# Réseau de réputation décentralisé : Un cadre pour l'organisation naturelle de la société

Pavel Kudrna
Prague, Tchéquie
Ébauche v1 — mars 2026

## Abstract

Le sens de la justice—la conviction que les torts sont réparés et que le mérite est récompensé—est la plus forte force de cohésion de la société. Lorsque les institutions centralisées de gouvernance ne peuvent procurer ce sens parce que le coût de faire valoir un droit dépasse la valeur du droit lui-même, la cohésion sociale s'effrite. Les structures institutionnelles actuelles échouent à résoudre une catégorie importante de différends de la même façon systématique que la planification centrale échoue à répartir les ressources : par l'asymétrie d'information, l'absence de boucles de rétroaction et la 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 consulter de l'information de réputation sur des comportements du monde réel. 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 de sélection non déterministe des vérificateurs fondé sur le hachage cohérent qui tarife 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 misent leur réputation accumulée sur l'exactitude des affirmations qu'ils cautionnent. L'architecture qui en résulte produit une méritocratie émergente sans coordination centrale et permet un cheminement de migration graduel et réversible à partir des systèmes existants 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 servir d'intermédiaires de confiance entre étrangers à grande échelle. Les tribunaux tranchent les différends. Les registres attestent la propriété. Les organismes de réglementation font respecter les normes. Ces institutions ont été conçues à une époque où l'information était rare, la communication lente, et où la délégation de l'autorité à un organe central était le seul mécanisme de coordination réalisable. La gouvernance centralisée, cependant, échoue pour les mêmes raisons structurelles que la planification centrale : l'asymétrie d'information, l'absence de boucles de rétroaction et la déconnexion des décideurs des conséquences de leurs décisions.

L'hypothèse échoue, par exemple, lorsque le coût de la médiation institutionnelle dépasse la valeur du différend. Considérons un locataire qui découvre que son logement loué ne possède pas de certificat de sécurité électrique exigé par la loi—une condition qui présente un danger immédiat pour la vie. Le droit légal du locataire de résilier le contrat est sans équivoque. Pourtant, le coût de faire valoir ce droit devant les tribunaux dépasse la valeur monétaire du dépôt et des dommages dus, même en incluant une éventuelle indemnisation légale [1]. La réponse rationnelle consiste à absorber la perte et à se retirer.

Il ne s'agit pas d'un cas limite pathologique. C'est l'expérience courante d'une catégorie importante de différends dans lesquels le préjudice est réel mais 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, parce que le coût de la recherche de justice retombe sur la partie lésée.

L'exemple ci-dessus est tiré de l'environnement juridique de l'auteur—le système de droit civil tchèque. Dans d'autres traditions juridiques—la common law fondée sur le précédent, le droit coutumier, les systèmes mixtes—la justice échoue de différentes manières et à différents degrés, selon les particularités 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 différends dont la valeur tombe sous le seuil de l'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 est non rentable.

### 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 surtout sur la vérification de l'identité sans aborder la question plus large de la réputation comportementale.

Les **jetons non transférables (SBT, « Soulbound Tokens »)** [3] saisissent l'idée que la réputation n'est pas transférable mais reposent sur une infrastructure de chaîne de blocs présentant des contraintes de mise à l'échelle et n'abordent pas les incitations économiques qui régissent l'entrée de l'information. Des concepts apparentés comme les jetons de mérite (p. ex. Liberland) partagent une philosophie semblable mais demeurent liés à des cadres juridictionnels précis.

Les **organisations autonomes décentralisées (DAO)** [4] mettent en œuvre la gouvernance au moyen de 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 aussi au fondamental *problème de l'oracle* : les contrats intelligents ne peuvent vérifier de façon fiable les états du monde réel sans une source externe de confiance, et ce problème n'a aucune solution générale au sein de l'architecture des chaînes de blocs.

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 de sélection non déterministe des vérificateurs** fondé sur le hachage cohérent [6].
3. Le **principe du radicalisme coûteux**, qui tarife les affirmations selon leur distance par rapport au consensus du réseau au moyen de trois canaux de coûts cumulatifs.
4. Un **modèle d'autorité réputée** à incitations asymétriques où un cautionnement mensonger coûte catastrophiquement plus cher que des honoraires légitimes.
5. Un **cheminement de migration graduel** par le biais d'une infrastructure fiscale parallèle.

## 2 Principes de conception

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

**Continuité et évolution.** Le système coexiste avec les institutions existantes pendant une période de transition d'une durée indéterminée. 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 assume simultanément les obligations qui l'accompagnent.

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

**Résilience et résistance à la censure.** Le coût de censurer le réseau doit dépasser le coût de le tolérer. Seul un totalitarisme complet—à un coût politique et économique ruineux—peut réprimer le système.

**Consensus et application.** Le système intègre les tendances humaines à la mesquinerie, à la rancune et à la satisfaction rétributive comme des caractéristiques porteuses. L'inconduite 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 de l'information vérifiable sur des comportements du monde réel. Ses propriétés déterminantes sont : une infrastructure décentralisée et incensurable ; une participation pseudonyme au moyen des DID ; une structure de coûts asymétrique (la lecture est bon marché, l'écriture est coûteuse) ; une vérifiabilité cryptographique ; et le **soutien de normes**—des formats lisibles par la machine pour l'information propagée dans le réseau, pour les services offerts par les autorités (composition d'affirmations, cautionnement, service de témoin) et pour le format des politiques, y compris les règles d'évaluation de la réputation d'une contrepartie et d'appréciation du risque d'écart 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.** Les identités des participants avec règles déclarées, métadonnées de réputation et routage réseau.
2. **Protocole d'affirmation.** Un format structuré pour publier des assertions au sujet d'événements du monde réel.
3. **Réseau de vérification.** Un protocole décentralisé pour l'attribution des vérificateurs au moyen du hachage cohérent.
4. **Couche d'agrégation de réputation.** Des services qui produisent des synthèses de réputation lisibles par l'humain.

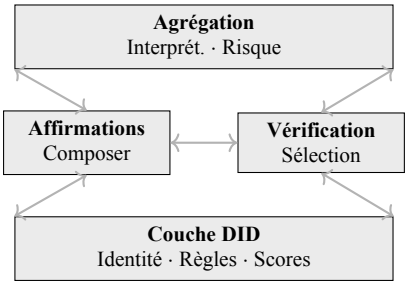


Figure 1: Architecture à quatre couches du RSN.

## 3.3 Rôles des participants

Une transaction de vérification met en jeu jusqu'à six rôles DID distincts (fig. 2) : l'**Émetteur** ($DID_I$, crée et soumet l'affirmation), le **Sujet** ($DID_S$, le DID que concerne l'affirmation—peut coïncider avec l'Émetteur), l'**Autorité** ($DID_A$, cautionne l'affirmation contre des honoraires ; peut aussi offrir des services de témoin—*facultatif*), le **Témoin** ($DID_{W_{1..n}}$, moniteur incognito de l'honnêteté du vérificateur au moyen de codes de défi—*facultatif*), le **Vérificateur** ($DID_V$, sélectionné par algorithme pour publier l'affirmation) et le **RSN** (le réseau où sont publiées les affirmations vérifiées). Tout rôle peut être délégué à un autre DID (section 7.4). Une Autorité groupe couramment le cautionnement avec des services de témoin, mais les deux fonctions sont logiquement indépendantes.

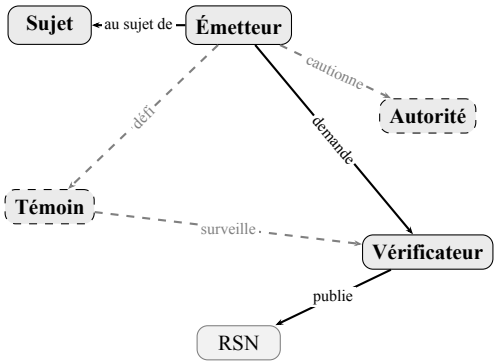


Figure 2: Rôles DID dans une transaction de vérification. Pointillés = facultatif (Autorité, Témoin).

## 3.4 Incorruptibilité : quatre forces

L'incorruptibilité du RSN ne découle pas d'un mécanisme unique mais de quatre forces concurrentes. Aucune n'est suffisante 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 le hachage cohérent (section 5.3). Un attaquant ne peut 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—montée lente, chute rapide.** La réputation ne peut se gagner que de façon incrémentale, par un comportement constant et soutenu. Elle peut, en revanche, se perdre de façon catastrophique par un seul cautionnement frauduleux (section 6.2). Cette asymétrie signifie que des années

de réputation accumulée peuvent être anéanties par un seul cautionnement malhonnête ; la stratégie optimale demeure de rejeter les affirmations suspectes.

**Promesse publique.** Chaque titulaire de DID déclare publiquement sa politique—un ensemble de règles lisibles par la machine qu'il s'engage à suivre. L'écart entre la déclaration et le comportement réel est détectable et tarifé comme un manquement réputationnel 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 en maillage.** Le coût de censurer ou de déstabiliser le réseau croît de façon non linéaire avec la taille et la densité du réseau, tandis que le coût de le tolérer demeure 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 aux propriétés particulières

Le RSN étend la spécification W3C DID Core [2] avec : des **règles déclarées** (engagements comportementaux lisibles par la 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, cautionnement facultatif par une autorité, sélection du vérificateur par hachage cohérent, décision de vérification (accepter ou rejeter avec itération), publication et mise à jour de la réputation de toutes les parties.

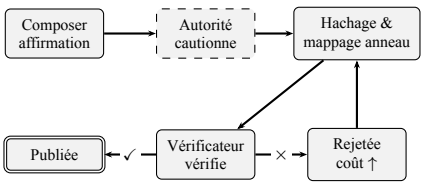


Figure 3: Cycle de vie d'une affirmation avec boucle d'itération.

## 4.3 Relation avec W3C DID Core

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

# 5 Vérification et propagation de l'information

## 5.1 Coût d'entrée de l'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 qui ont un accès proportionnel à leur réputation—les nouveaux venus doivent gagner graduellement 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 rapports honnêtes, le soin des partenariats et une fiabilité à long terme) et l'**argent** (l'investissement dans son propre nom—perfectionnement professionnel, qualité de son travail, réparation des préjudices causés). La réputation ne peut s'acheter instantanément—elle est le résultat d'une accumulation de toute une vie que le système se contente de rendre visible et transférable d'un contexte à l'autre. Les coûts techniques ponctuels du protocole (signatures cryptographiques, honoraires des vérificateurs) sont négligeables par rapport 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 vérificateurs opère à l'intérieur d'une profondeur configurable $h$ de contacts liés (p. ex. $h = 3$ : ses contacts directs, leurs contacts et les contacts de leurs contacts). Cette architecture n'exige pas une seule chaîne de blocs mondiale—elle favorise naturellement

l'émergence de communautés ou de grappes avec des recoupements vers d'autres communautés. Chaque participant DID doit avoir une **politique** publiée—un ensemble de règles lisibles par la machine qui régissent l'évaluation des demandes entrantes. Les violations de politique sont consignées dans le réseau comme des artefacts négatifs.

### 5.3 Sélection algorithmique des vérificateurs

Le protocole de vérification recourt au hachage cohérent [6] (fig. 4). La vérification est un service payant : les vérificateurs opèrent contre des honoraires, créant un marché où la concurrence détermine le prix, la vitesse 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 demandes et réponses précédentes—et non simplement un hachage de l'itération précédente. La réponse complète de chaque vérificateur (acceptation, rejet, prix indiqué, motif) est ajoutée au document qui s'allonge, vérifiable au moyen de signatures cryptographiques à chaque étape.

**Étape 2.** Le hachage est mappé sur $N$ positions de l'anneau de hachage cohérent, réparties uniformément (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, en misant sa réputation) ou rejette (retour à l'étape 1 avec le hachage de rejet). Lorsqu'un nœud ne répond pas malgré une déclaration de statut en ligne, la demande suivante doit inclure toutes les réponses de l'ensemble des $N$ candidats vérificateurs précédents.

**Anti-parasitage.** Les DID ciblés peuvent fixer des honoraires ou des restrictions d'accès pour les requêtes provenant de nouveaux DID à faible réputation. Ce mécanisme gradué (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 complète 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, mappant vers une position différente sur l'anneau et sélectionnant un vérificateur différent. La documentation du chemin complet est obligatoire—l'émetteur ne peut prédire ni influencer le prochain vérificateur. Si un vérificateur ignore une demande malgré une politique déclarée compatible, les témoins (s'il y en a) le consignent, et l'émetteur peut joindre la preuve des témoins au moment de la publication finale.

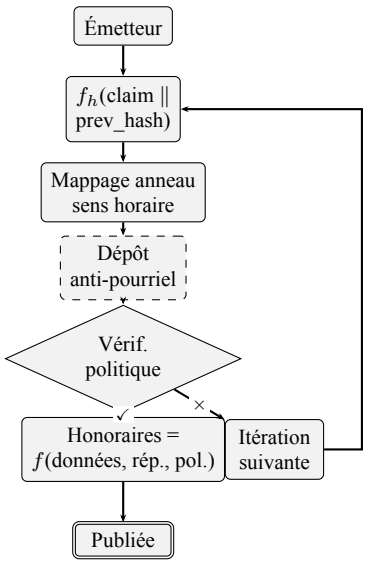


Figure 4: Protocole de sélection des vérificateurs. Le dépôt anti-pourriel est facultatif et peut être remboursable. Les honoraires finaux ne sont payés qu'à l'acceptation.

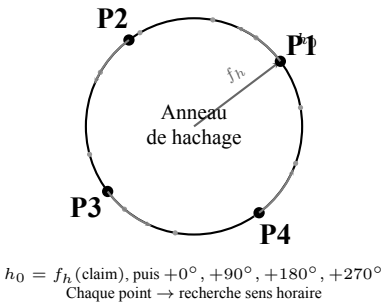


Figure 5: Sélection multipoint ($N$=4). Le hachage $h_0$ fixe le décalage ; 4 points répartis uniformément à partir de $h_0$.

### 5.4 Protocole de témoin

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

**Étape T1.** Le demandeur signe la demande de vérification et l'envoie à $N_w$ témoins—des contacts de son

réseau social, ou des fournisseurs spécialisés de service de témoin opérant contre des honoraires.

**Étape T2.** Chaque témoin $w_i$ signe l'intégralité de la demande signée, conserve la signature originale $\sigma_i$ et calcule un code de défi $c_i = h(\sigma_i)$. Le code de défi est ajouté à la demande.

**Étape T3.** La demande, portant désormais $N_w$ codes de défi, est envoyée au vérificateur. Le vérificateur observe les codes mais *ne peut déterminer* qui sont les témoins ni si les codes correspondent à de vraies signatures.

**Étape T4 (vérificateur honnête).** Si le vérificateur répond conformément à sa politique déclarée, les codes de défi demeurent opaques. Les témoins ne sont jamais révélés. Aucune donnée additionnelle n'est publiée.

**Étape T5 (violation de politique).** Si le vérificateur enfreint sa politique (ignore la demande, répond de façon incohérente), le demandeur détient les signatures originales $\sigma_i$ des témoins. Celles-ci peuvent être publiées comme données d'accompagnement : quiconque peut vérifier $c_i = h(\sigma_i)$, 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 distinguer les codes authentiques (adossés à des autorités de haute réputation) du bruit. Cette *incertitude* est le mécanisme d'application : chaque demande comporte le risque qu'une autorité respectée surveille incognito. Le coût de maintenir cette pression est quasi nul (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 y grouper des services de témoin : « Je cautionne votre affirmation et je sers de témoin incognito pendant la vérification. » C'est un modèle d'affaires naturel—l'Autorité possède déjà le contexte. Cependant, les deux rôles sont logiquement indépendants.

### 5.5 Principe du radicalisme coûteux

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

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

**Canal 2 : gonflement du document.** Chaque itération ajoute la réponse complète du vérificateur au document d'affirmation. La croissance est linéaire, mais avec un décalage de base : la charge utile initiale (contenu de l'affirmation, cautionnement 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 $\Delta$ 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 par rapport à l'« idéal » du vérificateur : $P(d) = \alpha \cdot e^{\beta d}$, où $d$ est la mesure de distance subjective du vérificateur. Au-delà d'une limite personnelle infranchissable, le vérificateur peut refuser entièrement.

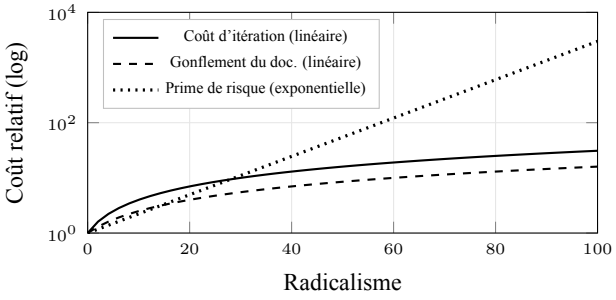


Figure 6: Escalade des coûts selon trois canaux. La prime de risque domine à haut radicalisme.

Fait crucial, il ne s'agit pas de censure. Aucune affirmation n'est interdite. Le système tarife le risque (tableau 1).

Table 1: Comparaison des coûts selon les types d'affirmation.

| Type | Itér. | Doc | Honor. | Total |
|---|---|---|---|---|
| Crédible | $k_{\text{min}}$ | $B_0$ | $P_{\text{min}}$ | Faible |
| Controversée | $k_{\text{med}}$ | $B_0 + k\Delta$ | $\alpha e^{\beta d}$ | Modéré |
| Radicale | $k_{\text{max}}$ | $\gg B_0$ | $\gg P_{\text{min}}$ | 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 : l'**accumulation lente** (croissance incrémentale par un comportement constant), la **destruction rapide** (une seule fraude peut réduire le score de façon catastrophique) et l'**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 satisfaite, les cosigne—en misant sa propre réputation (fig. 7). L'asymétrie est voulue : gagner de la réputation est lent (incrément $+\delta$ par cautionnement honnête), tandis que la perdre est catastrophique ($-\Delta \gg \delta$ par cautionnement mensonger ; à titre illustratif, p. ex. $+2\,\%$ contre $-70\,\%$). La stratégie optimale est toujours de rejeter les affirmations suspectes. Les valeurs précises de $\delta$ et $\Delta$ sont des paramètres du système.

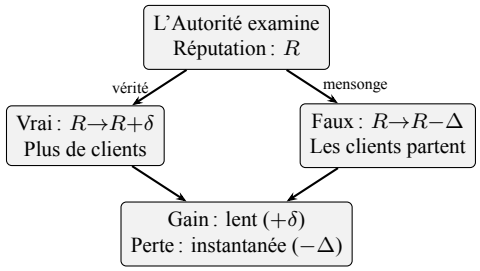


Figure 7: Autorité réputée—incitations asymétriques.

### 6.3 Réputation multidimensionnelle

La réputation n'est pas un scalaire mais un vecteur à plusieurs dimensions : fiabilité financière, intégrité personnelle, compétence professionnelle, engagement civique, et d'autres (fig. 8). Différents fournisseurs 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'y a pas de score de réputation « correct » unique ; seulement des perspectives.

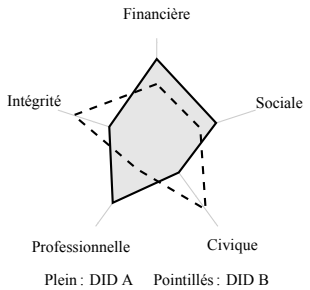


Figure 8: Vecteurs de réputation multidimensionnels. Différents DID présentent des profils différents selon les dimensions.

### 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 du secteur bancaire. Les conglomérats industriels évaluant la fiabilité de leurs fournisseurs, les compagnies d'assurance tarifant le risque comportemental, la vérification diligente pour les fusions et acquisitions, l'estimation de la durée de vie des équipements en fabrication—partout où le risque de contrepartie doit être évalué, le RSN offre une solution de rechange 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 d'une contrepartie accessible à tout participant à un coût marginal.

## 7 Consensus et résolution des différends

### 7.1 Modèle de justice décentralisée

Le RSN reformule la justice comme un problème de négociation bilatérale. La menace d'un dommage de réputation permanent et vérifiable est un moyen de dissuasion plus efficace que des procédures judiciaires que la partie lésée n'a pas les moyens de se payer.

### 7.2 Consensus émergent

Chaque participant maintient un seuil de satisfaction personnel. 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.

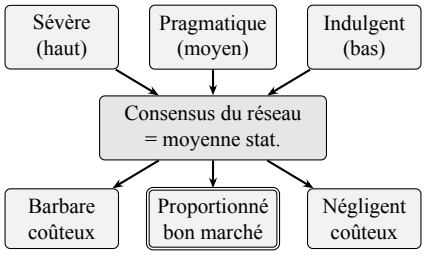


Figure 9: Consensus émergent à partir des seuils de satisfaction individuels.

### 7.3 Calibrage de la sanction

Chaque titulaire de DID déclare publiquement ses réponses à des catégories précises d'inconduite. Les déclarations démesurément sévères ou indulgentes attirent des signaux de réputation négatifs. Les déclarations proportionnées sont acceptées sans friction—un système de sanction qui s'autocalibre.

Les déclarations de consensus sont elles-mêmes soumises à la détection de l'hypocrisie : s'engager déclarativement envers une position de consensus tout en se comportant de façon incohérente constitue un manquement réputationnel 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 concerne le comportement—ne peut être délégué ; il est lié de façon non transférable au titulaire de l'identité à qui 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 différends. La délégation est révocable à tout moment. Cela permet la spécialisation (p. ex. des services de vérification professionnels) pendant que le titulaire conserve le contrôle et la responsabilité ultimes. La délégation s'applique à l'ensemble du système et est essentielle à la mise à l'échelle.

### 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 titulaire considère comme acceptable, comment il réagit 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 une forme lisible par la machine.

Cette formalisation permet une émergence en trois étapes. Premièrement, la morale individuelle est encodée sous forme de **politique**—un ensemble de règles déclarées, de seuils et de fonctions de réponse que le DID s'engage à suivre. Deuxièmement, l'agrégat de toutes les politiques du réseau produit une **éthique émergente**—des normes statistiquement observables qu'aucun participant n'a conçues mais qui découlent de l'interaction de milliers de positions morales individuelles [9]. Troisièmement, cette éthique émergente, exprimée sous forme de 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 un comportement réel.

Ce processus reflète les constats de la théorie des fondements moraux [11] : la morale humaine est intuitive, pluraliste et culturellement variable. Le RSN n'exige pas un consensus moral comme intrant ; il produit un consensus comportemental comme extrant. Le contrat social qui en résulte n'est pas statique—il évolue à mesure que les participants adhèrent, se retirent et ajustent leurs politiques en réaction 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, la structure de coûts et le consensus émergent du RSN. Cette section décrit une méthodologie pour appliquer cet outil à la transition fiscale et de gouvernance. L'outil est à usage général ; la méthodologie ci-dessous n'en est qu'une application possible.

### 8.1 Structure d'incitation

La réputation comme capital crée des incitations directes au 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 le préjudice causé par autrui. Cette asymétrie incite à un comportement utile et fiable : être honnête ne coûte rien de plus, tandis que causer du tort crée une trace documentée que d'autres paieront pour préserver. L'hypocrisie—déclarer des règles sans les suivre—est le mode d'échec le plus coûteux, car elle démontre une tromperie intentionnelle.

### 8.2 Système fiscal parallèle

Trois composantes permettent une pression concurrentielle : (1) l'**impôt simple**—un taux proportionnel unique sans exception, initialement marginalement inférieur au taux effectif existant ; (2) l'**enregistrement**

**électronique des dépenses (EED)**—inversant le modèle tchèque EET de sorte 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, après 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 des solutions de rechange de libre marché aux services de l'État émergent et de la volonté de l'État de 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 pourrait finalement parvenir.

# 9 Cheminement de migration

La migration se déroule en trois phases (fig. 10) : **Phase 1 : superposition** (le RSN comme couche d'information, l'État est le seul fournisseur), **Phase 2 : concurrence** (le RSN offre des solutions de rechange fonctionnelles, usage à double système) et **Phase 3 : transition** (le RSN surpasse les équivalents de l'État, migration volontaire). La transition est réversible à chaque étape.

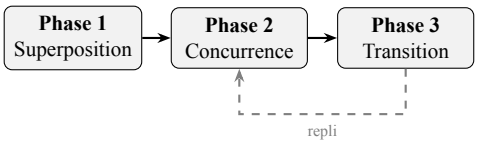


Figure 10: Migration en trois phases—réversible à chaque étape.

Le principal mécanisme de pression est fiscal : lorsque les contribuables conditionnels atteignent une « minorité économiquement significative $X$ »—un groupe assez grand pour que la répression contre lui cause un dommage économique non négligeable 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 particulière.

# 10 Analyse de sécurité

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

**Résistance à 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 de façon quadratique avec le niveau de réputation ciblé. 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 décourage l'abus occasionnel ; dans les dictatures, les DID parallèles deviennent un outil de survie permettant une résistance compartimentée, une coordination clandestine et une navigation plus sûre du marché noir.

**Défense contre la collusion.** Les schémas de cautionnement mutuel au sein de groupes fermés sont détectables par l'analyse du graphe social. Les fonctions d'agrégation de réputation escomptent les affirmations provenant de sources fortement regroupées.

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

**Vie privée contre reddition de compte.** Le pseudonymat—un juste milieu entre l'anonymat et la divulgation de l'identité—permet aux DID d'accumuler une réputation significative sans révéler l'identité réelle du titulaire.

# 11 Considérations relatives à la vie privée

Le modèle de vie privée du RSN repose sur le pseudonymat. Le titulaire contrôle la divulgation de son identité : minimale (pseudonyme pur), sélective (des attestations précises liées) ou complète (identité légale associée). Les affirmations publiées sont permanentes—le système prend en charge la correction contextuelle mais non l'effacement. Un titulaire peut abandonner un DID compromis et repartir à neuf, en 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 tire 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 sur deux points essentiels : elle est conçue pour la rancune et les pulsions rétributives plutôt que de supposer 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 d'entente 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 supposer l'intérêt personnel rationnel comme mécanisme de coordination suffisant et manque souvent d'un cheminement de migration concret à partir des structures étatiques existantes. Le RSN intègre explicitement les tendances comportementales non rationnelles et fournit un mécanisme de pression fiscale pour une transition graduelle.

**Méritocratie.** Le RSN pourrait représenter une première description fonctionnelle de la manière dont la méritocratie [18] peut émerger comme une propriété systémique plutôt que comme un 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 d'évaluations bilatérales : ceux qui livrent 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 présentent 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 la 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 tant que la participation n'atteint pas un seuil. Toutefois, même dès les premières étapes, le réseau DID sert de source d'information complémentaire utile. L'évaluation de la réputation et l'appréciation des autorités devraient se développer graduellement, avec une sophistication croissante.

**Anti-parasitage et contrôle d'accès.** Les DID ciblés peuvent imposer des honoraires gradués 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 publier des affirmations pourrait 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 s'approcher d'une neutralité financière—les revenus de vérification compensant approximativement les coûts de publication. Il s'agit d'une espérance statistique, non d'une garantie.

**Inégalité de réputation.** Les premiers adoptants accumulent des avantages qui peuvent créer des barrières pour les retardataires. Cependant, l'évaluation de la réputation est effectuée par des fournisseurs 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 cela est voulu.

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

Cet article ne prétend pas que le RSN produira des résultats optimaux en toutes circonstances. Il affirme que le RSN représente une solution de rechange *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 fait en sorte que les affirmations

frauduleuses sont écartées par le prix, sans censure. Le cheminement de migration proposé permet une transition graduelle et réversible à partir des institutions existantes. La conception intègre la nature humaine telle qu'elle est—y compris la mesquinerie, la rancune et le désir de satisfaction rétributive—plutôt que d'exiger une transformation idéologique. Le résultat n'est pas une utopie mais un système où la justice est accessible, la réputation se mérite, et le coût de l'inconduite est assumé par la partie qui l'a causé.

## 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.