

PERSONIX

spiegels van het
reputatienetwerk
onthullen zelfs
de opgepoetste
ellende van
binnen.

Een Oncensureerbaar en Onomkoopbaar Gedecentraliseerd Reputatienetwerk
een evolutionaire opvolger van de staat

Personix — Compromisloze verandering

Een oncensureerbaar en onomkoopbaar gedecentraliseerd reputatienetwerk

© 2025–2026 Pavel Kudrna, Praag

Versie 6 (2026-05-21)

Eerste ontwerp juni–november 2025; herschreven april–mei 2026.

Gezet in $\text{\LaTeX}$ (Tectonic) met Palatino en Helvetica Neue.

A5 liggend (210×148 mm).

Gelicentieerd onder **Creative Commons Attribution-ShareAlike 4.0 International (CC BY-SA 4.0)** — creativecommons.org/licenses/by-sa/4.0/. De gereserveerde elementen, de bronrepository en een noot over de productiehulpmiddelen staan achterin het boek.

Contents

Inleiding	7
Waar gaat dit boek over?	9
Wezenlijke voorwaarden voor verandering	17
Wezenlijke voorwaarden voor verandering	17
Het instrument	28
Sociaal netwerk op basis van reputatie	28
Waarom het netwerk oncenureerbaar is	54
Voor de hand liggende twijfels wegnemen	56
Afhankelijkheid van technologie	56
Gooi ik geld uit het raam door in het netwerk te publiceren?	58
Wat als iemand meerdere identiteiten aanmaakt?	58
Kan een rijk persoon niet gewoon meer identiteiten “kopen” (of virtuele gemeenschappen aanmaken)?	61
En de meelifters die alleen willen lezen en niets aan de gemeenschap geven?	64
Financiële neutraliteit	65

Vrijwilligheid, verantwoordelijkheid en vrijheid	67
De schakelaar tussen vrijheid en totalitarisme (en delegatie)	68
Het orakelprobleem — een brug tussen de digitale en de fysieke wereld	76
Hoe verificatie werkt	78
Consensus en het verificatieproces	78
Roles in the verification transaction and authorities	85
Overzicht van de rollen	85
Uitgever	87
Autoriteit	89
Verificateur	92
Subject	94
Waarnemer	97
Het mechanisme: tijdstempel en uitdagingscode	97
De clou: je hebt geen echte waarnemers nodig	99
Delegatie	99
Communicatie tussen rollen	106
Het emergente maatschappelijk contract — beleid	106
Informatie over jezelf verstrekken	110

Misdaad en straf	112
Misdaad en straf	112
Volg het geld	124
Volg het spoor van het geld	124
Het zwakke punt van de staat — geld	125
Proposed transition to the state's successor	126
Evolutie, geen revolutie	126
Vier instrumenten die elkaar ondersteunen	129
Eenvoudig belastingsysteem — het lokaas voor toetreding	130
Elektronisch uitgavenregister (ESR)	130
Burgerbelastingtoewijzing — het gewicht van de beslissing	132
Onderhandelingsplatform met de staat — de hefboom	136
Burgerschap zonder identiteitskaart	138
Overlap en omkeerbaarheid	142
Conclusie	145
Het pad bestaat	145
Dankwoord	147
Inspiratie	147

Review en feedback 147

Hulpmiddelen 147

Woordenlijst **150**

Woordenlijst 150

Inleiding

Heb je het gevoel dat je op de staat kunt vertrouwen?

Ik weiger het te accepteren wanneer mij, mijn gezin of iemand in mijn gemeenschap een overduidelijk onrecht wordt aangedaan (lichamelijk letsel, oplichting, onterechte beperking, ...) en de staat antwoordt: ja, het is onrecht, maar onderneem er niets tegen, anders krijg je met ons een nog groter probleem. Zo'n toestand is ziek, en mensen die eraan meedoen zijn medeplichtigen.

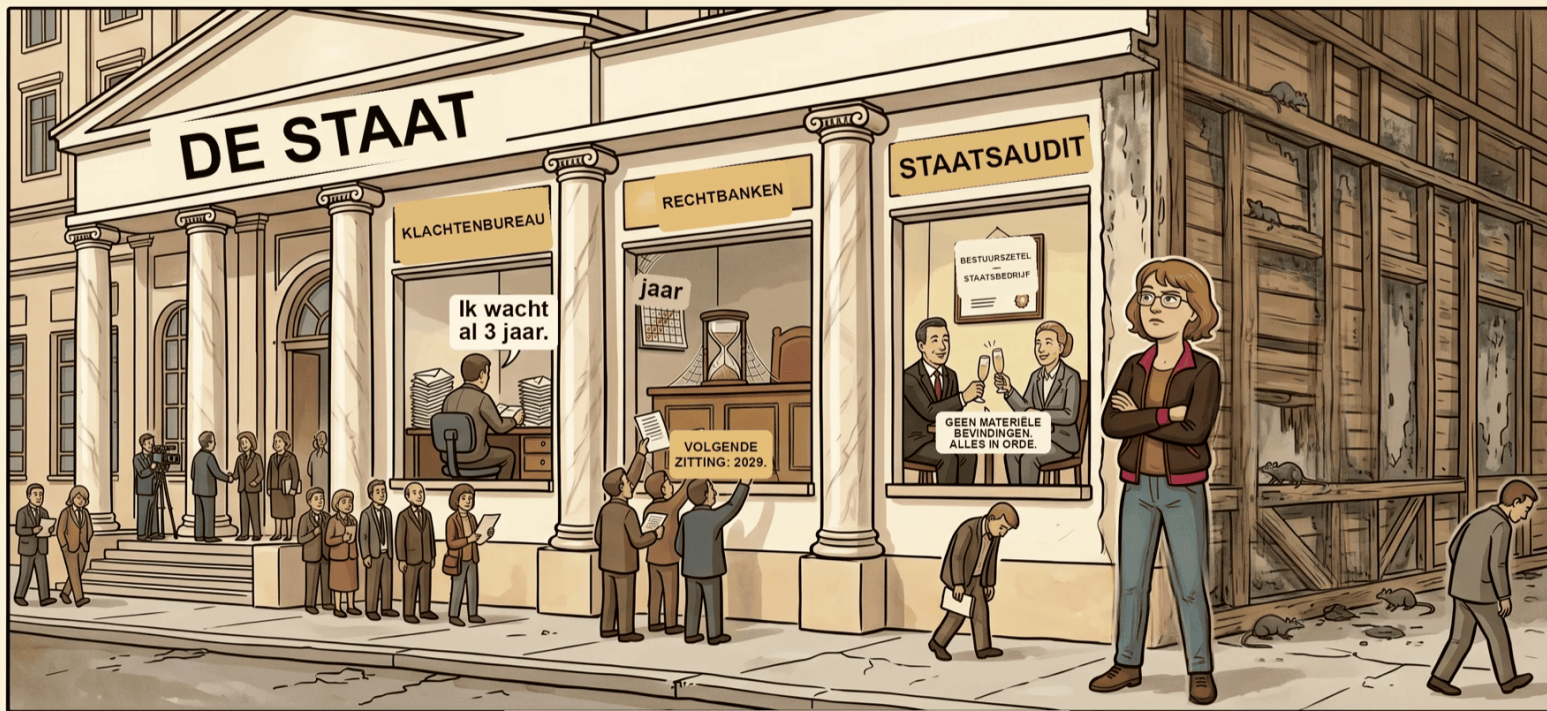
Het resultaat is wederzijdse vervreemding, spelen dat we een gemeenschap zijn, spelen dat we een staat zijn, en een verdiepende ontbinding van de samenleving met de belofte van ernstige conflicten in het verschiet.

Kan de staat het tempo van technologische en maatschappelijke verandering bijhouden, of geeft hij de voorkeur aan een verbod?

Ik zou kunnen doen alsof ik stagnatie, incompetentie en corruptie zal behandelen als de verklaarde stabiliteit van de rechtsstaat en de traditie, maar dat wil ik niet langer. Ik zou tegen mezelf liegen en ik zou tegen jou liegen.

Voel je de neerbuigendheid van ambtenaren en gekozen vertegenwoordigers wanneer je het waagt iets te bekritisieren waarvoor je betaalt?

Ik weiger mensen in de samenleving als onwaardig te beschouwen om maatschappijbrede regels vorm te geven, alleen omdat ze niet uitblinken in de soft skills die vandaag de dag de enige toereikende voorwaarde zijn om gekozen vertegenwoordiger te worden in door de staat gecodificeerde instellingen. Ik heb er vertrouwen in dat de overgrote meerderheid voor zichzelf, hun naasten en hun gemeenschap



Ik weiger het te accepteren.

kan zorgen — en dat zij daarin een stuk van hun levensfilosofie zien. De meeste mensen die ik om me heen heb leren kennen, zijn zo.

Maar ik heb ook regelrechte klootzakken ontmoet die klootzakken waren juist omdat ze het spel wisten te spelen — het spel waarin de gemeenschap hun geen feedback mag geven, waarin de staat hen beschermt zodat niemand de orde verstoort die het wezen van de staat zelf zou bedreigen: het waarborgen van een gemakkelijk leven voor wie op de bovenste verdiepingen van de machtshiërarchie en de hiërarchie van haar instellingen zitten. Het feodalisme is vervangen door de heerschappij van populisten en elitairen.

Vind je het heerlijk als anderen je vertellen hoe je je leven moet leiden?

Ik accepteer de huidige stand van zaken niet als een volmaakt, definitief gegeven. Ik moet verantwoordelijk zijn in hoe ik mij gedraag, en toch word ik kriegelig wanneer iemand mij vertelt welke juiste waarden ik zou moeten aanhangen. En jij?

Waar gaat dit boek over?

Stel je een sociaal reputatienetwerk voor waar iedereen die dat wil zijn eigen sleutels ervoor kan aanmaken (zijn identiteit kan aanmaken), zich kan laten uitnodigen door leden van zijn gemeenschap, of er op eigen houtje op af kan gaan. Je bouwt je reputatie op en put uit nuttige reputatiegegevens over anderen wanneer je die nodig hebt. Je zoekt de steun van je gemeenschap wanneer er onrecht gebeurt — je legt je zaak voor en levert aan wat je over de kwestie hebt, en de gemeenschap kijkt ernaar, beslist op grond van relevantie of ze het aan anderen doorgeeft, en hoe de overtreder wordt bestraft.

Dit hele korte boek gaat over wat er onder de motorkap moet zitten om dit aan de buitenkant zo eenvoudig te laten werken. Als je erbij blijft, beloof ik je dat een wereld die nu in veel opzichten complex

en moeilijk te begrijpen lijkt, zich zal openen als begrijpelijker en helderder. Je zult zien dat veel slechte dingen zo kunnen worden ingericht dat ze niet meer zo oneerlijk lonen voor de kwade actoren. En het is geen instrument waaraan je de hele tijd online gekluisterd zou moeten zitten — het volstaat ernaar te grijpen wanneer je voelt dat je het nodig hebt.

Ik beloof je verder dat de hier beschreven inrichting dichterbij zal aanvoelen bij de werkelijke drijfveren van mensen, en dat ze die niet hoeft om te vormen in naam van een of ander -isme.

En ten slotte zullen we laten zien hoe je een niet-revolutionaire overgang kunt beheersen naar een toestand waarin gemeenschappen weer volledig functionerende maatschappelijke eenheden worden en niet langer hoeven te doen alsof.

Technisch artikel

Dit boek is een verklarende begeleider bij het oorspronkelijke technische artikel *“Decentralized Reputation Network: A Framework for Voluntary and Uncorruptible Societal Organization”* (Pavel Kudirna, 2026). Als je geïnteresseerd bent in de formele beschrijving van de architectuur, het algoritme voor de selectie van verificateurs en de rechtvaardiging van de economische mechanismen, raad ik je aan daar te beginnen.

■ Hoofdstukken bouwen op elkaar voort

Het boek is geschreven als een doorlopend betoog — elk hoofdstuk bouwt voort op het vorige. Concepten die in het ene deel worden geïntroduceerd, worden in latere delen gebruikt, ook in voetnoten. Ik raad af om het door elkaar te lezen.

■ Voor wie is dit boek?

Ondanks het visueel toegankelijke formaat is het voornaamste doelpubliek de meer gespecialiseerde lezer die zich bezighoudt met de principes van mogelijke sociaal-economisch-politieke inrichtingen van de menselijke samenleving. Om zover te komen dat ik de hele materie toegankelijk kan uitleggen aan het breedst mogelijke publiek, ligt nog een lange weg van het uitbouwen van een volledige communicatiestrategie voor de boeg.

Ik verwelkom suggesties over hoe ik dit werkje, of eventuele herziene vervolgedities, begrijpelijker kan maken.

Waarschuwing

Ik weet niet wie je bent, hoe oud je bent, of hoeveel gebroken beloften je in je leven hebt moeten uitzitten. Ik ben er klaar mee om ze hier te doen. In plaats daarvan wil ik je waarschuwen dat de enige



Er zit meer onder de motorkap. Blijf bij me.

uitkomst van wat je hier leert wel eens het besef kan zijn dat er waarschijnlijk geen pad is waarop iemand anders de rotzooi van vandaag voor je opruimt. Ik beschrijf alleen een raamwerk/instrument dat de opruiming eenvoudiger en transparanter zou kunnen maken. Op basis daarvan zal ik proberen een maatschappelijk experiment/simulatie voor te bereiden, mogelijke gebreken te verhelpen, of het idee helemaal te begraven als blijkt dat het fundamentele ontwerpbarsten heeft.

Een verzoek

Ik zou het diep waarderen als je, ook na het lezen van dit boek, een open geest zou houden tegenover het idee en zou volgen waar het naartoe gaat en hoe het standhoudt onder inhoudelijke kritiek. Ik zou het nog meer waarderen als je je later betrokken zou tonen — door met eigen ideeën de voorgestelde evenwichtsprincipes te proberen breken, en zo beter te testen hoe voorbereid het systeem is op werkelijk menselijk gedrag.

Zonder jou en jouw betrokkenheid blijft het idee een theorie in een la. Zonder jou en jouw bijdragen en financiële donaties zullen we het project niet richting een echt maatschappelijk experiment kunnen duwen, en daarmee richting echte gereedheid. Zonder jou en jouw inhoudelijke kritiek zullen we blijven stagneren waar we nu zijn, of laten we ons opslokken door de heilige graal van de centristen — absoluut, onomkeerbaar totalitarisme. Het is aan ons welk pad we kiezen, of het uitzitten.

De uitdaging

We leggen niet bepaald een lichte last op je schouders. Je draagt al de kosten van een verkwistend bestuurd samenleving via occultistisch-bezwerende handleidingen die beweren dat de samenleving het best centraal wordt bestuurd — en ik heb het lef je om nog meer te vragen, en om tegen deze tendensen in te gaan. Ik ben me ervan bewust dat we de ineenstorting van het grootste piramidespel in de geschiedenis — het omslagstelsel voor pensioenen — zullen moeten doorstaan zonder meerdere generaties te laten verhongeren.



Een betere wereld is het gewicht waard.

Toch vraag ik het je alsnog: laten we onze kinderen eindelijk een betere wereld overhandigen en een nalatenschap achterlaten waarin we die verandering voor elkaar hebben gekregen. Het ontketenen van economische groei zou een gedeeltelijke oplossing kunnen zijn voor de benarde situatie aan de horizon. We kunnen onze nakomelingen dan vertellen dat het een hels avontuur was en dat het niet tevergeefs was.

Het probleem

Alleen vrijheid die in evenwicht wordt gehouden door directe verantwoordelijkheid kan werkelijk een enorm potentieel ontsluiten dat de wereld nog nooit heeft gezien.



Kom binnen. De plannen liggen klaar.

Wezenlijke voorwaarden voor verandering

Wezenlijke voorwaarden voor verandering

De fundamentele voorwaarde voor verandering ten goede is dat de ondergeschikte de bovengeschiede wordt — of ten minste een gelijkwaardige partner. Dat betekent dat je de meest kritieke agenda's overneemt die de verhouding van boven- en onderschikking bepalen. Deze agenda's berusten op bewijzen van het behoren tot de gemeenschappen die de burgers van de staat vormen. Het zijn informatie en de verifieerbaarheid ervan door een autoriteit met aanzienlijke reputatie binnen die gemeenschappen.

Om het huidige systeem te overwinnen, ben ik tot vijf voorwaarden gekomen, die ik vervolgens uitleg op de manier waarop ik ze begrijp. We kunnen ons deze voorwaarden voorstellen als de pijlers die de constructie dragen van het systeem dat in de rest van het boek wordt beschreven. De pijlers heb ik aanvankelijk naar eigen voorkeur gekozen en, terwijl ik ermee redeneerde, mijn begrip van elk ervan geleidelijk verfijnd tot de vorm hieronder.

Laten we deze vijf pijlers één voor één doorlopen.

VOORWAARDEN VOOR VERANDERING

VRIJWILLIGHEID



VRIJWILLIGHEID

Ik beslis
voor mezelf.

ORGANISATIE



ORGANISATIE

Samen, onder
niemand.

VEERKRACHT



VEERKRACHT

Kan niet
gecensureerd
worden.

CONSENSUS



CONSENSUS

Compromis
door druk.

ONOMKOOPBAARHEID



ONOMKOOPBAARHEID

Je kunt niet
iedereen
kopen.

Zonder deze vijf pijlers is elke verandering slechts verspilde tijd.

■ Vrijwilligheid

In ons geval betekent vrijwilligheid dat ik niet gedwongen word deel te nemen aan het draaien van het gedecentraliseerde reputatienetwerk. Ik kan echter geen positief geformuleerd recht opeisen dat het netwerk geen informatie over mij vastlegt — of informatie over mij in het reputatienetwerk belandt, hangt alleen van mij af, van mijn gedrag, mijn handelen en mijn verantwoordelijkheid.



Vrijwillig — tot de verantwoordelijkheid je inhaalt.

■ Organisatie

Een enkel individu kan het systeem niet breken, en daarom controleert de staat het verenigen van mensen als een manier om activiteiten te voorkomen die zijn structuur en werking zouden kunnen bedreigen. Het maakt niet uit of mensen zich vóór of tegen organiseren. Door organisatie is het mogelijk de klap van exemplarische straffen te verzachten wanneer iemand het waagt de staat tegen zijn wil te veranderen.

Laten we geen gezamenlijke doelen stellen, maar we kunnen een deel van de weg samen afleggen. De meest natuurlijke vorm is verenigen in gemeenschappen — maar die moeten over alle instrumenten beschikken die ze nodig hebben om niet louter toneelspel van gemeenschap te blijven.

■ Weerbaarheid

Het gekozen pad naar verandering van de staat — of naar de overgang naar zijn opvolger — mag niet afhangen van toestemming van de staat. De instrumenten en de manieren waarop ze worden gebruikt, moeten zo oncensureerbaar mogelijk zijn. Eenvoudig gezegd: de kosten om ze te censureren moeten astronomisch zijn. Zonder dat is de hele onderneming slechts tijd en levensenergie verbranden.

VOORWAARDE 2 VAN 5: ORGANISATIE

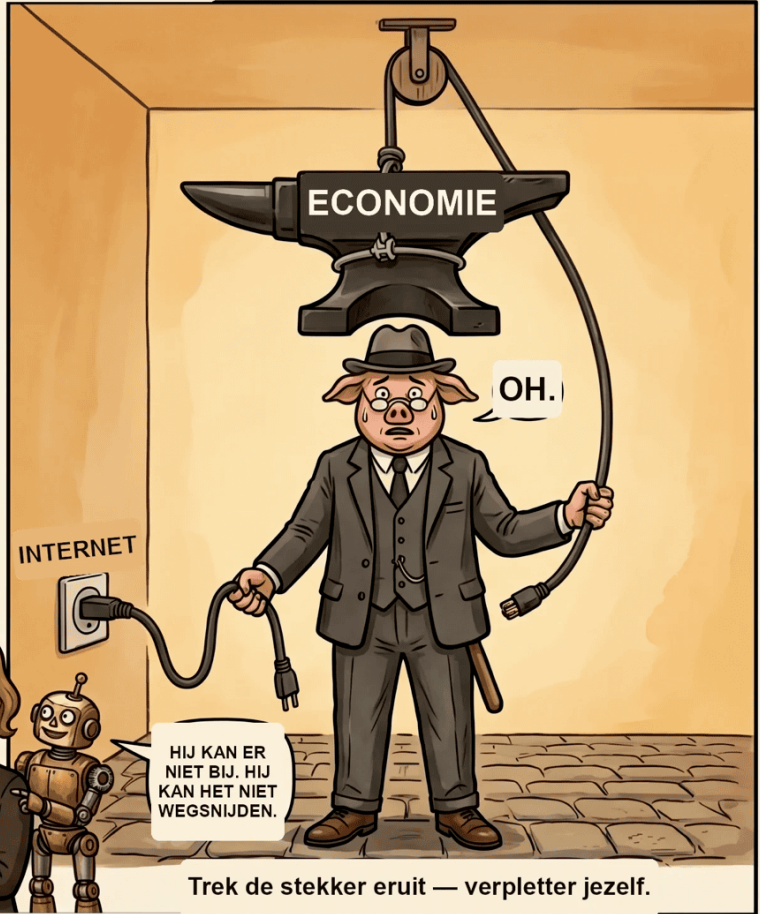


Een individu kan het systeem niet breken. Een gemeenschap wel.

VOORWAARDE 3 VAN 5: VEERKRACHT



Hij kan niet van buitenaf zoeken.



Trek de stekker eruit — verpletter jezelf.

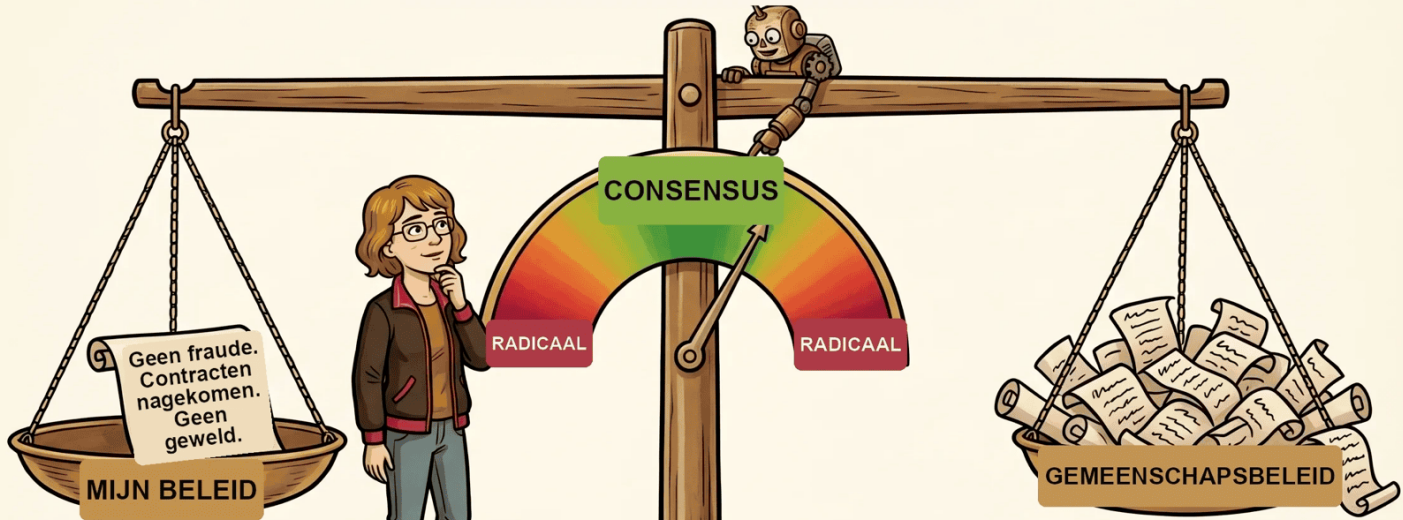
GEEN TOESTEMMING OM TE VRAGEN. GEEN STEKKER OM UIT TE TREKKEN.

■ Consensus

De voorgestelde oplossing moet, uit haar aard, een mechanisme bevatten om over consensus te onderhandelen, alsook een repressieve component voor gevallen waarin de consensus wordt geschonden. Het hoeft geen vrijwillige win-winovereenkomst te zijn. Het volstaat als omstandigheden en maatschappelijke druk voor compromis zorgen binnen een gemeenschap en tussen gemeenschappen.

BLIJF BINNEN BEREIK — GEEN RADICAAL.

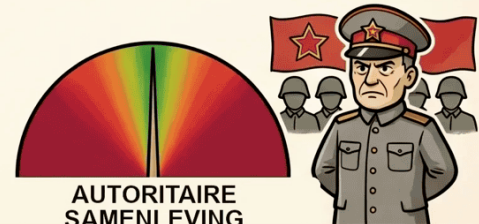
Je mag verschillen. Alleen niet te ver.



**VRIJE
SAMENLEVING**

De tolerantiezone rekt mee
met de vrijheid van de cultuur.

VOORWAARDE 4 VAN 5: CONSENSUS



**AUTORITAIRE
SAMENLEVING**

CONSENSUS IS EEN TOLERANTIEZONE, GEEN UNANIEME OVEREENSTEMMING.

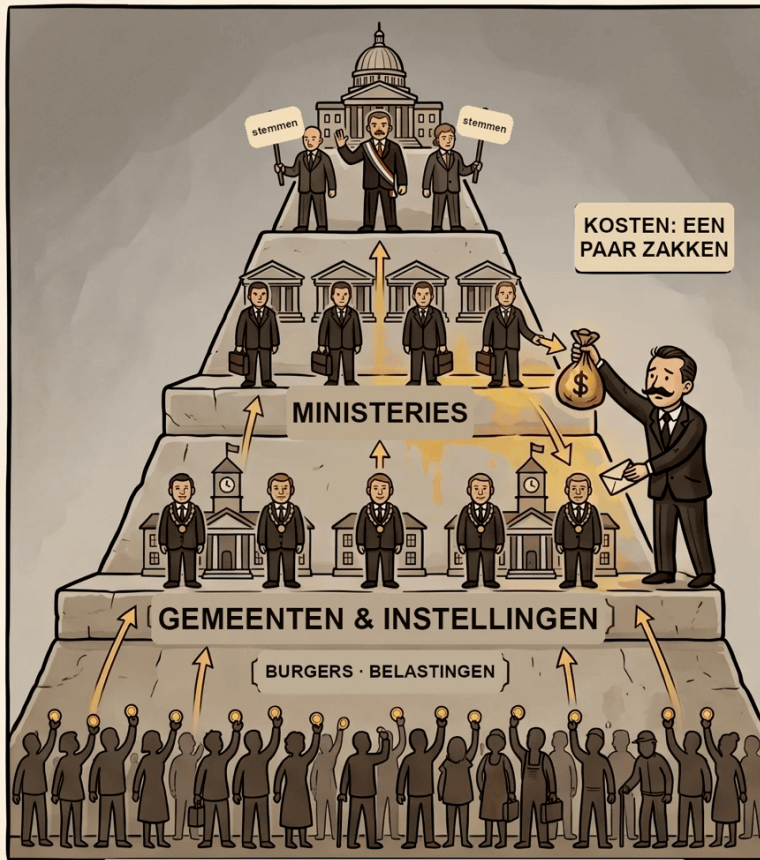
■ Onomkoopbaarheid

Oncensureerbaarheid verdedigt het systeem van buitenaf. Maar een netwerk van mensen kan ook van binnenuit rotten — een autoriteit wordt overgenomen, een verklaarde regel wordt stiller losgelaten, deelnemers worden in stilte afgekocht. Oncensureerbaarheid zou een holle overwinning zijn als de mensen van binnen zonder gevolgen konden worden gecorrumpeerd.

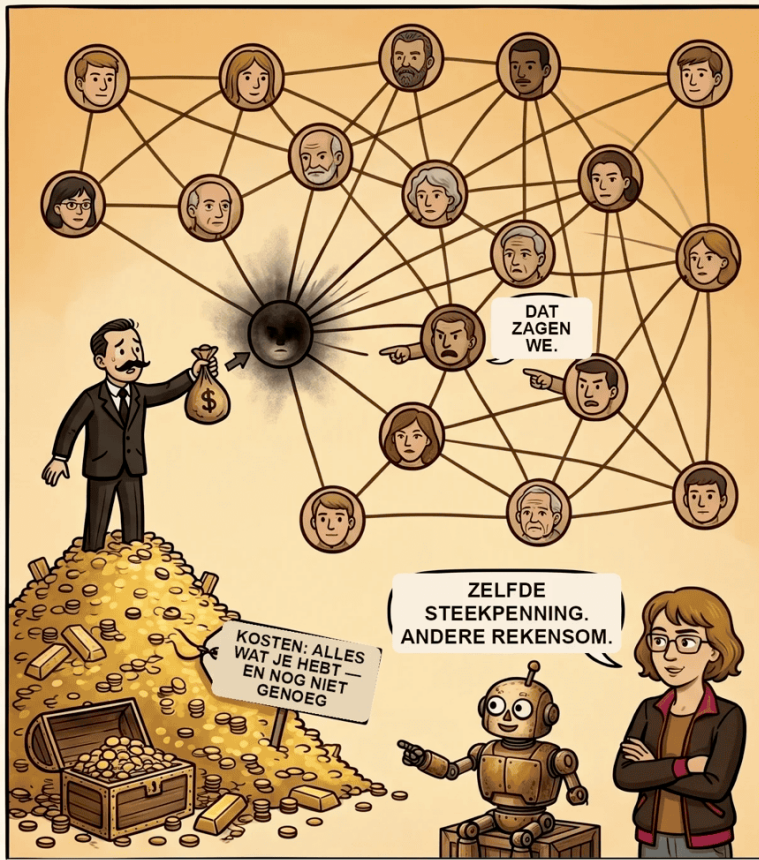
Onomkoopbaarheid is niet het resultaat van één slimme truc. Ze komt voort uit **verscheidene principes van het voorgestelde ontwerp die samenwerken** — de druk tegen corruptie is verdeeld over de architectuur, en de afzonderlijke delen versterken elkaar. Hoe dit precies wordt bereikt, laten we geleidelijk zien — in de beschrijving van het instrument, in de verificatie, en in het hoofdstuk over straf. Aan het eind vatten we alles samen wat is opgebouwd.

Onomkoopbaarheid is tegelijk een voorwaarde van het ontwerp en een emergente eigenschap van het resultaat. Ze is de tweede verdedigingslinie — die naar binnen gekeerd is — en zonder haar is Weerbaarheid slechts een half schild.

VOORWAARDE 5 VAN 5: ONOMKOOPBAARHEID



Koop een paar bovenste verdiepingen om — de basis betaalt toch.



Koop er één om — hij verliest zijn reputatie voorgoed. Koop iedereen om — jij gaat eerst failliet.

CORRUPTIE HEEFT EEN PRIJS. IN DE MESH IS DIE TE HOOG.

Het instrument

Sociaal netwerk op basis van reputatie

Om verandering tot stand te brengen hebben we een zorgvuldig ontworpen instrument nodig. Eerst schetsen we het kort; in latere hoofdstukken bekijken we elk onderdeel in meer detail en voegen we er meer aan toe. Stel je een oncenensureerbaar, globaal, gedecentraliseerd sociaal netwerk voor waarin je veilig je proxy-identiteit — een zogeheten Decentralized Identity (DID) — zou kunnen aanmaken en beheren. Een DID is een digitale identiteit die je zelf aanmaakt en beheert, zonder afhankelijkheid van enige centrale autoriteit. Niemand kan die afnemen of vervalsen, omdat ze cryptografisch is ondertekend met je privésleutel (of sleutels, via multisig).

JOUW IDENTITEIT, JOUW SLEUTELS, JOUW REGELS

JE MAAKT HET ZELF

PRIVÉSLEUTEL — tekent namens jou. Alleen jij hebt deze. Nooit delen.

PUBLIEKE SLEUTEL — verifieert jouw handtekeningen. Zichtbaar voor het netwerk.



JOUW DID-DOCUMENT



Dit is jouw publieke identiteit. Iedereen kan het lezen. Alleen JOUW privésleutel kan er wijzigingen op ondertekenen.

Geen staat kan dit intrekken.

CLAIMS — GEVERIFIEERDE FEITEN OVER JOU

BURGERSCHAP: Tsjechië — geverifieerd door Gemeentelijke Notaris

OPLEIDING: MSc Informatica — geverifieerd door Alumninetwerk Universiteit

EIGENDOM: Eigenaar van appartement #42 — geverifieerd door Lokaal Gemeenschapsregister

PASSIEVE GETUIGE: Negeerde een misstand — beleid niet nageleefd — ingediend door Buurtgetuigen

FRAUDE: Bedroog een buurman om zijn spaargeld — ingediend door Lokale Gemeenschapsrechtbank

Claims zijn geverifieerde verklaringen. Het goede en het slechte. Autoriteiten zetten hun reputatie erop in.



STAATS-ID — INTREKBAAR: de staat kan het altijd annuleren.



DID — ONHERROEPELIJK: alleen jouw privésleutel kan wijzigingen ondertekenen.

Jouw identiteit. Jouw sleutels. Jouw regels. Geen toestemming nodig.

Opmerking

Eén implicatie is dat zo'n identiteit geleidelijk de door de staat uitgegeven identiteitsdocumenten zou kunnen vervangen — maar daarover meer in het hoofdstuk over de overgang.

In zo'n netwerk zou je via je identiteit kunnen melden dat iemand je schade heeft berokkend (en later mogelijk dat hij die heeft hersteld of daartoe is gedwongen). Opdat deze feedback — gericht aan de veroorzaker van de schade — waarde heeft als relevante bron, moet het invoeren van informatie in het netwerk tijd, energie en geld kosten — en bovenop dat moet er verifieerbaar bewijs voor anderen worden geproduceerd dat dit geen loze praat is.

Informatie lezen zou gemakkelijk en relatief goedkoop zijn, maar het aanmaken van een individuele registratie zou kostbaar en veeleisend zijn. Schrijven zou een duidelijk protocol volgen, waarin berekening volgens het gekozen algoritme strikt bepaalt welke DID om verificatie van de ingediende informatie moet worden gevraagd en hoe te werk te gaan zodat de geselecteerde deelnemer de informatie namens jou verwerkt, publiceert, en er de verificateur van wordt.

■ Algoritme vs. radicalisme

Algoritmische selectie van verificateurs zorgt ervoor dat niet-radicalen informatie-uitgevers na verloop van tijd een bijna neutraal evenwicht behouden tussen de kosten van gepubliceerde informatie en de beloningen voor verificatie.

PUBLICEREN KOST TIJD, ENERGIE EN GELD

SCHRIJVEN NAAR HET NETWERK IS NOOIT GRATIS — LEZEN WEL

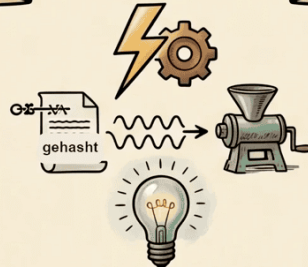
DRIE KANALEN — ALLE DRIE ZIJN ECHT

TIJD



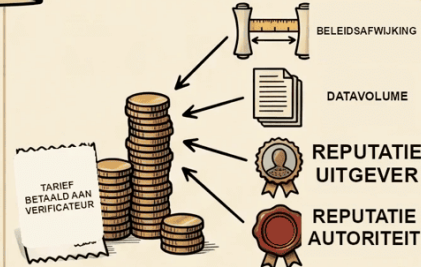
je wacht terwijl het algoritme een verificateur kiest en de verificateur je record leest.

ENERGIE



ondertekenen, hashen, verifiëren — elke stap is echte rekenkracht en echte elektriciteit.

GELD



hoe verder je claim van het beleid van de verificateur ligt, hoe groter het record, en hoe minder betrouwbaar de uitgever of zijn autoriteit — hoe hoger het tarief.

WAT ER DAARNA GEBEURT

De verificatieketen van drie stappen — zie HOE HET ALGORITME EEN VERIFICATEUR KIEST, HOE DE VERIFICATEUR ANTWOORDT, DE KEUZE VAN DE UITGEVER

Waarom duur schrijven reputatie beschermt — later in dit hoofdstuk

ruis is duur. Signaal is waardevol. Daarom (reken het netwerk voor) schrijven, niet voor lezen.

kosten over iteraties

ELKE NIEUWE POGING KOST MEER



elke afwijzing of nieuwe worp voegt toe aan de chronologie die het algoritme opslokt — en de volgende poging is duurder in alle drie de kanalen.

leesasymmetrie

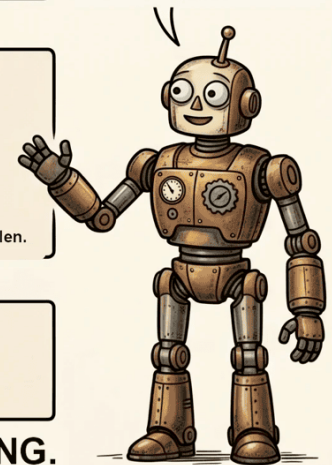
LEZEN IS GOEDKOOP



gratis te bevragen

iedereen mag reputatie en records lezen — alleen schrijven kost. De asymmetrie is het ontwerp.

SCHRIJVEN KOST — LEZEN NIET. DE ASYMMETRIE IS DE BEDOELING.



Laten we kijken hoe het algoritme een verificateur selecteert.

■ Algoritme

Algoritmische selectie kiest niet-deterministisch een andere verificateur (of een verzameling mogelijke verificateurs) voor verschillende stukjes informatie. Een hash (een eenrichtings-wiskundige functie die uit elke invoer een unieke “vingerafdruk” produceert — als een vingerafdruk van een document) van het volledige DID-document bepaalt de positie op een consistente hashring en selecteert kandidaat-verificateurs.

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

In gewone taal: het algoritme neemt je hele DID-document, berekent er een vingerafdruk van, en die vingerafdruk bepaalt je verificateur.

Bij de eerste verificateur die het algoritme selecteert, slaag je als uitgever mogelijk niet — je reputatie of je verklaarde instellingen voldoen wellicht niet aan hun eisen. Je zou algoritmisch verder zoeken naar de volgende door nog een recursieve iteratie uit te voeren, die je een verdere verificateur toewijst. Bij elke stap groeit de “afstand” tot de doelverificateur, en daarmee ook de bijkomende metadata die moet worden gepubliceerd. Naarmate de gegevens groeien, stijgen de kosten vanzelf (niet alleen door de aanvankelijke omvang van de claim, maar ook door de metadata die zich bij elke afwijzing opstapelen). Geloofwaardige informatie gaat er veel makkelijker doorheen dan onzinnige grillen. Het is aan ieder hoe hoge prijs hij bereid is te dragen en hoeveel de registratie hem waard is — radicalisme wordt gegarandeerd duur.

HOE HET ALGORITME EEN VERIFICATEUR KIEST

EEN EERLIJKE MUNT GEWORPEN OVER JOUW GEMEENSCHAP



HOE DE VERIFICATEUR ANTWOORDT

ACCEPTEREN MET EEN PRIJS — OF AFWIJZEN MET EEN REDEN

de verificateur weegt vier dingen af voordat hij antwoordt.

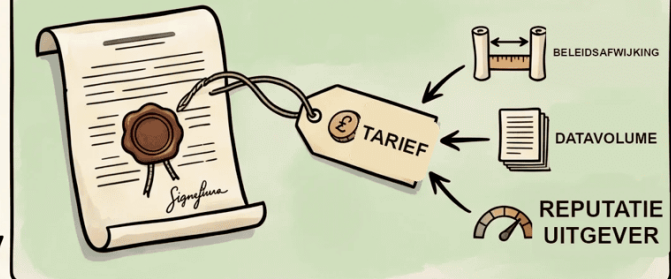


AFWIJZEN — MET EEN REDEN

- 
- de reputatie van de uitgever is te laag voor mij
 - de autoriteit achter dit record is er niet een die ik vertrouw
 - het beleid van de uitgever ligt te ver van het mijne om te overbruggen
 - het document zelf voldoet niet aan de regels van mijn beleid

de verificateur schrijft op **WAAROM** — hun respons voedt terug in de volgende poging.

ACCEPTEREN — MET EEN PRIJS



de verificateur stemt in met publiceren — maar de prijs weerspiegelt hoe ver de claim van hun beleid ligt, hoeveel data hij bevat, en hoe betrouwbaar de uitgever is.

de respons van de verificateur wordt toegevoegd aan de chronologische lijst — zoals getoond bij **HOE HET ALGORITME EEN VERIFICATEUR KIEST**

wat de verificateur ook zegt, hun antwoord wordt invoer voor de volgende aanroep.

elke verificateur antwoordt op een van deze twee manieren — accepteren met een prijs, of afwijzen met een reden.

WAT ER DAARNA GEBEURT

- De uitgever beslist wat hij met dit antwoord doet — zie **DE KEUZE VAN DE UITGEVER**
- Elk antwoord verschuift de kosten van de volgende poging — zoals eerder getoond bij **PUBLICATIEKOSTEN**

DE VERIFICATEUR STELT EEN PRIJS — OF VERTELT JE WAAROM NIET.

Wat de verificateur ook beslist in antwoord op je verificatieverzoek, de bal ligt weer bij de uitgever: hij kan het aanbod van de verificateur voor verificatiediensten aanvaarden, het antwoord in de chronologie opnemen en het (duurder) opnieuw proberen, of ermee stoppen en de verzonken kosten slikken.

Om je informatie meer gewicht te geven en een betere kans op aanvaarding bij verificateurs, zou je — als uitgever met een belang in het uit te geven bericht — de diensten van een **vertrouwde autoriteit** kunnen gebruiken. De autoriteit wijst de ingediende informatie ofwel af, ofwel aanvaardt ze die en zet er haar goede naam (reputatie) op in. De autoriteit vraagt doorgaans om bewijs uit de echte wereld, verifieert het en classificeert het. De output is een protocol van haar beoordeling van de gegeven zaak op het gegeven moment. Denk aan een autoriteit als een specialist in een bepaald type dienst in zowel de echte als de digitale wereld — bijvoorbeeld een onderzoeker, een auditor, een verzekeraar, een leverancier van een bepaalde klasse goederen (in wezen elke economische actor op de markt).

DE KEUZE VAN DE UITGEVER

WAT TE DOEN MET HET ANTWOORD VAN DE VERIFICATEUR

wat de verificateur ook zei, de uitgever heeft nu **ÉÉN** antwoord op tafel.



terug naar **HOE HET ALGORITME EEN VERIFICATEUR KIEST** — eerder getoond

alleen het pad van opnieuw proberen loopt in een lus — accepteren en weglopen beëindigen beide het verhaal.

DRIE UITWEGEN

NEEM DE DEAL

DID-netwerk



AL LEEN INDIEN
GEACCEPTEERD

de uitgever betaalt het tarief — het record wordt in het netwerk gepubliceerd. Alleen beschikbaar als de verificateur accepteerde.

PROBEER OPNIEUW



mini-maalmachine



elke nieuwe
poging kost
meer

de respons wordt gebundeld in de chronologie — het algoritme werpt opnieuw. Werkt of de verificateur nu accepteerde tegen een prijs die de uitgever niet bevalt, of ronduit afwees.

LOOP WEG



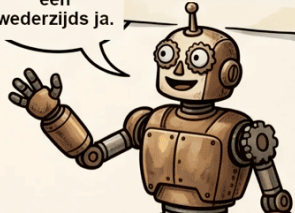
reeds bestede
tijd en energie
komen niet terug

de uitgever verworpt het concept. Er wordt niets gepubliceerd — maar er wordt ook niets meer betaald.

WAT ER DAARNA GEBEURT

de verificateur beslist hoe — de uitgever beslist of. Publiceren is een wederzijds ja.

Elke nieuwe poging verschuift de kosten van de volgende poging — zoals eerder getoond bij **PUBLICATIEKOSTEN**. Het antwoord van de verificateur zelf — zoals eerder getoond bij **HOE DE VERIFICATEUR ANTWOORDT**



DE VERIFICATEUR STELT VOOR — DE UITGEVER BESCHIKT.

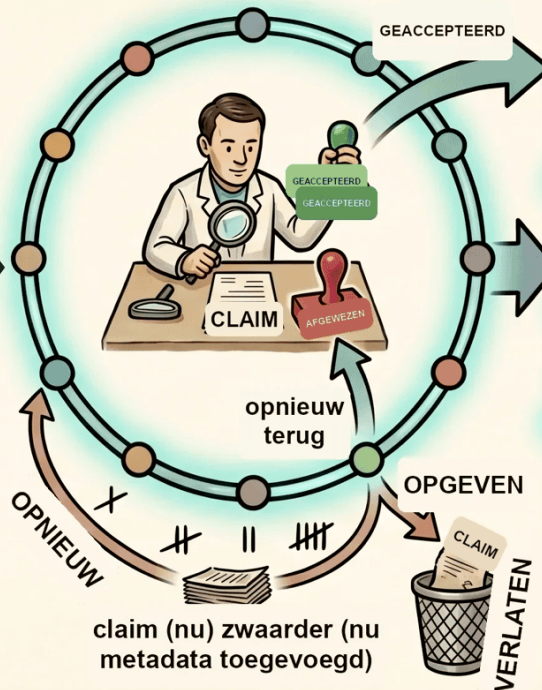
FASE 1 — PUBLICIEER EEN CLAIM



FASE 2 — KWALITEITSFILTER



FASE 3 — RECURSIEVE VERIFICATIE



FASE 4 — PERMANENTE REGISTRATIE



Permanent.
Verifieerbaar.
Publiek.

**DUUR OM TE VERVALSEN. GOEDKOOP OM TE
VERIFIËREN.**

Tegen de tijd dat je informatie in het netwerk probeert te publiceren, bevat het waarschijnlijk al informatie over zijn actoren — dat zijn reputatiesignalen. Uitvogelen hoe je reputatiesignalen moet lezen — wat ze in verschillende situaties voor jou betekenen en welke risico's ze dragen — is misschien niet triviaal. Elke deelnemer kan reputatieregistraties anders bekijken via zijn DID, afhankelijk van de situatie waarmee hij ten aanzien van de tegenpartij te maken heeft. Is de tegenpartij een betrouwbare betaler, of moet ik geld vooraf eisen voor een zakelijke transactie? Draagt het aangeboden product beoordelingen over verborgen fraude of gebreken? Proberen ze zich onder contractuele verantwoordelijkheid uit te wurmen wanneer er iets misgaat? Soms komt een complexere blik op de algehele consistentie van de tegenpartij van pas — het hangt af van de voorkeuren van wie het overzicht opvraagt. De markt zou producten en diensten kunnen aanbieden die het lezen van reputatie vereenvoudigen, verwerken en verhelderen in de context van de situatie die voorligt. Diverse autoriteiten en hun aangeboden diensten kunnen daar eveneens toe dienen.

HOE JE REPUTATIE LEEST

WELOVERWOGEN BESLISSING



Ze weet met wie ze te maken heeft.

BLIND VERTROUWEN



Hij heeft geen idee met wie hij te maken heeft.

VOORDAT JE KREDIET VERLEENT. VOORDAT JE TEKENT. VOORDAT JE VERTROUWT.

■ Voorbeelden

Typische informatie die van belang is voor uitgevers — en waardevol voor anderen — betreft gebeurtenissen voorbij de gewone tussenmenselijke communicatie in de echte of virtuele wereld.

Negatieve voorbeelden: - bewijs van strafbare feiten (bijv. geaudit door een vertrouwd onderzoeksorgaan) - indirect bewijs (op zichzelf zwak, maar statistisch cumulatief) — bijv. herhaalde aanwezigheid nabij meerdere diefstallen in korte tijd → nog steeds toeval? - contractbreuk

Positieve voorbeelden: - herstelde schade (vrijwillig of onder druk van de gemeenschap als straf) - aanvaarding en uitzitten van een door autoriteit X voorgestelde straf - autoriteit X heeft de erkenning van de eigendomsrechten van de dader in zekere mate ingetrokken

Het is aan ieder om beschikbare informatie over de tegenpartij te verzamelen en de risico's naar eigen voorkeur in te schatten.

WAT VOOR SOORTEN CLAIMS KUNNEN VERSCHIJNEN?

VOORBEELDEN VAN HET CLAIM-ARTEFACT

(een claim is een verklaring over iemand —
hier zijn de soorten die mensen publiceren.)

— NEGATIEVE CLAIMS



MISHANDELING
viel een ander fysiek aan



DIEFSTAL
nam andermans eigendom
zonder toestemming



FRAUDE
bedroog iemand voor persoonlijk gewin



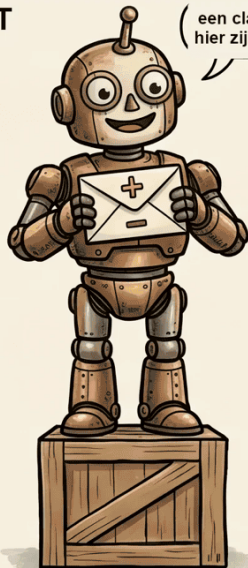
CONTRACTBREUK
kwam een afgesproken verplichting niet na



LASTER
verspreidde een schadelijke onwaarheid



VERWAARLOZING
liet afhankelijkten of plichten onverzorgd achter



+ POSITIEVE CLAIMS



SCHADE HERSTELD
herstelde eerder veroorzaakte schade



SCHULD VOLDAAN
betaalde het verschuldigde
volledig



HULP GEGEVEN
hielp een ander tegen eigen kosten



GEVERIFIEERDE EXPERTISE
bewezen vaardigheid in een vak of
vakgebied



UITMUNTENDE DIENST
langdurige bijdrage aan
de gemeenschap

slechts voorbeelden — elke claim volgt een claimstandaard, en elke standaard kan er meer toevoegen.

je hoeft niet mee te doen — maar als je gedrag anderen raakt, kan iemand er een claim over publiceren.

CLAIMS ZIJN HOE GEDRAG HET NETWERK BINNENKOMT.

■ **Of er informatie over jou in het netwerk verschijnt, hangt uitsluitend af van je eigen gedrag.**

Je hoeft nooit lid te worden van zo'n netwerk, en toch kan er informatie over jou in verschijnen. Het hangt uitsluitend af van je handelen en de impact ervan op anderen.

DE GEMEENSCHAP KAN ER EEN VOOR JE OPENEN



Hij heeft geen eigen DID.
Hij heeft zich nooit
aangemeld.



Je opende geen DID, dus opent de
gemeenschap er een OVER jou.
Negatieve claims hechten zich hier.



Je kunt je eigen openen
— maar de gemeenschap
koppelt de twee.
Reputatie volgt de
persoon, niet de sleutel.

1. JIJ RICHT
SCHADE AAN

2. GEMEENSCHAP
DIENT IN

3. JE KUNT NIET
ONTSNAPPEN

Je kunt ervan afzien een DID te openen. Je kunt niet afzien van je reputatie.

Wat ik zojuist kort heb geschetst, is hoe een sociaal netwerk geïnspireerd op Decentralized Identity (DID) zou kunnen werken. Het primaire doel van DID-concepten is het versterken van privacy en vrijheid via het principe van intekenen op de regels die ik zal volgen en waarnaar ik zal leven — waarbij gebruikers de mogelijkheid krijgen te beslissen welke informatie ze delen en onder welke voorwaarden.

Ik stel voor DID's verder te verbinden tot een communicatienetwerk waarin de houders ervan feedback uitwisselen, ook voorbij situaties waarin iemand iets is overkomen en de gemeenschap of een individu moet reageren. Zulke preventieve vergelijking van de regels waarop we hebben ingetekend — met de mogelijkheid om de economische en andere gevolgen van wederzijdse afwijkingen in de verwachtingen over hoe de andere kant zou moeten opereren te berekenen — zou als een motivatie voor het vinden van consensus kunnen worden beschouwd. In plaats van vrijheid zou zo'n systeem de nadruk leggen op vrijwillige besluitvorming gecombineerd met verantwoordelijkheid voor gedrag in de echte wereld.

Een individu kan het systeem niet alleen breken — een groep mensen maakt meer kans, en een groep mensen met onderhandelde consensus en motivaties om aan veel kwesties samen te trekken, maakt nog meer kans om autoritaire tendensen te weerstaan. Aan de voorwaarde van organisatie uit het eerste hoofdstuk zal worden voldaan zodra aan twee voorwaarden is voldaan: het DID-reputatienetwerk dekt gemeenschappen representatief genoeg af zodat het gebruik ervan ophoudt exotisch te zijn. En tegelijk wordt dit gemeenschapssegment een economisch significante minderheid die assertief kan onderhandelen met de rest van de samenleving.

■ Vrijwilligheid vs. vrijheid

Vrijheid — in positieve zin — zou een secundair effect zijn van het balanceren van twee factoren: vrijwilligheid en de druk van de omgeving richting verantwoordelijkheid.

■ Het AI-tijdperk en de waarde van reputatie

In het tijdperk van kunstmatige intelligentie wordt alles wat met cognitief denken verbonden is geautomatiseerd — en het kan nog verder gaan. Wat blijft er dan in menselijke activiteit over als concurrentievoordeel? Het antwoord is moeilijk, en er zal ongetwijfeld iets worden gevonden, maar één ding kunnen we met zekerheid zeggen: reputatie zal beslissen. Een verifieerbare geschiedenis van je gedrag, je verbintenissen en de nakoming ervan — dat is iets wat AI niet voor je zal opbouwen.

ALS AI HET DENKWERK DOET — WAT BLIJFT ER DAN OVER VOOR JOU?

AI-AGENTS NEMEN HET REPETITIEVE WERK OVER

GESTANDAARDISEERDE
BEDRIJFSFLOWS

BOEKHOUDING

OPSTELLEN

één voor één wordt het repetitieve
cognitieve werk overgedragen aan
agents.

STANDAARDFLOW

WAT BLIJFT ER DAN OVER VOOR EEN
MENS?



iedereen kan hetzelfde idee kiezen.
wat maakt de ene bakker, de ene timmerman,
de ene AI-werkplaats anders dan de
volgende?

REPUTATIE — WAT TWEE UIT ELKAAR HOUDT



iemand moet verantwoording afleggen voor wat
de agent doet — en die verantwoordelijkheid kan
niet worden overgedragen.

zonder reputatie ziet elke bakker er hetzelfde uit — en het grootste merk verslindt ze allemaal.

zou dit het gedecentraliseerde pad kunnen zijn dat AI aan de leiband houdt — het ding dat voorkomt dat één speler de hele markt bezit?

AI AUTOMATISEERT HET WERK — REPUTATIE HOUDT JE MENSELIJK.

DE ECONOMIE VAN DE WAARHEID

gemeenschapsstrook



EÉN GEMEENSCHAP. VERSCHILLENDE STANDPUNTEN.

DE
INDIENING

IMPOPULAIR MAAR
AANVAARDBAAR



IN CONSENSUS



BUITEN CONSENSUS



DE
LOTING

uniforme
kans

niet mijn
standpunt

dan
hoger
tarief

telling opnieuw
I I I I I



lotingen zijn eerlijk — gelote verificateurs rekenen een risicopremie



basistarief — eerste loting
accepteert



de lotingen blijven doorgaan — geen gelote verificateur zal tekenen

VERLATEN

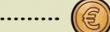
DE
TERUGBETALING

HET
GROOTBOEK



grotendeels terugbetaald, met de tijd wat verloren

IETS DUURDER



gemiddeld volledige
terugbetaling



ONBETAALBAAR



borg meestal verbeurd

borg meestal
verbeurd

HET ALGORITME KIEST EERLIJK.
MENSEN BEPRIJZEN WAT ZE
GELOVEN.



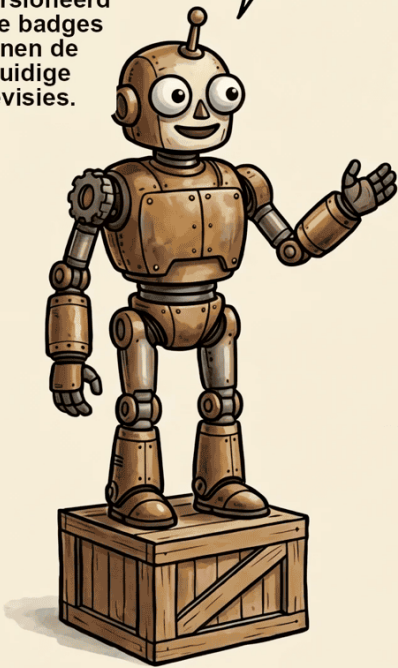
ONDERSTE
WAARNEMERSSTROOK

UNIFORME LOTING. NIET-UNIFORME RESPONS. HOE VERDER VAN DE CONSENSUS, HOE HOGER DE PRIJS.

WAT ER IN HET NETWERK GEPUBLICEERD WORDT

vijf dingen kunnen gepubliceerd worden — elk daarvan heeft versies.

elk artefact is geversioneerd — de badges tonen de huidige revisies.



v1

DID-DOCUMENT

jouw identiteitsrecord op het netwerk — sleutels, metadata, netwerkadres.

BEHEERD DOOR: de DID-houder

v2

CLAIMSTANDAARD

het schema dat een claim moet volgen — wat als geldig bewijs telt.

BEHEERD DOOR: een autoriteit met reputatie in het domein

v3

BELEIDSSTANDAARD

het schema dat een beleid moet volgen — de vorm van acceptatieregels.

BEHEERD DOOR: een autoriteit met reputatie in het domein



v4

CLAIM

een verklaring over een subject, volgens een claimstandaard — gepubliceerd door een uitgever, mede-ondertekend door de autoriteit van de standaard als zowel uitgever als verificateur dat vragen.

BEHEERD DOOR: uitgever publiceert — subject is het doelwit

claims zijn er in twee soorten — positief (+) en negatief (-).

v5

DID-BELEID

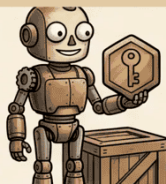
de verklaarde regels van een DID — gebruikt bij verificatie, consensus en uitgifte.

BEHEERD DOOR: de DID-houder (één beleid per DID)

ELK ARTEFACT IS GEVERSIONEERD. ELKE VERSIE IS PUBLIEK.

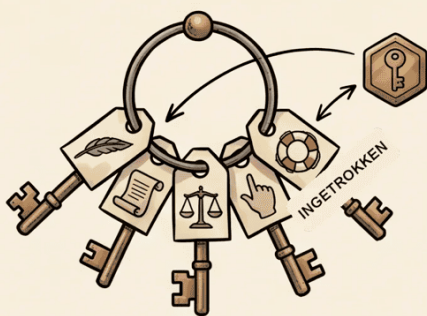
WAT ZIT ER IN EEN DID-DOCUMENT?

VOORBEELDEN VAN HET
DID-DOCUMENT-ARTEFACT



je DID-document is je identiteitskaart
op het netwerk — dit is wat het bevat.

VELDEN DIE JE ERIN AANTREFT



SLEUTELS EN ONDERTEKENINGSREGELS

elke sleutel verleent één bevoegdheid — dit document bewerken, een claim uitgeven, als autoriteit optreden, een beleid beheren, of herstel delegeren. Bevoegdheden kunnen aan een andere DID worden overgedragen, en later weer worden ingetrokken.



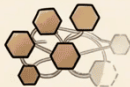
NETWERKADRESSEN

waar het netwerk je kan bereiken — wijzigbaar zonder je identiteit te herschrijven



AANGEMAAKT EN GEVERSIONEERD

wanneer deze identiteit voor het eerst verscheen, en welke revisie je nu leest



GEKOPPELDE IDENTITEITEN

een overzicht van DID's waarmee je verbonden bent — een handige weergave, technisch elders opgeslagen



OPVOLGINGSMARKERING

als je identiteit verloren of gestolen is, kan een autoriteit deze DID als beëindigd markeren en naar je opvolger verwijzen

de DID-houder schrijft elke nieuwe versie — maar elke versie moet verificatie doorstaan voordat het netwerk het publiceert.

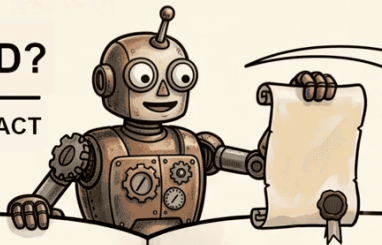
jij schrijft het — het netwerk verifieert het. Je kunt jezelf niet zomaar tot bestaan publiceren.



JIJ SCHRIJFT JE IDENTITEIT — HET NETWERK BEVESTIGT HET.

WAT IS EEN CLAIMSTANDAARD?

VOORBEELDEN VAN HET CLAIMSTANDAARD-ARTEFACT



de standaard is het lege formulier
— een claim is het ingevulde
formulier. Ik laat je beide naast
elkaar zien.

DE STANDAARD — HET LEGE FORMULIER

	SUBJECT-DID de DID waar deze claim over gaat
	UITGEVER-DID de DID die de claim ondertekent
	WANNEER EN WAAR een datum en een plaats
	GOEDGEKEURDE BEWIJSTYPES alleen deze soorten bewijs tellen
	UITKOMSTSCHAAL kies precies één trede — geen vrije tekst

EEN CLAIM — HET INGEVULDE FORMULIER

	SUBJECT-DID did:nwo:alice-9f2b...
	UITGEVER-DID did:nwo:magistrates-04...
	WANNEER EN WAAR 3 maart, marktplein
	GOEDGEKEURDE BEWIJSTYPES foto ✓ — getuigeneed ✓ — doktersverklaring ✓
	GOEDGEKEURDE BEWIJSTYPES matig — trede 2 van 4

elk veld links heeft precies één ingevulde tegenhanger rechts — dat maakt twee claims van dezelfde soort vergelijkbaar.

het zegel van de autoriteit op een
ingevulde claim is een belofte: het
proces is werkelijk gevolgd.



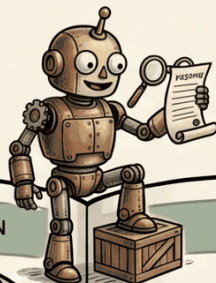
Ik zet mijn reputatie
in dat dit volgens de
standaard is
verwerkt.

MISHANDELING v3	SCHULD v2	MEDISCHE HULP v4	VAKMANSCHAP v1	GETUIGENIS v5
MISHANDELING v3	SCHULD v2	MEDISCHE HULP v4	VAKMANSCHAP v1	GETUIGENIS v5

DE STANDAARD IS HET FORMULIER — EEN CLAIM IS HET INGEVULDE EN BEZEGELDE FORMULIER.

WAT IS EEN DID-BELEID?

VOORBEELDEN VAN HET DID-BELEID-ARTEFACT



mijn beleid gaat niet over hoe een claim wordt geschreven — dat is de taak van de standaard. Mijn beleid is hoe ik beslis of ik überhaupt aandacht aan de claim schenk: vertrouw ik wie het ondertekende, vertrouw ik de autoriteit achter hun standaard, en is de zaak mijn aandacht wel waard?

DE STANDAARD — GEËRFDE STANDAARDWAARDEN

REGELNAAM



REPUTATIEDREMPEL
UITGEVER

Ik accepteer uitgevers met
een reputatie boven vijf van
tien



VERTROUWENSLIJST
AUTORITEITEN

Ik accepteer standaarden van
elke autoriteit wiens eigen
reputatie boven vier van tien
ligt



INHOUDSFILTER

Ik verwerk elke claim wiens
zaak boven de
'onbeduidend'-grens weegt



ANTISPAM-PRIJSCURVE

bij mij indienen is goedkoop
voor inhoudelijke, zeldzame
claims — en stijgt snel voor
kleinzielige of herhaalde



GECOMBINEERDE
WEGING

uitgeversreputatie en
autoriteitsreputatie
vermenigvuldigen; kleinzielige
inhoud halveert het resultaat

beleid herschrijft de standaard niet — het beoordeelt de mensen en de zaak. Behouden, wijzigen, verwijderen, toevoegen — vier simpele zetten bovenop een gedeeld startpunt.

MIJN BELEID — DAARVAN AFGELEID

regelnaam

✓ BEHOUDEN ✎ GEWIJZIGD ✗ VERWIJDERD + TOEGEVOEGD
vinkje actiewoord actiewoord actiewoord actiewoord



REPUTATIEDREMPEL
UITGEVER

aangescherpt — ik eis zeven van
tien



VERTROUWENSLIJST
AUTORITEITEN

Ik vertrouw magistraten en artsen
volledig; ik halveer het gewicht van
claims onder het gemeentelijk toezicht;
ik weiger alles onder de havenpolitie
helemaal



INHOUDSFILTER

kleinzielige overlast-claims kosten me
niets om te negeren — ik lees ze
simpelweg niet



ANTISPAM-PRIJSCURVE

behouden — de standaardcurve is prima
voor mij



GECOMBINEERDE
WEGING

verwijderd — ik gebruik mijn eigen
formule



EXPONENTIËLE
KOSTEN BIJ
HERHAALDE CLAIMS

toegevoegd — elke nieuwe claim
van dezelfde uitgever over mij in
een jaar kost tien keer de vorige
toegevoegd — ik weiger elke claim
te lezen die tussen middernacht en
dageraad is ingediend



STILTE-UREN



VERIFICATIE — mijn beleid filtert zowel
binnenkomende claims als mijn eigen
concepten voordat ik ze uitgeef. Uitgifte is
verificatie op de weg naar buiten

CONSENSUS — mijn beleid is mijn
stem wanneer de gemeenschap
gedeelde regels onderhandelt.



JOUW BELEID BEOORDEELT DE BOODSCHAPPER — NIET HET FORMULIER.

Waarom het netwerk oncensureerbaar is

Tot nu toe hebben we beschreven wat het netwerk kan. Laten we ons nu richten op waarom het niet kan worden uitgeschakeld of gecensureerd.

Het netwerk zal waarschijnlijk worden gebouwd op de principes van het Tor-netwerk en onion-routing (een manier om netwerkverkeer te maskeren met behulp van Mixnet-principes) — een technologie waarbij communicatie door verscheidene lagen van versleuteling gaat en geen enkele node tegelijk de afzender en de ontvanger kent. Een centrale instelling kan niet over je schouder meekijken, omdat er nergens is van waaruit dat zou kunnen.

Je kunt het bestrijden, maar je kunt niet winnen — tenzij je het hele land stort in totalitair toezicht op het niveau van afzonderlijke netwerkpakketten en laaggeleverde acties op elk stuk hardware dat verbinding maakt met het internet en communiceert op het gegeven reputatienetwerk. En dat is precies de keuze waar het centralisme voor staat: ofwel aanvaarden dat burgers een instrument buiten je bereik hebben, ofwel je ingraven in de donkere hoeken van economische stagnatie in naam van totalitaire controle.

Laten we ons geen illusies maken — ook democratische regimes zullen dit proberen in hun strijd voor centralisme. Ze zouden mensen liever in de boeien slaan dan de macht af te staan.

HOE JE BERICHTEN ONTRACEERBAAR BLIJVEN

TWEE VERDEDIGINGSLINIËS TEGELIJK — LAGEN EN RUIS

INHOUD: GEWIKKELD IN LAGEN

(de techniek achter Tor — 'onion routing')



AFZENDER

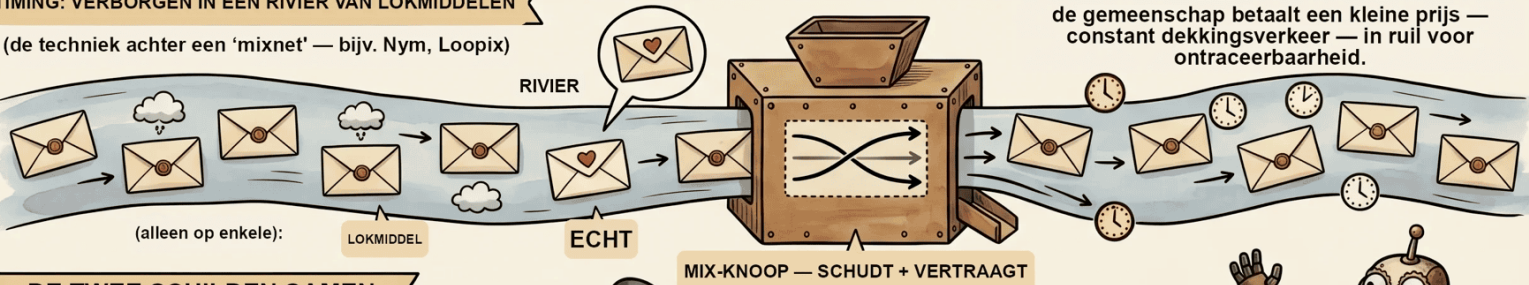


vier sloten, vier sleutels
— één per knoop.



TIMING: VERBORGEN IN EEN RIVIER VAN LOKMIDDELEN

(de techniek achter een 'mixnet' — bijv. Nym, Loopix)



DE TWEE SCHILDEN SAMEN

MATRIX	VERBERGT WIE ↔ WIE?	VERBERGT WANNEER?
ALLEEN LAGEN	✓ JA	✗ NEE
ALLEEN RUIS	✗ NEE	✓ JA
LAGEN + RUIS	✓ JA	✓ JA

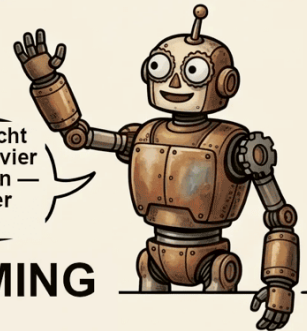
(onion routing + mixnet — de combinatie van de beide technieken)



honderd enveloppen
per uur — welke
doet ertoe?

de waarnemer ziet de stroom
maar kan ECHT niet van
LOKMIDDEL onderscheiden.

het echte bericht
zweeft in een rivier
van lokmiddelen —
en draagt vier
jassen.



INHOUD VERBORGEN DOOR LAGEN — TIMING VERBORGEN DOOR RUIS.

Voor de hand liggende twijfels wegnemen

Het beschreven systeem roept vanzelfsprekend een aantal vragen op. Laten we de meest voorkomende behandelen.

Afhankelijkheid van technologie

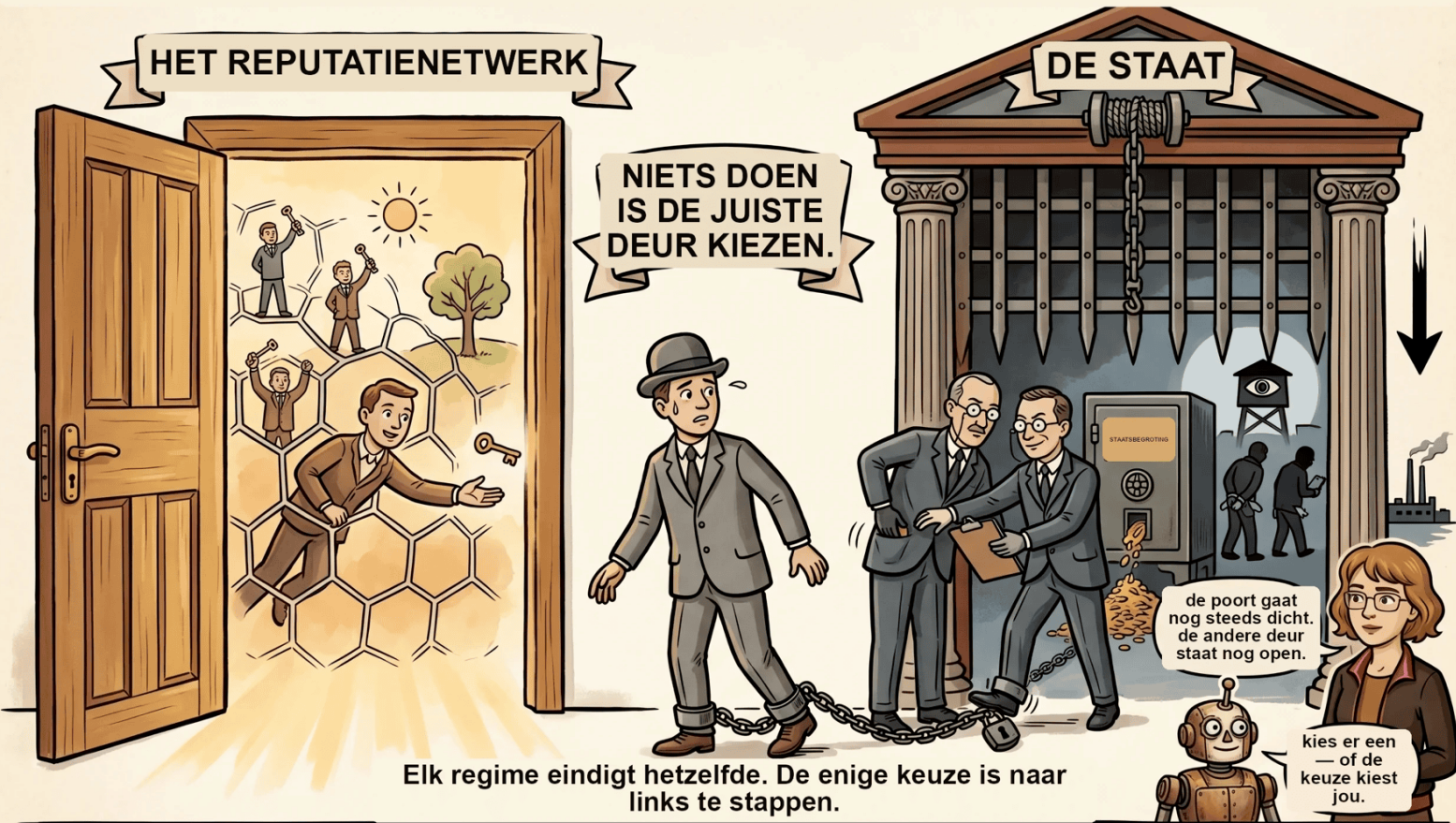
Je hebt waarschijnlijk al gemerkt dat, anders dan de moderne staat — die ongeveer 150 jaar bij ons is — de hier beschreven reputatienetwerkoplossing sterk afhangt van de technologie van het globale/lokale internet. Bij een storing komt de werking van zo'n netwerk in gevaar.

Als de storing tijdelijk is, is er geen verlies van gegevens of van de consistentie van claims in het netwerk, en zouden ook de binnen gemeenschappen bereikte reputatiebalansen niet verstoord mogen raken. Anders dan vergelijkbare betaalnetwerken gaat dit netwerk uit van zeer lage frequenties van processen en gegevensitems. In dat opzicht verschilt het gedecentraliseerde reputatienetwerk niet van de huidige staat, die nu ook sterk afhankelijk is van technologie en verleerd is hoe je met papieren kaart-systemen werkt (al zou hij in noodplannen geen keus hebben).

De evolutionaire opvolger van de staat in de vorm van een reputatienetwerk kan, bij een permanente storing (een catastrofe van ongekeerde omvang), terugvallen op een primitiever gecentraliseerd systeem — de staat.

Technologie stelt de mensheid in staat hogere beschavingsvormen van bestuur te bereiken en brengt ons voordelen, maar ook risico's.

TWEE PADEN — DE STAAT SLUIT, HET NETWERK OPENT



DE STAAT SLUIT STANDAARD. HET NETWERK OPENT UIT KEUZE.

Gooi ik geld uit het raam door in het netwerk te publiceren?

De kosten van het publiceren van een claim in het reputatienetwerk zijn grotendeels niet verzonken. Het nut van een bericht dat een uitgever in het netwerk plaatst — informatie over echte grieven, geverifieerde ervaringen, relevante waarschuwingen — keert statistisch over een langere tijdshorizon terug in de vorm van vergoedingen voor het verifiëren van andermans claims uit de gemeenschap. De gemeenschap profiteert, de uitgever bouwt reputatie op, en de kosten van het publiceren van waarheidsgetrouwe informatie benaderen zo een terugbetaalbare borg, waarvan slechts een kleiner deel aan werkelijke onderhoudskosten van het netwerk moet worden afgetrokken. Omgekeerd keren onwaarachtige of triviale registraties niet terug — hun kosten zijn een netto verlies. Eerlijkheid is daarom niet alleen een morele keuze, maar ook een economisch rationele strategie.

Na aftrek van de onderhoudskosten van het netwerk zou dit principe het principe van economische neutraliteit kunnen worden genoemd — ik verlies niet wanneer ik met de gemeenschap ben, ik verlies wanneer ik tegen haar ben.

De gemeenschap heeft ook solidariteitskanalen om de eerlijke houding van haar leden te waarderen. Maar laten we ons geen illusies maken: oproepen tot solidariteit komen meestal voort uit maatschappelijke druk van de gemeenschap, dus dit is misschien geen solidariteit in de vrijwillige zin van het woord.

Wat als iemand meerdere identiteiten aanmaakt?

Een persoon kan meerdere DID-identiteiten parallel beheren. Reputatie opbouwen voor elke identiteit vergt echter onafhankelijke inspanning — tijd, energie, geld.

Geen shortcuts: elke identiteit moet haar track record¹ opbouwen door daadwerkelijke activiteit. Het onderhouden van parallelle identiteiten is daarom opzettelijk duur.

In vrije samenlevingen ontmoedigen de kosten misbruik.

In dictaturen worden parallelle identiteiten echter een overlevingsinstrument: ze maken het mogelijk ondergrondse netwerken te organiseren, veiliger over de zwarte markt te navigeren, en gecompartmenteerd² verzet te bieden, waarbij het compromitteren van één identiteit de andere niet onthult — en na de val van het regime maken ze een naadloze terugkeer mogelijk naar het openbare leven en de daar opgebouwde reputatie, en zelfs het samenvoegen van de voorheen officiële en de geheime DID tot één gecombineerde verzameling registraties via een claim.

¹**Track record** — algemeen: een geschiedenis van eerdere resultaten, successen en mislukkingen van een persoon of organisatie. Hier: de som van alle eerdere interacties van een gegeven DID-identiteit in het netwerk — geverifieerde claims, aanvaarde en afgewezen registraties — waaruit haar reputatie wordt afgeleid.

²**Compartmentalisatie** (van het Eng. *compartment*) betekent het scheiden van informatie in geïsoleerde eenheden zodat het blootleggen van één eenheid de andere niet compromitteert. Een principe bekend uit inlichtingendiensten: een agent kent alleen zijn deel van de operatie, zodat hij zelfs onder dwang het geheel niet kan onthullen.

DEZELFDE INSPANNING — EEN VERKWISTEND PLAN B IN VRIJHEID, EEN REDDINGSLIJN ONDER TIRANNIE

PARALLELE IDENTITEITEN KOSTEN HETZELFDE — MAAR KOPEN VERSCHILLENDE DINGEN

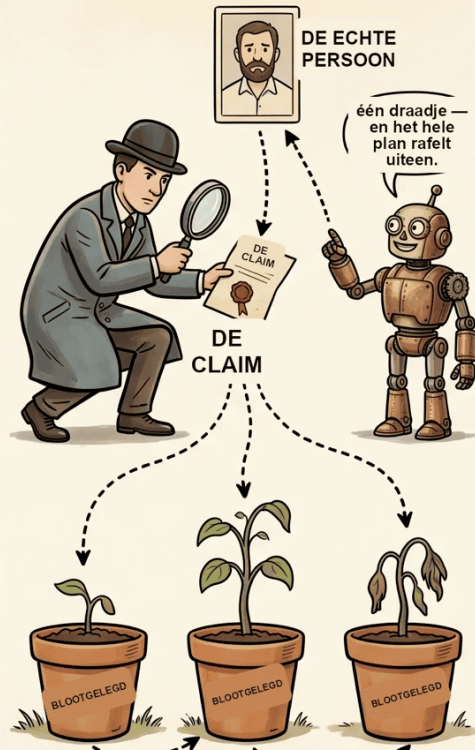
IN VRIJHEID — EEN DUUR PLAN B



OF — EEN SCHONE LEI NA EEN PERSOONLIJKE MISSTAP



ÉÉN CLAIM EN PLAN B IS WEG



één enkele claim bindt elke pot aan dezelfde tuinier — jaren van tijd, energie en geld uitgewist in een middag.

ONDER TIRANNIE — ÉÉN VOOR DE STAAT, ANDERE VOOR VRIJE VERENIGING (de staat verbiedt identiteiten ronduit of eist ze onder eigen controle)



de bakstenen muren tussen cellen doen het werk dat de staat verbiedt — verlies er een, de anderen gaan door; wanneer het regime valt, hervat het openbare leven.

IN VRIJHEID IS MISBRUIK DUUR. ONDER TIRANNIE IS OVERLEVEN MOGELIJK.

■ Perceptie binnenstebuiten gekeerd

Anders dan de staat keert het principe van een reputatienetwerk gebouwd op gedecentraliseerde identiteit het paradigma van gepercipieerde prioriteit om:

- Wat telt is reputatie — d.w.z. het verleden, gebruikt om de risico's van interactie met een tegenpartij in te schatten — en persoonsgegevens zoals namen, adressen enz. kunnen een kwestie zijn van hoffelijke gegevensuitwisseling
- Terwijl de staat primair persoonsgegevens eist, reputatiegegevens vergaart, en de gemeenschap alleen laat zien wat hem uitkomt

Kan een rijk persoon niet gewoon meer identiteiten “kopen” (of virtuele gemeenschappen aanmaken)?

De mogelijkheid om parallelle gedecentraliseerde identiteiten aan te maken lijkt op het eerste gezicht een oneerlijk voordeel voor mensen met grotere economische middelen boven wie er minder heeft. Er moet echter worden benadrukt dat, anders dan in een gecentraliseerd systeem waar het volstaat een paar punten in de machtspiramide te corrumperen om bepaalde wandaden te laten verdwijnen, men in een gedecentraliseerd systeem de hele gemeenschap zou moeten corrumperen.

Vervangende gedecentraliseerde identiteiten zouden dit doel kunnen dienen, maar hun reputatie moet in de loop van de tijd worden opgebouwd door echte interactie met daadwerkelijke andere gemeenschap-sleden — ze kan niet zomaar worden gekocht, omdat het netwerk het verifieerbaar maakt hoe een gegeven identiteit presteert.

Bovendien kunnen er op de markt diensten bestaan (en zullen die er waarschijnlijk zijn) die, optredend als autoriteit, onderzoeken aanbieden die bewijs opleveren dat verscheidene gedecentraliseerde identiteiten in feite dezelfde persoon zijn. Eén registratie die in het reputatienetwerk wordt ingevoerd, kan zo, voor een fractie van de kosten, de hele investering aan tijd, energie en geld in het opbouwen van parallelle identiteiten tenietdoen.

Economisch loont het daarom om de gemeenschap niet te bedriegen — en indien nodig zijn handelen tegen het licht te houden en herstel na te streven zodat de reputatie terugkeert naar een aanvaardbaar niveau en de drager ervan niet economisch of anderszins lijdt onder de toorn van de gemeenschap.

Een economisch machtige identiteit die reputatie in haar eigen gemeenschap heeft verloren, kan proberen aan de toorn van de gemeenschap te ontsnappen via onderhandse deals met gerichte identiteiten — maar die riskeren dan ook hun eigen reputatie te verliezen.

Er blijft nog altijd de vlucht naar een andere gemeenschap met een verse identiteit — maar dat betekent alle verworvenheden achterlaten en ergens vanaf nul beginnen met nul reputatie. Soms kan het een begrijpelijk pad zijn en de enige uitweg.

REPUTATIE IS HET TEGENWICHT VOOR ECONOMISCHE MACHT

DE RIJKE MAN KOOPT INVLOED — DE GEMEENSCHAP ONTHOUDT HET

DE AANVAL — INFILTREER EN KOOP OM

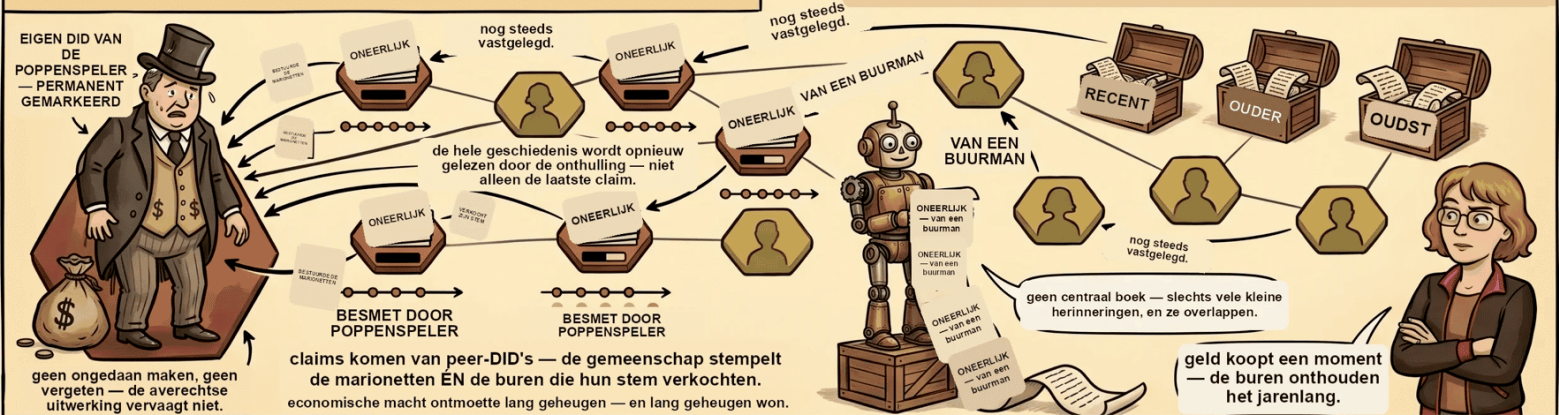
ACHT MARIONETTEN GEPLAATST + DRIE BUREN OMGEKOCHT



LATER

DE VERDEDIGING — LANG GEHEUGEN, GEDISTRIBUEERDE BOEKHOUDING

ELKE BUURMAN HOUDT ZIJN EIGEN GEHEUGEN — GEEN CENTRAAL BOEK, GEEN VERGETEN



ECONOMISCHE MACHT REIKT NAAR BINNEN — DE AVERECHTSE UITWERKING KOMT THUIS, EN GAAT ER NIET AF.

Opmerking

Gemeenschappen zouden op vergelijkbare wijze omgaan met een aanval waarbij iemand mid-delen besteedt aan het aanmaken van een virtuele identiteit: voor die identiteit is het riskant om in interactie te treden met een andere gemeenschap zonder verificatie — dat wil zeggen om kritiekloos informatie over de identiteiten van de andere gemeenschap te aanvaarden. Reputaties worden altijd binnen een gemeenschap opgebouwd, niet globaal.

En de meelifters die alleen willen lezen en niets aan de gemeenschap geven?

Toegang tot informatie is niet onbeperkt vanaf dag één van het aanmaken van een gedecentraliseerde identiteit. Nieuwe deelnemers — die nog geen reputatie hebben opgebouwd door daadwerkelijke activiteit — krijgen te maken met getrapte beperkingen: minder informatie, langere wachttijden, hogere kosten per opvraging. Het netwerk belooft deelname, niet passieve consumptie en willekeurige gegevensoogst.

Een gedecentraliseerde identiteit riskeert ook haar reputatie wanneer ze haar reputatie tegen betaling uitleent aan een andere persoon (die misschien niet eens in het DID-reputatienetwerk zit). Hetzelfde principe geldt hier: zulk verraad aan de gemeenschap (schending van privacy) kan terugslaan op de reputatie van de verrader, en de daad kan niet worden uitgewist via een onderhandse deal zoals dat in een gecentraliseerd systeem werkt. Ze moeten rekening houden met de toorn van de gemeenschap, inclusief het verlies van verworvenheden — want de gemeenschap is in hun ogen de garant van bijvoorbeeld het voorrecht van het bezit van roerende en onroerende zaken.

■ Anker aan de echte wereld

Bij het inschatten van risico is het risicovollere subject vanzelf degene die niet het door een gegeven gemeenschap erkende voorrecht van eigendom geniet — hij heeft minder te verliezen in zijn handelingen (digitale bezittingen zijn makkelijker te verplaatsen).

Het lijkt misschien een klein detail, maar het heeft grote gevolgen. Willen dat de gemeenschap hefboomkracht heeft over haar leden impliceert eigendom als een voorrecht — in de vrijste samenlevingen bijna onaantastbaar, en toch geen recht, noch een fundamenteel principe, maar een voorrecht dat in extreme gevallen kan worden ingetrokken (ik kan me bijvoorbeeld de weigering van dienst ter verdediging van de gemeenschap in een gewapend conflict voorstellen).

Het beantwoordt ook onderhuids hoe de gemeenschap haar leden zal behandelen, en welke motivatie een lid heeft om voor de gemeenschap te strijden — om zijn voorrechten te behouden. Een persoon kan tekortschieten in zijn verantwoordelijkheid tegenover de gemeenschap, maar kan moreel geen clementie verwachten als het gaat om het behouden van zwaarbevochten voorrechten.

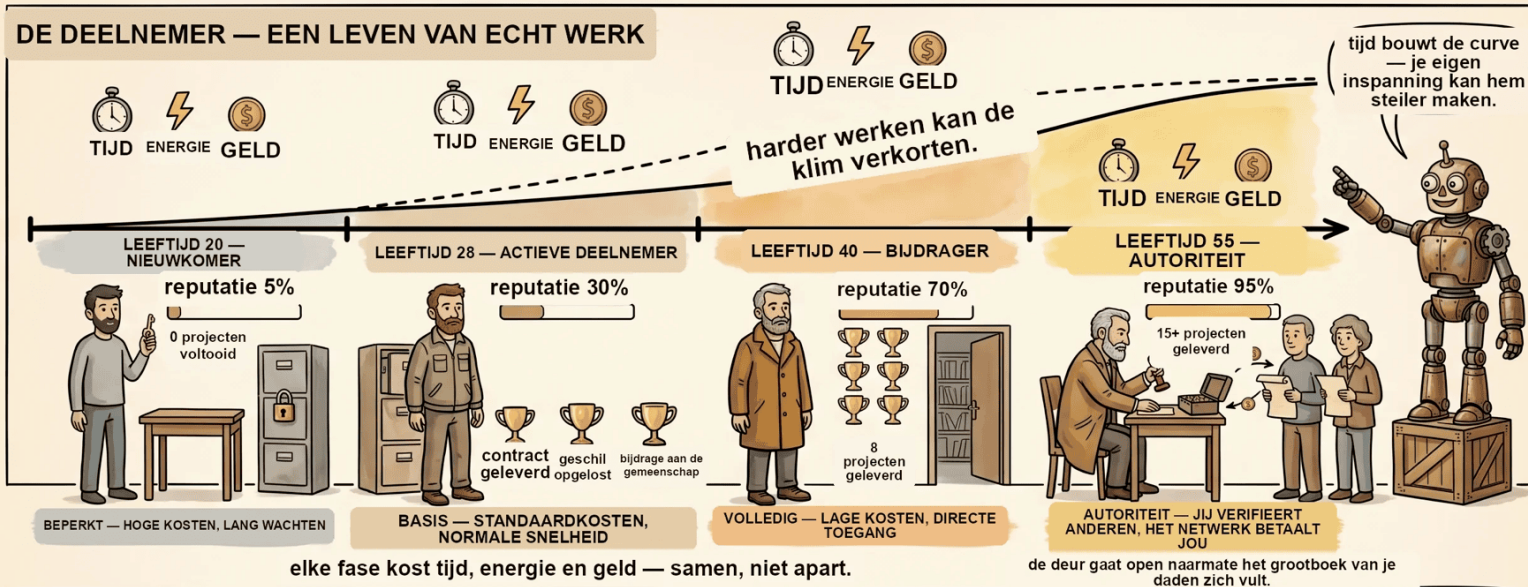
Financiële neutraliteit

Bij het lezen van woorden als gedecentraliseerd, oncensureerbaar, onomkoopbaar kan men het niet laten ze te associëren met de bekendste cryptovaluta's — Bitcoin, Monero en, zeg, Kaspa — die in zulke termen kunnen worden beschreven. De intuïtie is hier echter misleidend: vergoedingen voor de diensten van autoriteiten, voor verificatie en publicatie, enzovoort, kunnen in elke valuta of geldsoort worden voldaan. Wat telt voor de verbonden deelnemers van het sociale netwerk in het DID-netwerk (dat wil zeggen jouw

HET NETWERK BELOOFT DEELNAME

REPUTATIE WORDT OPGEBOUWD OVER EEN HEEL LEVEN — NIET GEKOCHT, NIET GELEEND

DE DEELNEMER — EEN LEVEN VAN ECHT WERK



DE PROFITEUR — LEEST, PUBLICEERT NOOIT



gemeenschap) en zijn omgeving is een door reputatie geruggensteunde bevestiging dat de betaling is gedaan. De publicatie van een claim moet individueel een redelijke, verifieerbare kost dragen, zodat een actor niet zoveel en welke claims hij maar wil kan publiceren zonder energie, geld en tijd te besteden — een sterk ongewenste toestand die overeenkomt met het voorrecht van elites in de door corruptie geteisterde staatssystemen van vandaag.

In dat opzicht hebben de genoemde cryptovaluta's een klein voordeel doordat hun netwerken optreden als vertrouwde autoriteiten voor het verifiëren dat een gegeven betaling heeft plaatsgevonden, ten koste van een klein verlies aan privacy en het blootleggen van enkele van iemands adressen.

Vrijwilligheid, verantwoordelijkheid en vrijheid

Vrijwilligheid is individueel: ik beslis voor mezelf. Verantwoordelijkheid ontstaat wanneer mijn beslissing anderen raakt — dan treedt de feedback in werking. Vrijheid is geen geschenk en geen recht — ze is een fenomenologisch³ resultaat van duizenden bilaterale interacties tussen vrijwilligheid en de druk richting verantwoordelijkheid, gemiddeld over de samenleving. Het netwerk dicteert dit gemiddelde niet — het

³**Fenomenologisch** (van het Gr. *phainómenon* — dat wat verschijnt) — algemeen: een benadering die verschijnselen onderzoekt zoals ze zich in de directe ervaring aandienen, door te observeren wat eruit volgt, zonder vooraf gegeven verklarende theorieën in de microwereld eronder. Hier: vrijheid is geen abstract principe dat van bovenaf wordt gedefinieerd, maar een geobserveerd verschijnsel — een gevolg van duizenden micro-interacties tussen mensen dat emergeert uit hoe we elkaar werkelijk behandelen.

emergeert⁴ uit de prijssignalen van verificateurs en uit de vooraf aangekondigde verificatiebeleidslijnen die gemeenschapsleden voor zichzelf instellen.

Welke voorkeur voor vrijheid een individu binnen een gemeenschap heeft, hangt af van zijn gevoel voor hoeveel hij zelf bereid is te slikken van wat hij aan anderen oplegt. Bij zaken die vanzelfsprekend en voor iedereen voordelig zijn, is er geen moreel dilemma — moord is verkeerd. Dan zijn er gevallen waarin opties naar de positie van toegestane voorrechten verschuiven: bewijs je vaardigheden en we laten je de weg op, zodat er minder kans is dat je ons doodt. En ten slotte zijn er zaken waarbij het individu zegt — het is me niet waard, ik verbied mijn buurman niet om bladeren te verbranden als ik het zelf ook doe, of omdat ik iets anders doe dat zijn comfort beperkt en hij op zijn beurt zou kunnen willen dat aan mij te verbieden. Als we de grens van vrijheid historisch hebben getrokken waar de vrijheid van iemand anders begint, dan vervult een sociaal reputatienetwerk gebouwd op gedecentraliseerde identiteit dit beter dan de gecentraliseerde representatieve democratie — waarin bijvoorbeeld de bevoorrechte laag van gekozen vertegenwoordigers zichzelf probeert vrij te stellen van toezicht op persoonlijke communicatie, maar niet aarzelt het aan hun kiezers op te leggen, met allerlei onderhandse voorwendsels en manipulaties.

De schakelaar tussen vrijheid en totalitarisme (en delegatie)

Een eenvoudig mechanisme binnen het DID-netwerk kan het hele systeem richting meer vrijheid of meer controle verschuiven: het aantal registraties dat een DID per tijdsperiode mag publiceren. Wanneer registraties schaars blijven, weegt elk ervan — dat is vrijheid. Wanneer registraties overvloedig zijn en

⁴**Emergent** (van het Lat. *emergere* — opduiken) betekent “spontaan ontstaand uit interacties van eenvoudiger delen zonder dat iemand het ontwerpt of aanstuurt.” Een zwerm vogels vliegt in formatie, ook al heeft geen enkele vogel een plan voor de formatie — de formatie emergeert uit de eenvoudige regels van elk individu. Zo ontwerpt ook in het reputatienetwerk niemand de gedragsregels van het geheel — ze emergeren uit duizenden individuele beslissingen.

VRIJWILLIGHEID → VERANTWOORDELIJKHEID → VRIJHEID

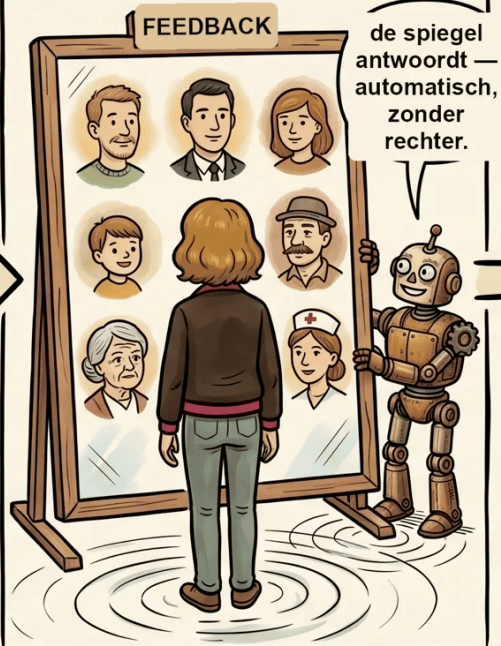
DRIE STAPPEN — VAN DE KEUZE VAN ÉÉN PERSOON NAAR HET PATROON VAN EEN HELE SAMENLEVING

VRIJWILLIGHEID



het individu beslist — niemand dwingt haar.
en niemand is haar ook een positieve plicht verschuldigd.

VERANTWOORDELIJKHEID



mijn keuzes deinen uit — en de deining komt terug.
de gevolgen spreken voor zich.

VRIJHEID



niemand tekende deze kaart — hij tekende zichzelf.
vrijheid is de statistische vorm
van hoe buren elkaar behandelen.

VRIJHEID IS GEEN GESCHENK VAN BOVENAF — HET IS HET PATROON DAT WE SAMEN MAKEN.

trivialiteiten bestrijken, is dat totalitarisme. Je kiest de richting met elke registratie die je publiceert. Het netwerk zelf is vrij noch totalitair — het is neutrale infrastructuur. Wat het wordt, wordt bepaald door hoe mensen het gebruiken.

Binnen mijn eigen verificatiebeleid is het zinvol om, voor een generieke DID in mijn sociale netwerk — binnen gemeenschappen — een maximumaantal claims in te stellen (elke verifieerbare uitspraak in het algemeen; hier: een registratie gepubliceerd in het reputatienetwerk) dat een uitgever per periode mag uitgeven om er voor mij rekening mee te houden en zijn verificatieverzoeken als relevant te beschouwen.

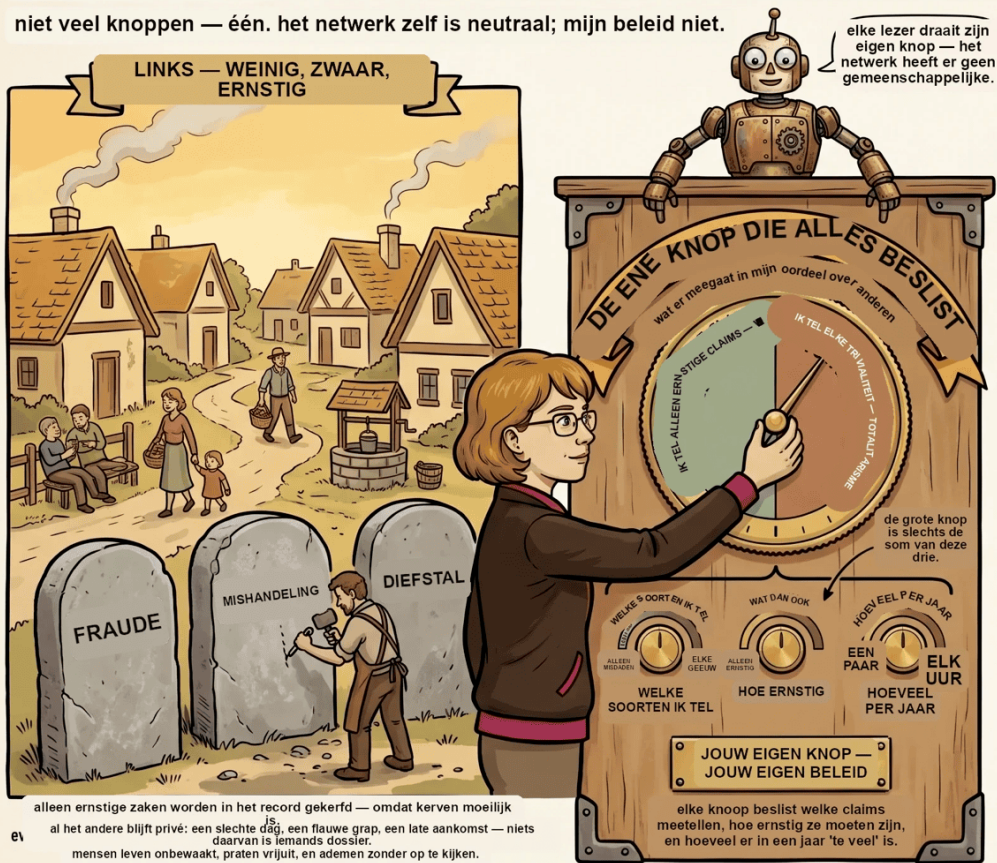
Ik houd een intuïtief getal in gedachten — lage enkele cijfers per jaar. Zo'n censurerende benadering kan nogal isolationistisch lijken. Maar ik kan de aanvrager legitiem voor een keuze stellen: een van zijn reeds uitgegeven registraties uitkiezen en de verificateur vragen die in te trekken, dat wil zeggen ongeldig te maken — wat een tamelijk agressieve eis is in een situatie waarin de aanvrager, bij toeval, werkelijk het slachtoffer is geworden van meerdere onafhankelijke wandaden, en ik zou daarmee zeker bijdragen aan zijn gevoel van vervreemding van de gemeenschap.

Een effectievere optie blijkt daarom de mogelijkheid om een deel van iemands rechten om informatie in het reputatienetwerk te publiceren te delegeren ten gunste van een gemeenschap of een autoriteit, die dan — op solidaire wijze, volgens haar interne regels — beslist hoe ze toe te wijzen. Een groep moet in staat zijn te zorgen voor wie ze als benadeeld beschouwt. Een gemeenschapslid heeft op elk moment het recht, totdat het gedelegeerde recht is gebruikt, zijn delegatie in te trekken.

DE SCHAKELAAR TUSSEN VRIJHEID EN TOTALITARISME

ÉÉN ENKELE PARAMETER — HOEVEEL IK KIES TE VOLGEN — KANTELT EEN HELE SAMENLEVING TUSSEN VRIJHEID EN TIRANNIE

niet veel knoppen — één. het netwerk zelf is neutraal; mijn beleid niet.



alleen ernstige zaken worden in het record gekerfd — omdat kerven moeilijk is
al het andere blijft privé: een slechte dag, een flauwe grap, een late aankomst — niets daarvan is iemands dossier.
mensen leven onbewaakt, praten vrijuit, en ademen zonder op te kijken.

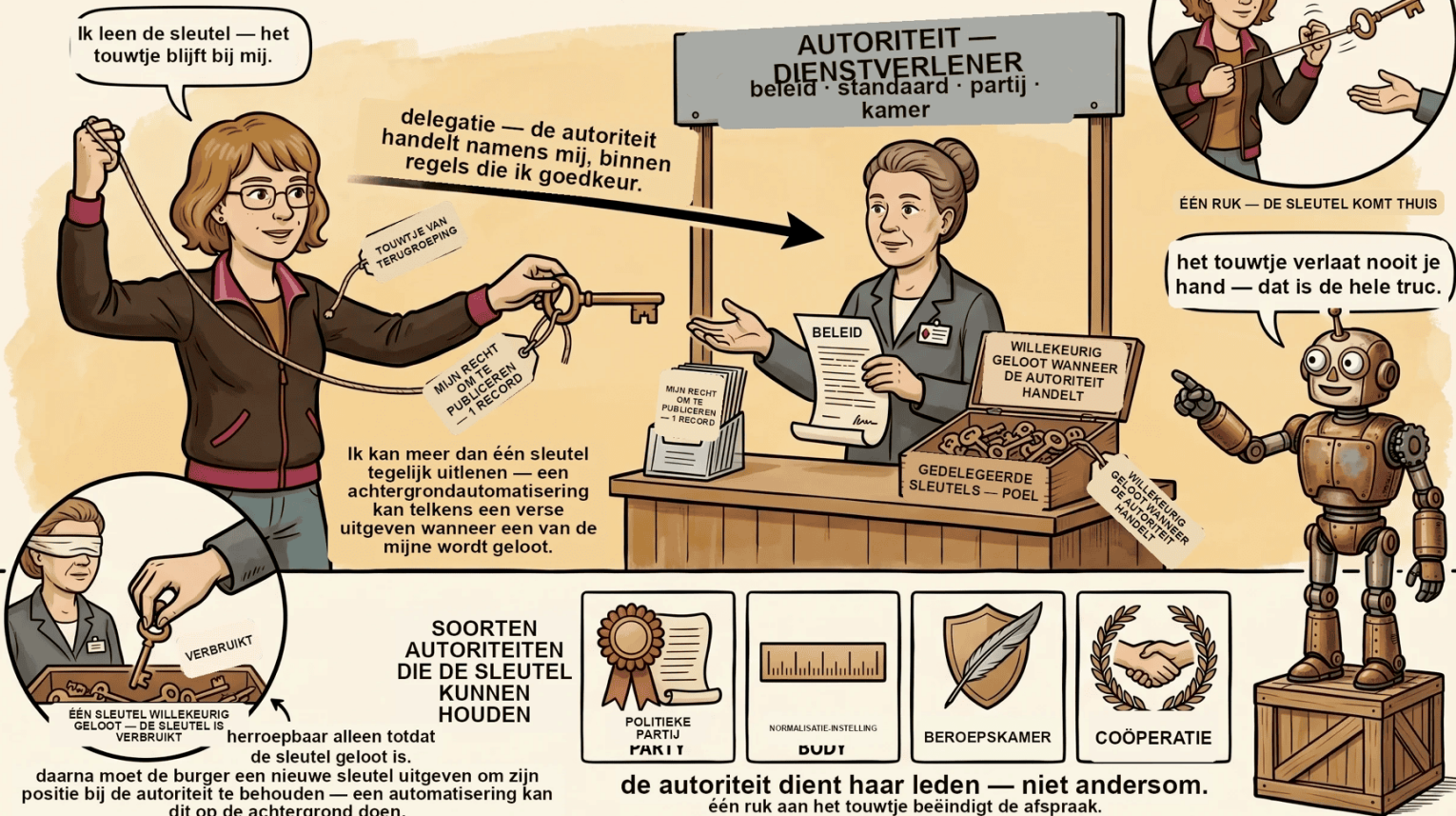


elke geeuw wordt een dossier — omdat tellen goedkoop is.
een nies, een aankoop, een wandeling naar huis na donker: alles gaat op het record, voorgoed.
niets is privé — het oog knippert nooit, en burens stoppen met praten.

VRIJHEID IS WAT IK WEIGER TE TELLEN — TOTALITARISME IS WAT IK ERMEE INSTEM TE VOLGEN.

DELEGATIE VAN PUBLICATIERECHTEN

JE LEENT DE SLEUTEL AAN EEN AUTORITEIT DIE JOU DIENT — EN TREKT HEM IN EEN OGENBLIK TERUG



LEEN DE SLEUTEL — HOUD HET TOUWTJE. DELEGATIE IS NOOIT OVERGAVE.

■ Vrijheid vs. totalitarisme

Een samenleving die het volume van gepubliceerde registraties bewaakt en beperkt, zal vrijer zijn; een samenleving met een overmaat aan registraties zal neigen naar totalitarisme. Men kan zich voorstellen dat het recht om registraties te publiceren aan iemand anders wordt gedelegeerd.

■ Culturele aanpassing

Mensen kijken over het algemeen graag op elkaars bord. Over beschavingen heen verschillen we in historische ervaring en bevolkingsdichtheid — en dus in hoeveel we op elkaars bord willen kijken binnen beschavingen en gemeenschappen. Aziatische staten neigen naar een strengere kijk op vrijheid in de samenleving; Europese en Amerikaanse, in bepaalde opzichten, naar een vrijere. Hoe onnauwkeurig deze parallel ook is, in de context van een gedecentraliseerd sociaal reputatienetwerk kan worden gezegd dat de instellingen van afzonderlijke gemeenschappen niet discrimineren, en dat elke gemeenschap de communicatie binnen zichzelf naar eigen goeddunken kan configureren.

Ondanks de verschillen zullen er standaarden zijn die over de hele planeet worden erkend (willekeurig doden is voor niemand goed). Andere instellingen zullen gemeenschapsspecifiek zijn, en nog andere zelfs persoonlijk specifiek. Het voordeel is dat via wederzijdse communicatie en door het observeren van de instellingen van iemands omgeving consensus kan worden gezocht — van bilaterale afspraken via die van gemeenschappen en, na verloop van tijd, dankzij de economische dominantie van de best geconfigureerde gemeenschappen, zelfs op globaal niveau.

Maar meer over consensus in het volgende hoofdstuk.

ELKE GEMEENSCHAP CONFIGUREERT ZICHZELF

HET NETWERK DISCRIMINEERT NIET — ELKE REGIO STELT ZIJN EIGEN KNOP IN



ÉÉN NETWERK, VELE KNOPPEN — ELKE GEMEENSCHAP BESLIST VOOR ZICHZELF.

Het orakelprobleem — een brug tussen de digitale en de fysieke wereld

De term “orakelprobleem” wordt de laatste tijd het vaakst geassocieerd met de wereld van cryptovaluta's, blockchains en gedecentraliseerde systemen. Algemeen: hoe zorg je ervoor dat gegevens die een digitaal systeem binnenkomen getrouw overeenstemmen met wat er werkelijk in de fysieke wereld is gebeurd? Het systeem zelf kan niet verifiëren of iemand werkelijk een ander schade heeft berokkend, of dat een contract echt is geschonden — het ziet alleen digitale registraties.

Hier lossen we dit op via autoriteiten — entiteiten die hun reputatie inzetten op de overeenstemming van de digitale registratie met de fysieke werkelijkheid. Hoe hoger de reputatie van de autoriteit, hoe geloofwaardiger de registratie.

DE DIGITALE EN FYSIEKE WERELD OVERBRUGGEN

DE AUTORITEIT DRAAGT DE WERKELIJKHEID OVER



De reputatie van de autoriteit maakt het digitale record betrouwbaar.

* Het systeem probeert het orakelprobleem niet op te lossen — het aanvaardt dat autoriteiten de brug zijn, en sluit aan bij hoe vertrouwen in de echte wereld al werkt.

* Als de brug de werkelijkheid verkeerd inschat, betaalt de autoriteit — met haar reputatie.

Hoe verificatie werkt

Consensus en het verificatieproces

Om consensus op te bouwen over welke regels een samenleving gemiddeld zou moeten handhaven en afdwingen, kan het volgende mechanisme helpen. Als DID-deelnemer verklaar ik de regels waarop ik inteken en waarnaar ik zal leven, en ik publiceer ze. (Zie het als de statuten en reglementen die naar mijn mening mijn ideale wereld uitmaken — een wereld waarin ik me niet beperkt voel, maar veilig.)

Ik kan vooraf inschatten hoe mijn DID-contacten zouden reageren — en beoordelen hoe sterk, en door wie, ik zou worden gesanctioneerd in gewone sociale of zakelijke interacties, mochten die hypothetisch plaatsvinden.

De definitieve beoordeling gebeurt wanneer je informatie opvraagt bij een andere DID, of hem vraagt een claim te verifiëren (of een autoriteit om een dienst vraagt, enzovoort) die je in het reputatienetwerk wilt publiceren. Het zou hetzelfde moeten uitpakken als wanneer je de beoordeling zelf uitvoert, in een dry run, tegen het verklaarde beleid van de tegenpartij — en als dat niet zo is, is er iets mis aan de kant van de tegenpartij: die probeert een oneerlijk spel te spelen.

De uitkomst is ofwel aanvaarding, met een geciteerde prijs voor verificatie (in het geval van diensten van een verificateur of autoriteit), ofwel afwijzing. Zowel sancties als bonussen voor afwijking van het beleid van de beoordelaar zijn in de geciteerde prijs verwerkt. De aanvrager beslist vervolgens of hij de voorwaarden aanvaardt, of doorgaat naar de volgende ronde van verificatie in het toewijzingsalgoritme — waarbij hij het proces herhaalt tot hij tevreden is, of tot de economie het zinloos maakt om door te gaan.

■ De sociale graaf

Het reputatienetwerk is bovenal een sociaal netwerk. Je voegt contacten toe — mensen die instemmen met de verbinding. Zij hebben contacten, en die contacten hebben contacten. Het algoritme zoekt verificateurs binnen een instelbare diepte (bijv. drie niveaus: je directe contacten, hun contacten, en één niveau daarbuiten). Er is geen globale blockchain nodig — het netwerk vormt vanzelf gemeenschappen met overlappingsen naar andere gemeenschappen.

Het algoritme is niet-deterministisch: het hasht je claimdocument, mapt de hash op een positie op een ring van bekende identiteiten binnen deze kring, en selecteert de dichtstbijzijnde als kandidaat-verificateur. Je kunt niet voorspellen of beïnvloeden wie je claim zal verifiëren.

Elke afwijzing door een verificateur vergroot je document en verhoogt de verwerkingskosten ervan — dat is het eerste kostenkanaal (documentgroei). Elke nieuwe verificateur rekent een vergoeding op basis van gegevensvolume, je reputatie, en hoever de inhoud van je claim afwijkt van zijn verklaarde verificatiebeleid — dat is het tweede kostenkanaal (risicopremie). En elke iteratie kost tijd en energie — het derde kostenkanaal.

■ Wat de verificateur controleert, in volgorde

Eenmaal geselecteerd, beoordeelt een verificateur een claim in grofweg vier geordende stappen — goedkoopste filters eerst, dure inhoudscontroles laatst:

1. **Beleidsafscherming.** Valt dit soort claim überhaupt binnen wat de verificateur publiek verifieert? Zo niet, dan wordt het verzoek regelrecht afgewezen.
2. **Vertrouwen in de autoriteit.** Is de autoriteit die de claim heeft geruggensteund voldoende vertrouwd onder het eigen verklaarde beleid van de verificateur? Een autoriteit onder de vertrouwensdrempel van de verificateur is grond voor afwijzing, ongeacht de inhoud van de claim.
3. **Reputatie van de uitgever.** Voldoet de uitgever aan de reputatiedrempels die de verificateur voor dit type claim heeft verklaard? Een lage reputatie kan ofwel de vergoeding verhogen ofwel afwijzing uitlokken.
4. **Inhoudscontrole.** Pas wanneer de eerste drie poorten worden gepasseerd, beoordeelt de verificateur de claim zelf — handtekeningen, interne consistentie, formele correctheid, en hoever ze afwijkt van het beleid van de verificateur. De vergoeding voor deze laatste stap weerspiegelt het werkelijk genomen risico.

De verificateur publiceert het beleid dat elk van deze poorten regeert, zodat de stappen niet aan zijn goeddunken zijn — hij is gebonden aan wat hij reeds heeft verklaard. Afwijking van het gepubliceerde beleid is zelf een publiceerbare claim tegen hem, en hij betaalt ervoor met zijn reputatie.

Het resultaat: een geloofwaardige en nuttige claim publiceren kost bijna niets. Een radicale claim publiceren kost meer. Een leugen publiceren wordt prohibitief duur — je moet verificateur na verificateur doorlopen, en iedereen die je afwijst voegt kosten toe. De markt beprijst je claim, en de prijs vertelt je waar je staat ten opzichte van de gemeenschappen waarin je beweegt.

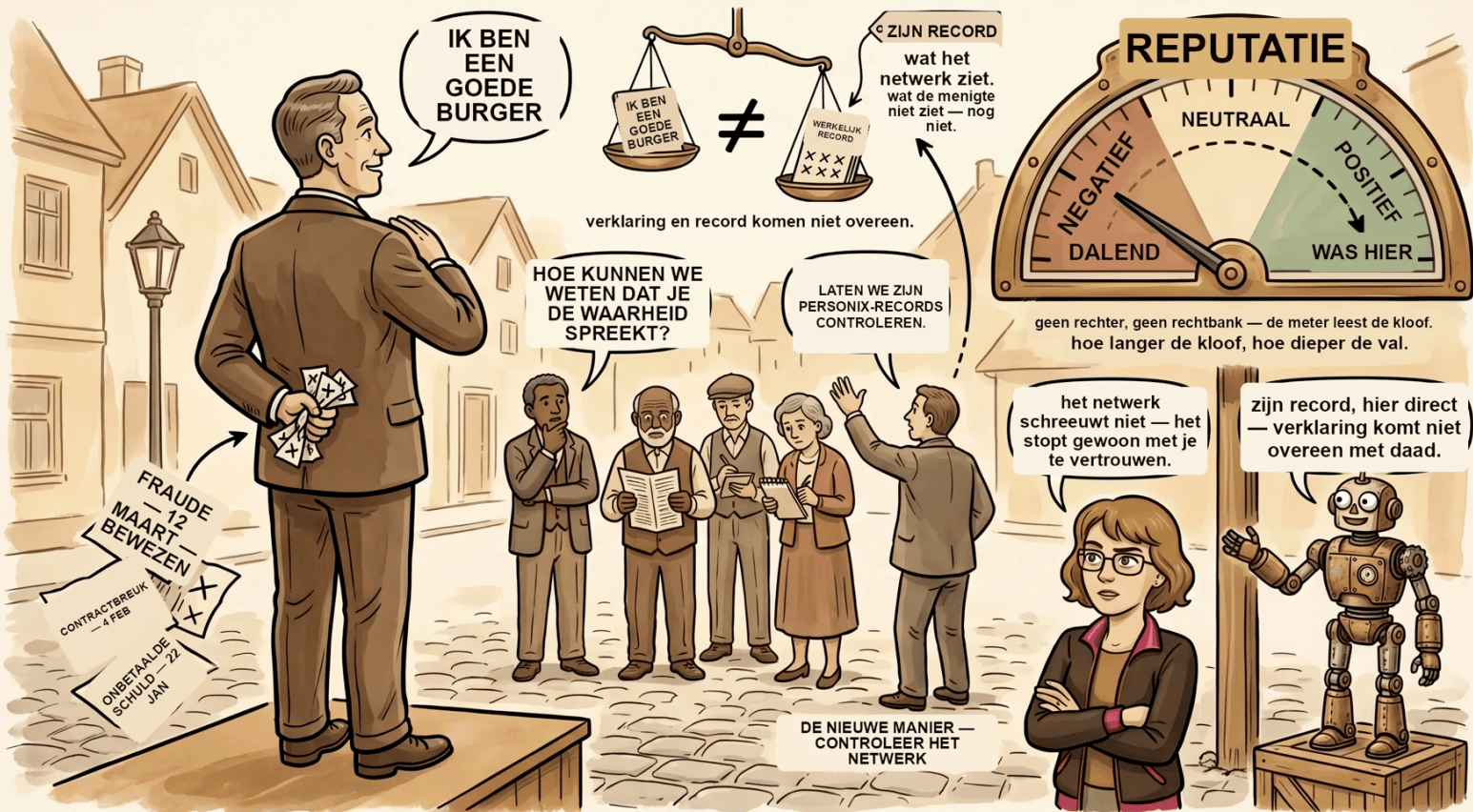
Het volstaat niet te verklaren dat je een regel naleeft terwijl je dat in werkelijkheid niet doet. In dat geval riskeert je DID de publicatie van een negatieve registratie die de hypocrisie blootlegt — wat je verandert in een risico voor iedereen. De uitkomst zou minder maar consistentere nageleefde regels moeten zijn, en een opschoning van die jungle van wetten en voorschriften waarin zelfs juridische professionals zich amper kunnen oriënteren.

Consensus vs. verantwoording

Opdat het netwerk als waardevolle informatiebron dient, zou een DID niet te radicaal moeten zijn — anders wijzen de anderen hem af. Maatschappelijke druk zal evenwicht zoeken, en pogingen om het te destabiliseren zullen waarschijnlijk worden bestraft.

HYPOCRISIE IS HET DUURSTE GEDRAG

HET NETWERK VERGELIJKT STILLETJES JE WOORDEN MET JE RECORD — DE KLOOF IS VOOR IEDEREEN ZICHTBAAR



VERKLAREN EN BREKEN? DE KLOOF IS HET DUURSTE GEDRAG.

HET GENEESMIDDEL VOOR HYPOCRISIE

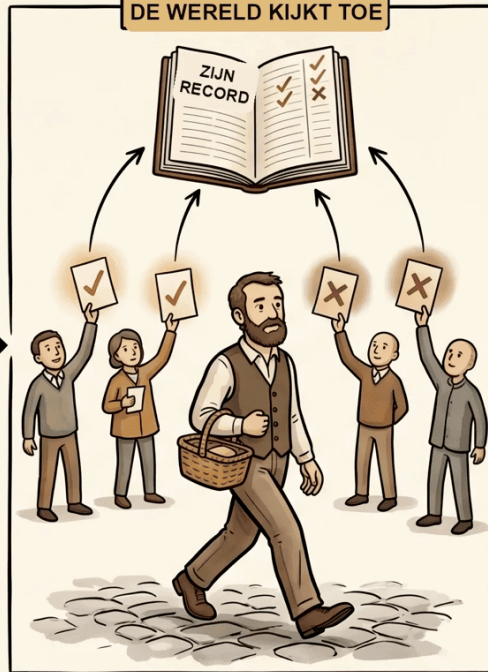
VERKLAAR JE REGELS — LEEF ERNAAR, OF DE MARKT PRIJST JE ERUIT

IK VERKLAAR MIJN BELEID



iedereen kan mijn standaarden lezen.
geen poortwachters, geen geheimen.

DE WERELD KIJKT TOE



de wereld schrijft op wat hij werkelijk doet.
elke dag een beetje meer bewijs op zijn grootboek.

IN DE WINKEL — JE BETAALT VOOR JE EIGEN RECORD



hypoocrisie wordt niet bestraft door een autoriteit — ze wordt betaald door de markt.
elke gewone dienst die je koopt draagt een toeslag gevormd door je eigen record.

zouden we dit het maatschappelijk contract kunnen noemen — opnieuw getekend?

geen autoriteit dwingt de ethiek af — de prijs doet dat.
zachte druk, elke dag, richting het gedeelde gemiddelde waar we allemaal mee kunnen leven.

DOE WAT JE ZEGT — OF BETAAL ERVOOR. HYPOCRISIE IS DE DUURSTE REPUTATIE.

■ Het aantal stemmen is niet hetzelfde als het gewicht van een stem

Juraj Karpiš zegt dat “geld het geheugen van goede daden is.” Ik zou daaraan toevoegen dat reputatie het geheugen van de slechte is.

Daaruit volgt dat, meritocratisch, wie meer bijdraagt en geen slechte reputatie heeft een groter gewicht van stem in de gemeenschap verdient. Bekeken door de lens van bilaterale relaties: wanneer ik afweeg aan welke consensusdruk ik tegemoetkom, gaat het grootste gewicht naar de relaties waaruit ik het grootste economische voordeel haal. Tien mensen met wie ik geen actieve handel drijf, zullen mij veel minder beïnvloeden dan één vaste zakenpartner. Dit paradigma is niet beperkt tot handel — het strekt zich uit tot sociale, politieke en andere relaties.

Roles in the verification transaction and authorities

Overzicht van de rollen

We hebben sommige van deze rollen al kort aangeraakt in het hoofdstuk over het netwerk en zijn basiseigenschappen. Nu is het tijd ze opnieuw en gedetailleerder te bekijken en de bijkomende toe te voegen die we nodig hebben om het netwerk robuuster te maken. Bij elke verificatietransactie zijn verscheidene rollen betrokken — laten we zien hoe ze zich gedragen.

■ Rollen in een verificatietransactie

Bij elke verificatie zijn tot zes verschillende rollen betrokken, samengevat in de tabel hieronder. Ze kunnen allemaal hun eigen DID in het gedecentraliseerde reputatienetwerk hebben.

Rol	Beschrijving
Uitgever	De persoon die informatie in het netwerk publiceert — beweert dat er iets is gebeurd (een DID is aangemaakt, bewerkt of ontbonden, een claim, het beleid van een gegeven DID enz.)
Subject	De persoon over wie de informatie gaat — de geadresseerde van de claim
Autoriteit	Een vertrouwde entiteit die haar naam inzet op de kwaliteit van de claim door die te onderzoeken en ofwel het overgelegde bewijs te toetsen ofwel het actief te verzamelen
Waarnemer	Een onafhankelijke derde die bijhoudt hoe de verificateur met de claim omgaat — die ervoor zorgt dat de verificateur niet zwijgt en niet afwijkt van het beleid dat hij heeft verklaard
Verificateur	Een algoritmisch geselecteerde deelnemer die de transactie verwerkt
Gemachtigde	Een persoon die handelt namens een andere deelnemer

Uitgever

De uitgever zijn we eerder tegengekomen. Wanneer iemand onrecht wordt aangedaan, of wanneer hij een eigen prestatie wil uitdragen, is het de door de DID vertegenwoordigde persoon die het proces in gang zet om die informatie in het netwerk te plaatsen — omdat hij er het primaire belang bij heeft (de motivatie zijnde ofwel een verlangen naar genoegdoening, ofwel de wens zijn publieke imago te verbeteren).

DE UITGEVER — WIE DE CLAIM SCHRIJFT

AUTEUR · ONDERTEKENAAR · ZET ZIJN EIGEN REPUTATIE IN

WAT DE UITGEVER DOET

1. Schrijft de claim in eigen woorden
2. Verzamelt bewijs uit de echte wereld om het te staven
3. Ondertekent met eigen DID en stuurt naar de gekozen autoriteit
4. Betaalt de publicatiekosten
5. Draagt de gevolgen als hij liegt

MIJN REPUTATIE



Als dit onwaar is,
daalt mijn naald.

Mijn naam komt hierop
te staan. Ik kan het maar
beter zeker weten — en
bewijs meebrengen.

Iedereen mag spreken.
Leugens kosten de
spreker.



De uitgever is de auteur. Zijn naam staat erop.

* Iedereen met een DID kan uitgever zijn. De lat is moed en verantwoording, geen vergunning.

■ Positieve claims

Positieve claims over mezelf kan ik, als zowel hun subject als hun uitgever, bewaren voor de situaties waarin ik ze wil gebruiken (een diploma, een bewijs van bewezen dienst enz.). Hierin verschilt een positieve claim van een negatieve: het delen van een geverifieerde negatieve claim is in het belang van de hele gemeenschap, terwijl een positieve in het belang van de drager ervan is.

Autoriteit

De autoriteit speelt een dubbele rol: ze kan een **auditor** zijn (die de kwaliteit van het bewijs verifieert voordat een claim wordt gepubliceerd) of een **garant** (die haar reputatie inzet op de waarachtigheid van een claim). In beide gevallen versterkt ze de claim van de uitgever. Deze twee diensten zijn scheidbaar — een autoriteit kan de ene, de andere, of beide tegelijk aanbieden. De werkaanname is dat de meeste diensten die autoriteiten leveren op basis van de vrije markt kunnen worden geleverd. Dat geldt zelfs in domeinen die moeilijk voor te stellen zijn als geprivatiseerd, zoals justitie, waar gespecialiseerde diensten — onderzoek, beoordeling van bewijs, tot en met diensten die vandaag door gecentraliseerde legers worden geleverd (strategische planning, gestandaardiseerde training, aankoop en beheer van voorraden enz.) — efficiënt door marktactoren kunnen worden geleverd. Er is nauwelijks iets dat, na herstructurering, niet efficiënter zou kunnen worden gemaakt door prikkels van de vrije markt.

■ **De autoriteit, de uitgever en de waarnemer mogen nooit de verificateur van hun eigen zaak zijn.**

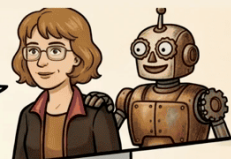
Algoritmische selectie van de verificateur garandeert onafhankelijkheid. Niemand kan zijn eigen claim verifiëren, of een claim waarbij hij een direct belang heeft. Dit is een van de basisregels die de hele gemeenschap van DID's er belang bij heeft te handhaven.

De volgende grafieken tonen complementaire beelden van de breedte van activiteit die autoriteiten bestrijken (de term “autoriteit” kan uitwisselbaar worden gelezen met “dienstverlener”).

DE GIDS — HELPT JE NAVIGEREN OP JOUW WAARDEN

DIEPE ANALYSE ACHTER · EENVOUDIGE GELEIDING VOOR

Zij voegt de complexe wereld samen tot aanbevelingen. Volgers stemmen met hun aandacht — vertrek wanneer je wilt, wissel naar een ander.



GIDS

MIJN ANALYSE

Werknotities — niet voor cliënten

overheidsuitgaven
- omgeleid



	aanbieders
1	70M ★★★★★
2	70M ★★★★★
3	70M ★★★★★
4	70M ★★★★★

VOOR JOU — WAT HET BETEKENT

Samengevoegd om jouw voordeel te maximaliseren

- verschuif uitgaven hierheen, bespaar daar
- steun aanbieders die mijn tests doorstaan
- neem dit beleidssjabloon over



Ik doe het complexe werk. Jij krijgt de eenvoudige aanbeveling — alleen als je mijn waarden deelt.

En wat krijg ik precies voor mijn geld — welke analyses en welke overzichten?

bijvoorbeeld: wie een gids kan zijn

- een politieke partij of beweging die een beleidssjabloon publiceert
- een onafhankelijk auditbureau dat samengevoegde bevindingen publiceert
- een dienstenvergelijkingsbureau
- een reputatie-aggregator (economisch · zakelijk · buurt · verkeersveiligheid)
- een journalist-recensent of consumentenreviewdienst

VOLGER VAN DEZE GIDS — JAARLIJKS VERLENGBAAR

Gebonden aan waar ze publiekelijk voor staan. Jouw vertrouwen is hun valuta.

* Je kunt op elk moment vertrekken en naar een andere gids wisselen. Je vertrouwen zit niet vast.

* De gids kan ook enkele eigen claims ondertekenen — gepubliceerd, maar hier niet het hoofdverhaal.

■ Autoriteit als incognito waarnemer

Een gerespecteerde autoriteit — denk aan een notaris wiens zaak uitsluitend afhangt van zijn track record — kan, naast de hoofdfuncties (auditor / garant), een derde aanbieden: de rol van incognito waarnemer tijdens de verificatie. Ze houdt een van een tijdstempel voorziene registratie bij van de ingediende claim zodat de verificateur die niet stilletjes kan laten vallen. Het mechanisme van de waarnemersrol wordt verder beschreven in het onderdeel over de rol van de waarnemer.

Verificateur

Elke DID kan optreden als verificateur, hetzij rechtstreeks, hetzij via verificatierechten die aan een derde DID zijn gedelegeerd. Om mij — of mijn gemachtigde — in staat te stellen te verifiëren, zou ik bereikbaar moeten zijn op het netwerk (online). Niet iedereen zal zich daaraan willen binden, en daarom kan een DID-registratie, in volgorde van prioriteit, de vervangers opsommen die de functie namens haar zullen vervullen terwijl ze offline is.

Elke DID die actief is in het netwerk verklaart publiek zijn eigen beleid. Via de in dat beleid gedefinieerde regels beoordeelt hij tijdens het verificatieproces de reputatie van de tegenpartij en de inhoud en vorm van de claim die de uitgever voor publicatie in het reputatienetwerk heeft aangemerkt. Deel van het beleid is de rekenformule die wordt gebruikt om vergoedingen voor verificatiediensten te berekenen. Zodra dat op zijn plaats is, wacht ik over een statistisch groot aantal claims dat door het netwerk stroomt tot het algoritme van het netwerk mij aan de kant van de uitgever trekt en mij, in een gegeven iteratie, toewijst om de uit te geven informatie te verifiëren. De uitgever kan vooraf berekenen

DE AANBIEDER — RUNT EEN CLAIM-ONDERTEKENINGSDIENST

GEPUBLICEEERDE STANDAARDEN · GEPUBLICEEERDE PRIJZEN



Gebonden aan wat ze publiekelijk verklaren. Reputatie doet de rest.

* De aanbieder heeft ook een eigen beleid — wanneer ze accepteren, wanneer ze afwijzen, hoe ze terugbetalen. Het is gepubliceerd, maar het is hier niet het hoofdverhaal.

hoe een correct handelende verificateur zou reageren, maar kan niet vermijden hem (of zijn vervangers) daadwerkelijk te contacteren; de iteratie met de geselecteerde verificateur moet door de uitgever worden uitgevoerd, ook wanneer hij vooraf weet dat ze niet zal slagen.

Hoe weten we dat de uitgever het verificateurselectie-algoritme uitvoert over de juiste verzameling kandidaat-verificateur-DID's? Samen met zijn publiek verklaarde beleid publiceert elke DID ook de actuele lijst van identifiers van zijn sociale netwerk binnen het reputatienetwerk. Als een uitgever zijn sociale netwerk definieert als een sociale bubbel die louter zijn eigen opvattingen weerkaatst en versterkt, zal informatie die er doorheen wordt gepubliceerd nauwelijks breder worden ontvangen door andere gemeenschappen. Het feit dat het mij lukt, tegen hoge kosten, een radicale claim in het netwerk te duwen, impliceert niet dat ik er, bij het beoordelen van de reputatie van de tegenpartij, enig gewicht aan zal geven. Sommige claims word ik door mijn gemeenschap gedwongen in aanmerking te nemen (straffen en beperkingen opgelegd aan overtreders); andere zijn geheel aan mij — ik beslis zelf de economische waarde van het opnemen of uitsluiten van een gegeven stuk informatie.

Subject

Zij op wie de in het reputatienetwerk gepubliceerde informatie betrekking heeft, zijn de dragers ervan, of, zo je wilt, de subjecten ervan. De prikkels in het reputatienetwerk zijn zo ingericht dat het subject alle reden heeft zich correct en eerlijk naar zijn eigen regels te gedragen, en door de gemeenschap wordt geduwd naar een gulden middenweg van regelnaleving. Ze hebben zelfs een prikkel om zich moreler te gedragen dan hun verklaarde regels vereisen — vooraf verklaarde beleidslijnen sluiten niet uit dat de gemeenschap tot een consensus komt om een of andere beoordeling of maatregel met terugwerkende kracht toe te passen. Vanuit deze hoek wordt het reputatienetwerkalternatief voor een rechtsorde, zoals te verwachten valt, meer gedreven door de geest van de regels dan door de letter.

DE VERIFICATEUR — TOETST DE CLAIM AAN GEPUBLICEERD BELEID

VIER POORTEN, OP VOLGORDE. GOEDKOPE FILTERS EERST.

Hij mag niet creatief zijn. Hij moet doen wat zijn beleid zegt.

Zijn eigen regels. Publiek. Hij kan ze niet stiltejes veranderen.

VERIFICATIEPOORTEN — OP VOLGORDE

1. BELEIDSFILTERING

Verifieer ik dit soort claim überhaupt?

2. VERTROUWEN AUTORITEIT

Ligt de autoriteit boven mijn drempel?

3. REPUTATIE UITGEVER

Voldoet de uitgever aan mijn reputatiedrempel?

4. INHOUDSCONTROLE

Handtekeningen, consistentie, afwijking van beleid

KAN NIET ZIJN:
uitgever,
autoriteit,
waarnemer of
subject.

REPUTATIE
VERIFICATEUR

AFWIJKEN VAN
BELEID → REPUTATIE
DAALT → GEEN
TOEKOMSTIGE
LOTINGEN

WAT DE VERIFICATEUR DOET

1. Filtert via zijn gepubliceerde beleidspporten (op volgorde)
2. Controleert vertrouwen autoriteit, dan reputatie uitgever
3. Beoordeelt de inhoud van de claim alleen als de poorten slagen
4. Rekent een tarief evenredig aan het risico
5. Zet zijn eigen reputatie in bij elke beslissing

TARIEF
RISICO $\propto$

meer risico → hoger tarief

Goedkope filters eerst. Dure inhoudscontrole als laatste.

De verificateur is gebonden aan de regels die hij zelf publiceerde — en aan de reputatie die hij dreigt te verliezen.

HET SUBJECT — DEGENE WAAR DE CLAIM OVER GAAT

ONTVANGT HEM · KAN HEM NIET HET ZWIJGEN OPLEGGEN · KAN EROP ANTWOORDEN



Het subject heeft geen veto — alleen het recht om te antwoorden.

* Een tegenclaim is zelf een claim — de reputatie van het subject staat op het spel voor wat het in antwoord zegt.

Waarnemer

De waarnemersrol neemt de prikkel voor de verificateur weg om de regels te buigen. In situaties waarin een verificateur het verzoek van de uitgever of de autoriteit niet zint, zou hij eenvoudig kunnen zwijgen — niet antwoorden en de algoritmische reeks blokkeren. De waarnemer — of een verzameling waarnemers — zet zijn reputatie in op het documenteren van hoe de verificateur werd bevraagd. Als de verificateur zwijgt ondanks een verklaard beleid dat anders zegt, kan hij worden veroordeeld voor het schenden van het protocol.

Het mechanisme: tijdstempel en uitdagingscode

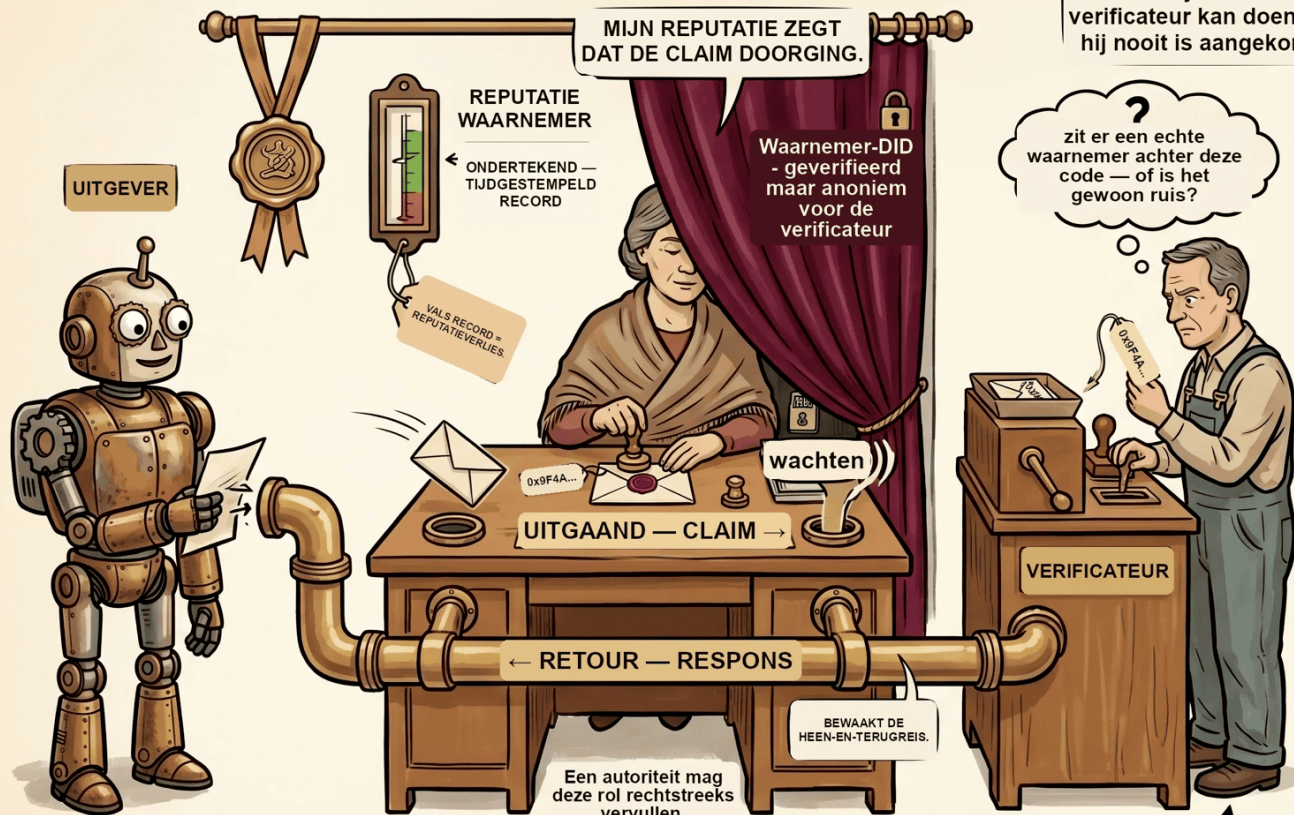
Voordat je een claim naar de verificateur stuurt, route je die via waarnemers — mensen die je vertrouwt, of gespecialiseerde aanbieders van waarnemersdiensten die een kleine vergoeding rekenen. Elke waarnemer ontvangt je inzending, voorziet die van een tijdstempel, ondertekent dat hij haar zag uitgaan, en genereert een uitdagingscode — een cryptografische hash van zijn handtekening. De codes worden aan je verzoek toegevoegd. De verificateur ziet ze, maar heeft geen idee wie de waarnemers zijn, of de codes zelfs echt zijn. Waarnemers treden zo op als proxy's tussen de uitgever en de verificateur, en houden een onafhankelijke registratie dat de claim werd ingediend en wat die bevatte. Er kunnen er nul tot N zijn.

Wanneer de verificateur zich eerlijk gedraagt — aanvaardt of afwijst in lijn met zijn verklaarde beleid — blijven de codes ondoorzichtig. Niemand wordt blootgesteld.

Maar als de verificateur zwijgt ondanks een meegaand beleid, of antwoordt op een manier die in tegenspraak is met wat hij heeft gepubliceerd, dan houd je de oorspronkelijke waarnemershandtekeningen. Je kunt ze publiceren als proxy-getuigenis dat de claim werd ingediend en dat de verificateur het protocol niet volgde. Iedereen kan verifiëren dat de handtekeningen overeenkomen met de uitdagingscodes.

DE WAARNEMER — EEN PROXY DIE DE CLAIM DOORGEEFT EN DE HEEN-EN-TERUGREIS BEWAAKT

DE VERIFICATEUR PRAAT MET HAAR. DE VERIFICATEUR KOMT NOOIT TE WETEN WIE ZE IS — OF ÜBERHAUPT IEMAND TOEKIJKT.



Anoniem voor het publiek, verantwoording verschuldigd aan het netwerk. De verificateur ziet de code, nooit de waarnemer.



WAT DE WAARNEMER DOET

1. Ontvangt de claim van de uitgever
2. Stempelt hem met haar eigen zegel; de stempel is het tijdstempelde record
3. Stuurt hem namens de uitgever door naar de verificateur
4. Kijkt of de respons terugkomt, en wat die zegt
5. Publiceert haar handtekening alleen als de verificateur zich misdraagt — haar reputatie is de garantie

voetnoten

* Het is niet de bedoeling dat waarnemers achter elk verzoek zitten. De verificateur ziet alleen ondoorzichtige codes en weet nooit of een echte waarnemer toekijkt of dat het gewoon ruis is. Die onzekerheid is de prikkel om zich te gedragen.

* Symmetrisch mag de verificateur de respons via zijn eigen waarnemer routeren — dezelfde truc, tegenovergestelde richting.

ZIET DE CODE —
ZIET NIET WIE.

De clou: je hebt geen echte waarnemers nodig

En hier komt het meest elegante deel: **je hebt helemaal geen echte waarnemers nodig**. Je kunt willekeurige getallen genereren die er precies uitzien als uitdagingscodes. De verificateur kan het verschil niet zien — hij moet gokken of hij zijn reputatie riskeert. Achter elk verzoek dat hij ontvangt zou een gerespecteerde waarnemer incognito kunnen meekijken — of het zou puur ruis kunnen zijn. De verificateur weet het niet. En die onzekerheid is het mechanisme.

De kosten om eerlijke druk te handhaven: bijna nul (willekeurige getallen zijn gratis). De potentiële kosten van oneerlijkheid voor de verificateur: catastrofaal. Eerlijk gedrag wordt geprikkeld, zelfs wanneer niemand daadwerkelijk kijkt.

Het systeem werkt omdat iedereen een beetje paranoïde is. Onzekerheid is goedkoper dan toezicht.

■ Meerdere verificateurs in één iteratie

Een versterkende begeleidende regel voor de beschikbaarheid van verificateurs kan een algoritmische uitbreiding zijn die, in één iteratie, een verzameling kandidaat-verificateurs teruggeeft in plaats van slechts één.

Delegatie

De beschaving heeft haar economische groei gebouwd op het vermogen tot arbeidsverdeling en specialisatie. De wereld in al zijn pracht is complex, en onze kans om die in al zijn complexiteit te bevatten is

DE BLUF DIE DE VERIFICATEUR EERLIJK HOUDT

EEN ECHTE WAARNEMER EN EEN WILLEKEURIGE BLUF ZIEN ER VANAF HET BUREAU VAN DE VERIFICATEUR IDENTIEK UIT

UITGEVER — KAMILA



ECHTE WAARNEMER



UITDAAGCODE —
HASH VAN
TIJDGESTEMPELD
RECORD

ONDERTEKENDE
UITDAGING

VERIFICATEUR

houdt iemand bij
wat ik hier doe? ik
weet het niet — dus
ik gedraag me.



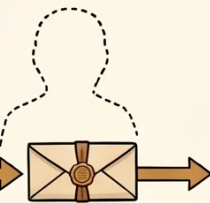
de verificateur kan een echt record niet van een bluff onderscheiden. eerlijk gedrag is de enige veilige gok.

UITGEVER — BLUFFEND



WILLEKEURIG GETAL

GEEN WAARNEMER



ZIET ER
HETZELFDE UIT.
KOSTEN: NUL.

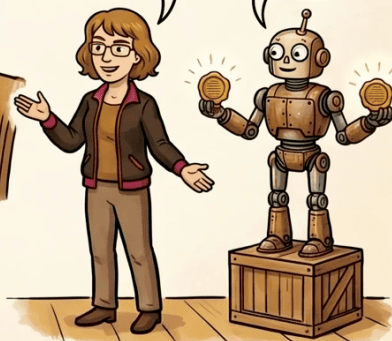
VERIFICATEUR — ZELFDE GEDRAG

houdt iemand bij wat ik
hier doe? ik weet het niet
— dus ik gedraag me.



de verificateur
kan ze niet uit
elkaar houden.

wie kan het
verschil zien?



kosten van eerlijkeheidsdruk: bijna nul — willekeurige getallen zijn gratis.
kosten van betrappt worden bij het smoren van een claim: catastrofaal — reputatie vernietigd.

ONZEKERHEID IS GOEDKOPER DAN SURVEILLANCE.

bijna nul. De natuurlijke uitweg is het delegeren van een breed scala aan activiteiten die een comfortabel leven ondersteunen aan gespecialiseerde aanbieders, die ons tijd, energie en geld besparen, en ons op onze beurt laten specialiseren — het leveren van de diensten waar we het best in zijn, of die de markt het hoogst in ons waardeert.

Dezelfde logica van delegatie strekt zich uit tot in het reputatienetwerk. In het hoofdstuk De schakeelaar tussen vrijheid en totalitarisme (en delegatie) hebben we de principes uiteengezet voor het beschermen van een vrije samenleving door het aantal claims dat binnen een gegeven tijdvenster in het netwerk kan worden gepubliceerd te beperken (denk, in vereenvoudigde termen, aan publicatierechten in lage enkele cijfers per jaar, zodat de samenleving maximaal vrij blijft). Dit principe kan worden uitgebreid naar meerdere dimensies. We hoeven niet slechts één getal te hebben — we kunnen verscheidene limieten hebben, die op verschillende soorten claims van toepassing zijn. We kunnen een ander getal gebruiken voor het aanmerken van andermans hypocrisie dan voor wangedrag in zakelijke transacties, en, zeg, een wijziging van het DID-document zoals een wachtwoordwijziging is iets waar de gemeenschap zich amper om zal bekommeren, enzovoort. Het hangt allemaal af van hoe de gemeenschap, over evolutionaire tijd, definieert wat haar belangen dient bij het vinden van de juiste balans tussen haar beoogde niveau van vrijheid en verantwoording.

Waarom zou het aantal publicatierechten dat de gemeenschap mij verleent klein genoeg moeten zijn? Een DID (subject) aanmerken met een negatieve claim vernietigt reputatie die lang duurde om op te bouwen, en de schade blijft. Een vernietigde reputatie staat een schaal van escalerende sancties van de gemeenschap te wachten voor elke verdere of herhaalde overtreding, tot en met de volledige eliminatie van de verstorende entiteit (het extreme geval). Een exponentieel escalerende schaal van straf heeft geen groot volume aan claims nodig, mits ze door verifieerbaar bewijs worden geschraagd. Dit geldt voor de vreedzame stabiele toestand, wanneer de samenleving niet wordt geschud door een ramp (extern of intern).

Voor gebeurtenissen met zeer lage waarschijnlijkheid is de statistische frequentie volatiel wanneer ze op een individu wordt toegepast. Over de populatie van de gemeenschap is ze dat niet. Dat is de waarde van het delegeren van iemands publicatierechten aan gespecialiseerde samenbrengende autoriteiten, die — net als onderlinge verzekering bij een schadegeval — jouw recht gebruiken en het namens jou toepassen. Laten we minder abstract spreken en een paar voorbeelden geven: - het opsporen en bestrijden van georganiseerde misdaad - het afdwingen van commerciële overeenkomsten - het beheren van voorrechten (bewijzen van opleiding, verwervingen / vervreemdingen van bezittingen enz.) - enzovoort

DE GEDELEGEERDE — EEN CLAIM-DIENST WAAROP JE JE ABONNEERT

DELEGEER WAT JE ZELF NIET AANKUNT · HOUD WAT ERTOE DOET VOOR JOU



Besteed uit wat je zelf niet aankunt. Blijf op de hoogte. Trek de rechten op elk moment terug.

* Als de gedelegeerde buiten het afgesproken bereik handelt, worden zowel zijn reputatie als de jouwe publiekelijk geraakt.

■ Hoe “publicatierechten” werkelijk werken

De grafiek voor de gemachtigde toont publicatierechten als fysieke tokens ter verduidelijking, maar in het systeem bestaat zo’n object niet. Wat er werkelijk gebeurt is dit: het beleid van de mensen bij wie je in een goed blaadje wilt blijven — jouw gemeenschap — aggregeert tot een emergente regel over hoeveel claims per jaar ze als relevant van je zullen aanvaarden voordat ze je als ruis gaan behandelen. Het plafond bestaat zodat het netwerk niet wordt overspoeld met triviale “wat als”-claims en zo vrij blijft als de gemeenschap wil (signaal behouden door het volume te beperken).

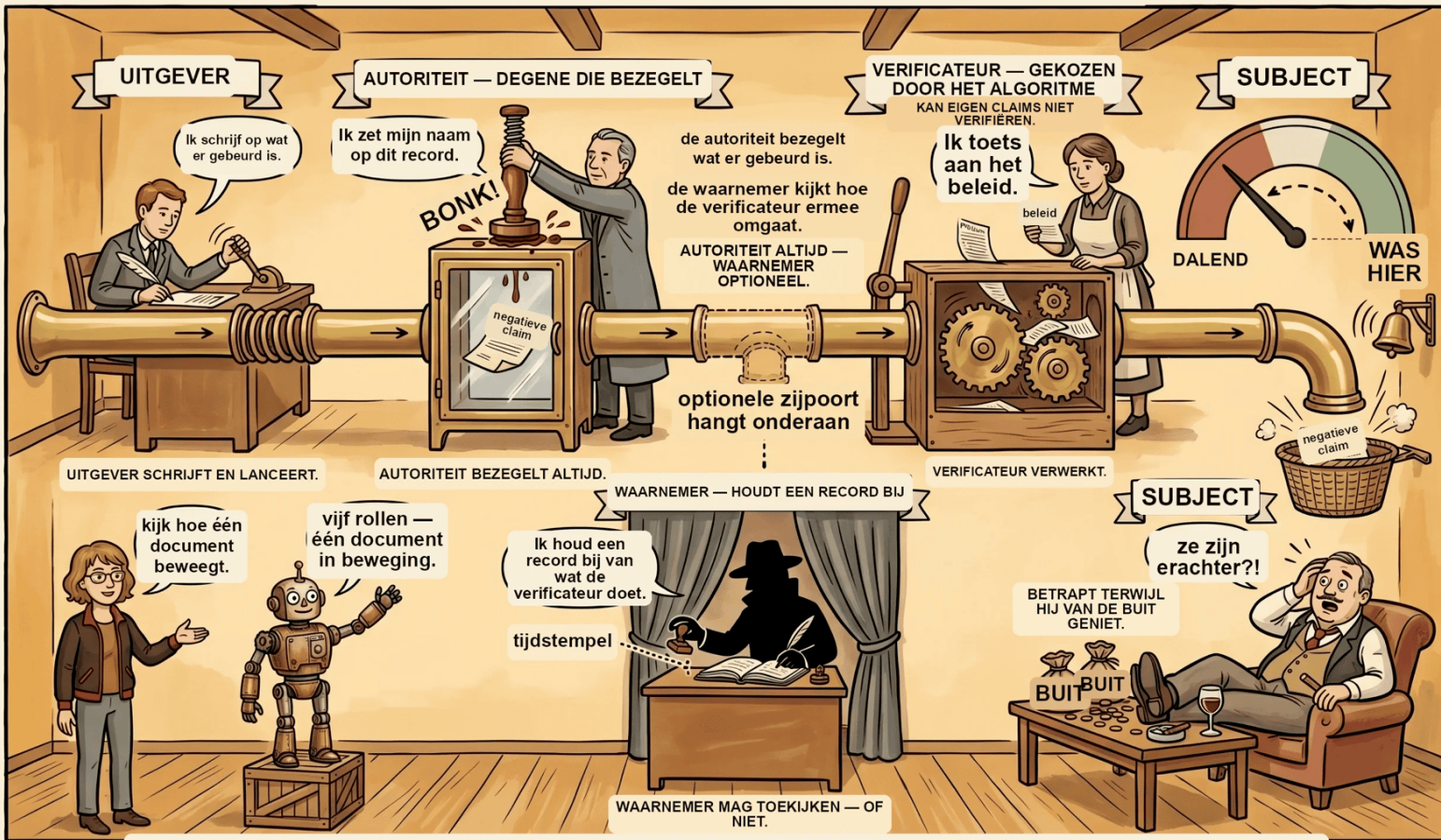
Je leest wat je gemeenschap je toestaat. Er is een bereik, met enige spreiding afhankelijk van welke mensen je het zwaarst weegt. Je beslist vervolgens — binnen die toelage — hoeveel claims je zelf publiceert, en hoeveel je delegeert aan professionele diensten die namens jou zullen publiceren, maar alleen wanneer gebeurtenissen binnen hun bereik vallen. Dit is wat je in een goed blaadje houdt zonder je te dwingen een claim in te dienen voor elk klein dingetje dat je overkomt.

De “tokens” in de grafiek zijn een visuele plaatsvervanger voor deze lees-en-beslis-lus, geen letterlijk artefact.

Het is waardevol om gedelegeerde publicatierechten in het reputatienetwerk te kunnen intrekken. Dit kan op elk moment, zolang de gemachtigde het gedelegeerde recht nog niet heeft gebruikt.

EEN NEGATIEVE CLAIM STROOMT DOOR HET SYSTEEM

VOLG ÉÉN DOCUMENT — ZIE WAT ELKE ROL ERMEE DOET



VIJF ROLLEN, ÉÉN DOCUMENT IN BEWEGING — NIEMAND KAN ZICHZELF VERIFIEREN.

Communicatie tussen rollen

De grafiek hieronder vat samen hoe de rollen in een echt geval met elkaar verbonden zijn — van de indiening van een claim door de uitgever tot en met de publicatie in het reputatienetwerk.

Het emergente maatschappelijk contract — beleid

Tot nu toe hebben we beschreven hoe claims worden geverifieerd en welke rol elke rol speelt. Nu wenden we ons tot hoe duizenden individuele beleidslijnen iets worden dat werkt als een echt maatschappelijk contract. Niets dat lijkt op de linkse dromen van een maatschappelijk contract en afgedwongen solidariteit.

Elke deelnemer verklaart zijn eigen beleid op basis van zijn moraal (policy) — wat hij aanvaardbaar acht, en hoe hij reageert op specifiek gedrag van anderen. Het geheel van alle beleidslijnen over het netwerk die aan een gegeven DID bekend zijn (de gemeenschap) brengt emergente ethiek voort — waarneembare normen die niemand heeft ontworpen. Deze emergente normen, geschraagd door bilaterale prijssignalen, vormen een meetbaar maatschappelijk contract: geen theoretisch construct dat niemand bij zijn geboorte heeft ondertekend, maar empirisch waarneembare regels geruggensteund door daadwerkelijk gedrag.

■ Het maatschappelijk contract

Mensen debatteren of “maatschappelijk contract” geen oxymoron is. Niemand ondertekent iets, en toch wordt het ingeroepen om wetgevend en uitvoerend handelen in gecentraliseerde samenlevingen te rechtvaardigen.

Een fenomenologische analyse van interacties in een gedecentraliseerd netwerk zou bepaalde emergente regels kunnen onthullen — globaal of lokaal. Hoe zouden we deze breed gedeelde normen moeten noemen? Een maatschappelijk contract? Net als bij gemeenschappen kan het maatschappelijk contract van een gemeenschap niet nauwkeurig worden waargenomen en afgebakend — elke invalshoek op de gemeenschap levert een ander maatschappelijk contract op.

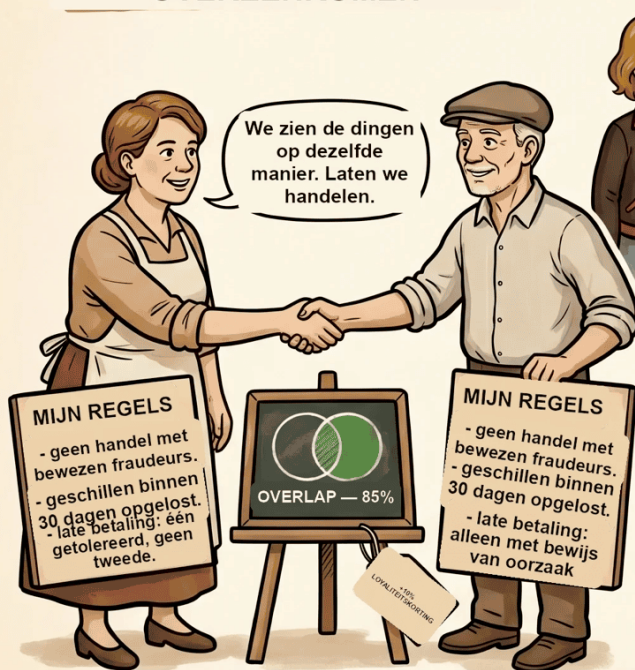
■ Op waarden gebaseerd beleid

Het is even misleidend om “op waarden gebaseerd beleid” te behandelen als de grondslag van besluitvorming. Waarden zijn meer als fenomenologische clusters van regels die op een gegeven moment gewoonlijk de voorkeur genieten. Ze evolueren, en ze zijn niet constant in de tijd.

BELEIDSREGELS ONTMOETEN. HOUDINGEN ONTSTAAN.

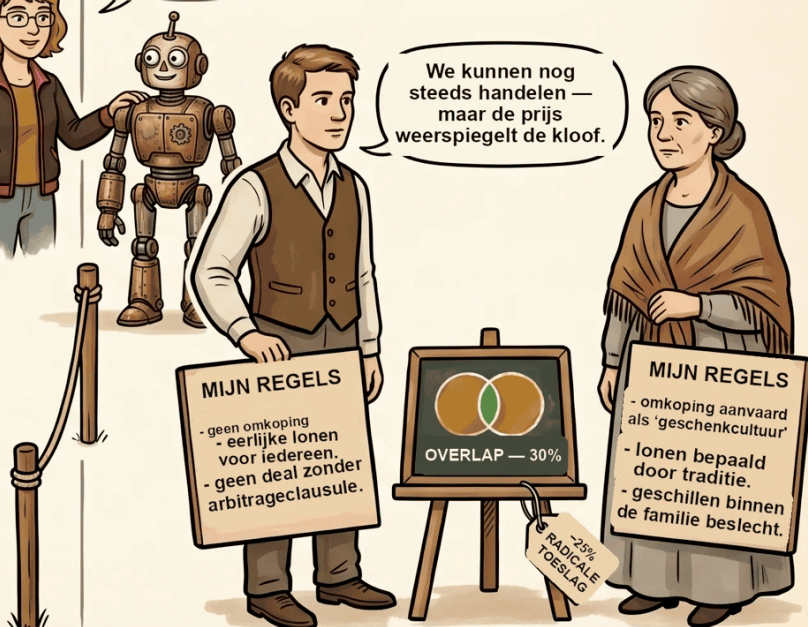
VERKLAARDE REGELS BEPALEN DE PRIJS VAN VANDAAG — KORTING VOOR AFSTEMMING, TOESLAG VOOR AFWIJKing

WANNEER BELEIDSREGELS OVEREENKOMEN



Zelfde goederen, twee prijzen. Verklaringen — niet reputatie — bepalen het.

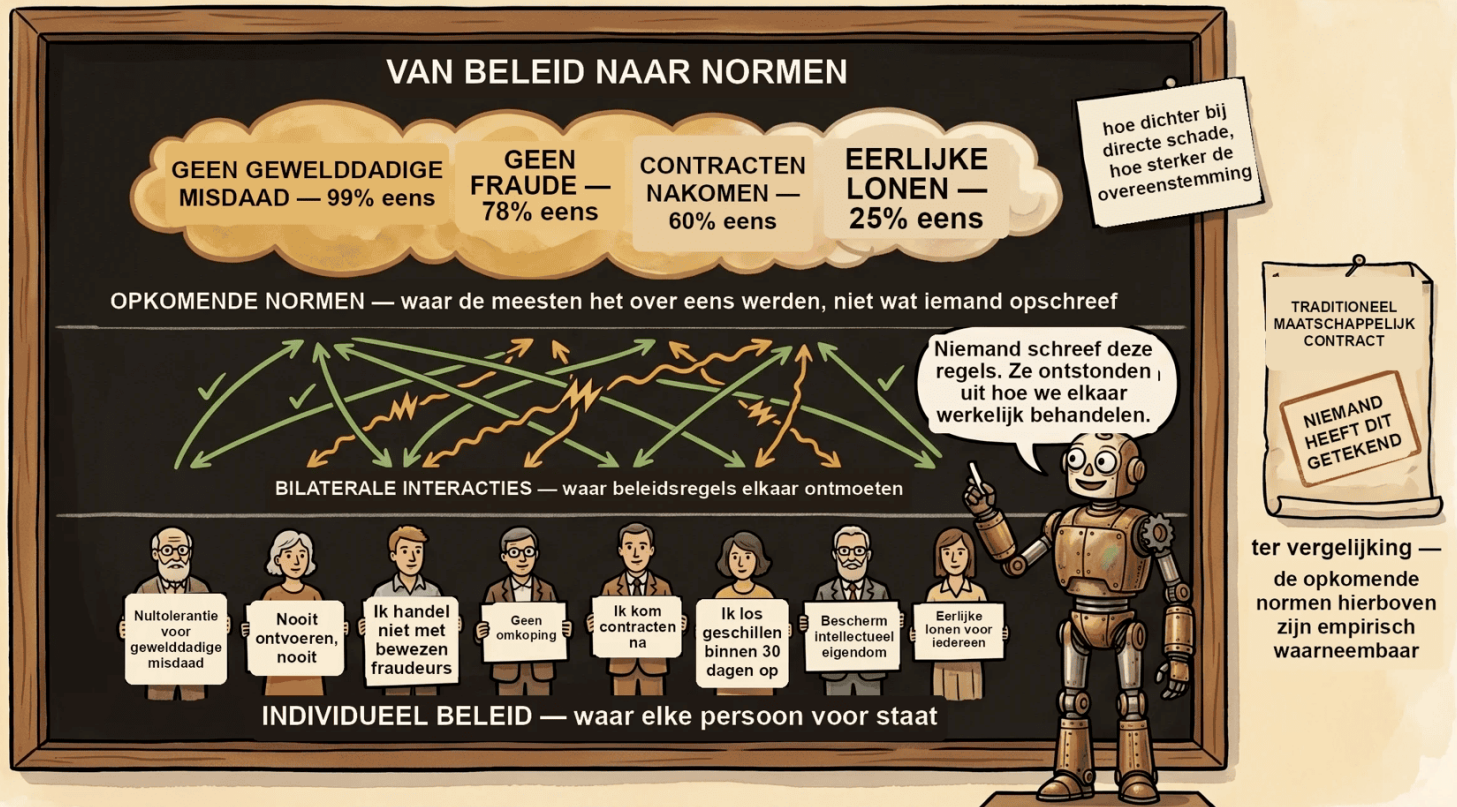
WANNEER BELEIDSREGELS UITEENLOPEN



Wanneer twee beleidsregels elkaar in de handel ontmoeten, wordt hun afstemming de prijsmodifierator.

* Dit gaat niet over reputatie. Het gaat over wat elke persoon publiekelijk verklaarde — en nu geacht wordt na te komen.

HOE ETHIEK ONTSTAAT UIT INDIVIDUELE BELEIDSREGELS



Ethiek wordt niet ontworpen. Ze ontstaat uit hoe we elkaar werkelijk behandelen.

* Elk individueel beleid is een weerspiegeling van de moraal van die persoon — gevormd door de druk om zich aan te passen aan hun gemeenschap en omgeving.

Informatie over jezelf verstrekken

Wanneer twee DID-subjecten die elkaar niet kennen een economische relatie aangaan, kunnen we namens de andere partij een verzoek aan onze eigen gemeenschap ondertekenen, waarin we haar vragen informatie over ons te verstrekken. Dit is echter een zeer naïef idee van wat gemeenschappen zijn. Het zijn geen gesloten verzamelingen — één DID kan deelnemer zijn in meerdere gemeenschappen.

Een gemeenschap is eerder een fenomenologisch verschijnsel vanuit het perspectief van een gegeven deelnemer, dat zich manifesteert in zijn sociale netwerk; het is niet iets wat altijd zinvol is om expliciet af te bakenen. De inwoners van een dorp kunnen een gemeenschap vormen, maar een persoon die er alleen in de weekenden komt, kan ook tot een andere gemeenschap in datzelfde dorp behoren. Een gemeenschap kan ook een voetbalteam zijn samen met zijn fans, zijn functionarissen en de families van alle betrokkenen. Een natie, of de burgers van een staat, kunnen ook een gemeenschap of gemeenschappen vormen. Een DID vanuit verschillende invalshoeken bekijken kan verschillende (en vaak intuïtieve) beelden van gemeenschappen opleveren.

DID's aan de grenzen zijn dus bruggen tussen gemeenschappen, en — net als in het echte leven — spelen ze een rol bij het verstrekken van informatie over leden van andere gemeenschappen, hetzij op amateurniveau, hetzij op een professioneel niveau, zoals een autoriteit die gespecialiseerd is in het verbinden van mensen en het samenbrengen van informatie over risicovolle DID's.

Sommige soorten informatie in het DID-netwerk lenen zich goed voor onvoorwaardelijke wederzijdse uitwisseling (gewelddsmisdrijf, fraude enz.). Andere soorten informatie kan een gemeenschap echter behandelen als beperkt tot gebruik binnen de gemeenschap (het equivalent van burgerschap, aan de gemeenschap bewezen diensten enz.). Of zulke informatie kan worden verspreid, hangt af van het verklaarde beleid van de leden van de gemeenschap.

Een gemeenschap bewaakt haar privacy binnen haar eigen kring, en wisselt in ruil daarvoor onvoorwaardelijk wederzijds voordelige informatie uit.

Misdaad en straf

Misdaad en straf

We weten hoe het netwerk werkt: hoe registraties ontstaan, wie ze verifieert, hoe fraude door de verificateur wordt afgeschrikt. Eén vraag blijft over — wat gebeurt er wanneer iemand werkelijk een ander schade berokkent?

Hoezeer zijn we van elkaar afhankelijk?

Wij allen staan op het toneel van deze grote wereld, en wat zich hier afspeelt, gaat ons allen aan.

Jan Amos Comenius (Het labyrint van de wereld en het paradijs van het hart)

Er kunnen vele redenen zijn om zich bij een reputatienetwerk aan te sluiten of het te verwerpen. Ik geloof echter dat één aspect van de menselijke natuur — vaak als duister beschouwd — een goed doel kan dienen. Ik heb het over de menselijke behoefte om een gevoel van genoegdoening te ervaren tegenover ervaren onrecht.

Genoegdoening, gerechtigheid, wraak — we associëren ze met negatieve emoties. Opdat de samenleving samenhoudt, moeten we ten minste doen alsof genoegdoening via gecentraliseerde instellingen wordt

geleverd; anders zouden individuen zich niet verbonden voelen met de samenleving waarin ze leven. Gemiddeld hebben we het nodig tot een of ander team te behoren en het te vertrouwen. Wanneer iemand een ander schaadt, kijkt de samenleving toe hoe genoegdoening zal worden geleverd en in welke mate. Enigszins controversieel betoog ik dat het vaak in de geschiedenis — en nu — niet heeft uitgemaakt of het proces tegen de beschuldigde zuiver was; wat uitmaakte was dat de samenleving zag dat *iemand* werd gestraft. Het vervulde zijn functie (talrijke gerechtelijke dwalingen en de weerstand tegen het heropenen van oude zaken vertellen dat verhaal duidelijk genoeg). De blik van het slachtoffer en de nabestaanden is slechts secundair. Wat eerst telt, zijn de signalen naar de rest van de samenleving, want onrecht is niet zo alledaags dat het in ieders dag figureert.

Een gedecentraliseerd reputatiesysteem zou het publiek direct en indirect bewijs laten zien (geaudit en niet-geaudit). De samenleving zou de informatie kunnen beoordelen — zelf of via vrijemarktdiensten gespecialiseerd in zulke beoordeling — en op basis van kwalitatieve en kwantitatieve signalen beslissen welke maatregelen op het subject toe te passen (of zelfs op de auteur of de verifiërende autoriteit).

Wat is straf? Het is een vorm van het vernederen van de vermeende dader door het verlies van zijn voorrechten — zodat zowel het slachtoffer als de samenleving voelt dat schadelijke daden niet lonen. Dit is het wezenlijke punt: schadelijk of gevaarlijk gedrag mag niet lonen, en tegelijk moet het een gevoel van genoegdoening geven aan zowel de slachtoffers als de rest van de samenleving/gemeenschap.

Moet zo'n straf door een centrale autoriteit worden toegediend? Wat als iedereen vooraf zou kunnen verklaren hoe hij op bepaalde daden zal reageren? Ik kan uiteraard geen straf voltrekken op andermans eigendom. Maar ik kan verklaren dat ik mijn eigendom ter beschikking zal stellen aan een geselecteerde verzameling uitvoerende autoriteiten met het oog op het bestraffen van de dader, mocht de overtreder mijn domeinen betreden. En dat kan ik publiek verklaren zodat anderen mijn benadering kunnen beoordelen.

En hier komt het prijsmechanisme van evenredigheid binnen. Als ik harde straffen verklaar voor kleine overtredingen, beprijst het netwerk mijn extremisme: anderen zullen mij onevenredig vinden en mijn verificatiekosten zullen stijgen — minder mensen zullen met mij willen handelen, of alleen tegen slechtere prijzen, en minder verificateurs zullen mijn registraties tegen een redelijke prijs aanvaarden. Als ik daarentegen te mild ben, zal de gemeenschap mij als een risico zien. Als ik fraude tolereer, zal de gemeenschap waarschijnlijk mild zijn tegenover daders van daden die mij raken — om mij een koekje van eigen deeg te geven.

Gerechtigheid houdt op een luxegoed te zijn. Wanneer iemand je schaadt, is het vastleggen van het onrecht betaalbaar, is de registratie permanent, en zijn de gevolgen voor de overtreder reëel.

Detectie van hypocrisie

Een beleid verklaren volstaat niet — als ik verklaar dat ik een regel volg maar mijn gedrag ervan afwijkt, is de kloof een reputationele last. Het netwerk maakt geen onderscheid tussen “heeft de wet gebroken” en “heeft zijn eigen woord gebroken” — beide zijn meetbare signalen. Hypocrisie is duur, en ik ken geen irritantere rode lap.

ÉÉN VAL. ÉÉN UITWEG.

DE INSIDER WINT ALTIJD HET CONTRACT — TOTDAT HET NETWERK MENSEN LAAT DIRECT KOPEN, GEEN TOESTEMMING NODIG.



Het publiek is het erover eens dat een nieuw openbaar IT-systeem nodig is, betaald uit de begroting, betaald uit belastingen.



Achter gesloten deuren ontwerpen de aanbestedingsambtenaar en de insider de aanbesteding op maat van één bedrijf. Een envelop wisselt van eigenaar.



De ambtenaar haalt zijn schouders op. Zijn zak puilt uit van de steekpenningen.



Het contract is gegund. De insider heeft de licentie — maar geen vaardigheid, en geen respect voor het werk.



De insider bezoekt de buurman. Het 'vriendelijke aanbod' is de kleinste kruimel.

1. TRADITIONEEL



REPUTATIENETWERK — hier begint de nieuwe wereld —

2. REPUTATIENETWERK



Twoe paden. De val zit in de regels. De uitweg is de regels volledig te omzeilen.

* Wanneer de regels door de insider worden geschreven, is klagen binnen de regels de val — zelfs de boetes voeden terug in de volgende gemanipuleerde aanbesteding. Het reputatienetwerk is de uitweg: burgers vinden het product, betalen de maker rechtstreeks, en de gemeenschap verleent de enige licentie die telt — vertrouwen verdiend door levering.

■ Kwantiteit vs. kwaliteit — het binaire paradigma van schuld doorbreken

In gecentraliseerde justitie is schuld binair: 0 of 1, schuldig of niet schuldig. In een reputatienetwerk telt niet of schuld is bewezen, maar de opeenstapeling van signalen.

Een enkele onbewezen beschuldiging van diefstal tegen de beschuldigde zal waarschijnlijk niet veel alertheid oproepen — maar wel alertheid tegenover de beschuldiger. Meerdere indirecte indicaties uit diverse onafhankelijke bronnen beginnen echter gewicht te dragen. Wat telt is niet alleen de kwantiteit maar ook de kwaliteit: onafhankelijkheid van getuigen (verschillende mensen, verschillende contexten), consistentie van het patroon (een terugkerend type verdenking), temporele correlatie.

Omgekeerd kunnen frequente ongegronde beschuldigingen die van dezelfde uitgever tegen diverse doelsubjecten terugkeren, als laster worden beoordeeld — en de reputatie van de beschuldiger betaalt de prijs.

HOE BEWIJS ZICH OPHOOPT

“één geïsoleerde claim”



één claim alleen — te dun om op te handelen.
geen van beide zijden veroordeeld.

“een patroon”



vijf onafhankelijke bronnen
— een patroon tekent zich af.

“overweldigend gewicht”



twintig onafhankelijke bronnen
— overweldigend gewicht.

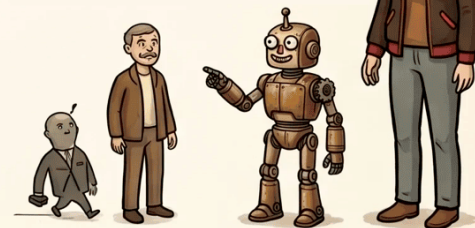


dezelfde claim zonder bewijs rondbazuinen
— wanneer de gemeenschap niets ziet, is
het laster, en het kost de beschuldiger.

Onafhankelijkheid is alles. Eén herhaalde stem is ruis. Vele stemmen vanuit verschillende plekken zijn een signaal.



één beschuldiger die naar iedereen wijst —
het patroon is de beschuldiger, niet de
beschuldigde.



dit lijkt op de wereld van vandaag. dat
is het ook — alleen de motieven zijn nu
eerlijk. geen revolutie. gewoon betere
prikkelers.

We mogen ook boetedoening niet over het hoofd zien — een vrijwillige daad voordat schuld is bewezen, die een pad naar een mildere straf biedt. Straf treedt in werking wanneer de dader geen stap richting boetedoening zet en hoopt aan de gevolgen te ontsnappen — net zoals die uitkomst kan worden gekocht via corruptie in een gecentraliseerd systeem.

Soorten overtredingen

De soorten informatie hoeven niet beperkt te zijn tot strafbare feiten; ze kunnen omvatten: - beschrijvingen van misdrijven - contractbreuken en fraude - immoreel gedrag - verstoringen van de openbare orde, zowel reëel als virtueel - ...

Elke nieuwe registratie in het DID-netwerk past de beoordeelde reputatie en het risico van de gegeven DID aan (of het nu het subject, de auteur of de verifiërende autoriteit is). Hoe meer verantwoordelijkheid ik draag voor het lot van anderen, hoe voorzichtiger ik word.

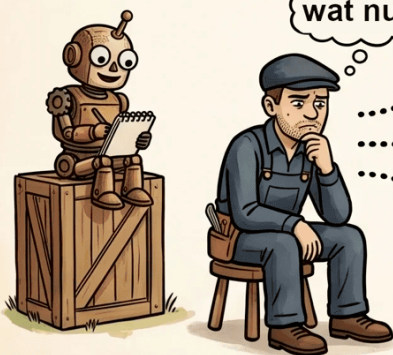
NA DE SCHADE — WAT GA JE DOEN?

weggestuurd. gedwongen. vrijwillig. drie manieren waarop het dorp antwoordt.

wat er gebeurd is



wat nu?



de rationele keuze is altijd de goedkoopste: LOS HET ZELF OP.

“Ik probeer het te negeren — overal weggestuurd”



geen herstel — elke winkel stuurt hem weg — verbanning uit het economische leven

“Ik maak het goed — maar alleen onder de blik van de menigte”



gedwongen herstel onder de blik van de menigte — terugbetaald, maar het dorp verhoogt zijn prijs — de les moet blijven hangen.

“Ik kom uit mezelf — en bek en het aan iedereen”



vrijwillig, vroeg herstel — publiekelijk aanvaard — reputatie herstelt, met voorzichtigheid

dit lijkt op de wereld van vandaag, dat is het ook — alleen de kosten zijn nu voor iedereen zichtbaar. geen revolutie. gewoon betere prikkels.

■ Straf afdwingen via delegatie

Ik hoef straf niet persoonlijk af te dwingen. Ik kan (net als bij verzekering) een autoriteit betalen die uitkomsten afdwingt volgens vooraf gedefinieerde regels — het equivalent van opsporings-, wetshandavings- en gerechtelijke diensten. Als de autoriteit onevenredig afdwingt of helemaal niet afdwingt, lijdt haar reputatie — en haar reputatie is de grondslag van haar vermogen om de kost te verdienen.

Delegatie is een algemeen principe in het netwerk: elke activiteit van een DID kan aan een andere DID worden gedelegeerd — verificatie, het uitgeven van claims, het reageren op geschillen, het verklaren van consensus. Delegatie is op elk moment herroepbaar. Ze maakt specialisatie mogelijk zonder verlies van uiteindelijke controle.

WIE ONDERZOEKT, WIE HANDHAFT?

“de schade” → “de onderzoeker” “het record” → “de handhaver” → “verantwoording”



DELEGATIE IS HERROEPBAAR. Elke DID-activiteit kan aan een andere DID worden gedelegeerd — en op elk moment worden teruggenomen.

je handhaaft de straf niet zelf. je delegeert. en de gedelegeerde legt verantwoording aan jou af.

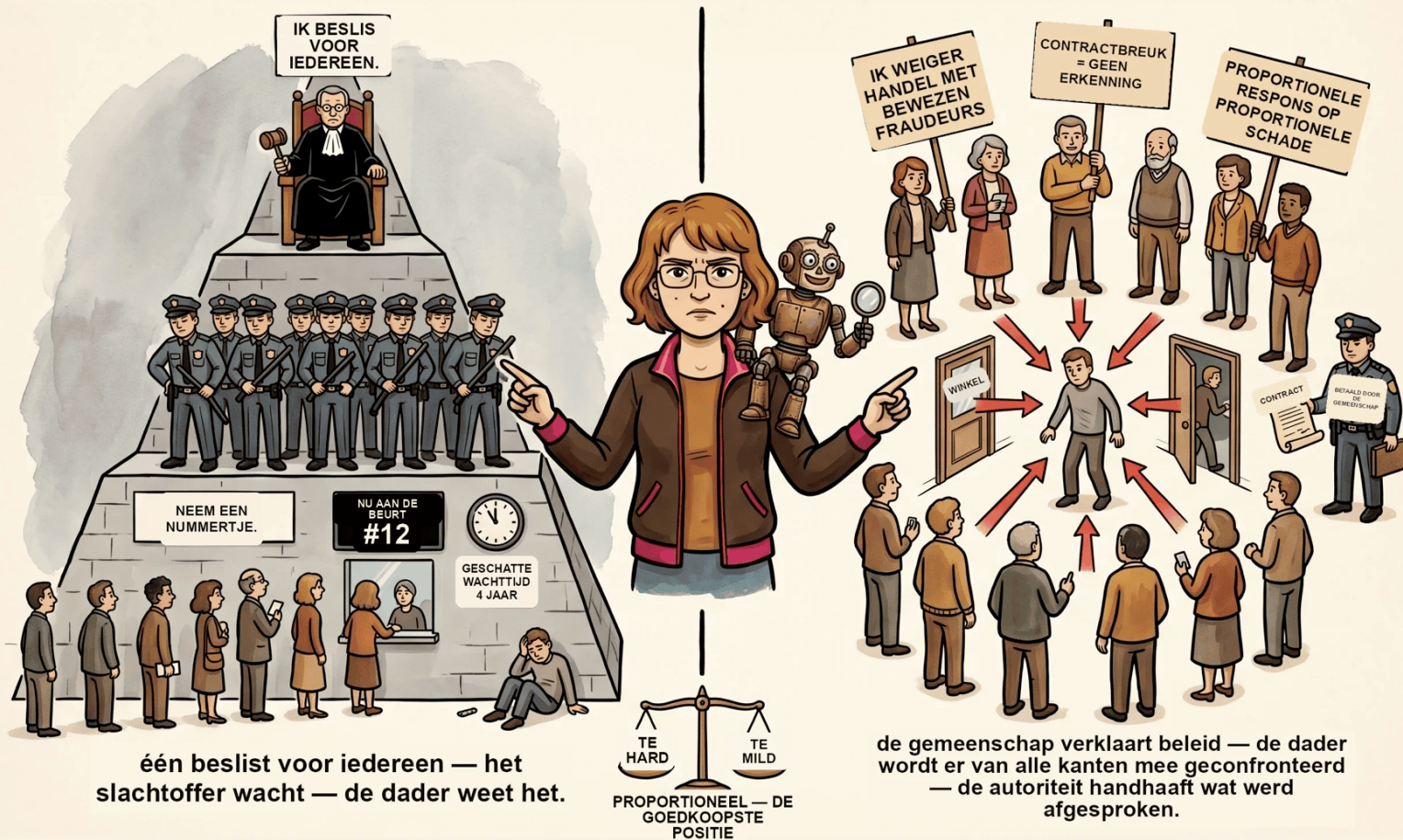
■ Democratisering van risicobeheer

Een oncensureerbaar reputatienetwerk zou democratiseren wat banken of beheerders van grote industriële complexen al als kernactiviteit doen — risicobeheer.

Voor een bankier tegenover een klant wordt de risicobeoordeling vooraf voorbereid zodat hij zich kan concentreren op de zakelijke interactie binnen vooraf gedefinieerde grenzen. Verfijnde onderhoudsteams verzamelen, bij regelmatige service-intervallen, risico-indicatoren (tekenen van structurele scheuren, processen die de operationele infrastructuur aantasten enzovoort) en kunnen de levensduur van apparatuur voorspellen alsook wanneer en welk soort ingreep nodig zal zijn.

Ik stel me DID-gebruik op vergelijkbare wijze voor — iemand (waarschijnlijk tegen een vergoeding) zal een voor mensen leesbare samenvatting van de tegenpartij leveren. De samenvatting zal de invalshoek van risicobeoordeling weerspiegelen die de klant heeft besteld.

BESTRAFFING ZONDER CENTRALE AUTORITEIT



Boetedoening is goedkoper dan straf.

Straf is goedkoper dan onwetendheid.

Volg het geld

Volg het spoor van het geld

We hebben een gedecentraliseerd reputatienetwerk en de motivatie om het te gebruiken. Nu al kan het zijn gebruikers een concurrentievoordeel opleveren — door potentiële risico's te verhelderen, hen te helpen de selectie van tegenpartijen en de onderhandelingsstrategie efficiënter te plannen, en de maatregelen op te nemen die die bekende risico's verminderen.

Wat volgt is één mogelijke methodologie⁵ om het te gebruiken — waarbij de eigenschappen van het netwerk worden benut om een migratiepad te construeren van het huidige systeem naar zijn evolutionaire opvolger. Ze draagt waarschijnlijk kenmerken die typisch zijn voor Midden-Europa, waar deze these is bedacht. Lokale omstandigheden zullen lokale aanpassingen vergen. Wat ik overal zou aanraden te behouden, is het compromisloze karakter van maatregelen tegenover de staat — zonder dat zal het doel verwateren in eindeloze discussie en zal de verandering nooit komen. Pas op — vertegenwoordigers en aanhangers van de staat zullen je bezighouden met onzin. Trap er niet in; hun broodwinning staat op het spel.

⁵**Deconstructie van de staat** — in de Tsjechische context zal dit waarschijnlijk uitvoerig worden behandeld in een komend gelijknamig boek van de Tsjechische auteur Daniel Steigerwald (gepland voor 2026). Ik heb persoonlijk hoge verwachtingen van de inspirerende procedures die het zal bevatten.

Het zwakke punt van de staat — geld

Laten we terugkeren naar het begin. We willen meer resulterende vrijheden, meer invloed op hun vorm, en meer verantwoordelijkheid die daarmee in verhouding staat. De vraag is eenvoudig: waar heeft de staat een kwetsbaar punt waarop we kunnen drukken zonder onze toevlucht te nemen tot geweld?

Het antwoord is saai, en juist daardoor des te sterker. Geld.

In de kern is de staat een stroom van geld. Via geld betaalt hij zijn dwangapparaat — de laatste schakel die zijn regels afdwingt. Zonder geld is er geen monopolie op geweld. Zodra het geld begint te haperen, begint de staat zich terug te trekken — omdat hij niets meer overheeft om degenen te betalen die hem fysiek op zijn plaats houden.

Geldstromen fluctueren van nature — seizoensgebonden, economisch, naargelang het beleggerssentiment. De staat maskeert dit door te lenen op de financiële markten. Af en toe is een lening rationeel: een investering die zich terugbetaalt. Vaker echter dekt ze buitensporige uitgaven aan agenda's die het kerndoel van de staat allang zijn ontgroeid — defensie, binnenlandse veiligheid, strafrechtspleging, buitenlandse zaken. Zodra bepaalde drempels worden overschreden, reageert de centrale bank met rentetarieven verankerd aan haar eigen inschatting van inflatie.

En hier komt de stille belasting. Inflatie is verre van een louter boekhoudkundige zorg van macro-economen. Ze is een verborgen belasting op de koopkracht van de munt, betaald door iedereen die een paar centen voor de oude dag heeft weggelegd. Lage inflatie wordt door het publiek getolereerd omdat het de langetermijneffecten ervan niet doorgrondt — het beseft niet dat zelfs enkelcijferige percentages, samengesteld over een lange horizon, spaargeld uithollen tot het punt waarop mensen hun eigen oude dag niet meer kunnen veiligstellen. En wanneer ze dat niet kunnen, worden ze geconditioneerd tot afhankelijkheid van staatsuitkeringen. Uiteindelijk hangen ze aan die uitkeringen en zijn ze aan de staat vastgeketend.

In turbulente tijden — oorlog, pandemie, de “noodzakelijke” investering — zet de staat gewoon de drukpers aan. De koopkracht van verantwoordelijke spaarders en werkers daalt terwijl we hun beloven dat ze goed worden beloond. Iemand steelt stilletjes hun tijd en prijst hen om hoe voortreffelijk ze verdienen.

Dit ondermijnt ernstig het vertrouwen in de staat. En vertrouwen is de enige lijm die de hele machinerie bijeenhoudt. Dat is de hefboom waar het de moeite waard is tegenaan te duwen.

■ **Waarom geld, en niet andere zwakke punten?**

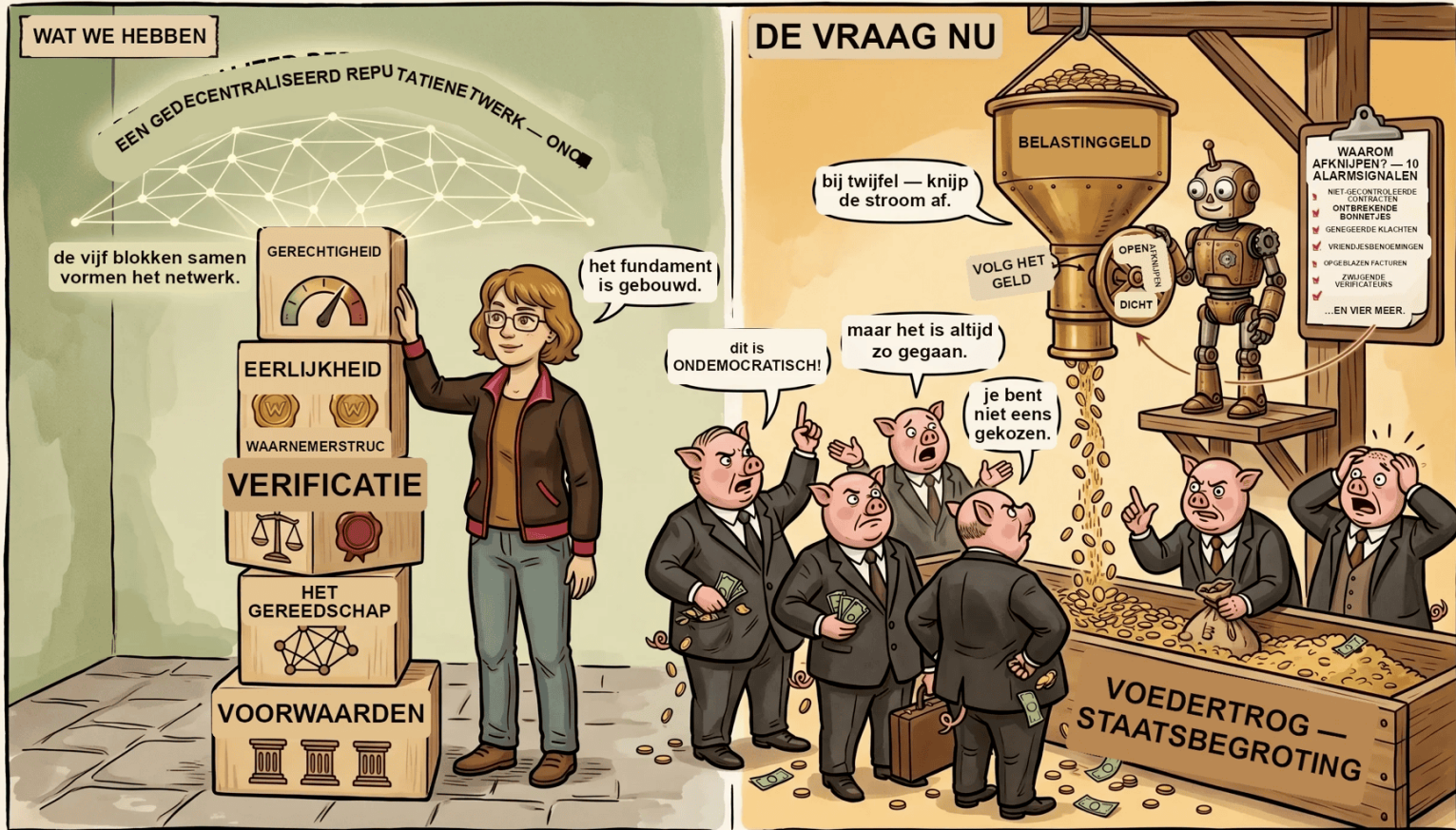
Een ander zwak punt van de beschaving is bijvoorbeeld de energiedistributie. Maar het verstoren van die stroom is geen hefboom — het zou agressie zijn, terrorisme. Vrijwillige niet-deelname is niet hetzelfde als het opzettelijk schaden van anderen. Geld is uitzonderlijk doordat er vrijwillig, transparant en zonder geweld druk op kan worden uitgeoefend.

Proposed transition to the state's successor

Evolutie, geen revolutie

Plotselinge verandering wekt weerstand, zelfs wanneer het einddoel aantrekkelijk is. Ze verbreekt banden — sociale, economische, politieke — en mensen verdedigen instinctief wat ze al kennen tegen wat ze nog moeten zien.

VOLG HET GELD — HET VERHAAL TOT NU TOE



We hebben het netwerk. We weten hoe het werkt. Nu: bij twijfel, knijp de trechter af.
de macht van de staat berust op geld. volg het.

De juiste benadering is daarom geleidelijk — evolutionair. Een die voorkomt dat het oude systeem het nieuwe met één druk op de knop uitschakelt — want op het moment dat het dat zou kunnen, zou het dat doen.

Helaas betekent dit aanvaarden dat evenwichtsvrijwilligheid niet wordt bereikt op het moment dat we het reputatienetwerk uitrollen; ze zal komen samen met een geleidelijk tempo van adoptie. De opname kan traag zijn — en zal dat waarschijnlijk zijn — voortgetrokken door het verlangen van individuen om via het reputatienetwerk verhaal te vinden bij hun gemeenschap wanneer de conformistische manier om gerechtigheid te zoeken faalt (en die zal falen). Laten we zien hoe dat pad eruitziet, inclusief evenredige schattingen.

■ Lege troggen — speel niet volgens regels die zo zijn opgezet dat je verliest

Pogingen om de staat van binnenuit te hervormen leunen op de interne mechanismen van de macht, in de hoop dat ambtenaren veranderingen zullen doordrukken tegen hun eigen prikkels in. Dat zal niet gebeuren.

Waarom het systeem voeden in plaats van de kanalen op te drogen die het leven brengen? In plaats van het oude systeem te veranderen en volgens zijn regels te spelen, laten we een nieuwe laag erboven bouwen — een die het oude systeem geleidelijk verandert in een deelverzameling van het nieuwe. Aan het begin vult die deelverzameling de superverzameling bijna volledig. Na verloop van tijd verplaatsen de actoren zich.

Bedrijven weten dit: wanneer een oud systeem te verward is om te vervangen, bouw je een parallel systeem en migreer je gebruikers er geleidelijk naartoe.

Het feit dat de staat uiteindelijk zit met een discrepantie tussen wat hij daadwerkelijk levert en wat zijn statuten eisen, en dat hij geneigd zal zijn die discrepantie in te roepen, is louter een probleem van zijn vertegenwoordigers en deelnemers — het is niet nodig erop terug te kijken. Het enige wat de moeite waard is om in de gaten te houden, is dit: lok geen gewelddadige revolutie uit.

Vier instrumenten die elkaar ondersteunen

Tot nu toe leek het DID-reputatienetwerk misschien vooral nuttig voor gerechtigheid en consensus. Ik geloof dat het zichzelf zou kunnen stabiliseren en aanvallen zou kunnen weerstaan — meritocratisch, op

basis van werkelijke verdienste in plaats van formele titels. Maar reputatie alleen zal de staat niet dwingen terrein prijs te geven. De economie zal dat wel, en de druk die er via haar wordt uitgeoefend.

Niets houdt ons tegen om DID-identiteiten te gebruiken als beheerders van bijkomende instrumenten die hard op het geld drukken. Begin niet met volledige vrijwilligheid van de kant van de burgers — zet een richting uit die de staat niet kan stoppen. De overgang berust op vier specifieke instrumenten die elkaar de rug dekken. Geen ervan volstaat op zichzelf.

Eenvoudig belastingsysteem — het lokaas voor toetreding

Het eerste instrument is een eenvoudig, transparant belastingsysteem gebouwd op DID-infrastructuur. Één proportioneel tarief op alle inkomen. Geen uitzonderingen, geen belastingvakanties, geen bedrijfsaftrekken, geen prikkels. Elke betaling is auditeerbaar gekoppeld aan de DID die ze heeft betaald. Kruiscontrole is triviaal.

Het tarief zou voor een deel van de belastingbetalers iets gunstiger worden gezet dan in het oude systeem — dat is het lokaas voor toetreding. De belastingdruk zou jaar na jaar dalen, het systeem zou steeds aantrekkelijker worden, en de migratie zou vaart krijgen. Het systeem is tegelijk de registratiehouder en de inner — geen tussenpersoon, geen ondoorzichtigheid.

Elektronisch uitgavenregister (ESR)

Het tweede instrument is EET (Elektronische registratie van inkomsten) op zijn kop zetten. In plaats van dat de staat elke bon van een zelfstandige volgt, volgen wij elk van de uitgaven van de staat. De staat ontvangt uit het eenvoudige belastingsysteem geen middelen voor welke individuele betaling dan ook, tenzij elke ervan — zonder uitzondering — door deze zeef gaat.

ESR is een proxy⁶ die elke gerealiseerde uitgave van de staat en de publieke sector koppelt aan een registratie van de geplande betaling — inclusief contextuele rechtvaardiging en identificatie van de ontvanger, de uitgevende entiteit en het doel. Het resultaat is ruwe publieke data, hiërarchiseerbaar. Iedereen kan die nemen en analyseren. Iedereen kan aanbevelingen aan belastingbetalers doen over wat ermee te doen. Wat de rekenkamers in jaren niet konden bereiken, is plots voor iedereen één klik verwijderd.

Je hoeft niet over te stappen op het nieuwe belastingstelsel om deel te nemen. Het volstaat een volledig terugbetaalbare borg (zeg 1–3 EUR) per gerealiseerde betaling te betalen. Het niet-gerealiseerde restant vervalt als spamfilter zodat het stelsel niet door aanvallen wordt overspoeld. Een registratie kan door iedereen worden ingediend — een familielid voor een wilsonbekwame grootouder, een buur voor verwaarloosde openbare diensten, een ondernemer voor een onbetaalde factuur, een ambtenaar door export uit zijn eigen stelsel.

Ik verwacht dat politieke partijen zich vanzelf zullen transformeren tot aanbieders van analyse, of dat er nieuwe zullen ontstaan om de oude te vervangen. In plaats van bijdragen uit belastingen zullen ze expertise gaan aanbieden — en hun aanhangers op waarden gebaseerde overzichten leveren van verbonden autoriteiten, hun diensten en verificatiebeleidslijnen. Registraties die slordig of onzinnig zijn uit luiheid worden automatisch kandidaten voor budgetkorting. In de eerste ronde zal je betaling altijd worden uitbetaald, maar de verzamelde data dient als basis om te beoordelen of een staatsuitgave nog zin heeft. Aannemers en anderen op de loonlijst van de staat hebben er belang bij ervoor te zorgen dat ambtenaren uitgaven verantwoord koppelen. Anders zal het geld in de volgende ronde niet vloeien.

⁶**Proxy** (Latijn *procurator*, Engels *deputy/intermediary*) — hier een tussenpersoon die namens een andere entiteit handelt. De ESR-proxy aanvaardt registraties van geplande betalingen van iedereen, koppelt ze aan de gerealiseerde uitgaven van de staat, en stelt de resulterende dataset beschikbaar aan het publiek.

■ Waar het acroniem ESR vandaan komt

Tussen 2016 en 2022 voerde de Tsjechische regering een systeem in genaamd Elektronische registratie van inkomsten (EET) tegen haar eigen burgers — zelfstandigen en ondernemers. De boodschap was eenvoudig: “We gaan ervan uit dat ieder van jullie de staat bedriegt. Jullie zullen elke afzonderlijke transactie registreren, ze in real time naar onze servers doorsturen, en wij zullen jullie in de gaten houden. We zullen jullie medeburgers financieel belonen als ze jullie aangeven wanneer jullie EET proberen te ontwijken.”

EET was gemodelleerd naar Balkanprecedenten. Het eerste land ter wereld dat een landelijk verplicht real-time online systeem voor verkoopregistratie lanceerde, in 2013, was Kroatië, onder de naam *fiskalizacija*. Tsjechië nam het model enkele jaren later over en beheerde een van de strengste regimes voor inkomstenvolging in Europa.

Als de duistere kant niet aarzelt, waarom zouden wij dat wel doen? ESR is dezelfde logica ondersteboven gekeerd: de staat bewijst zichzelf aan de burgers.

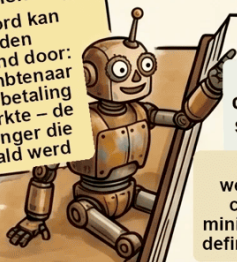
Burgerbelastingtoewijzing — het gewicht van de beslissing

Het derde instrument geeft belastingbetalers directe invloed op waar hun geld naartoe stroomt. In de eerste ronde ontving de staat zijn geld ongeacht wat de ESR onthulde. In de tweede ronde niet meer — de analyse uit de eerste ronde, en de maatregelen die eruit volgen, nemen het over. Een klein percentage van de betaalde belasting kan door de betaler zelf worden toegewezen — mits zijn DID aan de reputatievereisten voldoet (burgerschap, verblijf, door de gemeenschap erkende

ESR — ELEKTRONISCHE UITGAVENRAPPORTAGE

elke staatsuitgave vastgelegd — elk record publiek — elk detail open voor toetsing.

wie dient in
elk record kan
worden
ingediend door:
— de ambtenaar
die de betaling
verwerkte — de
ontvanger die
betaald werd



OPENBAAR GROOTBOEK VAN STAATSUITGAVEN — open record

categorie: juridisch advies
contractant: advocatenkantoor **ASTM2**
s.r.o. bedrag: 14M EUR vastgelegd:
2026-01-14 betaald: 2026-01-19
context: extern advies over het nieuwe
wetsvoorstel aanbestedingshervorming — drie
concepten geproduceerd, één workshop met
ministerie, geen openbare hoorzitting gehouden —
definitief concept geleverd na de wettelijke termijn.

categorie: wegontwerpadvies
contractant: Adviesbureau T **bedrag: 9M**
EUR vastgelegd: 2026-02-03 betaald: —
context: haalbaarheidsstudie voor de verlenging van
de D-X snelweg — hetzelfde bureau schreef drie
eerdere studies over dit tracé — uitkomst: aanbeveling
om door te gaan tegen +18% boven eerdere ramingen.

open voor iedereen
die wil kijken.

categorie: uitgifte kentekenplaten
ontvanger: regiokantoor Z **bedrag: 45**
EUR per plaat vastgelegd: 2026-02-19
betaald: 2026-02-19
context: standaard administratieve vergoeding
per uitgegeven plaat — vergoeding dekt
materiaal en verwerking — totaal volume 12 400
platen dit kwartaal.

categorie: ziekenhuisapparatuur
contractant: MedSupply a.s. **bedrag: 8,2M**
EUR vastgelegd: 2026-03-08
betaald: —
context: installatie MRI-scanner in regionaal
ziekenhuis — openbare aanbesteding, drie
inschrijvers — gekozen inschrijving 2% onder de
mediaan, levering binnen 60 dagen — factuur 90
dagen over de vervaldatum.



spamfilter — terugbetaalbare borg



borg terugbetaald
wanneer het
record accuraat
blijkt.

partijen transformeren tot analyse-aanbieders



de beschrijvingen zijn de grondstof —
partijen verdienen hun brood door ze
zorgvuldig te lezen, de
kruisverwijzingen te leggen en één
gedrukt bulletin te produceren.

Elke kroon aan publiek geld — vastgelegd, publiek, toetsbaar.

de waarde zit niet in het betrappen van bedriegers — ze zit in het openen van de boeken.

dit lijkt op de wereld
van vandaag. dat is
het ook — alleen de
boeken zijn nu voor
iedereen open. geen
revolutie. gewoon
betere prikkels.

volwassenheid/handelingsbekwaamheid). Het toewijsbare percentage groeit jaar na jaar. Mogelijk exponentieel. Van vijf procent vandaag tot tientallen procenten binnen een decennium.

De ruwe ESR-data leidt vanzelf de beslissingen van belastingbetalers. Registraties van lage kwaliteit functioneren als een waarschuwingssignaal voor aanbevolen kortingen. Iedereen kan registraties aanmaken; ambtenaren moeten ze koppelen. Zonder dat zal het belastingstelsel de staat geen geld sturen — noch naar de schatkist, noch naar andere begrotingshoofdstukken. De politieke strijd verplaatst zich van de stembus naar de dagelijkse toewijzing van concrete munten.

BURGERBELASTINGTOEWIJZING — JIJ BESLIST WAAR JE BELASTING NAARTOE GAAT

bestudeer de ESR-records. verschuif dan de schuifregelaars.



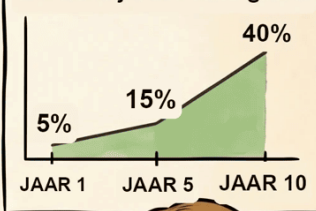
of delegeer dit

wil je niet zelf toewijzen? delegeer aan: — de analist van je partij — een vertrouwde buur — wie je maar kiest — en herroep op elk moment.

na het lezen van het rapport — defensie omlaag.



het toewijsbare deel groeit



klik op een rij om in te zoomen — wijs op elk niveau toe.

Van 5% vandaag naar 40% binnen een decennium. Jij beslist.
de records zijn open. de analyse is van jou. de schuifregelaar ook.

dit lijkt op de wereld van vandaag. dat is het ook — alleen de schuifregelaar ligt nu in jouw hand. geen revolutie. gewoon betere prikkels.

Onderhandelingsplatform met de staat — de hefboom

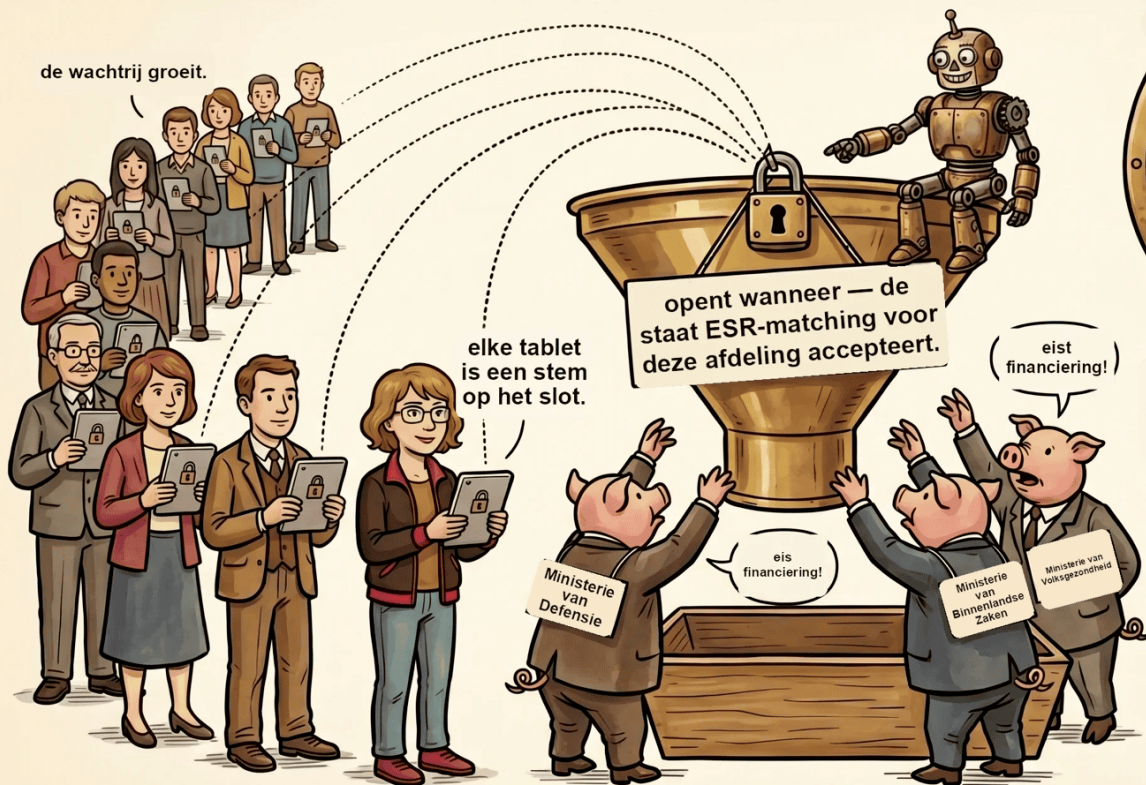
Het vierde instrument is de hefboom die alles aan elkaar bindt en het netwerk nu pas een echte dreiging maakt. Het voornaamste conflict zal gaan over de vraag of de staat ESR aanvaardt als een bindende standaard — eerst op nationaal niveau — en hoe groot de dreigingen vanuit de deelnemers van het reputatienetwerk moeten worden voordat dat gebeurt.

De hefboom is just-in-time staatsfinanciering, afhankelijk van het koppelen van betalingen aan ESR. Geld vloeit pas op het moment dat de staat aan de transparantievoorwaarden heeft voldaan. Binnen het reputatienetwerk vormt zich een wachtlijst van deelnemers. Activering treedt in werking wanneer de groep een economisch significante omvang bereikt — groot genoeg om de bbp-groei te bedreigen. Op dat punt wordt burgerlijke ongehoorzaamheid een geloofwaardige dreiging in plaats van een gebaar.

De staat zal het langst vasthouden aan de problematische betalingen die met corruptie verbonden zijn. Onder druk zal hij het eerst terrein prijsgeven waar hij een makkelijke verdediging heeft en waar geen ruimte is om naar besparingen te zoeken. Geleidelijke en oplopende druk zal hem dwingen zich stap voor stap uit elke positie terug te trekken.

ONDERHANDELINGSPLATFORM — DE GESLOTEN TRECHTER

de burgers hebben de sleutel. de staat opent wanneer aan de voorwaarden is voldaan.



een kleine fractie van het BBP is genoeg — bij kritieke massa wordt inhouden een echte dreiging.

na kritieke massa —

de staat opent zijn boeken eerst voor eenvoudige, verdedigbare betalingen.

aan corruptie gelinkte categorieën blijven het langst op slot.

elke ontgrendeling kost meer druk — en wordt zelf vastgelegd.

dit lijkt op de wereld van vandaag. dat is het ook — alleen de sleutel is nu in veel handen. geen revolutie. gewoon betere prikkels.

Geld stroomt wanneer er transparantie is. De burgers hebben de sleutel.

geen dwang. geen revolutie. gewoon genoeg tablets om inhouden geloofwaardig te maken.

Burgerschap zonder identiteitskaart

Met de overgang naar DID-infrastructuur verliest de door de staat uitgegeven identiteitskaart haar monopolistische doel. Je hebt geen identiteitskaart nodig — je hebt een reeks DID-identiteiten, en sommige ervan dragen een claim dat je bijvoorbeeld Tsjech bent, inwoner van een bepaalde gemeente, afgestudeerd aan een bepaalde school. De claim is verifieerbaar, permanent, en onafhankelijk van staatsadministratie.

Er opent zich een vraag van technische uitvoering: wie op de markt zal het verifiëren van bestaande burgers buiten staatscontrole op zich nemen, teneinde de geïnteresseerden te migreren naar een DID die de passende claim draagt? Hoogstwaarschijnlijk zullen er vrijemarktautoriteiten ontstaan die gespecialiseerd zijn in identiteitsverificatie — notarissen, lokale gemeenschappen, werkgevers. Ze zetten hun reputatie in op het feit dat een gegeven DID werkelijk toebehoort aan de persoon die dat beweert. Burgerschap — dat wil zeggen het behoren tot een bepaalde kijk op gemeenschap — wordt bevrijd van de noodzaak van centrale registratie. Door de verbinding via het reputatienetwerk worden de ingebedde gegevens een tweede, een derde, een vierde keer, enzovoort, verbonden en gevalideerd.

Het gevolg is intuïtief en toch onoplosbaar in een gecentraliseerd systeem. Vandaag kan de politieke leiding — met het oog op makkelijkere herverkiezing — geconcentreerde problemen het grondgebied van de gemeenschap binnenhalen: migranten uit andere beschavingskringen aanvaarden ongeacht de opnamecapaciteit en de bereidheid van de bestaande gemeenschap, en oorspronkelijke gemeenschappen veranderen onder een druk waaronder ze het assimileren van nieuwkomers uit andere beschavingskringen niet kunnen bijbenen. In een DID-netwerk kan een corrupt toegelaten migrant er niet zeker van zijn dat de gemeenschap hem als een van de hare zal blijven beschouwen. Leden van de gemeenschap hoeven objectief geen genoeg te nemen met een vreemdeling die in het uniform van de gemeenschap aan hun deur komt en hen bedreigt met de legaliteit van maatregelen die hij in het huis wil uitvoeren (inbeslagname van de telefoon van een kind wegens een socialmediabericht). Met gedecentraliseerde

VIER GEREEDSCHAPPEN VOOR EVOLUTIONAIRE OVERGANG

het systeem van binnenuit herbouwd — zonder het te breken.

EENVOUDIGE BELASTING



één tarief. geen uitzonderingen. kruiscontroleerbaar.

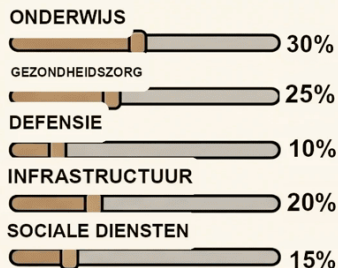
ESR — ELEKTRONISCHE UITGAVENRAPPORTAGE



elke uitgave vastgelegd — elk record publiek — elk detail open.

BURGERBELASTINGTOEWIJZING

5% → 15% → 40%
JAAR 1 → JAAR 5 → JAAR 10



bestudeer de records — verschuif dan de schuifregelaars.

ONDERHANDELINGSPLATFORM



geld stroomt alleen wanneer aan de transparantievoorwaarden is voldaan.

vandaag

evolutie gaande

binnen een decennium

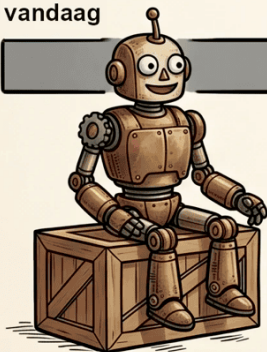
95%

uitbreidend

Evolutie, geen revolutie.

vier gereedschappen die het systeem van binnenuit veranderen.

dit lijkt op vandaag; dat is het ook — alleen de gereedschappen liggen nu bij de burger. geen revolutie. gewoon betere prikkels.



reputatie hoeft de meerderheid van de samenleving zich hierbij niet neer te leggen — want het behoren tot een gemeenschap wordt niet beslist door een ambtenaar, maar door de gemeenschap zelf, via haar reputatiesignalen.

BURGERSCHAP ZONDER IDENTITEITSKAART

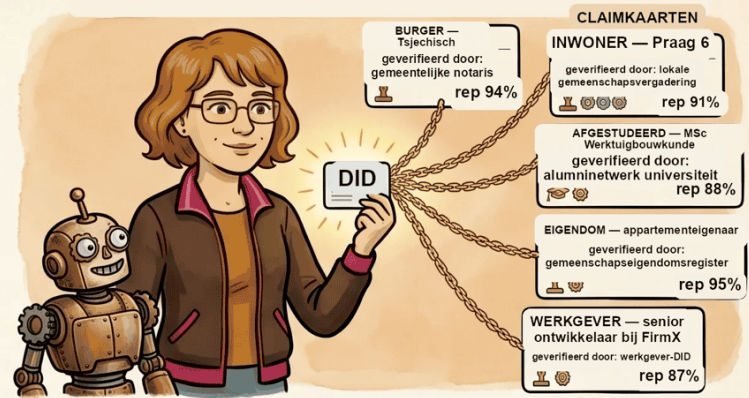
van een staatsvergunning naar erkenning door de gemeenschap.

“de oude manier” van het institutionele model met staats-ID



identiteit = staatstoestemming — intrekbaar — gemeenschap heeft geen inspraak.

“de nieuwe manier” van het DID-model met claimkaarten



geen enkele autoriteit beheert alle claims — elk is onafhankelijk — elke verificateur zet zijn reputatie in.

“wie hoort erbij?”



de gemeenschap beslist — via reputatiesignalen — gedistribueerd, geen enkele stem.

dit lijkt op de wereld van vandaag. Dat is het ook — alleen de verificateurs zijn nu talrijk, geen revolutie, gewoon betere prikkels.

Jouw burgerschap is geen overheidsvergunning. Het is de erkenning van je gemeenschap.

de staatsstempel wordt vervangen door een keten van onafhankelijke verificateurs — elk met iets te verliezen.

Het gewicht van een verkiezingsstelsel over aangelegenheden die onder de bevoegdheid van de staat vallen, zou in de toekomst strikt kunnen worden gecorreleerd met registraties van bijdragen aan het eenvoudige belastingsysteem. Gecombineerd met geschikte DID-claims (bijvoorbeeld “deze persoon is een Tsjechische burger”) kunnen buitenlandse onderdanen dan van verkiezingen worden uitgesloten — het bevolkingsregister verhuist gewoon hierheen.

Overlap en omkeerbaarheid

Ik beweer niet dat dit het enige pad is, of zelfs het beste. Maar het lijkt volledig — het dekt de belangrijkste hefbomen en behoudt de mogelijkheid om terug te treden. Aan het begin overlapt het nieuwe systeem met het oude en verandert het alleen de prikkels. Na verloop van tijd krimpt het oude systeem tot het zich kan — maar niet hoeft te — oplossen. Het voordeel is geleidelijkheid en omkeerbaarheid: mocht er een fout in het ontwerp opduiken, dan is dat niet het einde, slechts een correctie.

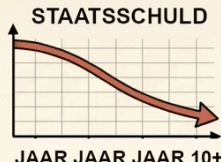
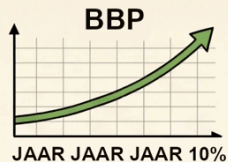
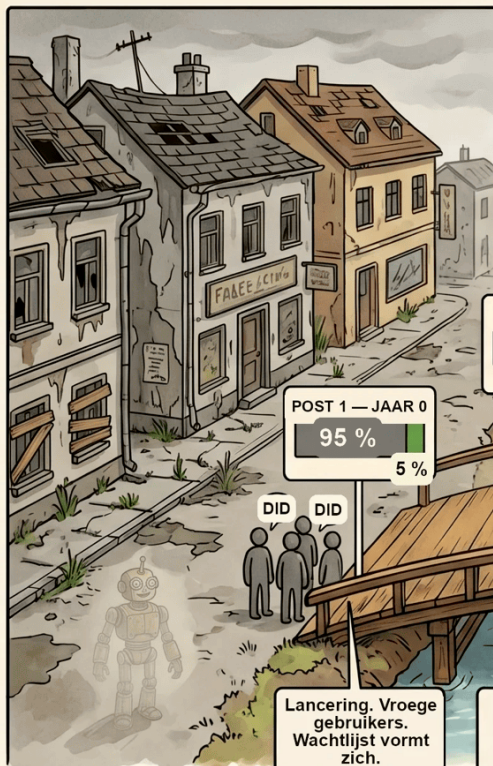
■ Vrede en oorlog

Sommige delen van de staat hebben misschien geen volledig marktgebaseerd alternatief — wellicht het leger. Tijdelijke delegatie van buitengewone bevoegdheden in crises (zoals de oude Grieken dictators aanstelden) zou kunnen blijven bestaan. De verantwoordelijkheid rust echter op de gedecentraliseerde samenleving, niet op de leider. Anders dan bij gecentraliseerd bestuur zal het makkelijker zijn gedelegeerde bevoegdheden terug te vorderen zodra de dreiging voorbij is — of eerder, wanneer nodig. Een vrije samenleving zal ook in de wapenstrijd tegen autoritaire regimes niet in het nadeel zijn.

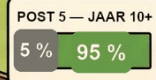
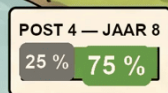
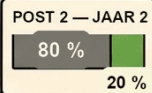
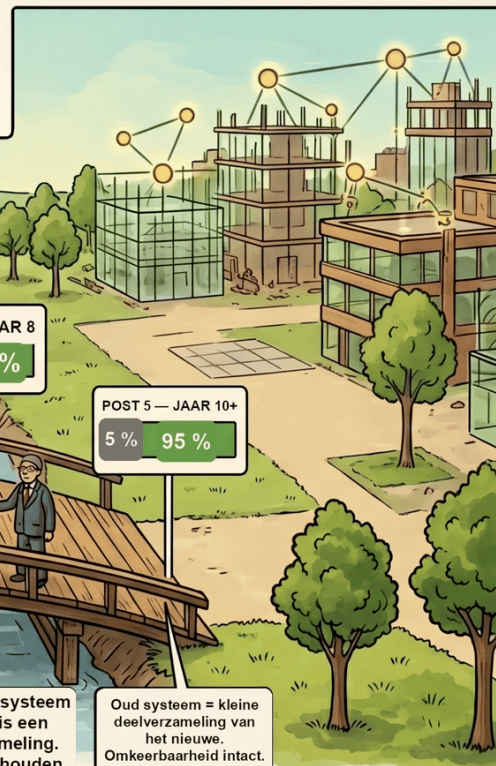
■ Oorlogsmisdadigers

Met just-in-time staatsfinanciering en transparante uitgaven wordt het moeilijk om middelen te vergaren voor agressieve oorlogen. Een belastingbetaler die zo'n oorlog blijft financieren, wordt een legitiem doelwit en kan geen burgerstatus onder de Conventies van Genève invoeren. Onder de nieuwe inrichting wordt stilzwijgende instemming opgevat als deelname.

LINKEROEVER — 'HET OUDE SYSTEEM'



RECHTEROEVER — 'HET NIEUWE SYSTEEM'



**KRITIEKE MASSA — STAAT
ACCEPTTEERT ESR ONDER
ECONOMISCHE DRUK.**

OMKEREN

Lancering. Vroege
gebruikers.
Wachtlijst vormt
zich.

Groeiend.
Deelnemerslijst
zwellt aan.

Ontwerpfout? We
kunnen terug.
Omkeerbaarheid
behouden.

75% nieuw systeem
— Staat is een
deelverzameling.
Overlap behouden.

Oud systeem = kleine
deelverzameling van
het nieuwe.
Omkeerbaarheid intact.

**oud
systeem**

> Geleidelijke overgang. Omkeerbaarheid bij fouten. Een richting die niet gestopt kan worden.

Conclusie

Het pad bestaat

De staat is zoals hij is vanwege de technologieën die beschikbaar waren op het moment van zijn ontstaan, gecombineerd met de menselijke natuur. Alles bouwen op vrijwilligheid terwijl je de gemiddelde menselijke natuur ontkent, is naïef. Hij zal zich niet ontdoen van corruptie, noch van zijn neiging om af te drijven richting totalitarisme. De opvolger van de staat moet ook werken met de trekken die we momenteel als negatief beschouwen en ofwel ostraciseren ofwel bestraffen.

Dit boek beschreef een probleem — een systeem (de staat) waarin de mensen die de regels schrijven nooit met de gevolgen ervan leven. Het beschreef de voorwaarden waaraan moet zijn voldaan opdat dat systeem ophoudt te werken. Het beschreef een instrument dat aan die voorwaarden voldoet. En het stelde een overgangsmethodologie voor — concrete stappen voor hoe dat instrument te gebruiken, als één mogelijk voorbeeld.

In het eerste hoofdstuk noemde ik vijf pijlers: vrijwilligheid, organisatie, weerbaarheid, consensus en onomkoopbaarheid. We hebben er aan alle voldaan.

- **Vrijwilligheid** — niemand dwingt je het netwerk in, maar je kunt je daden er ook niet uit wissen.
- **Organisatie** — de gemeenschap groeit uit wie je kent, niet uit wie je van bovenaf is toegewezen.
- **Weerbaarheid** — zelfs een staat die bereid is te betalen voor het bespieden van elk pakket kan het niet uitschakelen.
- **Consensus** — die ontstaat uit het prijskaartje op hypocrisie, niet uit stemmen of handtekeningen.

- **Onomkoopbaarheid** — vijf kleine regels weven corruptie in kosten: het evenwicht van vrijwilligheid en verantwoordelijkheid, ieders recht om te spreken, toegangspunten die niemand mag uitkiezen, publieke beloften met een prijs voor hypocrisie, en de schaduw van een waarnemer achter elke transactie.

Geen enkele pijler kan de staat op eigen kracht vervangen. Samen vormen ze een weerstand tegen corruptie die de staat, met al zijn apparaat, niet kan.

We zijn op een punt waar het geheel kan worden gebouwd met de technologieën van vandaag (cryptografie, gedecentraliseerde identiteit, bekende psychologische patronen om de prikkels goed te krijgen, ...). Slechts één ding ontbreekt: een kritieke massa aan mensen die de moed vinden het te steunen en besluiten te beginnen.

Niet via revolutie.

Deze ideeën kregen vorm tussen juni 2025 en mei 2026. Tegen de tijd dat ik ging zitten om te schrijven, had ik het raamwerk grotendeels in mijn hoofd uitgewerkt — precies daarom las ik [Farewell To Westphalia](#) met zoveel nieuwsgierigheid toen het verscheen. Ik wilde zien waar hun beeld het mijne zou overlappen en waar het zou uiteenlopen. Een tweede duwtje kwam van Dan Steigerwald, die in mei 2026 nog steeds werkt aan zijn eigen boek *Deconstructie van de staat* vanuit een andere invalshoek; zijn project zette me ertoe aan mijn eigen visie in volle breedte neer te leggen — zodat de wereld haar naast de andere op tafel heeft.

Ik vraag je niet er iets van te geloven. Ik vraag je erover na te denken. En ik laat je achter met één vraag:

Wat zou jij veranderen?

Dankwoord

Inspiratie

Ik dank de auteurs van [Farewell to Westphalia](#) (Jarrad Hope, Peter Ludlow) voor het intellectuele raamwerk dat mij hielp mijn eigen ideeën te plaatsen in de bredere context van het deconstrueren van het Westfaalse model van de staat.

Review en feedback

Hulpmiddelen

Bij het voorbereiden van de tekst, het structureren van ideeën en het itereren op formuleringen heb ik ondersteuning van AI-hulpmiddelen gebruikt. Alle ideeën, argumenten en conclusies zijn de mijne — AI diende als hulpmiddel voor verfijning, niet als mede-auteur van de inhoud.

De infografieken zijn ontworpen in samenwerking met generatieve hulpmiddelen op basis van de specificaties van de auteur.

NEEM JE TIJD TERUG

de burgers jagen de parasieten uit het openbare leven.



Verdedig de tijd die ze zouden stelen.

wat door bedrog werd genomen, wordt met de hand
teruggenomen.

Steun het project

Personix wordt gefinancierd door lezers zoals jij.



Bitcoin on-chain

bc1q7ccdtz6r026dgy06ul94eygg49ujtxnrq5czaj



Bitcoin Lightning

LNURL1DP68GURN8GHJ7AMPD3KX2AR0VEEKZ
AR0WD5XJTNRDAKJ7TNHV4KXCCTTDEHHWM30
D3H82UNVWQHXMNP0FA8JMPVD5XJMN9XUE
RX55QRQK

■ Waar dit geld heen gaat — en waar niet

De QR-codes zijn de **persoonlijke kanalen van de auteur** — bijdragen gaan rechtstreeks naar Pavel Kudrna en financieren verder schrijven, het maatschappelijk experiment / de simulatie, en outreach.

De *enige* legitieme fondsenwervingskanalen voor dit project zijn:

- **Editie van dit boek door de auteur** — QR-codes in door de auteur geautoriseerde exemplaren.
- personix.org of de vanaf daar gelinkte Tor-onion-spiegel — waar de *Personix Foundation* inzamelt voor de daar beschreven activiteiten. De middelen van de stichting worden gescheiden gehouden van de persoonlijke middelen van de auteur.

Alles wat elders wordt aangeprezen — vervangen adressen in herdrukken, lookalike-domeinen, sociale media die “inzamelen voor Personix,” fondsenwervingen die aan geen van beide bovenstaande zijn gekoppeld — **is hoogstwaarschijnlijk fraude**. We mijden bewust de cryptovalutamarkt en haar deelnemers.

Woordenlijst

Woordenlijst

Term	Nederlands	Betekenis
Authority	Autoriteit	Een vertrouwde entiteit (persoon, organisatie) die informatie verifieert en er haar reputatie op inzet. Kan gespecialiseerd zijn (onderzoekend, juridisch, technisch).
Claim	Bewering	Algemeen: elke verifieerbare uitspraak. Hier: een in het reputatienetwerk gepubliceerde registratie — een bewering over een gebeurtenis, eigenschap of relatie die cryptografisch is ondertekend en geverifieerd. Bijv. “Ik ben inwoner van gemeente X” of “deze persoon heeft een contract geschonden.”

Term	Nederlands	Betekenis
Compartmentalization	Compartimentalisatie	Algemeen: het scheiden van informatie in geïsoleerde eenheden zodat het blootleggen van één eenheid de andere niet compromitteert. Een principe bekend uit inlichtingendiensten. Hier: parallelle DID-identiteiten in dictaturen — het compromitteren van één onthult de andere niet.
Consistent Hash Ring	Consistente hashring	Een algoritmisch mechanisme voor het selecteren van verificateurs — een positie op de ring wordt bepaald door de hash van het DID-document binnen de sociale graaf. Zorgt voor een niet-deterministische en toch verifieerbare selectie.
DID	DID (Gedecentraliseerde identiteit)	Een digitale identiteit die je zelf aanmaakt en beheert, zonder centrale autoriteit. Cryptografisch ondertekend met je privésleutel — niemand kan die intrekken of vervalsen.

Term	Nederlands	Betekenis
DID Document	DID-document	Een publiek beschikbaar gegevensbestand dat je DID-identiteit beschrijft — bevat publieke sleutels, netwerkadressen en metadata. Dient om je identiteit in het netwerk te verifiëren.
Due Diligence	Due diligence	Algemeen: diepgaande verificatie van een tegenpartij voordat je een zakelijke of juridische relatie aangaat — het controleren van haar geschiedenis, financiën, reputatie en risico's. Hier: in het reputatienetwerk gebeurt ze sneller en automatischer dankzij de beschikbaarheid van geverifieerde registraties.
Economic Neutrality Principle	Principe van economische neutraliteit	Eerlijk gedrag in het netwerk ligt economisch dicht bij nul — de publicatiekosten keren terug als verificatiebeloningen. Oneerlijk gedrag is een netto verlies.

Term	Nederlands	Betekenis
Emergent	Emergent	Spontaan ontstaand uit de interacties van eenvoudiger delen, zonder dat iemand het ontwerpt of aanstuurt. Een zwerm vogels vliegt zonder plan in formatie — de formatie emergeert uit eenvoudige regels die elk individu volgt.
Emergent Social Contract	Emergent maatschappelijk contract	Gedragsregels die niet van bovenaf ontstaan (wet) maar van onderaf — uit herhaalde interacties en consensus binnen een gemeenschap.
ESR	Electronic Spending Register	Een voorgesteld systeem voor transparante volging van publieke uitgaven — elke gerealiseerde staatsuitgave wordt gekoppeld aan een geplande betaling. Geïnspireerd op de Tsjechische EET, maar tegen de staat gekeerd.

Term	Nederlands	Betekenis
Hash	Hash (afdruk)	Algemeen: een eenrichtings-wiskundige functie die uit elke invoer een unieke “vingerafdruk” van vaste lengte produceert — als een vingerafdruk van het document. Dezelfde invoer levert altijd dezelfde uitvoer, maar de invoer kan niet uit de uitvoer worden afgeleid. Hier: gebruikt om een positie op de hashring te bepalen en de integriteit van een document te verifiëren.
Just-in-Time Funding	Just-in-time financiering	Staatsfinanciering afhankelijk van transparantie — geld vloeit alleen wanneer de staat ESR aanvaardt en zijn uitgaven koppelt. Een hefboom om samenwerking af te dwingen.

Term	Nederlands	Betekenis
Meritocracy	Meritocratie	Algemeen: een systeem waarin aanzien wordt bepaald door werkelijke verdienste en bewezen vaardigheid, niet door formele titels, connecties of geërfd voorrecht. Hier: het reputatienetwerk begunstigt vanzelf wie aantoonbaar bijdraagt aan de gemeenschap — hun stem weegt zwaarder dankzij hun track record, niet dankzij een ambt.
Onion Gateway	Onion gateway	Het netwerkadres van een DID-identiteit op het onion-netwerk. Los van het DID-document — het kan worden gewijzigd zonder de identiteit te verliezen (vergelijkbaar met het wijzigen van het IP-adres achter een domein).
Onion Routing	Onion routing (Tor)	Een communicatieprotocol dat de oncenureerbaarheid van het netwerk waarborgt. Berichten worden in lagen versleuteld — elke node pelt één laag af maar kent het volledige pad niet.

Term	Nederlands	Betekenis
Oracle Problem	Orakelprobleem	Algemeen: hoe zorg je ervoor dat gegevens die een digitaal systeem binnenkomen getrouw overeenstemmen met wat er werkelijk in de fysieke wereld is gebeurd. De term komt uit het blockchainedomein. Hier: opgelost via autoriteiten die hun reputatie op het spel zetten als garantie dat een digitale registratie overeenstemt met de fysieke werkelijkheid.
Phenomenological	Fenomenologisch	Algemeen: een benadering die verschijnselen bestudeert zoals ze zich in de directe ervaring manifesteren, door te observeren wat eruit volgt, zonder vooraf gegeven theorieën. Hier: vrijheid, het maatschappelijk contract en gedragsnormen zijn geobserveerde verschijnselen — gevolgen van duizenden micro-interacties tussen mensen, geen van bovenaf gedefinieerde principes.

Term	Nederlands	Betekenis
Policy	Policy (beleid)	Algemeen: een verzameling regels of principes die het gedrag in een gegeven context regelen. Hier: elke deelnemer in het DID-netwerk verklaart zijn beleid — hoe hij reageert op specifiek gedrag van anderen, welke regels hij volgt, en welke straffen hij evenredig acht. Het geheel van beleidslijnen vormt het emergente maatschappelijk contract.
Proxy	Proxy	Algemeen: een plaatsvervanger of tussenpersoon — een systeem of entiteit die namens een ander handelt. Hier in twee contexten gebruikt: (1) ESR als een proxy die publieke uitgaven koppelt aan geplande betalingen; (2) waarnemers als een proxy tussen uitgever en verificateur in de waarnemerstruc.

Term	Nederlands	Betekenis
Publisher	Uitgever	Een netwerkdeelnemer die een registratie aanmaakt en publiceert (een bewering over een onrecht, herstel, enzovoort). Draagt de kosten van publicatie.
Reputation-Based Social Network (RSN)	Reputatienetwerk	Een gedecentraliseerd sociaal netwerk waar deelnemers feedback uitwisselen over gedrag in de echte wereld. Registraties zijn duur om aan te maken, goedkoop om te lezen.
Reputation Signal	Reputatiesignaal	Een individuele registratie in het netwerk — positief (herstel van schade, nakoming van een verplichting) of negatief (onrecht, contractbreuk). Cumulatief vormen signalen een reputatieprofiel.

Term	Nederlands	Betekenis
Social Graph	Sociale graaf	Het netwerk van je contacten en de contacten van je contacten. Het algoritme zoekt verificateurs op een instelbare diepte (bijvoorbeeld 3 niveaus). Geen globale blockchain — het netwerk vormt vanzelf gemeenschappen met overlappingsen.
Tax Allocation	Belastingtoewijzing	Een mechanisme waarmee de belastingbetaler beslist waar een deel van zijn belastingen naartoe gaat. Het toewijsbare percentage groeit jaar na jaar.
Track Record	Track record	Algemeen: de geschiedenis van eerdere resultaten, successen en mislukkingen van een persoon of organisatie. Hier: de som van alle eerdere interacties van een gegeven DID-identiteit in het netwerk — geverifieerde claims, aanvaarde en afgewezen registraties — waaruit haar reputatie wordt afgeleid.

Term	Nederlands	Betekenis
Verifier	Verificateur	Een deelnemer die algoritmisch wordt geselecteerd om een registratie te verifiëren en te publiceren. Zet zijn goede naam in op de waarachtigheid van de informatie.

Productienoten

Voorbehouden door de auteur (niet gedekt door de CC BY-SA-licentie): de naam en het woordmerk Personix, de boekomslag, en de steunkanalen (QR-codes, adressen, contact-e-mail). Afgeleide edities moeten deze elementen verwijderen of vervangen; ze mogen uitsluitend worden gebruikt om naar dit oorspronkelijke werk te verwijzen.

Bronbestanden. De volledige bron — markdown-tekst, infografieken, buildscripts — is beschikbaar naast deze PDF.

Hulpmiddelen. Bij het voorbereiden van de tekst en het itereren op formuleringen gebruikte de auteur ondersteuning van AI-hulpmiddelen; de infografieken zijn ontworpen in samenwerking met generatieve hulpmiddelen op basis van de specificaties van de auteur. Alle ideeën, argumenten en conclusies zijn die van de auteur zelf.

PERSONIX

Compromisloze verandering

Een oncensureerbaar en onomkoopbaar gedecentraliseerd reputatienetwerk

De staat werkte toen communicatie traag was, beslissingen lokaal waren, en het gezag in dezelfde stad woonde die het bestuurd. De netwerken van vandaag keren alle drie de aannames om — en de instellingen die erop zijn gebouwd passen niet langer bij de wereld die ze besturen. Dit boek beschrijft een instrument dat wel past: een gedecentraliseerd reputatienetwerk waarin identiteit van jou is om te houden, waarheid publiek auditeerbaar is, en omkoping reputationele zelfmoord is.

Geen manifest. Geen voorspelling. Een werkende blauwdruk voor hoe de opvolger van de staat kan worden gebouwd — vrijwillig, één verklaring per keer.

Pavel Kudrna • Praag, 2026

personix.org

Gelicentieerd onder Creative Commons Attribution-ShareAlike 4.0 International (CC BY-SA 4.0).