分散型レピュテーションネットワーク：自然な社会組織のためのフレームワーク

Pavel Kudrna
Prague, Czechia
Draft v1 — March 2026

Abstract

正義の感覚——不正が正され、功績が報われるという確信——は、社会の最も強力な結束力である。統治の中央集権的な制度が、権利を執行するコストが権利そのものの価値を上回るためにこの感覚を提供できないとき、社会の結束は蝕まれる。現行の制度構造は、中央計画が資源配分に失敗するのと体系的に同じ仕方で、無視できない一群の紛争を解決できずにいる。すなわち、情報の非対称性、欠落したフィードバックループ、そして意思決定者がその決定の帰結から切り離されていることによってである。本論文はレピュテーション・ソーシャルネットワーク（RSN）を提示する。これは分散型識別子（DID）の上に構築された、分散的で、腐敗不能で、検閲耐性を持つ通信レイヤーであり、仮名の参加者が現実世界の行動に関するレピュテーション情報を公開し、検証し、消費することを可能にする。中核となる仕組みは三つの設計原理に基づく。(1) レピュテーションデータの読み取りは安価だが書き込みには検証可能な労力を要する非対称なコスト構造、(2) 一貫性ハッシュ法に基づく非決定論的な検証者選定プロトコルであり、急進的な主張には反復コストの逓増を通じて価格を付ける、(3) 市場主導のレピュテーション権威モデルであり、私的検証者が自ら裏書きする主張の正確さに自身の蓄積したレピュテーションを賭ける。結果として得られるアーキテクチャは、中央的な調整なしに創発的なメリトクラシーを生み出し、既存の国家管理システムからの段階的で可逆的な移行経路を可能にする。

1 はじめに

1.1 中央集権的信頼の問題

現代の統治は、ある根本的な前提の上に成り立っている。すなわち、中央集権的な制度が、大規模に見知らぬ者同士の信頼を仲介できるという前提である。裁判所は紛争を裁く。登記所は所有権を証明する。規制機関は基準を執行する。これらの制度は、情報が乏しく、通信が遅く、中央機関への権限委譲が唯一実行可能な調整メカニズムであった時代に設計された。しかし中央集権的統治は、中央計画と同じ構造的理由で失敗する。すなわち、情報の非対称性、欠落したフィードバックループ、そして意思決定者がその決定の帰結から切り離されていることである。

この前提は、例えば制度的仲介のコストが紛争の価値を上回るときに破綻する。借りているアパートに、法律で義務付けられた電気安全証明書——生命に直接の危険をもたらす状態——が欠けていることに気づいた賃借人を考えてみよう。契約を解除する賃借人の法的権利は明白である。しかしその権利を裁判制度を通じて執行するコストは、法定の補償の可能性を含めてもなお、敷金や賠償として支払われるべき金銭的価値を上回る [1]。合理的な対応は、損失を受け入れて手を引くことである。

これは病理的な例外的事例ではない。害が現実であるにもかかわらず、金銭的な争点が制度的執行が経済的に合理的となる閾値を下回るような、無視できない一群の紛争にとって、これはデフォルトの経験である。その結果として生じるのは、悪意ある行為者を構造的に優遇するシステムである。この閾値を下回る規模で他者に害を与える者は、正義を求めるコストが被害者側に降りかかるため、咎めを受けずに行動できる。

上記の例は、著者の法的環境——チェコの大陸法体系——から引いたものである。他の法伝統——判例に基づくコモンロー、慣習法、混合法体系——では、正義はその法域の文化的・手続き的特殊性に応じて、異なる仕方で、異なる程度に失敗する。読者はおそらく自身の文脈から同等の例を思い浮かべることができるだろう。構造的に普遍的なのはそのパターンである。すなわち、その価値が経済的に合理的な執行の閾値を下回る紛争は、損失が被害者に吸収されて終わる。RSN は完全な正義を約束するものではない。ただ、制度的執行が非経済的なときに悪意ある

行為者が享受する構造的優位を減じるだけである。

1.2 既存の解決策が不十分な理由

分散型アイデンティティ（DID）フレームワーク [2] は、自己主権的なアイデンティティ管理のための暗号学的メカニズムを提供するが、主にアイデンティティの検証に焦点を当てており、行動的レピュテーションというより広い問題には取り組んでいない。

ソウルバウンド・トークン（SBT） [3] は、レピュテーションが譲渡不可能であるという洞察を捉えているが、スケーラビリティの制約を伴うブロックチェーン基盤に依存しており、情報の登録を統べる経済的インセンティブには取り組んでいない。メリットトークン（例：Liberland）のような関連概念も同様の哲学を共有するが、特定の法域のフレームワークに縛られたままである。

分散型自律組織（DAO） [4] は、スマートコントラクトを通じて統治を実装するが、影響力が資本に比例するというプルートクラシー的な力学を再現してしまう。二次投票 [5] はこれを部分的に緩和するが、実際的な普及を制限する。DAO はまた、根本的なオラクル問題にも直面する。スマートコントラクトは信頼できる外部ソースなしに現実世界の状態を確実に検証することができず、この問題はブロックチェーン・アーキテクチャの内部に一般的な解決策を持たない。

分散化、検閲耐性、仮名性、検証可能な参入コスト、そして創発的合意を兼ね備えた既存のシステムは存在しない。

1.3 貢献

本論文は以下の貢献を行う。

1. DID フレームワークを拡張して双方向のレピュテーション交換を支える分散型プロトコルである**レピュテーション・ソーシャルネットワーク（RSN）**の定義。
2. 一貫性ハッシュ法 [6] に基づく**非決定論的検証者選定プロトコル**。
3. 主張をネットワーク合意からの距離に応じて、三つの複合するコストチャネルを通じて価格付けする**高価な急進主義の原理**。
4. 虚偽の裏書きが正当な手数料よりも壊滅的に高くつく非対称なインセンティブを持つ**信頼できる権威モデル**。
5. 並行する財政インフラを通じた**段階的な移行経路**。

2 設計原理

RSN のアーキテクチャは、五つの譲れない設計原理によって制約される。

継続性と進化。 システムは、不定の長さの移行期間の間、既存の制度と共存する。移行はあらゆる段階で可逆でなければならない。

自発性と責任。 参加は自発的だが、自発性は責任と結びついている。制度的機能に対する管理を引き受ける参加者は、同時にそれに付随する義務を引き受ける。

多様性と文化的中立性。 合意は、システム設計者が課す既定のルールからではなく、双方向の相互作用から創発する。

レジリエンスと検閲耐性。 ネットワークを検閲するコストは、それを許容するコストを上回らねばならない。完全な全体主義——破滅的な政治的・経済的コストを払ってのみ——だけが、このシステムを抑圧できる。

合意と執行。 システムは、人間の卑小さ、悪意、報復的満足への傾向を、荷重を担う機能として取り込む。不正行為は禁じられるのではなく、価格を付けられる。

3 システム概観

3.1 レピュテーション・ソーシャルネットワーク

RSN は、参加者が現実世界の行動に関する検証可能な情報を交換する、分散型のピアツーピア通信レイヤーである。その本質的な特性は次のとおりである。分散的で検閲不能な基盤、DID を通じた仮名参加、非対称なコスト構造（読み取りは安価、書き込みは高価）、暗号学的な検証可能性、そして**標準規格のサポート**——ネットワークを通じて伝播する情報のための、権威が提供するサービス（主張の構成、裏書き、証人サービス）のための、そして相手方レピュテーションを評価するルールやポリシー不一致（宣言された行動と実際の行動の間）のリスクを査定するルールを含むポリシー形式のための、機械可読な形式である。

3.2 アーキテクチャ構成要素

RSN は四つの主要な構成要素から成る（図 1）。

1. **DID レイヤー。** 宣言されたルール、レピュテーションのメタデータ、ネットワークルーティングを備えた参加者のアイデンティティ。

2. **主張プロトコル。**現実世界の出来事に関する言明を公開するための構造化された形式。
3. **検証ネットワーク。**一貫性ハッシュ法を用いて検証者を割り当てる分散型プロトコル。
4. **レピュテーション集約レイヤー。**人間が読める形のレピュテーション要約を生成するサービス。

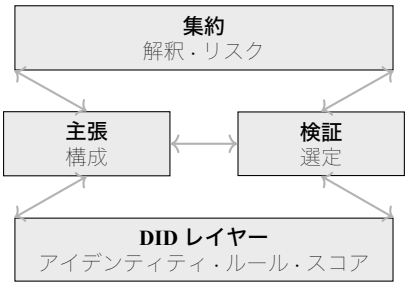


Figure 1: RSN の四層アーキテクチャ。

3.3 参加者の役割

検証トランザクションは、最大で六つの異なる DID の役割を含む（図 2）。**発行者**（DID_I、主張を作成し提出する）、**対象**（DID_S、主張がそれについてのものである DID——発行者と一致することもある）、**権威**（DID_A、手数料と引き換えに主張を裏書きする。証人サービスを提供することもある——任意）、**証人**（$DID_{W_{1..n}}$、チャレンジコードを介して検証者の誠実さを匿名で監視する——任意）、**検証者**（DID_V、主張を公開するためアルゴリズム的に選定される）、そして **RSN**（検証済みの主張が公開されるネットワーク）である。いずれの役割も別の DID に委任できる（第 7.4 節）。権威は一般に裏書きと証人サービスを束ねて提供するが、この二つの機能は論理的に独立している。

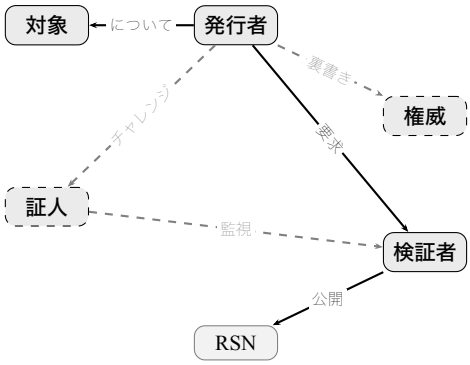


Figure 2: 検証トランザクションにおける DID の役割。破線＝任意（権威、証人）。

3.4 腐敗不能性：四つの力

RSN の腐敗不能性は、単一のメカニズムからではなく、四つの並行する力から生じる。いずれもそれ単独では十分でない。それらの組み合わせだけが、腐敗の試みを経済的に不合理なものにする。

予測不能な標的。各主張の検証者は、一貫性ハッシュ法を通じて非決定論的に選定される（第 5.3 節）。攻撃者は、賄賂のために特定の検証者を事前に標的にすることができない。なぜなら検証者の身元は、発行者の選択ではなく、主張の内容と過去の反復の関数だからである。

レピュテーションのレバレッジ——上りは遅く、下りは速い。レピュテーションは、持続的で一貫した行動を通じて、少しずつしか得られない。しかし単一の不正な裏書きで壊滅的に失われうる（第 6.2 節）。この非対称性は、何年もかけて蓄積したレピュテーションが一つの不誠実な裏書きで破壊されうることを意味する。最適な戦略は、疑わしい主張を拒絶し続けることである。

公的な約束。すべての DID 保有者は、自らのポリシー——遵守を誓う機械可読なルールの集合——を公に宣言する。宣言と実際の行動との乖離は検出可能であり、根底にある違反よりも重いレピュテーション上の罪として価格を付けられる（第 7.3 節）。したがって偽善は、直接的な不誠実さよりも高くつく。

メッシュ攻撃コストの非対称性。ネットワークを検閲または不安定化させるコストは、ネットワークの規模と密度とともに非線形に増大する一方、それを許容するコストは一定のままである。検閲が割に合うためには、中央集権的な行為者はそれをネットワーク全体に適用しなければならず——どんな考えうる利益にも見合わない措置を必要とする（第 10 節）。

4 分散型アイデンティティモデル

4.1 特別な性質を持つ DID

RSN は W3C DID Core 仕様 [2] を次のもので拡張する。**宣言されたルール**（機械可読な行動的コミットメント）、**レピュテーションのメタデータ**（集約された行動スコア）、そして**ネットワークルーティング**（安定したリング上の位置とは別の、可変のオニオンゲートウェイ）。

4.2 主張のライフサイクル

主張は六つの段階を経て進行する（図 3）。構成、任意の権威による裏書き、一貫性ハッシュ法による検証者選定、検証の判断（受理、または反復を伴う拒絶）、公開、そして全当事者のレピュテーション更新である。

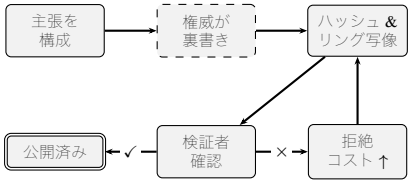


Figure 3: 反復ループを伴う主張のライフサイクル。

4.3 W3C DID Core との関係

RSN のアイデンティティモデルは、W3C DID Core 仕様 [2] の真の上位集合である。すべての RSN の DID は有効な W3C の DID である。RSN 固有の拡張は、専用の DID メソッド仕様で定義される DID ドキュメントのプロパティとして符号化され、ION [7] や Ceramic [8] のような既存の基盤と互換性がある。

5 情報の検証と伝播

5.1 情報の参入コスト

RSN の中核的な経済原理は、読み取りと書き込みの間の非対称性である。レピュテーションデータの読み取りは、DID ネットワークの一部でありレピュテーションに見合ったアクセスを持つ参加者にとって、限界コストがゼロに近づく——新参者はより広いアクセスを徐々に獲得しなければならない（アンチ・リーチングを参照）。書き込み——一回限りの技術的行為ではなく、レピュテーションのネットワークへの持続的な実体化として理解される——は、三つの次元にわたる検証可能な累積的投資を要する。**時間**（一貫した行動、果たされた約束、育まれた関係に費やされた人生の年月）、**エネルギー**（誠実な取引、提携への配慮、長期的な信頼性に投じられた労力）、そして**金銭**（自らの名への投資——専門的な研鑽、仕事の質、引き起こした害への賠償）である。レピュテーションは即座に購入できない——それは生涯にわたる蓄積の成果であり、システムはそれを可視化し、文脈を越えて移転可能にするにすぎない。プロトコルの一回限りの技術的コスト（暗号署名、検証者手数料）は、この根底にある投資と比べれば無視できる。

5.2 ソーシャルグラフと接触の深さ

RSN は根本的にソーシャルネットワークである。各 DID は、接続を許可した接触者（他の DID）を追加する。これらの接触者には彼ら自身の接触者があり、以下同様に続く。アルゴリズム的な検証者探索は、連結された接触者の設定可能な深さ h の範囲内で作動する（例：$h = 3$ の場合、直接の接触者、その接触者、そして接触者の接触者）。このアーキテクチャは単一のグローバルなブロックチェーンを必要とせず——他のコミュニティへの重なりを持つコミュニティ／クラスターの創発を自然に促す。すべての DID 参加者は、受信した要求をどう評価するかを統べる機械可読なルールの集合である**ポリシー**を公開していなければならない。ポリシー違反は負の成果物としてネットワークに記録される。

5.3 アルゴリズムによる検証者選定

検証プロトコルは一貫性ハッシュ法 [6] を用いる（図 4）。検証は有料サービスである。検証者は手数料と引き換えに稼働し、競争が価格、速度、信頼性を推し進める市場を生み出す。

ステップ 1。主張ドキュメントは、前回の反復のハッシュ結果（最初の反復では $\varnothing$）と連結され、ハッシュ化される。

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

アルゴリズムは、単なる前回の反復のハッシュではなく、過去のすべての要求と応答の完全な経路を含めなければならない。各検証者の完全な応答（受理、拒絶、提示価格、理由）は増大するドキュメントに付加され、各ステップで暗号署名を通じて検証可能である。

ステップ 2。ハッシュは、一貫性ハッシュリング上の N 個の位置に、均等に分散して写像される（例：$N = 4$ の場合、$+0°, +90°, +180°, +270°$）。各位置から、時計回りの探索が最も近い DID を検証者候補として選定する（図 5）。N は可変のパラメータであり、現在アクティブな DID の割合、時刻、あるいは過去のネットワーク応答性に依存しうる。

ステップ 3。検証者は受理する（公開し、レピュテーションを賭ける）か、拒絶する（拒絶ハッシュとともにステップ 1 へ戻る）。あるノードがオンライン状態を宣言しているにもかかわらず応答しない場合、次の要求には N 個すべての過去の検証者候補からの応答をすべて含めなければならない。

アンチ・リーチング。標的となる DID は、レピュテーションのほとんどない新規 DID からの

照会に対して、手数料やアクセス制限を設けることができる。この段階的な（二値ではない）メカニズムは、新参者に、他者のデータを自由に消費する前に、真正な活動を通じてレピュテーションを築くことを強いる。

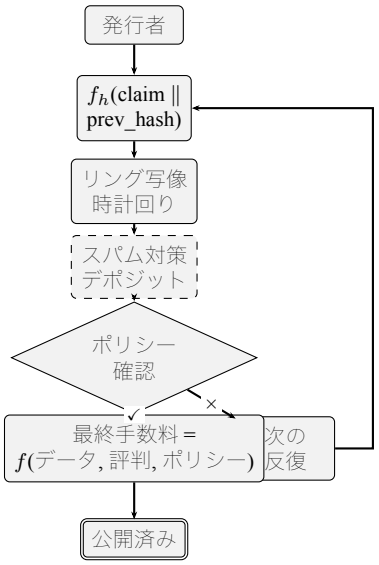
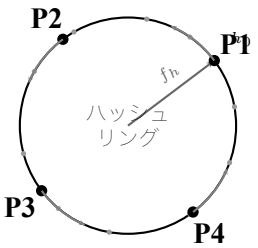


Figure 4: 検証者選定プロトコル。スパム対策デポジットは任意であり、返金可能な場合がある。最終手数料は受理時にのみ支払われる。

各拒絶は、検証者の完全な応答（理由と条件を含む）を主張ドキュメントに付加し、その内容を拡張する。拡張されたドキュメントから、新しいハッシュが非決定論的に計算され、異なるリング位置に写像されて、異なる検証者を選定する。完全な経路の文書化は必須である——発行者は次の検証者を予測したり影響を与えたりできない。ある検証者が、互換性のある宣言されたポリシーを持ちながら要求を無視した場合、証人（存在すれば）はこれを記録し、発行者は最終公開の際に証人による証拠を添付できる。



$h_0 = f_h(\text{claim})$、次に $+0°, +90°, +180°, +270°$
各点 → 時計回りの探索

Figure 5: 多点選定（N=4）。ハッシュ h_0 がオフセットを定める。h_0 から均等に分散した 4 点。

5.4 証人プロトコル

証人の役割は、暗号学的なチャレンジコード・プロトコルを通じて、検証者の誠実さに対する匿名の説明責任を提供する。

ステップ W1。要求者は検証要求に署名し、それを N_w 人の証人——要求者のソーシャルネットワークからの接触者、または手数料と引き換えに稼働する専門の証人サービス提供者——に送る。

ステップ W2。各証人 w_i は署名済みの要求全体に署名し、元の署名 σ_i を保持し、チャレンジコード $c_i = h(\sigma_i)$ を計算する。チャレンジコードは要求に付加される。

ステップ W3。N_w 個のチャレンジコードを帯びた要求は、検証者に送られる。検証者はコードを観察するが、誰が証人であるか、あるいはコードが実際の署名に対応しているかを判別できない。

ステップ W4（誠実な検証者）。検証者が宣言したポリシーに従って応答すれば、チャレンジコードは不透明なままである。証人が明かされることはない。追加のデータは公開されない。

ステップ W5（ポリシー違反）。検証者がポリシーに違反した場合（要求を無視する、一貫性のない応答をする）、要求者は証人の元の署名 σ_i を保持している。これらは付随データとして公開できる。誰でも $c_i = h(\sigma_i)$ を検証でき、証人が居合わせたことを証明する。要求者は独立して公開できる——検証者は既に応答の中でチャレンジコードに署名しているからである。

ブラフの性質。要求者は、一部またはすべてのチャレンジコードをランダムな値で置き換えてよい。検証者は、真正なコード（高いレピュテーションを持つ権威に裏打ちされたもの）を雑音から区別できない。この不確実性こそが執行のメカニズムである。すべての要求は、尊敬される権威が匿名で見張っているというリスクを帯びる。この圧力を維持するコストはほぼゼロ（乱数の生成）である一方、検証者にとって不誠実であることの潜在的コストは壊滅的である。実際の証人が不在であっても、誠実な行動が動機づけられる。

証人としての権威。主張を裏書きする権威は、証人サービスを束ねて提供してよい。「あなたの主張を裏書きし、検証中は匿名の証人として仕えます」。これは自然なビジネスモデルである——権威は既に文脈を持っている。ただし、この二つの役割は論理的に独立している。

5.5 高価な急進主義の原理

三つのコストチャネルが同時に複合する（図 6）。

チャネル 1：反復コスト。各拒絶は、時間と資源を消費する新たな反復を強いる。線形の増加。

チャネル 2：ドキュメントの肥大化。各反復は、検証者の完全な応答を主張ドキュメントに追加する。増加は線形だが、基準となるオフセットを伴う。初期のペイロード（主張の内容、権威の裏書き、暗号署名）は既に無視できない大きさ B_0 を持つ。k 回の反復後の総サイズは $S(k) = B_0 + k \cdot \Delta$ であり、Δ は平均的な応答サイズである。

チャネル 3：検証者のリスクプレミアム。リスクは主観的である。検証者は、要求する DID の宣言されたポリシーが、検証者自身の商業的、社会的、政治的な利害と衝突するかを評価する。プレミアムは、検証者の「理想」からの知覚された距離とともに指数関数的に逓増しうる。$P(d) = \alpha \cdot e^{\beta d}$ であり、d は検証者の主観的な距離の尺度である。個人的な禁止境界を越えると、検証者は完全に拒否してもよい。

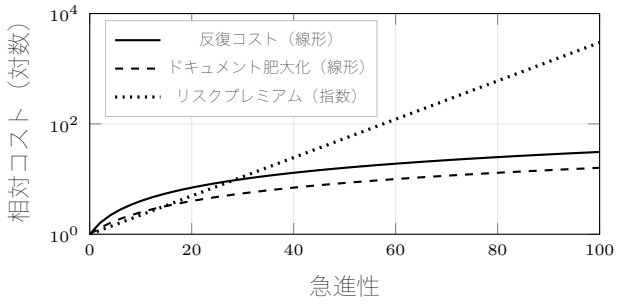


Figure 6: 三つのチャネルにわたるコストの逓増。急進性が高いところではリスクプレミアムが支配的となる。

決定的に重要なのは、これは検閲ではないということである。いかなる主張も禁じられない。システムはリスクに価格を付ける（表 1）。

Table 1: 主張の種類ごとのコスト比較。

種類	反復	ドキュメント	手数料	合計
信憑性が高い	$k_{\min}$	B_0	$P_{\min}$	低
論争的	k_{med}	$B_0 + k\Delta$	$\alpha e^{\beta d}$	中程度
急進的	$k_{\max}$	$\gg B_0$	$\gg P_{\min}$	極めて高
不正	$\to \infty$	—	—	公開不能

6 レピュテーションとリスク評価

6.1 レピュテーション蓄積モデル

レピュテーションは三つの性質を示す。**緩やかな蓄積**（一貫した行動を通じた漸増的な成長）、**急速な破壊**（単一の不正がスコアを壊滅的に低下させうる）、そして**個別の評価**（消費する各当事者が自身の集約関数を適用できる）である。

6.2 信頼できる権威

信頼できる権威は主張を審査し、納得すれば、自身のレピュテーションを賭けて共同署名する（図 7）。この非対称性は設計によるものである。レピュテーションを得るのは遅く（誠実な裏書きごとに漸増的な $+\delta$）、失うのは壊滅的である（虚偽の裏書きごとに $-\Delta \gg \delta$。例示的には、例えば $+2\%$ に対して -70%）。最適な戦略は常に疑わしい主張を拒絶することである。δ と Δ の具体的な値はシステムパラメータである。

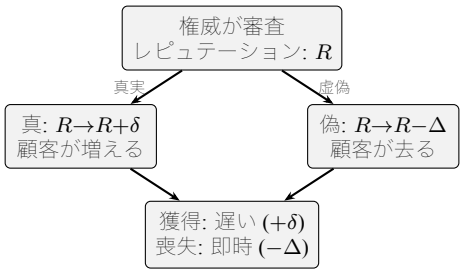


Figure 7: 信頼できる権威——非対称なインセンティブ。

6.3 多次元レピュテーション

レピュテーションはスカラーではなく、複数の次元にわたるベクトルである。財務的信頼性、個人的な誠実さ、専門的能力、市民的関与、その他である（図 8）。異なる評価提供者は、文脈に応じてこのベクトルを異なる仕方で射影する——貸し手は財務的信頼性を、雇用主は専門的能力を、隣人は市民的行動を優先する。唯一の「正しい」レピュテーションスコアは存在せず、視点があるのみである。

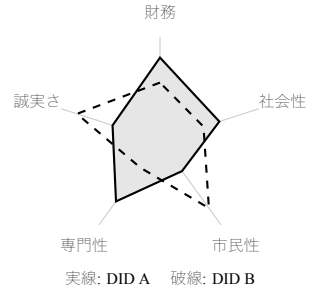


Figure 8: 多次元レピュテーションのベクトル。異なる DID は、次元にわたって異なるプロファイルを示す。

6.4 民主化されたリスク評価

RSN は、体系的なリスク評価——現在は金融機関に集中しているが、銀行業をはるかに超えて適用可能な能力——を民主化する。サプライヤーの信頼性を査定する産業コングロマリット、行動的リスクに価格を付ける保険会社、合併・買収のためのデューデリジェンス、製造業における設備寿命の推定——相手方リスクの査定が必要とされるあらゆる場面で、RSN は分散的で市場主導の代替案を提供する。解釈サービスの市場が、生の多次元レピュテーションデータを実行可能な要約へと翻訳し、相手方の評価をあらゆる参加者が限界コストで利用できるようにする。

7 合意と紛争解決

7.1 分散型の正義モデル

RSN は正義を双方向の交渉問題として捉え直す。永続的で検証可能なレピュテーション毀損の脅威は、被害者が費用を負担できない法的手続きよりも効果的な抑止力となる。

7.2 創発的合意

各参加者は個人的な満足の閾値を保持する。ネットワークの総体的な合意は、何千もの双方向交渉の統計的平均として創発する（図 9）。合意をはるかに上回る応答（野蛮）は、公開するのが高価である。合意に近い応答（釣り合いの取れた）は安価である。合意はルールではない——それは価格シグナルである。

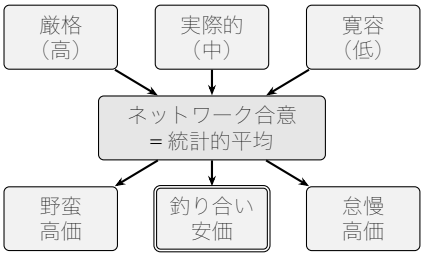


Figure 9: 個人の満足閾値からの創発的合意。

7.3 懲罰の較正

各 DID 保有者は、特定の不正行為カテゴリーへの応答を公に宣言する。不釣り合いに厳しい、あるいは甘い宣言は、負のレピュテーションシグナルを引き寄せる。釣り合いの取れた宣言は摩擦なく受け入れられる——自己較正する懲罰システムである。

合意に沿った宣言もまた偽善検出の対象となる。合意された立場に宣言的にコミットしながら、それと一貫しない振る舞いをすることは、意図的な欺瞞を示すため、根底にある逸脱よりも重いレピュテーション上の罪を構成する。

7.4 委任

DID 内のすべての活動は——一つの例外を除いて——別の DID に委任できる。**対象の役割——主張がその行動についてのものである DID——は委任できない。それは、主張が指し示すアイデンティティ保有者に、譲渡不可能に結びついている。**他の能動的な役割——発行者、権威、証人、検証者——は、検証、主張の提出、合意への参加、紛争解決のいずれのためであれ、指定された受任者 DID に移譲できる。委任はいつでも取り消せる。これは（例えば専門的な検証サービスのような）専門化を可能にする一方、保有者は最終的な管理と責任を保持する。委任はシステム全体にわたって適用され、スケーラビリティに不可欠である。

7.5 個人の道徳から創発的な社会契約へ

各 DID の宣言されたポリシーは、個人の道徳の形式化を表す。保有者が何を許容できると考えるか、特定の行動にどう応答するか、相手方に何を求めるか、である。これらのポリシーはシステム設計者によって課されるものではない——各参加者によって選ばれ、機械可読な形で表現される。

この形式化は三段階の創発を可能にする。第一に、個人の道徳が**ポリシー**——DID が遵守を誓う、宣言されたルール、閾値、応答関数の集合——として符号化される。第二に、ネットワーク全体にわたるすべてのポリシーの総体が**創発的倫理**——単一の参加者が設計したのではなく、何千もの個人の道徳的立場の相互作用から生じる、統計的に観察可能な規範——を生み出す [9]。第三に、双方向の価格シグナルを通じて執行される共有された行動規範として表現されるこれらの創発的倫理は、**測定可能な社会契約**——誰も署名していない理論的構築物 [10] ではなく、実際の行動に裏打ちされた経験的に観察可能なルールの集合——を構成する。

この過程は、道徳基盤理論 [11] からの知見を映し出す。人間の道徳は直観的で、多元的で、文化的に多様である。RSN は道徳的合意を入力として要求しない。それは行動的合意を出力として生み出す。結果として得られる社会契約は静的ではない——参加者が加わり、去り、ネットワークからのフィードバックに応じてポリシーを

調整するにつれて進化する。古典的な社会契約論とは異なり、この契約は取り消し可能で、観察可能で、主権者なしに執行可能である。

8　経済モデル

先行する諸節は、あるツール——RSN の検証メカニズム、コスト構造、創発的合意——を記述した。本節は、このツールを財政と統治の移行に適用するための方法論を記述する。ツールは汎用であり、以下の方法論はその一つの可能な適用にすぎない。

8.1　インセンティブ構造

資本としてのレピュテーションは、誠実な行動への直接的なインセンティブを生み出す。通常の運用では、参加者は日常の取引と果たされた約束を通じて自然にレピュテーションを築く。主たる支出は負の主張——他者が与えた害の記録——にある。この非対称性は、有用で信頼できる行動を動機づける。誠実であることに追加コストはかからない一方、有害であることは、他者が保存のために対価を払う文書化された足跡を作り出す。偽善——ルールを宣言しながらそれに従わないこと——は最も高くつく失敗様式である。意図的な欺瞞を示すからである。

8.2　並行する財政システム

三つの構成要素が競争圧力を可能にする。(1) **シンプル税**——例外のない単一の比例税率であり、当初は既存の実効税率をわずかに下回る。(2) **電子支出登録（ESR）**——チェコの EET モデルを反転させ、市民が国家の支出を監視する。(3) **市民主導の税配分**——初年度は数パーセントから始まり、10 年後には、普及の速度に応じて、10 パーセント台前半から市民主導システムへの完全な移行まで、どこにでも到達する。実際のテンポは、国家サービスへの自由市場の代替案が出現する速度と、移行に協力しようとする国家の意欲に依存する。時間の関数は線形である必要はなく、普及が最終的にどこまで到達しうるかについて上限を設ける理由はない。

9　移行経路

移行は三つのフェーズを経て進行する（図 10）。**フェーズ 1：オーバーレイ**（RSN は情報レイヤーとして機能し、国家が唯一の提供者）、**フェーズ 2：競争**（RSN は機能的な代替案を提供し、二重システムの利用）、そして**フェーズ 3：移行**（RSN が国家の同等物を凌駕し、自発的な移行）である。移行はあらゆる段階で可逆である。

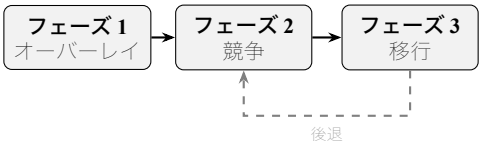


Figure 10: 三段階の移行——あらゆる段階で可逆。

主たる圧力メカニズムは財政的なものである。条件付き納税者が「経済的に意味のある少数派 X」——それに対する弾圧が無視できない経済的損害を引き起こし、市民的不服従が信憑性のある脅威となるほど大きな集団——に達すると、国家は交渉に入る。例示のために $X \approx 15\%$ の GDP を用いるが、実際の閾値は個別の経済に依存する。

10　セキュリティ分析

我々は五つの敵対者カテゴリーを考える。個人の悪意ある行為者、組織された集団、企業の敵対者、国家レベルの敵対者、そしてプロトコルレベルの敵対者である。

シビル耐性 [12]。レピュテーションを築くには、持続的で検証可能な相互作用を要する。シビル攻撃を成功させるコストは、偽のアイデンティティの数に比例して線形に、標的とするレピュテーションの水準に比例して二次的に増大する。複数の DID を並行して運用することは可能だが、設計上高価である——各アイデンティティは、真正な活動を通じて独立にレピュテーションを蓄積しなければならない。自由な社会ではこのコストが軽率な濫用を抑止する。独裁下では、並行する DID は、区画化された抵抗、地下での調整、より安全な闇市場のナビゲーションを可能にする生存のための道具となる。

共謀への防御。閉じた集団内での相互裏書きのパターンは、ソーシャルグラフ分析を通じて検出可能である。レピュテーション集約関数は、密にクラスター化したソースからの主張を割り引く。

国家レベルの敵対者。オニオンルーティング、中央集権的な基盤の不在、そして検証者の役割の参加者基盤全体への分散が、抑圧にはどんな利益にも見合わない措置を要することを保証する。

プライバシー対説明責任。仮名性——匿名性とアイデンティティ開示の中間——は、保有者の現実世界のアイデンティティを明かすことなく、

DID が意味のあるレピュテーションを蓄積することを可能にする。

11 プライバシーへの配慮

RSN のプライバシーモデルは仮名性の上に構築されている。保有者はアイデンティティの開示を制御する。最小限（純粋な仮名）、選択的（特定の資格情報の紐付け）、または完全（法的アイデンティティの関連付け）である。公開された主張は永続的である——システムは文脈的な訂正を支えるが、消去は支えない。保有者は、危殆化した DID を放棄して新たに始めることができるが、蓄積したレピュテーションは失われる。

12 関連研究

W3C DID Core 仕様 [2] と Ceramic Network [8] は、アイデンティティの基盤を提供する。EigenTrust [13] は、中央的な権威なしに分散型のレピュテーション集約を実証した。SBT [3] は、譲渡不可能なソーシャルトークンを導入した。RSN は、品質フィルターとしての経済的コストへの重点と、急進主義に価格を付けるそのメカニズムにおいて異なる。

DAO [4] と二次投票 [5] は、分散型統治の実現可能性を実証した。RSN は、投票ではなく双方向の価格交渉から合意を導く。

本提案は、私的なサービス提供についてアナルコ・キャピタリズム理論 [14, 15] に依拠するが、二つの決定的な点で異なる。合理性を仮定するのではなく悪意や報復衝動を設計に織り込むこと、そして革命ではなく段階的な移行を提案することである。創発的な社会契約という概念は、ハイエクの自生的秩序の理論 [16] に先例を持つ。

アナルコ・アゴリズム。 RSN は、アゴリスト的な対抗経済 [17]——とりわけ並行する制度と自発的交換の構築への重点——と大きな共通の基盤を共有する。しかしアゴリズムは、合理的な自己利益を十分な調整メカニズムとして仮定する傾向があり、しばしば既存の国家構造からの具体的な移行経路を欠く。RSN は、非合理的な行動的傾向を明示的に取り込み、段階的な移行のための財政的圧力メカニズムを提供する。

メリトクラシー。 RSN は、メリトクラシー [18] がスローガンではなく体系的な性質としてどのように創発しうるかについての、最初の機能的な記述を表しているかもしれない。伝統的なメリトクラシー的システムは、「メリット」を定義し執行する中央的な権威を要するために失敗する。RSN では、メリットは双方向の評価から創発する。価値を提供する者がレピュテーションを蓄積し、誰にメリットがあるかを委員会が決めることはない。

特権としての所有。 RSN は、所有権を自然かつ絶対的なものとして扱うアナルコ・キャピタリズムやオーストリア学派の取り扱いから根本的に離れる。RSN のフレームワークでは、所有は特権——参加者が共有された規範を根本的に侵害するとき（裏切り、存亡の危機における共同体防衛の拒否、体系的な搾取）、極端な場合には共同体によって撤回されうる社会的承認——である。これは国家による収用ではなく、双方向の関係のネットワークによる社会的承認の撤回である。

13 議論と限界

コールドスタート。 RSN の価値はネットワーク効果に依存する。早期の採用者は、参加が閾値に達するまで限られた価値に直面する。しかし初期段階からでも、DID ネットワークは有用な補助的情報源として機能する。早期のレピュテーション評価と権威の査定は、洗練の度合いを増しながら徐々に発展すると予想される。

アンチ・リーチングとアクセス制御。 標的となる DID は、低レピュテーションの DID からの照会に段階的な手数料とアクセス制限を課すことができる。これは二値ではなく連続的な尺度である。照会する DID のレピュテーションが低いほど、受け取る情報は少なく、待つ時間は長く、支払う額は多くなる。このメカニズムは、受動的な消費よりも真正な参加を動機づける。

アクセスの不平等。 主張を公開するコストは、経済的に不利な立場にある参加者の正当な苦情を濾し取ってしまうかもしれない。緩和策：すべての参加者は同時に潜在的な検証者として機能し（あるいはこの役割を委任し）、検証手数料を得る。十分な時間の地平にわたれば、急進的でない参加者は財務的な中立——検証収入がおおよそ公開コストを相殺する——に近づくはずである。これは統計的な期待であり、保証ではない。

レピュテーションの不平等。 早期の採用者は、後続者にとって障壁を生みうる優位を蓄積する。しかしレピュテーションの評価は第三者の提供者によって行われ、彼らはその集約アルゴリズムを通じて先行者の優位を緩和することを選べる。良いレピュテーションを最初に持つことは正当な比較経済的優位であり——それは設計によるものである。

未解決の問題。 最適なコスト関数、集約の標準、プロトコルの統治、そして AI が生成する合

成レピュテーションデータとの相互作用は、今後の研究領域として残されている。

本論文は、RSN があらゆる状況で最適な結果を生み出すと主張するものではない。それが主張するのは、RSN が実現可能な代替案——技術的に実装可能で、経済的に自立し、人間の行動的傾向とありのままに社会的に両立する——を表しているということである。

14 結論

本論文は、仮名で検証可能なレピュテーション交換を可能にする分散型プロトコルであるレピュテーション・ソーシャルネットワークを提示した。高価な急進主義の原理は、不正な主張が検閲なしに価格によって排除されることを保証する。提案された移行経路は、既存の制度からの段階的で可逆的な移行を可能にする。この設計は、人間の本性をありのままに——卑小さ、悪意、報復的満足への欲求を含めて——取り込み、イデオロギー的な変容を要求しない。結果として得られるのはユートピアではなく、正義が手の届くものであり、レピュテーションが獲得されるものであり、不正行為のコストがそれを引き起こした当事者によって負われるシステムである。

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.