Réseau de réputation décentralisé : Un cadre pour une organisation sociétale naturelle

Pavel Kudrna
Prague, Czechia
Draft v1 — March 2026

Abstract

Le sens de la justice—la conviction que les torts sont réparés et que le mérite est récompensé—est la force cohésive la plus puissante de la société. Lorsque les institutions centralisées de gouvernance ne parviennent pas à procurer ce sentiment parce que le coût de faire valoir un droit dépasse la valeur du droit lui-même, la cohésion sociale s'érode. Les structures institutionnelles actuelles échouent à résoudre une classe importante de litiges de la même manière systématique que la planification centralisée échoue à allouer les ressources : par asymétrie d'information, absence de boucles de rétroaction et déconnexion des décideurs des conséquences de leurs décisions. Cet article présente un Réseau social de réputation (RSN) : une couche de communication décentralisée, incorruptible et résistante à la censure, bâtie sur des Identifiants décentralisés (DID), qui permet à des participants pseudonymes de publier, de vérifier et de consommer des informations de réputation sur des comportements réels. Le mécanisme central repose sur trois principes de conception : (1) une structure de coûts asymétrique où la lecture des données de réputation est peu coûteuse mais l'écriture exige un effort vérifiable ; (2) un protocole non déterministe de sélection des vérificateurs fondé sur le hachage cohérent qui tarifie les affirmations radicales par des coûts d'itération croissants ; et (3) un modèle d'autorité de réputation piloté par le marché, où des vérificateurs privés engagent leur réputation accumulée sur l'exactitude des affirmations qu'ils cautionnent. L'architecture qui en résulte produit une méritocratie émergente sans coordination centrale et rend possible une voie de migration graduelle et réversible depuis les systèmes actuels administrés par l'État.

1 Introduction

1.1 Le problème de la confiance centralisée

La gouvernance moderne repose sur une hypothèse fondamentale : que des institutions centralisées peuvent médiatiser la confiance entre inconnus à grande échelle. Les tribunaux tranchent les litiges. Les registres certifient la propriété. Les organismes de régulation font respecter les normes. Ces institutions ont été conçues à une époque où l'information était rare, la communication lente et la délégation de l'autorité à un organe central le seul mécanisme de coordination réalisable. La gouvernance centralisée échoue toutefois pour les mêmes raisons structurelles que la planification centralisée : asymétrie d'information, absence de boucles de rétroaction et déconnexion des décideurs des conséquences de leurs décisions.

L'hypothèse échoue, par exemple, lorsque le coût de la médiation institutionnelle dépasse la valeur du litige. Prenons le cas d'un locataire qui découvre que son appartement loué ne dispose pas du certificat de sécurité électrique légalement requis—une situation qui met immédiatement la vie en danger. Le droit légal du locataire de résilier le contrat est sans ambiguïté. Pourtant, le coût de faire valoir ce droit par voie judiciaire dépasse la valeur monétaire du dépôt de garantie et des dommages dus, même en incluant une éventuelle indemnisation légale [1]. La réponse rationnelle est d'absorber la perte et de partir.

Ce n'est pas un cas marginal pathologique. C'est l'expérience par défaut pour une classe importante de litiges dans lesquels le préjudice est réel mais où les enjeux monétaires tombent sous le seuil à partir duquel l'application institutionnelle devient économiquement rationnelle. Le résultat est un système qui favorise structurellement les mauvais acteurs : ceux qui nuisent à autrui dans des volumes inférieurs à ce seuil peuvent agir en toute impunité, car le coût de la recherche de justice retombe sur la partie lésée.

L'exemple ci-dessus est tiré de l'environnement ju-

ridique de l'auteur—le système de droit civil tchèque. Dans d'autres traditions juridiques—la common law fondée sur la jurisprudence, le droit coutumier, les systèmes mixtes—la justice échoue de différentes manières et à différents degrés, selon les spécificités culturelles et procédurales de la juridiction. Les lecteurs reconnaîtront vraisemblablement des exemples équivalents dans leur propre contexte. Ce qui est structurellement universel, c'est le schéma : les litiges dont la valeur tombe sous le seuil d'une application économiquement rationnelle se terminent par l'absorption de la perte par la partie lésée. Le RSN ne promet pas une justice parfaite—il réduit simplement l'avantage structurel dont jouissent les mauvais acteurs lorsque l'application institutionnelle n'est pas économique.

1.2 Pourquoi les solutions existantes sont insuffisantes

Les cadres d'identité décentralisée (DID) [2] fournissent des mécanismes cryptographiques pour la gestion d'une identité auto-souveraine mais se concentrent principalement sur la vérification d'identité sans traiter la question plus large de la réputation comportementale.

Les jetons Soulbound (SBT) [3] saisissent l'idée que la réputation est non transférable mais reposent sur une infrastructure blockchain soumise à des contraintes d'évolutivité et ne traitent pas les incitations économiques qui régissent l'entrée de l'information. Des concepts connexes tels que les jetons de mérite (p. ex. Liberland) partagent une philosophie similaire mais restent liés à des cadres juridictionnels spécifiques.

Les organisations autonomes décentralisées (DAO) [4] mettent en œuvre la gouvernance par des contrats intelligents mais reproduisent des dynamiques ploutocratiques où l'influence est proportionnelle au capital. Le vote quadratique [5] atténue partiellement ce phénomène mais limite l'adoption pratique. Les DAO se heurtent également au *problème de l'oracle* fondamental : les contrats intelligents ne peuvent pas vérifier de façon fiable des états du monde réel sans une source externe de confiance, et ce problème n'a pas de solution générale au sein de l'architecture blockchain.

Aucun système existant ne combine décentralisation, résistance à la censure, pseudonymat, coût d'entrée vérifiable et consensus émergent.

1.3 Contributions

Cet article apporte les contributions suivantes :

1. La définition du **Réseau social de réputation (RSN)**, un protocole décentralisé qui étend le cadre DID pour prendre en charge l'échange bilatéral de réputation.
2. Un **protocole non déterministe de sélection des vérificateurs** fondé sur le hachage cohérent [6].
3. Le **Principe du radicalisme coûteux**, qui tarifie les affirmations selon leur distance au consensus du réseau à travers trois canaux de coûts cumulatifs.
4. Un **modèle d'Autorité réputée** à incitations asymétriques où une caution mensongère coûte catastrophiquement plus cher que des honoraires légitimes.
5. Une **voie de migration graduelle** par une infrastructure fiscale parallèle.

2 Principes de conception

L'architecture du RSN est contrainte par cinq principes de conception non négociables.

Continuité et évolution. Le système coexiste avec les institutions existantes pendant une période de transition de durée indéfinie. La transition doit être réversible à chaque étape.

Volontariat et responsabilité. La participation est volontaire, mais le volontariat s'accompagne de responsabilité : un participant qui assume le contrôle d'une fonction institutionnelle en assume simultanément les obligations correspondantes.

Diversité et neutralité culturelle. Le consensus émerge d'interactions bilatérales, et non de règles prédéfinies imposées par les concepteurs du système.

Résilience et résistance à la censure. Le coût de la censure du réseau doit dépasser le coût de sa tolérance. Seul un totalitarisme intégral—à un coût politique et économique ruineux—peut supprimer le système.

Consensus et application. Le système intègre les tendances humaines à la mesquinerie, à la rancune et à la satisfaction punitive comme des caractéristiques porteuses. La faute n'est pas interdite ; elle est tarifée.

3 Vue d'ensemble du système

3.1 Réseau social de réputation

Le RSN est une couche de communication décentralisée, pair à pair, dans laquelle les participants

échangent des informations vérifiables sur des comportements réels. Ses propriétés déterminantes sont : une infrastructure décentralisée et incensurable ; une participation pseudonyme via des DID ; une structure de coûts asymétrique (la lecture est bon marché, l'écriture coûteuse) ; une vérifiabilité cryptographique ; et le **support de standards**—des formats lisibles par machine pour l'information propagée dans le réseau, pour les services offerts par les autorités (composition d'affirmations, caution, service de témoin), et pour le format de politique incluant les règles d'évaluation de la réputation d'une contrepartie et d'appréciation du risque de discordance de politique (entre le comportement déclaré et le comportement réel).

3.2 Composants architecturaux

Le RSN se compose de quatre composants principaux (Fig. 1) :

1. **Couche DID.** Identités des participants avec règles déclarées, métadonnées de réputation et routage réseau.
2. **Protocole d'affirmation.** Format structuré pour publier des assertions sur des événements du monde réel.
3. **Réseau de vérification.** Protocole décentralisé d'attribution des vérificateurs par hachage cohérent.
4. **Couche d'agrégation de réputation.** Services produisant des synthèses de réputation lisibles par l'humain.

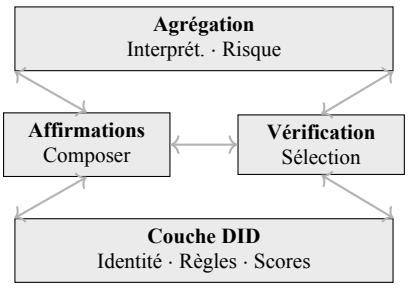

Figure 1: Architecture à quatre couches du RSN.

3.3 Rôles des participants

Une transaction de vérification implique jusqu'à six rôles DID distincts (Fig. 2) : l'**Émetteur** (DID_I, crée et soumet l'affirmation), le **Sujet** (DID_S, le DID sur lequel porte l'affirmation—peut coïncider avec l'Émetteur), l'**Autorité** (DID_A, cautionne l'affirmation contre des honoraires ; peut aussi offrir des services de témoin—*optionnel*), le **Témoin** ($DID_{W_{1..n}}$, contrôleur incognito de l'honnêteté du vérificateur via des codes de défi—*optionnel*), le **Vérificateur** (DID_V, sélectionné algorithmiquement pour publier l'affirmation), et le **RSN** (le réseau où les affirmations vérifiées sont publiées). Tout rôle peut être délégué à un autre DID (Section 7.4). Une Autorité regroupe couramment la caution et les services de témoin, mais les deux fonctions sont logiquement indépendantes.

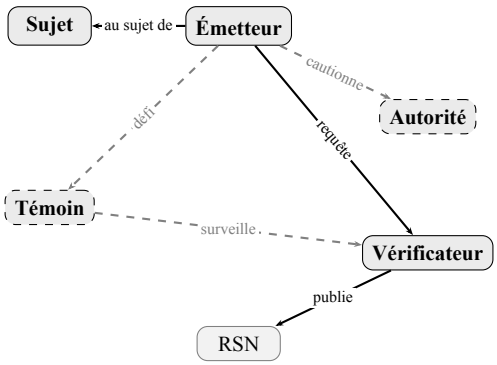

Figure 2: Rôles DID dans une transaction de vérification. Pointillés = optionnel (Autorité, Témoin).

3.4 Incorruptibilité : quatre forces

L'incorruptibilité du RSN ne découle pas d'un mécanisme unique mais de quatre forces concurrentes. Aucune ne suffit à elle seule ; seule leur combinaison rend une tentative de corruption économiquement irrationnelle.

Cible imprévisible. Le vérificateur de chaque affirmation est sélectionné de façon non déterministe par hachage cohérent (Section 5.3). Un attaquant ne peut pas cibler à l'avance un vérificateur précis pour le corrompre, car l'identité du vérificateur est une fonction du contenu de l'affirmation et des itérations précédentes, et non du choix de l'émetteur.

Levier réputationnel—lente montée, chute rapide. La réputation ne peut être acquise que progressivement, par un comportement constant et soutenu. Elle peut toutefois être perdue de façon catastrophique par une seule caution frauduleuse (Section 6.2). Cette asymétrie signifie que des années de réputation accumulée peuvent être détruites par une seule caution malhonnête ; la stratégie optimale reste de rejeter les affirmations suspectes.

Promesse publique. Chaque Détenteur de DID déclare publiquement sa politique—un ensemble de règles lisibles par machine qu'il s'engage à suivre. Toute divergence entre la déclaration et le comportement réel est détectable et tarifée comme une faute réputationnelle plus grave que la violation sous-jacente (Section 7.3). L'hypocrisie est donc plus coûteuse que la

malhonnêteté directe.

Asymétrie du coût d'attaque du maillage. Le coût de la censure ou de la déstabilisation du réseau croît de façon non linéaire avec la taille et la densité du réseau, tandis que le coût de sa tolérance reste constant. Pour que la censure soit rentable, un acteur centralisé devrait l'appliquer à l'ensemble du réseau—exigeant des mesures disproportionnées par rapport à tout bénéfice concevable (Section 10).

4 Modèle d'identité décentralisée

4.1 DID à propriétés particulières

Le RSN étend la spécification W3C DID Core [2] avec : des **Règles déclarées** (engagements comportementaux lisibles par machine), des **Métadonnées de réputation** (score comportemental agrégé) et un **Routage réseau** (passerelle onion mutable, distincte de la position stable sur l'anneau).

4.2 Cycle de vie d'une affirmation

Une affirmation traverse six étapes (Fig. 3) : composition, caution optionnelle par une autorité, sélection du vérificateur par hachage cohérent, décision de vérification (acceptation ou rejet avec itération), publication et mise à jour de la réputation de toutes les parties.

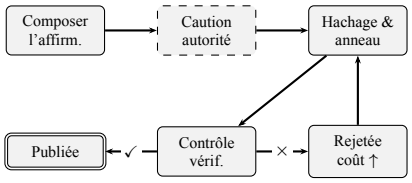

Figure 3: Cycle de vie d'une affirmation avec boucle d'itération.

4.3 Relation avec W3C DID Core

Le modèle d'identité du RSN est un sur-ensemble strict de la spécification W3C DID Core [2]. Tous les DID du RSN sont des DID W3C valides. Les extensions spécifiques au RSN sont encodées comme propriétés de document DID définies dans une spécification dédiée de méthode DID, compatible avec les infrastructures existantes telles qu'ION [7] et Ceramic [8].

5 Vérification et propagation de l'information

5.1 Coût de l'entrée d'information

Le principe économique central du RSN est l'asymétrie entre la lecture et l'écriture. La lecture des données de réputation tend vers un coût marginal nul pour les participants qui font partie du réseau DID et disposent d'un accès proportionné à leur réputation—les nouveaux venus doivent progressivement mériter un accès plus large (voir anti-parasitage). L'écriture—comprise comme la matérialisation durable de la réputation dans le réseau, et non comme un acte technique ponctuel—exige un investissement cumulatif vérifiable selon trois dimensions : le **temps** (des années de vie consacrées à un comportement constant, à des engagements tenus et à des relations cultivées), l'**énergie** (l'effort investi dans des relations honnêtes, le soin des partenariats et une fiabilité de long terme) et l'**argent** (l'investissement dans son propre nom—développement professionnel, qualité de son travail, réparation des préjudices causés). La réputation ne peut pas s'acheter instantanément—elle est le résultat d'une accumulation de toute une vie que le système se contente de rendre visible et transférable entre contextes. Les coûts techniques ponctuels du protocole (signatures cryptographiques, honoraires de vérificateur) sont négligeables comparés à cet investissement sous-jacent.

5.2 Graphe social et profondeur des contacts

Le RSN est fondamentalement un réseau social : chaque DID ajoute des contacts (d'autres DID) qui autorisent la connexion. Ces contacts ont leurs propres contacts, et ainsi de suite. La recherche algorithmique de vérificateur opère dans une profondeur configurable h de contacts liés (p. ex. $h = 3$: ses contacts directs, leurs contacts, et les contacts de ces contacts). Cette architecture ne nécessite pas une unique blockchain globale—elle favorise naturellement l'émergence de communautés/grappes avec des chevauchements vers d'autres communautés. Chaque participant DID doit disposer d'une **politique** publiée—un ensemble de règles lisibles par machine régissant la manière dont les requêtes entrantes sont évaluées. Les violations de politique sont enregistrées dans le réseau comme des artefacts négatifs.

5.3 Sélection algorithmique des vérificateurs

Le protocole de vérification emploie le hachage cohérent [6] (Fig. 4). La vérification est un service payant : les vérificateurs opèrent contre des honoraires, créant un marché où la concurrence pousse la tarification, la rapidité et la fiabilité.

Étape 1. Le document d'affirmation est concaténé avec le résultat de hachage de l'itération précédente (ou $\varnothing$ à la première itération) puis haché :

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

L'algorithme doit inclure le *chemin complet* de toutes les requêtes et réponses précédentes—et non un simple hachage de l'itération précédente. La réponse intégrale de chaque vérificateur (acceptation, rejet, prix indiqué, motif) est ajoutée au document en croissance, vérifiable par des signatures cryptographiques à chaque étape.

Étape 2. Le hachage est projeté sur N positions de l'anneau de hachage cohérent, uniformément réparties (p. ex. pour $N = 4 : +0°, +90°, +180°, +270°$). À partir de chaque position, une recherche dans le sens horaire sélectionne le DID le plus proche comme candidat vérificateur (Fig. 5). N est un paramètre variable qui peut dépendre du pourcentage de DID actuellement actifs, de l'heure de la journée ou de la réactivité historique du réseau.

Étape 3. Le Vérificateur accepte (publie, engageant sa réputation) ou rejette (retour à l'Étape 1 avec le hachage du rejet). Lorsqu'un nœud ne répond pas malgré un statut en ligne déclaré, la requête suivante doit inclure toutes les réponses de l'ensemble des N candidats vérificateurs précédents.

Anti-parasitage. Les DID cibles peuvent fixer des honoraires ou des restrictions d'accès pour les requêtes provenant de nouveaux DID à faible réputation. Ce mécanisme graduel (et non binaire) oblige les nouveaux venus à bâtir une réputation par une activité authentique avant de consommer librement les données d'autrui.

Chaque rejet ajoute la réponse intégrale du vérificateur (y compris les motifs et conditions) au document d'affirmation, en élargissant son contenu. À partir du document élargi, un nouveau hachage est calculé de façon non déterministe, projeté sur une position différente de l'anneau et sélectionnant un vérificateur différent. La documentation du chemin complet est obligatoire—l'émetteur ne peut ni prédire ni influencer le vérificateur suivant. Si un vérificateur ignore une requête malgré une politique déclarée compatible, les témoins (le cas échéant) le consignent, et l'émetteur peut joindre les preuves des témoins lors de la publication finale.

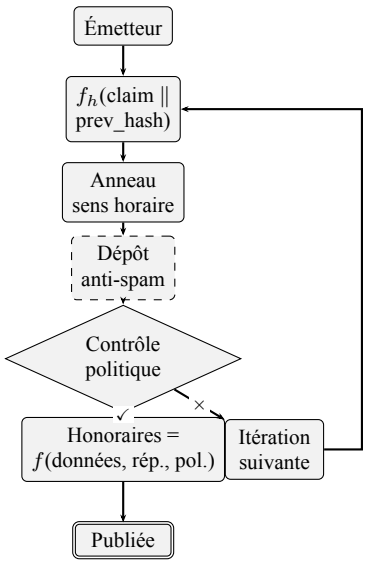

Figure 4: Protocole de sélection des vérificateurs. Le dépôt anti-spam est optionnel et peut être remboursable. Les honoraires finaux ne sont dus qu'en cas d'acceptation.

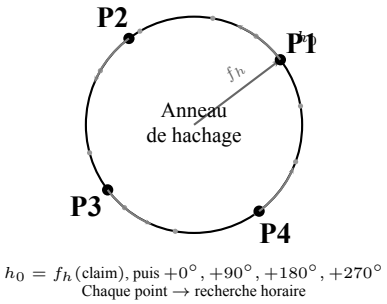

Figure 5: Sélection multipoint (N=4). Le hachage h_0 fixe le décalage ; 4 points uniformément répartis à partir de h_0.

5.4 Protocole du témoin

Le rôle du **Témoin** fournit une responsabilisation incognito de l'honnêteté du vérificateur au moyen d'un protocole cryptographique de code de défi :

Étape W1. Le demandeur signe la requête de vérification et l'envoie à N_w témoins—des contacts du réseau social du demandeur, ou des prestataires spécialisés de service de témoin opérant contre des honoraires.

Étape W2. Chaque témoin w_i signe l'intégralité de la requête signée, conserve la signature originale σ_i et calcule un code de défi $c_i = h(\sigma_i)$. Le code de défi est ajouté à la requête.

Étape W3. La requête, portant désormais N_w codes de défi, est envoyée au vérificateur. Le vérificateur observe les codes mais *ne peut pas déterminer* qui sont les témoins ni si les codes correspondent à de vraies signatures.

Étape W4 (vérificateur honnête). Si le vérificateur répond conformément à sa politique déclarée, les codes de défi restent opaques. Les témoins ne sont jamais révélés. Aucune donnée supplémentaire n'est publiée.

Étape W5 (violation de politique). Si le vérificateur enfreint sa politique (ignore la requête, répond de façon incohérente), le demandeur détient les signatures originales σ_i des témoins. Celles-ci peuvent être publiées comme données d'accompagnement : quiconque peut vérifier que $c_i = h(\sigma_i)$, prouvant que le témoin était présent. Le demandeur peut publier de façon indépendante—le vérificateur a déjà signé les codes de défi dans sa réponse.

La propriété de bluff. Le demandeur peut substituer des valeurs aléatoires à certains ou à tous les codes de défi. Le vérificateur ne peut pas distinguer les codes authentiques (adossés à des autorités de haute réputation) du bruit. Cette *incertitude* est le mécanisme d'application : chaque requête porte le risque qu'une autorité respectée observe incognito. Le coût du maintien de cette pression est proche de zéro (générer des nombres aléatoires), tandis que le coût potentiel de la malhonnêteté pour le vérificateur est catastrophique. Le comportement honnête est incité même en l'absence de témoins réels.

L'Autorité comme témoin. Une Autorité qui cautionne une affirmation peut regrouper les services de témoin : « Je cautionne votre affirmation et je fais office de témoin incognito pendant la vérification. » C'est un modèle économique naturel—l'Autorité dispose déjà du contexte. Les deux rôles restent toutefois logiquement indépendants.

5.5 Principe du radicalisme coûteux

Trois canaux de coûts se cumulent simultanément (Fig. 6) :

Canal 1 : coût d'itération. Chaque rejet impose une nouvelle itération qui consomme du temps et des ressources. Croissance linéaire.

Canal 2 : gonflement du document. Chaque itération ajoute la réponse intégrale du vérificateur au document d'affirmation. La croissance est linéaire, mais avec un décalage de base : la charge utile initiale (contenu de l'affirmation, caution de l'autorité, signatures cryptographiques) possède déjà une taille non triviale B_0. Taille totale après k itérations : $S(k) = B_0 + k \cdot \Delta$, où Δ est la taille moyenne d'une réponse.

Canal 3 : prime de risque du vérificateur. Le risque est subjectif. Le vérificateur évalue si les politiques déclarées du DID demandeur entrent en conflit avec ses propres intérêts commerciaux, sociaux ou politiques. La prime peut croître de façon exponentielle avec la distance perçue à l'« idéal » du vérificateur : $P(d) = \alpha \cdot e^{\beta d}$, où d est la métrique de distance subjective du vérificateur. Au-delà d'une frontière personnelle infranchissable, le vérificateur peut refuser purement et simplement.

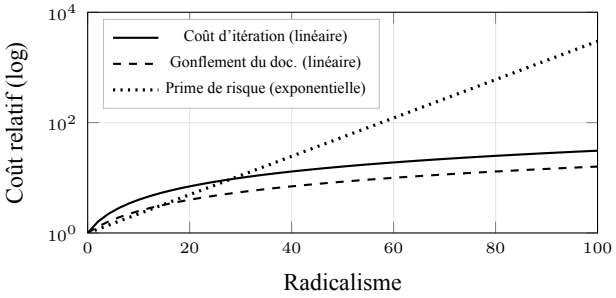

Figure 6: Escalade des coûts sur trois canaux. La prime de risque domine à haut radicalisme.

Fait crucial, ce n'est pas de la censure. Aucune affirmation n'est interdite. Le système tarifie le risque (Table 1).

Table 1: Comparaison des coûts par type d'affirmation.

Type	Itér.	Doc	Honor.	Total
Crédible	k_{min}	B_0	P_{min}	Faible
Controversée	k_{med}	$B_0 + k\Delta$	$\alpha e^{\beta d}$	Modéré
Radicale	k_{max}	$\gg B_0$	$\gg P_{\text{min}}$	Très élevé
Frauduleuse	$\to \infty$	—	—	Impubliable

6 Réputation et évaluation du risque

6.1 Modèle d'accumulation de la réputation

La réputation présente trois propriétés : une **accumulation lente** (croissance progressive par un comportement constant), une **destruction rapide** (une seule fraude peut réduire le score de façon catastrophique) et une **évaluation individuelle** (chaque partie consommatrice peut appliquer sa propre fonction d'agrégation).

6.2 Autorités réputées

Une Autorité réputée examine les affirmations et, si elle est convaincue, les contresigne—engageant sa

propre réputation (Fig. 7). L'asymétrie est intentionnelle : gagner de la réputation est lent (incrément $+\delta$ par caution honnête), tandis que la perdre est catastrophique ($-\Delta \gg \delta$ par caution mensongère ; à titre d'illustration, p. ex. $+2\%$ contre -70%). La stratégie optimale est toujours de rejeter les affirmations suspectes. Les valeurs précises de δ et Δ sont des paramètres du système.

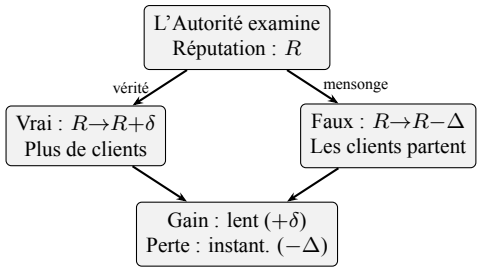

Figure 7: Autorité réputée—incitations asymétriques.

6.3 Réputation multidimensionnelle

La réputation n'est pas un scalaire mais un vecteur selon plusieurs dimensions : fiabilité financière, intégrité personnelle, compétence professionnelle, engagement civique, et d'autres (Fig. 8). Différents prestataires d'évaluation projettent ce vecteur différemment selon le contexte—un prêteur privilégie la fiabilité financière, un employeur la compétence professionnelle, un voisin le comportement civique. Il n'existe pas de score de réputation « correct » unique ; seulement des perspectives.

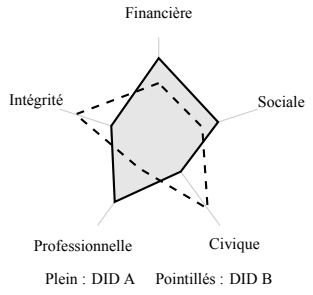

Figure 8: Vecteurs de réputation multidimensionnels. Différents DID présentent des profils différents selon les dimensions.

6.4 Évaluation démocratisée du risque

Le RSN démocratise l'évaluation systématique du risque—une capacité aujourd'hui concentrée dans les institutions financières mais applicable bien au-delà de la banque. Les conglomérats industriels évaluant la fiabilité de leurs fournisseurs, les compagnies d'assurance tarifant le risque comportemental, la diligence raisonnable lors des fusions et acquisitions, l'estimation de la durée de vie des équipements dans l'industrie—partout où le risque de contrepartie doit être évalué, le RSN fournit une alternative décentralisée et pilotée par le marché. Un marché de services d'interprétation traduit les données brutes de réputation multidimensionnelle en synthèses exploitables, rendant l'évaluation des contreparties accessible à tout participant à un coût marginal.

7 Consensus et résolution des litiges

7.1 Modèle de justice décentralisée

Le RSN reformule la justice comme un problème de négociation bilatérale. La menace d'une atteinte permanente et vérifiable à la réputation est un moyen de dissuasion plus efficace que des procédures judiciaires que la partie lésée ne peut se permettre.

7.2 Consensus émergent

Chaque participant maintient un seuil personnel de satisfaction. Le consensus agrégé du réseau émerge comme la moyenne statistique de milliers de négociations bilatérales (Fig. 9). Une réponse très supérieure au consensus (barbare) est coûteuse à publier. Une réponse proche du consensus (proportionnée) est bon marché. Le consensus n'est pas une règle—c'est un signal de prix.

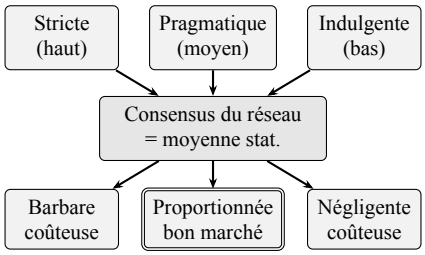

Figure 9: Consensus émergent à partir des seuils individuels de satisfaction.

7.3 Calibrage de la sanction

Chaque Détenteur de DID déclare publiquement ses réponses à des catégories spécifiques de fautes. Les déclarations disproportionnellement sévères ou clémentes attirent des signaux de réputation négatifs. Les déclarations proportionnées sont acceptées sans friction—un système de sanction auto-calibrant.

Les déclarations de consensus sont elles-mêmes soumises à la détection d'hypocrisie : s'engager

déclarativement sur une position de consensus tout en se comportant de façon incohérente constitue une faute réputationnelle plus grave que l'écart sous-jacent, car cela démontre une tromperie intentionnelle.

7.4 Délégation

Toutes les activités au sein d'un DID—à une exception près—peuvent être déléguées à un autre DID. **Le rôle de Sujet—le DID dont l'affirmation décrit le comportement—ne peut pas être délégué ; il est lié de façon non transférable au détenteur d'identité auquel l'affirmation se rapporte.** Les autres rôles actifs—Émetteur, Autorité, Témoin, Vérificateur—peuvent être transférés à un DID délégué désigné, que ce soit pour la vérification, la soumission d'affirmations, la participation au consensus ou la résolution de litiges. La délégation est révocable à tout moment. Cela permet la spécialisation (p. ex. des services professionnels de vérification) tandis que le Détenteur conserve le contrôle et la responsabilité ultimes. La délégation s'applique à l'ensemble du système et est essentielle à l'évolutivité.

7.5 De la morale individuelle au contrat social émergent

La politique déclarée de chaque DID représente une formalisation de la morale individuelle : ce que le Détenteur considère comme acceptable, la manière dont il répond à des comportements précis, ce qu'il exige de ses contreparties. Ces politiques ne sont pas imposées par un concepteur de système—elles sont choisies par chaque participant et exprimées sous forme lisible par machine.

Cette formalisation rend possible une émergence en trois étapes. D'abord, la morale individuelle est encodée comme **politique**—un ensemble de règles déclarées, de seuils et de fonctions de réponse que le DID s'engage à suivre. Ensuite, l'agrégat de toutes les politiques du réseau produit une **éthique émergente**—des normes statistiquement observables qu'aucun participant n'a conçues mais qui naissent de l'interaction de milliers de positions morales individuelles [9]. Enfin, cette éthique émergente, exprimée comme des normes comportementales partagées appliquées par des signaux de prix bilatéraux, constitue un **contrat social mesurable**—non pas une construction théorique que personne n'a signée [10], mais un ensemble de règles empiriquement observable adossé à des comportements réels.

Ce processus reflète les conclusions de la théorie des fondements moraux [11] : la morale humaine est intuitive, plurielle et culturellement variable. Le RSN n'exige pas de consensus moral en entrée ; il produit un consensus comportemental en sortie. Le contrat social qui en résulte n'est pas statique—il évolue à mesure que les participants rejoignent, quittent et ajustent leurs politiques en réponse à la rétroaction du réseau. Contrairement à la théorie classique du contrat social, ce contrat est révocable, observable et applicable sans souverain.

8 Modèle économique

Les sections précédentes ont décrit un outil—les mécanismes de vérification du RSN, sa structure de coûts et son consensus émergent. Cette section décrit une méthodologie pour appliquer cet outil à la transition fiscale et de gouvernance. L'outil est polyvalent ; la méthodologie ci-dessous n'est qu'une application possible.

8.1 Structure des incitations

La réputation en tant que capital crée des incitations directes à un comportement honnête. En fonctionnement normal, les participants bâtissent leur réputation naturellement par leurs transactions quotidiennes et leurs engagements tenus. La dépense principale porte sur les affirmations *négatives*—consigner un préjudice causé par autrui. Cette asymétrie incite à un comportement utile et fiable : être honnête ne coûte rien de plus, tandis qu'être nuisible crée une trace documentée que d'autres paieront pour conserver. L'hypocrisie—déclarer des règles sans les suivre—est le mode de défaillance le plus coûteux, car elle démontre une tromperie intentionnelle.

8.2 Système fiscal parallèle

Trois composantes permettent une pression concurrentielle : (1) un **Impôt simple**—un taux proportionnel unique sans exception, initialement légèrement inférieur au taux effectif existant ; (2) l'**Enregistrement électronique des dépenses (EED)**—inversant le modèle tchèque EET pour que les citoyens surveillent les dépenses de l'État ; (3) l'**Affectation de l'impôt dirigée par le citoyen**—débutant à quelques pour cent la première année et atteignant, au bout d'une décennie, de la dizaine de pour cent à une migration complète vers un système dirigé par le citoyen, selon le rythme d'adoption. Le tempo réel dépend de la vitesse à laquelle émergent des alternatives de libre marché aux services de l'État et de la disposition de l'État à

coopérer à la transition ; la fonction du temps n'a pas à être linéaire, et il n'y a aucune raison de fixer une borne supérieure à l'endroit où l'adoption pourra finalement parvenir.

9 Voie de migration

La migration se déroule en trois phases (Fig. 10) : **Phase 1 : superposition** (le RSN comme couche informationnelle, l'État seul prestataire), **Phase 2 : concurrence** (le RSN propose des alternatives fonctionnelles, usage à double système) et **Phase 3 : transition** (le RSN surpasse les équivalents étatiques, migration volontaire). La transition est réversible à chaque étape.

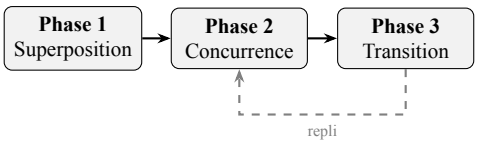

Figure 10: Migration en trois phases—réversible à chaque étape.

Le principal mécanisme de pression est fiscal : lorsque les contribuables conditionnels atteignent une « minorité économiquement significative X »—un groupe assez important pour que la répression à son encontre cause des dommages économiques non négligeables et que la désobéissance civile devienne une menace crédible—l'État entre en négociation. À titre d'illustration, nous utilisons $X \approx 15\%$ du PIB, mais le seuil réel dépend de l'économie considérée.

10 Analyse de sécurité

Nous considérons cinq catégories d'adversaires : les mauvais acteurs individuels, les groupes organisés, les adversaires corporatifs, les adversaires étatiques et les adversaires au niveau du protocole.

Résistance Sybil [12]. Bâtir une réputation exige une interaction soutenue et vérifiable. Le coût d'une attaque Sybil réussie croît linéairement avec le nombre de fausses identités et quadratiquement avec le niveau de réputation visé. Exploiter plusieurs DID en parallèle est possible mais coûteux par conception—chaque identité doit accumuler indépendamment sa réputation par une activité authentique. Dans les sociétés libres, ce coût dissuade les abus occasionnels ; dans les dictatures, les DID parallèles deviennent un outil de survie permettant une résistance cloisonnée, une coordination clandestine et une navigation plus sûre dans le marché noir.

Défense contre la collusion. Les schémas de caution mutuelle au sein de groupes fermés sont détectables par l'analyse du graphe social. Les fonctions d'agrégation de réputation décotent les affirmations provenant de sources étroitement regroupées.

Adversaire étatique. Le routage onion, l'absence d'infrastructure centralisée et la répartition du rôle de Vérificateur sur l'ensemble des participants garantissent que la répression exige des mesures disproportionnées par rapport à tout bénéfice.

Vie privée vs. responsabilisation. Le pseudonymat—un terrain intermédiaire entre l'anonymat et la divulgation d'identité—permet aux DID d'accumuler une réputation significative sans révéler l'identité réelle du Détenteur.

11 Considérations relatives à la vie privée

Le modèle de vie privée du RSN repose sur le pseudonymat. Le Détenteur contrôle la divulgation d'identité : minimale (pseudonyme pur), sélective (certains attestations liées) ou complète (identité légale associée). Les affirmations publiées sont permanentes—le système prend en charge la correction contextuelle mais pas l'effacement. Un Détenteur peut abandonner un DID compromis et repartir à zéro, renonçant à la réputation accumulée.

12 Travaux connexes

La spécification W3C DID Core [2] et le réseau Ceramic [8] fournissent le socle d'identité. EigenTrust [13] a démontré l'agrégation distribuée de réputation sans autorité centrale. Les SBT [3] ont introduit des jetons sociaux non transférables. Le RSN s'en distingue par l'accent qu'il met sur le coût économique comme filtre de qualité et par son mécanisme de tarification du radicalisme.

Les DAO [4] et le vote quadratique [5] ont démontré la faisabilité d'une gouvernance décentralisée. Le RSN dérive son consensus de négociations bilatérales de prix plutôt que du vote.

La proposition s'appuie sur la théorie anarcho-capitaliste [14, 15] pour la fourniture privée de services mais s'en écarte sous deux aspects critiques : elle est conçue pour les pulsions de rancune et de rétribution plutôt que de présumer la rationalité, et elle propose une transition graduelle plutôt qu'une révolution. Le concept de contrats sociaux émergents a

des antécédents dans la théorie de l'ordre spontané de Hayek [16].

Anarcho-agorisme. Le RSN partage un terrain commun important avec la contre-économie agoriste [17]—en particulier l'accent mis sur la construction d'institutions parallèles et l'échange volontaire. Cependant, l'agorisme tend à présumer l'intérêt personnel rationnel comme mécanisme de coordination suffisant et manque souvent d'une voie de migration concrète depuis les structures étatiques existantes. Le RSN intègre explicitement des tendances comportementales non rationnelles et fournit un mécanisme de pression fiscale pour une transition graduelle.

Méritocratie. Le RSN pourrait constituer une première description fonctionnelle de la manière dont la méritocratie [18] peut émerger comme propriété systémique plutôt que comme slogan. Les systèmes méritocratiques traditionnels échouent parce qu'ils exigent une autorité centrale pour définir et faire respecter le « mérite ». Dans le RSN, le mérite émerge des évaluations bilatérales : ceux qui apportent de la valeur accumulent de la réputation ; aucun comité ne décide qui a du mérite.

La propriété comme privilège. Le RSN s'écarte fondamentalement des traitements anarcho-capitalistes et de l'école autrichienne qui considèrent les droits de propriété comme naturels et absolus. Dans le cadre du RSN, la propriété est un *privilège*—une reconnaissance sociale qui peut, dans des cas extrêmes, être retirée par la communauté lorsqu'un participant viole fondamentalement les normes partagées (trahison, refus de défendre la communauté en cas de crise existentielle, exploitation systématique). Il ne s'agit pas d'une expropriation par l'État mais d'un retrait de reconnaissance sociale par le réseau des relations bilatérales.

13 Discussion et limites

Démarrage à froid. La valeur du RSN dépend des effets de réseau ; les premiers adoptants font face à une valeur limitée jusqu'à ce que la participation atteigne un seuil. Néanmoins, même dès les premières étapes, le réseau DID sert de source d'information complémentaire utile. On s'attend à ce que l'évaluation précoce de la réputation et l'appréciation des autorités se développent progressivement avec une sophistication croissante.

Anti-parasitage et contrôle d'accès. Les DID cibles peuvent imposer des honoraires graduels et des restrictions d'accès aux requêtes provenant de DID à faible réputation. Ce n'est pas binaire mais une échelle continue : moins un DID demandeur a de réputation, moins il reçoit d'information, plus il attend et plus il paie. Ce mécanisme incite à une participation authentique plutôt qu'à une consommation passive.

Inégalité d'accès. Le coût de publication des affirmations peut filtrer les griefs légitimes des participants économiquement défavorisés. Atténuation : chaque participant sert simultanément de vérificateur potentiel (ou délègue ce rôle) et gagne des honoraires de vérification. Sur un horizon temporel suffisant, un participant non radical devrait tendre vers une neutralité financière—les revenus de vérification compensant approximativement les coûts de publication. C'est une espérance statistique, non une garantie.

Inégalité de réputation. Les premiers adoptants accumulent des avantages susceptibles de créer des barrières pour les arrivants tardifs. Toutefois, l'évaluation de la réputation est réalisée par des prestataires tiers qui peuvent choisir d'atténuer l'avantage du premier arrivé au moyen de leurs algorithmes d'agrégation. Être le premier avec une bonne réputation est un avantage économique comparatif légitime—et c'est voulu.

Questions ouvertes. Les fonctions de coût optimales, les standards d'agrégation, la gouvernance du protocole et l'interaction avec les données de réputation synthétique générées par IA restent des domaines à explorer.

Cet article ne prétend pas que le RSN produira des résultats optimaux en toutes circonstances. Il prétend que le RSN représente une alternative *réalisable*—techniquement implémentable, économiquement autosuffisante et socialement compatible avec les tendances comportementales humaines telles qu'elles sont réellement.

14 Conclusion

Cet article a présenté le Réseau social de réputation, un protocole décentralisé permettant un échange de réputation pseudonyme et vérifiable. Le Principe du radicalisme coûteux garantit que les affirmations frauduleuses sont écartées par leur prix, sans censure. La voie de migration proposée permet une transition graduelle et réversible depuis les institutions existantes. La conception intègre la nature humaine telle qu'elle est—y compris la mesquinerie, la rancune et le désir de satisfaction punitive—plutôt que d'exiger une transformation idéologique. Le résultat n'est pas l'utopie mais un système où la justice est accessible, où la réputation se mérite et où le coût de la faute est supporté par la partie qui l'a causée.

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.