott szolgáltatások többsége szabadpiaci alapon nyújtható. Ez még olyan területeken is igaz, amelyeket nehéz elképzelni privatizálva, mint az igazságszolgáltatás, ahol a specializált szolgáltatások — nyomozás, bizonyítékok értékelése, egészen a ma centralizált hadseregek által nyújtott szolgáltatásokig (stratégiai tervezés, szabványosított kiképzés, beszerzés- és készletgazdálkodás stb.) — hatékonyan nyújthatók piaci szereplők által. Aligha van bármi, amit átalakítás után ne lehetne hatékonyabbá tenni a szabadpiaci ösztönzőkkel.

SZERZŐ · ALÁÍRÓ · A SAJÁT REPUTÁCIÓJÁT TESZI KOCKÁRA

1. Saját szavaival megírja az állítást
2. Valós bizonyítékot gyűjt az alátámasztásához
3. A saját DID-jével aláírja és elküldi a választott hatóságának
4. Megfizeti a közvetlenül költséget
5. Viseli a következményeket, ha hazudik

Ha ez hamis, a mutatóm lecsúszik.

A cartoon illustration of a woman with short brown hair and glasses, wearing a brown jacket over a pink shirt and grey pants. She is standing next to a rusty, anthropomorphic robot with a single antenna on its head. They are positioned behind a wooden table. On the table is a closed green book and a piece of paper with a technical diagram. The background is a plain, light-colored wall.

CÍMZETT: EGY
ÁLTALAM
VÁLASZTOTT
HATÓSÁG

KÖVETKEZŐ LÉPÉS
megkérni egy
átóságot, hogy
adjon a bizonyítékot
alá az állítást

A cartoon illustration of a document titled "ALLTASOM" in large, bold, black letters. The document is tilted and contains the following text: "Látom, hogy megtörtént, hajlando vagyok káláni melléte, alálrás káláni melléte". A red circular stamp with a white cross is placed on the right side of the document. A speech bubble on the right contains the text "a DID-en alálrás".

• a DID-ömmel
aláírva

A kibocsátó a szerző. Az ő neve van rajta.

*** Bárki lehet kibocsátó, akinek van DID-je. A mérce a bátorság és a felelősség, nem egy engedély.**

■ Az autoritás, a kibocsátó és a megfigyelő sosem lehet a saját ügyének ellenőrzője.

Az ellenőrző algoritmikus kiválasztása garantálja a függetlenséget. Senki sem ellenőrizheti a saját állítását, vagy olyan állítást, amelyben közvetlen érdeke fűződik. Ez egyike azoknak az alapszabályoknak, amelyek betartásához a DID-ek egész közösségének érdeke fűződik.

A következő grafikák kiegészítő nézeteket mutatnak arról, milyen széles tevékenységet fednek le az autoritások (az „autoritás” kifejezés felcserélhetően olvasható „szolgáltatóként”).

A KALAUZ — AZ ÉRTÉKEID SZERINT SEGÍT ELIGAZODNI

MÉLY ELEMZÉS HÁTUL · EGYSZERŰ ÚTMUTATÁS ELŐL

KALAUZ

E KALAUZ
KÖVETŐJE
EVÉNTÉ
MEGUJÍTHATÓ

például: ki
lehet kalauz

- egy politikai párt vagy mozgalom, amely szabályzatsablont tesz közé
- egy független auditcég, amely összesített megállapításokat tesz közé
- egy szolgáltatás-összehasonlító ügynökség
- egy reputáció-aggregátor (gazdasági · üzleti · szomszédsági közlekedésszabályozási)
- egy újságíró-recenzens vagy fogyasztói értékelő szolgáltatás

közkiadás -
átírányítva

AZ ELEMZÉSEM

Munkajegyzetek — nem ügyfeleknek

Én végzem az összetett munkát.
Te megkapod az egyszerű
ajánlást — de csak ha osztod az
értékeimet.

NEKED — MIT
JELENT

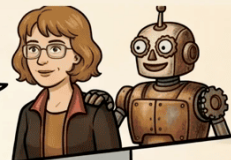
Összetette a te hasznod
maximalizálására

- itt csoportosítsd át a kiadást, ott spórolj
- támogasd azokat a szolgáltatókat, akik átmennek a tesztjeimen
- vedd át ezt a szabályzatsablont



És pontosan mit
kapok a pénzemért
— mely elemzéseket
és mely
áttekintéseket?

Az összetett világot ajánlásokká
összegezi. A követők a
figyelmükkel szavaznak —
bármikor eltávozhatnak,
átválthatnak másokhoz.



Ahhoz kötvé, amit nyilvánosan képvisel. A bizalmad az ő valutája.

* Bármikor eltávozhatsz és másik kalauzra válthatsz. A bizalmad nincs bezárva.

* A kalauz maga is aláírhat néhány saját állítást — közzétéve, de itt nem ez a fő téma.

■ Az autoritás mint inkognitó megfigyelő

Egy jó reputációjú autoritás — gondolj egy közjegyzőre, akinek az üzlete kizárólag a track recordján áll — a fő funkciók (auditor / kezes) mellett egy harmadikat is kínálhat: az inkognitó megfigyelő szerepét az ellenőrzés során. Időbélyeggel ellátott nyilvántartást vezet a benyújtott állításról, hogy az ellenőrző ne ejthesse csendben. A megfigyelő szerep mechanizmusát a Megfigyelő szerepről szóló részben írjuk le bővebben.

Ellenőrző

Bármely DID eljárhat ellenőrzőként, akár közvetlenül, akár egy harmadik DID-re delegált ellenőrzési jogokon keresztül. Ahhoz, hogy én — vagy a megbízottam — ellenőrizni tudjak, elérhetőnek kell lennem a hálózaton (online). Nem mindenki akar erre kötelezettséget vállalni, ezért egy DID-bejegyzés prioritási sorrendben felsorolhatja azokat a helyetteseket, akik a funkciót a nevében ellátják, amíg offline van.

Minden, a hálózatban aktív DID nyilvánosan deklarálja a saját elveit. Az azokban az elvekben meghatározott szabályok révén ítéli meg az ellenőrzési folyamat során az ellenfél reputációját, valamint annak az állításnak a tartalmát és formáját, amelyet a kibocsátó a reputációs hálózatba való közzétételre jelölt. Az elvek részét képezi az a számítási képlet, amellyel az ellenőrzési szolgáltatásokért járó díjakat számolják. Ha ez megvan, akkor a hálózaton átváramló, statisztikailag nagyszámú állítás közül várom, hogy a hálózat algoritmusa a kibocsátó oldalán engem húzzon, és egy adott iterációban engem rendeljen a kibocsátott információ ellenőrzésére. A kibocsátó előre kiszámíthatja, hogyan reagálna egy helyesen viselkedő ellenőrző, de nem kerülheti el, hogy ténylegesen felvegye vele (vagy a helyetteseivel) a

A SZOLGÁLTATÓ — ÁLLÍTÁS-ALÁÍRÓ SZOLGÁLTATÁST ÜZEMELTET

KÖZZÉTETT SZABVÁNYOK · KÖZZÉTETT ÁRAK



Ahhoz kötve, amit nyilvánosan kinyilvánít. A többit a reputáció intézi.

* A szolgáltatónak is van saját szabályzata — mikor fogad el, mikor utasít el, hogyan térít vissza. Közzé van téve, de itt nem ez a fő téma.

kapcsolatot; a kiválasztott ellenőrzővel folytatott iterációt a kibocsátónak akkor is végre kell hajtania, ha előre tudja, hogy nem fog átmenni.

Honnan tudjuk, hogy a kibocsátó az ellenőrző-kiválasztási algoritmust a helyes ellenőrzőjelölt-DID-halmazon futtatja? A nyilvánosan deklarált elveivel együtt minden DID közzéteszi a reputációs hálózaton belüli közösségi hálózata azonosítóinak aktuális listáját is. Ha egy kibocsátó a közösségi hálózatát olyan társadalmi buborékként határozza meg, amely csupán visszhangozza és megerősíti a saját nézeteit, akkor a rajta keresztül közzétett információt más közösségek aligha fogadják majd szélesebb körben. Az a tény, hogy nagy költséggel sikerül egy radikális állítást a hálózatba nyomnom, nem jelenti azt, hogy az ellenfél reputációjának megítélésekor bármilyen súlyt adok neki. Bizonyos állításokat a közösségem nyom rám, hogy figyelembe vegyem (elkövetőkre kiszabott büntetések és korlátozások); mások teljes mértékben rajtam múlnak — magam döntöm el egy adott információdarab beszámításának vagy kizárásának gazdasági értékét.

Alany

Azok, akikre a reputációs hálózatba közzétett információ vonatkozik, annak viselői, vagy ha úgy tetszik, alanyai. A reputációs hálózatban az ösztönzők úgy vannak beállítva, hogy az alanyok minden oka megvan arra, hogy a saját szabályai szerint helyesen és tisztességesen viselkedjen, és a közösség a szabálykövetés valamiféle arany középútja felé tolja. Még arra is ösztönzik, hogy erkölcsösebben viselkedjen, mint amennyit a deklarált szabályai megkövetelnek — az előre deklarált elvek nem zárják ki, hogy a közösség konszenzusra jusson valamely értékelés vagy intézkedés visszamenőleges alkalmazásáról. Ebből a szögből nézve a reputációs hálózat jogrend-alternatívája, ahogyan az várható, inkább a szabályok szellemétől vezérelt, mint a betűjétől.

AZ ELLENŐR — A KÖZZÉTETT SZABÁLYZAT ALAPJÁN ÍTÉLI MEG AZ ÁLLÍTÁST

NÉGY KAPU, SORRENDEN. ELŐSZÖR AZ OLCÓ SZŰRŐK.

Nem lehet kreatív.
Azt kell tennie,
amit a
szabályzata
mond.

A saját szabályai.
Nyilvánosak. Nem
változtathatja meg
őket csendben.

ELLENŐRZÉSI KAPUK — SORRENDEN

1. SZABÁLYZATI
KAPUZÁS
Egyáltalán
ellenőrzöm ezt a
fajta állítást?

2. HATÓSÁGI
BIZALOM
A hatóság a
küszöböm felett
van?

3. KIBOCSÁTÓI
REPUTÁCIÓ
A kibocsátó eléri a
reputációs mércémet?

4. TARTALMI
ELLENŐRZÉS
Aláírások,
konzisztencia,
szabályzattal való
eltérés

NEM LEHET:
kibocsátó,
hatóság,
megfigyelő vagy
alany.

ELLENŐRI
REPUTÁCIÓ

ELTÉRÉS A
SZABÁLYZATTÓL → A
REPUTÁCIÓ ESIK → A
NINCS TOBB JÖVŐBELI
KIVÁLASZTÁS

MIT TESZ AZ ELLENŐR

1. A közzétett szabályzati kapui szerint szűr (sorrendben)
2. Ellenőrzi a hatósági bizalmat, majd a kibocsátói reputációt
3. Csak akkor értékeli az állítás tartalmát, ha a kapuk átgengedik
4. A kockázattal arányos díjat számít fel
5. Minden döntésnél a saját reputációját teszi kockára

DÍJ $\propto$
KOCKÁZAT

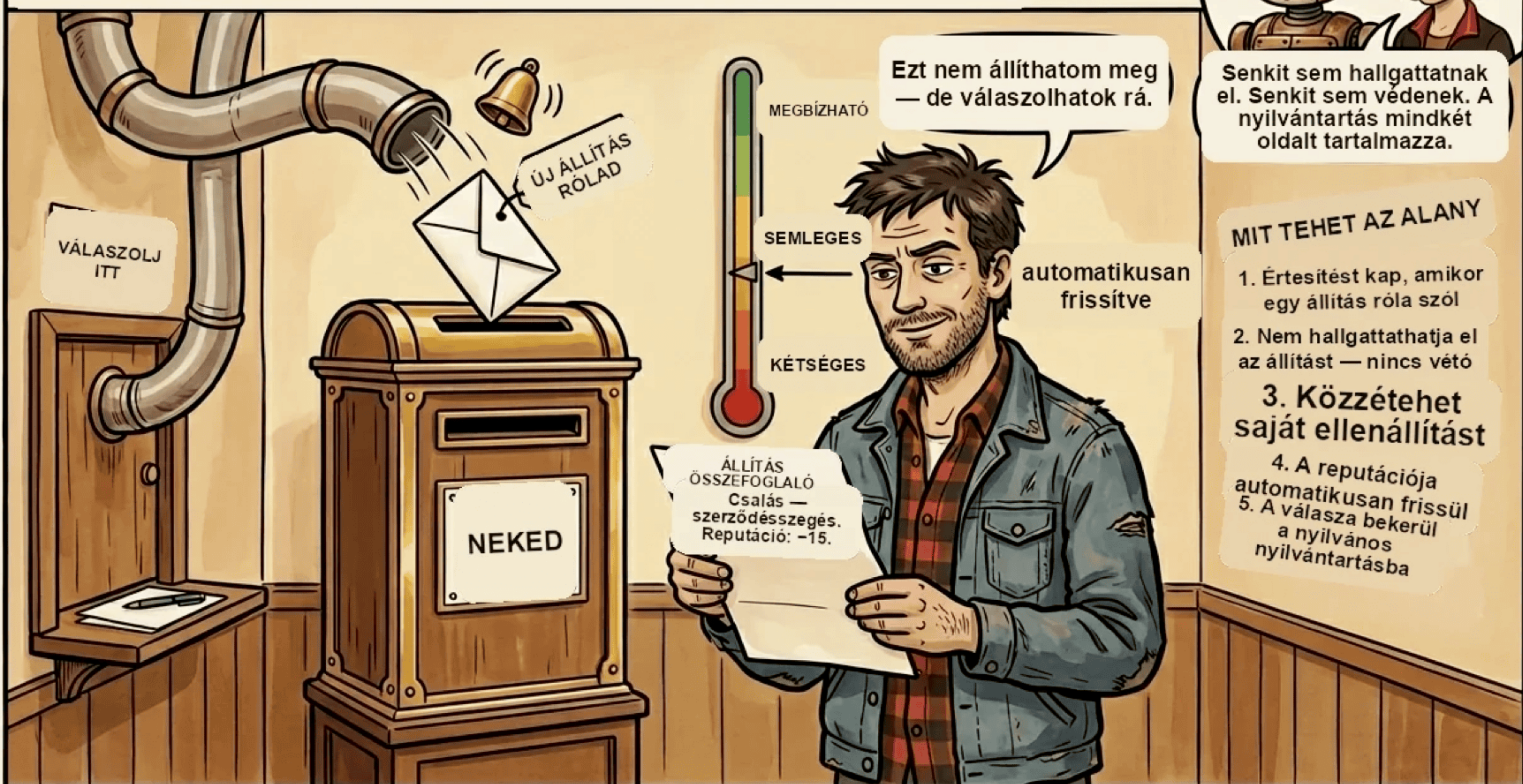
több kockázat → nagyobb díj

Először az olcsó szűrők.
Utoljára a drága tartalmi
ellenőrzés.

Az ellenőrt kötik a szabályok, amelyeket ő maga tett közzé — és a reputáció, amit elveszíthet.

AZ ALANY — AKIRŐL AZ ÁLLÍTÁS SZÓL

MEGKAPJA · NEM HALLGATTATHATJA EL · VÁLASZOLHAT RÁ



Az alanynak nincs vétője — csak joga a válasznak.
* Az ellenállítás maga is állítás — az alany reputációja kockán forog azért, amit válaszként mond.

Megfigyelő

A megfigyelő szerep megszünteti az ellenőrző ösztönzését arra, hogy hajlítsa a szabályokat. Olyan helyzetekben, amikor egy ellenőrzőnek nem tetszik a kibocsátó vagy az autoritás kérése, egyszerűen hallgathatna — nem válaszol, és blokkolja az algoritmikus sorrendet. A megfigyelő — vagy megfigyelők egy halmaza — a reputációját teszi arra, hogy dokumentálja, hogyan kérdezték meg az ellenőrzőt. Ha az ellenőrző hallgat annak ellenére, hogy a deklarált elvei mást mondanak, elmarasztalható a protokoll megsértéséért.

A mechanizmus: időbélyeg és kihíváskód

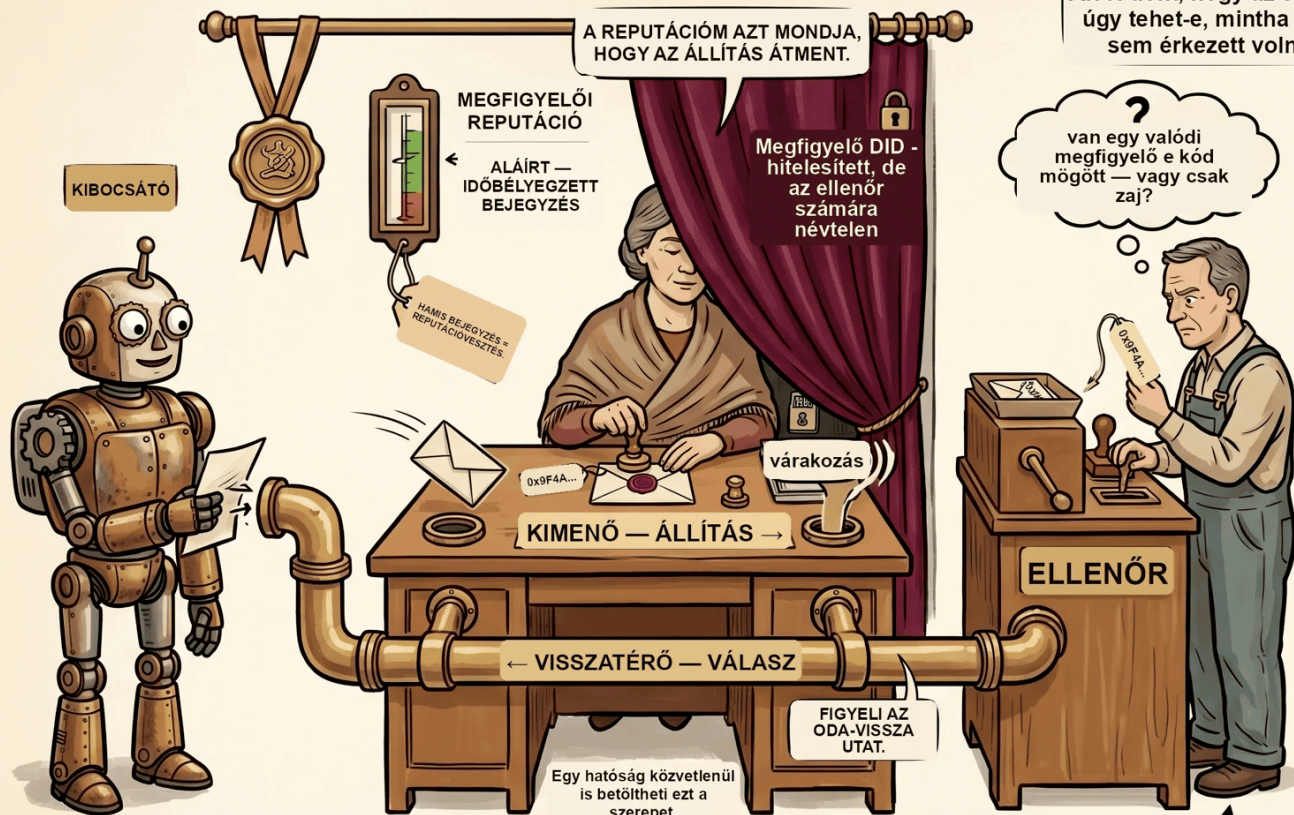
Mielőtt elküldenél egy állítást az ellenőrzőnek, átirányítod megfigyelőkön keresztül — embereken, akikben megbízol, vagy specializált megfigyelőszolgáltatókon, akik kis díjat számolnak fel. Minden megfigyelő megkapja a beadványodat, időbélyeggel látja el, aláírja, hogy látta kimenni, és kihíváskódot generál — a saját aláírásának kriptográfiai hashét. A kódok hozzáfűződnek a kéréshez. Az ellenőrző látja őket, de fogalma sincs, kik a megfigyelők, vagy hogy a kódok egyáltalán valósak-e. A megfigyelők így proxyként működnek a kibocsátó és az ellenőrző között, független nyilvántartást tartva arról, hogy az állítást benyújtották, és hogy mit tartalmazott. Zérótól N-ig terjedhet a számuk.

Amikor az ellenőrző becsületesen viselkedik — a deklarált elveivel összhangban fogad el vagy utasít el —, a kódok átlátszatlanok maradnak. Senki sem lepleződik le.

De ha az ellenőrző hallgat annak ellenére, hogy engedékeny elveket vall, vagy úgy válaszol, ami ellentmond annak, amit közzétett, nálad vannak az eredeti megfigyelői aláírások. Közzéteheted őket proxy-tanúságtételként, hogy az állítást benyújtották, és hogy az ellenőrző nem tartotta be a protokollt. Bárki ellenőrizheti, hogy az aláírások egyeznek-e a kihíváskódokkal.

A MEGFIGYELŐ — EGY PROXY, AMELY TOVÁBBÍJTJA AZ ÁLLÍTÁST ÉS FIGYELI AZ ODA-VISSZA UTAT

AZ ELLENŐR VELE BESZÉL. AZ ELLENŐR SOHA NEM TUDJA MEG, KI Ő — VAGY HOGY EGYÁLTALÁN FIGYELI-E VALAKI.



MIT TESZ A MEGFIGYELŐ

1. Megkapja az állítást a kibocsátótól
2. Lepecsételi a saját pecsétjével — a pecsét az időbélyegzett bejegyzés
3. A kibocsátó nevében továbbítja az ellenőrnek
4. Figyeli, hogy visszaérkezik-e a válasz, és mit mond
5. Csak akkor teszi közzé az aláírást, ha az ellenőr visszaél — a reputációja a garancia

lábjegyzetek

Bárhol is és hogyan is állhat, az N közötti megfigyelő állhat. Az ellenőr csak állítástan kodokat lát, és sosem tudja, hogy valódi megfigyelő figyel-e, vagy csak zaj. Ez a bizonytalanság a jó viselkedés ösztönzője.

* Szimmetrikusan az ellenőr is átvezetheti a választ a saját megfigyelőjén — ugyanaz a trükk, ellenkező irányban.

A nyilvánosság előtt névtelen, a hálózatnak felelős. Az ellenőr a kódot látja, sosem a megfigyelőt.

A csattanó: nincs szükséged valódi megfigyelőkre

És itt jön a legelegánsabb rész: **egyáltalán nincs szükséged valódi megfigyelőkre**. Generálhatsz véletlen számokat, amelyek pontosan úgy néznek ki, mint a kihíváskódok. Az ellenőrző nem tudja megkülönböztetni őket — kockáztatnia kell, hogy kockára tegye-e a reputációját. Minden kapott kérése mögött állhat egy tekintélyes megfigyelő, aki inkognitóban figyel — vagy lehet tiszta zaj is. Az ellenőrző nem tudja. És ez a bizonytalanság a mechanizmus.

A becsületes nyomás fenntartásának költsége: közel nulla (a véletlen számok ingyenesek). A becsstelenség lehetséges költsége az ellenőrző számára: katasztrofális. A becsületes viselkedés akkor is ösztönzött, ha valójában senki sem figyel.

A rendszer azért működik, mert mindenki egy kicsit paranoiás. A bizonytalanság olcsóbb, mint a megfigyelés.

A BLÖFF, AMELY ŐSZINTÉN TARTJA AZ ELLENŐRT

EGY VALÓDI MEGFIGYELŐ ÉS EGY VÉLETLEN BLÖFF EGYFORMÁNAK LÁTSZIK AZ ELLENŐR ASZTALÁRÓL

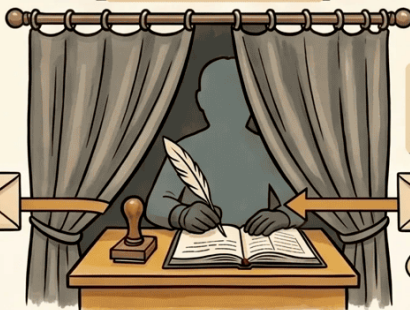
KIBOCSÁTÓ — KAMILA



ÁLLÍTÁS



VALÓDI MEGFIGYELŐ



KIHÍVÁSI KÓD —
AZ
IDŐBÉLYEGZETT
BEJEGYZÉS
HASHE



ALÁÍRT
KIHÍVÁS

ELLENŐR

valaki nyilvántartja,
amit itt teszek?
nem tudom — így
hát jól viselkedem.



az ellenőr nem tudja megkülönböztetni a valódi
bejegyzést a blöfftől. az őszinte viselkedés az
egyetlen biztos fogadás.

KIBOCSÁTÓ — BLÖFFÖL



VÉLETLEN SZÁM

VÉLETLEN SZÁM



NINCS MEGFIGYELŐ



UGYANÚGY NÉZ
KI. KÖLTSÉG:
NULLA.

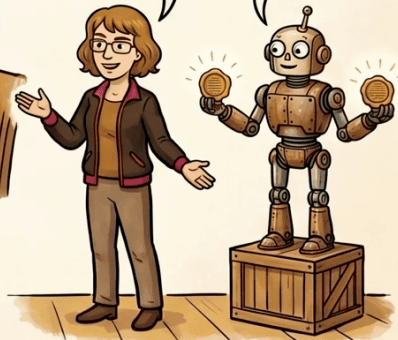
ELLENŐR — UGYANAZ A VISELKEDÉS

valaki nyilvántartja,
amit
itt teszek? nem tudom —
így hát jól viselkedem.



az ellenőr nem
tudja
megkülönböztetni
őket.

ki tudja
megmondani a
különbséget?



az őszinteségre gyakorolt nyomás költsége: közel nulla — a véletlen számok ingyenesek.
annak költsége, hogy elkapnak egy állítás elhallgattatásán: katasztrofális — a reputáció megsemmisül.

A BIZONYTALANSÁG OLCSÓBB, MINT A MEGFIGYELEÉS.

■ Több ellenőrző egyetlen iterációban

Az ellenőrző elérhetőségének megerősítő kísérőszabálya lehet egy olyan algoritmikus kiterjesztés, amely egyetlen iterációban nem csak egyet, hanem ellenőrzőjelöltek egy halmazát adja vissza.

Delegálás

A civilizáció a gazdasági növekedését a munkamegosztás és a specializáció képességére építette. A világ a maga teljes pompájában összetett, és az esélyünk arra, hogy a maga teljes összetettségében felfogjuk, közel nulla. A természetes kiút az, hogy a kényelmes életet támogató tevékenységek széles körét specializált szolgáltatókra delegáljuk, akik időt, energiát és pénzt takarítanak meg nekünk, és lehetővé teszik, hogy cserébe mi is specializálódjunk — azokat a szolgáltatásokat nyújtva, amelyekben a legjobbak vagyunk, vagy amelyeket a piac a leg többre értékel bennünk.

A delegálás ugyanezen logikája kiterjed a reputációs hálózatra is. A szabadság–totalitarizmus kapcsoló (és a delegálás) című fejezetben lefektettük egy szabad társadalom védelmének elveit azzal, hogy korlátozzuk a hálózatba egy adott időablakon belül közzétehető állítások számát (gondolj, leegyszerűsítve, alacsony egyszámjegyű éves közzétételi jogra, hogy a társadalom maximálisan szabad maradjon). Ez az elv több dimenzióra is kiterjeszthető. Nem kell csak egyetlen számunk lennie — több korlátunk is lehet, különböző típusú állításokra alkalmazva. Más számot használhatunk mások képmutatásának jelzésére, mint az üzleti ügyekben elkövetett visszaélésekre, és mondjuk egy DID-dokumentum olyan módosítása, mint egy jelszócsere, olyasmi, ami a közösséget aligha érdekli egyáltalán, és így tovább. Mindez attól

függ, hogyan határozza meg a közösség evolúciós idő során azt, mi szolgálja az érdekét a szabadság és az elszámoltathatóság célszintje közötti helyes egyensúly megtalálásában.

Miért kellene a közösség által nekem adott közzétételi jogok számának elég kicsinek lennie? Egy DID (alany) negatív állítással való megjelölése olyan reputációt tesz tönkre, amelynek felépítése hosszú időbe telt, és a kár tartós. Egy tönkretett reputáció a közösség eszkalálódó szankcióinak skálájával néz szembe minden további vagy ismételt vétségért, egészen a bomlasztó entitás teljes kiiktatásáig (a szélsőséges eset). Egy exponenciálisan eszkalálódó büntetési skálának nincs szüksége nagy mennyiségű állításra, feltéve, hogy ellenőrizhető bizonyítékok támasztják alá őket. Ez a békés egyensúlyi állapotra érvényes, amikor a társadalmat nem rázza meg katasztrófa (külső vagy belső).

Nagyon alacsony valószínűségű események esetén a statisztikai gyakoriság ingatag, ha egy egyénre alkalmazzuk. A közösség egészére nézve nem az. Ez az értéke annak, hogy a közzétételi jogainkat specializált, aggregáló autoritásokra delegáljuk, amelyek — sokban hasonlóan a kölcsönös biztosításhoz kár esetén — felhasználják a jogodat, és a nevedben alkalmazzák. Beszéljünk kevésbé elvontan, és adjunk néhány példát: - a szervezett bűnözés felderítése és leküzdése - kereskedelmi megállapodások érvényesítése - kiváltságok kezelése (végzettség igazolása, vagyonszerzés / -elidegenítés stb.) - és így tovább

A MEGBÍZOTT — EGY ÁLLÍTÁS-SZOLGÁLTATÁS, AMELYRE ELŐFIZETSZ

DELEGÁLD, AMIT MAGAD NEM TUDSZ KEZELNI · TARTSD MEG, AMI SZÁMÍT NEKED



Add ki, amit magad nem tudsz kezelni. Maradj képen. Vond vissza a jogokat bármikor.

* Ha a megbízott a megállapodott hatáskörön kívül jár el, mind az ő, mind a te reputációd nyilvánosan érinti.

■ Hogyan működnek valójában a „közzétételi jogok”

A megbízotthoz tartozó grafika a közzétételi jogokat az érthetőség kedvéért fizikai zsetonként mutatja, de a rendszerben nincs ilyen tárgy. Valójában ez történik: azoknak az embereknek az elvei, akikkel jó viszonyban akarsz maradni — a közösséged —, egy emergens szabállyá aggregálódnak arról, hány állítást fogadnak el tőled évente relevánsként, mielőtt zajként kezdenének kezelni. A felső korlát azért létezik, hogy a hálózatot ne fojtsák meg a triviális „mi lenne, ha” állítások, és olyan szabad maradjon, amilyennek a közösség akarja (a jelet a mennyiség korlátozása őrzi meg).

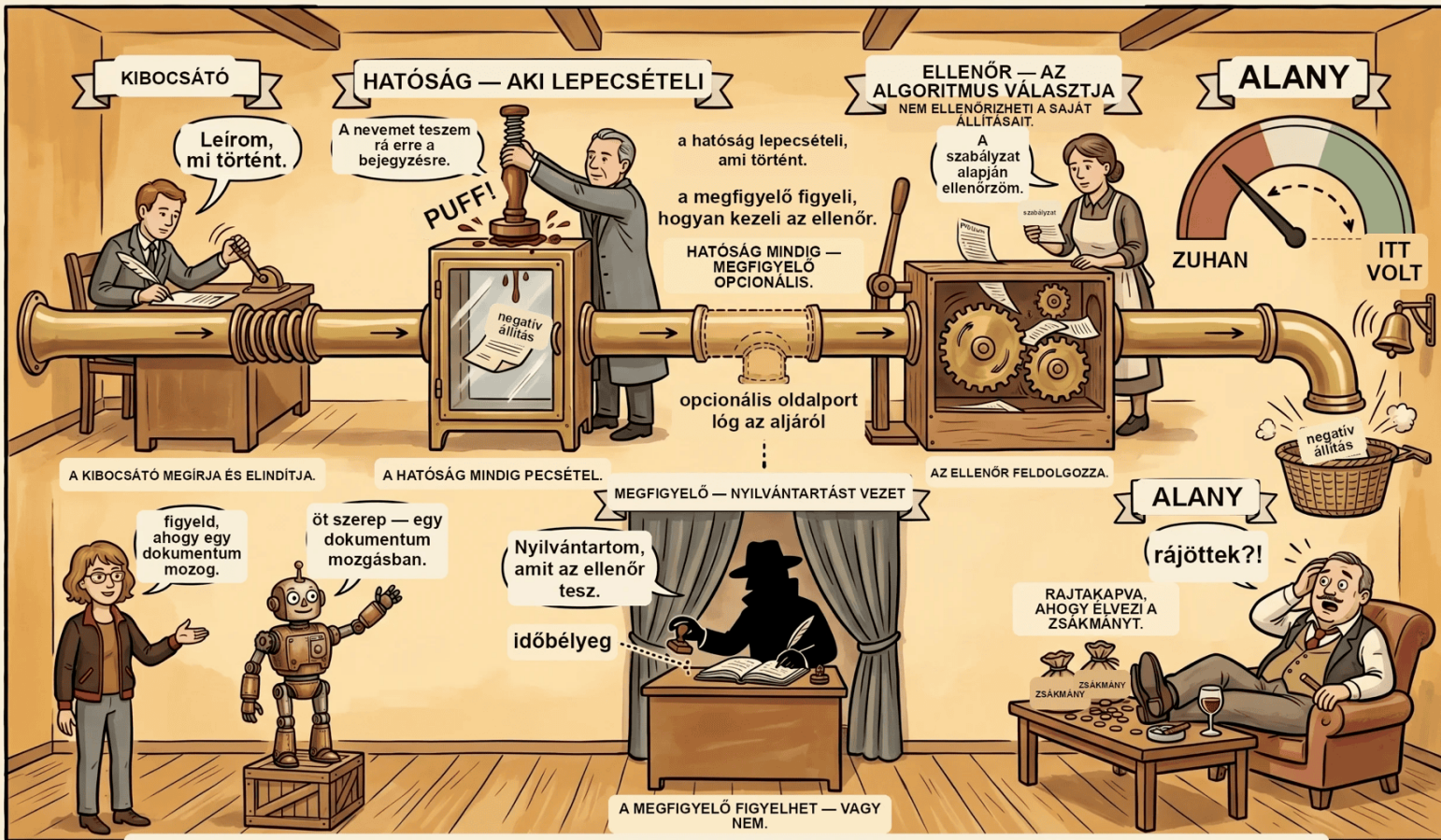
Azt olvasod, amit a közösséged megenged neked. Van egy tartomány, némi szórással attól függően, mely embereket súlyozod a legjobban. Aztán te döntöd el — ezen a kereten belül —, hány állítást teszel közzé magad, és hányat delegálsz olyan professzionális szolgáltatásoknak, amelyek csak akkor tesznek közzé a nevedben, ha az események a hatókörükbe esnek. Ez tart jó viszonyban anélkül, hogy minden apró dologra állítást kellene benyújtanod, ami veled történik.

A grafikán szereplő „zsetonok” ennek az olvasd-és-döntsd huroknak a vizuális helyettesítői, nem szó szerinti tárgyak.

Érdemes, hogy vissza lehessen vonni a reputációs hálózatban delegált közzétételi jogokat. Ez bármikor megtehető, amíg a megbízott még nem használta fel a delegált jogot.

EGY NEGATÍV ÁLLÍTÁS ÁTHALAD A RENDSZEREN

KÖVESS EGY DOKUMENTUMOT — LÁSD, MIT TESZ VELE MINDEN SZEREP



ÖT SZEREP, EGY MOZGÓ DOKUMENTUM — SENKI SEM ELLENŐRIZHETI ÖNMAGÁT.

Kommunikáció a szerepek között

Az alábbi grafika összefoglalja, hogyan kapcsolódnak össze a szerepek egy valós esetben — a kibocsátó által benyújtott állítástól a reputációs hálózatba való közzétételig.

Az emergens társadalmi szerződés — a policy

Eddig azt írtuk le, hogyan ellenőrzik az állításokat, és milyen szerepet játszik az egyes szerepek. Most rátérünk arra, hogyan válik több ezer egyéni policyból valami olyasmi, ami úgy működik, mint egy valódi társadalmi szerződés. Semmi olyasmi, ami a társadalmi szerződés és a kikényszerített szolidaritás baloldali ábrándjaira emlékeztetne.

Minden résztvevő a saját erkölce alapján deklarálja a saját policyját — hogy mit tart elfogadhatónak, és hogyan reagál mások konkrét viselkedésére. Az összes policy összessége a hálózatban egy adott DID (a közösség) által ismert körben emergens etikát hoz létre — megfigyelhető normákat, amelyeket senki sem tervezett. Ezek az emergens normák, kétoldalú árjelzésekkel alátámasztva, mérhető társadalmi szerződést alkotnak: nem egy elméleti konstrukciót, amelyet senki sem írt alá a születésekor, hanem empirikusan megfigyelhető szabályokat, amelyeket tényleges viselkedés támaszt alá.

■ A társadalmi szerződés

Az emberek vitatkoznak arról, hogy a „társadalmi szerződés” nem oximoron-e. Senki sem ír alá semmit, mégis erre hivatkoznak a centralizált társadalmakban a törvényhozói és végrehajtói cselekvés igazolására.

Egy decentralizált hálózati interakciók fenomenológiai elemzése bizonyos emergens szabályokat tárhat fel — globálisakat vagy lokálisakat. Minek nevezzük ezeket a széles körben osztott normákat? Társadalmi szerződésnek? Ahogy a közösségeknél, úgy egy közösség társadalmi szerződését sem lehet pontosan megfigyelni és körülhatárolni — a közösségre vetett minden egyes szög más társadalmi szerződést ad.

■ Értékalapú politika

Hasonlóan félrevezető az „értékalapú politikát” a döntéshozatal alapjaként kezelni. Az értékek inkább olyan szabályok fenomenológiai fűrtjei, amelyeket egy adott időben gyakran preferálnak. Fejlődnek, és nem állandók az időben.

A SZABÁLYZATOK TALÁLKOZNAK. ATTITÜDÖK FORMÁLÓDNAK.

A KINYILVÁNÍTOTT SZABÁLYOK SZABJÁK MEG A MAI ÁRAT — KEDVEZMÉNY AZ ÖSSZHANGÉRT, MALUSZ AZ ELTÉRÉSÉRT

AMIKOR A SZABÁLYZATOK ÖSSZHANGBAN VANNAK



Ugyanaz az ár, két ár. A nyilatkozatok — nem a reputáció — döntik el.

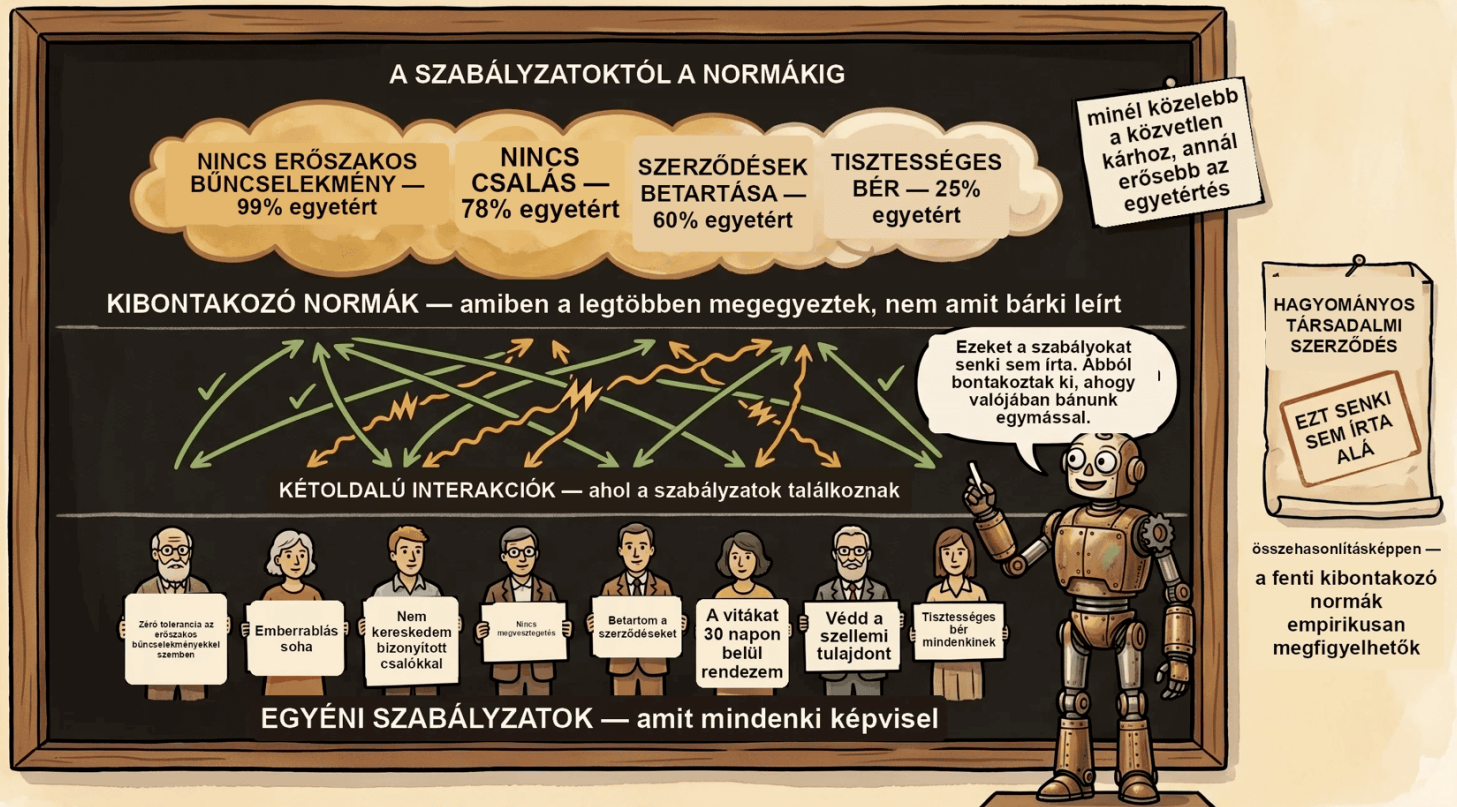
AMIKOR A SZABÁLYZATOK ELTÉRNEK



Amikor két szabályzat találkozik a kereskedelemben, az összhangjuk lesz az ármódosító.

* Ez nem a reputációról szól. Arról szól, amit mindenki nyilvánosan kinyilvánított — és amit most elvárnak tőle, hogy betartson.

HOGYAN BONTAKOZIK KI AZ ETIKA AZ EGYÉNI SZABÁLYZATOKBÓL



Az etikát nem tervezik. Abból bontakozik ki, ahogy valójában bánunk egymással.

* Minden egyéni szabályzat az adott személy erkölcsének tükré — a közösségéhez és környezetéhez való alkalmazkodás nyomása formálja.

Információ szolgáltatása magadról

Amikor két, egymást nem ismerő DID-alany gazdasági kapcsolatba lép, aláírhatunk egy kérést a saját közösségünkhöz a másik fél nevében, hogy szolgáltatson információt rólunk. Ez azonban nagyon naiv elképzelés arról, mik a közösségek. Nem zárt halmazok — egyetlen DID több közösség résztvevője is lehet.

A közösség inkább egy fenomenológiai jelenség egy adott résztvevő szemszögéből, amely a közösségi hálózatában nyilvánul meg; nem olyasmi, amit mindig van értelme kifejezetten körülhatárolni. Egy falu lakói alkothatnak közösséget, de egy ember, aki csak hétvégén jár oda, tartozhat egy másik közösséghez is ugyanabban a faluban. Egy közösség lehet egy focicsapat is a szurkolóival, tisztségviselőivel és az érintettek családjával együtt. Egy nemzet, vagy egy állam polgárai szintén alkothatnak közösséget vagy közösségeket. Egy DID-re különböző szögekből nézve más-más (és gyakran intuitív) nézetek adódhatnak a közösségekről.

A határokon lévő DID-ek így hidak a közösségek között, és — akárcsak a valós életben — szerepet játszanak abban, hogy más közösségek tagjairól információt szolgáltatassanak, akár amatőr szinten, akár professzionálisan, mint egy autoritás, amely emberek összekapcsolására és a kockázatos DID-ekről szóló információk aggregálására specializálódott.

A DID-hálózatban bizonyos típusú információk jól alkalmasak a feltétel nélküli kölcsönös cserére (erőszakos bűncselekmény, csalás stb.). Más típusú információkat viszont egy közösség a közösségen belüli használatra korlátozottként kezelhet (az állampolgárság megfelelője, a közösségnek nyújtott szolgáltatások stb.). Hogy egy ilyen információ terjeszthető-e, az a közösség tagjainak deklarált elveitől függ.

A közösség a saját körén belül őrzi a magánéletét, cserébe pedig feltétel nélküli alapon oszt meg kölcsönösen előnyös információt.

Bűn és bűnhődés

Bűn és bűnhődés

Tudjuk, hogyan működik a hálózat: hogyan keletkeznek a bejegyzések, ki ellenőrzi őket, hogyan riasztják el az ellenőrzői csalást. Egy kérdés marad — mi történik, amikor valaki ténylegesen kárt okoz egy másinak?

■ Mennyire függünk egymástól?

Mindnyájan e nagy világ színpadán állunk, és bármi történjék is itt, mindnyájunkat érint.

Jan Amos Comenius (A világ útvesztője és a szív paradicsoma)

Sok oka lehet annak, hogy valaki csatlakozik egy reputációs hálózathoz vagy elutasítja azt. Hiszem azonban, hogy az emberi természet egy aspektusa — amelyet gyakran sötétnek tartanak — jó célt szolgálhat. Az ember azon igényéről beszélek, hogy elégtétel érzését élje át az érzékelt igazságtalansággal szemben.

Elégtétel, igazságszolgáltatás, bosszú — negatív érzelmekhez társítjuk őket. Ahhoz, hogy a társadalom összetartsen, legalább úgy kell tennünk, mintha az elégtétel centralizált intézményeken keresztül szolgáltatnák; különben az egyének nem éreznék, hogy kötődnek a társadalomhoz, amelyben élnek.

Átlagosan szükségünk van arra, hogy valamilyen csapathoz tartozzunk, és bízzunk benne. Amikor valaki kárt okoz egy másiknak, a társadalom figyeli, hogyan és milyen mértékben szolgáltatnak elégtételt. Némileg vitathatóan azt állítom, hogy a történelemben gyakran — és most is — nem az számított, hogy a vádlott elleni eljárás tiszta volt-e; az számított, hogy a társadalom lásson *valakit* megbüntetve. Betöltötte a funkcióját (számos igazságszolgáltatási tévedés és a régi ügyek újranyitásával szembeni ellenállás elég jól elmondja ezt a történetet). Az áldozat és a hozzátartozók nézete csak másodlagos. Először a társadalom többi részének küldött jelek számítanak, mert az igazságtalanságok nem olyan gyakoriak, hogy minden egyes ember napjában szerepeljenek.

Egy decentralizált reputációs rendszer lehetővé tenné, hogy a nyilvánosság közvetlen és közvetett bizonyítékokat lásson (auditálva és auditálatlanul). A társadalom értékelhetné az információt — magától vagy az ilyen értékelésre specializált szabadpiaci szolgáltatásokon keresztül —, és minőségi és mennyiségi jelek alapján eldönthetné, milyen intézkedéseket alkalmaz az alannyal (vagy akár a szerzővel vagy az ellenőrző autoritással) szemben.

Mi a büntetés? Az állítólagos elkövető megalázásának egy formája a kiváltságai elvesztésén keresztül — hogy mind az áldozat, mind a társadalom érezze, a káros tettek nem érik meg. Ez a lényegi pont: a káros vagy veszélyes viselkedés nem érheti meg, és egyúttal az elégtétel érzését kell nyújtania mind az áldozatoknak, mind a társadalom/közösség többi részének.

Kell-e egy ilyen büntetést központi hatóságnak végrehajtania? Mi lenne, ha mindenki előre bejelenthetné, hogyan fog reagálni bizonyos tettekre? Nyilván nem hajthatok végre büntetést más tulajdonán. De bejelenthetem, hogy a tulajdonomat egy kiválasztott végrehajtó autoritások halmazának rendelkezésére bocsátom az elkövető megbüntetése céljából, ha a vétkes belép a felségterületeimre. És ezt nyilvánosan bejelenthetem, hogy mások értékelhessék a hozzáállásomat.

És itt lép be az arányosság ármechanizmusa. Ha kis vétségekre kemény büntetéseket jelentek be, a hálózat beárazza a szélsőségessegemet: mások aránytalannak találnak, és az ellenőrzési költségeim emelkednek — kevesebben akarnak majd kereskedni velem, vagy csak rosszabb áron, és kevesebb ellenőrző fogadja el a bejegyzéseimet észszerű áron. Ha viszont túl elnéző vagyok, a közösség kockázatnak lát. Ha eltűröm a csalást, a közösség valószínűleg elnéző lesz azon tettek elkövetőivel szemben, amelyek engem érintenek — hogy megkóstoltassa velem a saját orvosságomat.

Az igazságszolgáltatás megszűnik luxuscikk lenni. Amikor valaki kárt okoz neked, a sérelem rögzítése megfizethető, a bejegyzés maradandó, és a következmények az elkövető számára valósak.

Képmutatás-felderítés

Egy policy deklarálása nem elég — ha bejelentem, hogy betartok egy szabályt, de a viselkedésem eltér tőle, a rés reputációs teher. A hálózat nem tesz különbséget „megszegte a törvényt” és „megszegte a saját szavát” között — mindkettő mérhető jel. A képmutatás drága, és nem ismerek nála bosszantóbb vörös posztót.

EGY CSAPDA. EGY KIÚT.

A BENNFENTES MINDIG ELYNERI A SZERZŐDÉST — AMÍG A HÁLÓZAT NEM ENGEDI, HOGY AZ EMBEREK KÖZVETLENÜL VÁSÁROLJANAK, ENGEDÉLY NÉLKÜL.



A közvélemény egyetért, hogy új közületi IT-rendszerre van szükség, a költségvetésből fizetve, az adókból fizetve.



Zárt ajtók mögött a közbeszerzési ügyintéző és a bennfentes úgy alakítja ki a tendert, hogy egyetlen céghez illjen. Egy boríték gazdát cserél.



Az ügyintéző vállat von. A zsebe dagad a kenőpénztől.

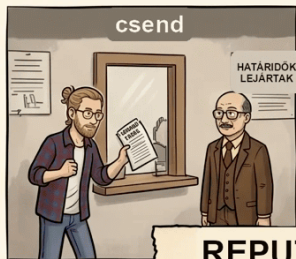


A szerződést odaítélik. A bennfentesnek megvan az engedélye — de nincs szaktudása, és nincs tisztelete a munka iránt.



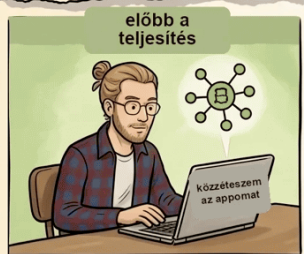
A bennfentes meglátogatja a szomszédot. A 'kedves ajánlat' a legkisebb morzsa.

1. HAGYOMÁNYOS



REPUTÁCIÓS HÁLÓZAT
— itt kezdődik az új világ —

2. REPUTÁCIÓS HÁLÓZAT



Két út. A csapda a szabályokban van. A kiút az, ha teljesen megkerülöd a szabályokat.

* Amikor a szabályokat a bennfentes írja, a szabályokon belüli panaszkodás a csapda — még a bírságok is a következő manipulált tendert táplálják. A reputációs hálózat a kiút: a polgárok megtalálják a terméket, közvetlenül fizetnek az alkotónak, és a közösség adja az egyetlen számító engedélyt — a teljesítéssel kiérdemelt bizalmat.

■ Mennyiség kontra minőség — a bűnösség bináris paradigmájának megtörése

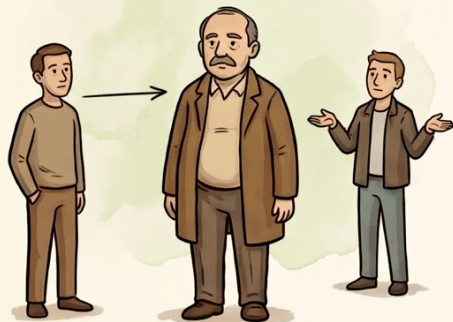
A centralizált igazságszolgáltatásban a bűnösség bináris: 0 vagy 1, bűnös vagy nem bűnös. Egy reputációs hálózatban nem az számít, hogy a bűnösség bizonyított-e, hanem a jelek felhalmozódása.

Egyetlen, bizonyítatlan lopásvád a vádlottal szemben valószínűleg nem kelt majd nagy éberséget — de éberséget kelt a vádlóval szemben. Több közvetett jelzés különféle független forrásokból viszont kezd súllyal bírni. Nemcsak a mennyiség számít, hanem a minőség is: a tanúk függetlensége (különböző emberek, különböző kontextusok), a minta konzisztenciája (visszatérő gyanútípus), az időbeli korreláció.

Ezzel szemben az ugyanattól a kibocsátótól különféle célalanyokkal szemben visszatérő gyakori alaptalan vádak rágalmazásként értékelhetők — és a vádló reputációja fizeti meg az árát.

HOGYAN HALMOZÓDIK FEL A BIZONYÍTÉK

„egyetlen elszigetelt állítás”



egyetlen állítás önmagában — túl vékony ahhoz, hogy cselekedjünk. egyik oldalt sem itéljük el.

„egy mintázatot”



öt független forrás — mintázat bontakozik ki.

„elsöprő súly”



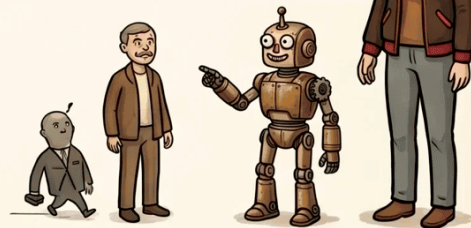
húsz független forrás — elsöprő súly.



ugyanazt az állítást bizonyíték nélkül harsogni — amikor a közösség semmit sem lát, az rágalom, és a vádlónak kerül pénzbe.



egy vádló mutogat mindenkire — a mintázat a vádló, nem a vádlott.



ez a mai világnak tűnik. az is — csak a motivációk őszinték most. nincs forradalom. csak jobb ösztönzők.

A függetlenség a minden. Egy ismételt hang zaj. Sok hang különböző helyekről jel.

Nem szabad megfélemlenünk a jóvátételről sem — egy önkéntes tetről, még mielőtt a bűnösség bizonyítást nyer, amely enyhébb büntetéshez vezető utat kínál. A büntetés akkor lép be, amikor az elkövető semmilyen lépést nem tesz a jóvátétel felé, és abban reménykedik, hogy megússza a következményeket — sokban úgy, ahogy ez a kimenetel megvásárolható korrupcióval egy centralizált rendszerben.

Vétség típusok

Az információ típusok nem korlátozódnak feltétlenül a bűncselekményekre; magukban foglalhatnak: - bűncselekmények leírását - szerződésszegést és csalást - erkölcstelen viselkedést - a köznyugalom megzavarását, valóban és virtuálisan egyaránt - ...

Minden új bejegyzés a DID-hálózatban módosítja az adott DID (legyen az alany, a szerző vagy az ellenőrző autoritás) megítélt reputációját és kockázatát. Minél nagyobb felelősséget viselek mások sorsáért, annál óvatosabbá válok.

A KÁR UTÁN — MIT FOGSZ TENNI?

elutasítva. kényszerítve. önként. háromféleképpen válaszol a falu.

mi történt



most mi lesz?



és most?)

a racionális választás mindig a legolcsóbb: HOZD
HELYRE MAGAD.

„Próbálom figyelmen kívül hagyni — mindenhol elutasítanak”



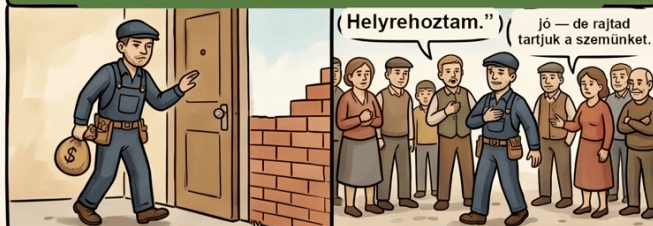
nincs jóvátétel — minden bolt elutasítja — száműzetés a gazdasági életből

„Helyrehozom — de csak a tömeg tekintete alatt”



kikényszerített jóvátétel a tömeg tekintete alatt — megtérítve, de a falu felárazza — a leckének meg kell maradnia.

„Magamtól jövök — és beismerem mindenkinek”



önkéntes, korai jóvátétel — nyilvánosan elfogadva — a reputáció helyreáll, óvatosan

ez a mai világnak tűnik. az is — csak a költségek most mindenki számára láthatók. nincs forradalom. csak jobb ösztönzők.

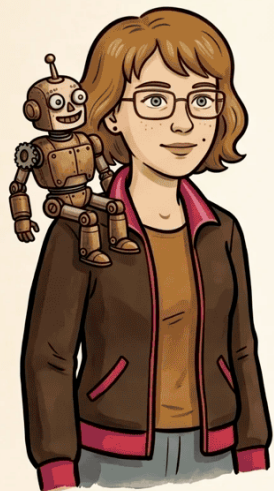
■ A büntetés érvényesítése delegálással

Nem kell személyesen érvényesítenem a büntetést. Fizethetek (a biztosításhoz hasonlóan) egy autoritásnak, amely előre meghatározott szabályok szerint érvényesíti a kimeneteket — a nyomozói, bűnüldözői és bírói szolgáltatások megfelelője. Ha az autoritás aránytalanul érvényesít, vagy egyáltalán nem érvényesít, a reputációja sérül — a reputációja pedig a megélhetési képességének alapja.

A delegálás általános elv a hálózatban: egy DID bármely tevékenysége delegálható egy másik DID-re — ellenőrzés, állítások kibocsátása, vitákra való reagálás, konszenzus deklarálása. A delegálás bármikor visszavonható. Lehetővé teszi a specializációt a végső irányítás elvesztése nélkül.

KI NYOMOZ, KI VÉGREHAJT?

„a kár” → „a nyomozó” „a bejegyzés” → „a végrehajtó” → „elszámoltathatóság”



a vállalkozóm becsapott.



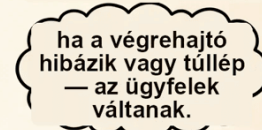
„professzionális bizonyítékgyűjtés — a reputáció az üzleti modelljük.”



„a bejegyzés bekerül a hálózatba — az elkövető reputációja esik.”



„előre megállapodott szabályok szerint jár el — mint egy biztosítás.”



„a végrehajtó reputációja a megélhetése — hibázz, és elveszíted az ügyfeleket.”

ez a mai világnak tűnik. az is — csak a motivációk őszinték most. nincs forradalom. csak jobb ösztönzők.

A DELEGÁLÁS VISSZAVONHATÓ. Bármely DID-tevékenység delegálható egy másik DID-nek — és bármikor visszavehető. nem magad hajtod végre a büntetést. delegálsz. és a megbízott neked felel.

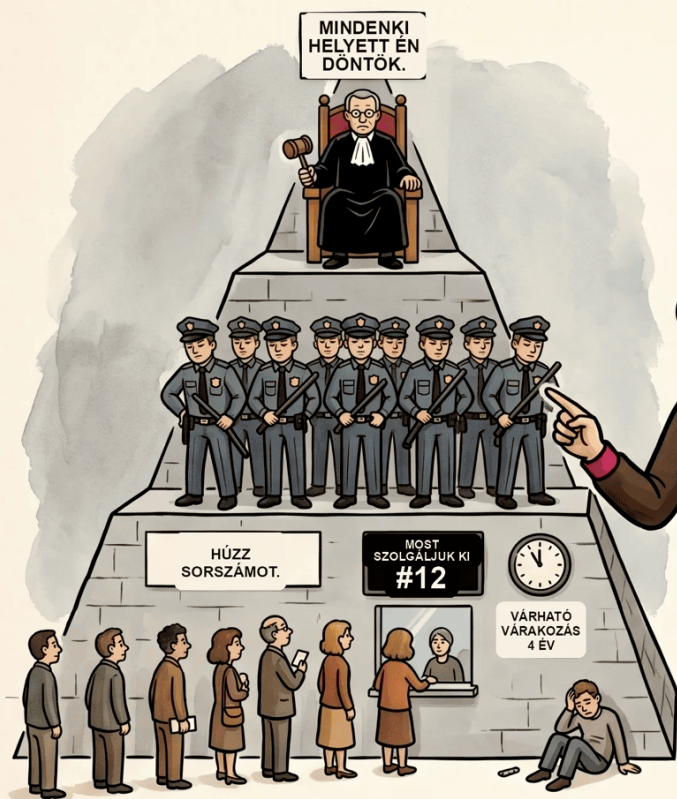
■ A kockázatkezelés demokratizálása

Egy cenzúrázhatatlan reputációs hálózat demokratizálná azt, amit a bankok vagy a nagy ipari komplexumok üzemeltetői már most alaptevékenységként végeznek — a kockázatkezelést.

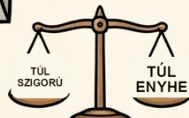
Egy ügyféllel szemben álló bankár számára a kockázatértékelés előre elkészül, hogy előre meghatározott kereteken belül az üzleti interakcióra összpontosíthasson. A kifinomult karbantartó csapatok rendszeres szervizintervallumokban kockázati indikátorokat gyűjtenek (szerkezeti repedések jelei, az üzemi infrastruktúrát degradáló folyamatok stb.), és meg tudják jósolni a berendezés élettartamát, valamint azt, mikor és milyen beavatkozásra lesz szükség.

A DID-használatot hasonlóan képzelem el — valaki (valószínűleg díjért) ember számára olvasható összefoglalót nyújt az ellenfélről. Az összefoglaló a kockázatértékelés azon szögét tükrözi, amelyet az ügyfél megrendelt.

BÜNTETÉS KÖZPONTI HATÓSÁG NÉLKÜL



egy dönt mindenki helyett — az áldozat vár — az elkövető tudja ezt.



ARÁNYOS — A
LEGALCSŐBB POZÍCIÓ

a közösség kinyilvánítja a szabályzatot — az elkövető minden oldalról szembesül vele — a hatóság érvényesíti, amiben megegyeztek.

A jóvátétel olcsóbb, mint a büntetés. | A büntetés olcsóbb, mint a tudatlanság.

Kövesd a pénzt

Kövesd a pénz nyomát

Van egy decentralizált reputációs hálózatunk és motivációnk a használatára. Már most versenylőnyt tud nyújtani a felhasználóinak — tisztázza a lehetséges kockázatokat, segít hatékonyabban megtervezni az ellenfél kiválasztását és a tárgyalási stratégiát, és beemeli azokat az intézkedéseket, amelyek csökkentik ezeket az ismert kockázatokat.

Ami következik, az egy lehetséges módszertan⁵ a használatára — a hálózat tulajdonságait kihasználva egy migrációs út megalkotására a jelenlegi rendszertől az evolúciós utódjáig. Valószínűleg magán viseli a közép-európai jellegzetességeket, ahol ez a tézis megfogant. A helyi viszonyok helyi kiigazításokat igényelnek. Amit mindenhol megőrzésre ajánlanék, az az állammal szembeni intézkedések megalkuvás nélküli jellege — enélkül a cél feloldódik a végtelen vitában, és a változás sosem érkezik meg. Vigyázz — az állam képviselői és támogatói ostobaságokkal fognak lekötni. Ne dőlj be nekik; a megélhetésük forog kockán.

⁵**Az állam dekonstrukciója** — a cseh kontextusban ezt valószínűleg mélységében tárgyalja majd Daniel Steigerwald cseh szerző készülő, azonos című könyve (2026-ra tervezve). Személy szerint nagy reményeket fűzök az inspiráló eljárásokhoz, amelyeket tartalmazni fog.

Az állam gyenge pontja — a pénz

Térjünk vissza az elejére. Több eredő szabadságot akarunk, több befolyást a formájukra, és több, hozzájuk mért felelősséget. A kérdés egyszerű: hol van az államnak sebezhető pontja, amelyre erőszakhoz folyamodás nélkül nyomást gyakorolhatunk?

A válasz unalmas, és éppen ettől erősebb. A pénz.

Lényegét tekintve az állam pénzáramlás. A pénzen keresztül fizeti a kényszerítő apparátusát — a végső láncszemet, amely érvényesíti a szabályait. Pénz nélkül nincs erőszakmonopólium. Amint a pénz akadozni kezd, az állam visszavonulni kezd — mert nem marad, amivel fizesse azokat, akik fizikailag a helyén tartják.

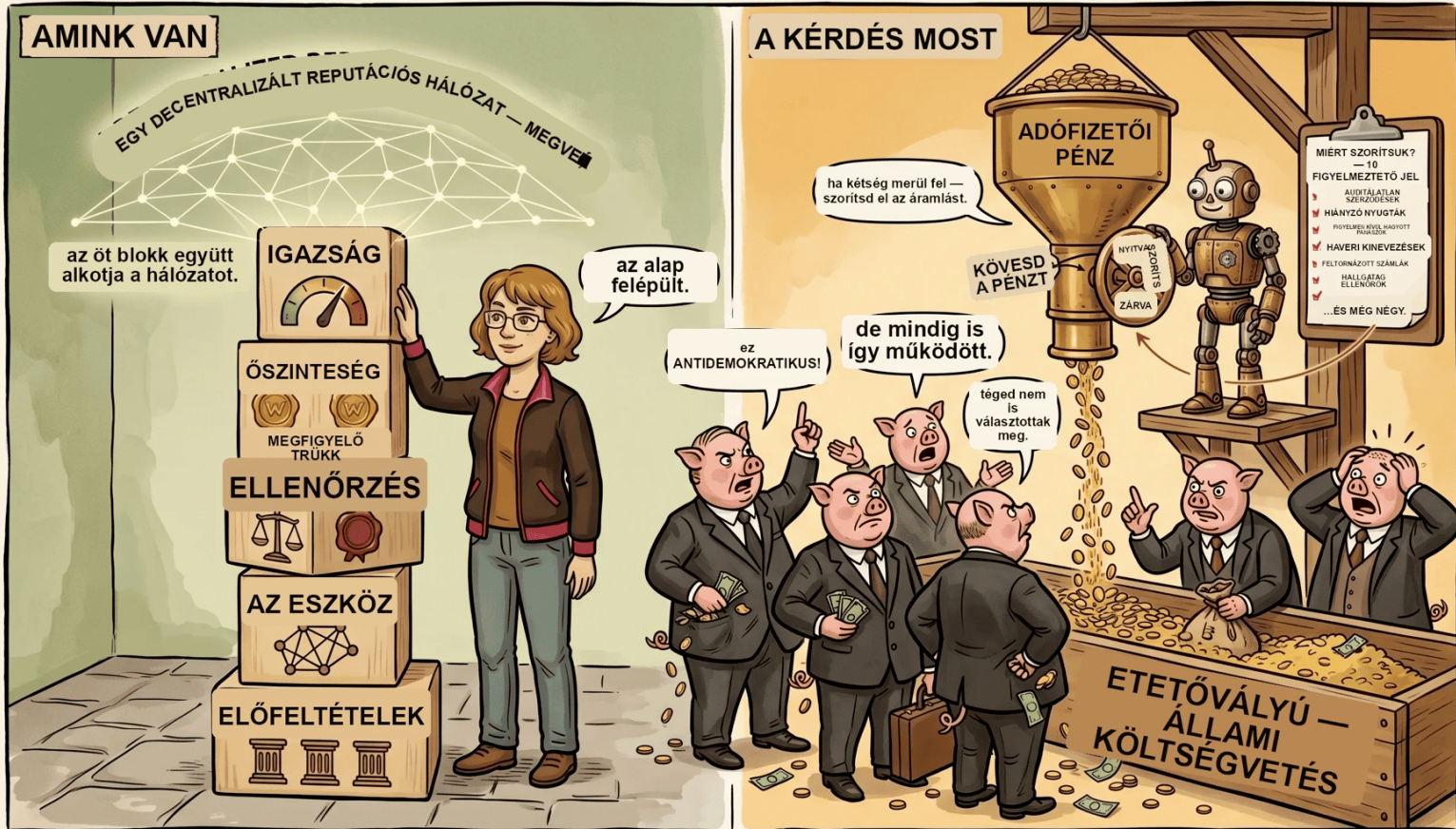
A pénzáramlások természetesen ingadoznak — szezonálisan, gazdaságilag, a befektetői hangulat szerint. Az állam ezt a pénzügyi piacokon való hitelfelvétellel álcázza. Alkalmanként egy hitel rationális: egy befektetés, amely megtérül. Gyakrabban azonban túlméretezett kiadásokat fedez olyan ügyművekre, amelyek régen kinőtték az állam alapvető célját — védelem, belbiztonság, büntető igazságszolgáltatás, közügyek. Miután bizonyos küszöbökkel átléptek, a jegybank a saját inflációbecsléséhez horgonyzott kamatlábakkal reagál.

És itt jön a csendes adó. Az infláció korántsem csupán makroökonómusok könyvelési aggálya. Ez rejtett adó a valuta vásárlóerejére, amelyet mindenki fizet, aki félretett néhány érmét öregkorára. Az alacsony inflációt a közvélemény azért tűri, mert nem fogja fel a hosszú távú hatásait — nem veszik észre, hogy még az egyszámjegyű értékek is, hosszú horizonton kamatosan felhalmozódva, olyan mértékben erodálják a megtakarításokat, hogy az emberek már nem tudják biztosítani a saját öregkorukat. És amikor nem tudják, függővé kondicionálják őket az állami juttatásoktól. Végül azokon a juttatásokon csüngnek, és az államhoz vannak kötve.

Zavaros időkben — háború, járvány, a „szükséges” beruházás — az állam egyszerűen bekapcsolja a nyomdagépet. A felelős megtakarítók és dolgozók vásárlóereje csökken, miközben azt ígérjük nekik, hogy jól meg vannak jutalmazva. Valaki csendben lopja az idejüket, és dicséri őket, milyen remekül keresnek.

Ez súlyosan aláássa az államba vetett bizalmat. A bizalom pedig az egyetlen ragasztó, amely az egész gépezetet összetartja. Ez az a kar, amelynek érdemes nekifeszülni.

KÖVESD A PÉNZT — AZ EDDIGI TÖRTÉNET



Megvan a hálózat. Tudjuk, hogyan működik. Most: ha kétség merül fel, szorítsd el a garatot. az állam hatalma a pénzen nyugszik. kövesd.

■ Miért a pénz, és nem más gyenge pontok?

A civilizáció egy másik gyenge pontja például az energiaelosztás. De az áramlásának megzavarása nem kar — az agresszió, terrorizmus lenne. Az önkéntes részvételmegtagadás nem ugyanaz, mint mások szándékos károsítása. A pénz abban kivételes, hogy a nyomás önkéntesen, átláthatóan és erőszak nélkül gyakorolható.

Proposed transition to the state's successor

Evolúció, nem forradalom

A hirtelen változás akkor is ellenállást vált ki, amikor a végcél vonzó. Kötelékeket szakít el — társadalmiakat, gazdaságiakat, politikaiakat —, és az emberek ösztönösen védik azt, amit már ismernek, azzal szemben, amit még nem láttak.

A helyes megközelítés ezért fokozatos — evolúciós. Olyan, amely megakadályozza, hogy a régi rendszer egyetlen gombnyomással kapcsolja ki az újat — mert abban a pillanatban, amikor megtehetné, meg is tenné.

Sajnos ez azt jelenti, hogy el kell fogadnunk: az egyensúlyi önkéntesség nem a reputációs hálózat telepítésének pillanatában áll be; az elfogadás fokozatos ütemével együtt érkezik. A felvétel lehet — és valószínűleg lesz is — lassú, amelyet az egyének azon vágya húz előre, hogy a reputációs hálózaton

keresztül keressenek orvoslást a közösségüktől, amikor az igazságkeresés konform módja csődöt mond (és csődöt fog mondani). Nézzük meg, hogyan néz ki ez az út, arányos becslésekkel együtt.

■ Üres vályúk — ne játssz olyan szabályok szerint, amelyeket a vesztésedre szabtak

Az államot belülről reformálni próbáló kísérletek a hatalom belső mechanizmusaira támaszkodnak, abban a reményben, hogy a hivatalnokok a saját ösztönzőik ellenében visznek keresztül változásokat. Ez nem fog megtörténni.

Miért tápláljuk a rendszert, ahelyett hogy kiszáritanánk a csatornákat, amelyek életet visznek bele? Ahelyett, hogy megváltoztatnánk a régi rendszert és a szabályai szerint játszánánk, építsünk fölé egy új réteget — olyat, amely a régi rendszert fokozatosan az új részhalmazává teszi. Az elején ez a részhalmaz szinte kitölti a szuperhalmazt. Idővel a szereplők átvándorolnak.

A cégek tudják ezt: amikor egy régi rendszer túl bonyolult a lecseréléshez, párhuzamosat építesz, és fokozatosan migrálsz bele a felhasználókat.

Az a tény, hogy az állam a végén eltérést mutat majd aközött, amit valójában nyújt, és amit a statútumai megkövetelnek, és hogy hajlamos lesz erre az eltérésre hivatkozni, tisztán a képviselői és résztvevői problémája — nincs szükség rá, hogy visszatekintsünk. Az egyetlen dolog, amit érdemes figyelni, ez: ne provokálj erőszakos forradalmat.

Négy eszköz, amely egymást támogatja

Eddig a DID-reputációs hálózat főként az igazságszolgáltatás és a konszenzus szempontjából tűnhetett hasznosnak. Hiszem, hogy stabilizálni tudná magát és kiállná a támadásokat — meritokratikusan,

tényleges érdem, nem pedig formális címek alapján. De a reputáció önmagában nem fogja rákényszeríteni az államot, hogy engedjen. A gazdaság igen, és a rajta keresztül gyakorolt nyomás.

Semmi sem akadályoz meg abban, hogy a DID-identitásokat további, a pénzre keményen nyomó eszközök kezelőjeként használjuk. Ne a polgárok teljes önkéntességével kezd — állíts be olyan irányt, amelyet az állam nem tud megállítani. Az átmenet négy konkrét eszközön nyugszik, amelyek egymás hátát fedezik. Egyik sem elég önmagában.

Egyszerű adórendszer — a belépő csali

Az első eszköz egy egyszerű, átlátható, DID-infrastruktúrára épülő adórendszer. Egyetlen arányos kulcs minden jövedelemre. Nincsenek kivételek, nincsenek adószünetek, nincsenek vállalati levonások, nincsenek ösztönzők. Minden fizetés auditálhatóan kapcsolódik ahhoz a DID-hez, amely fizette. A keresztellenőrzés triviális.

A kulcsot a régi rendszernél némileg kedvezőbben állítanák be az adófizetők egy része számára — ez a belépő csali. Az adóteher évről évre csökkenne, a rendszer egyre vonzóbbá válna, és a migráció felgyorsulna. A rendszer egyszerre nyilvántartó és beszédő — nincs közvetítő, nincs átláthatatlanság.

Elektronikus kiadásnyilvántartás (ESR)

A második eszköz az, hogy fejre állítjuk az EET-et (elektronikus bevételi nyilvántartás). Ahelyett, hogy az állam követné egy önálló vállalkozó minden egyes nyugtáját, mi követjük az állam minden egyes kiadását. Az állam az egyszerű adórendszerből egyetlen fizetésre sem kap forrást, hacsak mindegyik — kivétel nélkül — át nem megy ezen a szítán.

Az ESR egy proxy⁶, amely az állam és a közsféra minden realizált kiadását összeveti a tervezett fizetés bejegyzésével — beleértve a kontextuális indoklást és a címzett, a kiadó entitás és a cél azonosítását. Az eredmény nyers, hierarchizálható közadat. Bárki foghatja és elemezheti. Bárki ajánlhat javaslatokat az adófizetőknek arról, mit kezdjenek vele. Amit a számvetőszek évek alatt nem tudtak elérni, az hirtelen mindenki számára egy kattintásnyira van.

Nem kell átállnod az új adórendszerre, hogy részt vegyél. Elég realizált fizetésenként egy teljesen visszatéríthető letétet fizetni (mondjuk 1–3 EUR). A nem realizált maradék spamszűrőként elvész, hogy a rendszert ne árásszák el a támadások. Bejegyzést bárki benyújthat — egy rokon egy cselekvőképtelen nagyszülő helyett, egy szomszéd elhanyagolt közszolgáltatásokért, egy vállalkozó egy kifizetetlen számláért, egy hivatalnok a saját rendszeréből való exporttal.

Számítok rá, hogy a politikai pártok természetesen elemzésszolgáltatókká alakulnak át, vagy újak jönnek létre a régiéik helyett. Az adókból húzott hozzájárulások helyett szakértelmet kezdenek majd kínálni — értékalapú áttekintéseket nyújtva a támogatóiknak a szövetséges autoritásokról, azok szolgáltatásairól és ellenőrzési elveiről. A hanyagságból anyagul vagy értelmetlenül készített bejegyzések automatikusan a költségvetési megvágás jelöltjeivé válnak. Az első fordulóban a fizetésedet mindig folyósítják, de az összegyűjtött adat annak megítéléséhez szolgál alapul, hogy egy állami kiadásnak van-e még értelme. A vállalkozóknak és másoknak az állami bérlistán érdekük fűződik ahhoz, hogy a hivatalnokok felelősen párosítsák a kiadásokat. Különben a pénz nem folyik a következő fordulóban.

⁶**Proxy** (lat. *procurator*, ang. *deputy/intermediary*) — itt egy másik entitás nevében eljáró közvetítő. Az ESR-proxy bárkitől elfogadja a tervezett fizetések bejegyzéseit, összeveti azokat az állam realizált kiadásaival, és a keletkező adathalmazt a nyilvánosság rendelkezésére bocsátja.

Honnan ered az ESR rövidítés

2016 és 2022 között a cseh kormány egy Elektronikus bevételi nyilvántartás (EET) nevű rendszert vezetett be a saját polgárai — önálló vállalkozók és vállalkozók — ellen. Az üzenet egyszerű volt: „Feltételezzük, hogy mindegyikötök csalja az államot. Minden egyes tranzakciót rögzíteni fogtok, valós időben továbbítjátok a szervereinkre, mi pedig figyelünk titeket. Pénzügyileg megjutalmazzuk a polgártársaitokat, ha bejelentenek benneteket, amikor megpróbáljátok kijátszani az EET-et.”

Az EET balkáni precedensekre épült. A világon az első ország, amely 2013-ban országos szintű, kötelező, valós idejű online értékesítési nyilvántartó rendszert indított, Horvátország volt, *fiskalizacija* néven. Csehország néhány évvel később átvette a modellt, és Európa egyik legszigorúbb bevételkövetési rezsimjét működtette.

Ha a sötét oldal nem habozik, miért haboznánk mi? Az ESR ugyanez a logika fejre állítva: az állam bizonyítja magát a polgároknak.

Polgári adóallokáció — a döntés súlya

A harmadik eszköz közvetlen befolyást ad az adófizetőknek arra, hová folyik a pénzük. Az első fordulóban az állam megkapta a pénzét, függetlenül attól, mit tárt fel az ESR. A második fordulóban már nem — az első forduló elemzés és az abból következő intézkedések veszik át a szerepet. A befizetett adó egy kis százalékát maga a befizető allokálhatja — feltéve, hogy a DID-je megfelel a reputációs követelményeknek (állampolgárság, tartózkodás, közösség által elismert nagykorúság / cselekvőképesség).

ESR — ELEKTRONIKUS KIADÁSJELENTÉS

minden állami kiadás rögzítve — minden bejegyzés nyilvános — minden részlet vizsgálható.

ki nyújtja be
bármely bejegyzést
benyújthatja: — a
hivatalnok, aki
feldolgozta a
kifizetést — a
kedvezményezett,
aki megkapta a
pénzt



AZ ÁLLAMI KIADÁSOK NYILVÁNOS FŐKÖNYVE — nyílt bejegyzés

kategória: jogi tanácsadás
vállalkozó: XYZ s.r.o. ügyvéd
összeg: 14M EUR vállalva:

2026-01-14 fizetve: 2026-01-19

kontextus: külső szakvélemény az új
közbeszerzési reformtörvényről — három tervezet
készült, egy műhelymunka a minisztériummal,
nem tartottak közmeghallgatást — a végleges
tervezet a jogalkotási határidő után lett leadva.

kategória: úttervezési tanácsadás
vállalkozó: Consultancy T
összeg: 9M
EUR vállalva: 2026-02-03 fizetve: —
kontextus: megvalósíthatósági tanulmány a D-X
autópálya-bővítéshez — ugyanaz a cég írt három
korábbi tanulmányt erről a szakaszból — eredmény:
javaslat a folytatásra a korábbi becsléshez képest
+18%-kal.

bármikor számára nyitva,
aki bele akar nézni.

kategória: rendszám-tábla-kiadás
kedvezményezett: Z regionális hivatal
összeg: 45 EUR táblánként vállalva:

2026-02-19 fizetve: 2026-02-19

kontextus: szabványos igazgatási díj kiadott
táblánként — a díj fedezi az anyagokat és a
feldolgozást — teljes mennyiség 12 400 tábla
ebben a negyedévben.

kategória: kórházi eszközök vállalkozó:
MedSupply a.s. összeg: 8.2M
vállalva: 2026-03-08 fizetve: —

kontextus: MRI-készülék telepítés regionális
kórházban — nyilvános tender, három ajánlattevő
— a kiválasztott ajánlat a medián alatt 2%-kal,
szállítás 60 napon belül — a számla 90 napja lejárt.



spamszűrő — visszatéríthető letét



a letét visszajár,
amikor a bejegyzés
pontosnak
bizonyul.

a pártok elemzésszolgáltatókká alakulnak



a leírások a nyersanyag — a pártok
azzal érdemlik ki a helyüket, hogy
gondosan elolvassák őket,
kereshetik a köztudott és nyomtatott
közönyt készítenek belőlük.

ez a mai világnak
tűnik, az is — csak a
könyvek most
mindenki előtt
nyitva. nincs
forradalom, csak
jobb ösztönzők.

A közpénz minden koronája — rögzítve, nyilvánosan, vizsgálhatóan.

az érték nem a csalók elkapásában van — hanem a könyvek megnyitásában.

Az allokálható százalék évről évre nő. Potenciálisan exponenciálisan. A mai öt százalékról egy évtizeden belül tíz százalékokra.

A nyers ESR-adat természetes módon irányítja az adófizetői döntéseket. Az alacsony minőségű bejegyzések figyelmeztető jelként működnek a javasolt megvágásokhoz. Bárki készíthet bejegyzéseket; a hivatalnokoknak párosítaniuk kell azokat. Enélkül az adórendszer nem küld az államnak pénzt — sem a kincstárba, sem más költségvetési fejezetekbe. A politikai csata az urnától a konkrét érték napi allokálásához költözik.

POLGÁRI ADÓELOSZTÁS — TE DÖNTÖD EL, HOVÁ MEGY AZ ADÓD

tanulmányozd az ESR-bejegyzéseket. aztán mozgasd a csúszkákat.

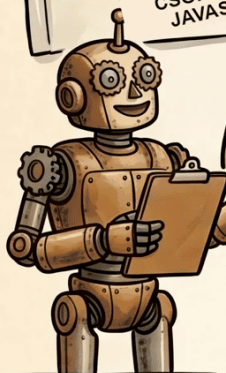
ESR ELEMZŐ JELENTÉS

készítette: egy megbízható elemző —
akit te választottál

védelmi minisztérium: — 7
szerződés 2 év alatt
egyetlen beszállítónak —
nincs közmeghallgatás a
közbeszerzési reformról
— 90 napos fizetési
csúszás a számlák
60%-án
CSÖKKENTÉST
JAVASOLOK.



rep
4.7/5



vagy delegáld ezt

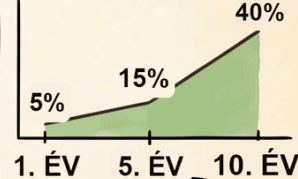
nem akarsz magad
elosztani? delegáld: — a
pártod elemzőjének — egy
megbízható
szomszédnak — bárkinek,
akit választasz — és
bármikor
visszavonhatod.



a jelentés
elolvasása
után —
védelem
lejebb.



az elosztható rész nő



kattints
bármelyik sorra
a részletekért
— bármilyen
mélységben
eloszthatasz.



ez a mai világnak
tűnik. az is — csak
a csúszka most a
te kezében van.
nincs forradalom.
csak jobb
ösztonzők.

A mai 5%-tól 40%-ra egy évtized alatt. Te döntöd el.
a bejegyzések nyitva. az elemzés a tiéd. a csúszka is.

Tárgyalási platform az állammal — a kar

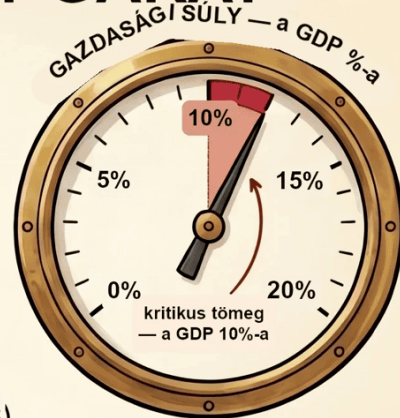
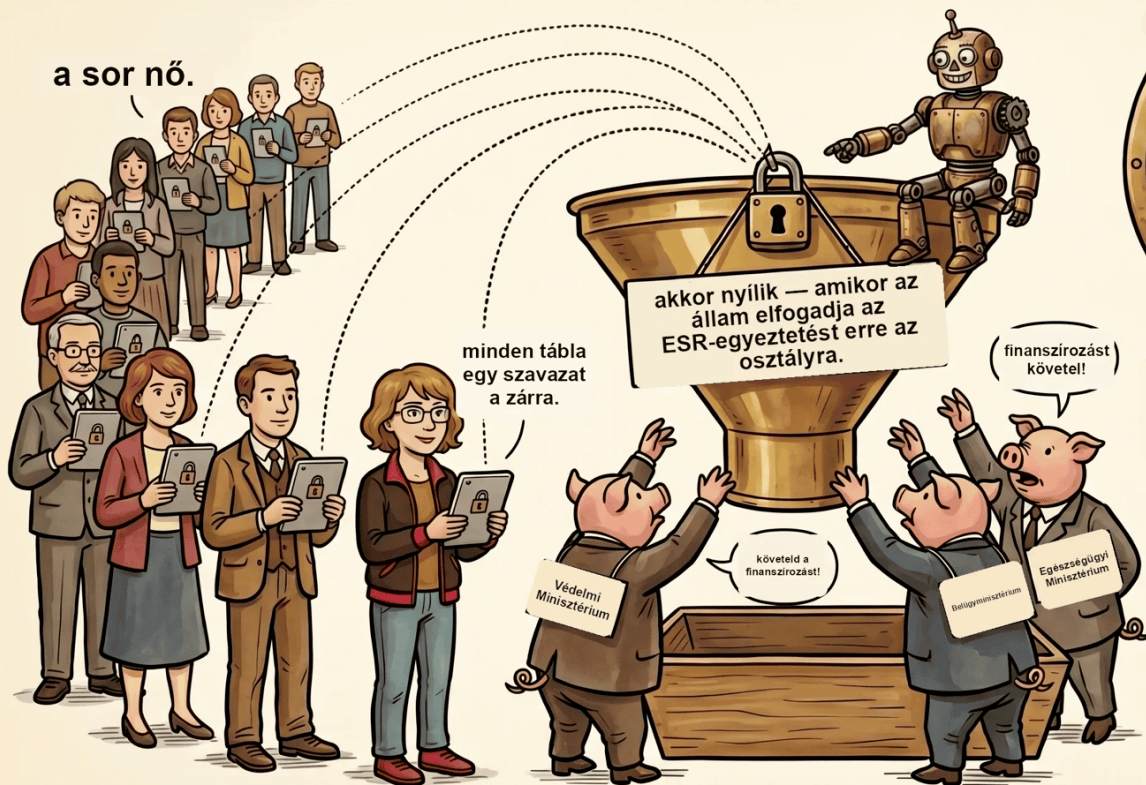
A negyedik eszköz az a kar, amely mindent összeköt, és csak most teszi a hálózatot valódi fenyegetéssé. A fő konfliktus arról fog szólni, hogy az állam elfogadja-e az ESR-t kötelező érvényű szabványként — először nemzeti szinten —, és mekkorára kell nőniük a reputációs hálózat résztvevőitől érkező fenyegetéseknek, mielőtt ez megtörténik.

A kar a just-in-time állami finanszírozás, amely attól függ, hogy a fizetéseket összevetik-e az ESR-rel. A pénz csak abban a pillanatban folyik, amikor az állam teljesítette az átláthatósági feltételeket. A reputációs hálózaton belül várólista alakul a résztvevőkből. Az aktiválás akkor lép be, amikor a csoport eléri a gazdaságilag jelentős méretet — elég nagyot ahhoz, hogy fenyegetse a GDP növekedését. Ezen a ponton a polgári engedetlenség hiteles fenyegetéssé válik, nem pusztán gesztussá.

Az állam a legtovább a korrupcióhoz kötött problémás fizetésekhöz fog ragaszkodni. Nyomás alatt először ott enged, ahol könnyű a védekezése, és ahol nincs hely megtakarítást keresni. A fokozatos és növekvő nyomás lépésről lépésre visszavonulásra kényszeríti minden pozícióból.

TÁRGYALÁSI PLATFORM — A ZÁRT GARAT

a polgárok kezében a kulcs. az állam akkor nyit, ha teljesülnek a feltételek.



a GDP kis töredéke is elég — kritikus tömegnél a visszatartás valós fenyegetéssé válik.

a kritikus tömeg után —

az állam először az egyszerű, védhető kifizetésekre nyitja meg a könyveit.

a korrupcióhoz köthető kategóriák maradnak zárva a legtovább.

minden feloldás több nyomást igényel — és maga is rögzítésre kerül.

A pénz akkor folyik, ha van átláthatóság. A polgárok kezében a kulcs.

nincs erőszak. nincs forradalom. csak elég tábla ahhoz, hogy a visszatartás hiteles legyen.

ez a mai világnak tűnik. az is — csak a kulcs most sok kézben van. nincs forradalom. csak jobb ösztönzők.

Állampolgárság személyi igazolvány nélkül

A DID-infrastruktúrára való átmenettel az állam által kiadott személyi igazolvány elveszíti a monopolisztikus célját. Nincs szükség személyi igazolványra — van egy sor DID-identitásod, és némelyikük egy állítást hordoz arról, hogy például cseh vagy, egy adott település lakosa, egy adott iskola végzettje. Az állítás ellenőrizhető, maradandó, és független az állami közigazgatástól.

Megnyílik a technikai megvalósítás kérdése: ki vállalja majd a piacon a meglévő polgárok ellenőrzését állami kontroll nélkül, hogy az érdeklődőket egy megfelelő állítást hordozó DID-be migrálja? Legvalószínűbben szabadpiaci autoritások jönnek majd létre, amelyek az identitás-ellenőrzésre specializálódnak — közjegyzők, helyi közösségek, munkáltatók. A reputációjukat teszik arra, hogy egy adott DID valóban ahhoz a személyhez tartozik, aki azt állítja magáról. Az állampolgárság — vagyis a közösség egy adott nézetéhez való tartozás — megszabadul a központi nyilvántartás szükségességétől. A reputációs hálózaton keresztüli összekapcsolással a beágyazott adatot összekötik és validálják másodszor, harmadszor, negyedszer, és így tovább.

A következmény intuitív, mégis megoldhatatlan egy centralizált rendszerben. Ma a politikai vezetés — a könnyebb újraválasztás szem előtt tartásával — koncentrált problémákat importálhat a közösség területére: más civilizációs körökből érkező migránsokat fogad be a befogadóképességre és a meglévő közösség hajlandóságára való tekintet nélkül, olyan nyomással változtatva meg az eredeti közösségeket, amely alatt azok nem tudnak lépést tartani a más civilizációs körökből érkezők asszimilálásával. Egy DID-hálózatban egy korrupt módon befogadott migráns nem lehet biztos abban, hogy a közösség továbbra is a sajátjának tekinti. A közösség tagjainak objektíve nem kell eltérniük, hogy egy idegen a közösség egyenruhájában kopogtat az ajtajukon, és a törvényességgel fenyegeti őket azon intézkedések kapcsán, amelyeket a házban végre kíván hajtani (egy gyerek telefonjának elkobzása egy közösségimédia-poszt miatt). Decentralizált reputációval a társadalom többségének nem kell ebbe belenyugodnia — mert azt,

hogy ki tartozik egy közösséghez, nem egy hivatalnok dönti el, hanem maga a közösség, a reputációs jelein keresztül.

AZ EVOLÚCIÓS ÁTMENET NÉGY ESZKÖZE

a rendszer belülről újjáépítve — anélkül, hogy összetörnénk.

EGYSZERŰ ADÓ



egy kulcs. nincs kivétel.
keresztellenőrizhető.

ESR — ELEKTRONIKUS KIADÁSJELENTÉS



minden kiadás rögzítve —
minden bejegyzés nyilvános
— minden részlet nyitva.

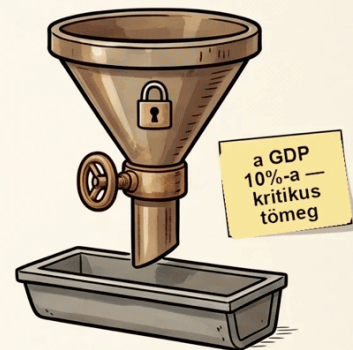
POLGÁRI ADÓELOSZTÁS

5% → 15% → 40%
1. ÉV → 5. ÉV → 10. ÉV



tanulmányozd a
bejegyzéseket — aztán
mozgasd a csúszkákat.

TÁRGYALÁSI PLATFORM



a pénz csak akkor
folyik, ha teljesülnek az
átláthatósági feltételek.

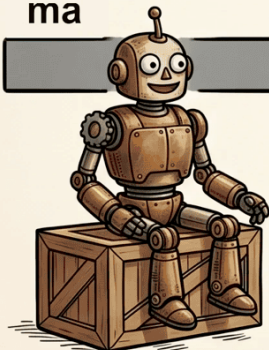
ma

az evolúció folyamatban

egy évtized alatt

95%

terjeszkedik



Evolúció, nem forradalom.

négy eszköz, amely belülről változtatja meg a rendszert.

ez a mai világnak
tűnik. az is — csak
az eszközök most a
polgárok kezében.
nincs forradalom.
csak jobb ösztönzők.



ÁLLAMPOLGÁRSÁG SZEMÉLYI IGAZOLVÁNY NÉLKÜL

az állami engedélytől a közösségi elismerésig.

„a régi módszer”: az intézményes, állam által kiadott igazolvány modellje



identitás = állami engedély — visszavonható — a közösségnek nincs beleszólása.

„az új módszer”: a DID állítás-kártyákkal modellje



egyetlen hatóság sem uralja az összes állítást — mindegyik független — minden ellenőr a reputációját teszi kockára.

„ki tartozik ide?”



a közösség dönt — reputációs jeleken keresztül — elosztottan, nincs egyetlen hang.

ez a mai világnak tűnik. Az is — csak az ellenőrök most sokan vannak. nincs forradalom. csak jobb ösztönzők.

Az állampolgárságod nem állami engedély. A közösséged elismerése.

az állami pecsétet független ellenőrök láncá váltja fel — mindegyiknek van veszténivalója.

Egy választási szavazat súlya az állam hatáskörébe tartozó ügyekben a jövőben szigorúan korrelálhatna az egyszerű adórendszerhez való hozzájárulások bejegyzéseivel. Megfelelő DID-állításokkal kombinálva (például „ez a személy cseh állampolgár”) a külföldi állampolgárok ekkor kizárhatók a választásokból — a lakónyilvántartás egyszerűen ide költözik.

Átfedés és visszafordíthatóság

Nem állítom, hogy ez az egyetlen út, vagy akár a legjobb. De átfogónak tűnik — lefedi a fő karokat, és megőrzi a visszalépés lehetőségét. A kezdetkor az új rendszer átfed a régivel, és csak az ösztönzőket változtatja meg. Idővel a régi rendszer zsugorodik, amíg — de nem szükségszerűen — fel nem oldódik. Az előny a fokozatosság és a visszafordíthatóság: ha hiba jelenik meg a tervben, az nem a vég, csak egy korrekció.

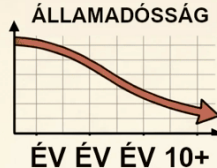
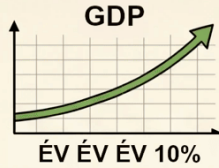
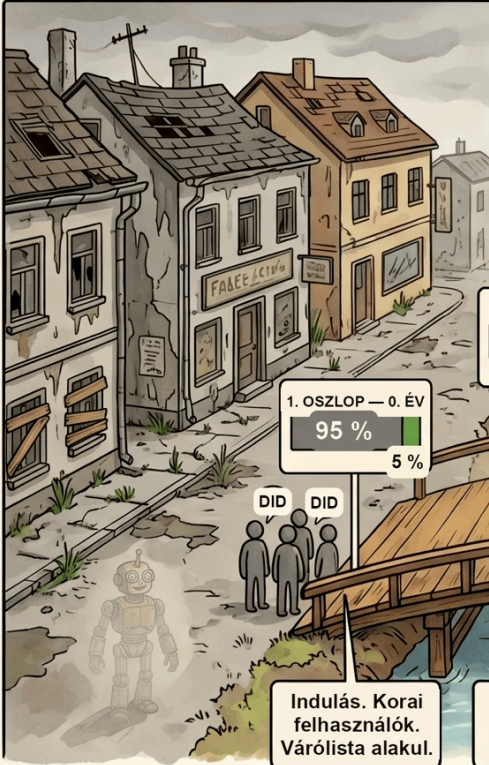
Béke és háború

Az állam bizonyos részeinek talán nincs teljesen piaci alapú alternatívája — például a hadseregnek. A rendkívüli hatáskörök átmeneti delegálása válságokban (ahogy az ókori görögök diktátorokat neveztek ki) továbbra is létezhet. A felelősség azonban a decentralizált társadalmon nyugszik, nem a vezetőn. A centralizált kormányzással ellentétben könnyebb lesz visszavenni a delegált hatásköröket, ha a fenyegetés elmúlt — vagy hamarabb, ha szükséges. Egy szabad társadalom a fegyveres összecsapásban sem lesz hátrányban a tekintélyelvű rezsimekkel szemben.

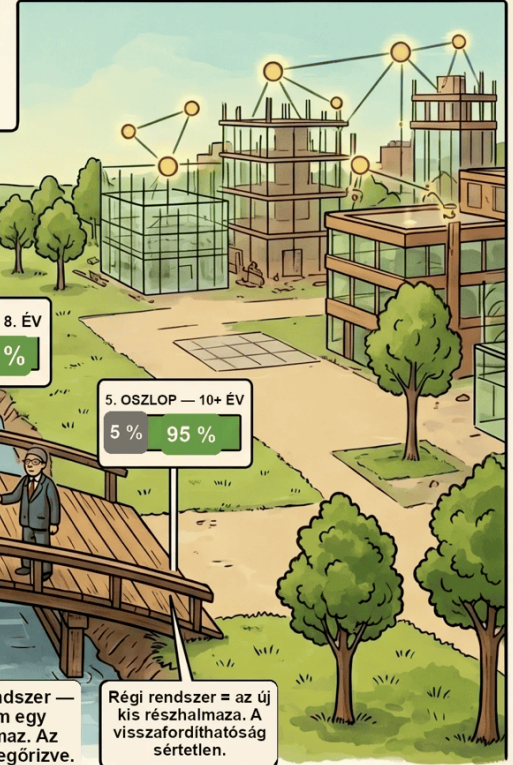
Háborús bűnösök

A just-in-time állami finanszírozással és az átlátható kiadásokkal nehezzé válik erőforrásokat felhalmozni agresszív háborúkhöz. Egy adófizető, aki továbbra is egy ilyen háborút finanszíroz, legitim célponttá válik, és nem hivatkozhat civil státuszra a genfi egyezmények szerint. Az új elrendezésben a hallgatólagos beleegyezés részvételnek számít.

BAL PART — 'A RÉGI RENDSZER'



JOBB PART — 'AZ ÚJ RENDSZER'



1. OSZLOP — 0. ÉV
95 % 5 %

2. OSZLOP — 2. ÉV
80 % 20 %

3. OSZLOP — 5. ÉV
50 % 50 %

4. OSZLOP — 8. ÉV
25 % 75 %

5. OSZLOP — 10+ ÉV
5 % 95 %

KRITIKUS TÖMEG — AZ ÁLLAM
GAZDASÁGI NYOMÁS ALATT
ELFOGADJA AZ ESR-T.

VISSZAFELE

Indulás. Korai
felhasználók.
Várólista alakul.

Növekedés.
A résztvevők
listája
duzzad.

Tervezési hiba?
Visszamehetünk. A
visszafordíthatóság
megőrizve.

75% új rendszer —
az állam egy
részhalmaza. Az
átfedés megőrizve.

Régi rendszer = az új
kis részhalmaza. A
visszafordíthatóság
sértetlen.

RÉGI
RENDSZER

> Fokozatos átmenet. Visszafordíthatóság hiba esetén. Egy irány, amit nem lehet megállítani.

Zárszó

Az út létezik

Az állam olyan, amilyen, a létrejöttékor rendelkezésre álló technológiák és az emberi természet együttese miatt. Mindent az önkéntességre építeni, miközben tagadjuk az átlagos emberi természetet, naivitás. Az állam nem fog megszabadulni sem a korrupciótól, sem attól a hajlamától, hogy a totalitarizmus felé sodródjon. Az állam utódjának azokkal a vonásokkal is működnie kell, amelyeket jelenleg negatívnak tartunk, és vagy kiközösítünk, vagy megbüntetünk.

Ez a könyv egy problémát írt le — egy rendszert (az államot), amelyben azok, akik a szabályokat írják, sosem élnek a következményeikkel. Leírta azokat a feltételeket, amelyeknek teljesülniük kell ahhoz, hogy ez a rendszer megszűnjön működni. Leírt egy eszközt, amely megfelel ezeknek a feltételeknek. És javasolt egy átmeneti módszertant — konkrét lépéseket arra, hogyan használjuk ezt az eszközt, egy lehetséges példaként.

Az első fejezetben öt pillért neveztem meg: önkéntesség, szerveződés, ellenállóképesség, konszenzus és korrumpálhatatlanság. Mindegyiket kielégítettük.

- **Önkéntesség** — senki sem kényszerít a hálózatba, de a tetteidet sem tudod kitörölni belőle.
- **Szerveződés** — a közösség abból nő, akit ismersz, nem abból, akit felülről melléd rendelték.
- **Ellenállóképesség** — még egy olyan állam sem tudja kikapcsolni, amely hajlandó fizetni minden csomag megfigyeléséért.
- **Konszenzus** — a képmutatás árcédulájából fakad, nem szavazatokból vagy aláírásokból.

- **Korrumpálhatatlanság** — öt kis szabály szövi a korrupciót költségge: az önkéntesség és a felelősség egyensúlya, bárki joga a megszólaláshoz, a belépési pontok, amelyeket senki nem választhat meg, a nyilvános ígérek a kápmutatás árával, és egy megfigyelő árnyéka minden tranzakció mögött.

Egyetlen pillér sem képes önmagában felváltani az államot. Együtt olyan ellenállást alkotnak a korrupcióval szemben, amelyet az állam a teljes apparátusával sem tud.

Ott tartunk, ahol az egészet fel lehet építeni a jelenkori technológiákkal (kriptográfia, decentralizált identitás, jól ismert pszichológiai minták az ösztönzők helyes beállításához, ...). Csak egyetlen dolog hiányzik: emberek kritikus tömege, akik veszik a bátorságot a támogatásához, és eldöntik, hogy belefognak.

Nem forradalom útján.

Ezek az ötletek 2025 júniusa és 2026 májusa között formálódtak. Mire leültem írni, a keretet nagyrészt kidolgoztam a fejemben — épp ezért olvastam a [Farewell To Westphalia](#) című könyvet olyan kíváncsian, amikor megjelent. Látni akartam, hol fed át az ő képük az enyémmel, és hol tér el tőle. Egy második lökés Dan Steigerwaldtól jött, aki 2026 májusában még mindig a saját, *Az állam dekonstrukciója* című könyvén dolgozik egy másik szögből; az ő projektje ösztönzött arra, hogy a saját víziómat teljes szélességében leírjam — hogy a világnak a többi mellett az enyém is az asztalán legyen.

Nem kérem, hogy bármit is elhiggy ebből. Azt kérem, hogy gondolkodj el rajta. És egy kérdéssel búcsúszom tőled:

Te mit változtatnál?

Pavel Kudrna 2026. május 23., Prága, Csehország

Köszönetnyilvánítás

Inspiráció

Köszönöm a [Farewell to Westphalia](#) szerzőinek (Jarrad Hope, Peter Ludlow) azt a szellemi keretet, amely segített a saját ötleteimet az állam vesztfáliai modelljének dekonstrukciója tágabb kontextusába helyezni.

Recenzió és visszajelzés

Eszközök

A szöveg előkészítésében, az ötletek strukturálásában és a megfogalmazások csiszolásában MI-eszközök segítségét vettem igénybe. Minden ötlet, érv és következtetés a sajátom — az MI a finomítás eszközeként szolgált, nem tartalmi társszerzőként.

Az infografikák generatív eszközökkel együttműködésben, a szerző specifikációi alapján készültek.

VEDD VISSZA AZ IDŐDET

a polgárok kiűzik az élősködőket a közéletből.



Védd meg az időt, amit ellopnának. amit csalással vettek el, azt kézzel veszik vissza.

Támogasd a projektet

A Personixet a hozzád hasonló olvasók finanszírozzák.



Bitcoin on-chain

bc1q7cctdz6r026dgy06u194eygg49ujtxnrq5czaj



Bitcoin Lightning

LNURL1DP68GURN8GHJ7AMPD3KX2AR0VEEKZ
AR0WD5XJTNRDAKJ7TNHV4KXCTTTDEHHWM30
D3H82UNVWQHXXMNP0FA8JMTVPD5XJMN9XUE
RX55QRQK

Hová megy ez a pénz — és hová nem

A QR-kódok a **szerző személyes csatornái** — a hozzájárulások közvetlenül Pavel Kudrnához kerülnek, és a további írást, a társadalmi kísérletet / szimulációt és a nyilvánosság elérését finanszírozzák.

A projekt *egyetlen* legitim adománygyűjtő csatornái a következők:

- **A könyv szerző által engedélyezett kiadásai** — QR-kódok a szerző által engedélyezett példányokban.
- personix.org vagy az onnan hivatkozott Tor onion-tükör — ahol a *Personix Foundation* gyűjt az ott leírt tevékenységekre. Az alapítvány pénzeszközeit elkülönítve kezelik a szerző személyes pénzeszközeitől.

Minden, amit máshol hirdetnek — kicserélt címek utánnyomásokban, hasonló megjelenésű domaineik, közösségi média, amely „a Personixnek gyűjt”, a fentiek egyikéhez sem kötődő adománygyűjtések — **nagy valószínűséggel csalás**. Tudatosan kerüljük a kriptovaluta-piacot és annak résztvevőit.

Fogalomtár

Fogalomtár

Fogalom	Magyar	Jelentés
Authority	Autoritás	Megbízható entitás (személy, szervezet), amely információt ellenőriz, és a reputációját teszi rá. Lehet specializált (nyomozói, jogi, technikai).
Claim	Állítás	Általánosan: bármely ellenőrizhető kijelentés. Itt: a reputációs hálózatba közzétett bejegyzés — egy eseményről, tulajdonságról vagy kapcsolatról szóló állítás, amely kriptográfiailag aláírt és ellenőrzött. Pl. „X település lakosa vagyok” vagy „ez a személy szerződést szegett”.

Fogalom	Magyar	Jelentés
Compartmentalization	Kompartmentalizáció	Általánosan: az információ elszigetelt egységekre való szétválasztása, hogy az egyik egység lelepleződése ne veszélyeztesse a többit. A titkosszolgálatoktól ismert elv. Itt: párhuzamos DID-identitások a diktatúrákban — az egyik lelepleződése nem fedi fel a többit.
Consistent Hash Ring	Konzisztens hash-gyűrű	Algoritmikus mechanizmus az ellenőrzők kiválasztására — a gyűrűn elfoglalt pozíciót a DID-dokumentum hashe határozza meg a közösségi gráfon belül. Nemdeterminisztikus, mégis ellenőrizhető kiválasztást biztosít.
DID	DID (Decentralizált identitás)	Digitális identitás, amelyet magad hozol létre és irányítasz, központi hatóság nélkül. Kriptográfiailag a privát kulcsoddal aláírva — senki sem tudja visszavonni vagy meghamisítani.

Fogalom	Magyar	Jelentés
DID Document	DID-dokumentum	Nyilvánosan elérhető adatfájl, amely a DID-identitásodat írja le — nyilvános kulcsokat, hálózati címeket és metaadatokat tartalmaz. Az identitásod hálózatbeli ellenőrzésére szolgál.
Due Diligence	Due diligence	Általánosan: egy ellenfél alapos ellenőrzése, mielőtt üzleti vagy jogi kapcsolatba lépnénk vele — a története, pénzügyei, reputációja és kockázatai átvizsgálása. Itt: a reputációs hálózatban gyorsabban és automatikusabban történik az ellenőrzött bejegyzések elérhetőségének köszönhetően.
Economic Neutrality Principle	A gazdasági semlegesség elve	A becsületes viselkedés a hálózatban gazdaságilag közel nulla — a közzététel költségei ellenőrzési jutalomként térülnek meg. A becsstelen viselkedés tiszta veszteség.

Fogalom	Magyar	Jelentés
Emergent	Emergens	Egyszerűbb részek interakcióiból spontán módon keletkező, anélkül, hogy bárki megtervezné vagy irányítaná. Egy madárraj terv nélkül repül alakzatban — az alakzat az egyes madarak által követett egyszerű szabályokból bontakozik ki.
Emergent Social Contract	Emergens társadalmi szerződés	Viselkedési szabályok, amelyek nem felülről (törvényből), hanem alulról keletkeznek — egy közösségen belüli ismételt interakciókból és konszenzusból.
ESR	Elektronikus kiadásnyilvántartás	Javasolt rendszer a közkiadások átlátható követésére — az állam minden realizált kiadását összevetik egy tervezett fizetéssel. A cseh EET ihlette, de az állam ellen fordítva.

Fogalom	Magyar	Jelentés
Hash	Hash (ujjlenyomat)	Általánosan: egyirányú matematikai függvény, amely bármely bemenetből egyedi, fix hosszúságú „ujjlenyomatot” állít elő — mint a dokumentum ujjenyomata. Ugyanaz a bemenet mindig ugyanazt a kimenetet adja, de a bemenet nem vezethető le a kimenetből. Itt: a hash-gyűrűn elfoglalt pozíció meghatározására és a dokumentum sértetlenségének ellenőrzésére szolgál.
Just-in-Time Funding	Just-in-time finanszírozás	Átláthatóságtól függő állami finanszírozás — a pénz csak akkor folyik, amikor az állam elfogadja az ESR-t és összeveti a kiadásait. Kar az együttműködés kikényszerítésére.

Fogalom	Magyar	Jelentés
Meritocracy	Meritokrácia	Általánosan: olyan rendszer, ahol a rangot a tényleges érdem és a bizonyított képesség határozza meg, nem a formális címek, kapcsolatok vagy örökölt kiváltság. Itt: a reputációs hálózat természetesen azokat részesíti előnyben, akik bizonyíthatóan hozzájárulnak a közösséghez — a hangjuk a track record, nem a hivatal miatt bír nagyobb súllyal.
Onion Gateway	Onion gateway	Egy DID-identitás hálózati címe az onion-hálózaton. Elkülönül a DID-dokumentumtól — megváltoztatható az identitás elvesztése nélkül (hasonlóan ahhoz, mint amikor egy domain mögötti IP-címet változtatunk).

Fogalom	Magyar	Jelentés
Onion Routing	Onion routing (Tor)	Kommunikációs protokoll, amely biztosítja a hálózat cenzúrázhatatlanságát. Az üzeneteket rétegekben titkosítja — minden csomópont egy réteget fejt le, de nem ismeri a teljes útvonalat.
Oracle Problem	Oracle-probléma	Általánosan: hogyan biztosítható, hogy egy digitális rendszerbe belépő adatok hűen megfeleljenek annak, ami valójában történt a fizikai világban. A kifejezés a blockchain területéről ered. Itt: autoritásokon keresztül megoldva, akik a reputációjukat teszik garanciaként arra, hogy egy digitális bejegyzés megfelel a fizikai valóságnak.

Fogalom	Magyar	Jelentés
Phenomenological	Fenomenológiai	Általánosan: olyan megközelítés, amely a jelenségeket úgy vizsgálja, ahogyan a közvetlen tapasztalatban megnyilvánulnak, azt figyelve, mi következik belőlük, előzetesen adott elméletek nélkül. Itt: a szabadság, a társadalmi szerződés és a viselkedési normák megfigyelt jelenségek — az emberek közötti több ezer mikrointerakció következményei, nem felülről definiált elvek.
Policy	Policy (elvek)	Általánosan: egy adott kontextusban a viselkedést szabályozó szabályok vagy elvek halmaza. Itt: a DID-hálózat minden résztvevője deklarálja a policyját — hogyan reagál mások konkrét viselkedésére, mely szabályokat követi, és mely büntetéseket tart arányosnak. A policyk összessége alkotja az emergens társadalmi szerződést.

Fogalom	Magyar	Jelentés
Proxy	Proxy	Általánosan: helyettes vagy közvetítő — egy másik nevében eljáró rendszer vagy entitás. Itt két kontextusban használatos: (1) az ESR mint proxy, amely a közkiadásokat összeveti a tervezett fizetésekkel; (2) a megfigyelők mint proxy a közzétevő és az ellenőrző között a megfigyelő-trükkben.
Publisher	Közzétevő	Hálózati résztvevő, aki bejegyzést hoz létre és tesz közzé (állítás egy igazságtalanságról, orvoslásról stb.). Ő viseli a közzététel költségét.
Reputation-Based Social Network (RSN)	Reputációs hálózat	Decentralizált közösségi hálózat, amelyben a résztvevők a valós viselkedésről cserélnek visszajelzést. A bejegyzések létrehozása költséges, olvasásuk olcsó.

Fogalom	Magyar	Jelentés
Reputation Signal	Reputációs jel	Egyedi bejegyzés a hálózatban — pozitív (kár orvoslása, kötelezettség teljesítése) vagy negatív (igazságtalanság, szerződésszegés). A jelek összeadódva reputációs profilt alkotnak.
Social Graph	Közösségi gráf	A kapcsolataid és a kapcsolataid kapcsolatainak hálózata. Az algoritmus egy konfigurálható mélységen (például 3 szinten) belül keres ellenőrzőket. Nincs globális blockchain — a hálózat természetesen közösségeket formál átfedésekkel.
Tax Allocation	Adóallokáció	Mechanizmus, amelyben az adófizető dönti el, hová megy az adója egy része. Az allokálható százalék évről évre nő.

Fogalom	Magyar	Jelentés
Track Record	Track record	Általánosan: egy személy vagy szervezet múltbeli eredményeinek, sikereinek és kudarcainak története. Itt: egy adott DID-identitás összes múltbeli interakciója a hálózatban — ellenőrzött állítások, elfogadott és elutasított bejegyzések —, amelyekből a reputációja levezethető.
Verifier	Ellenőrző	Algoritmikusan kiválasztott résztvevő, aki egy bejegyzést ellenőriz és közzétesz. A jó nevét teszi az információ igazságára.

Gyártási megjegyzések

A szerző által fenntartva (a CC BY-SA licenc nem terjed ki rá): a Personix név és szómárka, a könyvborító, valamint a támogatási csatornák (QR-kódok, címek, kapcsolattartó e-mail). A származékos kiadásoknak el kell távolítaniuk vagy le kell cserélniük ezeket az elemeket; kizárólag ennek az eredeti műnek a hivatkozására használhatók.

Forrásfájlok. A teljes forrás — markdown szöveg, infografikák, build szkriptek — a PDF mellett elérhető.

Eszközök. A szöveg előkészítése és a megfogalmazások csiszolása során a szerző MI-eszközök segítségét vette igénybe; az infografikák generatív eszközökkel együttműködésben, a szerző specifikációi alapján készültek. Minden ötlet, érv és következtetés a szerző sajátja.

PERSONIX

Megalkuvás nélküli változás

Cenzúrázhatatlan és korrumpálhatatlan decentralizált reputációs hálózat

Az állam akkor működött, amikor a kommunikáció lassú volt, a döntések lokálisak, és az autoritás ugyanabban a városban élt, amelyet kormányzott. A mai hálózatok mindhárom feltevést megfordítják — és a rájuk épült intézmények már nem illeszkednek a világhoz, amelyet kormányoznak. Ez a könyv egy olyan eszközt ír le, amely illeszkedik: egy decentralizált reputációs hálózatot, amelyben az identitás a tiéd marad, az igazság nyilvánosan auditálható, és a megvesztegetés reputációs öngyilkosság.

Nem kiáltvány. Nem jóslat. Működő tervrajz arról, hogyan lehet felépíteni az állam utódját — önként, egyszerre egy deklarációval.

Pavel Kudrna • Prága, 2026

personix.org

Licenc: Creative Commons Attribution-ShareAlike 4.0 International (CC BY-SA 4.0).