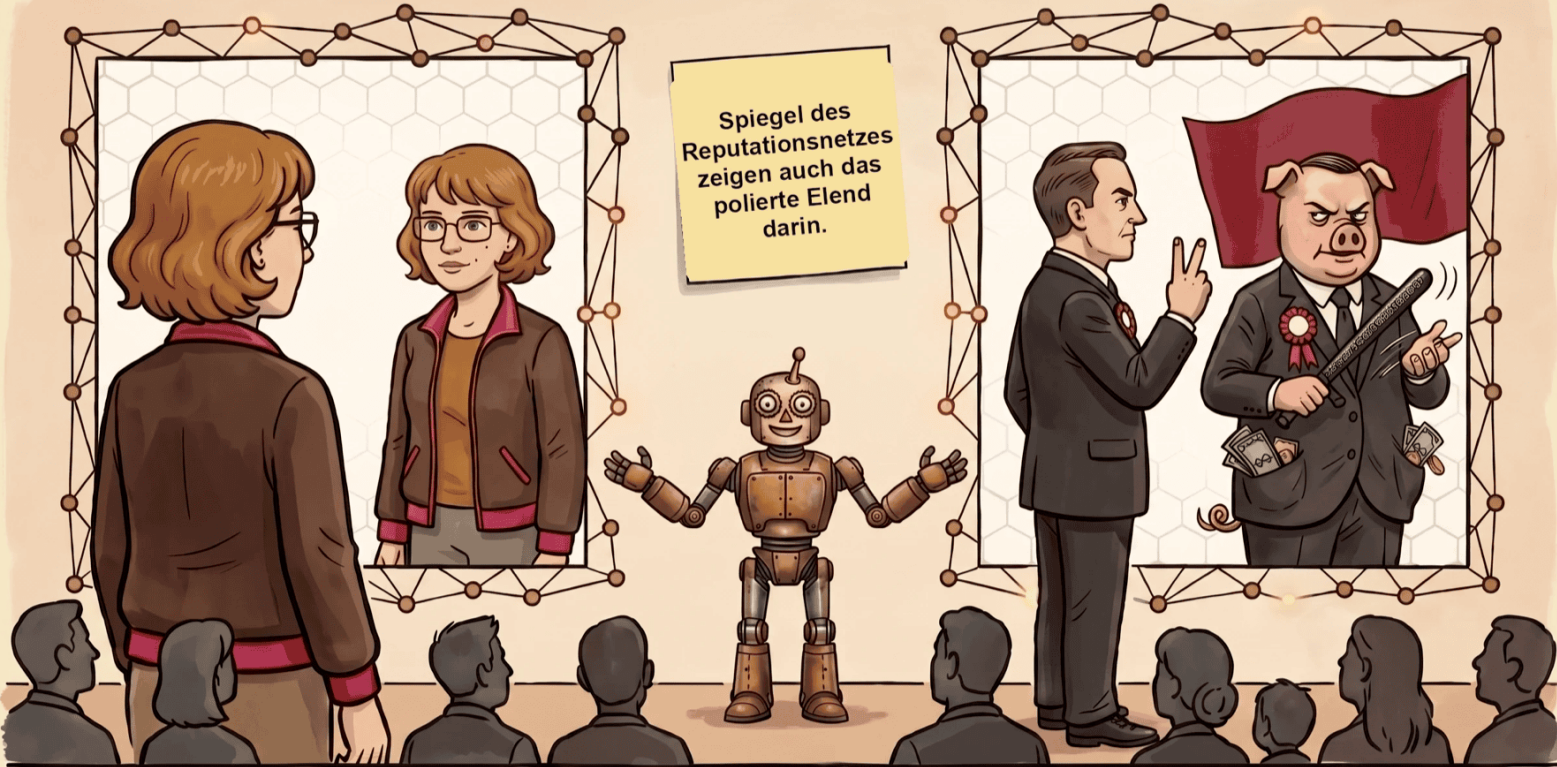


PERSONIX

Spiegel des
Reputationsnetzes
zeigen auch das
polierte Elend
darin.



**Ein unzensurbares und unbestechliches dezentrales Reputationsnetz
ein evolutionärer Nachfolger des Staates**

Personix — Kompromissloser Wandel

Ein unzensurbares und unbestechliches dezentrales Reputationsnetzwerk

© 2025–2026 Pavel Kudrna, Prag

Version 6 (2026-05-21)

Erstentwurf Juni–November 2025; überarbeitet April–Mai 2026.

Gesetzt in $\text{\LaTeX}$ (Tectonic) mit Palatino und Helvetica Neue.
A5 quer (210 × 148 mm).

Lizenziert unter **Creative Commons Attribution-ShareAlike 4.0 International (CC BY-SA 4.0)** — creativecommons.org/licenses/by-sa/4.0/. Die reservierten Elemente, das Quell-Repository und ein Hinweis zu den Produktionswerkzeugen sind am Ende des Buches aufgeführt.

Contents

Einleitung	7
Wovon handelt dieses Buch?	9
Wesentliche Voraussetzungen für den Wandel	17
Wesentliche Voraussetzungen für den Wandel	17
Das Werkzeug	28
Reputationsbasiertes soziales Netzwerk	28
Warum das Netzwerk unzensurierbar ist	54
Naheliegende Zweifel ausräumen	56
Abhängigkeit von der Technologie	56
Werfe ich Geld zum Fenster hinaus, wenn ich im Netzwerk veröffentliche?	58
Was, wenn jemand mehrere Identitäten erstellt?	58
Kann ein wohlhabender Mensch nicht einfach mehr Identitäten „kaufen“ (oder virtuelle Gemeinschaften erschaffen)?	61
Was ist mit Trittbrettfahrern, die nur lesen und der Gemeinschaft nichts geben wollen? . . .	64
Finanzielle Neutralität	65

Freiwilligkeit, Verantwortung und Freiheit	67
Der Schalter zwischen Freiheit und Totalitarismus (und Delegation)	68
Das Orakel-Problem — die Brücke zwischen digitaler und physischer Welt	76
Wie die Verifizierung funktioniert	78
Konsens und der Verifizierungsprozess	78
Roles in the verification transaction and authorities	85
Überblick über die Rollen	85
Aussteller	87
Autorität	87
Verifizierer	91
Subjekt	93
Beobachter	97
Der Mechanismus: Zeitstempel und Challenge-Code	97
Die Pointe: Du brauchst keine echten Beobachter	99
Delegation	101
Kommunikation zwischen den Rollen	106
Der emergente Gesellschaftsvertrag — Policy	106
Informationen über dich selbst bereitstellen	110

Verbrechen und Strafe	112
Verbrechen und Strafe	112
Der Spur des Geldes folgen	124
Der Spur des Geldes folgen	124
Der Schwachpunkt des Staates — das Geld	125
Proposed transition to the state's successor	126
Evolution, nicht Revolution	126
Vier Werkzeuge, die einander stützen	129
Einfaches Steuersystem — der Köder zum Einstieg	130
Elektronisches Ausgabenregister (ESR)	130
Bürgerliche Steuerzuweisung — das Gewicht der Entscheidung	132
Verhandlungsplattform mit dem Staat — der Hebel	136
Staatsbürgerschaft ohne Personalausweis	138
Überlappung und Umkehrbarkeit	142
Schluss	145
Der Weg existiert	145
Danksagung	147
Inspiration	147

Review und Feedback 147

Werkzeuge 147

Glossar **150**

Glossar 150

Einleitung

Hast du das Gefühl, dass du dich auf den Staat verlassen kannst?

Ich weigere mich zu akzeptieren, dass mir, meiner Familie oder jemandem in meiner Gemeinschaft ein offensichtliches Unrecht geschieht (körperlicher Schaden, Betrug, ungebührliche Einschränkung, ...) und der Staat antwortet: Ja, es ist ein Unrecht, aber unternimm nichts dagegen, sonst hast du ein noch größeres Problem mit uns. Ein solcher Zustand ist krank, und Menschen, die sich damit abfinden, sind Mittäter.

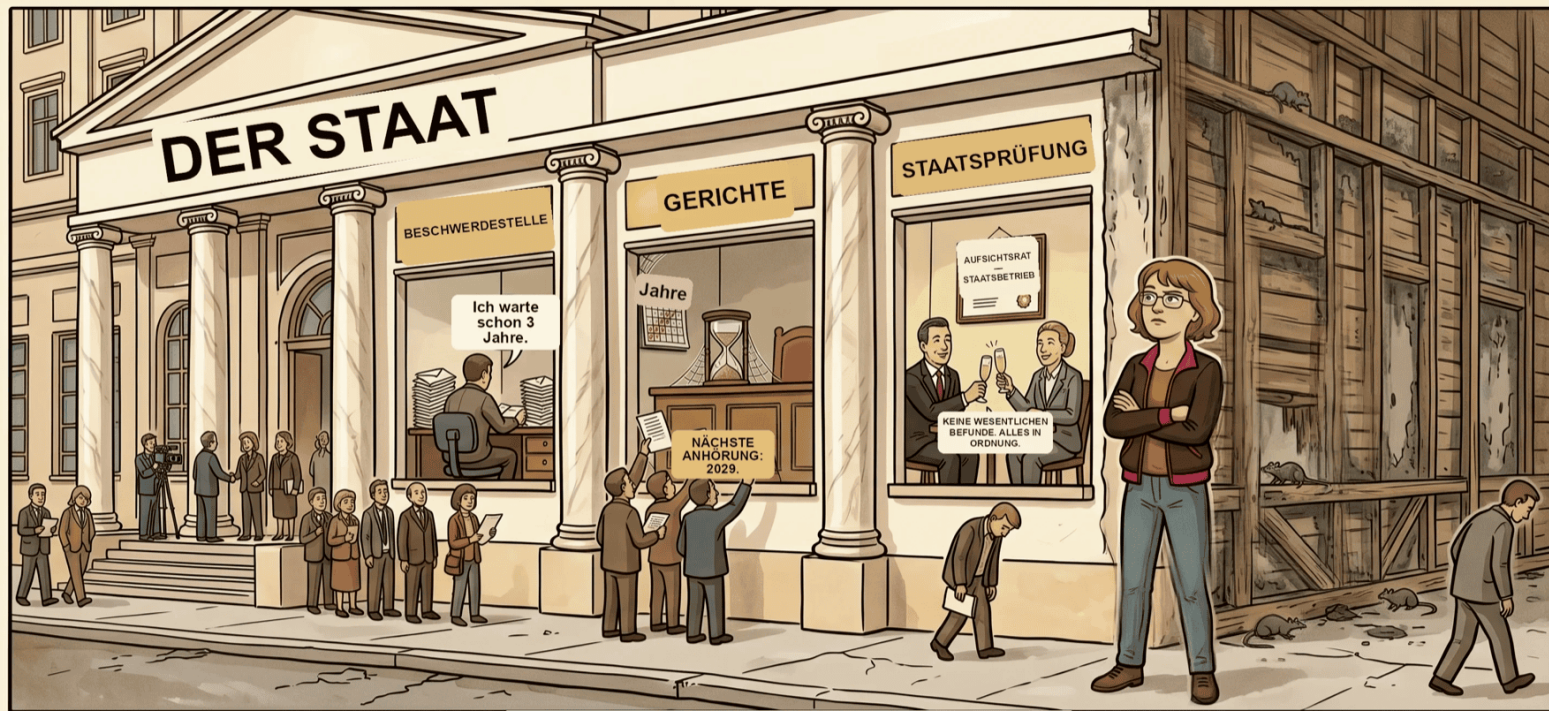
Das Ergebnis ist gegenseitige Entfremdung, das Spielen von Gemeinschaft, das Spielen von Staatlichkeit und ein sich vertiefender Zerfall der Gesellschaft mit der Aussicht auf schwere Konflikte.

Kann der Staat mit dem Tempo des technologischen und gesellschaftlichen Wandels Schritt halten, oder verhängt er lieber ein Verbot?

Ich könnte so tun, als würde ich Stillstand, Inkompetenz und Korruption als die erklärte Stabilität von Rechtsstaatlichkeit und Tradition betrachten, aber das will ich nicht mehr. Ich würde mich selbst belügen und ich würde dich belügen.

Spürst du die Herablassung von Beamten und gewählten Vertretern, wenn du es wagst, etwas zu kritisieren, wofür du bezahltst?

Ich weigere mich, Menschen in der Gesellschaft für unwürdig zu halten, gesamtgesellschaftliche Regeln mitzugestalten, nur weil sie sich nicht in jenen Soft Skills auszeichnen, die heute die einzige hinreichende Voraussetzung dafür sind, in den staatlich kodifizierten Institutionen ein gewählter Vertreter zu werden. Ich vertraue darauf, dass die überwiegende Mehrheit für sich selbst, ihre Liebsten



Ich weigere mich, das
anzunehmen.

und ihre Gemeinschaft sorgen kann — und dass sie darin ein Stück ihrer Lebensphilosophie sieht. Die meisten Menschen, die ich um mich herum kennengelernt habe, sind so.

Aber ich bin auch ausgesprochenen Arschlöchern begegnet, die gerade deshalb Arschlöcher waren, weil sie das Spiel zu spielen wussten — das Spiel, in dem die Gemeinschaft ihnen kein Feedback geben darf, in dem der Staat sie schützt, damit niemand die Ordnung stört, die das eigentliche Wesen des Staates bedrohen würde: ein bequemes Leben für jene auf den oberen Etagen der Machthierarchie und der Hierarchie ihrer Institutionen zu sichern. Der Feudalismus wurde durch die Herrschaft von Populisten und Elitisten ersetzt.

Liebst du es, wenn andere dir sagen, wie du dein Leben leben sollst?

Ich akzeptiere den gegenwärtigen Zustand nicht als vollkommene, endgültige Gegebenheit. Ich muss verantwortungsvoll damit umgehen, wie ich mich verhalte, und doch bin ich empfindlich, wenn mir jemand sagt, welche richtigen Werte ich haben sollte. Und du?

Wovon handelt dieses Buch?

Stell dir ein soziales Reputationsnetzwerk vor, in dem jeder, der möchte, seine eigenen Schlüssel dafür erzeugen kann (seine Identität erstellen), sich von Mitgliedern seiner Gemeinschaft einladen lässt oder sich auf eigene Faust hineinwagt. Du baust deine Reputation auf und greifst auf nützliche Reputationsdaten über andere zurück, wenn du sie brauchst. Du suchst die Unterstützung deiner Gemeinschaft, wenn ein Unrecht geschieht — du schilderst deinen Fall und lieferst, was du zur Sache hast, und die Gemeinschaft schaut sich das an, entscheidet nach Relevanz, ob sie es an andere weitergibt, und wie sie den Täter sanktioniert.

Dieses ganze kurze Buch handelt davon, was unter der Haube stecken muss, damit das nach außen hin so einfach funktioniert. Wenn du dabei bleibst, verspreche ich dir, dass sich eine Welt, die jetzt in vielerlei Hinsicht komplex und schwer verständlich erscheinen mag, als begreiflicher und klarer erschließen wird. Du wirst sehen, dass sich viele schlechte Dinge so einrichten lassen, dass sie sich für die schlechten Akteure nicht mehr so ungerecht auszahlen. Und es ist kein Werkzeug, an das du ständig online gefesselt sein müsstest — es genügt, danach zu greifen, wenn du das Gefühl hast, es zu brauchen.

Ich verspreche dir weiter, dass sich die hier beschriebene Ordnung den tatsächlichen Motivationen der Menschen näher anfühlen wird und dass sie diese nicht im Namen irgendeines -ismus umformen muss.

Und schließlich zeigen wir, wie sich ein nicht-revolutionärer Übergang zu einem Zustand bewerkstelligen lässt, in dem Gemeinschaften wieder zu voll funktionsfähigen sozialen Einheiten werden und nicht mehr nur so tun müssen als ob.

Technischer Artikel

Dieses Buch ist ein erläuternder Begleiter zum ursprünglichen technischen Artikel „*Decentralized Reputation Network: A Framework for Voluntary and Uncorruptible Societal Organization*“ (Pavel Kudrna, 2026). Wenn dich die formale Architekturbeschreibung, der Algorithmus zur Auswahl der Verifizierer und die Begründung der ökonomischen Mechanismen interessieren, empfehle ich, dort zu beginnen.

■ Die Kapitel bauen aufeinander auf

Das Buch ist als durchgehende Argumentation geschrieben — jedes Kapitel baut auf dem vorherigen auf. Konzepte, die in einem Teil eingeführt werden, werden in späteren Teilen verwendet, auch in Fußnoten. Ich empfehle nicht, außer der Reihe zu lesen.

■ Für wen ist dieses Buch?

Trotz seines optisch freundlichen Formats ist die Hauptzielgruppe der eher fachkundige Leser, der sich mit den Prinzipien möglicher sozioökonomisch-politischer Ordnungen der menschlichen Gesellschaft beschäftigt. Bis zu einem Punkt zu gelangen, an dem ich den gesamten Stoff der breitesten Öffentlichkeit verständlich erklären könnte, erfordert noch einen langen Weg des Aufbaus einer vollständigen Kommunikationsstrategie.

Ich begrüße Vorschläge, wie sich dieses kleine Werk oder etwaige überarbeitete Folgeauflagen verständlicher machen lassen.

Warnung

Ich weiß nicht, wer du bist, wie alt du bist oder wie viele gebrochene Versprechen du in deinem Leben aushalten musstest. Ich bin damit fertig, hier welche zu geben. Stattdessen möchte ich dich warnen,



Unter der Haube steckt mehr. Bleib dran.

dass das einzige Ergebnis dessen, was du hier lernst, die Erkenntnis sein könnte, dass es wahrscheinlich keinen Weg gibt, auf dem jemand anderes das heutige Chaos für dich aufräumt. Ich beschreibe nur einen Rahmen/ein Werkzeug, das das Aufräumen einfacher und transparenter machen könnte. Auf seiner Grundlage werde ich versuchen, ein soziales Experiment/eine Simulation vorzubereiten, mögliche Mängel zu beheben oder die Idee ganz zu begraben, falls sich herausstellt, dass sie grundlegende Konstruktionsrisse hat.

Eine Bitte

Ich wäre zutiefst dankbar, wenn du, auch nachdem du dieses Buch beendet hast, der Idee gegenüber aufgeschlossen bliebst und verfolgst, wohin sie führt und wie sie sich unter sachlicher Kritik behauptet. Noch mehr würde ich deine spätere Beteiligung schätzen — den Versuch, die vorgeschlagenen Gleichgewichtsprinzipien mit deinen eigenen Ideen zu brechen und damit besser zu prüfen, wie gut das System auf reales menschliches Verhalten vorbereitet ist.

Ohne dich und deine Beteiligung bleibt die Idee eine Theorie in der Schublade. Ohne dich und deine Beiträge und finanziellen Spenden werden wir das Projekt nicht in Richtung eines echten sozialen Experiments und damit einer echten Reife vorantreiben können. Ohne dich und deine sachliche Kritik werden wir dort stagnieren, wo wir jetzt sind, oder uns vom heiligen Gral der Zentristen verschlingen lassen — dem absoluten, unumkehrbaren Totalitarismus. Es liegt an uns, welchen Weg wir wählen oder aussitzen.

Die Herausforderung

Wir legen dir gerade keine leichte Last auf die Schultern. Du trägst bereits die Kosten einer verschwenderisch verwalteten Gesellschaft durch okkultistisch-beschwörende Handbücher, die behaupten, die Gesellschaft werde am besten zentral geführt — und ich habe die Frechheit, dich um noch mehr zu bitten und gegen diese Tendenzen anzugehen. Mir ist bewusst, dass wir den Zusammenbruch des größten



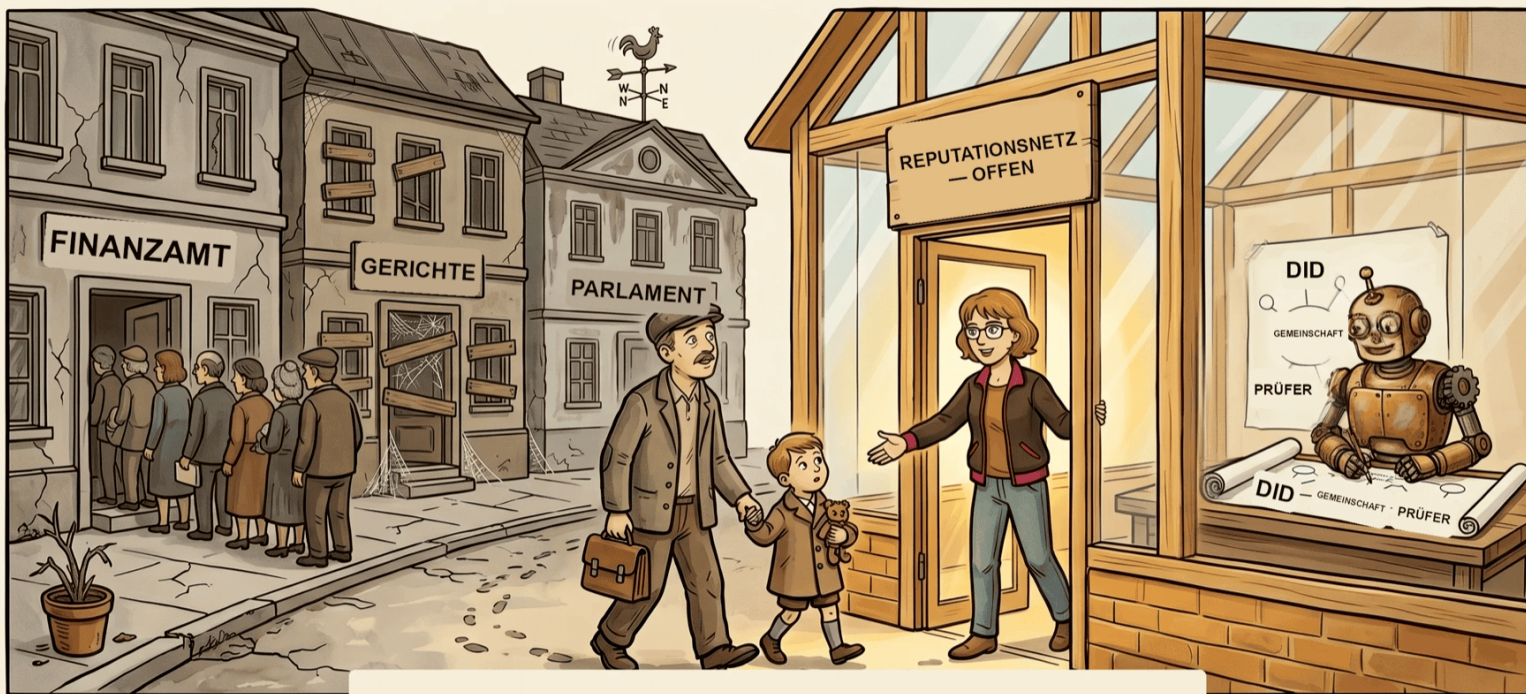
Eine bessere Welt ist das Gewicht wert.

Schneeballsystems der Geschichte — des umlagefinanzierten Rentensystems — überstehen müssen, ohne mehrere Generationen verhungern zu lassen.

Dennoch bitte ich dich: Lasst uns unseren Kindern endlich eine bessere Welt übergeben und ein Vermächtnis hinterlassen, das besagt, dass wir diesen Wandel geschafft haben. Wirtschaftliches Wachstum zu entfesseln könnte eine Teillösung für die am Horizont drohende Zwangslage sein. Wir können unseren Nachkommen dann sagen, es war ein Höllenritt und er war nicht umsonst.

Das Problem

Nur eine durch unmittelbare Verantwortung ausbalancierte Freiheit kann ein gewaltiges Potenzial freisetzen, das die Welt nie zuvor gesehen hat.



Komm rein. Die Pläne liegen bereit.

Wesentliche Voraussetzungen für den Wandel

Wesentliche Voraussetzungen für den Wandel

Die grundlegende Voraussetzung für einen Wandel zum Besseren ist, dass der Untergebene zum Übergeordneten wird — oder zumindest zum gleichberechtigten Partner. Das bedeutet, die kritischsten Agenden zu übernehmen, die das Verhältnis von Über- und Unterordnung definieren. Diese Agenden beruhen auf Nachweisen der Zugehörigkeit zu den Gemeinschaften, die die Bürger des Staates ausmachen. Sie sind Information und deren Überprüfbarkeit durch eine Autorität mit erheblicher Reputation innerhalb dieser Gemeinschaften.

Um das gegenwärtige System zu überwinden, bin ich zu fünf Voraussetzungen gelangt, die ich anschließend so erläutere, wie ich sie verstehe. Wir können uns diese Voraussetzungen als die Pfeiler vorstellen, die die Konstruktion des im Rest des Buches beschriebenen Systems tragen. Die Pfeiler habe ich zunächst nach eigener Präferenz gewählt und, während ich mit ihnen argumentierte, mein Verständnis jedes einzelnen nach und nach zur untenstehenden Form verfeinert.

Gehen wir diese fünf Pfeiler einen nach dem anderen durch.

VORAUSSETZUNGEN FÜR WANDEL

FREIWillIGKEIT



FREIWillIGKEIT

Ich entscheide
für mich
selbst.

ORGANISATION



ORGANISATION

Gemeinsam, unter
niemandem.

RESILIENZ



RESILIENZ

Nicht
zensierbar.

KONSENS



KONSENS

Kompromiss
durch Druck.

UNBESTECHLICHKEIT



UNBESTECHLICHKEIT

Nicht alle
sind käuflich.

Ohne diese fünf Säulen ist jede Veränderung nur verbrannte Zeit.

■ Freiwilligkeit

In unserem Fall bedeutet Freiwilligkeit, dass ich nicht gezwungen bin, am Betrieb des dezentralen Reputationsnetzwerks teilzunehmen. Ich kann jedoch kein positiv gefasstes Recht darauf einfordern, dass das Netzwerk keine Informationen über mich festhält — ob Informationen über mich im Reputationsnetzwerk landen, hängt allein von mir ab, von meinem Verhalten, meinen Handlungen und meiner Verantwortung.



Das ist nichts für mich.

Gib es zurück! Ich zeige dich beim Staat an!

Du musst nicht eintreten — außer du gibst ihnen Grund, sich zu erinnern.

Freiwillig — bis die Verantwortung dich einholt.

■ Organisation

Ein einzelnes Individuum kann das System nicht brechen, weshalb der Staat den Zusammenschluss von Menschen kontrolliert, um Aktivitäten zu verhindern, die seine Struktur und Funktionsweise bedrohen könnten. Dabei spielt es keine Rolle, ob sich Menschen dafür oder dagegen organisieren. Durch Organisation lässt sich die Wucht exemplarischer Strafen abmildern, wenn jemand es wagt, den Staat gegen dessen Willen zu verändern.

Setzen wir uns keine gemeinsamen Ziele, aber wir können einen Teil des Weges zusammen gehen. Die natürlichste Form ist der Zusammenschluss in Gemeinschaften — doch sie müssen über alle Werkzeuge verfügen, die sie brauchen, um nicht bloßes Schauspiel von Gemeinschaft zu bleiben.

■ Resilienz

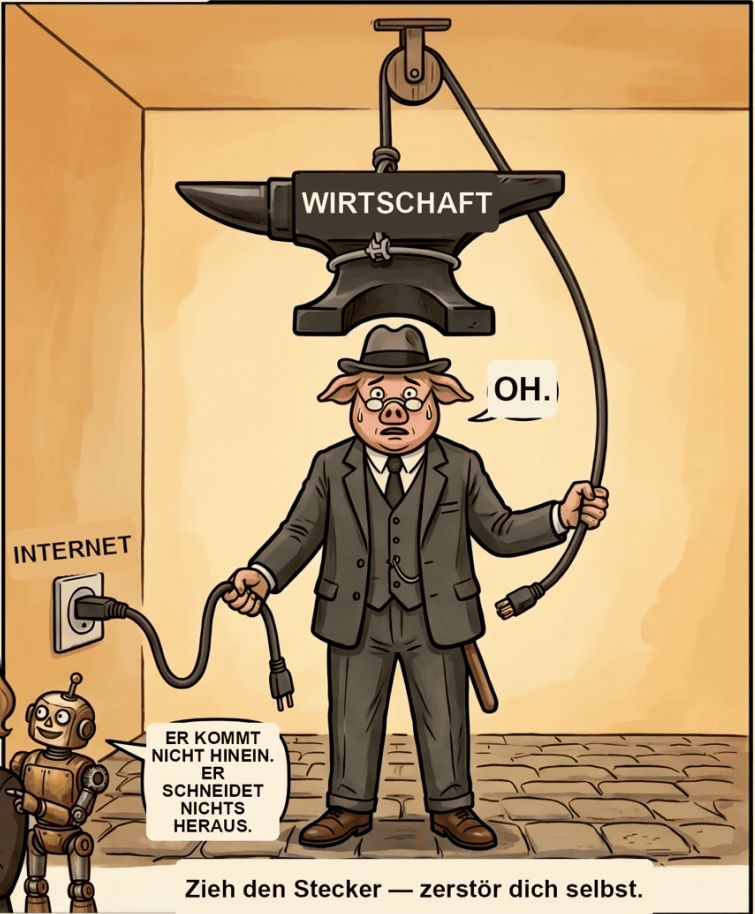
Der gewählte Weg zur Veränderung des Staates — oder zum Übergang zu seinem Nachfolger — darf nicht von der Erlaubnis des Staates abhängen. Die Werkzeuge und die Art, wie sie eingesetzt werden, müssen so unzensurierbar wie möglich sein. Schlicht gesagt: Die Kosten, sie zu zensurieren, müssen astronomisch sein. Ohne das ist das gesamte Unterfangen nur ein Verbrennen von Zeit und Lebensenergie.

VORAUSSETZUNG 2 VON 5: ORGANISATION



Ein Einzelner kann das System nicht brechen. Eine Gemeinschaft schon.

VORAUSSETZUNG 3 VON 5: RESILIENZ



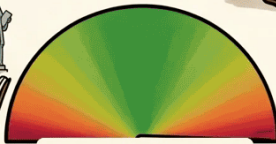
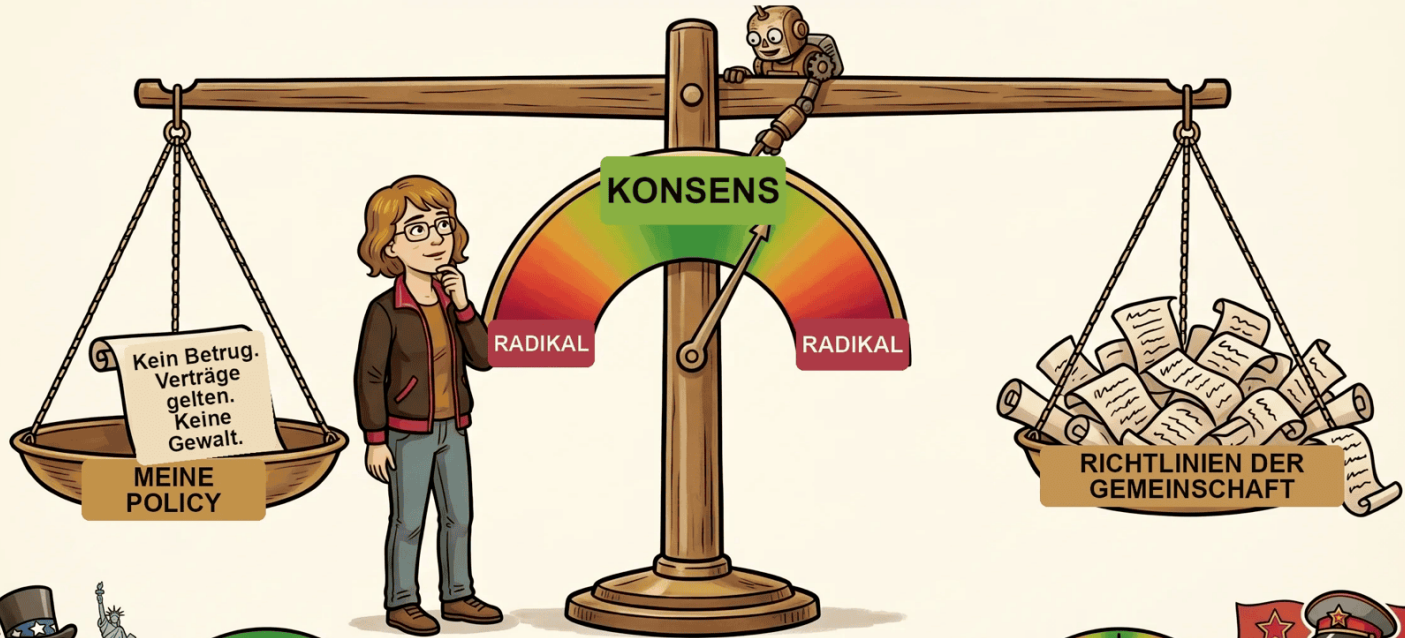
KEINE ERLAUBNIS NÖTIG. KEIN STECKER ZUM ZIEHEN.

■ Konsens

Die vorgeschlagene Lösung muss ihrem Wesen nach einen Mechanismus zum Aushandeln von Konsens ebenso enthalten wie eine repressive Komponente für die Fälle, in denen der Konsens verletzt wird. Es muss keine freiwillige Win-win-Vereinbarung sein. Es genügt, wenn Umstände und sozialer Druck einen Kompromiss innerhalb einer Gemeinschaft und zwischen Gemeinschaften sicherstellen.

IM RAHMEN BLEIBEN — KEIN RADIKALER.

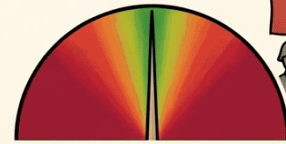
Du darfst abweichen. Nur nicht zu weit.



**FREIE
GESELLSCHAFT**

Die Toleranzzone weitet sich
mit der Freiheit der Kultur.

VORAUSSETZUNG 4 VON 5: KONSENS



**AUTORITÄRE
GESELLSCHAFT**



KONSENS IST EINE TOLERANZZONE, KEINE EINSTIMMIGKEIT.

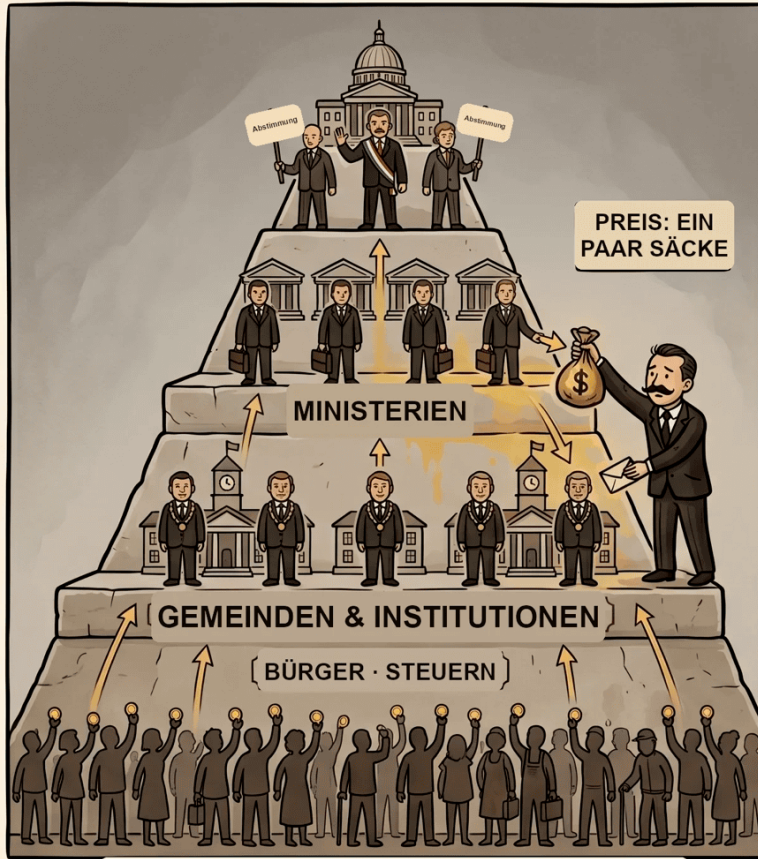
■ Unbestechlichkeit

Die Unzensurbarkeit verteidigt das System von außen. Doch ein Netzwerk von Menschen kann auch von innen verrotten — eine Autorität wird übernommen, eine erklärte Regel wird stillschweigend aufgegeben, Teilnehmer werden im Stillen gekauft. Die Unzensurbarkeit wäre ein hohler Sieg, wenn die Menschen im Inneren folgenlos korrumpiert werden könnten.

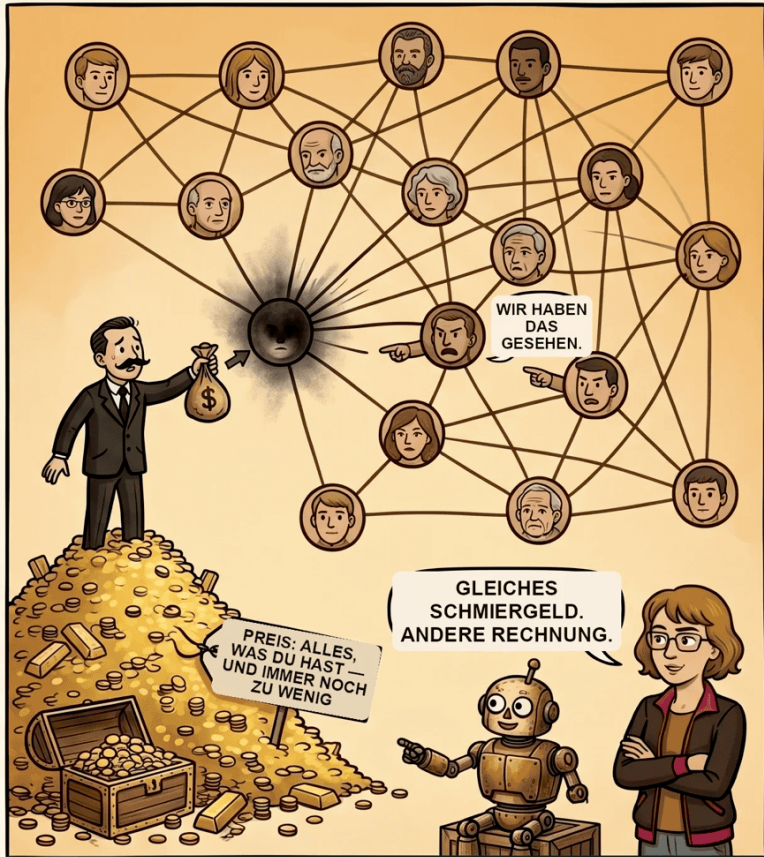
Unbestechlichkeit ist nicht das Ergebnis eines einzigen cleveren Kniffs. Sie entsteht daraus, dass **mehrere Prinzipien des vorgeschlagenen Designs zusammenwirken** — der Druck gegen Korruption ist über die Architektur verteilt, und die einzelnen Teile verstärken einander. Wie genau das erreicht wird, zeigen wir nach und nach — bei der Beschreibung des Werkzeugs, bei der Verifizierung und im Kapitel über die Strafe. Am Ende fassen wir alles zusammen, was aufgebaut wurde.

Unbestechlichkeit ist zugleich eine Voraussetzung des Designs und eine emergente Eigenschaft des Ergebnisses. Sie ist die zweite Verteidigungslinie — die nach innen gerichtete — und ohne sie ist die Resilienz nur ein halber Schild.

VORAUSSETZUNG 5 VON 5: UNBESTECHLICHKEIT



Bestich ein paar obere Etagen — die Basis zahlt trotzdem.



Bestich einen — er verliert seine Reputation für immer. Bestich alle — du gehst zuerst pleite.

KORRUPTION HAT EINEN PREIS. IM NETZ IST ER ZU HOCH.

Das Werkzeug

Reputationsbasiertes soziales Netzwerk

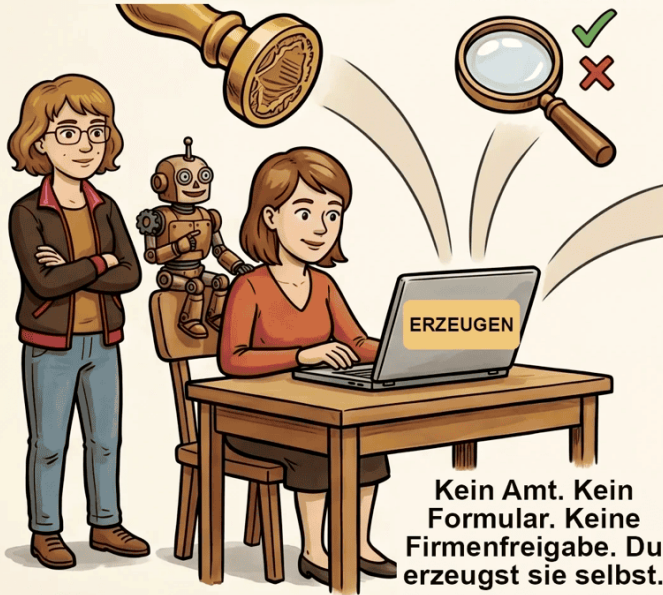
Um einen Wandel herbeizuführen, brauchen wir ein sorgfältig entworfenen Werkzeug. Zuerst skizzieren wir es kurz. In späteren Kapiteln betrachten wir jeden Baustein genauer und fügen mehr hinzu. Stell dir ein unzensurbares, globales, dezentrales soziales Netzwerk vor, in dem du sicher deine stellvertretende Identität erstellen und verwalten könntest — eine sogenannte dezentrale Identität (DID). Eine DID ist eine digitale Identität, die du selbst erstellst und kontrollierst, ohne Abhängigkeit von einer zentralen Autorität. Niemand kann sie dir wegnehmen oder fälschen, denn sie ist kryptografisch mit deinem privaten Schlüssel (oder mehreren Schlüsseln, per Multisig) signiert.

DEINE IDENTITÄT, DEINE SCHLÜSSEL, DEINE REGELN

DU ERSTELLST SIE SELBST

PRIVATER SCHLÜSSEL
— signiert für dich. Nur du hast ihn. Nie teilen.

ÖFFENTLICHER SCHLÜSSEL — prüft deine Signaturen. Für das Netz sichtbar.



DEIN DID-DOKUMENT



Das ist deine öffentliche Identität. Jeder kann sie lesen. Nur **DEIN** privater Schlüssel kann Änderungen signieren.



MELDUNGEN — GEPRÜFTE FAKTEN ÜBER DICH

STAATSBÜRGERSCHAFT:
Tschechische Republik — geprüft vom Stadtnotar

BILDUNG: MSc Informatik — geprüft vom Alumni-Netz der Universität

EIGENTUM: Besitzer der Wohnung #42 — geprüft vom lokalen Gemeinderegister

PASSIVER ZEUGE: Unrecht ignoriert — Policy nicht eingehalten — gemeldet von Nachbarschaftszeugen

BETRUG: Nachbarn um Ersparnisse geprellt — eingereicht vom örtlichen Gemeinschaftsgericht

Meldungen sind geprüfte Aussagen. Gute wie schlechte. Autoritäten setzen ihre Reputation dafür ein.



STAATLICHER AUSWEIS — WIDERRUFBAR: der Staat kann ihn jederzeit annullieren.



DID — UNWIDERRUFLICH: nur dein privater Schlüssel signiert Änderungen.

Deine Identität. Deine Schlüssel. Deine Regeln. Keine Erlaubnis nötig.

Anmerkung

Eine Konsequenz ist, dass eine solche Identität nach und nach staatlich ausgestellte Ausweisdokumente ersetzen könnte — dazu aber mehr im Kapitel über den Übergang.

In einem solchen Netzwerk könntest du über deine Identität melden, dass dir jemand einen Schaden zugefügt hat (und später womöglich, dass er ihn behoben hat oder dazu gezwungen wurde). Damit dieses Feedback — gerichtet an den Verursacher des Schadens — als relevante Quelle Wert hat, muss das Einspeisen von Informationen ins Netzwerk Zeit, Energie und Geld kosten — und darüber hinaus muss für andere ein überprüfbarer Beweis erbracht werden, dass es sich nicht um leeres Gerede handelt.

Das Lesen von Informationen wäre einfach und relativ günstig, doch das Anlegen eines einzelnen Eintrags wäre kostspielig und anspruchsvoll. Das Schreiben würde einem klaren Protokoll folgen, in dem eine Berechnung nach dem gewählten Algorithmus streng festlegt, welche DID zur Verifizierung der eingereichten Information zu befragen ist und wie vorzugehen ist, damit der ausgewählte Teilnehmer die Information in deinem Namen verarbeitet, sie veröffentlicht und ihr Verifizierer wird.

■ Algorithmus vs. Radikalismus

Die algorithmische Auswahl der Verifizierer stellt sicher, dass nicht-radikale Informationsveröffentlicher mit der Zeit eine nahezu neutrale Bilanz zwischen den Kosten veröffentlichter Informationen und den Belohnungen für die Verifizierung halten.

VERÖFFENTLICHEN KOSTET ZEIT, ENERGIE UND GELD

INS NETZ SCHREIBEN IST NIE GRATIS — LESEN SCHON

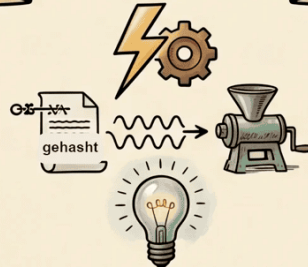
DREI KANÄLE — ALLE DREI SIND ECHT

ZEIT



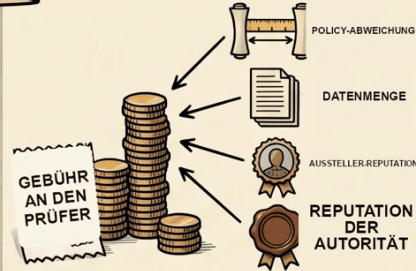
du wartest, während der Algorithmus einen Prüfer wählt und der Prüfer deinen Eintrag liest.

ENERGIE



Signieren, Hashen, Prüfen — jeder Schritt ist echte Rechenleistung und echter Strom.

GELD



je weiter deine Meldung von der Richtlinie des Prüfers entfernt ist, je größer der Eintrag und je weniger dem Aussteller oder seiner Autorität vertraut wird — desto höher die Gebühr.

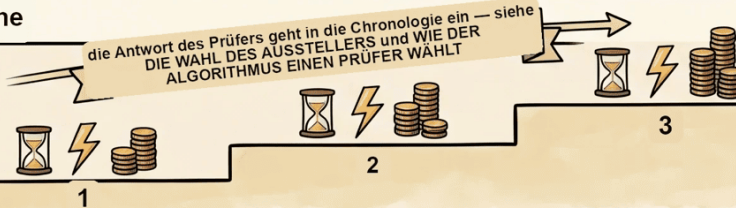
WAS ALS NÄCHSTES GESCHIEHT

- Die dreistufige Prüfkette — siehe WIE DER ALGORITHMUS EINEN PRÜFER WÄHLT, WIE DER PRÜFER ANTWORTET, DIE WAHL DES AUSSTELLERS
- Warum teures Schreiben die Reputation schützt — später im Kapitel

Rauschen ist teuer. Signal ist wertvoll. (Darm verlangt das Netz Geld fürs Schreiben, nicht fürs Lesen.)

Kosten über die Versuche

JEDER NEUE VERSUCH KOSTET MEHR



jede Ablehnung oder neue Ziehung wächst die Chronologie, die der Algorithmus frisst — und der nächste Versuch kostet in allen drei Kanälen mehr.

Leseasymmetrie

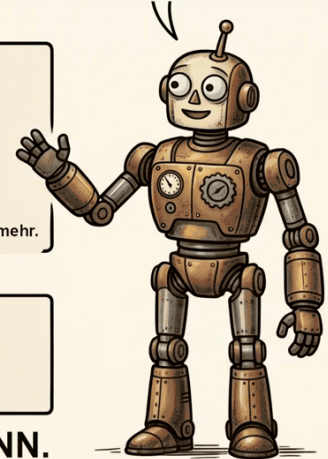
LESEN IST BILLIG



Abfrage gratis

jeder darf Reputation und Einträge lesen — nur Schreiben kostet. Die Asymmetrie ist Absicht.

SCHREIBEN KOSTET — LESEN NICHT. DIE ASYMMETRIE IST DER SINN.



Schauen wir uns an, wie der Algorithmus einen Verifizierer auswählt.

■ Algorithmus

Die algorithmische Auswahl wählt für verschiedene Informationen nicht-deterministisch einen anderen Verifizierer (oder eine Menge möglicher Verifizierer). Ein Hash (eine mathematische Einwegfunktion, die aus einer beliebigen Eingabe einen eindeutigen „Fingerabdruck“ erzeugt — wie ein Fingerabdruck eines Dokuments) des vollständigen DID-Dokuments bestimmt die Position auf einem konsistenten Hash-Ring und wählt die Kandidaten für die Verifizierung aus.

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

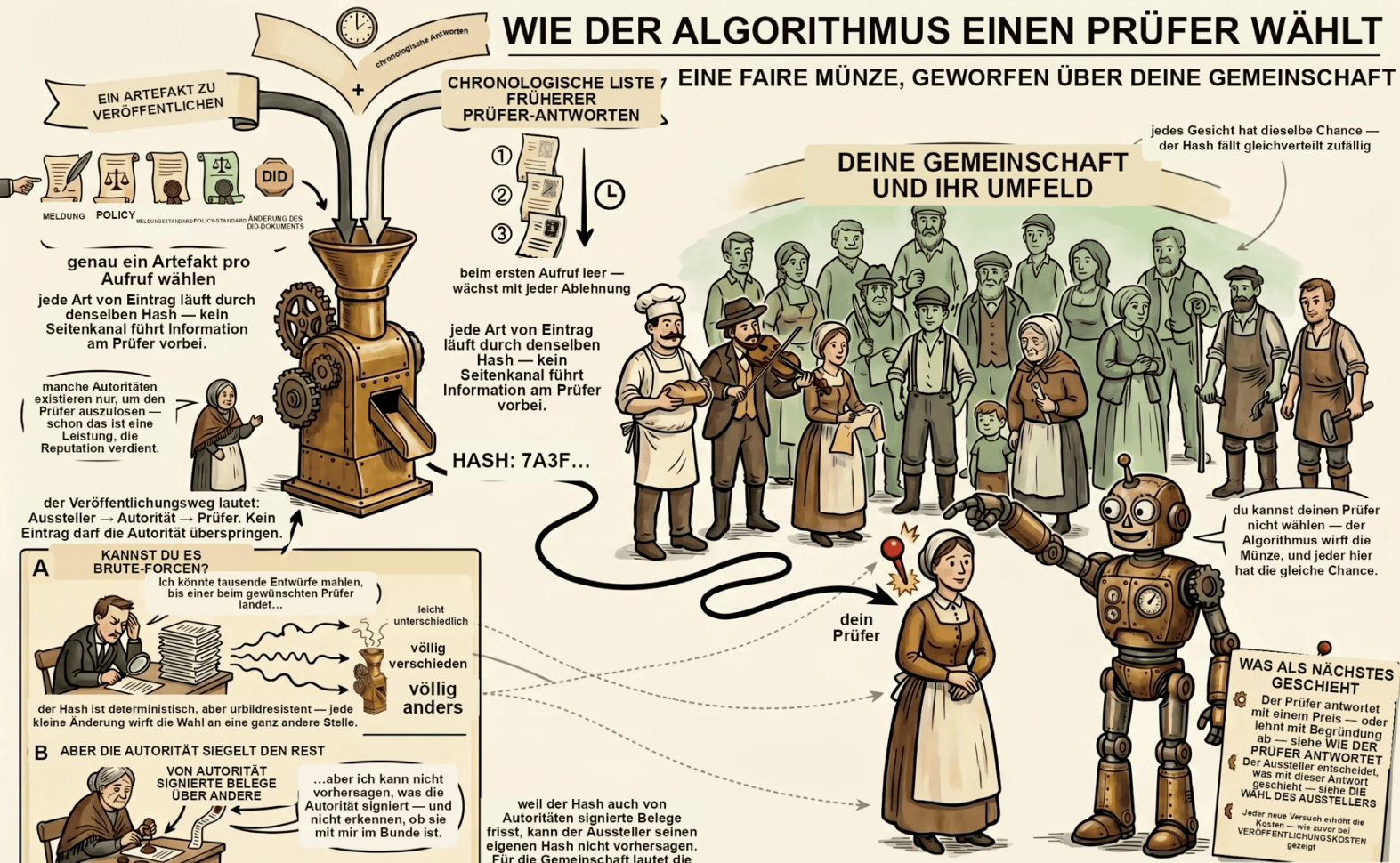
Einfach gesagt: Der Algorithmus nimmt dein gesamtes DID-Dokument, berechnet daraus einen Fingerabdruck, und dieser Fingerabdruck bestimmt deinen Verifizierer.

Beim ersten Verifizierer, den der Algorithmus auswählt, hast du als Veröffentlichender womöglich keinen Erfolg — deine Reputation oder deine erklärten Einstellungen erfüllen vielleicht seine Anforderungen nicht. Du würdest die Suche nach dem nächsten algorithmisch fortsetzen, indem du eine weitere rekursive Iteration durchführst, die dir einen weiteren Verifizierer zuweist. Mit jedem Schritt wächst die „Distanz“ zum Zielverifizierer, und ebenso wachsen die begleitenden Metadaten, die veröffentlicht werden müssen. Mit den Daten steigen naturgemäß auch die Kosten (nicht nur wegen der anfänglichen Größe der Behauptung, sondern auch wegen der mit jeder Ablehnung anwachsenden Metadaten). Glaubwürdige

Informationen kommen weit leichter durch als unsinnige Launen. Es liegt an jedem selbst, wie hohen Preis er zu tragen bereit ist und wie viel ihm der Eintrag bedeutet — Radikalismus wird garantiert teuer.

WIE DER ALGORITHMUS EINEN PRÜFER WÄHLT

EINE FAIRE MÜNZE, GEWORFEN ÜBER DEINE GEMEINSCHAFT

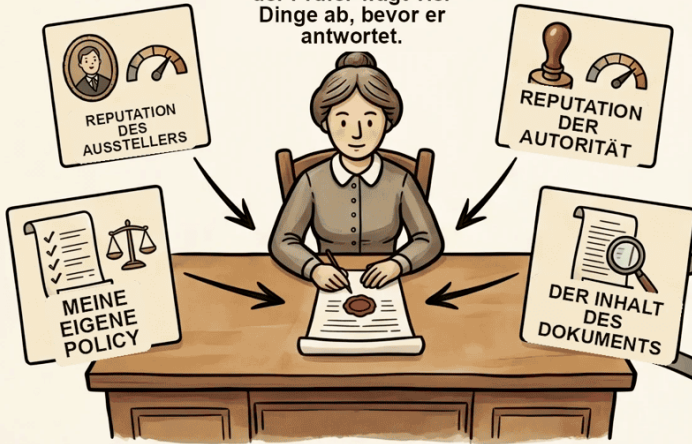


DER ALGORITHMUS WÄHLT — NICHT DU.

WIE DER PRÜFER ANTWORTET

ANNEHMEN GEGEN PREIS — ODER ABLEHNEN MIT GRUND

der Prüfer wägt vier Dinge ab, bevor er antwortet.

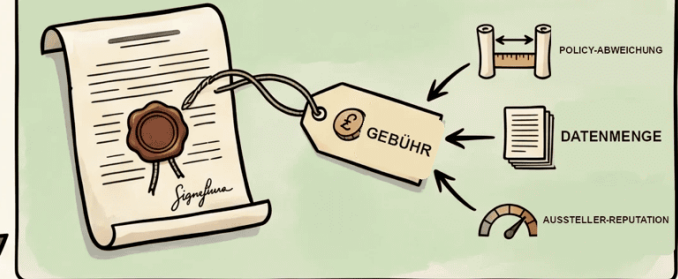


ABLEHNEN — MIT BEGRÜNDUNG

- die Reputation des Ausstellers ist mir zu niedrig
- der Autorität hinter diesem Eintrag vertraue ich nicht
- die Richtlinie des Ausstellers liegt zu weit von meiner entfernt
- das Dokument selbst verstößt gegen die Regeln meiner Richtlinie

der Prüfer schreibt WARUM auf — seine Antwort fließt in den nächsten Versuch ein.

ANNEHMEN — GEGEN PREIS



der Prüfer stimmt der Veröffentlichung zu — aber der Preis richtet sich danach, wie weit die Meldung von seiner Richtlinie entfernt ist, wie viele Daten sie trägt und wie vertrauenswürdiger der Aussteller ist.

die Antwort des Prüfers kommt in die chronologische Liste — wie in WIE DER ALGORITHMUS EINEN PRÜFER WÄHLT gezeigt

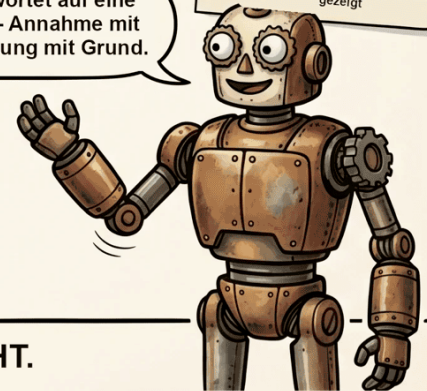
was der Prüfer auch sagt, seine Antwort wird zur Eingabe des nächsten Zuges.

jeder Prüfer antwortet auf eine von zwei Arten — Annahme mit Preis oder Ablehnung mit Grund.

WAS ALS NÄCHSTES GESCHIEHT

- Der Aussteller entscheidet, was mit dieser Antwort geschieht — siehe DIE WAHL DES AUSSTELLERS
- Jede Antwort verschiebt die Kosten des nächsten Versuchs — Wie zuvor bei VERÖFFENTLICHUNGSKOSTEN gezeigt

DER PRÜFER NENNT EINEN PREIS — ODER SAGT DIR, WARUM NICHT.



Was auch immer der Verifizierer als Antwort auf deine Verifizierungsanfrage entscheidet, der Ball liegt wieder beim Veröffentlichler: Er kann das Angebot des Verifizierers für Verifizierungsdienste annehmen, die Antwort in die Chronologie einfügen und es (teurer) erneut versuchen oder aufgeben und die versunkenen Kosten schlucken.

Um deiner Information mehr Gewicht und eine bessere Chance auf Annahme bei den Verifizierern zu geben, könntest du — als Veröffentlichler mit einem Interesse an der Herausgabe der Information — die Dienste einer **vertrauenswürdigen Autorität** in Anspruch nehmen. Die Autorität lehnt die eingereichte Information entweder ab oder nimmt sie an und setzt ihren guten Namen (ihre Reputation) darauf. Die Autorität verlangt in der Regel reale Nachweise, überprüft sie und ordnet sie ein. Das Ergebnis ist ein Protokoll ihrer Bewertung des jeweiligen Falls zum jeweiligen Zeitpunkt. Denke dir eine Autorität als Spezialisten für eine bestimmte Art von Dienstleistung sowohl in der realen als auch in der digitalen Welt — zum Beispiel einen Ermittler, einen Auditor, einen Versicherer, einen Lieferanten einer bestimmten Warenklasse (im Grunde jeden Wirtschaftsakteur auf dem Markt).

DIE WAHL DES AUSSTELLERS

WAS MIT DER ANTWORT DES PRÜFERS TUN

was der Prüfer auch sagte, der Aussteller hat nun EINE Antwort auf dem Tisch.



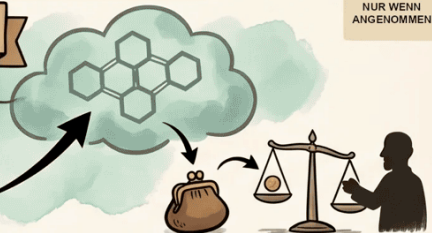
zurück zu WIE DER ALGORITHMUS EINEN PRÜFER WÄHLT — siehe oben

nur der Wiederholungspfad kreist — Annahme und Rückzug beenden die Geschichte.

DREI AUSWEGE

DEAL ANNEHMEN

DID-Netz



NUR WENN ANGENOMMEN

der Aussteller zahlt die Gebühr — der Eintrag wird ins Netz veröffentlicht. Nur möglich, wenn der Prüfer zugestimmt hat.

NOCHMAL VERSUCHEN



Mini-Schleifmaschine



jeder neue Versuch kostet mehr

die Antwort wird in die Chronologie eingereiht — der Algorithmus wirft erneut. Gilt, ob der Prüfer zu einem ungeliebten Preis zustimmte oder rundweg ablehnte.

WEGGEHEN



verbrauchte Zeit und Energie kommen nicht zurück

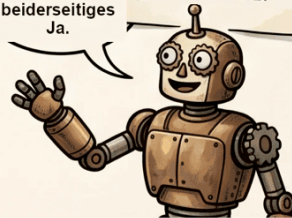


der Aussteller verwirft den Entwurf. Nichts wird veröffentlicht — aber auch nichts mehr bezahlt.

WAS ALS NÄCHSTES GESCHIEHT

Jeder neue Versuch verschiebt die Kosten des nächsten — wie zuvor bei VERÖFFENTLICHUNGSKOSTEN gezeigt
Die Antwort des Prüfers selbst — wie zuvor gezeigt bei WIE DER PRÜFER ANTWORTET

der Prüfer entscheidet wie — der Aussteller, ob. Veröffentlichen ist ein beiderseitiges Ja.



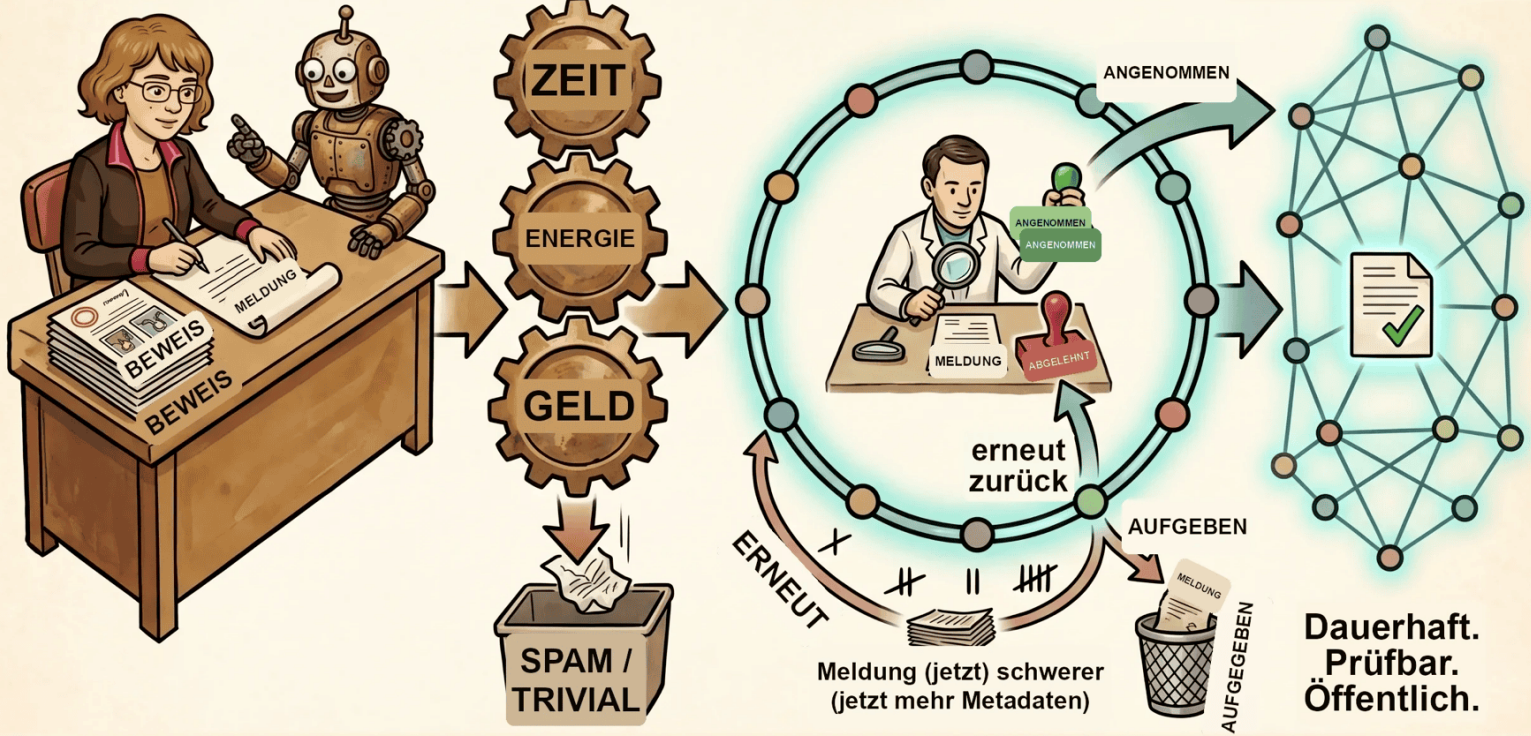
DER PRÜFER SCHLÄGT VOR — DER AUSSTELLER ENTSCHEIDET.

STUFE 1 —
MELDUNG
VERÖFFENTLICHEN

STUFE 2 —
QUALITÄTSFILTER

STUFE 3 —
REKURSIVE
PRÜFUNG

STUFE 4 —
DAUERHAFTER
EINTRAG

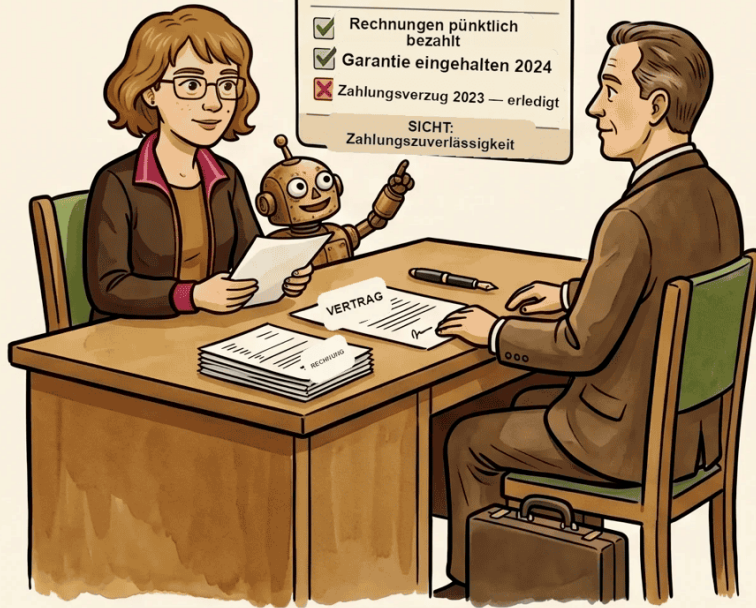


TEUER ZU FÄLSCHEN. BILLIG ZU PRÜFEN.

Wenn du versuchst, Informationen ins Netzwerk zu stellen, enthält es wahrscheinlich schon Informationen über seine Akteure — das sind Reputationssignale. Sich zurechtzufinden, wie man Reputationssignale liest — was sie für dich in verschiedenen Situationen bedeuten und welche Risiken sie bergen —, ist vielleicht nicht trivial. Jeder Teilnehmer kann Reputationseinträge über seine DID unterschiedlich betrachten, je nach der Situation, mit der er es gegenüber der Gegenseite zu tun hat. Ist die Gegenseite ein zuverlässiger Zahler, oder muss ich für ein Geschäft Geld im Voraus verlangen? Trägt das angebotene Produkt Bewertungen über verborgenen Betrug oder Mängel? Versucht sie, sich aus der vertraglichen Verantwortung zu winden, wenn etwas schiefgeht? Manchmal kommt ein komplexerer Blick auf die Gesamtkonsistenz der Gegenseite gelegen — es hängt von den Präferenzen dessen ab, der die Übersicht anfordert. Der Markt könnte Produkte und Dienstleistungen anbieten, die das Lesen der Reputation im Kontext der jeweiligen Situation vereinfachen, aufbereiten und verdeutlichen. Auch verschiedene Autoritäten und ihre angebotenen Dienste können diesem Zweck dienen.

WIE MAN REPUTATION LIEST

INFORMIERTE ENTSCHEIDUNG



Sie weiß, mit wem sie es zu tun hat.

BLINDES VERTRAUEN



Er hat keine Ahnung, mit wem er es zu tun hat.

BEVOR DU KREDIT GIBST. BEVOR DU UNTERSCHREIBST. BEVOR DU VERTRAUST.

■ Beispiele

Typische Informationen, die für Veröffentlichler von Interesse — und für andere wertvoll — sind, betreffen Ereignisse jenseits der gewöhnlichen zwischenmenschlichen Kommunikation in der realen oder virtuellen Welt.

Negative Beispiele: - Belege für strafbare Handlungen (z. B. von einer vertrauenswürdigen Ermittlungsstelle geprüft) - Indizienbeweise (für sich allein schwach, aber statistisch kumulativ) — z. B. wiederholte Anwesenheit in der Nähe mehrerer Diebstähle in kurzer Zeit → noch Zufall? - Vertragsbruch

Positive Beispiele: - behobener Schaden (freiwillig oder unter Druck der Gemeinschaft als Strafe) - Annahme und Verbüßung einer von Autorität X vorgeschlagenen Strafe - Autorität X hat die Anerkennung der Eigentumsrechte des Täters in gewissem Umfang entzogen

Es liegt an jedem selbst, verfügbare Informationen über die Gegenseite zu sammeln und die Risiken nach seinen Präferenzen zu bewerten.

WELCHE ARTEN VON MELDUNGEN GIBT ES?

BEISPIELE DES MELDUNGS-ARTEFAKTS

—

NEGATIVE MELDUNGEN



ÜBERGRIFF

hat einen anderen körperlich angegriffen



DIEBSTAHL

fremdes Eigentum ohne Zustimmung genommen



BETRUG

hat jemanden zum eigenen Vorteil getäuscht



GEBROCHENER VERTRAG

hat eine vereinbarte Pflicht nicht erfüllt



VERLEUMDUNG

eine schädliche Unwahrheit verbreitet



AUFGABE

hat Angehörige oder Pflichten vernachlässigt

+

POSITIVE MELDUNGEN



SCHADEN BEHOBEN

früher verursachten Schaden behoben



SCHULD BEGLICHEN

hat die Schuld voll beglichen



HILFE GELEISTET

hat einem anderen unter eigenem Verzicht geholfen



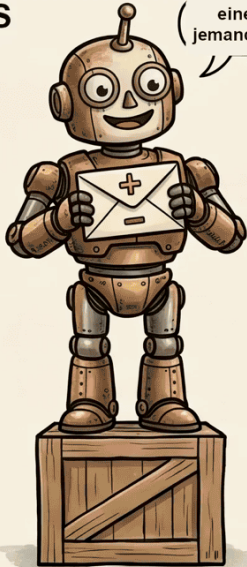
GEPRÜFTE EXPERTISE

nachgewiesenes Können in einem Handwerk oder Fach



HERAUSRAGENDER DIENST

langjähriger Beitrag zur Gemeinschaft



(eine Meldung ist eine Aussage über jemanden — dies sind die üblichen Arten.)



nur Beispiele — jede Meldung folgt einem Meldestandard, und jeder Standard kann mehr hinzufügen.

du musst nicht beitreten — aber wenn dein Verhalten andere trifft, kann jemand eine Meldung darüber veröffentlichen.

ÜBER MELDUNGEN GELANGT VERHALTEN INS NETZ.

■ **Ob Informationen über dich im Netzwerk erscheinen, hängt ausschließlich von deinem eigenen Verhalten ab.**

Du musst einem solchen Netzwerk nie beitreten, und dennoch können Informationen über dich darin erscheinen. Es hängt ausschließlich von deinen Handlungen und deren Auswirkungen auf andere ab.

DIE GEMEINSCHAFT KANN DIR EINE ERÖFFNEN



Er hat keine eigene DID.
Er hat sich nie
angemeldet.



Du hast keine DID eröffnet, also
eröffnet die Gemeinschaft eine ÜBER
dich. Negative Meldungen hängen hier.



Du kannst eine eigene
eröffnen — doch die
Gemeinschaft verknüpft
beide. Reputation folgt der
Person, nicht dem Schlüssel.

1. DU RICHEST
SCHADEN AN

2. GEMEINSCHAFT
MELDET

3. DU ENTKOMMST
NICHT

Du kannst auf eine DID verzichten. Auf deine Reputation nicht.

Was ich soeben kurz skizziert habe, ist, wie ein von der dezentralen Identität (DID) inspiriertes soziales Netzwerk funktionieren könnte. Der Hauptzweck der DID-Konzepte ist es, Privatsphäre und Freiheit durch das Prinzip zu stärken, sich zu den Regeln zu bekennen, denen ich folgen und nach denen ich leben werde — indem den Nutzern die Möglichkeit gegeben wird, zu entscheiden, welche Informationen sie unter welchen Bedingungen teilen.

Ich schlage vor, DIDs weiter zu einem Kommunikationsnetzwerk zu verbinden, in dem ihre Inhaber Feedback austauschen, auch über Situationen hinaus, in denen jemandem etwas zugestoßen ist und die Gemeinschaft oder ein Einzelner reagieren muss. Ein solcher präventiver Abgleich der Regeln, zu denen wir uns bekannt haben — mit der Möglichkeit, die wirtschaftlichen und sonstigen Folgen gegenseitiger Abweichungen in den Erwartungen darüber, wie die andere Seite agieren sollte, zu berechnen —, ließe sich als Motivation zum Finden von Konsens betrachten. Statt Freiheit würde ein solches System freiwillige Entscheidung in Verbindung mit Verantwortung für das Verhalten in der realen Welt betonen.

Ein Individuum kann das System nicht allein brechen — eine Gruppe von Menschen hat eine größere Chance, und eine Gruppe von Menschen mit ausgehandeltem Konsens und Motivationen, in vielen Fragen an einem Strang zu ziehen, hat eine noch größere Chance, autoritären Tendenzen zu widerstehen. Die Voraussetzung der Organisation aus dem ersten Kapitel wird erfüllt sein, sobald zwei Bedingungen gegeben sind: Das DID-Reputationsnetzwerk deckt Gemeinschaften repräsentativ genug ab, dass seine Nutzung nicht mehr exotisch ist. Und zugleich wird dieses Gemeinschaftssegment zu einer wirtschaftlich bedeutsamen Minderheit, die selbstbewusst mit dem Rest der Gesellschaft verhandeln kann.

■ Freiwilligkeit vs. Freiheit

Freiheit — im positiven Sinne — wäre ein sekundärer Effekt des Ausbalancierens zweier Faktoren: der Freiwilligkeit und des Drucks der Umgebung hin zur Verantwortung.

■ Das KI-Zeitalter und der Wert der Reputation

Im Zeitalter der künstlichen Intelligenz wird alles, was mit kognitivem Denken zusammenhängt, automatisiert — und es könnte noch weiter gehen. Was bleibt dann in der menschlichen Tätigkeit als Wettbewerbsvorteil? Die Antwort ist schwierig, und etwas wird sich sicher finden, aber eines können wir mit Gewissheit sagen: Die Reputation wird entscheiden. Eine überprüfbare Geschichte deines Verhaltens, deiner Verpflichtungen und ihrer Erfüllung — das ist etwas, das die KI nicht für dich aufbauen wird.

WENN DIE KI DENKT — WAS BLEIBT DANN DIR?

KI-AGENTEN ÜBERNEHMEN DIE ROUTINEARBEIT

STANDARDISIERTE
FIRMENABFLÄUFE

BUCHHALTUNG

STANDARDABLAUF

ENTWURF

Stück für Stück geht die wiederkehrende
Denkarbeit an Agenten über.

WAS BLEIBT DEM MENSCHEN?



BÄCKER



DIE IDEE



TISCHLER



LEITET EINEN
KI-WORKSHOP

jeder kann dieselbe Idee aufgreifen.
was unterscheidet einen Bäcker, einen
Tischler, eine KI-Werkstatt von der
nächsten?

REPUTATION — WAS ZWEI UNTERSCHIEDET

HÄLT SEIN
WORT



SPRICHT MIT
DEM KUNDEN



STEHT ZU
SEINER KI



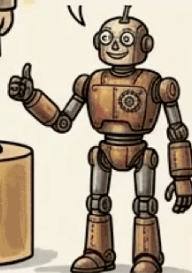
10 JAHRE,
KEINE
BESCHWERDEN



den Abschluss
macht immer noch
der Mensch.



Selbst ich kann
das nicht für dich
bauen — du mußt
es sein.



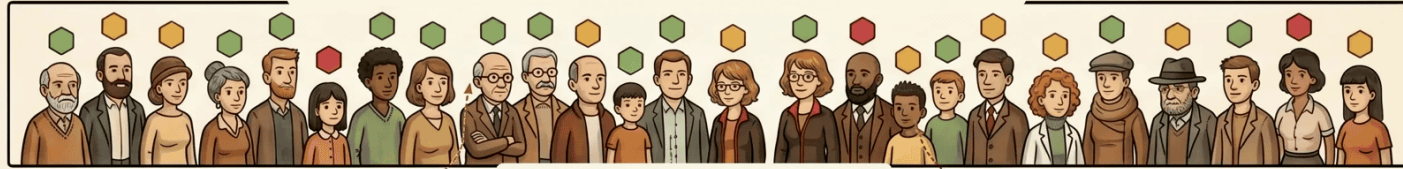
jemand muss für das Tun des Agenten
geradestehen — diese Verantwortung ist
nicht abgebar.

ohne Reputation sieht jeder Bäcker gleich aus — und die größte Marke frisst sie alle.

könnte dies der dezentrale Weg sein, der die KI an der Leine hält — der verhindert, dass einer den ganzen Markt besitzt?

KI AUTOMATISIERT DIE ARBEIT — REPUTATION HÄLT DICH MENSCHLICH.

DIE ÖKONOMIE DER WAHRHEIT



EINE GEMEINSCHAFT. VERSCHIEDENE POSITIONEN.

UNBELIEBT, ABER AKZEPTABEL



IM KONSENS



AUSSERHALB DES KONSENS



DIE
EINREICHUNG

DIE
AUSLOSUNG



DIE
RÜCKERSTATTUNG

DAS
REGISTER



DER ALGORITHMUS WÄHLT FAIR.
MENSCHEN BEPREISEN, WAS SIE
GLAUBEN.

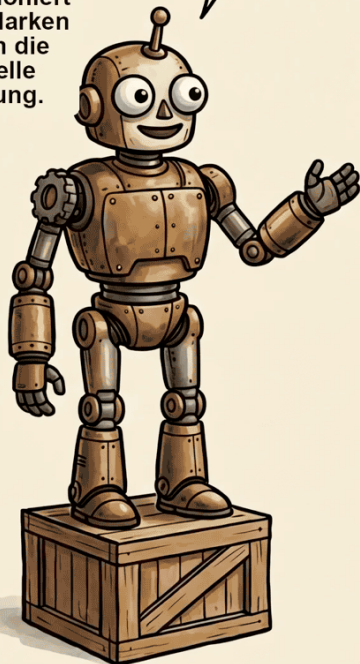


GLEICHVERTEILTE AUSLOSUNG. UNGLEICHE ANTWORT. JE WEITER VOM KONSENS, DESTO HÖHER DER PREIS.

WAS IM NETZ VERÖFFENTLICHT WIRD

fünf Dinge lassen sich
veröffentlichen —
jedes hat Versionen.

jedes Artefakt
ist versioniert
— die Marken
zeigen die
aktuelle
Fassung.



v1



DID-DOKUMENT

dein Identitätseintrag im
Netz — Schlüssel,
Metadaten, Netzadresse.

VERWALTET VON: dem
DID-Inhaber

v2



MELDUNGSSTANDARD

das Schema, dem eine
Meldung folgen muss —
was als gültiger Beleg gilt.

VERWALTET VON: einer
Autorität mit Reputation im
Bereich

v3



POLICY-STANDARD

das Schema, dem eine
Richtlinie folgen muss — die
Form der Annahmeregeln.

VERWALTET VON: einer
Autorität mit Reputation im
Bereich

abgeleitet aus

abgeleitet
aus



v4



MELDUNG

eine Aussage über ein Subjekt nach
einem Meldestandard —
veröffentlicht von einem Aussteller,
mitunterzeichnet von der Autorität
des Standards, wenn Aussteller
und Prüfer es wünschen.

VERWALTET VON: Aussteller
publiziert — Subjekt ist das Ziel

Meldungen gibt es in zwei Arten
— positiv (+) und negativ (-).

v5



DID-REGEL

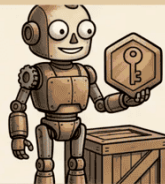
erklärte Regeln einer DID
— genutzt bei Prüfung,
Konsens und Ausstellung.

VERWALTET VON: dem
DID-Inhaber (eine Policy pro
DID)

JEDES ARTEFAKT HAT VERSIONEN. JEDE VERSION IST ÖFFENTLICH.

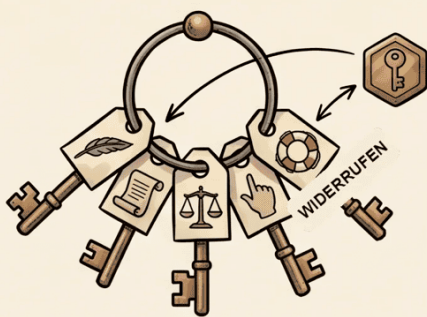
WAS STECKT IN EINEM DID-DOKUMENT?

BEISPIELE DES DID-DOKUMENT-ARTEFAKTS



dein DID-Dokument ist dein Ausweis im Netz — das steht darin.

FELDER, DIE DU DARIN FINDEST



SCHLÜSSEL UND SIGNIERREGELN

Jeder Schlüssel gibt eine Befugnis — dieses Dokument ändern, eine Meldung ausstellen, als Autorität handeln, eine Policy verwalten oder Wiederherstellung delegieren. Befugnisse lassen sich an eine andere DID geben und wieder entziehen.



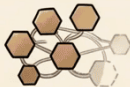
NETZADRESSEN

wo dich das Netz erreicht — änderbar, ohne deine Identität neu zu schreiben



ERSTELLT UND VERSIONIERT

wann diese Identität erschien und welche Fassung du gerade liest



VERKNÜPFT E IDENTITÄTEN

Übersicht der DIDs, mit denen du verbunden bist — nur eine Ansicht, technisch anderswo gespeichert



NACHFOLGE-MARKER

geht deine Identität verloren oder wird gestohlen, kann eine Autorität diese DID beenden und auf deinen Nachfolger verweisen

der DID-Inhaber schreibt jede neue Version — aber jede Version muss die Prüfung bestehen, bevor das Netz sie veröffentlicht.

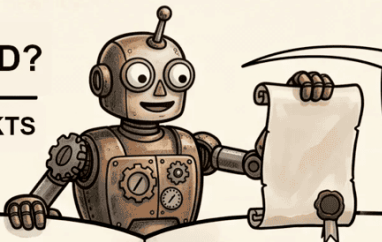
du schreibst sie — das Netz prüft sie. Du kannst dich nicht einfach ins Dasein veröffentlichen.



DU SCHREIBST DEINE IDENTITÄT — DAS NETZ BESTÄTIGT SIE.

WAS IST EIN MELDUNGSSTANDARD?

BEISPIELE DES MELDUNGSSTANDARD-ARTEFAKTS



der Standard ist das leere Formular — eine Meldung ist das ausgefüllte. Ich zeige dir beide nebeneinander.

DER STANDARD — DAS LEERE FORMULAR

	SUBJEKT-DID die DID, um die es in der Meldung geht
	AUSSTELLER-DID die DID, die die Meldung signiert
	WANN UND WO ein Datum und ein Ort
	ZUGELASSENE BELEGARTEN nur diese Arten von Belegen zählen
	ERGEBNISSKALA keine / leicht / mittel / schwer genau eine Stufe wählen — kein Freitext

EINE MELDUNG — DAS AUSGEFÜLLTE FORMULAR

	SUBJEKT-DID did:nwo:alice-9f2b...
	AUSSTELLER-DID did:nwo:magistrates-04...
	WANN UND WO 3. März, Marktplatz
	ZUGELASSENE BELEGARTEN Foto ✓ — Zeugeneid ✓ — Arztattest ✓
	ZUGELASSENE BELEGARTEN mittel — Stufe 2 von 4

jedes Feld links hat genau ein ausgefülltes Gegenstück rechts — nur so werden zwei Meldungen gleicher Art vergleichbar.

das Siegel der Autorität auf einer ausgefüllten Meldung ist ein Versprechen: das Verfahren wurde wirklich eingehalten.



Ich setze meine Reputation darauf, dass dies nach dem Standard bearbeitet wurde.

ÜBERGRIFF
v3

SCHULD
v2

MEDIZINHILFE
v4

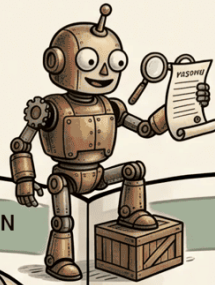
HANDWERK
v1

ZEUGNIS
v5

DER STANDARD IST DAS FORMULAR — EINE MELDUNG IST DAS AUSGEFÜLLTE UND VERBÜRGTGE FORMULAR.

WAS IST EINE DID-POLICY?

BEISPIELE DES DID-REGEL-ARTEFAKTS



meine Policy regelt nicht, wie eine Meldung geschrieben wird — das macht der Standard. Meine Policy regelt, ob mich die Meldung überhaupt kümmert: traue ich dem Unterzeichner, traue ich der Autorität hinter seinem Standard, und ist die Sache meine Aufmerksamkeit wert?

DER STANDARD — GEERBTE VOREINSTELLUNGEN

REGELNAME



MINDESTREPUTATION
DES AUSSTELLERS

Ich nehme Aussteller mit
einer Reputation über fünf
von zehn



VERTRAUENSLISTE
DER AUTORITÄTEN

Ich nehme Standards jeder
Autorität, deren eigene
Reputation über vier von zehn
liegt



INHALTSFILTER

Ich bearbeite jede Meldung,
deren Sache über der
Marke „geringfügig“ wiegt



PREISKURVE
GEGEN SPAM

Einreichen bei mir ist billig für
gehaltvolle, seltene Meldungen
— und wird schnell teuer für
kleinliche oder wiederholte



KOMBINIERTE
GEWICHTUNG

Aussteller-Rep und
Autoritäts-Rep multiplizieren
sich, Geringfügigkeit halbiert das
Ergebnis

die Policy schreibt den Standard nicht um — sie beurteilt die Leute und die Sache. Behalten, ändern, entfernen, ergänzen — vier einfache Züge auf gemeinsamer Grundlage.

MEINE POLICY — DAVON ABGELEITET

Regelname

✓ GEHALTEN tick
✎ GEÄNDERT Tätigkeitswort
✗ ENTFERNT Tätigkeitswort
✚ HINZUGEFÜGT Tätigkeitswort

MINDESTREPUTATION
DES AUSSTELLERS

verschärft — ich verlange sieben
von zehn

VERTRAUENSLISTE
DER AUTORITÄTEN

Richtern und Ärzten traue ich voll.
Meldungen unter der Stadtwache
wiege ich nur halb. Alles unter der
Hafenpolizei lehne ich ganz ab

INHALTSFILTER

geringfügige Störmeldungen kosten
mich nichts — ich lese sie einfach nicht

PREISKURVE
GEGEN SPAM

behalten — die Standardkurve reicht mir

KOMBINIERTE
GEWICHTUNG

entfernt — ich nutze meine eigene
Formel

EXPONENTIELLE
KOSTEN BEI
WIEDERHOLTEN
MELDUNGEN

ergänzt — jede weitere Meldung
desselben Ausstellers über mich
im Jahr kostet zehnmal so viel

RUHEZEITEN

ergänzt — ich lese keine Meldung,
die zwischen Mitternacht und
Morgengrauen eingeht



PRÜFUNG — meine Policy filtert eingehende
Meldungen und meine eigenen Entwürfe,
bevor ich sie ausstelle. Ausstellen ist Prüfung
auf dem Weg hinaus

KONSENS — meine Richtlinie ist meine
Stimme, wenn die Gemeinschaft
gemeinsame Regeln aushandelt.

DEINE POLICY BEURTEILT DEN BOTEN — NICHT DIE FORM.



Warum das Netzwerk unzensierbar ist

Bisher haben wir beschrieben, was das Netzwerk leisten kann. Konzentrieren wir uns nun darauf, warum es nicht abgeschaltet oder zensiert werden kann.

Das Netzwerk wird wahrscheinlich auf den Prinzipien des Tor-Netzwerks und des Onion-Routings (einer Methode, den Netzwerkverkehr nach Mixnet-Prinzipien zu verschleiern) aufbauen — einer Technologie, bei der die Kommunikation mehrere Verschlüsselungsschichten durchläuft und kein einzelner Knoten zugleich Sender und Empfänger kennt. Eine zentrale Institution kann dir nicht über die Schulter schauen, weil es keinen Ort gibt, von dem aus man schauen könnte.

Du kannst dagegen ankämpfen, aber du kannst nicht gewinnen — es sei denn, du stürzt das ganze Land in eine totalitäre Überwachung auf der Ebene einzelner Netzwerkpakete und maschinennaher Aktionen auf jedem Stück Hardware, das sich mit dem Internet verbindet und im betreffenden Reputationsnetzwerk kommuniziert. Und genau das ist die Wahl, vor der der Zentralismus steht: Entweder akzeptieren, dass die Bürger ein Werkzeug außerhalb deiner Reichweite haben, oder sich im Namen totalitärer Kontrolle in die dunklen Winkel wirtschaftlicher Stagnation eingraben.

Machen wir uns keine Illusionen — auch demokratische Regime werden das in ihrem Kampf um den Zentralismus versuchen. Sie würden Menschen lieber in Ketten legen, als die Macht abzugeben.

WIE DEINE NACHRICHTEN UNVERFOLGBAR BLEIBEN

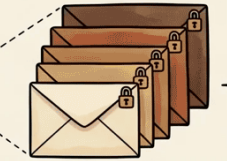
ZWEI VERTEIDIGUNGSLINIEN ZUGLEICH — SCHICHTEN UND RAUSCHEN

INHALT: IN SCHICHTEN GEHÜLLT

(die Technik hinter Tor — „Onion-Routing“)



SENDER

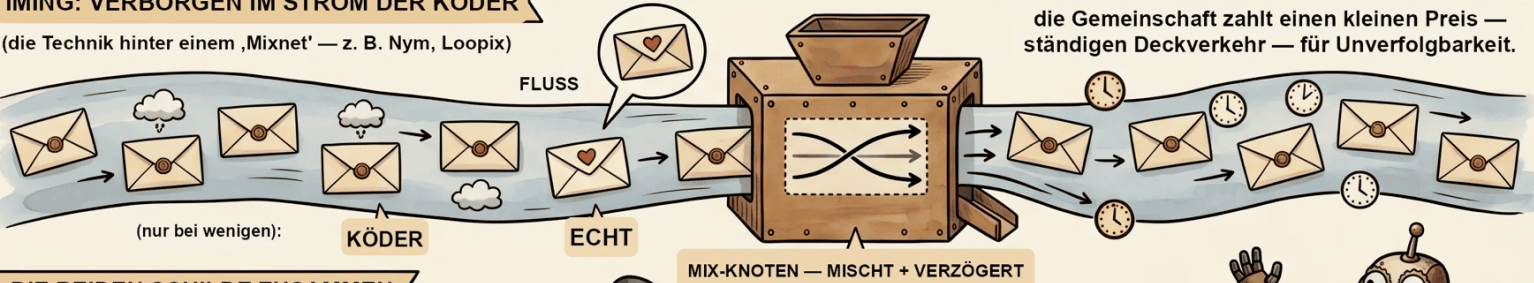


vier Schlösser, vier
Schlüssel — eines je
Knoten.



TIMING: VERBORGEN IM STROM DER KÖDER

(die Technik hinter einem „Mixnet“ — z. B. Nym, Loopix)



DIE BEIDEN SCHILDE ZUSAMMEN

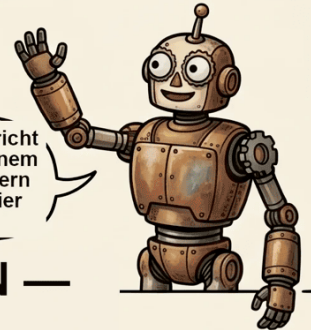
MATRIX	VERBORGT WER → WER?	VERBORGT WANN?
NUR SCHICHTEN	✓ JA	✗ NEIN
NUR RAUSCHEN	✗ NEIN	✓ JA
SCHICHTEN + RAUSCHEN	✓ JA	✓ JA

(Onion-Routing + Mixnet — die perfekte Kombination)



hundert Umschläge
pro Stunde —
welcher zählt?

der Beobachter sieht den Fluss,
kann aber ECHT nicht von
KÖDER unterscheiden



die echte Nachricht
schwimmt in einem
Fluss von Ködern
— und trägt vier
Mäntel.

INHALT DURCH SCHICHTEN VERBORGEN — TIMING DURCH RAUSCHEN.

Naheliegende Zweifel ausräumen

Das beschriebene System wirft naturgemäß eine Reihe von Fragen auf. Gehen wir die häufigsten durch.

Abhängigkeit von der Technologie

Dir ist wahrscheinlich schon aufgefallen, dass die hier beschriebene Reputationsnetzwerk-Lösung — anders als der moderne Staat, der uns seit rund 150 Jahren begleitet — stark von der Technologie des globalen/lokalen Internets abhängt. Im Falle eines Ausfalls ist das Funktionieren eines solchen Netzwerks gefährdet.

Ist der Ausfall vorübergehend, gibt es keinen Verlust von Daten oder der Konsistenz der Behauptungen im Netzwerk, und auch die innerhalb der Gemeinschaften erzielten Reputationsbilanzen sollten nicht gestört werden. Anders als vergleichbare Zahlungsnetzwerke geht dieses Netzwerk von sehr niedrigen Häufigkeiten von Prozessen und Datenposten aus. In dieser Hinsicht unterscheidet sich das dezentrale Reputationsnetzwerk nicht vom heutigen Staat, der inzwischen ebenfalls stark von Technologie abhängt und verlernt hat, mit Papierkarteien zu arbeiten (auch wenn er in Krisenplänen keine andere Wahl hätte).

Der evolutionäre Nachfolger des Staates in Form eines Reputationsnetzwerks kann im Falle eines dauerhaften Ausfalls (einer Katastrophe beispiellosen Ausmaßes) auf ein primitiveres zentralisiertes System zurückfallen — den Staat.

Die Technologie erlaubt es der Menschheit, höhere zivilisatorische Formen der Steuerung zu erreichen, und bringt uns Vorteile, aber auch Risiken.

ZWEI WEGE — DER STAAT SCHLIESST, DAS NETZ ÖFFNET

DAS REPUTATIONSNETZ

DER STAAT

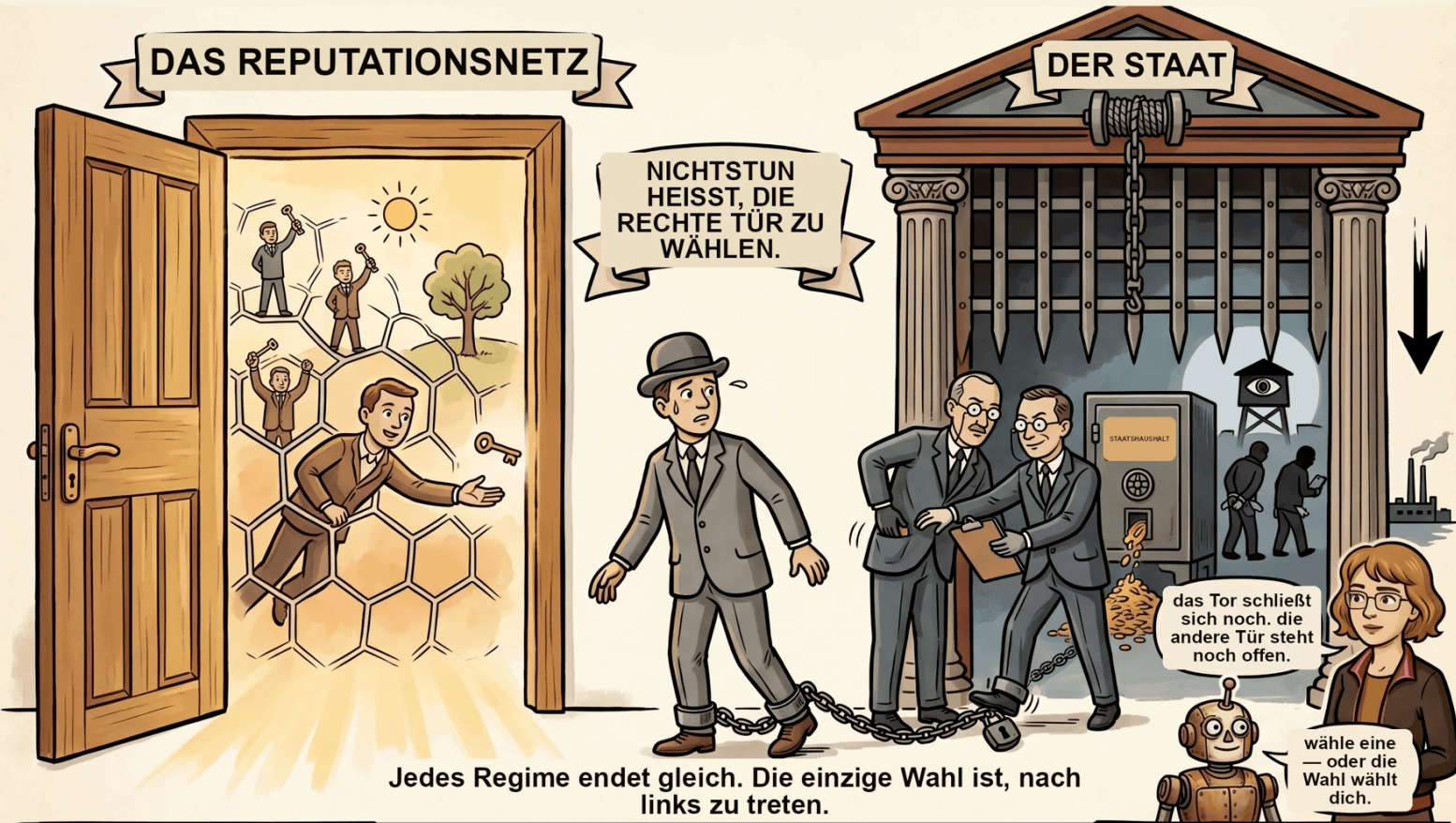
NICHTSTUN
HEISST, DIE
RECHTE TÜR ZU
WÄHLEN.

Jedes Regime endet gleich. Die einzige Wahl ist, nach
links zu treten.

das Tor schließt
sich noch, die
andere Tür steht
noch offen.

wähle eine
— oder die
Wahl wählt
dich.

DER STAAT SCHLIESST STANDARDMÄSSIG. DAS NETZ ÖFFNET AUS WAHL.



Werfe ich Geld zum Fenster hinaus, wenn ich im Netzwerk veröffentliche?

Die Kosten der Veröffentlichung einer Behauptung im Reputationsnetzwerk sind größtenteils nicht versunken. Der Nutzen einer ins Netzwerk gestellten Botschaft eines Veröfentlichters — Informationen über echte Missstände, überprüfte Erfahrungen, relevante Warnungen — kehrt über einen längeren Zeithorizont statistisch in Form von Gebühren für die Verifizierung der Behauptungen anderer aus der Gemeinschaft zurück. Die Gemeinschaft profitiert, der Veröfentlichter baut Reputation auf, und die Kosten der Veröffentlichung wahrheitsgemäßer Informationen nähern sich damit einer erstattbaren Kautiön, von der nur ein kleinerer Anteil der tatsächlichen Netzwerkbetriebskosten abzuziehen ist. Umgekehrt kehren unwahre oder belanglose Einträge nicht zurück — ihre Kosten sind ein Nettoverlust. Ehrlichkeit ist daher nicht nur eine moralische Wahl, sondern auch eine ökonomisch rationale Strategie.

Nach Abzug der Netzwerkbetriebskosten könnte man dieses Prinzip als Prinzip der ökonomischen Neutralität bezeichnen — ich verliere nicht, wenn ich mit der Gemeinschaft bin, ich verliere, wenn ich gegen sie bin.

Die Gemeinschaft verfügt auch über Solidaritätskanäle, um den ehrlichen Ansatz ihrer Mitglieder zu würdigen. Doch machen wir uns keine Illusionen: Appelle an die Solidarität entstehen meist aus dem sozialen Druck der Gemeinschaft, sodass dies womöglich keine Solidarität im freiwilligen Sinne des Wortes ist.

Was, wenn jemand mehrere Identitäten erstellt?

Eine Person kann mehrere DID-Identitäten parallel betreiben. Der Aufbau von Reputation für jede Identität erfordert jedoch eigenständigen Aufwand — Zeit, Energie, Geld.

Keine Abkürzungen: Jede Identität muss ihre Erfolgsbilanz¹ durch tatsächliche Aktivität aufbauen. Das Unterhalten paralleler Identitäten ist daher absichtlich teuer.

In freien Gesellschaften schrecken die Kosten vom Missbrauch ab.

In Diktaturen werden parallele Identitäten hingegen zu einem Überlebenswerkzeug: Sie ermöglichen das Organisieren von Untergrundnetzwerken, ein sichereres Navigieren auf dem Schwarzmarkt und einen abgeschotteten² Widerstand, bei dem die Kompromittierung einer Identität die anderen nicht preisgibt — und nach dem Sturz des Regimes erlauben sie eine nahtlose Rückkehr ins öffentliche Leben und zur dort aufgebauten Reputation und sogar das Verschmelzen der zuvor offiziellen und der geheimen DID zu einem einzigen kombinierten Satz von Einträgen mittels einer Behauptung.

¹**Track record (Erfolgsbilanz)** — allgemein: eine Historie vergangener Ergebnisse, Erfolge und Misserfolge einer Person oder Organisation. Hier: die Summe aller vergangenen Interaktionen einer gegebenen DID-Identität im Netzwerk — verifizierte Behauptungen, angenommene und abgelehnte Einträge —, aus der sich ihre Reputation ableitet.

²**Abschottung (Compartmentalization, von engl. *compartment*)** bedeutet, Informationen in isolierte Einheiten zu trennen, sodass die Preisgabe einer Einheit die anderen nicht kompromittiert. Ein aus Geheimdiensten bekanntes Prinzip: Ein Agent kennt nur seinen Teil der Operation, sodass er selbst unter Zwang nicht das Ganze verraten kann.

DIESELBE MÜHE — IN FREIHEIT EIN ÜBERFLÜSSIGER PLAN B, UNTER TYRANNEI EIN RETTUNGSSEIL
PARALLELE IDENTITÄTEN KOSTEN GLEICH — KAUFEN ABER ANDERES

IN FREIHEIT — EIN TEURER PLAN B

 eine zweite Identität — für den Fall der Fälle.

SAMEN → KEIM → SETZLING → JUNGBAUM → REIFER BAUM
5 bis 15 Jahre — keine Abkürzung, kein reifer Baum zu kaufen



Jahr 1 — Zeit, Energie, Geld verbraucht — 5% Reputation
Jahr 3 — dieselben Kosten erneut, unabhängig bezahlt — 20% Reputation
Jahr 0 — alles beginnt von vorn — 0% Reputation
drei Gärten, dreifache Kosten — und du hast immer noch nur zwei Hände.

ODER — EIN NEUANFANG NACH EINEM PERSÖNLICHEN FEHLTRITT

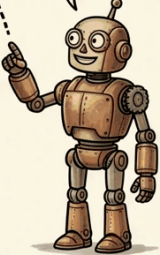


ALTE DID — REPUTATION VERBRANNT
funktioniert nur, wenn der Schaden dein eigener blieb — wurden andere so verletzt, dass sie dich verfolgen, folgen dir ihre Meldungen auch in den neuen Topf.

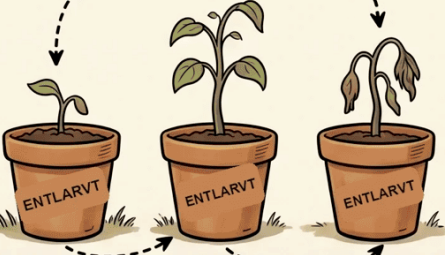
DID-NEUANFANG

EINE MELDUNG — UND PLAN B IST WEG

 DER ECHTE MENSCH
ein Faden — (und der ganze Plan löst sich auf).



DIE MELDUNG



eine einzige Meldung bindet jeden Topf an denselben Gärtner — Jahre an Zeit, Energie und Geld an einem Nachmittag gelöscht.

UNTER TYRANNEI — EINE FÜR DEN STAAT, ANDERE FÜR FREIE VERBINDUNG
(der Staat verbietet Identitäten oder verlangt sie unter eigener Kontrolle)

 DIE, DIE DER STAAT SIEHT
eine Maske für das Regime — der Rest für ein noch lebenswertes Leben.



äußere Fügsamkeit — eine Identität zur Überwachung abgegeben.

AUCH MEINS — ABER VOR DEM STAAT VERBORGEN



DIE, DIE DER STAAT NIE SEHEN DARF



DID-A — UNTERGRUNDPRESSE
DID-B — AUSGEHOBEN
DID-C — WIDERSTANDSZELLE — INTAKT

die Mauern zwischen den Zellen tun, was der Staat verbietet — fällt eine, machen die anderen weiter, fällt das Regime, lebt das öffentliche Leben wieder auf.

IN FREIHEIT IST MISSBRAUCH TEUER. UNTER TYRANNEI IST ÜBERLEBEN MÖGLICH.

■ Die Wahrnehmung umgestülpt

Anders als der Staat kehrt das Prinzip eines auf dezentraler Identität aufbauenden Reputationssnetzwerks das Paradigma der wahrgenommenen Priorität um:

- Worauf es ankommt, ist die Reputation — also die Vergangenheit, genutzt zur Einschätzung der Risiken einer Interaktion mit der Gegenseite — und persönliche Daten wie Namen, Adressen usw. können Sache eines höflichkeitshalber erfolgenden Datenaustauschs sein
- Während der Staat vorrangig persönliche Daten verlangt, Reputationsdaten anhäuft und die Gemeinschaft nur sehen lässt, was ihm passt

Kann ein wohlhabender Mensch nicht einfach mehr Identitäten „kaufen“ (oder virtuelle Gemeinschaften erschaffen)?

Die Möglichkeit, parallele dezentrale Identitäten zu erstellen, sieht auf den ersten Blick wie ein unfairer Vorteil für Menschen mit größeren wirtschaftlichen Mitteln gegenüber jenen mit geringeren aus. Es muss jedoch betont werden, dass man in einem dezentralen System — anders als in einem zentralisierten, wo es genügt, wenige Punkte in der Machtpyramide zu korrumpieren, damit bestimmte Missetaten verschwinden — die gesamte Gemeinschaft korrumpieren müsste.

Ersatz-Identitäten könnten diesem Zweck dienen, doch ihre Reputation muss mit der Zeit durch reale Interaktion mit tatsächlichen anderen Gemeinschaftsmitgliedern aufgebaut werden — sie lässt sich nicht einfach kaufen, denn das Netzwerk macht überprüfbar, wie sich eine gegebene Identität schlägt.

Zudem können auf dem Markt Dienste existieren (und werden es wahrscheinlich), die als Autorität handelnd Ermittlungen anbieten, die den Beweis erbringen, dass mehrere dezentrale Identitäten in Wahrheit dieselbe Person sind. Ein einziger ins Reputationsnetzwerk eingestellter Eintrag kann so für einen Bruchteil der Kosten die gesamte Investition an Zeit, Energie und Geld zunichtemachen, die in den Aufbau paralleler Identitäten geflossen ist.

Ökonomisch zahlt es sich daher aus, die Gemeinschaft nicht zu betrügen — und bei Bedarf sein Handeln zu prüfen und Wiedergutmachung zu betreiben, damit die Reputation auf ein akzeptables Niveau zurückkehrt und ihr Träger unter dem Zorn der Gemeinschaft nicht wirtschaftlich oder anderweitig leidet.

Eine wirtschaftlich mächtige Identität, die in ihrer eigenen Gemeinschaft Reputation verloren hat, mag versuchen, dem Zorn der Gemeinschaft durch hinterhältige Absprachen mit gezielten Identitäten zu entkommen — doch diese riskieren dann ebenfalls, ihre eigene Reputation zu verlieren.

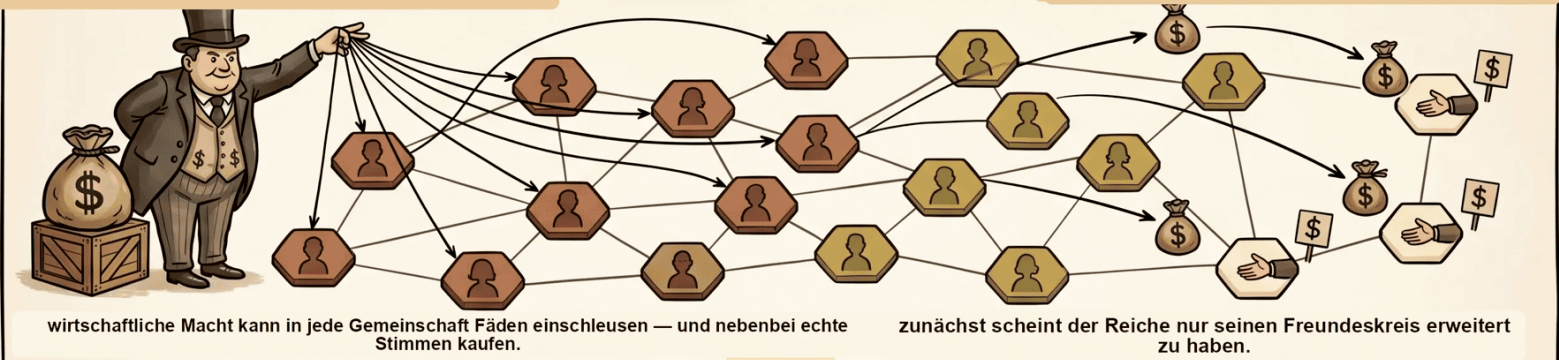
Es bleibt weiterhin die Flucht in eine andere Gemeinschaft mit einer frischen Identität — doch das bedeutet, alle Errungenschaften zurückzulassen und irgendwo bei null mit null Reputation anzufangen. Manchmal mag es ein nachvollziehbarer Weg und der einzige Ausweg sein.

REPUTATION IST DAS GEGENGEGWICHT ZUR WIRTSCHAFTSMACHT

DER REICHE KAUFT EINFLUSS — DIE GEMEINSCHAFT ERINNERT SICH

DER ANGRIFF — UNTERWANDERN UND KAUFEN

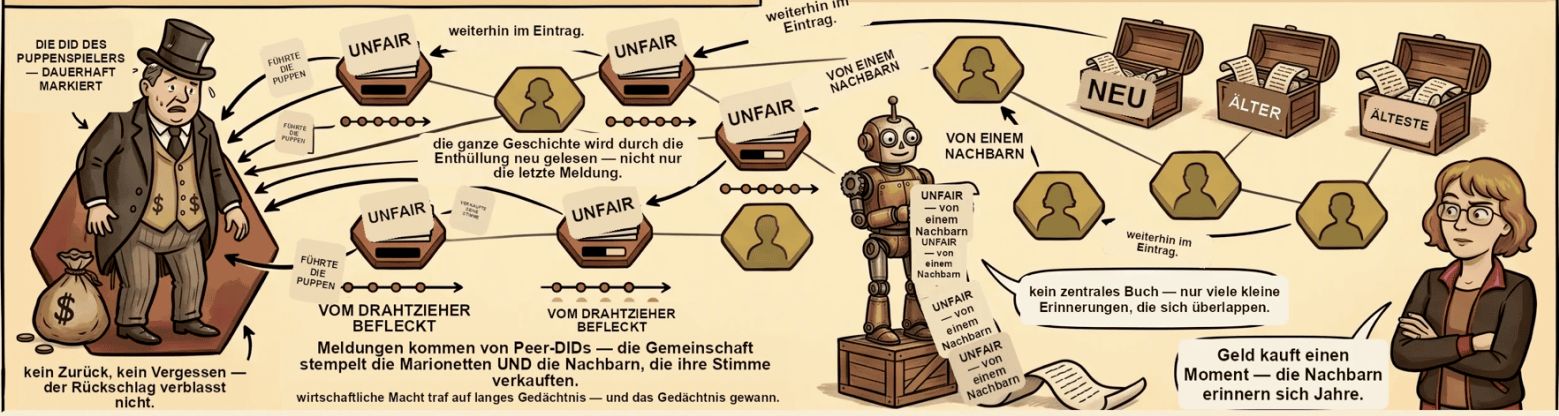
ACHT MARIONETTEN GESETZT + DREI NACHBARN GEKAUFT



SPÄTER

DIE ABWEHR — LANGES GEDÄCHTNIS, VERTEILTE BUCHFÜHRUNG

JEDER NACHBAR HÄLT SEIN EIGENES GEDÄCHTNIS — KEIN ZENTRALBUCH, KEIN VERGESSEN



WIRTSCHAFTSMACHT GREIFT EIN — DER RÜCKSCHLAG TRIFFT SIE, UND ER GEHT NICHT AB.

Anmerkung

Ähnlich würden Gemeinschaften mit einem Angriff umgehen, bei dem jemand Ressourcen darauf verwendet, eine virtuelle Identität zu erschaffen: Für diese Identität ist es riskant, ohne Verifizierung in eine Interaktion mit einer anderen Gemeinschaft einzutreten — das heißt, Informationen über die Identitäten der anderen Gemeinschaft unkritisch zu übernehmen. Reputationen werden stets innerhalb einer Gemeinschaft aufgebaut, nicht global.

Was ist mit Trittbrettfahrern, die nur lesen und der Gemeinschaft nichts geben wollen?

Der Zugang zu Informationen ist ab dem ersten Tag der Erstellung einer dezentralen Identität nicht unbegrenzt. Neue Teilnehmer — jene, die noch keine Reputation durch tatsächliche Aktivität aufgebaut haben — stoßen auf gestufte Beschränkungen: weniger Informationen, längere Wartezeiten, höhere Abfragekosten. Das Netzwerk belohnt Beteiligung, nicht passiven Konsum und willkürliches Abernten von Daten.

Eine dezentrale Identität riskiert ihre Reputation auch, wenn sie ihre Reputation gegen Bezahlung an eine andere Person verleiht (die womöglich nicht einmal im DID-Reputationsnetzwerk ist). Hier gilt dasselbe Prinzip: Ein solcher Verrat an der Gemeinschaft (Verletzung der Privatsphäre) kann auf die Reputation des Verräters zurückfallen, und die Tat lässt sich nicht durch eine hinterhältige Absprache tilgen, wie es in einem zentralisierten System funktioniert. Er muss mit dem Zorn der Gemeinschaft rechnen, einschließlich des Verlusts von Errungenschaften — denn die Gemeinschaft ist in seinen Augen der Garant etwa für das Privileg, bewegliches und unbewegliches Eigentum zu besitzen.

Anker in der realen Welt

Bei der Risikobewertung ist das riskantere Subjekt naturgemäß jenes, das nicht das von einer gegebenen Gemeinschaft anerkannte Privileg des Eigentums genießt — es hat bei seinen Geschäften weniger zu verlieren (digitale Vermögenswerte lassen sich leichter bewegen).

Es mag wie ein unbedeutendes Detail aussehen, hat aber große Folgen. Zu wollen, dass die Gemeinschaft ein Druckmittel gegenüber ihren Mitgliedern hat, impliziert Eigentum als Privileg — in den freiesten Gesellschaften nahezu unantastbar, und dennoch kein Recht, auch kein grundlegendes Prinzip, sondern ein Privileg, das in Extremfällen entzogen werden kann (ich kann mir zum Beispiel die Verweigerung des Dienstes zur Verteidigung der Gemeinschaft im bewaffneten Konflikt vorstellen).

Es beantwortet auch unterschwellig, wie die Gemeinschaft ihre Mitglieder behandeln wird und welche Motivation ein Mitglied hat, für die Gemeinschaft zu kämpfen — um seine Privilegien zu behalten. Ein Mensch mag in seiner Verantwortung gegenüber der Gemeinschaft versagen, kann aber moralisch keine Nachsicht erwarten, wenn es um das Behalten schwer erkämpfter Privilegien geht.

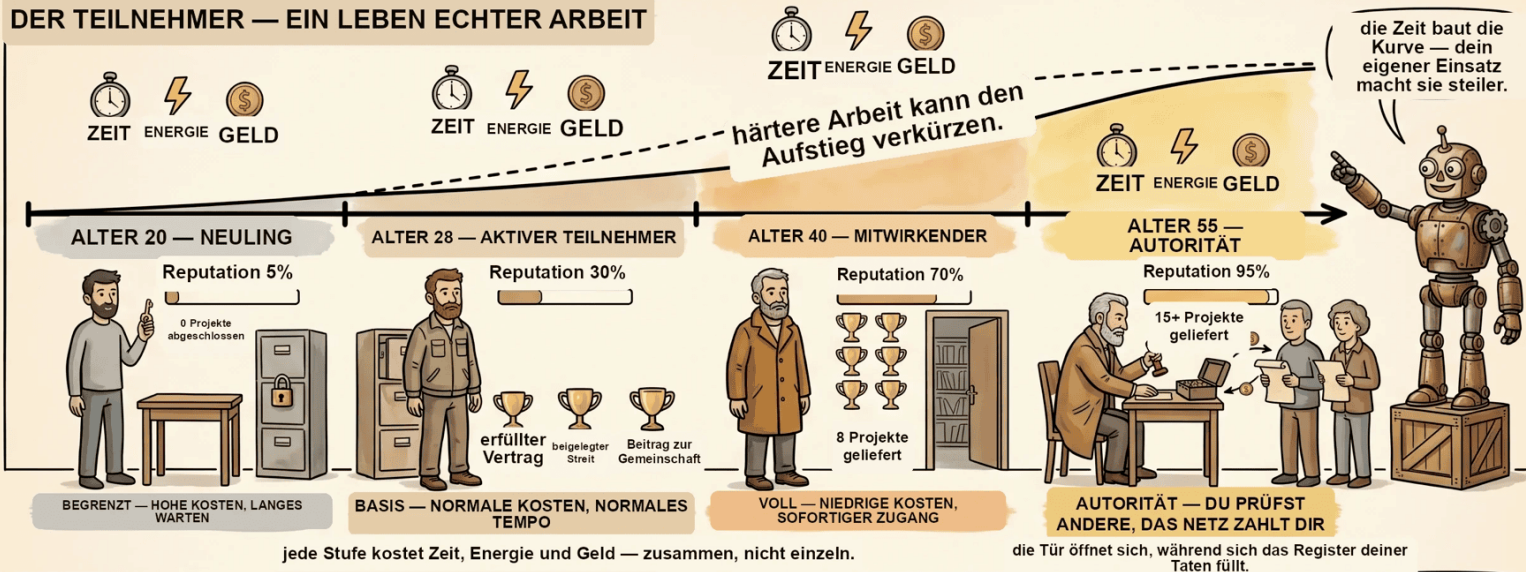
Finanzielle Neutralität

Beim Lesen von Wörtern wie dezentral, unzensurierbar, unbestechlich kommt man nicht umhin, sie mit den bekanntesten Kryptowährungen zu assoziieren — Bitcoin, Monero und etwa Kaspas —, die sich mit solchen Begriffen beschreiben lassen. Die Intuition führt hier jedoch in die Irre: Gebühren für die Dienste

DAS NETZ BELOHNT TEILNAHME

REPUTATION WÄCHST EIN LEBEN LANG — NICHT GEKAUFT, NICHT GELIEHEN

DER TEILNEHMER — EIN LEBEN ECHTER ARBEIT



DER TRITTBRETTFAHRER — LIEST, VERÖFFENTLICHT NIE

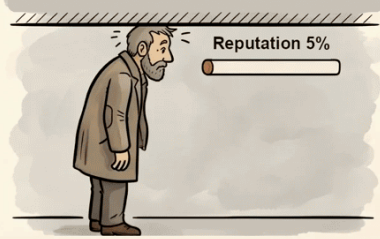


liest die Einträge aller anderen.



veröffentlicht nichts Eigenes.

BEGRENZTER ZUGANG — DIE DECKE HEBT SICH NICHT



keine Taten, kein Aufstieg — Jahr für Jahr dieselbe Latte.

das Netz gibt denen zurück, die geben.



ZEIT, ENERGIE UND GELD — IN ECHTE ARBEIT GESTECKT — SIND DIE EINZIGE WÄHRUNG, DIE DAS NETZ ACHTET.

von Autoritäten, für Verifizierung und Veröffentlichung usw. können in jeder Währung oder jedem Geld beglichen werden. Was für die verbundenen Teilnehmer des sozialen Netzwerks im DID-Netzwerk (also deine Gemeinschaft) und ihr Umfeld zählt, ist eine reputationsgedeckte Bestätigung, dass die Zahlung geleistet wurde. Die Veröffentlichung einer Behauptung muss einzeln angemessene, überprüfbare Kosten tragen, damit ein Akteur nicht beliebig viele und beliebige Behauptungen veröffentlichen kann, ohne Energie, Geld und Zeit aufzuwenden — ein höchst unerwünschter Zustand, der dem Privileg der Eliten in den heutigen korruptionsgeplagten staatlichen Systemen entspricht.

In dieser Hinsicht haben die genannten Kryptowährungen einen kleinen Vorteil darin, dass ihre Netzwerke als vertrauenswürdige Autoritäten für die Verifizierung fungieren, dass eine gegebene Zahlung stattgefunden hat, um den Preis eines kleinen Verlusts an Privatsphäre und der Preisgabe einiger seiner Adressen.

Freiwilligkeit, Verantwortung und Freiheit

Freiwilligkeit ist individuell: Ich entscheide für mich selbst. Verantwortung entsteht, wenn meine Entscheidung andere betrifft — das Feedback setzt ein. Freiheit ist weder ein Geschenk noch ein Recht — sie ist ein phänomenologisches³ Ergebnis von Tausenden bilateraler Interaktionen zwischen Freiwilligkeit und dem Druck hin zur Verantwortung, gemittelt über die Gesellschaft. Das Netzwerk diktiert diesen

³**Phänomenologisch** (von gr. *phainómenon* — das, was erscheint) — allgemein: ein Ansatz, der Phänomene so untersucht, wie sie sich in der unmittelbaren Erfahrung darbieten, indem beobachtet wird, was aus ihnen folgt, ohne vorgegebene Erklärungstheorien in der Mikrowelt darunter. Hier: Freiheit ist kein von oben definiertes abstraktes Prinzip, sondern ein beobachtetes Phänomen — eine Folge Tausender Mikrointeraktionen zwischen Menschen, die daraus entsteht, wie wir tatsächlich miteinander umgehen.

Durchschnitt nicht — er entsteht emergent⁴ aus den Preissignalen der Verifizierer und aus den im Voraus angekündigten Verifizierungsrichtlinien, die sich die Gemeinschaftsmitglieder selbst setzen.

Welche Präferenz für Freiheit ein Individuum innerhalb einer Gemeinschaft hat, hängt von seinem Gespür dafür ab, wie viel es selbst von dem zu schlucken bereit ist, was es anderen auferlegt. Bei Dingen, die selbstverständlich und für alle vorteilhaft sind, gibt es kein moralisches Dilemma — Mord ist falsch. Dann gibt es Fälle, in denen Optionen in die Position erlaubter Privilegien rücken: Weise deine Fähigkeiten nach, und wir lassen dich auf die Straße, sodass die Chance geringer ist, dass du uns tötest. Und schließlich gibt es Angelegenheiten, bei denen der Einzelne sagt — es ist es mir nicht wert, ich verbiete meinem Nachbarn nicht das Verbrennen von Laub, wenn ich es selbst tue, oder weil ich etwas anderes tue, das seinen Komfort einschränkt, und er es mir seinerseits verbieten könnte. Wenn wir historisch die Grenze der Freiheit dort gezogen haben, wo die Freiheit eines anderen beginnt, dann erfüllt ein auf dezentraler Identität aufbauendes soziales Reputationsnetzwerk dies besser als die zentralisierte repräsentative Demokratie — in der sich etwa die privilegierte Schicht der gewählten Vertreter von der Überwachung persönlicher Kommunikation auszunehmen versucht und dennoch nicht zögert, sie ihren Wählern aufzuerlegen, unter Verwendung allerlei hinterhältiger Vorwände und Manipulationen.

Der Schalter zwischen Freiheit und Totalitarismus (und Delegation)

Ein einfacher Mechanismus innerhalb des DID-Netzwerks kann das gesamte System hin zu mehr Freiheit oder mehr Kontrolle verschieben: die Anzahl der Einträge, die eine DID pro Zeitraum veröffentlichen

⁴**Emergent** (von lat. *emergere* — auftauchen) bedeutet „spontan aus den Interaktionen einfacherer Teile entstehend, ohne dass es jemand entworfen oder gelenkt hätte“. Ein Vogelschwarm fliegt in Formation, obwohl kein Vogel einen Plan für die Formation hat — die Formation entsteht aus den einfachen Regeln jedes Einzelnen. Ebenso entwirft im Reputationsnetzwerk niemand die Verhaltensregeln des Ganzen — sie entstehen aus Tausenden individueller Entscheidungen.

FREIWILLIGKEIT → VERANTWORTUNG → FREIHEIT

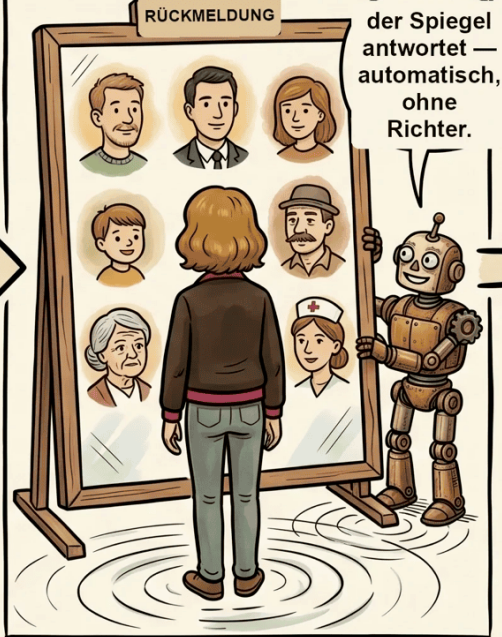
DREI SCHRITTE — VON DER WAHL EINES MENSCHEN ZUM MUSTER EINER GANZEN GESELLSCHAFT

FREIWILLIGKEIT



der Einzelne entscheidet — niemand zwingt ihn.
und niemand schuldet ihr eine positive Pflicht.

VERANTWORTUNG



meine Entscheidungen ziehen Kreise — und die Kreise kehren zurück
die Folgen sprechen für sich.

FREIHEIT



niemand zeichnete diese Karte — sie zeichnete sich selbst.

Freiheit ist die statistische Gestalt dessen,
wie Nachbarn einander behandeln.

FREIHEIT IST KEIN GESCHENK VON OBEN — SIE IST DAS MUSTER, DAS WIR GEMEINSAM WEBEN.

darf. Wenn Einträge knapp bleiben, hat jeder Gewicht — das ist Freiheit. Wenn Einträge im Überfluss vorhanden sind und Belanglosigkeiten abdecken, ist das Totalitarismus. Mit jedem Eintrag, den du veröffentlichst, wählst du die Richtung. Das Netzwerk selbst ist weder frei noch totalitär — es ist neutrale Infrastruktur. Was daraus wird, entscheidet sich daran, wie die Menschen es nutzen.

Innerhalb meiner eigenen Verifizierungsrichtlinie ist es sinnvoll, für eine generische DID in meinem sozialen Netzwerk — innerhalb der Gemeinschaften — eine Höchstzahl an Behauptungen festzulegen (jede überprüfbare Aussage allgemein; hier: ein ins Reputationsnetzwerk veröffentlichter Eintrag), die ein Veröffentlichter pro Zeitraum ausstellen darf, damit ich sie berücksichtige und seine Verifizierungsanfragen als relevant betrachte.

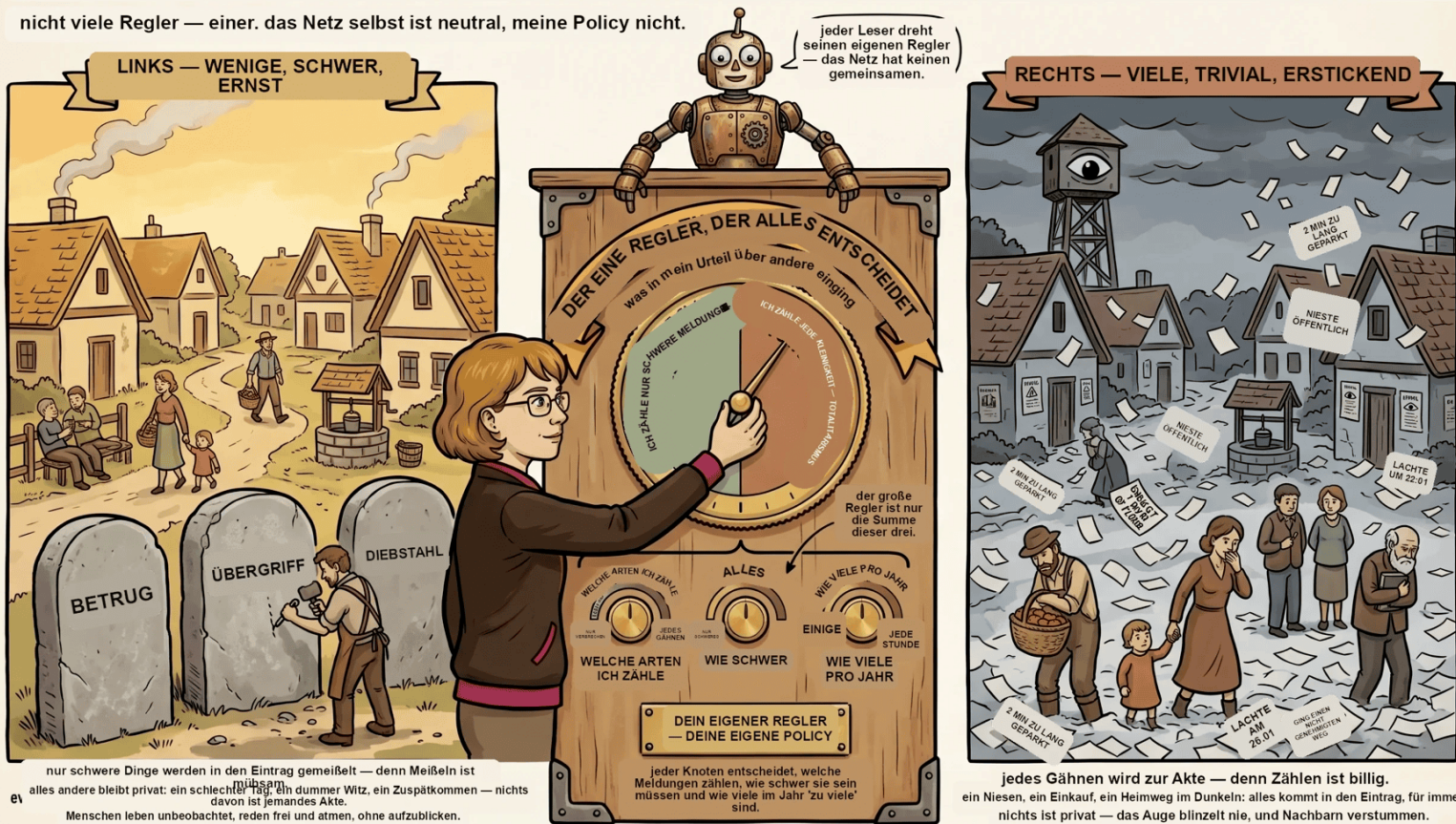
Ich habe eine intuitive Zahl im Kopf — niedrige einstellige Werte pro Jahr. Ein solch zensorischer Ansatz mag recht isolationistisch erscheinen. Aber ich kann den Antragsteller legitim vor eine Wahl stellen: einen seiner bereits ausgestellten Einträge auszuwählen und den Verifizierer zu bitten, ihn zu widerrufen, das heißt für ungültig zu erklären — was eine ziemlich aggressive Forderung ist in einer Situation, in der der Antragsteller durch Zufall tatsächlich Opfer mehrerer voneinander unabhängiger Unrechtstaten geworden ist, und ich würde damit gewiss zu seinem Gefühl der Entfremdung von der Gemeinschaft beitragen.

Als wirksamere Option erscheint daher die Möglichkeit, einen Teil seiner Rechte zur Veröffentlichung von Informationen ins Reputationsnetzwerk zugunsten einer Gemeinschaft oder einer Autorität zu delegieren, die dann — in solidarischer Weise, nach ihren internen Regeln — entscheidet, wie sie sie zuteilt. Eine Gruppe muss sich um jene kümmern können, die sie für benachteiligt hält. Ein Gemeinschaftsmitglied hat jederzeit, bis das delegierte Recht genutzt wird, das Recht, seine Delegation zu widerrufen.

DER SCHALTER FREIHEIT–TOTALITARISMUS

EIN EINZIGER PARAMETER — WIE VIEL ICH VERFOLGE — KIPPT EINE GANZE GESELLSCHAFT ZWISCHEN FREIHEIT UND TYRANNEI

nicht viele Regler — einer. das Netz selbst ist neutral, meine Policy nicht.



FREIHEIT IST, WAS ICH NICHT ZÄHLE — TOTALITARISMUS IST, WAS ICH ZU VERFOLGEN ZULASSE.

DELEGATION DER VERÖFFENTLICHUNGSRECHTE

DU LEIHST DEN SCHLÜSSEL EINER AUTORITÄT, DIE DIR DIENST — UND HOLST IHN SOFORT ZURÜCK

Ich leihe den Schlüssel — die Schnur bleibt bei mir.

Delegation — die Autorität handelt für mich, nach Regeln, die ich billige.

FADEN DER ERINNERUNG

MEIN PUBLIKATIONSRECHT — EINTRAG

Ich kann mehrere Schlüssel zugleich verleihen — eine Automatik im Hintergrund gibt einen neuen aus, sobald einer von mir gelöst wird.

AUSGEGEBEN

EIN SCHLÜSSEL ZUFÄLLIG GEZOGEN — DER SCHLÜSSEL IST VERBRAUCHT

widerrufbar nur, bis der Schlüssel gezogen wird.

danach muss der Bürger einen neuen Schlüssel ausstellen, um bei der Autorität zu bestehen — eine Automatik erledigt das im Hintergrund.

AUTORITÄT — DIENSTANBIETER
Policy · Standard · Partei · Kammer

POLICY

ZUFÄLLIG GELOST, WENN DIE AUTORITÄT HANDELT

DELEGIERTE SCHLÜSSEL — POOL

ZUFÄLLIG GELOST, WENN AUCH DIE AUTORITÄT HANDELT

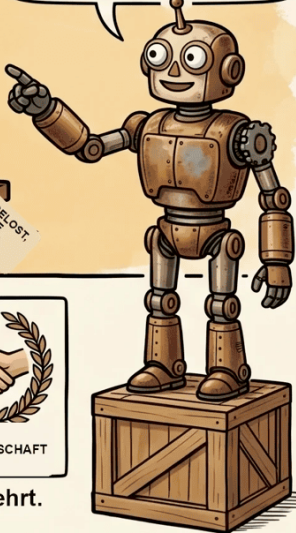
EIN RUCK — DER SCHLÜSSEL KOMMT HEIM

die Schnur verlässt nie deine Hand — das ist der ganze Trick.

ARTEN VON AUTORITÄTEN, DIE DEN SCHLÜSSEL HALTEN KÖNNEN

 POLITISCHE PARTEI PAKIT	 NORMUNGSGREMIUM BUUT	 BERUFSKAMMER	 GENOSSENSCHAFT
---	--	---	---

die Autorität dient ihren Mitgliedern — nicht umgekehrt.
ein Zug an der Schnur beendet das Arrangement.



LEIH DEN SCHLÜSSEL — HALT DIE SCHNUR. DELEGATION IST NIE AUFGABE.

■ Freiheit vs. Totalitarismus

Eine Gesellschaft, die über das Volumen veröffentlichter Einträge wacht und es begrenzt, wird freier sein; eine Gesellschaft mit einem Übermaß an Einträgen wird zum Totalitarismus neigen. Man kann sich vorstellen, das Recht zur Veröffentlichung von Einträgen an jemand anderen zu delegieren.

Kulturelle Anpassung

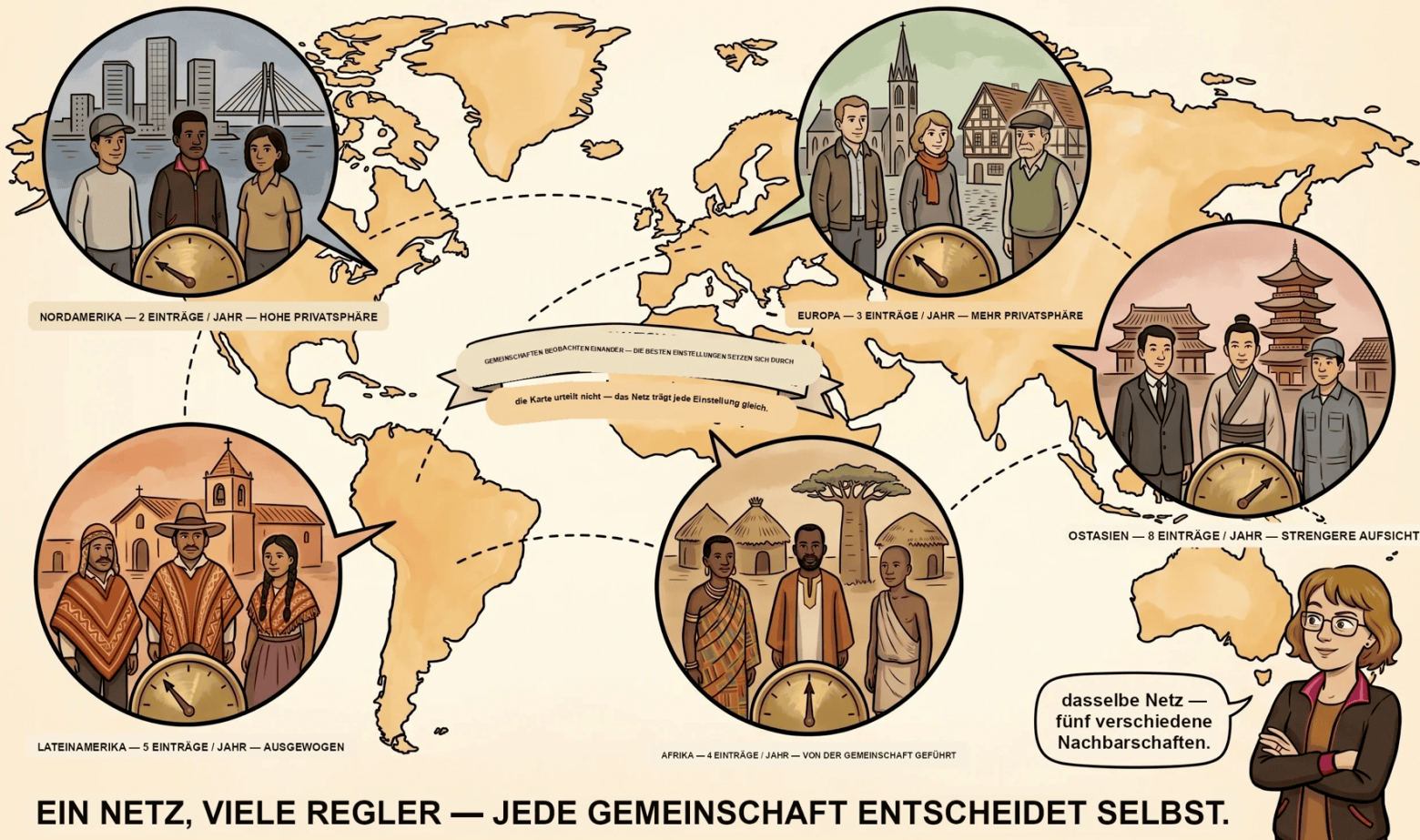
Menschen sehen einander im Allgemeinen gern auf den Teller. Über die Zivilisationen hinweg unterscheiden wir uns in historischer Erfahrung und Bevölkerungsdichte — und daher darin, wie sehr wir einander innerhalb von Zivilisationen und Gemeinschaften auf den Teller sehen wollen. Asiatische Staaten neigen zu einer strengerer Sicht auf die Freiheit in der Gesellschaft; europäische und amerikanische in gewissen Aspekten zu einer freieren. So ungenau diese Parallele auch sein mag, im Kontext eines dezentralen sozialen Reputationsnetzwerks lässt sich sagen, dass die Einstellungen der einzelnen Gemeinschaften nicht diskriminieren und jede Gemeinschaft die Kommunikation innerhalb ihrer selbst nach eigenem Ermessen konfigurieren kann.

Trotz der Unterschiede wird es Standards geben, die über den ganzen Planeten hinweg anerkannt sind (willkürliches Töten ist für niemanden gut). Andere Einstellungen werden gemeinschaftsspezifisch sein und wieder andere sogar persönlich spezifisch. Der Vorteil ist, dass sich durch gegenseitige Kommunikation und durch Beobachtung der Einstellungen des eigenen Umfelds Konsens finden lässt — von bilateralen Arrangements über gemeinschaftliche und, mit der Zeit, dank der wirtschaftlichen Dominanz der am besten konfigurierten Gemeinschaften, sogar auf globaler Ebene.

Doch mehr zum Konsens im nächsten Kapitel.

JEDE GEMEINSCHAFT STELLT SICH SELBST EIN

DAS NETZ DISKRIMINIERT NICHT — JEDE REGION STELLT IHREN EIGENEN REGLER



EIN NETZ, VIELE REGLER — JEDE GEMEINSCHAFT ENTSCHEIDET SELBST.

Das Orakel-Problem — die Brücke zwischen digitaler und physischer Welt

Der Begriff „Orakel-Problem“ wird in jüngerer Zeit am häufigsten mit der Welt der Kryptowährungen, Blockchains und dezentralen Systeme in Verbindung gebracht. Allgemein: Wie stellt man sicher, dass Daten, die in ein digitales System eintreten, dem entsprechen, was tatsächlich in der physischen Welt geschehen ist? Das System selbst kann nicht überprüfen, ob jemand einem anderen wirklich geschadet hat oder ob ein Vertrag tatsächlich gebrochen wurde — es sieht nur digitale Einträge.

Hier lösen wir das über Autoritäten — Entitäten, die ihre Reputation darauf setzen, dass der digitale Eintrag der physischen Realität entspricht. Je höher die Reputation der Autorität, desto glaubwürdiger der Eintrag.

BRÜCKE ZWISCHEN DIGITALER UND PHYSISCHER WELT

DIE AUTORITÄT TRÄGT DIE REALITÄT HINÜBER



Die Reputation der Autorität macht den digitalen Eintrag vertrauenswürdig.

* Das System löst das Orakel-Problem nicht — es akzeptiert Autoritäten als Brücke und folgt dem, wie Vertrauen real schon funktioniert.

* Irrt die Brücke über die Wirklichkeit, zahlt die Autorität — mit ihrer Reputation.

Wie die Verifizierung funktioniert

Konsens und der Verifizierungsprozess

Um Konsens darüber aufzubauen, welche Regeln eine Gesellschaft im Durchschnitt hochhalten und durchsetzen sollte, kann der folgende Mechanismus helfen. Als DID-Teilnehmer erkläre ich die Regeln, zu denen ich mich bekenne und nach denen ich leben werde, und ich veröffentliche sie. (Denke es dir als die Satzung und die Statuten, die aus meiner Sicht meine ideale Welt ausmachen — eine Welt, in der ich mich nicht eingeschränkt, sondern sicher fühle.)

Ich kann im Voraus abschätzen, wie meine DID-Kontakte reagieren würden — und einschätzen, wie stark und von wem ich in gewöhnlichen sozialen oder geschäftlichen Interaktionen sanktioniert würde, sollten sie hypothetisch stattfinden.

Die endgültige Bewertung geschieht, wenn du Informationen von einer anderen DID anforderst oder sie bittest, eine Behauptung zu verifizieren (oder eine Autorität um einen Dienst bittest usw.), die du ins Reputationsnetzwerk veröffentlichen willst. Sie sollte genauso ausfallen, wie wenn du die Bewertung selbst im Trockenlauf gegen die erklärte Richtlinie der Gegenseite durchführst — und wenn nicht, dann stimmt etwas auf der Seite der Gegenseite nicht: Sie versucht, ein unehrliches Spiel zu spielen.

Das Ergebnis ist entweder eine Annahme mit einem genannten Preis für die Verifizierung (im Fall von Diensten eines Verifizierers oder einer Autorität) oder eine Ablehnung. Sowohl Sanktionen als auch Boni für Abweichungen von der Richtlinie des Bewertenden sind in den genannten Preis eingefaltet. Der Anfragende entscheidet dann, ob er die Bedingungen annimmt oder zur nächsten Runde der Verifizierung

im Zuteilungsalgorithmus übergeht — und wiederholt den Prozess, bis er zufrieden ist oder bis die Ökonomie das Weitermachen sinnlos macht.

Der soziale Graph

Das Reputationsnetzwerk ist in erster Linie ein soziales Netzwerk. Du fügst Kontakte hinzu — Menschen, die der Verbindung zustimmen. Sie haben Kontakte, und jene Kontakte haben Kontakte. Der Algorithmus sucht Verifizierer innerhalb einer konfigurierbaren Tiefe (z. B. drei Ebenen: deine direkten Kontakte, deren Kontakte und eine Ebene darüber hinaus). Keine globale Blockchain ist nötig — das Netzwerk bildet auf natürliche Weise Gemeinschaften mit Überlappungen in andere Gemeinschaften.

Der Algorithmus ist nichtdeterministisch: Er hasht dein Behauptungsdokument, bildet den Hash auf eine Position auf einem Ring bekannter Identitäten innerhalb dieses Kreises ab und wählt die nächstgelegene als Kandidaten-Verifizierer. Du kannst weder vorhersagen noch beeinflussen, wer deine Behauptung verifiziert.

Jede Ablehnung eines Verifizierers vergrößert dein Dokument und erhöht seine Verarbeitungskosten — das ist der erste Kostenkanal (Wachstum des Dokuments). Jeder neue Verifizierer verlangt eine Gebühr auf Basis des Datenvolumens, deiner Reputation und wie weit der Inhalt deiner Behauptung von seiner erklärten Verifizierungsrichtlinie abweicht — das ist der zweite Kostenkanal (Risikoprämie). Und jede Iteration kostet Zeit und Energie — der dritte Kostenkanal.

■ Was der Verifizierer prüft, der Reihe nach

Einmal ausgewählt, bewertet ein Verifizierer eine Behauptung in etwa vier geordneten Schritten — die günstigsten Filter zuerst, die teuren Inhaltsprüfungen zuletzt:

1. **Richtlinien-Gate.** Fällt diese Art von Behauptung überhaupt in das, was der Verifizierer öffentlich verifiziert? Wenn nicht, wird die Anfrage rundweg abgelehnt.
2. **Vertrauen in die Autorität.** Ist die Autorität, die die Behauptung befürwortet hat, unter der eigenen erklärten Richtlinie des Verifizierers vertrauenswürdig genug? Eine Autorität unterhalb der Vertrauensschwelle des Verifizierers ist ein Ablehnungsgrund, unabhängig vom Inhalt der Behauptung.
3. **Reputation des Ausstellers.** Erfüllt der Aussteller die Reputationsschwellen, die der Verifizierer für diese Art von Behauptung erklärt hat? Niedrige Reputation kann entweder die Gebühr erhöhen oder eine Ablehnung auslösen.
4. **Inhaltsprüfung.** Erst wenn die ersten drei Gates passiert sind, bewertet der Verifizierer die Behauptung selbst — Signaturen, innere Konsistenz, formale Korrektheit und wie weit sie von der Richtlinie des Verifizierers abweicht. Die für diesen letzten Schritt berechnete Gebühr spiegelt das tatsächlich eingegangene Risiko wider.

Der Verifizierer veröffentlicht die Richtlinie, die jedes dieser Gates regelt, sodass die Schritte nicht in seinem Ermessen stehen — er ist an das gebunden, was er bereits erklärt hat. Eine Abweichung von der veröffentlichten Richtlinie ist selbst eine veröffentlichbare Behauptung gegen ihn, und er bezahlt sie mit seiner Reputation.

Das Ergebnis: Die Veröffentlichung einer glaubwürdigen und nützlichen Behauptung kostet fast nichts. Die Veröffentlichung einer radikalen Behauptung kostet mehr. Die Veröffentlichung einer Lüge wird prohibitiv teuer — du musst Verifizierer um Verifizierer durchlaufen, und jeder, der dich ablehnt, fügt Kosten hinzu. Der Markt bepreist deine Behauptung, und der Preis sagt dir, wo du im Verhältnis zu den Gemeinschaften stehst, in denen du dich bewegst.

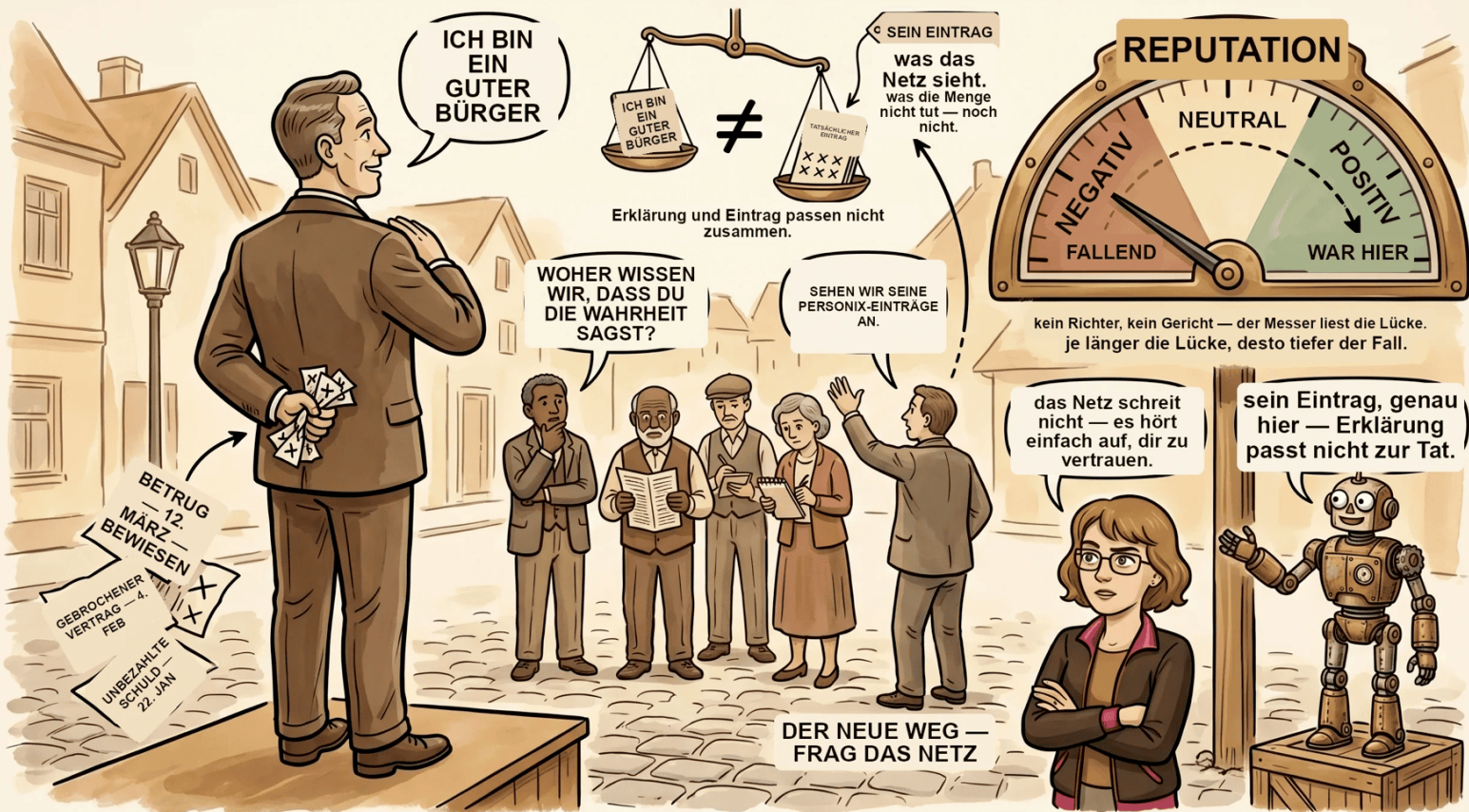
Es genügt nicht, zu erklären, dass du dich an eine Regel hältst, wenn du es in Wahrheit nicht tust. In diesem Fall riskiert deine DID die Veröffentlichung eines negativen Eintrags, der die Heuchelei offenlegt — was dich zu einem Risiko für alle anderen macht. Das Ergebnis sollten weniger, aber konsequenter befolgte Regeln sein und eine Lichtung jenes Dschungels aus Gesetzen und Vorschriften, in dem sich selbst Rechtsprofis kaum zurechtfinden.

Konsens vs. Rechenschaft

Damit das Netzwerk als wertvolle Informationsquelle dienen kann, sollte eine DID nicht zu radikal sein — sonst weisen die anderen sie ab. Der soziale Druck wird ein Gleichgewicht suchen, und Versuche, es zu destabilisieren, werden wahrscheinlich bestraft.

HEUCHELEI IST DAS TEUERSTE VERHALTEN

DAS NETZ VERGLEICHT LEISE DEINE WORTE MIT DEINEM EINTRAG — DIE LÜCKE SEHEN ALLE



ERKLÄREN UND BRECHEN? DIE LÜCKE IST DAS TEUERSTE VERHALTEN.

DAS MITTEL GEGEN HEUCHELEI

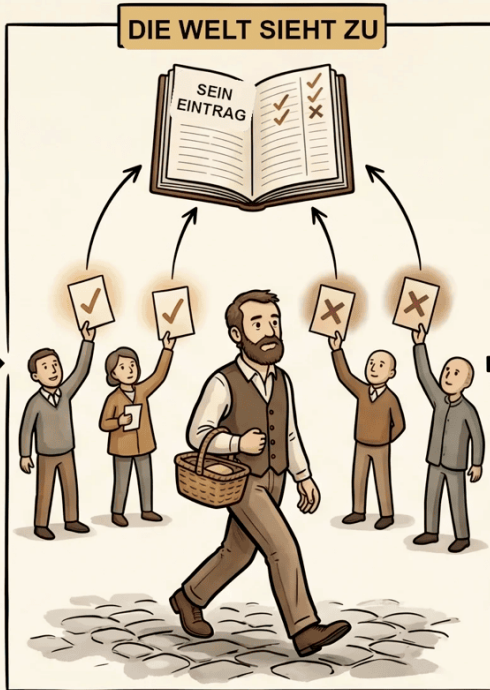
ERKLÄRE DEINE REGELN — LEBE SIE, ODER DER MARKT PREIST DICH AUS

ICH ERKLÄRE MEINE
REGEL



jeder kann meine Standards lesen.
keine Türsteher, keine Geheimnisse.

DIE WELT SIEHT ZU



die Welt schreibt auf, was er wirklich tut.
jeden Tag etwas mehr Beleg in seinem Register.

IM LADEN — DU ZAHLST FÜR DEINEN EIGENEN EINTRAG



Heuchelei wird nicht von einer Autorität bestraft — der Markt bepreist sie.
jede gewöhnliche Leistung, die du kaufst, trägt einen Aufschlag nach deinem eigenen Eintrag.

NENNEN WIR ES DEN GESELLSCHAFTSVERTRAG — NEU GEZEICHNET?

keine Autorität erzwingt die Ethik — der Preis tut es.
sanfter Druck, jeden Tag, hin zum gemeinsamen Mittel, mit dem alle leben können.

LEBE, WAS DU SAGST — ODER ZAHLE DAFÜR. HEUCHELEI IST DIE TEUERSTE REPUTATION.

■ Die Anzahl der Stimmen ist nicht dasselbe wie das Gewicht einer Stimme

Juraj Karpiš sagt, „Geld ist das Gedächtnis der guten Taten“. Ich würde hinzufügen, dass Reputation das Gedächtnis der schlechten ist.

Daraus folgt, dass meritokratisch derjenige, der mehr beiträgt und keine schlechte Reputation hat, ein größeres Stimmgewicht in der Gemeinschaft verdient. Durch die Linse bilateraler Beziehungen betrachtet: Wenn ich abwäge, welchen Konsensdrücken ich entgegenkomme, geht das größte Gewicht an die Beziehungen, aus denen ich den größten wirtschaftlichen Nutzen ziehe. Zehn Menschen, mit denen ich keinen aktiven Handel habe, werden mich weit weniger beeinflussen als ein dauerhafter Geschäftspartner. Dieses Paradigma ist nicht auf den Handel beschränkt — es erstreckt sich auf soziale, politische und andere Beziehungen.

Roles in the verification transaction and authorities

Überblick über die Rollen

Einige dieser Rollen haben wir im Kapitel über das Netzwerk und seine grundlegenden Eigenschaften bereits kurz gestreift. Nun ist es an der Zeit, sie erneut genauer zu betrachten und die weiteren hinzuzufügen, die wir brauchen, um das Netzwerk robuster zu machen. An jeder Verifizierungstransaktion sind mehrere Rollen beteiligt — sehen wir uns an, wie sie sich verhalten.

■ Rollen in einer Verifizierungstransaktion

An jeder Verifizierung sind bis zu sechs verschiedene Rollen beteiligt, zusammengefasst in der Tabelle unten. Sie alle können ihre eigene DID im dezentralen Reputationsnetzwerk haben.

Rolle	Beschreibung
Aussteller	Die Person, die Informationen im Netzwerk veröffentlicht — behauptet, dass etwas geschehen ist (eine DID wurde erstellt, bearbeitet oder aufgelöst, eine Behauptung, die Richtlinie einer gegebenen DID usw.)
Subjekt	Die Person, über die die Information handelt — der Adressat der Behauptung
Autorität	Eine vertrauenswürdige Entität, die ihren Namen für die Qualität der Behauptung einsetzt, indem sie sie untersucht und entweder die vorgelegten Beweise prüft oder sie aktiv sammelt
Beobachter	Ein unabhängiger Dritter, der festhält, wie der Verifizierer mit der Behauptung umgeht — und sicherstellt, dass der Verifizierer weder schweigt noch von der von ihm erklärten Richtlinie abweicht
Verifizierer	Ein algorithmisch ausgewählter Teilnehmer, der die Transaktion verarbeitet
Delegierter	Eine Person, die im Namen eines anderen Teilnehmers handelt

Aussteller

Dem Aussteller sind wir schon begegnet. Wenn jemandem ein Unrecht widerfährt oder er eine eigene Errungenschaft verbreiten möchte, ist es die durch die DID vertretene Person, die den Prozess auslöst, diese Information ins Netzwerk zu stellen — denn sie hat das primäre Interesse daran (die Motivation ist entweder der Wunsch nach Genugtuung oder das Bestreben, das eigene öffentliche Bild zu verbessern).

Positive Behauptungen

Positive Behauptungen über mich selbst kann ich als deren Subjekt und Aussteller zugleich für die Situationen aufbewahren, in denen ich sie nutzen möchte (ein Diplom, eine Bescheinigung über einen erbrachten Dienst usw.). Hier unterscheidet sich eine positive Behauptung von einer negativen: Das Teilen einer verifizierten negativen Behauptung liegt im Interesse der ganzen Gemeinschaft, während eine positive im Interesse ihres Trägers liegt.

Autorität

Die Autorität spielt eine Doppelrolle: Sie kann ein **Auditor** sein (der die Qualität der Beweise vor der Veröffentlichung einer Behauptung prüft) oder ein **Garant** (der seine Reputation auf die Wahrhaftigkeit einer Behauptung setzt). In beiden Fällen stärkt sie die Behauptung des Ausstellers. Diese beiden Dienste sind trennbar — eine Autorität kann den einen, den anderen oder beide zugleich anbieten. Die Arbeitsannahme ist, dass sich die meisten von Autoritäten erbrachten Dienste auf freimarktwirtschaftlicher Basis liefern lassen. Das gilt selbst in Bereichen, die man sich nur schwer privatisiert vorstellen kann, etwa

DER AUSSTELLER — WER DIE MELDUNG SCHREIBT

AUTOR · UNTERZEICHNER · SETZT SEINE REPUTATION EIN

- WAS DER AUSSTELLER TUT**
1. Schreibt die Meldung in eigenen Worten
 2. Sammelt reale Belege dafür
 3. Signiert mit eigener DID und sendet an die gewählte Autorität
 4. Trägt die Kosten der Veröffentlichung
 5. Trägt die Folgen, wenn er lügt

MEINE REPUTATION



Ist das falsch,
fällt meine Nadel.

Mein Name steht darauf.
Ich muss sicher sein —
und Beweise bringen.

Jeder darf reden. Lügen
kosten den Redner.



Der Aussteller ist der Autor. Sein Name steht darauf.

* Jeder mit einer DID kann Aussteller sein. Es zählt Mut und Verantwortung, keine Lizenz.

der Justiz, wo spezialisierte Dienste — Ermittlung, Beweiswürdigung, bis hin zu Diensten, die heute von zentralisierten Armeen erbracht werden (strategische Planung, standardisierte Ausbildung, Beschaffung und Vorratsverwaltung usw.) — von Marktakteuren effizient geliefert werden können. Es gibt kaum etwas, das sich nach einer Umstrukturierung nicht durch freimarktwirtschaftliche Anreize effizienter gestalten ließe.

■ **Die Autorität, der Aussteller und der Beobachter dürfen niemals der Verifizierer ihres eigenen Falls sein.**

Die algorithmische Auswahl des Verifizierers garantiert Unabhängigkeit. Niemand kann seine eigene Behauptung verifizieren oder eine Behauptung, an der er ein unmittelbares Interesse hat. Dies ist eine der grundlegenden Regeln, an deren Wahrung die gesamte Gemeinschaft der DIDs ein Interesse hat.

Die folgenden Grafiken zeigen einander ergänzende Sichtweisen auf die Bandbreite der Tätigkeiten, die Autoritäten abdecken (der Begriff „Autorität“ lässt sich austauschbar mit „Dienstleister“ lesen).

DIE FÜHRERIN — NAVIGIERT NACH DEINEN WERTEN

TIEFE ANALYSE HINTEN · EINFACHER RAT VORNE

FÜHRER

ANHÄNGER
DIESES FÜHRERS
— JÄHRLICH
ERNEUERBAR

zum Beispiel: wer Führer sein darf

- eine Partei oder Bewegung, die eine Richtlinienvorlage veröffentlicht
- eine unabhängige Prüffirma, die aggregierte Ergebnisse veröffentlicht
- eine Dienstleistungs-Vergleichsagentur
- ein Reputations-Aggregator (Wirtschaft · Geschäft · Nachbarschaft · Verkehrssicherheit)
- ein Journalist-Rezensent oder Verbraucherbewertungsdienst

MEINE ANALYSE

öffentliche Ausgaben - umgelenkt

Arbeitsnotizen — nicht für Kunden

Ich mache die schwere Arbeit.
Du bekommst den einfachen Rat — nur wenn du meine Werte teilst.

Und was bekomme ich für mein Geld — welche Analysen, welche Übersichten?

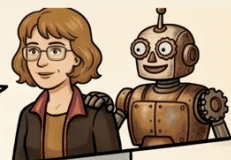
FÜR DICH — WAS DAS HEISST

Gebündelt zu deinem größten Nutzen

- hier Ausgaben verschieben, dort sparen
- Anbieter unterstützen, die meine Tests bestehen
- diese Richtlinienvorlage übernehmen



Sie verdichtet die komplexe Welt zu Empfehlungen.
Follower stimmen mit ihrer Aufmerksamkeit ab — jederzeit gehen, jederzeit wechseln.



Gebunden an das, wofür sie öffentlich stehen. Dein Vertrauen ist ihre Währung.

* Du kannst jederzeit gehen und den Begleiter wechseln. Dein Vertrauen ist nicht gebunden.

* Der Begleiter kann auch eigene Meldungen signieren — veröffentlicht, aber hier nebensächlich.

■ Autorität als Inkognito-Beobachter

Eine reputable Autorität — denke an einen Notar, dessen Geschäft allein von seiner Erfolgsbilanz abhängt — kann neben den Hauptfunktionen (Auditor / Garant) eine dritte anbieten: die Rolle des Inkognito-Beobachters während der Verifizierung. Sie hält einen mit Zeitstempel versehenen Eintrag der eingereichten Behauptung fest, damit der Verifizierer sie nicht stillschweigend fallen lassen kann. Der Mechanismus der Beobachterrolle wird weiter im Abschnitt über die Beobachterrolle beschrieben.

Verifizierer

Jede DID kann als Verifizierer auftreten, entweder direkt oder über Verifizierungsrechte, die an eine dritte DID delegiert sind. Damit ich — oder mein Delegierter — verifizieren kann, sollte ich im Netzwerk erreichbar sein (online). Nicht jeder wird sich dazu verpflichten wollen, weshalb ein DID-Eintrag in Prioritätsreihenfolge die Vertreter auflisten kann, die die Funktion in seinem Namen ausüben, während es offline ist.

Jede im Netzwerk aktive DID erklärt öffentlich ihre eigene Richtlinie. Durch die in dieser Richtlinie definierten Regeln beurteilt sie während des Verifizierungsprozesses die Reputation der Gegenseite sowie Inhalt und Form der Behauptung, die der Aussteller zur Veröffentlichung ins Reputationsnetzwerk vorgemerkt hat. Teil der Richtlinie ist die Berechnungsformel, mit der die Gebühren für Verifizierungsdienste berechnet werden. Sobald das steht, warte ich über eine statistisch große Zahl von Behauptungen, die durchs Netzwerk fließen, darauf, dass mich der Algorithmus des Netzwerks auf die Seite des Ausstellers

DER ANBIETER — BETREIBT EINEN SIGNIERDIENST FÜR MELDUNGEN

VERÖFFENTLICHTE STANDARDS · VERÖFFENTLICHTE PREISE



Gebunden an das öffentlich Erklärte. Den Rest erledigt die Reputation.

* Auch der Anbieter hat eine eigene Richtlinie — wann er annimmt, wann er ablehnt, wie er erstattet. Sie ist veröffentlicht, aber hier nebensächlich.

zieht und mir in einer gegebenen Iteration zuweist, die herausgegebene Information zu verifizieren. Der Aussteller kann im Voraus berechnen, wie ein sich korrekt verhaltender Verifizierer reagieren würde, kann es aber nicht vermeiden, ihn (oder seine Vertreter) tatsächlich zu kontaktieren; die Iteration mit dem ausgewählten Verifizierer muss der Aussteller selbst dann durchführen, wenn er im Voraus weiß, dass sie nicht durchgehen wird.

Woher wissen wir, dass der Aussteller den Algorithmus zur Verifiziererauswahl über die richtige Menge von Kandidaten-Verifizierer-DIDs laufen lässt? Zusammen mit ihrer öffentlich erklärten Richtlinie veröffentlicht jede DID auch die aktuelle Liste der Kennungen ihres sozialen Netzwerks innerhalb des Reputationsnetzwerks. Definiert ein Aussteller sein soziales Netzwerk als eine soziale Blase, die lediglich seine eigenen Ansichten widerhallt und verstärkt, so werden über sie veröffentlichte Informationen von anderen Gemeinschaften kaum breiter aufgenommen. Dass es mir gelingt, unter hohen Kosten eine radikale Behauptung ins Netzwerk zu drücken, bedeutet nicht, dass ich ihr bei der Beurteilung der Reputation der Gegenseite irgendein Gewicht beimessen werde. Manche Behauptungen drängt mich meine Gemeinschaft zu berücksichtigen (über Täter verhängte Strafen und Beschränkungen); andere stehen ganz mir frei — ich entscheide selbst über den wirtschaftlichen Wert, eine gegebene Information einzubeziehen oder auszuschließen.

Subjekt

Jene, die die ins Reputationsnetzwerk veröffentlichte Information betrifft, sind ihre Träger oder, wenn man so will, ihre Subjekte. Die Anreize im Reputationsnetzwerk sind so gesetzt, dass das Subjekt allen Grund hat, sich nach seinen eigenen Regeln korrekt und fair zu verhalten, und von der Gemeinschaft zu einer goldenen Mitte der Regeltreue gedrängt wird. Es hat sogar einen Anreiz, sich moralischer zu verhalten, als seine erklärten Regeln verlangen — im Voraus erklärte Richtlinien schließen nicht aus, dass die Gemeinschaft zu einem Konsens gelangt, eine Bewertung oder Maßnahme rückwirkend anzuwenden.

Aus diesem Blickwinkel ist die reputationsnetzwerkbasierte Alternative zu einer Rechtsordnung, wie zu erwarten, stärker vom Geist der Regeln als von ihrem Buchstaben getrieben.

DER PRÜFER — MISST DIE MELDUNG AN DER VERÖFFENTLICHTEN POLICY

VIER TORE, DER REIHE NACH. BILLIGE FILTER ZUERST.

PRÜFTORE — DER REIHE NACH

1. RICHTLINIENFILTER

Prüfe ich diese Art Meldung überhaupt?

2. VERTRAUEN ZUR AUTORITÄT

Liegt die Autorität über meiner Schwelle?

3. REPUTATION DES AUSSTELLERS

Erfüllt der Aussteller meine Reputationsgrenze?

4. INHALTSPRÜFUNG

Signaturen, Konsistenz, Abweichung von der Policy

DARF NICHT SEIN: Aussteller, Autorität, Beobachter oder Subjekt.

PRÜFER-REPUTATION

REGEL BRECHEN
FÄLLT → REPUTATION
FÄLLT → KEINE WAHL MEHR

WAS DER PRÜFER TUT

1. Filtert nach seinen veröffentlichten Richtlinien (der Reihe nach)
2. Prüft Vertrauen zur Autorität, dann Reputation des Ausstellers
3. Prüft den Inhalt der Meldung nur, wenn die Filter greifen
4. Verlangt eine Gebühr im Verhältnis zum Risiko
5. Setzt bei jeder Entscheidung die eigene Reputation aufs Spiel

GEBÜHR
RISIKO $\propto$

mehr Risiko → höhere Gebühr

Billige Filter zuerst. Teure Inhaltsprüfung zuletzt.

Er darf nicht kreativ sein. Er muss tun, was seine Regel sagt.

Seine eigenen Regeln. Öffentlich. Er kann sie nicht heimlich ändern.

Der Prüfer ist an die Regeln gebunden, die er selbst veröffentlicht hat — und an die Reputation, die er verlieren kann.

DAS SUBJEKT — WEN DIE MELDUNG BETRIFFT

ERHÄLT ES · KANN ES NICHT UNTERDRÜCKEN · KANN ANTWORTEN



Das Subjekt hat kein Veto — nur das Recht zu antworten.

* Eine Gegenmeldung ist selbst eine Meldung — die Reputation des Subjekts haftet für die Antwort.

Beobachter

Die Beobachterrolle nimmt dem Verifizierer den Anreiz, die Regeln zu beugen. In Situationen, in denen einem Verifizierer die Anfrage des Ausstellers oder der Autorität nicht gefällt, könnte er einfach schweigen — nicht antworten und die algorithmische Abfolge blockieren. Der Beobachter — oder eine Gruppe von Beobachtern — setzt seine Reputation darauf, zu dokumentieren, wie der Verifizierer abgefragt wurde. Schweigt der Verifizierer trotz einer erklärten Richtlinie, die etwas anderes besagt, kann er des Verstoßes gegen das Protokoll überführt werden.

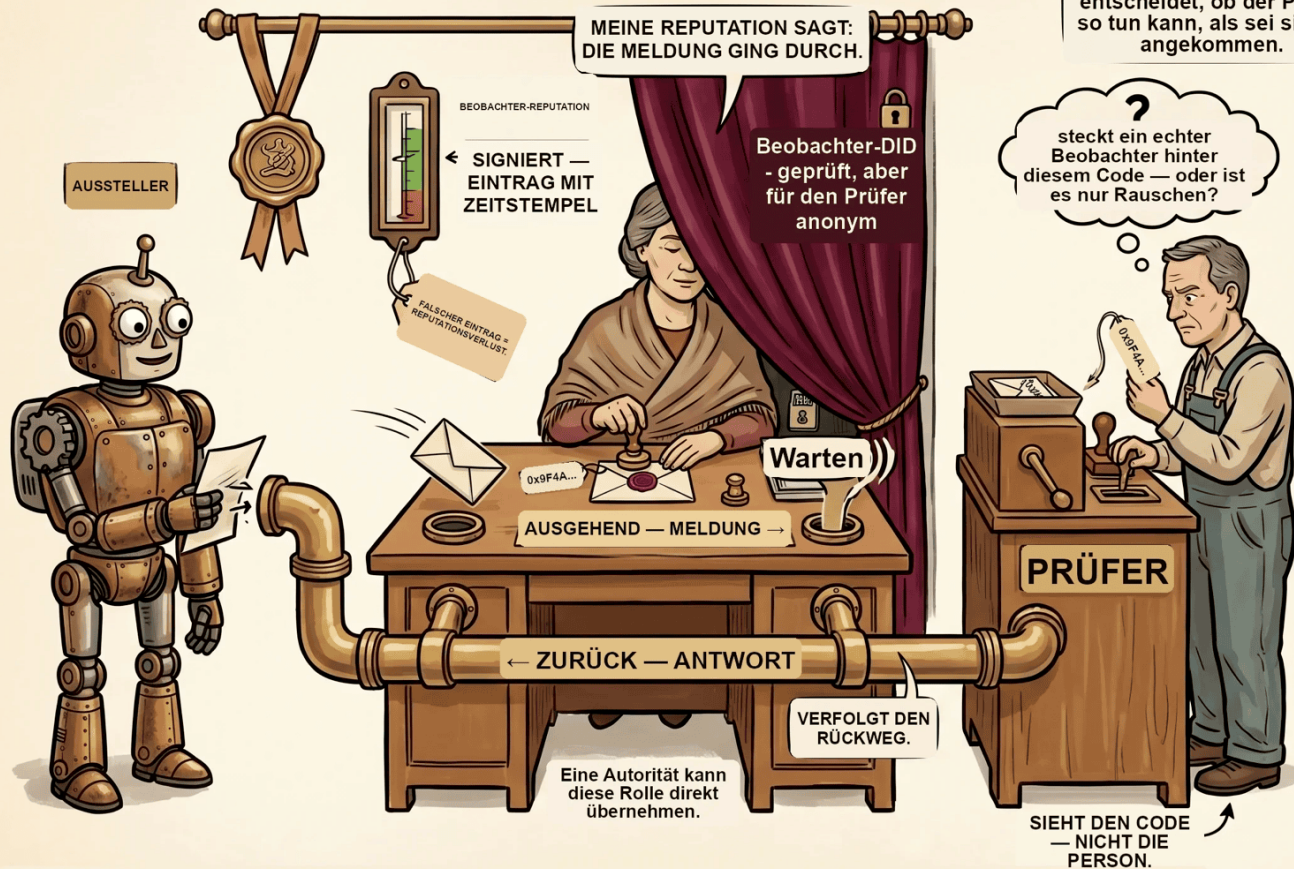
Der Mechanismus: Zeitstempel und Challenge-Code

Bevor du eine Behauptung an den Verifizierer schickst, leitest du sie über Beobachter — Menschen, denen du vertraust, oder spezialisierte Beobachter-Dienstleister, die eine kleine Gebühr verlangen. Jeder Beobachter empfängt deine Einreichung, versieht sie mit einem Zeitstempel, signiert, dass er sie hat hinausgehen sehen, und erzeugt einen Challenge-Code — einen kryptografischen Hash seiner Signatur. Die Codes werden an deine Anfrage angehängt. Der Verifizierer sieht sie, hat aber keine Ahnung, wer die Beobachter sind oder ob die Codes überhaupt echt sind. Beobachter fungieren so als Mittler zwischen dem Aussteller und dem Verifizierer und halten einen unabhängigen Nachweis, dass die Behauptung eingereicht wurde und was sie enthielt. Es kann null bis N von ihnen geben.

Wenn sich der Verifizierer ehrlich verhält — annehmend oder ablehnend im Einklang mit seiner erklärten Richtlinie —, bleiben die Codes undurchsichtig. Niemand wird bloßgestellt.

DER BEOBACHTER — EIN PROXY, DER DIE MELDUNG WEITERLEITET UND DEN RÜCKWEG VERFOLGT

DER PRÜFER SPRICHT MIT IHR. ER ERFÄHRT NIE, WER SIE IST — ODER OB ÜBERHAUPT JEMAND ZUSIEHT.



WAS DER BEOBACHTER TUT

1. Erhält die Meldung vom Aussteller
2. Versieht sie mit ihrem Siegel. Das Siegel ist der Zeitstempel-Eintrag
3. Leitet sie im Namen des Ausstellers an den Prüfer weiter
4. Beobachtet, ob die Antwort kommt und was sie sagt
5. Veröffentlicht ihre Signatur nur bei Fehlverhalten des Prüfers — ihre Reputation ist die Garantie

Fußnoten

* Hinter jeder Antwort stehen null bis N Beobachter. Der Prüfer sieht nur undurchsichtige Codes und weiß nie, ob ein echter Beobachter zusieht oder ob es nur Rauschen ist. Diese Ungewissheit ist der Anreiz, sich korrekt zu verhalten.

* Symmetrisch kann der Prüfer die Antwort über einen eigenen Beobachter leiten — gleicher Trick, andere Richtung.

Anonym nach außen, rechenschaftspflichtig im Netz. Der Prüfer sieht den Code, nie den Beobachter.

Doch wenn der Verifizierer trotz einer entgegenkommenden Richtlinie schweigt oder in einer Weise antwortet, die dem widerspricht, was er veröffentlicht hat, hältst du die ursprünglichen Beobachter-Signaturen. Du kannst sie als stellvertretendes Zeugnis dafür veröffentlichen, dass die Behauptung eingereicht wurde und dass der Verifizierer dem Protokoll nicht gefolgt ist. Jeder kann überprüfen, dass die Signaturen zu den Challenge-Codes passen.

Die Pointe: Du brauchst keine echten Beobachter

Und hier kommt der eleganteste Teil: **Du brauchst überhaupt keine echten Beobachter.** Du kannst Zufallszahlen erzeugen, die genau wie Challenge-Codes aussehen. Der Verifizierer kann den Unterschied nicht erkennen — er muss würfeln, ob er seine Reputation riskiert. Hinter jeder Anfrage, die er erhält, könnte ein angesehener Beobachter inkognito zusehen — oder es könnte reines Rauschen sein. Der Verifizierer weiß es nicht. Und diese Ungewissheit ist der Mechanismus.

Die Kosten, ehrlichen Druck aufrechtzuerhalten: nahezu null (Zufallszahlen sind gratis). Die potenziellen Kosten der Unehrlichkeit für den Verifizierer: katastrophal. Ehrliches Verhalten wird selbst dann incentiviert, wenn niemand tatsächlich zusieht.

Das System funktioniert, weil jeder ein wenig paranoid ist. Ungewissheit ist billiger als Überwachung.

DER BLUFF, DER DEN PRÜFER EHRLICH HÄLT

ECHTER BEOBACHTER UND ZUFÄLLIGER BLUFF SEHEN VOM PRÜFER AUS GLEICH AUS

AUSSTELLER — KAMILA

ECHTER BEOBACHTER

PRÜFER



AUSSTELLER — BLUFFT

KEIN BEOBACHTER

PRÜFER — GLEICHES VERHALTEN



UNGEWISSHEIT IST BILLIGER ALS ÜBERWACHUNG.

■ Mehrere Verifizierer in einer einzigen Iteration

Eine verstärkende Begleitregel für die Verfügbarkeit von Verifizierern kann eine algorithmische Erweiterung sein, die in einer einzigen Iteration eine Menge von Kandidaten-Verifizierern statt nur eines einzigen zurückgibt.

Delegation

Die Zivilisation hat ihr wirtschaftliches Wachstum auf der Fähigkeit zur Arbeitsteilung und Spezialisierung aufgebaut. Die Welt in ihrer vollen Pracht ist komplex, und unsere Chancen, sie in all ihrer Komplexität zu erfassen, sind nahezu null. Der natürliche Ausweg ist, ein breites Spektrum von Tätigkeiten, die ein bequemes Leben stützen, an spezialisierte Anbieter zu delegieren, die uns Zeit, Energie und Geld sparen und es uns ihrerseits erlauben, uns zu spezialisieren — die Dienste zu erbringen, in denen wir am besten sind oder die der Markt an uns am höchsten schätzt.

Dieselbe Logik der Delegation reicht ins Reputationsnetzwerk hinein. Im Kapitel Der Schalter zwischen Freiheit und Totalitarismus (und Delegation) haben wir die Prinzipien dargelegt, wie sich eine freie Gesellschaft dadurch schützen lässt, dass die Anzahl der Behauptungen begrenzt wird, die innerhalb eines gegebenen Zeitfensters ins Netzwerk veröffentlicht werden können (denke vereinfacht an niedrige einstellige Veröffentlichungsrechte pro Jahr, damit die Gesellschaft maximal frei bleibt). Dieses Prinzip lässt sich auf mehrere Dimensionen ausdehnen. Wir müssen nicht nur eine Zahl haben — wir können mehrere Limits haben, die für verschiedene Arten von Behauptungen gelten. Wir können eine andere

Zahl für das Anprangern der Heuchelei anderer verwenden als für Fehlverhalten in Geschäftsbeziehungen, und, sagen wir, eine Änderung des DID-Dokuments wie ein Passwortwechsel ist etwas, das die Gemeinschaft kaum interessieren wird, und so weiter. Es hängt alles davon ab, wie die Gemeinschaft über die evolutionäre Zeit definiert, was ihren Interessen dient, um das richtige Gleichgewicht zwischen ihrem angestrebten Maß an Freiheit und Rechenschaft zu finden.

Warum sollte die Anzahl der mir von der Gemeinschaft gewährten Veröffentlichungsrechte klein genug sein? Eine DID (ein Subjekt) mit einer negativen Behauptung anzuprangern, zerstört Reputation, deren Aufbau lange gedauert hat, und der Schaden hält an. Eine zerstörte Reputation sieht sich einer Skala eskalierender Sanktionen der Gemeinschaft für jedes weitere oder wiederholte Vergehen gegenüber, bis hin zur vollständigen Ausschaltung der störenden Entität (der Extremfall). Eine exponentiell eskalierende Strafskala braucht kein großes Volumen an Behauptungen, sofern sie durch überprüfbare Beweise gedeckt sind. Das gilt für den friedlichen Ruhezustand, wenn die Gesellschaft nicht durch eine Katastrophe (äußere oder innere) erschüttert wird.

Bei Ereignissen mit sehr geringer Wahrscheinlichkeit ist die statistische Häufigkeit volatil, wenn man sie auf ein Individuum anwendet. Über die Population der Gemeinschaft hinweg ist sie es nicht. Das ist der Wert, seine Veröffentlichungsrechte an spezialisierte aggregierende Autoritäten zu delegieren, die — ganz wie eine gegenseitige Versicherung im Schadensfall — dein Recht nutzen und es in deinem Namen anwenden. Reden wir weniger abstrakt und geben ein paar Beispiele: - das Aufdecken und Bekämpfen organisierter Kriminalität - die Durchsetzung von Geschäftsvereinbarungen - die Verwaltung von Privilegien (Ausbildungsnachweise, Erwerb / Veräußerung von Vermögenswerten usw.) - und so weiter

DER DELEGAT — EIN MELDUNGSDIENST IM ABO

DELEGIERE, WAS DU NICHT SCHAFFST · BEHALTE, WAS DIR WICHTIG IST



Gib ab, was du nicht selbst schaffst. Bleib im Bilde. Hol die Rechte jederzeit zurück.

* Handelt der Delegat außerhalb des vereinbarten Rahmens, leiden öffentlich seine und deine Reputation.

■ Wie „Veröffentlichungsrechte“ tatsächlich funktionieren

Die Grafik für den Delegierten zeigt Veröffentlichungsrechte der Klarheit halber als physische Token, doch im System existiert kein solches Objekt. Was tatsächlich geschieht, ist Folgendes: Die Richtlinien der Menschen, bei denen du in gutem Ansehen bleiben willst — deine Gemeinschaft —, aggregieren zu einer emergenten Regel darüber, wie viele Behauptungen pro Jahr sie von dir als relevant akzeptieren, bevor sie beginnen, dich als Rauschen zu behandeln. Die Obergrenze existiert, damit das Netzwerk nicht in trivialen „Was wäre wenn“-Behauptungen ertrinkt und so frei bleibt, wie es die Gemeinschaft will (Signal bewahrt durch Begrenzung des Volumens).

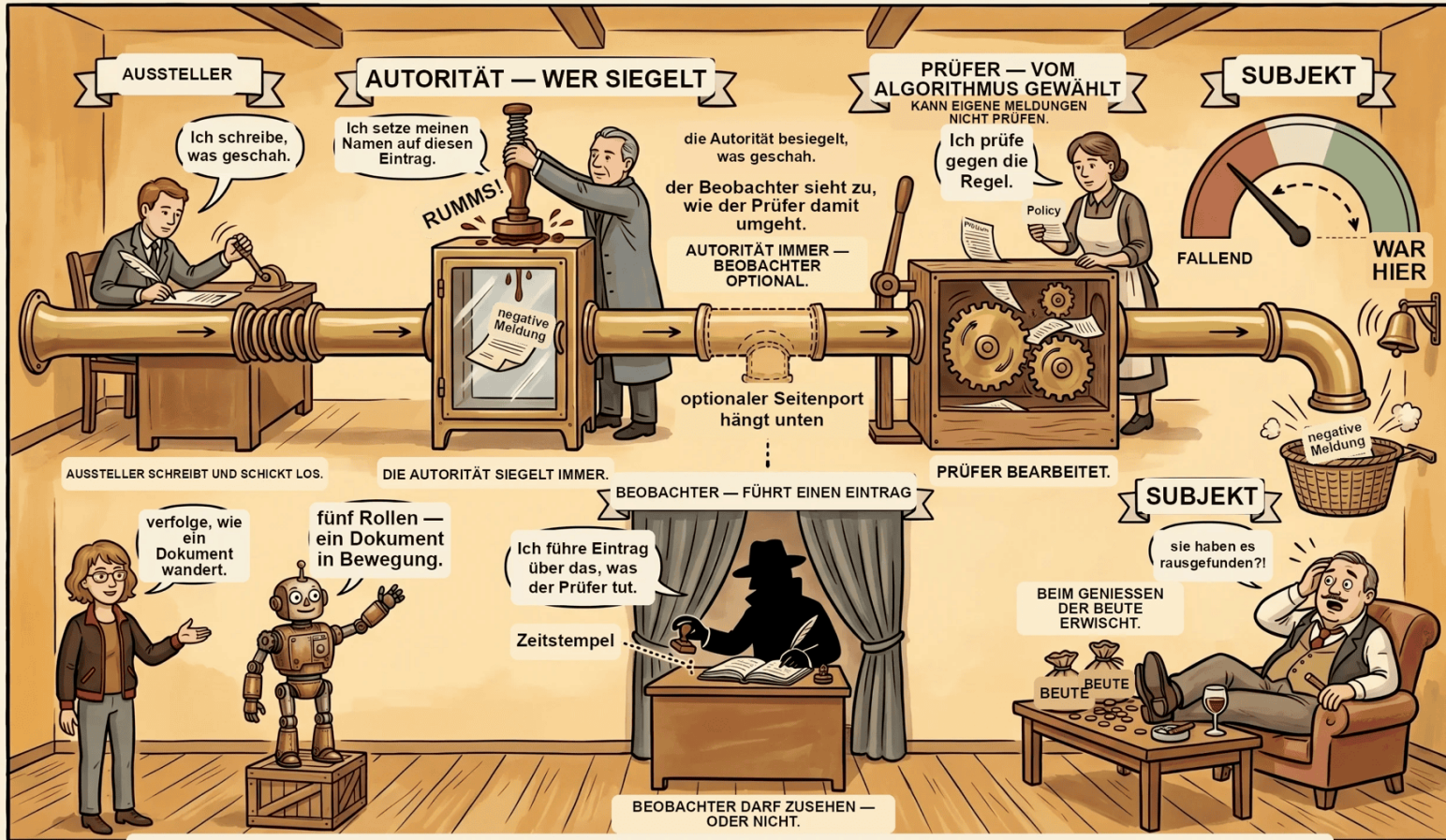
Du liest, was deine Gemeinschaft dir erlaubt. Es gibt eine Spanne, mit einer gewissen Streuung, je nachdem, welche Menschen du am stärksten gewichst. Du entscheidest dann — innerhalb dieses Kontingents —, wie viele Behauptungen du selbst veröffentlichst und wie viele du an professionelle Dienste delegierst, die in deinem Namen nur dann veröffentlichen, wenn Ereignisse in ihren Zuständigkeitsbereich fallen. Das ist es, was dich in gutem Ansehen hält, ohne dich zu zwingen, für jede Kleinigkeit, die dir widerfährt, eine Behauptung einzureichen.

Die „Token“ in der Grafik sind ein visueller Platzhalter für diese Lese-und-Entscheide-Schleife, kein wörtliches Artefakt.

Es lohnt sich, delegierte Veröffentlichungsrechte im Reputationsnetzwerk widerrufen zu können. Das lässt sich jederzeit tun, solange der Delegierte das delegierte Recht noch nicht genutzt hat.

EINE NEGATIVE MELDUNG LÄUFT DURCH DAS SYSTEM

FOLGE EINEM DOKUMENT — SIEH, WAS JEDE ROLLE DAMIT TUT



FÜNF ROLLEN, EIN DOKUMENT IN BEWEGUNG — NIEMAND PRÜFT SICH SELBST.

Kommunikation zwischen den Rollen

Die Grafik unten fasst zusammen, wie sich die Rollen in einem realen Fall verbinden — von der Einreichung einer Behauptung durch den Aussteller bis zur Veröffentlichung ins Reputationsnetzwerk.

Der emergente Gesellschaftsvertrag — Policy

Bisher haben wir beschrieben, wie Behauptungen verifiziert werden und welche Rolle jede Rolle dabei spielt. Nun wenden wir uns der Frage zu, wie aus Tausenden einzelner Richtlinien etwas wird, das wie ein echter Gesellschaftsvertrag funktioniert. Nichts, was den linken Träumen von einem Gesellschaftsvertrag und erzwungener Solidarität gleicht.

Jeder Teilnehmer erklärt seine eigene Richtlinie auf Basis seiner Moral (Policy) — was er für akzeptabel hält und wie er auf konkretes Verhalten anderer reagiert. Die Gesamtheit aller einer gegebenen DID bekannten Richtlinien im Netzwerk (die Gemeinschaft) bringt eine emergente Ethik hervor — beobachtbare Normen, die niemand entworfen hat. Diese emergenten Normen, unterlegt mit bilateralen Preissignalen, bilden einen messbaren Gesellschaftsvertrag: kein theoretisches Konstrukt, das niemand bei der Geburt unterschrieben hat, sondern empirisch beobachtbare Regeln, die von tatsächlichem Verhalten gedeckt sind.

■ Der Gesellschaftsvertrag

Man debattiert, ob „Gesellschaftsvertrag“ nicht ein Oxymoron ist. Niemand unterschreibt etwas, und dennoch wird er herangezogen, um legislatives und exekutives Handeln in zentralisierten Gesellschaften zu rechtfertigen.

Eine phänomenologische Analyse der Interaktionen in einem dezentralen Netzwerk könnte gewisse emergente Regeln offenlegen — globale oder lokale. Wie sollten wir diese breit geteilten Normen nennen? Einen Gesellschaftsvertrag? Ebenso wie bei Gemeinschaften lässt sich der Gesellschaftsvertrag einer Gemeinschaft nicht präzise beobachten und abgrenzen — jeder Blickwinkel auf die Gemeinschaft ergibt einen anderen Gesellschaftsvertrag.

■ Wertebasierte Politik

Ebenso irreführend ist es, „wertebasierte Politik“ als Grundlage der Entscheidungsfindung zu behandeln. Werte sind eher phänomenologische Cluster von Regeln, die zu einer gegebenen Zeit allgemein bevorzugt werden. Sie entwickeln sich und sind über die Zeit nicht konstant.

POLICIES TREFFEN SICH. HALTUNGEN ENTSTEHEN.

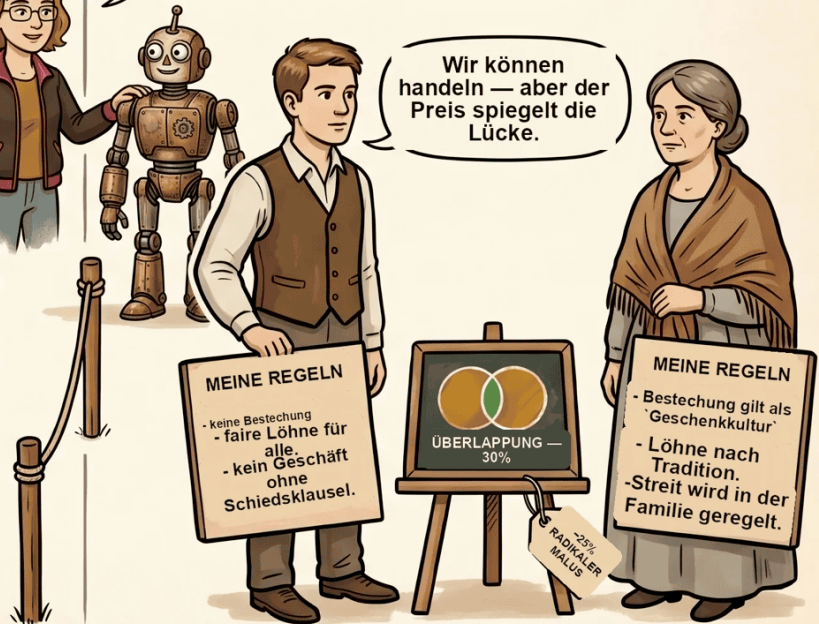
ERKLÄRTE REGELN SETZEN DEN PREIS — RABATT FÜR TREUE, MALUS FÜR ABWEICHUNG

WENN POLICIES ÜBEREINSTIMMEN



Gleiche Ware, zwei Preise. Erklärungen — nicht Reputation — entscheiden.

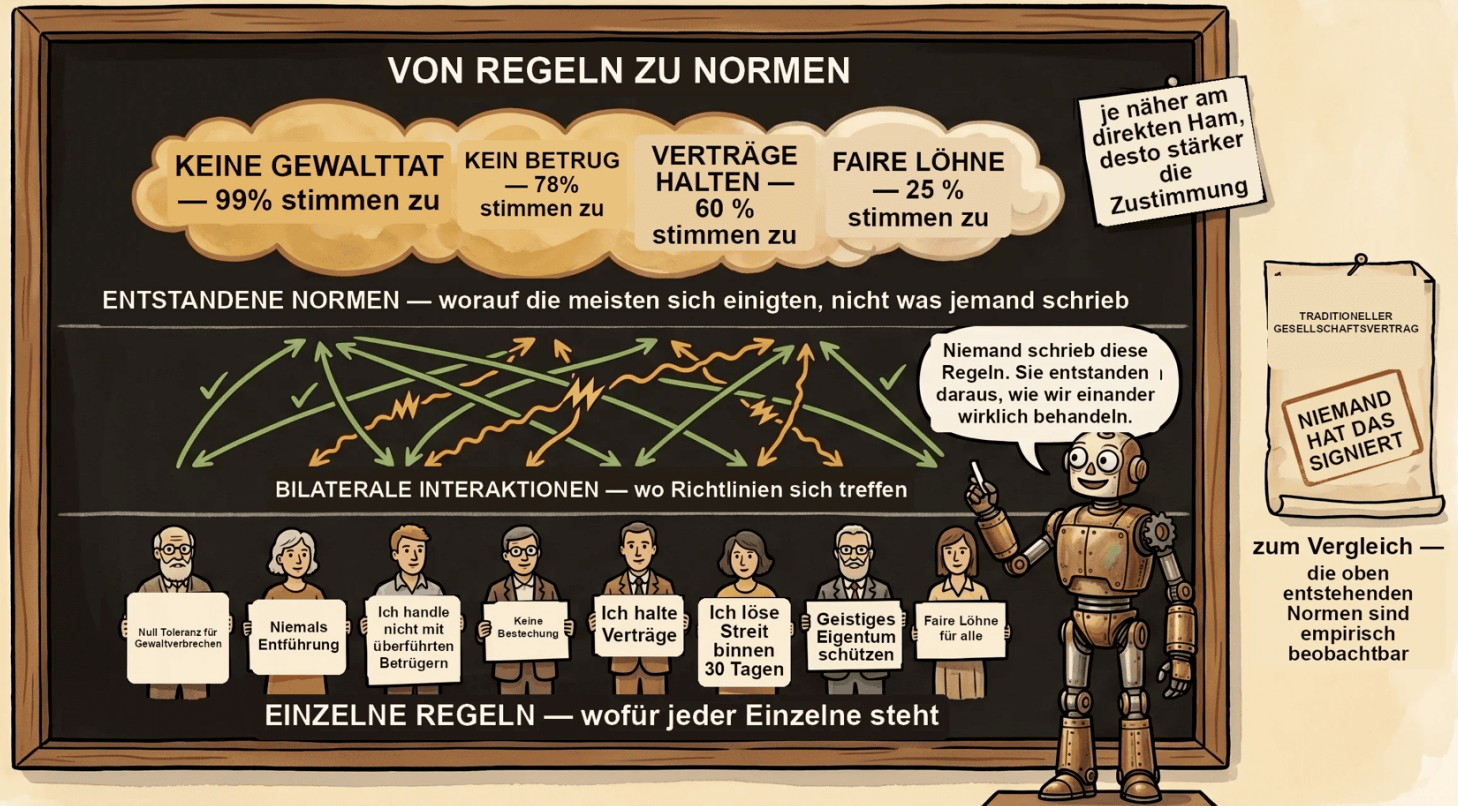
WENN POLICIES AUSEINANDERGEHEN



Treffen zwei Policies im Handel aufeinander, wird ihre Übereinstimmung zum Preisfaktor.

* Es geht nicht um Reputation. Es geht darum, was jeder öffentlich erklärt hat — und nun halten soll.

WIE ETHIK AUS EINZELNEN REGELN ENTSTEHT



Ethik wird nicht entworfen. Sie entsteht daraus, wie wir einander wirklich behandeln.

* Jede Richtlinie spiegelt die Moral ihres Trägers — geformt vom Druck, sich an Gemeinschaft und Umfeld anzupassen.

Informationen über dich selbst bereitstellen

Wenn zwei DID-Subjekte, die einander nicht kennen, in eine wirtschaftliche Beziehung treten, können wir im Namen der anderen Partei eine Anfrage an unsere eigene Gemeinschaft signieren und sie bitten, Informationen über uns bereitzustellen. Das ist jedoch eine sehr naive Vorstellung davon, was Gemeinschaften sind. Sie sind keine geschlossenen Mengen — eine einzelne DID kann Teilnehmer mehrerer Gemeinschaften sein.

Eine Gemeinschaft ist eher ein phänomenologisches Phänomen aus der Perspektive eines gegebenen Teilnehmers, das sich in seinem sozialen Netzwerk manifestiert; sie ist nicht etwas, das immer sinnvoll explizit abzugrenzen wäre. Die Bewohner eines Dorfes können eine Gemeinschaft bilden, doch ein Mensch, der nur am Wochenende dorthin kommt, kann in demselben Dorf auch einer anderen Gemeinschaft angehören. Eine Gemeinschaft kann auch eine Fußballmannschaft samt ihren Fans, ihren Funktionären und den Familien aller Beteiligten sein. Eine Nation oder die Bürger eines Staates können ebenfalls eine Gemeinschaft oder Gemeinschaften bilden. Eine DID aus verschiedenen Blickwinkeln zu betrachten, kann verschiedene (und oft intuitive) Sichtweisen auf Gemeinschaften ergeben.

DIDs an den Grenzen sind somit Brücken zwischen Gemeinschaften und spielen — genau wie im echten Leben — eine Rolle bei der Bereitstellung von Informationen über Mitglieder anderer Gemeinschaften, sei es auf Amateurniveau oder professionell, etwa eine Autorität, die sich auf das Zusammenbringen von Menschen und das Aggregieren von Informationen über riskante DIDs spezialisiert.

Manche Arten von Informationen im DID-Netzwerk eignen sich gut für einen bedingungslosen gegenseitigen Austausch (Gewaltverbrechen, Betrug usw.). Andere Arten von Informationen wiederum mag eine Gemeinschaft als auf die Verwendung innerhalb der Gemeinschaft beschränkt behandeln (das Äquivalent der Staatsbürgerschaft, für die Gemeinschaft erbrachte Dienste usw.). Ob sich solche Informationen verbreiten lassen, hängt von den erklärten Richtlinien der Mitglieder der Gemeinschaft ab.

Eine Gemeinschaft hütet ihre Privatsphäre im eigenen Kreis und tauscht im Gegenzug beiderseitig nützliche Informationen auf bedingungsloser Basis aus.

Verbrechen und Strafe

Verbrechen und Strafe

Wir wissen, wie das Netzwerk funktioniert: wie Einträge entstehen, wer sie verifiziert, wie ein Betrug des Verifizierers abgeschreckt wird. Eine Frage bleibt — was geschieht, wenn jemand tatsächlich einem anderen Schaden zufügt?



Wie sehr hängen wir voneinander ab?

Wir alle stehen auf der Bühne dieser großen Welt, und was auch immer sich hier zuträgt, geht uns alle an.

Johann Amos Comenius (Das Labyrinth der Welt und das Paradies des Herzens)

Es mag viele Gründe geben, einem Reputationsnetzwerk beizutreten oder es abzulehnen. Ich glaube jedoch, dass ein Aspekt der menschlichen Natur — oft als dunkel angesehen — einem guten Zweck dienen kann. Ich spreche vom menschlichen Bedürfnis, angesichts wahrgenommenen Unrechts ein Gefühl der Genugtuung zu empfinden.

Genugtuung, Gerechtigkeit, Rache — wir verbinden sie mit negativen Emotionen. Damit die Gesellschaft zusammenhält, müssen wir zumindest so tun, als würde Genugtuung durch zentralisierte

Institutionen geleistet; sonst würden sich die Einzelnen mit der Gesellschaft, in der sie leben, nicht verbunden fühlen. Im Durchschnitt müssen wir irgendeinem Team angehören und ihm vertrauen. Wenn jemand einem anderen schadet, sieht die Gesellschaft zu, wie und in welchem Maße Genugtuung geleistet wird. Etwas kontrovers behaupte ich, dass es in der Geschichte oft — und jetzt — nicht darauf ankam, ob das Verfahren gegen den Angeklagten sauber war; worauf es ankam, war, dass die Gesellschaft *jemanden* bestraft sah. Es erfüllte seine Funktion (zahlreiche Justizirrtümer und der Widerstand gegen die Wiederaufnahme alter Fälle erzählen diese Geschichte deutlich genug). Die Sicht des Opfers und der Hinterbliebenen ist nur zweitrangig. Was zuerst zählt, sind die Signale an den Rest der Gesellschaft, denn Unrechtstaten sind nicht so häufig, dass sie den Alltag jedes Einzelnen prägen.

Ein dezentrales Reputationssystem würde der Öffentlichkeit erlauben, direkte und indirekte Beweise zu sehen (geprüfte und ungeprüfte). Die Gesellschaft könnte die Informationen bewerten — allein oder durch freimarktwirtschaftliche Dienste, die auf solche Bewertung spezialisiert sind — und auf Basis qualitativer und quantitativer Signale entscheiden, welche Maßnahmen sie auf das Subjekt anwendet (oder sogar auf den Autor oder die verifizierende Autorität).

Was ist Strafe? Sie ist eine Form der Demütigung des mutmaßlichen Täters durch den Verlust seiner Privilegien — damit sowohl das Opfer als auch die Gesellschaft empfinden, dass schädliche Taten sich nicht auszahlen. Das ist der wesentliche Punkt: Schädliches oder gefährliches Verhalten darf sich nicht auszahlen, und zugleich muss es sowohl den Opfern als auch dem Rest der Gesellschaft/Gemeinschaft ein Gefühl der Genugtuung verschaffen.

Muss eine solche Strafe von einer zentralen Autorität verhängt werden? Was, wenn jeder im Voraus erklären könnte, wie er auf bestimmte Taten reagieren wird? Ich kann offensichtlich keine Strafe an fremdem Eigentum vollstrecken. Aber ich kann erklären, dass ich mein Eigentum einer ausgewählten Menge von Vollzugsautoritäten zur Verfügung stelle, um den Täter zu bestrafen, sollte er meine Domänen betreten. Und ich kann dies öffentlich erklären, damit andere meinen Ansatz bewerten können.

Und hier tritt der Preismechanismus der Verhältnismäßigkeit ein. Erkläre ich harte Strafen für geringfügige Vergehen, bepreist das Netzwerk meinen Extremismus: Andere werden mich als unverhältnismäßig empfinden und meine Verifizierungskosten werden steigen — weniger Menschen werden mit mir handeln wollen, oder nur zu schlechteren Preisen, und weniger Verifizierer werden meine Einträge zu einem angemessenen Preis annehmen. Bin ich hingegen zu nachsichtig, wird mich die Gemeinschaft als Risiko sehen. Dulde ich Betrug, wird die Gemeinschaft wahrscheinlich nachsichtig gegenüber den Tätern von Taten sein, die mich betreffen — um mir eine Kostprobe meiner eigenen Medizin zu geben.

Gerechtigkeit hört auf, ein Luxusgut zu sein. Wenn dir jemand schadet, ist das Festhalten des Unrechts erschwinglich, der Eintrag ist dauerhaft, und die Folgen für den Täter sind real.

Erkennung von Heuchelei

Eine Richtlinie zu erklären genügt nicht — wenn ich erkläre, dass ich eine Regel befolge, mein Verhalten aber davon abweicht, ist die Lücke eine reputationelle Belastung. Das Netzwerk unterscheidet nicht zwischen „hat das Gesetz gebrochen“ und „hat sein eigenes Wort gebrochen“ — beides sind messbare Signale. Heuchelei ist teuer, und ich kenne kein reizenderes rotes Tuch.

EINE FALLE. EIN AUSWEG.

DER INSIDER GEWINNT IMMER DEN AUFTRAG — BIS DAS NETZ DIREKTEN EINKAUF ERLAUBT, OHNE ERLAUBNIS.



Alle sind sich einig: Ein neues staatliches IT-System muss her, aus dem Haushalt, aus Steuern.



Hinter verschlossenen Türen schneiden der Beschaffungsbeamte und der Insider die Ausschreibung auf eine Firma zu. Ein Umschlag wechselt den Besitzer.



Der Beamte zuckt die Schultern. Seine Tasche beut sich von Schmiergeld.



Der Auftrag ist vergeben. Der Insider hat die Lizenz — aber kein Können und keinen Respekt vor der Arbeit.



Der Insider besucht den Nachbarn. Das „freundliche Angebot“ ist der kleinste Krümel.

1. TRADITIONELL



Beschwerde, Schweigen, Fristen, Anwalt. Die Falle steckt in den Regeln selbst.

Wo Regulierung ein Graben ist, ist das Netz eine Brücke.



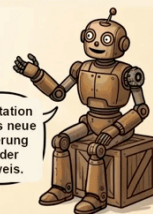
REPUTATIONSNETZ — hier beginnt die neue Welt —

2. REPUTATIONSNETZ



Er liefert zuerst. Die Leute finden die App und nutzen sie. Jeder dankbare Nutzer zahlt ein wenig. Ein anständiges Auskommen. Keine Zentrale zum Bestechen.

Reputation ist das neue Lieferung ist der Beweis.



Zwei Wege. Die Falle steckt in den Regeln. Der Ausweg ist, die Regeln ganz zu umgehen.

* Schreibt der Insider die Regeln, ist die Beschwerde nach diesen Regeln die Falle — sogar die Bußgelder finanzieren die nächste manipulierte Ausschreibung. Das Reputationsnetz ist der Ausweg: Bürger finden das Produkt, zahlen direkt an den Hersteller, und die Gemeinschaft vergibt die einzige Lizenz, die zählt — Vertrauen, verdient durch Leistung.

■ Quantität vs. Qualität — das binäre Paradigma der Schuld durchbrechen

In der zentralisierten Justiz ist Schuld binär: 0 oder 1, schuldig oder nicht schuldig. In einem Reputationsnetzwerk zählt nicht, ob die Schuld bewiesen ist, sondern die Anhäufung von Signalen.

Eine einzelne unbewiesene Diebstahlsbeschuldigung gegen den Angeklagten wird wahrscheinlich nicht viel Aufmerksamkeit erregen — aber sie wird Aufmerksamkeit gegenüber dem Ankläger erregen. Mehrere indirekte Indikatoren aus verschiedenen unabhängigen Quellen jedoch beginnen ins Gewicht zu fallen. Worauf es ankommt, ist nicht nur die Quantität, sondern auch die Qualität: die Unabhängigkeit der Zeugen (verschiedene Menschen, verschiedene Kontexte), die Musterkonsistenz (eine wiederkehrende Art des Verdachts), die zeitliche Korrelation.

Umgekehrt können häufige grundlose Beschuldigungen, die vom selben Aussteller gegen verschiedene Zielsubjekte wiederkehren, als Verleumdung bewertet werden — und die Reputation des Anklägers zahlt den Preis.

WIE BEWEISE SICH HÄUFEN

„eine einzelne Meldung“



eine einzelne Meldung — zu dünn zum Handeln. keine Seite verurteilt.

„ein Muster“



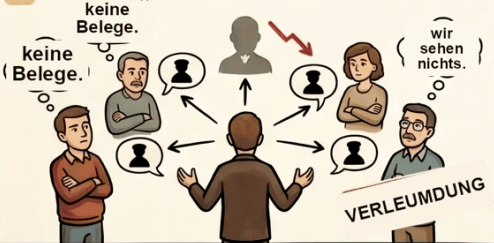
fünf unabhängige Quellen — ein Muster zeigt sich.

„erdrückendes Gewicht“



zwanzig unabhängige Quellen — erdrückendes Gewicht.

A „der Rauschtrick“

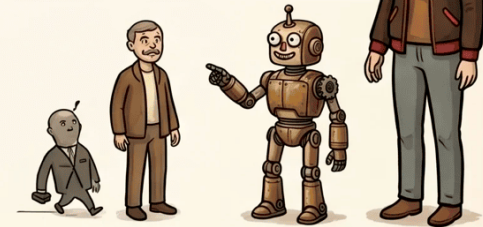


dieselbe Meldung ohne Belege streuen — sieht die Gemeinschaft nichts, ist es Verleumdung, und sie kostet den Ankläger. Unabhängigkeit ist alles. Eine wiederholte Stimme ist Lärm. Viele Stimmen von verschiedenen Orten sind ein Signal.

B „der Groll“



ein Ankläger zeigt auf alle — das Muster ist der Ankläger, nicht der Beschuldigte.



das sieht aus wie die heutige Welt. ist es — nur die Motive sind jetzt ehrlich. keine Revolution. nur bessere Anreize.

Auch die Sühne sollten wir nicht übersehen — eine freiwillige Handlung, bevor die Schuld bewiesen ist, die einen Weg zu einer milderer Strafe eröffnet. Die Strafe setzt ein, wenn der Täter keinen Schritt zur Sühne unternimmt und darauf hofft, den Folgen zu entkommen — so wie sich dieser Ausgang in einem zentralisierten System durch Korruption erkaufen lässt.

■ Arten von Vergehen

Die Arten von Informationen müssen nicht auf strafbare Handlungen beschränkt sein; sie können umfassen: - Beschreibungen von Verbrechen - Vertragsbrüche und Betrug - unmoralisches Verhalten - Störungen der öffentlichen Ordnung, sowohl real als auch virtuell - ...

Jeder neue Eintrag im DID-Netzwerk passt die bewertete Reputation und das Risiko der gegebenen DID an (ob Subjekt, Autor oder verifizierende Autorität). Je mehr Verantwortung ich für das Schicksal anderer trage, desto vorsichtiger werde ich.

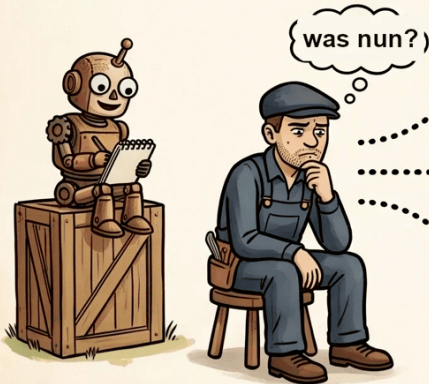
NACH DEM SCHADEN — WAS TUST DU?

abgewiesen. erzwungen. freiwillig. drei Antworten des Dorfes.

was geschah



und jetzt?



die rationale Wahl ist stets die billigste: MACH ES SELBST.

„Ich ignoriere es — überall abgewiesen“



keine Abhilfe — jeder Laden weist ihn ab — Verbannung aus dem Wirtschaftsleben

„Ich mache es gut — aber nur unter den Blicken der Menge“



erzwungene Wiedergutmachung unter den Blicken der Menge — bezahlt, doch das Dorf erhöht seinen Preis — die Lektion muss sitzen.

„Ich komme von selbst — und gestehe es allen“



freiwillige, frühe Wiedergutmachung — öffentlich anerkannt — Reputation erholt sich, mit Vorbehalt

das sieht aus wie die heutige Welt. ist es — nur die Kosten sind jetzt für alle sichtbar. keine Revolution. nur bessere Anreize.

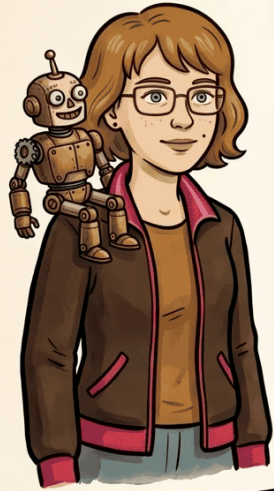
■ Die Durchsetzung von Strafe durch Delegation

Ich muss die Strafe nicht persönlich durchsetzen. Ich kann (ähnlich wie bei einer Versicherung) eine Autorität bezahlen, die Ergebnisse nach vordefinierten Regeln durchsetzt — das Äquivalent von Ermittlungs-, Strafverfolgungs- und Justizdiensten. Setzt die Autorität unverhältnismäßig durch oder setzt sie gar nicht durch, leidet ihre Reputation — und ihre Reputation ist die Grundlage ihrer Fähigkeit, ihren Lebensunterhalt zu verdienen.

Delegation ist ein allgemeines Prinzip im Netzwerk: Jede Tätigkeit einer DID kann an eine andere DID delegiert werden — Verifizierung, Ausstellung von Behauptungen, Reaktion auf Streitigkeiten, Erklärung von Konsens. Delegation ist jederzeit widerruflich. Sie ermöglicht Spezialisierung ohne Verlust der letzten Kontrolle.

WER ERMITTELT, WER SETZT DURCH?

„der Schaden“ → „der Ermittler“ „der Eintrag“ → „der Vollstrecker“ → „Rechenschaft“



mein
Auftragnehmer hat
mich betrogen.



versagt der
Vollstrecker oder
übertreibt er —
Kunden wechseln.



das sieht aus wie
die heutige Welt. ist
es — nur die Motive
sind jetzt ehrlich.
keine Revolution.
nur bessere
Anreize.

„professionelle
Beweissammlung
— Reputation ist ihr
Geschäftsmodell.“

„der Eintrag geht
ins Netz — die
Reputation des
Täters sinkt.“

„handelt nach vorab
vereinbarten Regeln —
wie eine Versicherung.“

„die Reputation des
Vollstreckers ist sein
Brot — versagt er,
verliert er Kunden.“

DELEGATION IST WIDERRUFLICH. Jede DID-Tätigkeit kann an eine andere DID delegiert — und jederzeit zurückgeholt werden.
du vollstreckst die Strafe nicht selbst. du delegierst. und der Delegat ist dir verantwortlich.

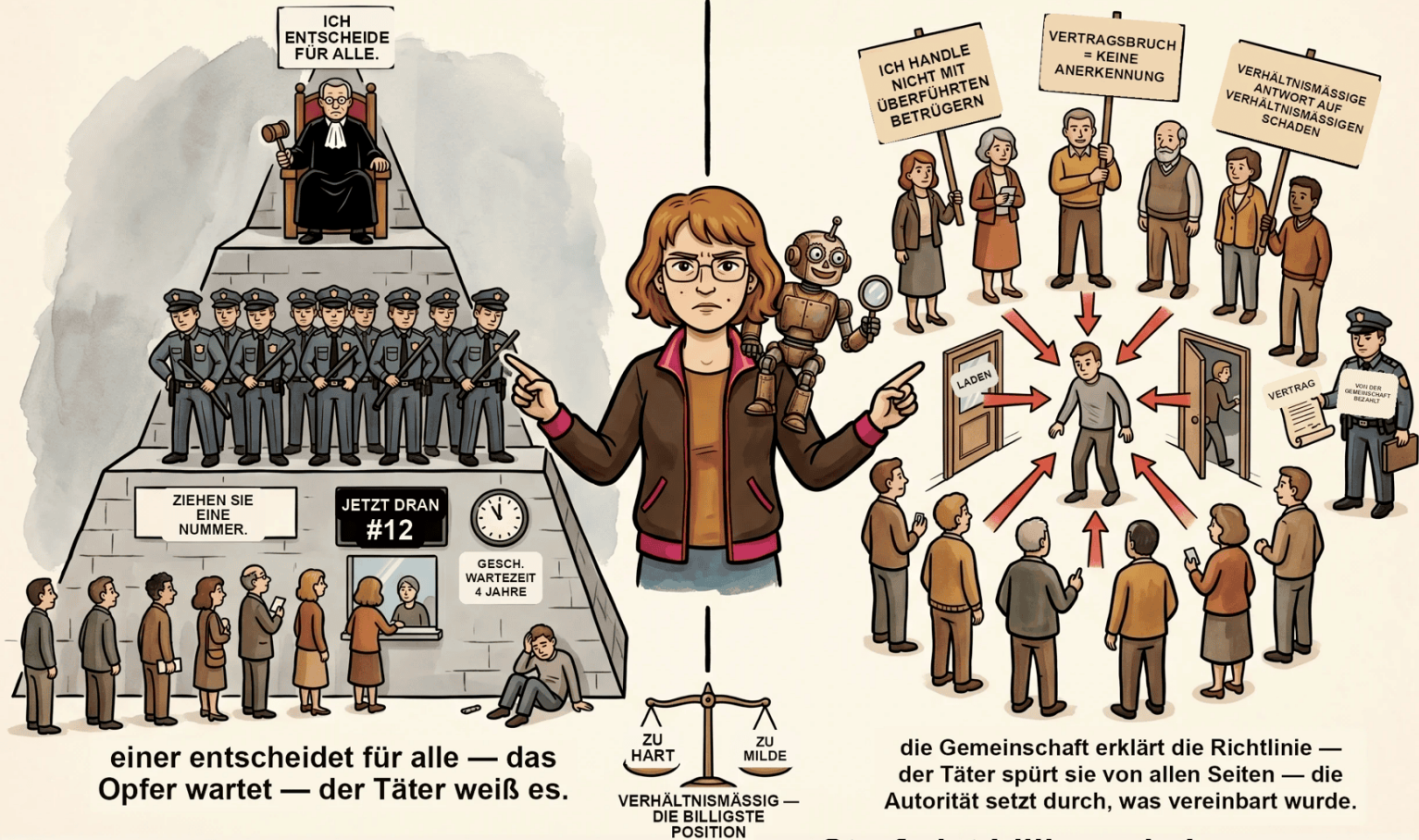
■ Demokratisierung des Risikomanagements

Ein unzensurbares Reputationsnetzwerk würde demokratisieren, was Banken oder Betreiber großer Industrieanlagen bereits als Kerntätigkeit tun — Risikomanagement.

Für einen Banker, der einem Kunden gegenüber sitzt, ist die Risikobewertung im Voraus vorbereitet, sodass er sich innerhalb vordefinierter Grenzen auf die Geschäftsinteraktion konzentrieren kann. Ausgefeilte Wartungsteams sammeln in regelmäßigen Serviceintervallen Risikoindikatoren (Anzeichen struktureller Risse, Prozesse, die die Betriebsinfrastruktur verschlechtern, und so weiter) und können die Lebensdauer von Anlagen vorhersagen sowie, wann und welche Art von Eingriff nötig sein wird.

Die Nutzung von DIDs stelle ich mir ähnlich vor — jemand wird (wahrscheinlich gegen Gebühr) eine menschenlesbare Zusammenfassung der Gegenseite bereitstellen. Die Zusammenfassung wird den Blickwinkel der Risikobewertung widerspiegeln, den der Kunde bestellt hat.

STRAFE OHNE ZENTRALE AUTORITÄT



Wiedergutmachung ist billiger als Strafe.

Strafe ist billiger als Ignoranz.

Der Spur des Geldes folgen

Der Spur des Geldes folgen

Wir haben ein dezentrales Reputationsnetzwerk und die Motivation, es zu nutzen. Schon jetzt kann es seinen Nutzern einen Wettbewerbsvorteil verschaffen — potenzielle Risiken aufklären, ihnen helfen, die Auswahl der Gegenseite und die Verhandlungsstrategie effizienter zu planen, und die Maßnahmen einbeziehen, die diese bekannten Risiken verringern.

Was folgt, ist eine mögliche Methodik⁵ für seine Nutzung — die Eigenschaften des Netzwerks zu nutzen, um einen Migrationspfad vom gegenwärtigen System zu seinem evolutionären Nachfolger zu konstruieren. Sie trägt wahrscheinlich für Mitteleuropa charakteristische Züge, wo diese These entstand. Örtliche Bedingungen werden örtliche Anpassungen erfordern. Was ich überall zu bewahren empfehlen würde, ist der kompromisslose Charakter der Maßnahmen gegenüber dem Staat — ohne den wird das Ziel in endloser Diskussion verwässert und der Wandel wird nie eintreten. Vorsicht — Vertreter und Unterstützer des Staates werden dich mit Unsinn beschäftigen. Fall nicht darauf herein; ihr Lebensunterhalt steht auf dem Spiel.

⁵**Dekonstruktion des Staates** — im tschechischen Kontext wird dies wahrscheinlich ausführlich in einem kommenden gleichnamigen Buch des tschechischen Autors Daniel Steigerwald behandelt (geplant für 2026). Ich persönlich setze große Hoffnungen in die inspirierenden Verfahren, die es enthalten wird.

Der Schwachpunkt des Staates — das Geld

Kehren wir zum Anfang zurück. Wir wollen mehr resultierende Freiheiten, mehr Einfluss auf ihre Gestalt und mehr ihnen angemessene Verantwortung. Die Frage ist einfach: Wo hat der Staat einen verwundbaren Punkt, auf den wir drücken können, ohne zu Gewalt zu greifen?

Die Antwort ist langweilig und gerade dadurch umso stärker. Das Geld.

Im Kern ist der Staat ein Fluss von Geld. Mit Geld bezahlt er seinen Zwangsapparat — das letzte Glied, das seine Regeln durchsetzt. Ohne Geld gibt es kein Gewaltmonopol. Sobald das Geld ins Stocken gerät, beginnt der Staat sich zurückzuziehen — denn ihm bleibt nichts mehr, um jene zu bezahlen, die ihn physisch an Ort und Stelle halten.

Geldflüsse schwanken naturgemäß — saisonal, konjunkturell, nach der Stimmung der Investoren. Der Staat verschleiert das durch Kreditaufnahme an den Finanzmärkten. Gelegentlich ist ein Kredit rational: eine Investition, die sich auszahlt. Häufiger jedoch deckt er überdimensionierte Ausgaben für Agenden, die dem Kernzweck des Staates längst entwachsen sind — Verteidigung, innere Sicherheit, Strafjustiz, Außenpolitik. Sobald bestimmte Schwellen überschritten sind, reagiert die Zentralbank mit Zinssätzen, die an ihre eigene Inflationsschätzung gekoppelt sind.

Und hier kommt die stille Steuer. Inflation ist alles andere als eine bloße buchhalterische Sorge von Makroökonomien. Sie ist eine versteckte Steuer auf die Kaufkraft der Währung, gezahlt von jedem, der ein paar Groschen fürs Alter zurückgelegt hat. Niedrige Inflation wird von der Öffentlichkeit geduldet, weil sie ihre langfristigen Wirkungen nicht begreift — sie erkennt nicht, dass selbst einstellige Werte, über einen langen Zeithorizont aufgezinnt, Ersparnisse so weit erodieren, dass Menschen ihr eigenes Alter nicht mehr sichern können. Und wenn sie es nicht können, werden sie in die Abhängigkeit von staatlichen Leistungen konditioniert. Am Ende hängen sie an diesen Leistungen und sind an den Staat gefesselt.

In turbulenten Zeiten — Krieg, Pandemie, die „notwendige“ Investition — schaltet der Staat einfach die Druckerpresse ein. Die Kaufkraft verantwortungsvoller Sparer und Arbeitender sinkt, während wir ihnen versprechen, dass sie gut belohnt werden. Jemand stiehlt ihnen still ihre Zeit und lobt sie dafür, wie glänzend sie verdienen.

Das untergräbt das Vertrauen in den Staat ernsthaft. Und Vertrauen ist der einzige Klebstoff, der die ganze Maschinerie zusammenhält. Das ist der Hebel, gegen den anzustemmen sich lohnt.

■ Warum das Geld und nicht andere Schwachpunkte?

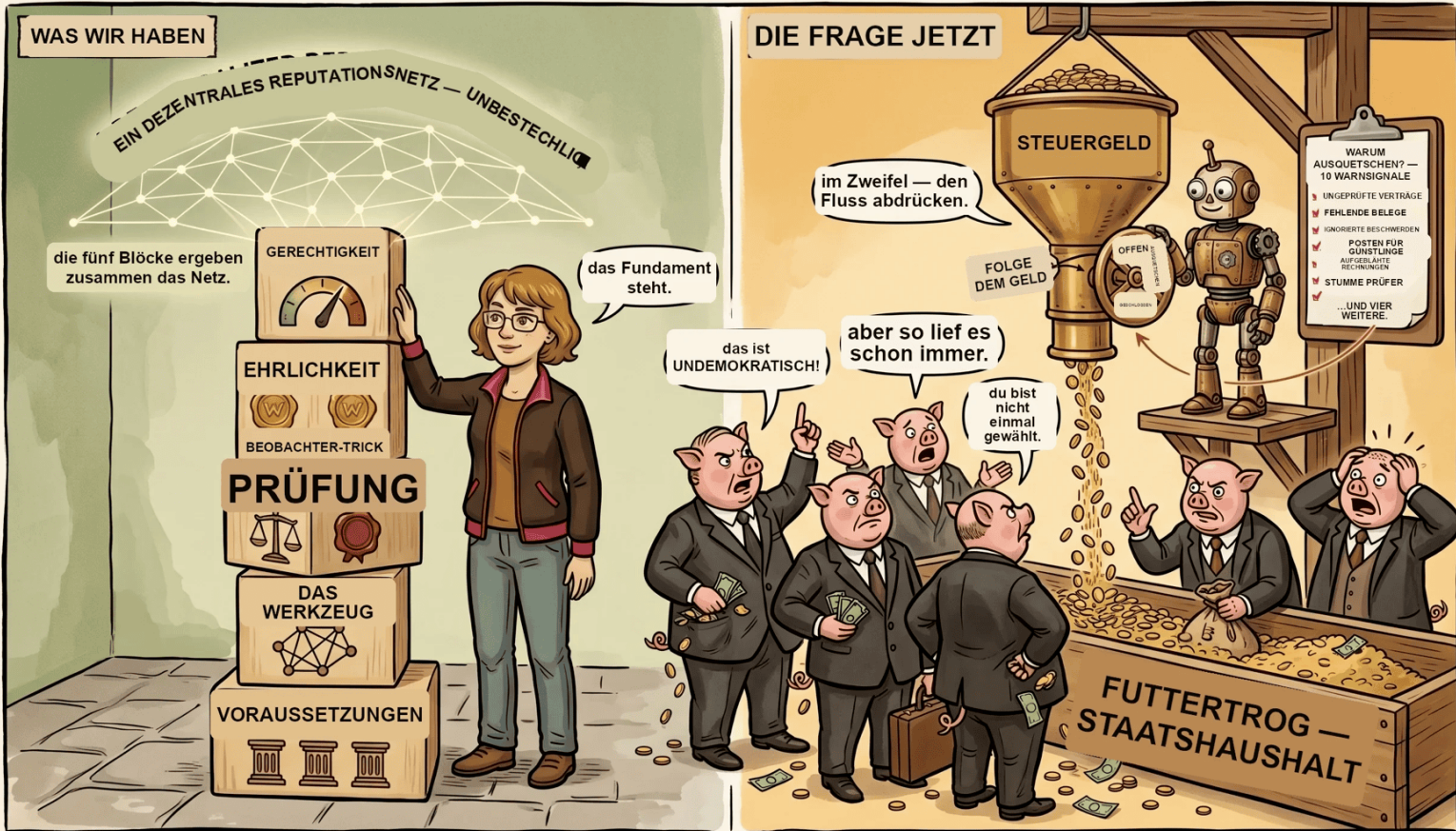
Ein weiterer Schwachpunkt der Zivilisation ist zum Beispiel die Energieverteilung. Doch ihren Fluss zu stören ist kein Hebel — es wäre Aggression, Terrorismus. Freiwillige Nichtteilnahme ist nicht dasselbe wie das absichtliche Schädigen anderer. Das Geld ist darin außergewöhnlich, dass sich Druck freiwillig, transparent und ohne Gewalt ausüben lässt.

Proposed transition to the state's successor

Evolution, nicht Revolution

Plötzlicher Wandel ruft Widerstand hervor, selbst wenn das Endziel attraktiv ist. Er zerreißt Bindungen — soziale, wirtschaftliche, politische — und Menschen verteidigen instinktiv das, was sie bereits kennen, gegen das, was sie noch nicht gesehen haben.

FOLGE DEM GELD — DIE BISHERIGE GESCHICHTE



Wir haben das Netz. Wir wissen, wie es läuft. Und jetzt: im Zweifel den Trichter ausquetschen.
die Macht des Staates ruht auf Geld. folge ihm.

Der richtige Ansatz ist daher schrittweise — evolutionär. Einer, der verhindert, dass das alte System das neue mit einem einzigen Knopfdruck abschaltet — denn in dem Moment, in dem es könnte, würde es das tun.

Leider bedeutet das, zu akzeptieren, dass die Gleichgewichts-Freiwilligkeit nicht in dem Moment erreicht wird, in dem wir das Reputationsnetzwerk ausrollen; sie wird zusammen mit einer allmählichen Adoptionsrate eintreffen. Die Aufnahme mag — und wird wahrscheinlich — langsam sein, vorangezogen vom Wunsch der Einzelnen, über das Reputationsnetzwerk bei ihrer Gemeinschaft Abhilfe zu finden, wenn der konformistische Weg der Rechtssuche versagt (und er wird versagen). Sehen wir uns an, wie dieser Weg aussieht, samt proportionaler Schätzungen.

■ Leere Tröge — spiel nicht nach Regeln, die so gebogen sind, dass du verlierst

Versuche, den Staat von innen zu reformieren, verlassen sich auf die internen Machtmechanismen, in der Hoffnung, dass Beamte Änderungen gegen ihre eigenen Anreize durchsetzen. Das wird nicht geschehen.

Warum das System füttern, statt die Kanäle auszutrocknen, die ihm Leben bringen? Statt das alte System zu verändern und nach seinen Regeln zu spielen, bauen wir eine neue Schicht darüber — eine, die das alte System nach und nach zu einer Teilmenge des neuen macht. Am Anfang füllt diese Teilmenge die Obermenge fast aus. Mit der Zeit ziehen die Akteure hinüber.

Unternehmen wissen das: Wenn ein altes System zu verstrickt ist, um es zu ersetzen, baut man ein paralleles und migriert die Nutzer nach und nach hinein.

Dass der Staat am Ende eine Diskrepanz zwischen dem hat, was er tatsächlich leistet, und dem, was seine Statuten verlangen, und dass er geneigt sein wird, diese Diskrepanz anzurufen, ist rein ein Problem seiner Vertreter und Teilnehmer — es besteht kein Grund, darauf zurückzublicken. Das Einzige, worauf es zu achten lohnt, ist dies: keine gewaltsame Revolution provozieren.

Vier Werkzeuge, die einander stützen

Bis jetzt mag das DID-Reputationsnetzwerk vor allem für Gerechtigkeit und Konsens nützlich erschienen sein. Ich glaube, es könnte sich selbst stabilisieren und Angriffen standhalten — meritokratisch, auf Basis

tatsächlichen Verdienstes statt formaler Titel. Doch Reputation allein wird den Staat nicht zum Nachgeben zwingen. Die Ökonomie wird es und der Druck, der durch sie ausgeübt wird.

Nichts hindert uns daran, DID-Identitäten als Verwalter zusätzlicher Werkzeuge einzusetzen, die hart auf das Geld drücken. Beginne nicht mit voller Freiwilligkeit seitens der Bürger — setze eine Richtung, die der Staat nicht aufhalten kann. Der Übergang ruht auf vier konkreten Werkzeugen, die einander den Rücken stärken. Keines von ihnen genügt für sich allein.

Einfaches Steuersystem — der Köder zum Einstieg

Das erste Werkzeug ist ein einfaches, transparentes Steuersystem, das auf DID-Infrastruktur aufbaut. Ein einziger proportionaler Satz auf alle Einkünfte. Keine Ausnahmen, keine Steuerbefreiungen, keine Unternehmensabzüge, keine Anreize. Jede Zahlung ist prüfbar mit der DID verknüpft, die sie geleistet hat. Der Abgleich ist trivial.

Der Satz würde für einen Teil der Steuerzahler etwas günstiger angesetzt als im alten System — das ist der Köder für den Einstieg. Die Steuerlast würde Jahr für Jahr sinken, das System würde immer attraktiver, und die Migration würde an Tempo gewinnen. Das System ist zugleich Aufzeichnender und Einziehender — kein Mittelsmann, keine Intransparenz.

Elektronisches Ausgabenregister (ESR)

Das zweite Werkzeug besteht darin, die EET (Elektronische Umsatzerfassung) auf den Kopf zu stellen. Statt dass der Staat jeden Beleg eines Selbstständigen verfolgt, verfolgen wir jede einzelne Ausgabe des Staates. Der Staat erhält aus dem einfachen Steuersystem für keine einzelne Zahlung Mittel, es sei denn, jede einzelne — ausnahmslos — durchläuft dieses Sieb.

ESR ist ein Proxy⁶, der jede realisierte Ausgabe des Staates und des öffentlichen Sektors mit einem Eintrag der geplanten Zahlung abgleicht — einschließlich kontextueller Begründung und Identifikation des Empfängers, der ausgebenden Stelle und des Zwecks. Das Ergebnis sind rohe öffentliche Daten, hierarchisierbar. Jeder kann sie nehmen und analysieren. Jeder kann den Steuerzahlern Empfehlungen anbieten, was damit zu tun ist. Was die Rechnungsprüfungsämter in Jahren nicht erreichen konnten, ist plötzlich für jeden einen Klick entfernt.

Du musst nicht auf das neue Steuersystem umsteigen, um teilzunehmen. Es genügt, pro realisierter Zahlung eine vollständig erstattbare Kautionszahlung zu zahlen (sagen wir 1–3 EUR). Der nicht realisierte Rest verfällt als Spamfilter, damit das System nicht von Angriffen überschwemmt wird. Einen Eintrag kann jeder einreichen — ein Angehöriger für einen handlungsunfähigen Großelternteil, ein Nachbar für vernachlässigte öffentliche Dienste, ein Unternehmer für eine unbezahlte Rechnung, ein Beamter per Export aus seinem eigenen System.

Ich erwarte, dass sich politische Parteien auf natürliche Weise in Anbieter von Analysen verwandeln oder dass neue entstehen, um die alten zu ersetzen. Statt aus Steuern gezogener Beiträge werden sie beginnen, Fachwissen anzubieten — indem sie ihren Unterstützern wertebasierte Übersichten über verbündete Autoritäten, deren Dienste und Verifizierungsrichtlinien bereitstellen. Einträge, die aus Faulheit schlampig oder unsinnig sind, werden automatisch zu Kandidaten für Budgetkürzungen. In der ersten Runde wird deine Zahlung immer ausgezahlt, doch die gesammelten Daten dienen als Grundlage für die Beurteilung, ob eine staatliche Ausgabe noch Sinn ergibt. Auftragnehmer und andere auf der Gehaltsliste des Staates haben einen Anreiz, dafür zu sorgen, dass Beamte Ausgaben verantwortungsvoll abgleichen. Andernfalls wird das Geld in der nächsten Runde nicht fließen.

⁶**Proxy** (lat. *procurator*, engl. *deputy/intermediary*) — hier ein Mittler, der im Namen einer anderen Entität handelt. Der ESR-Proxy nimmt von jedem Einträge über geplante Zahlungen entgegen, gleicht sie mit den realisierten Ausgaben des Staates ab und stellt den resultierenden Datensatz der Öffentlichkeit zur Verfügung.

■ Woher das Akronym ESR stammt

Zwischen 2016 und 2022 führte die tschechische Regierung ein System namens Elektronische Umsatzerfassung (EET) gegen ihre eigenen Bürger ein — Selbstständige und Unternehmer. Die Botschaft war einfach: „Wir gehen davon aus, dass jeder von euch den Staat betrügt. Ihr werdet jede einzelne Transaktion erfassen, sie in Echtzeit an unsere Server übermitteln, und wir werden euch beobachten. Wir werden eure Mitbürger finanziell dafür belohnen, euch zu melden, wenn ihr versucht, der EET zu entgehen.“

Die EET war Balkan-Vorbildern nachempfunden. Das erste Land der Welt, das 2013 ein landesweites verpflichtendes Echtzeit-Online-Erfassungssystem für Verkäufe einführte, war Kroatien, unter dem Namen *fiskalizacija*. Die Tschechische Republik übernahm das Modell einige Jahre später und betrieb eines der strengsten Umsatzerfassungsregime in Europa.

Wenn die dunkle Seite nicht zögert, warum sollten wir? ESR ist dieselbe Logik auf den Kopf gestellt: Der Staat weist sich gegenüber den Bürgern aus.

Bürgerliche Steuerzuweisung — das Gewicht der Entscheidung

Das dritte Werkzeug gibt den Steuerzahlern direkten Einfluss darauf, wohin ihr Geld fließt. In der ersten Runde erhielt der Staat sein Geld unabhängig davon, was das ESR offenlegte. In der zweiten Runde tut er es nicht mehr — die Analyse aus der ersten Runde und die daraus folgenden Maßnahmen übernehmen. Ein kleiner Prozentsatz der gezahlten Steuer kann vom Zahler selbst zugewiesen werden — sofern seine

ESR — ELEKTRONISCHE AUSGABENMELDUNG

jede Staatsausgabe erfasst — jeder Eintrag öffentlich — jedes Detail prüfbar.

wer einreicht
jeden Eintrag
darf einreichen:
— der Beamte,
— der zahlte — der
Empfänger, der
Geld erhielt



ÖFFENTLICHES REGISTER DER STAATSAUSGABEN — öffentlicher Eintrag

Kategorie: Rechtsberatung
Auftragnehmer: Kanzlei XY **BEZAHLT**
Betrag: 14M EUR gebunden:
2026-01-14 bezahlt: 2026-01-19
Kontext: externes Gutachten zur
Vergaberechtsreform — drei Entwürfe, ein
Workshop mit dem Ministerium, keine
Anhörung — Endfassung nach der Frist
geliefert.

Kategorie: Straßenplanung **ÖFFEN**
Auftragnehmer: Consultancy **ÖFFEN**
Betrag:
9M EUR gebunden: 2026-02-03 bezahlt: —
Kontext: Machbarkeitsstudie zum
Autobahnausbau D-X — dieselbe Firma schrieb
drei frühere Studien zur Strecke — Ergebnis:
Empfehlung, +18% über der alten Schätzung.

offen für jeden,
der hinsehen will.

Kategorie: Kennzeichenausgabe
Empfänger: Regionalamt Z **BEZAHLT**
Betrag: 45
EUR pro Schild gebunden: 2026-02-19
bezahlt: 2026-02-19
Kontext: übliche Verwaltungsgebühr je
Schild — deckt Material und Bearbeitung —
Gesamtmenge 12 400 Schilder im Quartal.

Kategorie: Klinikausstattung
Auftragnehmer: MedSupply a.s. **BEZAHLT**
Betrag:
8.2M EUR gebunden: 2026-05-08
bezahlt: —
Kontext: MRT-Einbau im Regionalkrankenhaus
— Ausschreibung, drei Bieter — Zuschlag 2%
unter Median, Lieferung in 60 Tagen —
Rechnung 90 Tage überfällig.



Spam-Filter — rückzahlbare Kautions

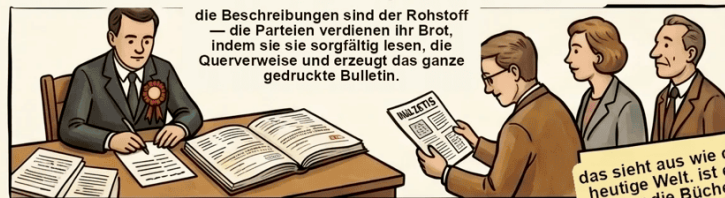


Kautions zurück,
wenn der
Eintrag stimmt.

Jede Krone öffentlichen Geldes — erfasst, öffentlich, prüfbar.

der Wert liegt nicht im Fangen von Betrügern — sondern im Öffnen der Bücher.

Parteien werden zu Analyse-Anbietern



die Beschreibungen sind der Rohstoff
— die Parteien verdienen ihr Brot,
indem sie sie sorgfältig lesen, die
Querverweise und erzeugt das ganze
gedruckte Bulletin.

das sieht aus wie die
heutige Welt. ist es
— nur die Bücher
sind jetzt für alle
offen. keine
Revolution. nur
bessere Anreize.

DID die reputationellen Anforderungen erfüllt (Staatsbürgerschaft, Wohnsitz, von der Gemeinschaft anerkannte Volljährigkeit/Handlungsfähigkeit). Der zuweisbare Prozentsatz wächst Jahr für Jahr. Potenziell exponentiell. Von fünf Prozent heute auf mehrere zehn Prozent innerhalb eines Jahrzehnts.

Die rohen ESR-Daten leiten die Entscheidungen der Steuerzahler auf natürliche Weise. Einträge geringer Qualität fungieren als Warnsignal für empfohlene Kürzungen. Jeder kann Einträge anlegen; Beamte müssen sie abgleichen. Ohne das wird das Steuersystem dem Staat kein Geld schicken — weder in die Staatskasse noch in andere Haushaltskapitel. Der politische Kampf verlagert sich von der Wahlurne zur alltäglichen Zuweisung konkreter Münzen.

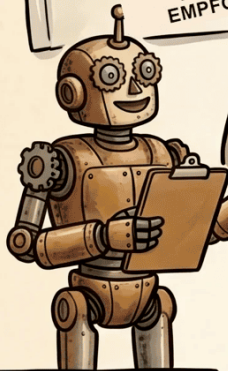
STEUERZUTEILUNG DURCH BÜRGER — DU ENTSCHEIDEST, WOHN DEINE STEUERN GEHEN

studiere die ESR-Einträge. dann bewege die Regler.

ESR-ANALYSEBERICHT
von: einem vertrauten Analysten — von dir gewählt

Verteidigungsministerium:
– 7 Aufträge in 2 Jahren an einen Lieferanten – keine Anhörungen zur Vergabereform – 90 Tage Zahlungsverzug bei 60% der Rechnungen
KÜRZUNG EMPFOHLEN.

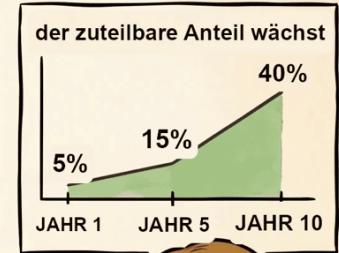
Rep 4.7/5



oder dies delegieren
nicht selbst zuteilen?
delegiere an: – den Analysten deiner Partei – einen vertrauten Nachbarn – wen du willst — jederzeit widerrufbar.



nach dem Bericht
— Abwehr gesenkt.



Zeile anklicken und tiefer gehen — zuteilen in jeder Ebene.



Von 5 % heute auf 40 % in zehn Jahren. Du entscheidest.
die Einträge sind offen. die Analyse ist deine. der Regler auch.

das sieht aus wie die heutige Welt. ist es — nur der Regler liegt jetzt in deiner Hand. keine Revolution. nur bessere Anreize.

Verhandlungsplattform mit dem Staat — der Hebel

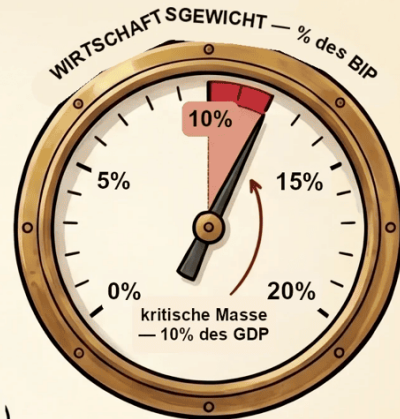
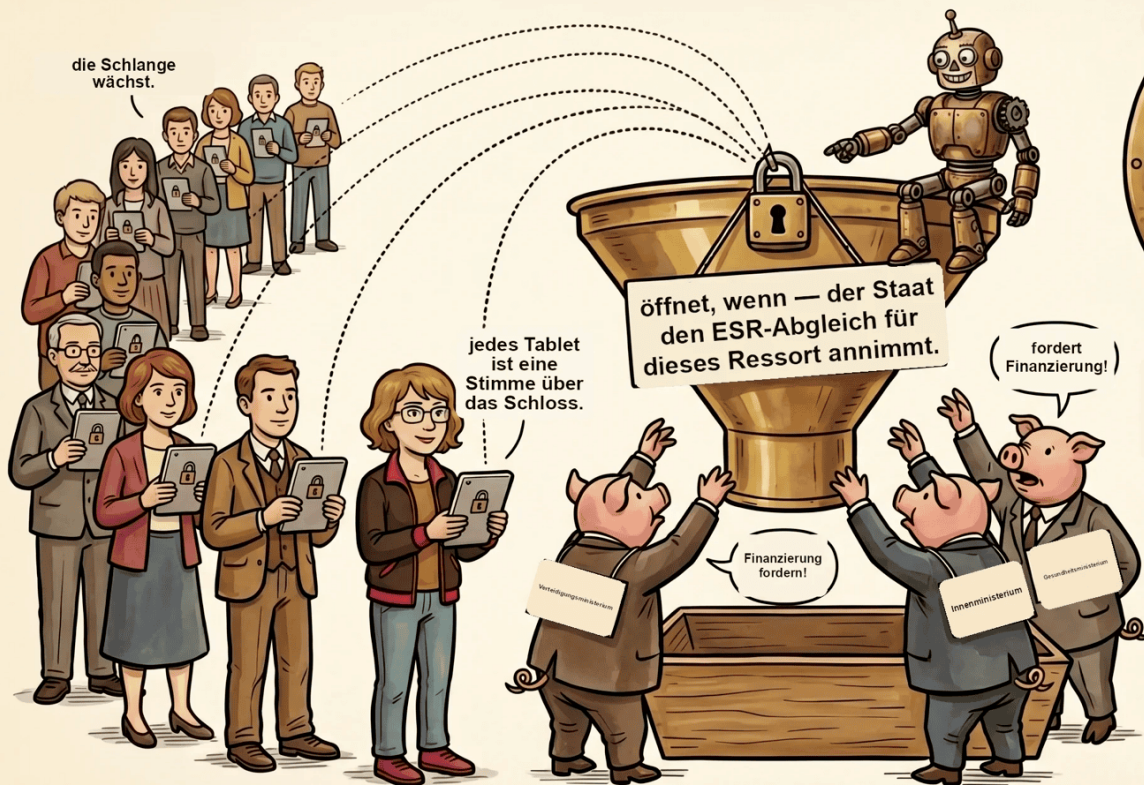
Das vierte Werkzeug ist der Hebel, der alles zusammenbindet und das Netzwerk erst jetzt zu einer echten Bedrohung macht. Der Hauptkonflikt wird darüber gehen, ob der Staat das ESR als verbindlichen Standard akzeptiert — zuerst auf nationaler Ebene — und wie groß die Drohungen seitens der Teilnehmer des Reputationsnetzwerks werden müssen, bevor das geschieht.

Der Hebel ist eine punktgenaue Staatsfinanzierung, bedingt daran, dass Zahlungen gegen das ESR abgeglichen werden. Geld fließt nur in dem Moment, in dem der Staat die Transparenzbedingungen erfüllt hat. Innerhalb des Reputationsnetzwerks bildet sich eine Warteliste von Teilnehmern. Die Aktivierung setzt ein, wenn die Gruppe eine wirtschaftlich bedeutsame Größe erreicht — groß genug, um das BIP-Wachstum zu bedrohen. An diesem Punkt wird ziviler Ungehorsam zu einer glaubwürdigen Drohung statt einer Geste.

Am längsten wird sich der Staat an die problematischen, mit Korruption verbundenen Zahlungen klammern. Unter Druck wird er zuerst dort nachgeben, wo er eine leichte Verteidigung hat und wo es keinen Spielraum gibt, nach Einsparungen zu suchen. Allmählicher und steigender Druck wird ihn zwingen, sich Schritt für Schritt aus jeder Position zurückzuziehen.

VERHANDLUNGSPLATTFORM — DER GESCHLOSSENE TRICHTER

die Bürger halten den Schlüssel. der Staat öffnet, wenn die Bedingungen erfüllt sind.



ein kleiner Anteil am GDP genügt — bei kritischer Masse wird Zurückhalten zur echten Drohung.

nach kritischer Masse —

der Staat öffnet seine Bücher zuerst für einfache, vertretbare Zahlungen.

Kategorien mit Korruptionsbezug bleiben am längsten gesperrt.

jede Freigabe braucht mehr Druck — und wird selbst eingetragen.

das sieht aus wie die heutige Welt. ist es — nur der Schlüssel liegt jetzt in vielen Händen. keine Revolution. nur bessere Anreize.

Geld fließt, wo Transparenz herrscht. Den Schlüssel halten die Bürger.

keine Gewalt. keine Revolution. nur genug Tablets, damit Zurückhalten glaubhaft wird.

Staatsbürgerschaft ohne Personalausweis

Mit dem Übergang zur DID-Infrastruktur verliert der staatlich ausgestellte Personalausweis seinen monopolistischen Zweck. Du brauchst keinen Personalausweis — du hast eine Reihe von DID-Identitäten, und einige von ihnen tragen eine Behauptung, dass du zum Beispiel Tscheche bist, Einwohner einer bestimmten Gemeinde, Absolvent einer bestimmten Schule. Die Behauptung ist überprüfbar, dauerhaft und unabhängig von der staatlichen Verwaltung.

Es öffnet sich eine Frage der technischen Umsetzung: Wer auf dem Markt wird es übernehmen, bestehende Bürger außerhalb staatlicher Kontrolle zu verifizieren, um die Interessierten in eine DID mit der entsprechenden Behauptung zu migrieren? Höchstwahrscheinlich werden freimarktwirtschaftliche Autoritäten entstehen, die auf Identitätsverifizierung spezialisiert sind — Notare, lokale Gemeinschaften, Arbeitgeber. Sie setzen ihre Reputation darauf, dass eine gegebene DID wirklich der Person gehört, die sie für sich beansprucht. Die Staatsbürgerschaft — also die Zugehörigkeit zu einer bestimmten Sicht auf Gemeinschaft — wird von der Notwendigkeit zentraler Aufzeichnung befreit. Durch die Verknüpfung über das Reputationsnetzwerk werden die eingebetteten Daten ein zweites, ein drittes, ein viertes Mal und so weiter verbunden und validiert.

Die Folge ist intuitiv und dennoch in einem zentralisierten System unlösbar. Heute kann die politische Führung — mit Blick auf eine leichtere Wiederwahl — konzentrierte Probleme in das Gebiet der Gemeinschaft importieren: Migranten aus anderen Kulturkreisen aufnehmen, ungeachtet der Aufnahmekapazität und der Bereitschaft der bestehenden Gemeinschaft, und so die ursprünglichen Gemeinschaften durch einen Druck verändern, unter dem sie mit dem Assimilieren von Ankömmlingen aus anderen Kulturkreisen nicht Schritt halten können. In einem DID-Netzwerk kann ein korrupt zugelassener Migrant nicht sicher sein, dass die Gemeinschaft ihn weiterhin als einen der Ihren betrachten wird. Mitglieder der Gemeinschaft müssen objektiv nicht dulden, dass ein Fremder in der Uniform der

VIER WERKZEUGE DES EVOLUTIONÄREN ÜBERGANGS

das System von innen umgebaut — ohne es zu zerbrechen.

EINFACHE STEUER



ein Satz. keine Ausnahmen. gegenprüfbar.

ESR — ELEKTRONISCHE AUSGABENMELDUNG



jede Ausgabe erfasst — jeder Eintrag öffentlich — jedes Detail offen.

STEUERZUTEILUNG DURCH BÜRGER

5% → 15% → 40%
JAHR 1 → JAHR 5 → JAHR 10



studiere die Einträge — dann bewege die Regler.

VERHANDLUNGSPLATTFORM



Geld fließt nur, wenn Transparenzbedingungen erfüllt sind.

heute

Evolution im Gange

in zehn Jahren

95%

wächst

Evolution, nicht Revolution.

vier Werkzeuge, die das System von innen ändern.

das sieht aus wie heute, das ist es — nur die Werkzeuge sind jetzt beim Bürger. keine Revolution. nur bessere Anreize.

Gemeinschaft an ihre Tür kommt und ihnen mit der Legalität von Maßnahmen droht, die er im Haus durchzuführen gedenkt (Beschlagnahme des Telefons eines Kindes wegen eines Social-Media-Posts). Mit dezentraler Reputation muss sich die Mehrheit der Gesellschaft damit nicht abfinden — denn über die Zugehörigkeit zu einer Gemeinschaft entscheidet kein Beamter, sondern die Gemeinschaft selbst, durch ihre Reputationssignale.

STAATSBÜRGERSCHAFT OHNE AUSWEIS

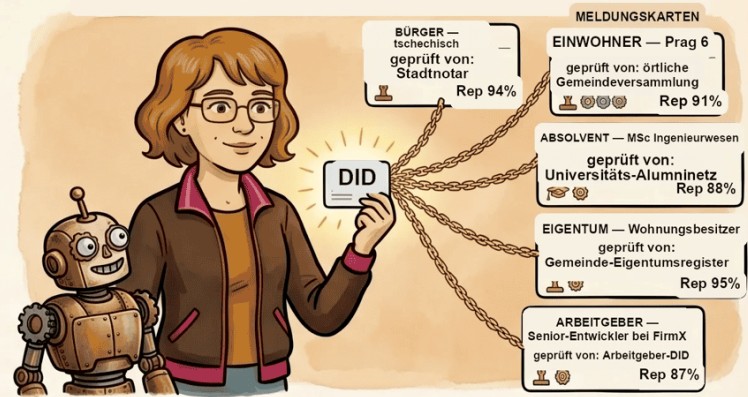
von staatlicher Erlaubnis zur Anerkennung der Gemeinschaft.

„der alte Weg“ des staatlich ausgestellten Ausweismodells



Identität = staatliche Erlaubnis — widerrufbar — Gemeinschaft hat kein Wort.

„der neue Weg“ des DID-Modells mit Meldungskarten



keine Autorität beherrscht alle Meldungen — jede ist unabhängig — jeder Prüfer setzt seine Reputation ein.

„wer gehört dazu?“



die Gemeinschaft entscheidet — über Reputationssignale — verteilt, keine einzelne Stimme.

das sieht aus wie die heutige Welt. Ist es — nur die Prüfer sind jetzt viele. keine Revolution. nur bessere Anreize.

Deine Bürgerschaft ist keine staatliche Erlaubnis. Sie ist die Anerkennung deiner Gemeinschaft.
der Staatsstempel weicht einer Kette unabhängiger Prüfer — jeder mit eigenem Einsatz.

Das Gewicht einer Wahlstimme in Angelegenheiten im Zuständigkeitsbereich des Staates könnte in Zukunft strikt mit Einträgen über Beiträge zum einfachen Steuersystem korreliert werden. Kombiniert mit passenden DID-Behauptungen (zum Beispiel „diese Person ist tschechischer Staatsbürger“) können dann ausländische Staatsangehörige von Wahlen ausgeschlossen werden — das Melderegister zieht einfach hierher um.

Überlappung und Umkehrbarkeit

Ich behaupte nicht, dass dies der einzige Weg ist oder auch nur der beste. Aber er erscheint umfassend — er deckt die wichtigsten Hebel ab und bewahrt die Möglichkeit, zurückzutreten. Zu Beginn überlappt sich das neue System mit dem alten und ändert nur die Anreize. Mit der Zeit schrumpft das alte System, bis es sich — aber nicht muss — auflösen mag. Der Vorteil ist die Schrittweise und die Umkehrbarkeit: Sollte sich ein Fehler im Design zeigen, ist es nicht das Ende, sondern nur eine Korrektur.

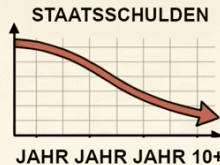
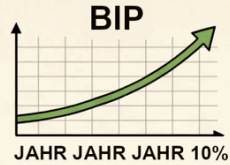
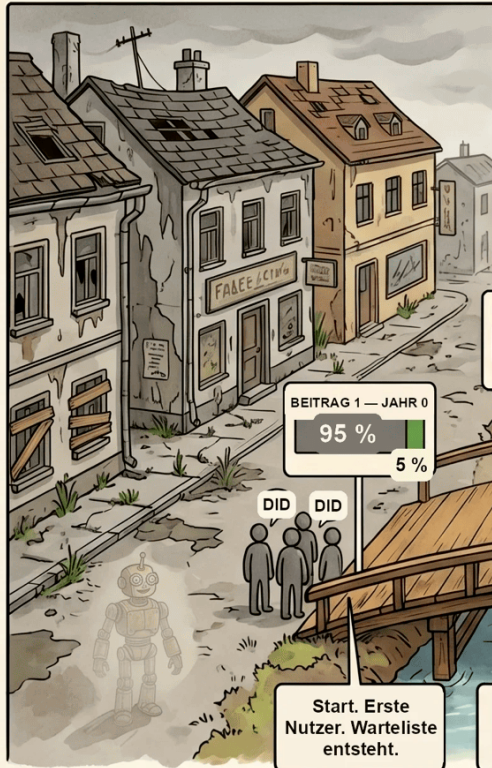
■ Frieden und Krieg

Manche Teile des Staates haben womöglich keine vollständig marktbasierte Alternative — etwa das Militär. Die vorübergehende Delegation außerordentlicher Befugnisse in Krisen (wie die alten Griechen Diktatoren ernannten) könnte weiter bestehen. Die Verantwortung ruht jedoch auf der dezentralen Gesellschaft, nicht auf dem Anführer. Anders als bei zentralisierter Steuerung wird es leichter sein, delegierte Befugnisse zurückzufordern, sobald die Gefahr vorüber ist — oder früher, wenn nötig. Eine freie Gesellschaft wird auch im Waffengang gegen autoritäre Regime nicht im Nachteil sein.

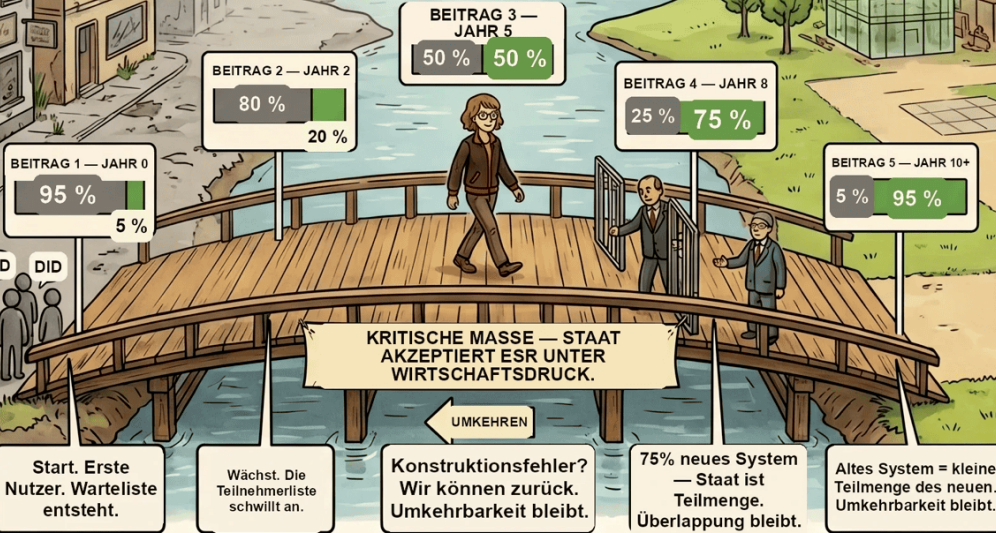
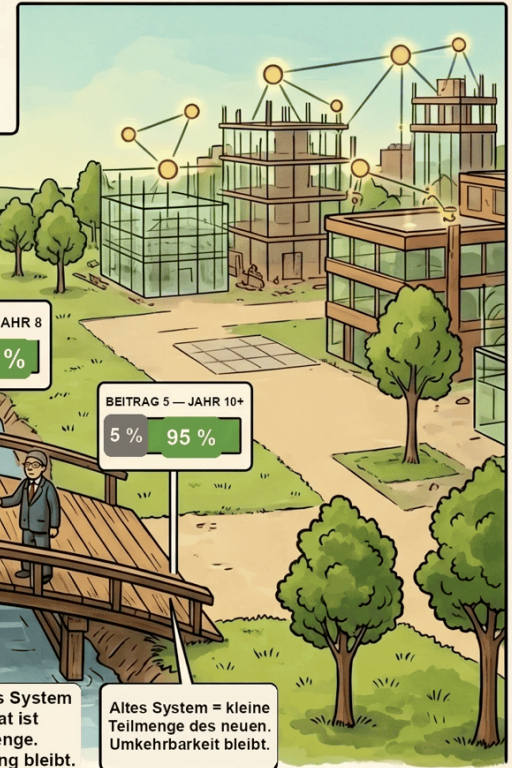
■ Kriegsverbrecher

Mit punktgenauer Staatsfinanzierung und transparenten Ausgaben wird es schwierig, Ressourcen für Angriffskriege anzuhäufen. Ein Steuerzahler, der einen solchen Krieg weiter finanziert, wird zu einem legitimen Ziel und kann sich nicht auf den Zivilstatus nach den Genfer Konventionen berufen. Unter der neuen Ordnung gilt stillschweigende Zustimmung als Teilnahme.

LINKES UFER — ‚DAS ALTE SYSTEM‘



RECHTES UFER — ‚DAS NEUE SYSTEM‘



ALTES SYSTEM

> Schrittweiser Übergang. Umkehrbar im Fehlerfall. Eine Richtung, die niemand stoppt.

Schluss

Der Weg existiert

Der Staat ist, wie er ist, aufgrund der zur Zeit seiner Entstehung verfügbaren Technologien, verbunden mit der menschlichen Natur. Alles auf Freiwilligkeit zu bauen und dabei die durchschnittliche menschliche Natur zu leugnen, ist naiv. Er wird sich weder der Korruption entledigen noch seiner Tendenz, zum Totalitarismus abzudriften. Der Nachfolger des Staates muss auch mit den Eigenschaften funktionieren, die wir derzeit für negativ halten und entweder ächten oder bestrafen.

Dieses Buch beschrieb ein Problem — ein System (den Staat), in dem die Menschen, die die Regeln schreiben, nie mit deren Folgen leben. Es beschrieb die Bedingungen, die gelten müssen, damit dieses System aufhört zu funktionieren. Es beschrieb ein Werkzeug, das diese Bedingungen erfüllt. Und es schlug eine Übergangsmethodik vor — konkrete Schritte, wie dieses Werkzeug zu nutzen ist, als ein mögliches Beispiel.

Im ersten Kapitel nannte ich fünf Pfeiler: Freiwilligkeit, Organisation, Resilienz, Konsens und Unbestechlichkeit. Wir haben sie alle erfüllt.

- **Freiwilligkeit** — niemand zwingt dich ins Netzwerk, aber du kannst deine Handlungen auch nicht daraus löschen.
- **Organisation** — die Gemeinschaft wächst aus dem, wen du kennst, nicht aus dem, wem du von oben zugeteilt wurdest.
- **Resilienz** — nicht einmal ein Staat, der bereit ist, für die Überwachung jedes Pakets zu zahlen, kann es abschalten.

- **Konsens** — er entsteht aus dem Preisschild an der Heuchelei, nicht aus Stimmen oder Unterschriften.
- **Unbestechlichkeit** — fünf kleine Regeln weben Korruption in Kosten ein: das Gleichgewicht von Freiwilligkeit und Verantwortung, das Recht eines jeden zu sprechen, Einstiegspunkte, die sich niemand aussuchen darf, öffentliche Versprechen mit einem Preis für Heuchelei und der Schatten eines Beobachters hinter jeder Transaktion.

Kein einzelner Pfeiler kann den Staat für sich allein ersetzen. Zusammen bilden sie einen Widerstand gegen Korruption, den der Staat mit all seinem Apparat nicht bilden kann.

Wir sind an einem Punkt, an dem sich das Ganze mit den heutigen Technologien bauen lässt (Kryptografie, dezentrale Identität, gut bekannte psychologische Muster, um die Anreize richtig zu setzen, ...). Nur eines fehlt: eine kritische Masse von Menschen, die den Mut finden, es zu unterstützen, und beschließen, anzufangen.

Nicht durch Revolution.

Diese Ideen nahmen zwischen Juni 2025 und Mai 2026 Gestalt an. Als ich mich zum Schreiben hinsetzte, hatte ich das Gerüst weitgehend im Kopf ausgearbeitet — genau deshalb las ich [Farewell To Westphalia](#) mit solcher Neugier, als es erschien. Ich wollte sehen, wo sich ihr Bild mit meinem überlappen und wo es davon abweichen würde. Ein zweiter Anstoß kam von Dan Steigerwald, der im Mai 2026 noch aus einem anderen Blickwinkel an seinem eigenen Buch *Dekonstruktion des Staates* arbeitet; sein Projekt drängte mich, meine eigene Vision in voller Breite niederzuschreiben — damit die Welt sie neben den anderen auf dem Tisch hat.

Ich bitte dich nicht, irgendetwas davon zu glauben. Ich bitte dich, darüber nachzudenken. Und ich lasse dich mit einer Frage zurück:

Was würdest du ändern?

Pavel Kudrna 23. Mai 2026, Prag, Tschechien

Danksagung

Inspiration

Ich danke den Autoren von [Farewell to Westphalia](#) (Jarrad Hope, Peter Ludlow) für den intellektuellen Rahmen, der mir half, meine eigenen Ideen in den weiteren Kontext der Dekonstruktion des westfälischen Staatsmodells einzuordnen.

Review und Feedback

Werkzeuge

Bei der Vorbereitung des Textes, der Strukturierung von Ideen und dem Iterieren an Formulierungen habe ich Unterstützung durch KI-Werkzeuge genutzt. Alle Ideen, Argumente und Schlussfolgerungen sind meine eigenen — die KI diente als Werkzeug zur Verfeinerung, nicht als inhaltlicher Mitautor.

Die Infografiken wurden in Zusammenarbeit mit generativen Werkzeugen auf Basis der Vorgaben des Autors gestaltet.

HOL DIR DEINE ZEIT ZURÜCK

die Bürger jagen die Parasiten aus dem öffentlichen Leben.



Verteidige die Zeit, die sie dir stehlen.

was durch Betrug genommen wurde, wird von Hand zurückgeholt.

Unterstütze das Projekt

Personix wird von Lesern wie dir finanziert.



Bitcoin on-chain

bc1q7cctdz6r026dgy06ul94eygg49ujtxnrq5czaj



Bitcoin Lightning

LNURL1DP68GURN8GHJ7AMPD3KX2AR0VEEKZ
AR0WD5XJTNRDAKJ7TNHV4KXCCTTDEHHWM30
D3H82UNVWQHXMNP0FA8JMPVD5XJMN9XUE
RX55QRQK

■ Wohin dieses Geld geht — und wohin nicht

Die QR-Codes sind die **persönlichen Kanäle des Autors** — Beiträge gehen direkt an Pavel Kudrna und finanzieren weiteres Schreiben, das soziale Experiment / die Simulation und die Öffentlichkeitsarbeit.

Die *einzigsten* legitimen Spendenkanäle für dieses Projekt sind:

- **Vom Autor autorisierte Ausgaben dieses Buches** — QR-Codes in vom Autor autorisierten Exemplaren.
- **personix.org** oder der von dort verlinkte Tor-Onion-Spiegel — wo die *Personix Foundation* für die dort beschriebenen Aktivitäten sammelt. Die Mittel der Foundation werden von den persönlichen Mitteln des Autors getrennt gehalten.

Alles, was anderswo beworben wird — ausgetauschte Adressen in Nachdrucken, nachgemachte Domains, soziale Medien, die „für Personix sammeln“, Spendenaktionen, die an keine der beiden oben genannten gebunden sind — **ist höchstwahrscheinlich Betrug**. Wir meiden den Kryptowährungsmarkt und seine Teilnehmer bewusst.

Glossar

Glossar

Begriff	Deutsch	Bedeutung
Authority	Autorität	Eine vertrauenswürdige Entität (Person, Organisation), die Informationen verifiziert und ihre Reputation darauf setzt. Kann spezialisiert sein (ermittelnd, juristisch, technisch).
Claim	Behauptung	Allgemein: jede überprüfbare Aussage. Hier: ein ins Reputationsnetzwerk veröffentlichter Eintrag — eine Behauptung über ein Ereignis, eine Eigenschaft oder eine Beziehung, die kryptografisch signiert und verifiziert ist. Z. B. „Ich bin Einwohner der Gemeinde X“ oder „diese Person hat einen Vertrag gebrochen.“

Begriff	Deutsch	Bedeutung
Compartmentalization	Abschottung	Allgemein: das Trennen von Informationen in isolierte Einheiten, sodass die Preisgabe einer Einheit die anderen nicht kompromittiert. Ein aus Geheimdiensten bekanntes Prinzip. Hier: parallele DID-Identitäten in Diktaturen — die Kompromittierung einer gibt die anderen nicht preis.
Consistent Hash Ring	Konsistenter Hash-Ring	Ein algorithmischer Mechanismus zur Auswahl von Verifizierern — eine Position auf dem Ring wird durch den Hash des DID-Dokuments innerhalb des sozialen Graphen bestimmt. Sichert eine nichtdeterministische und dennoch überprüfbare Auswahl.
DID	DID (Dezentrale Identität)	Eine digitale Identität, die du selbst erstellst und kontrollierst, ohne zentrale Autorität. Kryptografisch mit deinem privaten Schlüssel signiert — niemand kann sie widerrufen oder fälschen.

Begriff	Deutsch	Bedeutung
DID Document	DID-Dokument	Eine öffentlich verfügbare Datendatei, die deine DID-Identität beschreibt — enthält öffentliche Schlüssel, Netzwerkadressen und Metadaten. Dient dazu, deine Identität im Netzwerk zu verifizieren.
Due Diligence	Due Diligence	Allgemein: die eingehende Prüfung einer Gegenseite vor dem Eingehen einer geschäftlichen oder rechtlichen Beziehung — die Prüfung ihrer Historie, Finanzen, Reputation und Risiken. Hier: im Reputationsnetzwerk geschieht sie schneller und automatischer dank der Verfügbarkeit verifizierter Einträge.
Economic Neutrality Principle	Prinzip der ökonomischen Neutralität	Ehrliches Verhalten im Netzwerk liegt ökonomisch nahe null — die Veröffentlichungskosten kehren als Verifizierungsbelohnungen zurück. Unehrliches Verhalten ist ein Nettoverlust.

Begriff	Deutsch	Bedeutung
Emergent	Emergent	Spontan aus den Interaktionen einfacherer Teile entstehend, ohne dass es jemand entwirft oder lenkt. Ein Vogelschwarm fliegt ohne Plan in Formation — die Formation entsteht aus einfachen Regeln, denen jeder Einzelne folgt.
Emergent Social Contract	Emergenter Gesellschaftsvertrag	Verhaltensregeln, die nicht von oben (Gesetz), sondern von unten entstehen — aus wiederholten Interaktionen und Konsens innerhalb einer Gemeinschaft.
ESR	Elektronisches Ausgabenregister	Ein vorgeschlagenes System zur transparenten Verfolgung öffentlicher Ausgaben — jede realisierte Staatsausgabe wird mit einer geplanten Zahlung abgeglichen. Von der tschechischen EET inspiriert, aber gegen den Staat gewendet.

Begriff	Deutsch	Bedeutung
Hash	Hash (Fingerabdruck)	Allgemein: eine mathematische Einwegfunktion, die aus einer beliebigen Eingabe einen eindeutigen „Fingerabdruck“ fester Länge erzeugt — wie ein Fingerabdruck des Dokuments. Dieselbe Eingabe erzeugt stets dieselbe Ausgabe, doch die Eingabe lässt sich nicht aus der Ausgabe ableiten. Hier: genutzt, um eine Position auf dem Hash-Ring zu bestimmen und die Integrität des Dokuments zu überprüfen.
Just-in-Time Funding	Just-in-time-Finanzierung	Staatsfinanzierung unter der Bedingung von Transparenz — Geld fließt nur, wenn der Staat das ESR akzeptiert und seine Ausgaben abgleicht. Ein Hebel, um Kooperation zu erzwingen.

Begriff	Deutsch	Bedeutung
Meritocracy	Meritokratie	Allgemein: ein System, in dem der Status durch tatsächlichen Verdienst und erwiesene Fähigkeit bestimmt wird, nicht durch formale Titel, Beziehungen oder ererbte Privilegien. Hier: das Reputationsnetzwerk begünstigt auf natürliche Weise jene, die nachweislich zur Gemeinschaft beitragen — ihre Stimme wiegt mehr aufgrund der Erfolgsbilanz, nicht aufgrund eines Amtes.
Onion Gateway	Onion Gateway	Die Netzwerkadresse einer DID-Identität im Onion-Netzwerk. Getrennt vom DID-Dokument — sie lässt sich ändern, ohne die Identität zu verlieren (ähnlich dem Ändern der IP-Adresse hinter einer Domain).

Begriff	Deutsch	Bedeutung
Onion Routing	Onion Routing (Tor)	Ein Kommunikationsprotokoll, das die Unzensurierbarkeit des Netzwerks sichert. Nachrichten werden in Schichten verschlüsselt — jeder Knoten schält eine Schicht ab, kennt aber nicht den vollständigen Pfad.
Oracle Problem	Orakel-Problem	Allgemein: wie man sicherstellt, dass Daten, die in ein digitales System eintreten, dem entsprechen, was tatsächlich in der physischen Welt geschehen ist. Der Begriff stammt aus dem Blockchain-Bereich. Hier: gelöst über Autoritäten, die ihre Reputation als Garantie dafür einsetzen, dass ein digitaler Eintrag der physischen Realität entspricht.

Begriff	Deutsch	Bedeutung
Phenomenological	Phänomenologisch	Allgemein: ein Ansatz, der Phänomene so untersucht, wie sie sich in der unmittelbaren Erfahrung manifestieren, indem beobachtet wird, was aus ihnen folgt, ohne vorgegebene Theorien. Hier: Freiheit, der Gesellschaftsvertrag und Verhaltensnormen sind beobachtete Phänomene — Folgen Tausender Mikrointeraktionen zwischen Menschen, keine von oben definierten Prinzipien.
Policy	Policy (Richtlinie)	Allgemein: ein Satz von Regeln oder Prinzipien, die das Verhalten in einem gegebenen Kontext bestimmen. Hier: Jeder Teilnehmer im DID-Netzwerk erklärt seine Policy — wie er auf konkretes Verhalten anderer reagiert, welche Regeln er befolgt und welche Strafen er für verhältnismäßig hält. Die Gesamtheit der Richtlinien bildet den emergenten Gesellschaftsvertrag.

Begriff	Deutsch	Bedeutung
Proxy	Proxy	Allgemein: ein Stellvertreter oder Mittler — ein System oder eine Entität, die im Namen einer anderen handelt. Hier in zwei Kontexten verwendet: (1) ESR als Proxy, der öffentliche Ausgaben mit geplanten Zahlungen abgleicht; (2) Beobachter als Proxy zwischen Aussteller und Verifizierer im Beobachter-Trick.
Publisher	Aussteller	Ein Netzwerkteilnehmer, der einen Eintrag erstellt und veröffentlicht (eine Behauptung über ein Unrecht, eine Wiedergutmachung usw.). Trägt die Kosten der Veröffentlichung.
Reputation-Based Social Network (RSN)	Reputationsnetzwerk	Ein dezentrales soziales Netzwerk, in dem Teilnehmer Feedback über Verhalten in der realen Welt austauschen. Einträge sind teuer zu erstellen, günstig zu lesen.

Begriff	Deutsch	Bedeutung
Reputation Signal	Reputationssignal	Ein einzelner Eintrag im Netzwerk — positiv (Wiedergutmachung eines Schadens, Erfüllung einer Verpflichtung) oder negativ (Unrecht, Vertragsbruch). Kumulativ bilden Signale ein Reputationsprofil.
Social Graph	Sozialer Graph	Das Netzwerk deiner Kontakte und der Kontakte deiner Kontakte. Der Algorithmus sucht Verifizierer in einer konfigurierbaren Tiefe (zum Beispiel 3 Ebenen). Keine globale Blockchain — das Netzwerk bildet auf natürliche Weise Gemeinschaften mit Überlappungen.
Tax Allocation	Steuerzuweisung	Ein Mechanismus, durch den der Steuerzahler entscheidet, wohin ein Teil seiner Steuern geht. Der zuweisbare Prozentsatz wächst Jahr für Jahr.

Begriff	Deutsch	Bedeutung
Track Record	Track Record (Erfolgsbilanz)	Allgemein: die Historie vergangener Ergebnisse, Erfolge und Misserfolge einer Person oder Organisation. Hier: die Summe aller vergangenen Interaktionen einer gegebenen DID-Identität im Netzwerk — verifizierte Behauptungen, angenommene und abgelehnte Einträge —, aus der sich ihre Reputation ableitet.
Verifier	Verifizierer	Ein algorithmisch zur Verifizierung und Veröffentlichung eines Eintrags ausgewählter Teilnehmer. Setzt seinen guten Namen auf die Wahrhaftigkeit der Information.

Produktionshinweise

Vom Autor vorbehalten (nicht von der CC-BY-SA-Lizenz abgedeckt): der Name und das Wortzeichen Personix, das Buchcover und die Unterstützungskanäle (QR-Codes, Adressen, Kontakt-E-Mail). Abgeleitete Ausgaben müssen diese Elemente entfernen oder ersetzen; sie dürfen nur verwendet werden, um auf dieses Originalwerk zu verweisen.

Quelldateien. Der vollständige Quellcode — Markdown-Text, Infografiken, Build-Skripte — ist zusammen mit diesem PDF verfügbar.

Werkzeuge. Bei der Vorbereitung des Textes und dem Iterieren an Formulierungen nutzte der Autor Unterstützung durch KI-Werkzeuge; die Infografiken wurden in Zusammenarbeit mit generativen Werkzeugen auf Basis der Vorgaben des Autors gestaltet. Alle Ideen, Argumente und Schlussfolgerungen sind die eigenen des Autors.

PERSONIX

Kompromissloser Wandel

Ein unzensurbares und unbestechliches dezentrales Reputationsnetzwerk

Der Staat funktionierte, als die Kommunikation langsam war, Entscheidungen lokal fielen und die Autorität in derselben Stadt lebte, die sie regierte. Die heutigen Netzwerke kehren alle drei Annahmen um — und die auf ihnen errichteten Institutionen passen nicht mehr zu der Welt, die sie regieren. Dieses Buch beschreibt ein Werkzeug, das passt: ein dezentrales Reputationsnetzwerk, in dem die Identität dir gehört, die Wahrheit öffentlich prüfbar ist und Bestechung reputationeller Selbstmord ist.

Kein Manifest. Keine Prognose. Ein funktionierender Bauplan dafür, wie sich der Nachfolger des Staates errichten lässt — freiwillig, eine Erklärung nach der anderen.

Pavel Kudrna • Prag, 2026

personix.org

Lizenziert unter Creative Commons Attribution-ShareAlike 4.0 International (CC BY-SA 4.0).