Decentralized Reputation Network: A Framework for Natural Societal Organization

Pavel Kudrna
Prague, Czechia
Draft v1 — March 2026

Abstract

Das Gerechtigkeitsempfinden—die Überzeugung, dass Unrecht wiedergutgemacht und Verdienst belohnt wird—ist die stärkste zusammenhaltende Kraft der Gesellschaft. Wenn zentralisierte Regierungsinstitutionen dieses Empfinden nicht liefern können, weil die Kosten der Durchsetzung eines Rechts den Wert des Rechts selbst übersteigen, erodiert der gesellschaftliche Zusammenhalt. Die gegenwärtigen institutionellen Strukturen versagen bei der Beilegung einer bedeutenden Klasse von Streitigkeiten systematisch auf dieselbe Weise, wie die Zentralplanung bei der Ressourcenallokation versagt: durch Informationsasymmetrie, fehlende Rückkopplungsschleifen und die Loslösung der Entscheidungsträger von den Folgen ihrer Entscheidungen. Diese Arbeit stellt ein Reputationsnetzwerk (Reputation Social Network, RSN) vor: eine dezentrale, unbestechliche, zensurresistente Kommunikationsschicht, die auf dezentralen Identifikatoren (Decentralized Identifiers, DIDs) aufbaut und pseudonymen Teilnehmern ermöglicht, Reputationsinformationen über reales Verhalten zu veröffentlichen, zu verifizieren und zu konsumieren. Der Kernmechanismus beruht auf drei Gestaltungsprinzipien: (1) einer asymmetrischen Kostenstruktur, bei der das Lesen von Reputationsdaten kostengünstig ist, das Schreiben jedoch nachweisbaren Aufwand erfordert; (2) einem nichtdeterministischen Protokoll zur Auswahl von Verifizierern auf Basis von konsistentem Hashing, das radikale Behauptungen durch eskalierende Iterationskosten bepreist; und (3) einem marktgetriebenen Modell der Reputationsautorität, bei dem private Verifizierer ihre angesammelte Reputation auf die Richtigkeit der von ihnen bestätigten Behauptungen setzen. Die daraus resultierende Architektur erzeugt eine emergente Meritokratie ohne zentrale Koordination und ermöglicht einen schrittweisen, umkehrbaren Migrationspfad von bestehenden staatlich verwalteten Systemen.

1 Einleitung

1.1 Das Problem des zentralisierten Vertrauens

Moderne Regierungsführung beruht auf einer grundlegenden Annahme: dass zentralisierte Institutionen Vertrauen zwischen Fremden in großem Maßstab vermitteln können. Gerichte entscheiden Streitigkeiten. Register beglaubigen Eigentum. Regulierungsbehörden setzen Standards durch. Diese Institutionen wurden in einer Zeit entworfen, in der Informationen knapp waren, Kommunikation langsam war und die Delegation von Autorität an eine zentrale Stelle der einzig machbare Koordinationsmechanismus war. Zentralisierte Regierungsführung versagt jedoch aus denselben strukturellen Gründen wie die Zentralplanung: Informationsasymmetrie, fehlende Rückkopplungsschleifen und die Loslösung der Entscheidungsträger von den Folgen ihrer Entscheidungen.

Die Annahme versagt beispielsweise dann, wenn die Kosten der institutionellen Vermittlung den Wert der Streitigkeit übersteigen. Man stelle sich einen Mieter vor, der entdeckt, dass seiner Mietwohnung ein gesetzlich vorgeschriebenes Zertifikat über die elektrische Sicherheit fehlt—ein Zustand, der eine unmittelbare Lebensgefahr darstellt. Das gesetzliche Recht des Mieters, vom Vertrag zurückzutreten, ist eindeutig. Dennoch übersteigen die Kosten der Durchsetzung dieses Rechts über das Gerichtssystem den Geldwert der Kaution und der geschuldeten Schäden, selbst unter Einbeziehung einer möglichen gesetzlichen Entschädigung [1]. Die rationale Reaktion besteht darin, den Verlust hinzunehmen und auszuscheiden.

Dies ist kein pathologischer Sonderfall. Es ist die Standarderfahrung bei einer bedeutenden Klasse von Streitigkeiten, bei denen der Schaden real ist, aber der finanzielle Einsatz unter die Schwelle fällt, ab der eine institutionelle Durchsetzung wirtschaftlich rational wird. Das Ergebnis ist ein System, das strukturell schlechte Akteure begünstigt: Wer anderen in Mengen unterhalb dieser Schwelle schadet, kann unges-

traft handeln, weil die Kosten der Rechtssuche auf die geschädigte Partei fallen.

Das obige Beispiel stammt aus dem Rechtsumfeld des Autors—dem tschechischen zivilrechtlichen System. In anderen Rechtstraditionen—dem auf Präzedenzfällen beruhenden Common Law, dem Gewohnheitsrecht, gemischten Systemen—versagt die Gerechtigkeit auf unterschiedliche Weise und in unterschiedlichem Ausmaß, je nach den kulturellen und verfahrenstechnischen Besonderheiten der jeweiligen Rechtsordnung. Die Leser werden vermutlich vergleichbare Beispiele aus ihrem eigenen Umfeld erkennen. Strukturell universell ist das Muster: Streitigkeiten, deren Wert unter die Schwelle einer wirtschaftlich rationalen Durchsetzung fällt, enden damit, dass der Verlust von der geschädigten Partei getragen wird. Das RSN verspricht keine perfekte Gerechtigkeit—es verringert lediglich den strukturellen Vorteil, den schlechte Akteure genießen, wenn die institutionelle Durchsetzung unwirtschaftlich ist.

1.2 Warum bestehende Lösungen zu kurz greifen

Frameworks für dezentrale Identität (DID) [2] bieten kryptografische Mechanismen für ein selbstbestimmtes Identitätsmanagement, konzentrieren sich jedoch in erster Linie auf die Identitätsverifizierung, ohne die umfassendere Frage der Verhaltensreputation zu behandeln.

Soulbound Tokens (SBTs) [3] erfassen die Erkenntnis, dass Reputation nicht übertragbar ist, sind jedoch auf eine Blockchain-Infrastruktur mit Skalierbarkeitsbeschränkungen angewiesen und behandeln nicht die wirtschaftlichen Anreize, die den Informationseintrag steuern. Verwandte Konzepte wie Verdiensttoken (z. B. Liberland) teilen eine ähnliche Philosophie, bleiben jedoch an spezifische rechtsordnungsgebundene Rahmenwerke gebunden.

Dezentrale autonome Organisationen (DAOs) [4] implementieren Governance über Smart Contracts, replizieren jedoch plutokratische Dynamiken, bei denen der Einfluss proportional zum Kapital ist. Quadratisches Abstimmen [5] mildert dies teilweise, begrenzt jedoch die praktische Verbreitung. DAOs stehen zudem vor dem grundlegenden *Orakel-Problem*: Smart Contracts können reale Zustände nicht zuverlässig verifizieren, ohne eine vertrauenswürdige externe Quelle, und dieses Problem hat innerhalb der Blockchain-Architektur keine allgemeine Lösung.

Kein bestehendes System vereint Dezentralisierung, Zensurresistenz, Pseudonymität, nachweisbare Eintrittskosten und emergenten Konsens.

1.3 Beiträge

Diese Arbeit leistet die folgenden Beiträge:

1. Definition des **Reputationsnetzwerks (Reputation Social Network, RSN)**, eines dezentralen Protokolls, das das DID-Framework um die Unterstützung eines bilateralen Reputationsaustauschs erweitert.
2. Ein **nichtdeterministisches Protokoll zur Auswahl von Verifizierern** auf Basis von konsistentem Hashing [6].
3. Das **Prinzip des teuren Radikalismus**, das Behauptungen entsprechend ihrer Distanz zum Netzwerkkonsens über drei sich verstärkende Kostenkanäle bepreist.
4. Ein **Modell der reputablen Autorität** mit asymmetrischen Anreizen, bei dem eine falsche Bestätigung katastrophal mehr kostet als legitime Gebühren.
5. Ein **schrittweiser Migrationspfad** über eine parallele fiskalische Infrastruktur.

2 Gestaltungsprinzipien

Die RSN-Architektur wird durch fünf nicht verhandelbare Gestaltungsprinzipien eingeschränkt.

Kontinuität und Evolution. Das System koexistiert mit bestehenden Institutionen während einer Übergangszeit von unbestimmter Länge. Der Übergang muss in jeder Phase umkehrbar sein.

Freiwilligkeit und Verantwortung. Die Teilnahme ist freiwillig, aber Freiwilligkeit ist mit Verantwortung verbunden: Ein Teilnehmer, der die Kontrolle über eine institutionelle Funktion übernimmt, übernimmt zugleich die damit einhergehenden Pflichten.

Vielfalt und kulturelle Neutralität. Der Konsens entsteht aus bilateralen Interaktionen, nicht aus voreingestellten Regeln, die von den Systemgestaltern auferlegt werden.

Widerstandsfähigkeit und Zensurresistenz. Die Kosten der Zensur des Netzwerks müssen die Kosten seiner Duldung übersteigen. Nur ein vollständiger Totalitarismus—zu ruinösen politischen und wirtschaftlichen Kosten—kann das System unterdrücken.

Konsens und Durchsetzung. Das System integriert menschliche Neigungen zu Kleinlichkeit, Boshaftigkeit und vergeltender Genugtuung als tragende Merkmale. Fehlverhalten ist nicht verboten; es

wird bepreist.

3 Systemübersicht

3.1 Reputationsnetzwerk

Das RSN ist eine dezentrale Peer-to-Peer-Kommunikationsschicht, in der Teilnehmer verifizierbare Informationen über reales Verhalten austauschen. Seine definierenden Eigenschaften sind: dezentrale und unzensierbare Infrastruktur; pseudonyme Teilnahme über DIDs; asymmetrische Kostenstruktur (Lesen ist günstig, Schreiben ist teuer); kryptografische Verifizierbarkeit; und **Standardunterstützung**—maschinenlesbare Formate für Informationen, die durch das Netzwerk propagiert werden, für Dienste, die von Autoritäten angeboten werden (Zusammenstellung von Behauptungen, Bestätigung, Zeugendienst), und für das Richtlinienformat einschließlich der Regeln zur Bewertung der Reputation der Gegenpartei und zur Einschätzung des Risikos einer Richtliniendiskrepanz (zwischen deklariertem und tatsächlichem Verhalten).

3.2 Architektonische Komponenten

Das RSN besteht aus vier primären Komponenten (Abb. 1):

1. **DID-Schicht.** Teilnehmeridentitäten mit deklarierten Regeln, Reputationsmetadaten und Netzwerkrouting.
2. **Behauptungsprotokoll.** Strukturiertes Format zur Veröffentlichung von Aussagen über reale Ereignisse.
3. **Verifizierungsnetzwerk.** Dezentrales Protokoll zur Zuweisung von Verifizierern mittels konsistentem Hashing.
4. **Reputationsaggregationsschicht.** Dienste, die menschenlesbare Reputationszusammenfassungen erzeugen.

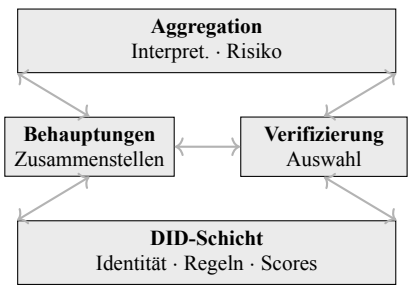

Figure 1: Vierschichtige RSN-Architektur.

3.3 Teilnehmerrollen

An einer Verifizierungstransaktion sind bis zu sechs unterschiedliche DID-Rollen beteiligt (Abb. 2): **Aussteller** (DID_I, erstellt und übermittelt die Behauptung), **Subjekt** (DID_S, die DID, um die es in der Behauptung geht—kann mit dem Aussteller zusammenfallen), **Autorität** (DID_A, bestätigt die Behauptung gegen eine Gebühr; kann auch Zeugendienste anbieten—*optional*), **Zeuge** ($DID_{W_{1..n}}$, inkognito überwachende Instanz der Ehrlichkeit des Verifizierers über Challenge-Codes—*optional*), **Verifizierer** (DID_V, algorithmisch ausgewählt, um die Behauptung zu veröffentlichen) und das **RSN** (das Netzwerk, in dem verifizierte Behauptungen veröffentlicht werden). Jede Rolle kann an eine andere DID delegiert werden (Abschnitt 7.4). Eine Autorität bündelt üblicherweise Bestätigung mit Zeugendiensten, aber die beiden Funktionen sind logisch unabhängig.

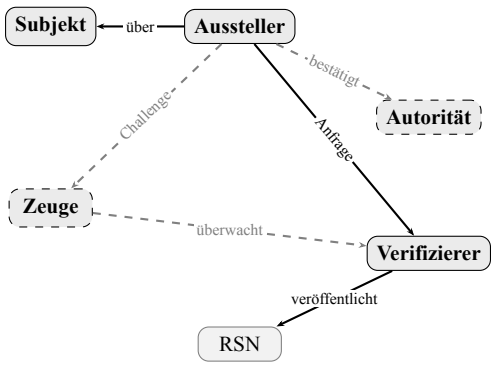

Figure 2: DID-Rollen in einer Verifizierungstransaktion. Gestrichelt = optional (Autorität, Zeuge).

3.4 Unbestechlichkeit: Vier Kräfte

Die Unbestechlichkeit des RSN entsteht nicht aus einem einzigen Mechanismus, sondern aus vier gleichzeitig wirkenden Kräften. Keine ist für sich allein ausreichend; erst ihre Kombination macht einen Korruptionsversuch wirtschaftlich irrational.

Unvorhersehbares Ziel. Der Verifizierer für jede Behauptung wird nichtdeterministisch durch konsistentes Hashing ausgewählt (Abschnitt 5.3). Ein Angreifer kann keinen bestimmten Verifizierer für eine Bestechung vorab ins Visier nehmen, weil die Identität des Verifizierers eine Funktion des Inhalts der Behauptung und vorheriger Iterationen ist, nicht der Wahl des Ausstellers.

Reputationshebel—langsam hoch, schnell runter. Reputation kann nur schrittweise gewonnen werden, durch anhaltendes konsistentes Verhalten. Sie

kann jedoch in einer einzigen betrügerischen Bestätigung katastrophal verloren gehen (Abschnitt 6.2). Diese Asymmetrie bedeutet, dass jahrelang angesammelte Reputation durch eine einzige unehrliche Bestätigung zerstört werden kann; die optimale Strategie bleibt, verdächtige Behauptungen abzulehnen.

Öffentliches Versprechen. Jeder DID-Inhaber deklariert öffentlich seine Richtlinie—einen maschinenlesbaren Satz von Regeln, deren Einhaltung er sich verpflichtet. Eine Abweichung zwischen der Deklaration und dem tatsächlichen Verhalten ist erkennbar und wird als Reputationsvergehen bepreist, das schwerer wiegt als der zugrunde liegende Verstoß (Abschnitt 7.3). Heuchelei ist daher kostspieliger als direkte Unehrlichkeit.

Asymmetrie der Angriffskosten im Netz. Die Kosten der Zensur oder Destabilisierung des Netzwerks wachsen nichtlinear mit der Größe und Dichte des Netzwerks, während die Kosten seiner Duldung konstant bleiben. Damit sich Zensur lohnt, müsste ein zentralisierter Akteur sie über das gesamte Netzwerk anwenden—was Maßnahmen erfordern würde, die in keinem Verhältnis zu einem denkbaren Nutzen stehen (Abschnitt 10).

4 Modell der dezentralen Identität

4.1 DID mit besonderen Eigenschaften

Das RSN erweitert die W3C-DID-Core-Spezifikation [2] um: **Deklarierte Regeln** (maschinenlesbare Verhaltensverpflichtungen), **Reputationsmetadaten** (aggregierter Verhaltensscore) und **Netzwerkrouting** (veränderliches Onion-Gateway, getrennt von der stabilen Ringposition).

4.2 Lebenszyklus einer Behauptung

Eine Behauptung durchläuft sechs Phasen (Abb. 3): Zusammenstellung, optionale Bestätigung durch eine Autorität, Auswahl des Verifizierers über konsistentes Hashing, Verifizierungsentscheidung (Annahme oder Ablehnung mit Iteration), Veröffentlichung und Reputationsaktualisierung für alle Parteien.

4.3 Verhältnis zu W3C DID Core

Das Identitätsmodell des RSN ist eine echte Obermenge der W3C-DID-Core-Spezifikation [2]. Alle RSN-DIDs sind gültige W3C-DIDs. Die RSN-spezifischen Erweiterungen sind als DID-Dokumenteigenschaften kodiert, die in einer eigenen DID-Methodenspezifikation definiert sind und mit bestehender Infrastruktur wie ION [7] und Ceramic [8] kompatibel sind.

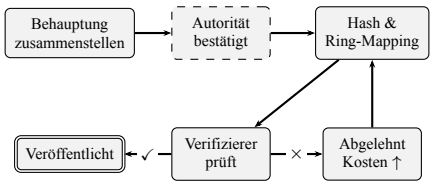

Figure 3: Lebenszyklus einer Behauptung mit Iterationsschleife.

5 Informationsverifizierung und -verbreitung

5.1 Kosten des Informationseintrags

Das ökonomische Kernprinzip des RSN ist die Asymmetrie zwischen Lesen und Schreiben. Das Lesen von Reputationsdaten nähert sich für Teilnehmer, die Teil des DID-Netzwerks sind und über einen ihrer Reputation angemessenen Zugang verfügen, den marginalen Kosten von null—Neulinge müssen sich einen breiteren Zugang schrittweise verdienen (siehe Anti-Leeching). Schreiben—verstanden als die dauerhafte Materialisierung von Reputation in das Netzwerk, nicht als einmaliger technischer Akt—erfordert nachweisbare kumulative Investitionen über drei Dimensionen: **Zeit** (Lebensjahre, die auf konsistentes Verhalten, erfüllte Verpflichtungen und gepflegte Beziehungen verwendet werden), **Energie** (in ehrliches Handeln, die Pflege von Partnerschaften und langfristige Vertrauenswürdigkeit investierter Aufwand) und **Geld** (Investition in den eigenen Namen—berufliche Entwicklung, die Qualität der eigenen Arbeit, Wiedergutmachung für verursachte Schäden). Reputation kann nicht sofort erworben werden—sie ist das Ergebnis einer lebenslangen Akkumulation, die das System lediglich sichtbar und über Kontexte hinweg übertragbar macht. Die einmaligen technischen Kosten des Protokolls (kryptografische Signaturen, Verifiziergebühren) sind im Vergleich zu dieser zugrunde liegenden Investition vernachlässigbar.

5.2 Sozialer Graph und Kontakttiefe

Das RSN ist grundsätzlich ein soziales Netzwerk: Jede DID fügt Kontakte hinzu (andere DIDs), die die Verbindung zulassen. Diese Kontakte haben ihre eigenen Kontakte, und so weiter. Die algorithmische Verifiziersuche operiert innerhalb einer konfig-

urierbaren Tiefe h verknüpfter Kontakte (z. B. $h = 3$: die eigenen direkten Kontakte, deren Kontakte und die Kontakte der Kontakte). Diese Architektur erfordert keine einzige globale Blockchain—sie begünstigt naturgemäß die Entstehung von Gemeinschaften/Clustern mit Überschneidungen in andere Gemeinschaften. Jeder DID-Teilnehmer muss eine veröffentlichte **Richtlinie** haben—einen maschinenlesbaren Satz von Regeln, der bestimmt, wie eingehende Anfragen bewertet werden. Richtlinienverstöße werden im Netzwerk als negative Artefakte erfasst.

5.3 Algorithmische Auswahl des Verifizierers

Das Verifizierungsprotokoll verwendet konsistentes Hashing [6] (Abb. 4). Verifizierung ist ein kostenpflichtiger Dienst: Verifizierer arbeiten gegen eine Gebühr und schaffen einen Markt, in dem der Wettbewerb Preisgestaltung, Geschwindigkeit und Zuverlässigkeit antreibt.

Schritt 1. Das Behauptungsdokument wird mit dem Hash-Ergebnis der vorherigen Iteration verkettet (oder $\varnothing$ bei der ersten Iteration) und gehasht:

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

Der Algorithmus muss den *vollständigen Pfad* aller vorherigen Anfragen und Antworten einbeziehen—nicht nur einen Hash der vorherigen Iteration. Die vollständige Antwort jedes Verifizierers (Annahme, Ablehnung, angebotener Preis, Begründung) wird an das wachsende Dokument angehängt und ist durch kryptografische Signaturen bei jedem Schritt verifizierbar.

Schritt 2. Der Hash wird auf N Positionen auf dem konsistenten Hash-Ring abgebildet, gleichmäßig verteilt (z. B. für $N = 4$: $+0°, +90°, +180°, +270°$). Von jeder Position aus wählt eine im Uhrzeigersinn verlaufende Suche die nächstgelegene DID als Verifizierer-Kandidat aus (Abb. 5). N ist ein variabler Parameter, der vom Prozentsatz der derzeit aktiven DIDs, der Tageszeit oder der historischen Netzwerk-Reaktionsfähigkeit abhängen kann.

Schritt 3. Der Verifizierer nimmt an (veröffentlicht, setzt Reputation ein) oder lehnt ab (Rückkehr zu Schritt 1 mit dem Ablehnungs-Hash). Wenn ein Knoten trotz deklariertem Online-Status nicht antwortet, muss die nächste Anfrage alle Antworten aller N vorherigen Verifizierer-Kandidaten enthalten.

Anti-Leeching. Ziel-DIDs können Gebühren oder Zugangsbeschränkungen für Anfragen von neuen DIDs mit geringer Reputation festlegen. Dieser abgestufte Mechanismus (nicht binär) zwingt Neulinge dazu, durch echte Aktivität Reputation aufzubauen, bevor sie die Daten anderer frei konsumieren können.

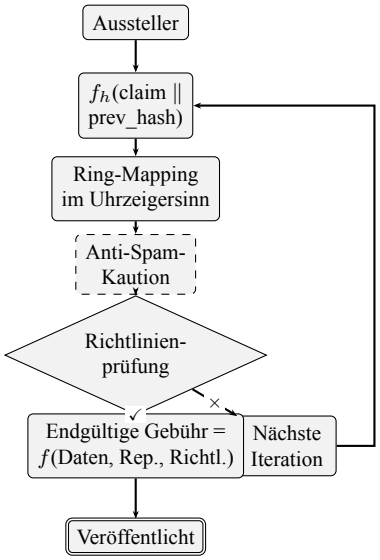

Figure 4: Protokoll zur Auswahl des Verifizierers. Die Anti-Spam-Kaution ist optional und kann erstattungsfähig sein. Die endgültige Gebühr wird nur bei Annahme gezahlt.

Jede Ablehnung hängt die vollständige Antwort des Verifizierers (einschließlich Gründe und Bedingungen) an das Behauptungsdokument an und erweitert dessen Inhalt. Aus dem erweiterten Dokument wird nichtdeterministisch ein neuer Hash berechnet, der auf eine andere Ringposition abgebildet wird und einen anderen Verifizierer auswählt. Die Dokumentation des vollständigen Pfades ist obligatorisch—der Aussteller kann den nächsten Verifizierer weder vorhersagen noch beeinflussen. Wenn ein Verifizierer eine Anfrage trotz kompatibler deklarierter Richtlinie ignoriert, halten Zeugen (sofern vorhanden) dies fest, und der Aussteller kann bei der endgültigen Veröffentlichung Zeugenbeweise beifügen.

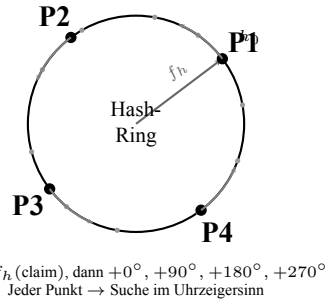

Figure 5: Mehrpunkt-Auswahl (N=4). Der Hash h_0 legt den Versatz fest; 4 Punkte gleichmäßig von h_0 verteilt.

5.4 Zeugenprotokoll

Die Rolle des **Zeugen** bietet über ein kryptografisches Challenge-Code-Protokoll inkognito Rechenschaftspflicht für die Ehrlichkeit des Verifizierers:

Schritt W1. Der Anfragende signiert die Verifizierungsanfrage und sendet sie an N_w Zeugen—Kontakte aus dem sozialen Netzwerk des Anfragenden oder spezialisierte Zeugendienstanbieter, die gegen eine Gebühr arbeiten.

Schritt W2. Jeder Zeuge w_i signiert die gesamte signierte Anfrage, behält die ursprüngliche Signatur σ_i und berechnet einen Challenge-Code $c_i = h(\sigma_i)$. Der Challenge-Code wird an die Anfrage angehängt.

Schritt W3. Die Anfrage, die nun N_w Challenge-Codes trägt, wird an den Verifizierer gesendet. Der Verifizierer beobachtet die Codes, kann aber *nicht feststellen*, wer die Zeugen sind oder ob die Codes echten Signaturen entsprechen.

Schritt W4 (ehrlicher Verifizierer). Antwortet der Verifizierer gemäß seiner deklarierten Richtlinie, bleiben die Challenge-Codes undurchsichtig. Zeugen werden niemals offengelegt. Es werden keine zusätzlichen Daten veröffentlicht.

Schritt W5 (Richtlinienverstoß). Verstößt der Verifizierer gegen seine Richtlinie (ignoriert die Anfrage, antwortet inkonsistent), hält der Anfragende die ursprünglichen Signaturen σ_i der Zeugen. Diese können als Begleitdaten veröffentlicht werden: Jeder kann $c_i = h(\sigma_i)$ verifizieren und damit beweisen, dass der Zeuge anwesend war. Der Anfragende kann unabhängig veröffentlichen—der Verifizierer hat die Challenge-Codes in seiner Antwort bereits signiert.

Die Bluff-Eigenschaft. Der Anfragende kann für einige oder alle Challenge-Codes zufällige Werte einsetzen. Der Verifizierer kann echte Codes (gedeckt durch Autoritäten mit hoher Reputation) nicht von Rauschen unterscheiden. Diese *Ungewissheit* ist der Durchsetzungsmechanismus: Jede Anfrage birgt das Risiko, dass eine angesehene Autorität inkognito zusieht. Die Kosten, diesen Druck aufrechtzuerhalten, liegen nahe null (Erzeugung von Zufallszahlen), während die potenziellen Kosten der Unehrlichkeit für den Verifizierer katastrophal sind. Ehrliches Verhalten wird selbst in Abwesenheit tatsächlicher Zeugen begünstigt.

Autorität als Zeuge. Eine Autorität, die eine Behauptung bestätigt, kann Zeugendienste bündeln: „Ich bestätige Ihre Behauptung und diene während der Verifizierung als Inkognito-Zeuge.“ Dies ist ein natürliches Geschäftsmodell—die Autorität verfügt bereits über den Kontext. Die beiden Rollen sind jedoch logisch unabhängig.

5.5 Prinzip des teuren Radikalismus

Drei Kostenkanäle verstärken sich gleichzeitig (Abb. 6):

Kanal 1: Iterationskosten. Jede Ablehnung erzwingt eine neue Iteration, die Zeit und Ressourcen verbraucht. Lineares Wachstum.

Kanal 2: Dokumentenaufblähung. Jede Iteration fügt die vollständige Verifiziererantwort zum Behauptungsdokument hinzu. Das Wachstum ist linear, jedoch mit einem Basisversatz: Die anfängliche Nutzlast (Behauptungsinhalt, Bestätigung durch die Autorität, kryptografische Signaturen) hat bereits eine nicht triviale Größe B_0. Gesamtgröße nach k Iterationen: $S(k) = B_0 + k \cdot \Delta$, wobei Δ die durchschnittliche Antwortgröße ist.

Kanal 3: Risikoaufschlag des Verifizierers. Risiko ist subjektiv. Der Verifizierer beurteilt, ob die deklarierten Richtlinien der anfragenden DID mit den eigenen kommerziellen, sozialen oder politischen Interessen des Verifizierers in Konflikt stehen. Der Aufschlag kann exponentiell mit der wahrgenommenen Distanz vom „Ideal“ des Verifizierers eskalieren: $P(d) = \alpha \cdot e^{\beta d}$, wobei d die subjektive Distanzmetrik des Verifizierers ist. Jenseits einer persönlichen No-Go-Grenze kann der Verifizierer vollständig ablehnen.

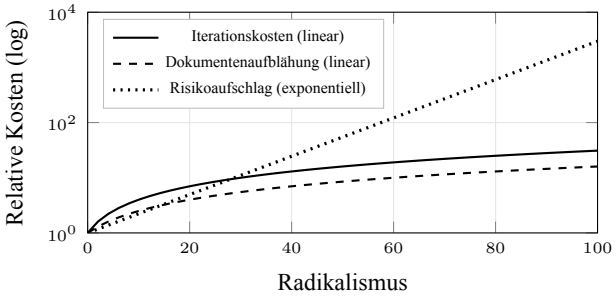

Figure 6: Kosteneskalation über drei Kanäle. Der Risikoaufschlag dominiert bei hohem Radikalismus.

Entscheidend ist: Dies ist keine Zensur. Keine Behauptung ist verboten. Das System bepreist das Risiko (Tabelle 1).

Table 1: Kostenvergleich über verschiedene Behauptungstypen.

Typ	Iter.	Dok.	Gebühr	Gesamt
Glaubwürdig	$k_{\min}$	B_0	$P_{\min}$	Niedrig
Kontrovers	k_{med}	$B_0 + k\Delta$	$\alpha e^{\beta d}$	Mittel
Radikal	$k_{\max}$	$\gg B_0$	$\gg P_{\min}$	Sehr hoch
Betrügerisch	$\to \infty$	—	—	Unveröffentlichbar

6 Reputation und Risikobewertung

6.1 Modell der Reputationsakkumulation

Reputation weist drei Eigenschaften auf: **langsame Akkumulation** (schrittweises Wachstum durch konsistentes Verhalten), **schnelle Zerstörung** (ein einziger Betrug kann den Score katastrophal senken) und **individuelle Bewertung** (jede konsumierende Partei kann ihre eigene Aggregationsfunktion anwenden).

6.2 Reputable Autoritäten

Eine reputable Autorität prüft Behauptungen und mitunterzeichnet sie, sofern sie überzeugt ist—und setzt dabei ihre eigene Reputation ein (Abb. 7). Die Asymmetrie ist beabsichtigt: Reputation zu gewinnen ist langsam (schrittweise $+\delta$ pro ehrlicher Bestätigung), während ihr Verlust katastrophal ist ($-\Delta \gg \delta$ pro falscher Bestätigung; veranschaulichend etwa $+2\%$ gegenüber -70%). Die optimale Strategie besteht immer darin, verdächtige Behauptungen abzulehnen. Die konkreten Werte von δ und Δ sind Systemparameter.

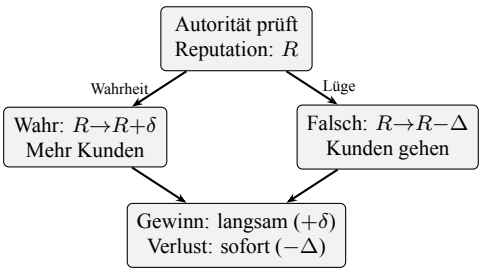

Figure 7: Reputable Autorität—asymmetrische Anreize.

6.3 Mehrdimensionale Reputation

Reputation ist kein Skalar, sondern ein Vektor über mehrere Dimensionen: finanzielle Zuverlässigkeit, persönliche Integrität, fachliche Kompetenz, bürgerschaftliches Engagement und andere (Abb. 8). Verschiedene Bewertungsanbieter projizieren diesen Vektor je nach Kontext unterschiedlich—ein Kreditgeber priorisiert die finanzielle Zuverlässigkeit, ein Arbeitgeber die fachliche Kompetenz, ein Nachbar das bürgerschaftliche Verhalten. Es gibt keinen einzigen „richtigen“ Reputationsscore; nur Perspektiven.

6.4 Demokratisierte Risikobewertung

Das RSN demokratisiert die systematische Risikobewertung—eine Fähigkeit, die derzeit bei

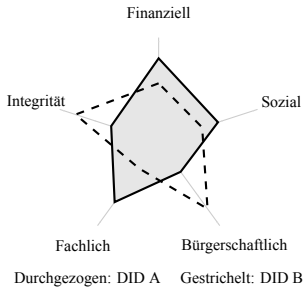

Figure 8: Mehrdimensionale Reputationsvektoren. Verschiedene DIDs weisen unterschiedliche Profile über die Dimensionen hinweg auf.

Finanzinstituten konzentriert ist, aber weit über das Bankwesen hinaus anwendbar ist. Industriekonglomerate, die die Zuverlässigkeit von Lieferanten bewerten, Versicherungsunternehmen, die Verhaltensrisiken bepreisen, Due Diligence bei Fusionen und Übernahmen, Schätzung der Lebensdauer von Anlagen in der Fertigung—überall dort, wo das Risiko der Gegenpartei bewertet werden muss, bietet das RSN eine dezentrale, marktgetriebene Alternative. Ein Markt für Interpretationsdienste übersetzt rohe mehrdimensionale Reputationsdaten in handlungsleitende Zusammenfassungen und macht die Bewertung der Gegenpartei für jeden Teilnehmer zu marginalen Kosten zugänglich.

7 Konsens und Streitbeilegung

7.1 Modell dezentraler Gerechtigkeit

Das RSN formuliert Gerechtigkeit als bilaterales Verhandlungsproblem neu. Die Drohung eines dauerhaften, verifizierbaren Reputationsschadens ist ein wirksameres Abschreckungsmittel als Gerichtsverfahren, die sich die geschädigte Partei nicht leisten kann.

7.2 Emergenter Konsens

Jeder Teilnehmer unterhält eine persönliche Zufriedenheitsschwelle. Der aggregierte Konsens des Netzwerks entsteht als statistischer Durchschnitt tausender bilateraler Verhandlungen (Abb. 9). Eine Reaktion weit oberhalb des Konsenses (barbarisch) ist teuer zu veröffentlichen. Eine Reaktion nahe dem Konsens (verhältnismäßig) ist günstig. Der Konsens ist keine Regel—er ist ein Preissignal.

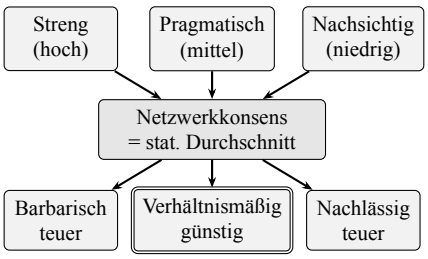

Figure 9: Emergenter Konsens aus individuellen Zufriedenheitsschwellen.

7.3 Kalibrierung der Bestrafung

Jeder DID-Inhaber deklariert öffentlich Reaktionen auf bestimmte Kategorien von Fehlverhalten. Unverhältnismäßig harte oder milde Deklarationen ziehen negative Reputationssignale nach sich. Verhältnismäßige Deklarationen werden reibungslos akzeptiert—ein sich selbst kalibrierendes Bestrafungssystem.

Konsensdeklarationen unterliegen selbst der Heuchelei-Erkennung: sich deklarativ zu einer Konsensposition zu verpflichten und dabei inkonsistent zu handeln, stellt ein Reputationsvergehen dar, das schwerer wiegt als die zugrunde liegende Abweichung, da es eine absichtliche Täuschung belegt.

7.4 Delegation

Alle Aktivitäten innerhalb einer DID können—mit einer Ausnahme—an eine andere DID delegiert werden. **Die Subjekt-Rolle—die DID, um deren Verhalten es in der Behauptung geht—kann nicht delegiert werden; sie ist nicht übertragbar an den Identitätsinhaber gebunden, auf den sich die Behauptung bezieht.** Die anderen aktiven Rollen—Aussteller, Autorität, Zeuge, Verifizierer—können an eine benannte Delegat-DID übertragen werden, sei es zur Verifizierung, zur Übermittlung von Behauptungen, zur Konsensbeteiligung oder zur Streitbeilegung. Die Delegation ist jederzeit widerrufbar. Dies ermöglicht Spezialisierung (z. B. professionelle Verifizierungsdienste), während der Inhaber die letztliche Kontrolle und Verantwortung behält. Delegation gilt im gesamten System und ist für die Skalierbarkeit unerlässlich.

7.5 Von individueller Moral zum emergenten Gesellschaftsvertrag

Die deklarierte Richtlinie jeder DID stellt eine Formalisierung der individuellen Moral dar: was der Inhaber für akzeptabel hält, wie er auf bestimmte Verhaltensweisen reagiert, was er von Gegenparteien verlangt. Diese Richtlinien werden nicht von einem Systemgestalter auferlegt—sie werden von jedem Teilnehmer gewählt und in maschinenlesbarer Form ausgedrückt.

Diese Formalisierung ermöglicht eine dreistufige Emergenz. Erstens wird individuelle Moral als **Richtlinie** kodiert—ein Satz deklarierter Regeln, Schwellenwerte und Reaktionsfunktionen, deren Einhaltung sich die DID verpflichtet. Zweitens erzeugt die Gesamtheit aller Richtlinien über das Netzwerk hinweg eine **emergente Ethik**—statistisch beobachtbare Normen, die kein einzelner Teilnehmer entworfen hat, die aber aus der Interaktion tausender individueller moralischer Positionen entstehen [9]. Drittens bilden diese emergenten Ethiken, ausgedrückt als geteilte Verhaltensnormen, die durch bilaterale Preissignale durchgesetzt werden, einen **messbaren Gesellschaftsvertrag**—kein theoretisches Konstrukt, das niemand unterzeichnet hat [10], sondern ein empirisch beobachtbarer Satz von Regeln, der durch tatsächliches Verhalten gedeckt ist.

Dieser Prozess spiegelt Erkenntnisse der Theorie der moralischen Grundlagen wider [11]: Die menschliche Moral ist intuitiv, pluralistisch und kulturell variabel. Das RSN erfordert keinen moralischen Konsens als Eingabe; es erzeugt einen Verhaltenskonsens als Ausgabe. Der resultierende Gesellschaftsvertrag ist nicht statisch—er entwickelt sich weiter, während Teilnehmer beitreten, ausscheiden und ihre Richtlinien als Reaktion auf Netzwerk-Feedback anpassen. Anders als bei der klassischen Gesellschaftsvertragstheorie ist dieser Vertrag widerrufbar, beobachtbar und ohne einen Souverän durchsetzbar.

8 Ökonomisches Modell

Die vorangegangenen Abschnitte beschrieben ein Werkzeug—die Verifizierungsmechanismen, die Kostenstruktur und den emergenten Konsens des RSN. Dieser Abschnitt beschreibt eine Methodik zur Anwendung dieses Werkzeugs auf den fiskalischen und Governance-Übergang. Das Werkzeug ist von allgemeinem Zweck; die nachfolgende Methodik ist eine mögliche Anwendung.

8.1 Anreizstruktur

Reputation als Kapital schafft direkte Anreize für ehrliches Verhalten. Im Normalbetrieb bauen Teilnehmer auf natürliche Weise Reputation durch alltägliche Transaktionen und erfüllte Verpflichtungen

auf. Die primäre Ausgabe entfällt auf *negative* Behauptungen—die Erfassung von Schaden, der von anderen verursacht wurde. Diese Asymmetrie fördert nützliches, zuverlässiges Verhalten: Ehrlich zu sein kostet nichts zusätzlich, während schädliches Verhalten eine dokumentierte Spur schafft, deren Erhaltung andere sich etwas kosten lassen. Heuchelei—Regeln zu deklarieren, ohne sie zu befolgen—ist der teuerste Fehlermodus, da sie eine absichtliche Täuschung belegt.

8.2 Paralleles Fiskalsystem

Drei Komponenten ermöglichen Wettbewerbsdruck: (1) **Einfache Steuer**—ein einziger proportionaler Satz ohne Ausnahmen, anfänglich marginal unter dem bestehenden effektiven Satz; (2) **Elektronische Ausgabenregistrierung (ESR)**—eine Umkehrung des tschechischen EET-Modells, sodass Bürger die staatlichen Ausgaben überwachen; (3) **Bürgergesteuerte Steuerzuweisung**—beginnend bei einigen Prozent im ersten Jahr und nach einem Jahrzehnt irgendwo zwischen einem niedrigen zweistelligen Bereich und einer vollständigen Migration zu einem bürgergesteuerten System erreichend, je nach Adoptionsrate. Das tatsächliche Tempo hängt von der Geschwindigkeit ab, mit der freimarktwirtschaftliche Alternativen zu staatlichen Diensten entstehen, sowie von der Bereitschaft des Staates, mit dem Übergang zu kooperieren; die Funktion der Zeit muss nicht linear sein, und es gibt keinen Grund, eine Obergrenze dafür festzulegen, wo die Adoption letztlich ankommen kann.

9 Migrationspfad

Die Migration verläuft über drei Phasen (Abb. 10): **Phase 1: Overlay** (RSN als informationelle Schicht, Staat ist alleiniger Anbieter), **Phase 2: Wettbewerb** (RSN bietet funktionale Alternativen, Nutzung eines Doppelsystems) und **Phase 3: Übergang** (RSN übertrifft staatliche Entsprechungen, freiwillige Migration). Der Übergang ist in jeder Phase umkehrbar.

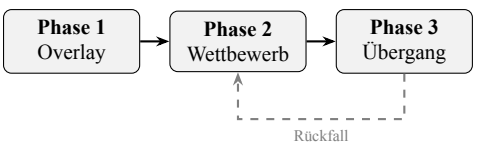

Figure 10: Dreiphasige Migration—in jeder Phase umkehrbar.

Der primäre Druckmechanismus ist fiskalisch: Wenn bedingte Steuerzahler eine „wirtschaftlich bedeutsame Minderheit X“ erreichen—eine Gruppe, die groß genug ist, dass Repression gegen sie nicht triviale wirtschaftliche Schäden verursacht und ziviler Ungehorsam zu einer glaubwürdigen Bedrohung wird—tritt der Staat in Verhandlungen ein. Zur Veranschaulichung verwenden wir $X \approx 15\%$ des BIP, aber die tatsächliche Schwelle hängt von der jeweiligen Volkswirtschaft ab.

10 Sicherheitsanalyse

Wir betrachten fünf Kategorien von Angreifern: einzelne schlechte Akteure, organisierte Gruppen, unternehmerische Angreifer, staatliche Angreifer und Angreifer auf Protokollebene.

Sybil-Resistenz [12]. Der Aufbau von Reputation erfordert anhaltende, verifizierbare Interaktion. Die Kosten eines erfolgreichen Sybil-Angriffs skalieren linear mit der Anzahl gefälschter Identitäten und quadratisch mit dem angestrebten Reputationsniveau. Der parallele Betrieb mehrerer DIDs ist möglich, aber konstruktionsbedingt teuer—jede Identität muss unabhängig Reputation durch echte Aktivität akkumulieren. In freien Gesellschaften schreckt diese Kosten von beiläufigem Missbrauch ab; in Diktaturen werden parallele DIDs zu einem Überlebenswerkzeug, das kompartimentierten Widerstand, konspirative Koordination und eine sicherere Navigation auf dem Schwarzmarkt ermöglicht.

Kollusionsabwehr. Muster gegenseitiger Bestätigung innerhalb geschlossener Gruppen sind durch Analyse des sozialen Graphen erkennbar. Reputationsaggregationsfunktionen gewichten Behauptungen aus eng geclusterten Quellen ab.

Staatlicher Angreifer. Onion-Routing, das Fehlen zentralisierter Infrastruktur und die Verteilung der Verifizierer-Rolle über die Teilnehmerbasis stellen sicher, dass eine Unterdrückung Maßnahmen erfordert, die in keinem Verhältnis zu irgendeinem Nutzen stehen.

Datenschutz vs. Rechenschaftspflicht. Pseudonymität—ein Mittelweg zwischen Anonymität und Identitätsoffenlegung—erlaubt DIDs, bedeutsame Reputation zu akkumulieren, ohne die reale Identität des Inhabers preiszugeben.

11 Datenschutzüberlegungen

Das Datenschutzmodell des RSN beruht auf Pseudonymität. Der Inhaber kontrolliert die Identität-

soffenlegung: minimal (reines Pseudonym), selektiv (bestimmte Berechtigungsnachweise verknüpft) oder vollständig (rechtliche Identität zugeordnet). Veröffentlichte Behauptungen sind dauerhaft—das System unterstützt kontextuelle Korrektur, aber keine Löschung. Ein Inhaber kann eine kompromittierte DID aufgeben und neu beginnen, wobei er die angesammelte Reputation verwirkt.

12 Verwandte Arbeiten

Die W3C-DID-Core-Spezifikation [2] und das Ceramic Network [8] bilden die Identitätsgrundlage. EigenTrust [13] demonstrierte eine verteilte Reputationsaggregation ohne zentrale Autorität. SBTs [3] führten nicht übertragbare soziale Token ein. Das RSN unterscheidet sich in seiner Betonung ökonomischer Kosten als Qualitätsfilter und in seinem Mechanismus zur Bepreisung von Radikalismus.

DAOs [4] und quadratisches Abstimmen [5] demonstrierten die Machbarkeit dezentraler Governance. Das RSN leitet Konsens aus bilateralen Preisverhandlungen statt aus Abstimmungen ab.

Der Vorschlag stützt sich auf die anarcho-kapitalistische Theorie [14, 15] für die private Diensterbringung, weicht jedoch in zwei entscheidenden Punkten ab: Er ist auf Boshaftigkeit und Vergeltungsimpulse ausgelegt, statt Rationalität anzunehmen, und schlägt einen schrittweisen Übergang statt einer Revolution vor. Das Konzept emergenter Gesellschaftsverträge hat Vorläufer in Hayeks Theorie der spontanen Ordnung [16].

Anarcho-Agorismus. Das RSN teilt bedeutende Gemeinsamkeiten mit der agoristischen Gegenökonomie [17]—insbesondere die Betonung des Aufbaus paralleler Institutionen und des freiwilligen Austauschs. Der Agorismus neigt jedoch dazu, rationales Eigeninteresse als hinreichenden Koordinationsmechanismus anzunehmen, und es fehlt ihm oft ein konkreter Migrationspfad von bestehenden Staatsstrukturen. Das RSN integriert ausdrücklich nicht-rationale Verhaltensneigungen und stellt einen fiskalischen Druckmechanismus für einen schrittweisen Übergang bereit.

Meritokratie. Das RSN könnte eine erste funktionale Beschreibung dessen darstellen, wie Meritokratie [18] als systemische Eigenschaft statt als Schlagwort entstehen kann. Traditionelle meritokratische Systeme scheitern, weil sie eine zentrale Autorität erfordern, um „Verdienst“ zu definieren und durchzusetzen. Im RSN entsteht Verdienst aus bilateralen Bewertungen: Wer Wert liefert, akkumuliert Reputation; kein Komitee entscheidet, wer Verdienst hat.

Eigentum als Privileg. Das RSN weicht grundlegend von anarcho-kapitalistischen und österreichisch-schulischen Behandlungen von Eigentumsrechten als natürlich und absolut ab. Im RSN-Rahmenwerk ist Eigentum ein *Privileg*—eine gesellschaftliche Anerkennung, die in extremen Fällen von der Gemeinschaft zurückgezogen werden kann, wenn ein Teilnehmer geteilte Normen grundlegend verletzt (Verrat, Weigerung, die Gemeinschaft in einer existenziellen Krise zu verteidigen, systematische Ausbeutung). Dies ist keine staatliche Enteignung, sondern ein Entzug gesellschaftlicher Anerkennung durch das Netzwerk bilateraler Beziehungen.

13 Diskussion und Grenzen

Kaltstart. Der Wert des RSN hängt von Netzwerkeffekten ab; frühe Anwender sehen sich mit begrenztem Nutzen konfrontiert, bis die Teilnahme eine Schwelle erreicht. Doch selbst in frühen Stadien dient das DID-Netzwerk als nützliche ergänzende Informationsquelle. Es ist zu erwarten, dass sich die frühe Reputationsbewertung und Autoritätseinschätzung mit zunehmender Ausgereiftheit schrittweise entwickeln.

Anti-Leeching und Zugangskontrolle. Ziel-DIDs können abgestufte Gebühren und Zugangsbeschränkungen für Anfragen von DIDs mit niedriger Reputation verhängen. Dies ist nicht binär, sondern eine kontinuierliche Skala: Je weniger Reputation eine anfragende DID hat, desto weniger Informationen erhält sie, desto länger wartet sie und desto mehr zahlt sie. Dieser Mechanismus fördert echte Teilnahme gegenüber passivem Konsum.

Ungleichheit des Zugangs. Die Kosten der Veröffentlichung von Behauptungen können legitime Beschwerden wirtschaftlich benachteiligter Teilnehmer herausfiltern. Abhilfe: Jeder Teilnehmer dient gleichzeitig als potenzieller Verifizierer (oder delegiert diese Rolle) und verdient Verifiziergebühren. Über einen ausreichenden Zeithorizont sollte sich ein nicht-radikaler Teilnehmer der finanziellen Neutralität annähern—die Verifiziereinnahmen gleichen die Veröffentlichungskosten näherungsweise aus. Dies ist eine statistische Erwartung, keine Garantie.

Reputationsungleichheit. Frühe Anwender akkumulieren Vorteile, die Barrieren für Nachzügler schaffen können. Die Reputationsbewertung wird jedoch von Drittanbietern durchgeführt, die sich dafür entscheiden können, den Vorteil des Erstanwenders durch ihre Aggregationsalgorithmen abzumildern. Als

Erster über eine gute Reputation zu verfügen, ist ein legitimer komparativer wirtschaftlicher Vorteil—und das ist beabsichtigt.

Offene Fragen. Optimale Kostenfunktionen, Aggregationsstandards, Protokoll-Governance und die Interaktion mit KI-generierten synthetischen Reputationsdaten bleiben Bereiche für künftige Arbeiten.

Diese Arbeit erhebt nicht den Anspruch, dass das RSN unter allen Umständen optimale Ergebnisse liefern wird. Sie beansprucht, dass das RSN eine *machbare* Alternative darstellt—technisch umsetzbar, wirtschaftlich selbsttragend und sozial kompatibel mit menschlichen Verhaltensneigungen, wie sie tatsächlich sind.

14 Schlussfolgerung

Diese Arbeit hat das Reputationsnetzwerk vorgestellt, ein dezentrales Protokoll, das einen pseudonymen, verifizierbaren Reputationsaustausch ermöglicht. Das Prinzip des teuren Radikalismus stellt sicher, dass betrügerische Behauptungen ohne Zensur aus dem Markt gepreist werden. Der vorgeschlagene Migrationspfad ermöglicht einen schrittweisen, umkehrbaren Übergang von bestehenden Institutionen. Der Entwurf integriert die menschliche Natur, wie sie ist—einschließlich Kleinlichkeit, Boshaftigkeit und dem Verlangen nach vergeltender Genugtuung—, statt eine ideologische Transformation zu verlangen. Das Ergebnis ist keine Utopie, sondern ein System, in dem Gerechtigkeit zugänglich ist, Reputation verdient wird und die Kosten des Fehlverhaltens von derjenigen Partei getragen werden, die es verursacht hat.

References

[1] Czech Republic, "Act no. 549/1991 coll., on court fees, as amended," 1991, fee schedule for court proceedings; cost rules per Act No. 99/1963 Coll. (Code of Civil Procedure) and Decree No. 177/1996 Coll. (Attorney Tariff).

[2] M. Sporny, D. Longley, M. Sabadello, D. Reed, O. Steele, and C. Allen, "Decentralized identifiers (DIDs) v1.0," W3C Recommendation, Jul. 2022.

[3] E. G. Weyl, P. Ohlhaver, and V. Buterin, "Decentralized society: Finding Web3's soul," *SSRN Electronic Journal*, May 2022.

[4] V. Buterin, "DAOs, DACs, DAs and more: An incomplete terminology guide," Ethereum Blog, May 2014.

[5] V. Buterin, Z. Hitzig, and E. G. Weyl, "A flexible design for funding public goods," *Management Science*, vol. 65, no. 11, pp. 5171–5187, 2019.

[6] D. Karger, E. Lehman, T. Leighton, R. Panigrahy, M. Levine, and D. Lewin, "Consistent hashing and random trees: Distributed caching protocols for relieving hot spots on the World Wide Web," in *Proc. 29th ACM STOC*, 1997, pp. 654–663.

[7] D. Buchner, "ION — a scalable DID method based on Bitcoin," Microsoft, 2021.

[8] Ceramic Network, "Ceramic protocol specification," GitHub, 2023. [Online]. Available: https://github.com/ceramicnetwork

[9] É. Durkheim, *The Division of Labor in Society*. Free Press, 1893, english translation 1984.

[10] J. Rawls, *A Theory of Justice*. Harvard University Press, 1971.

[11] J. Haidt, *The Righteous Mind: Why Good People Are Divided by Politics and Religion*. Vintage Books, 2012.

[12] J. R. Douceur, "The Sybil attack," in *Proc. 1st International Workshop on Peer-to-Peer Systems (IPTPS)*, 2002, pp. 251–260.

[13] S. D. Kamvar, M. T. Schlosser, and H. Garcia-Molina, "The EigenTrust algorithm for reputation management in P2P networks," in *Proc. 12th International Conference on World Wide Web*, 2003, pp. 640–651.

[14] M. N. Rothbard, *For a New Liberty: The Libertarian Manifesto*. Macmillan, 1973.

[15] H.-H. Hoppe, *Democracy: The God That Failed*. Transaction Publishers, 2001.

[16] F. A. Hayek, *Law, Legislation and Liberty*. University of Chicago Press, 1973.

[17] S. E. I. Konkin, *An Agorist Primer*. KoPubCo, 2006.

[18] M. Young, *The Rise of the Meritocracy*. Thames and Hudson, 1958.