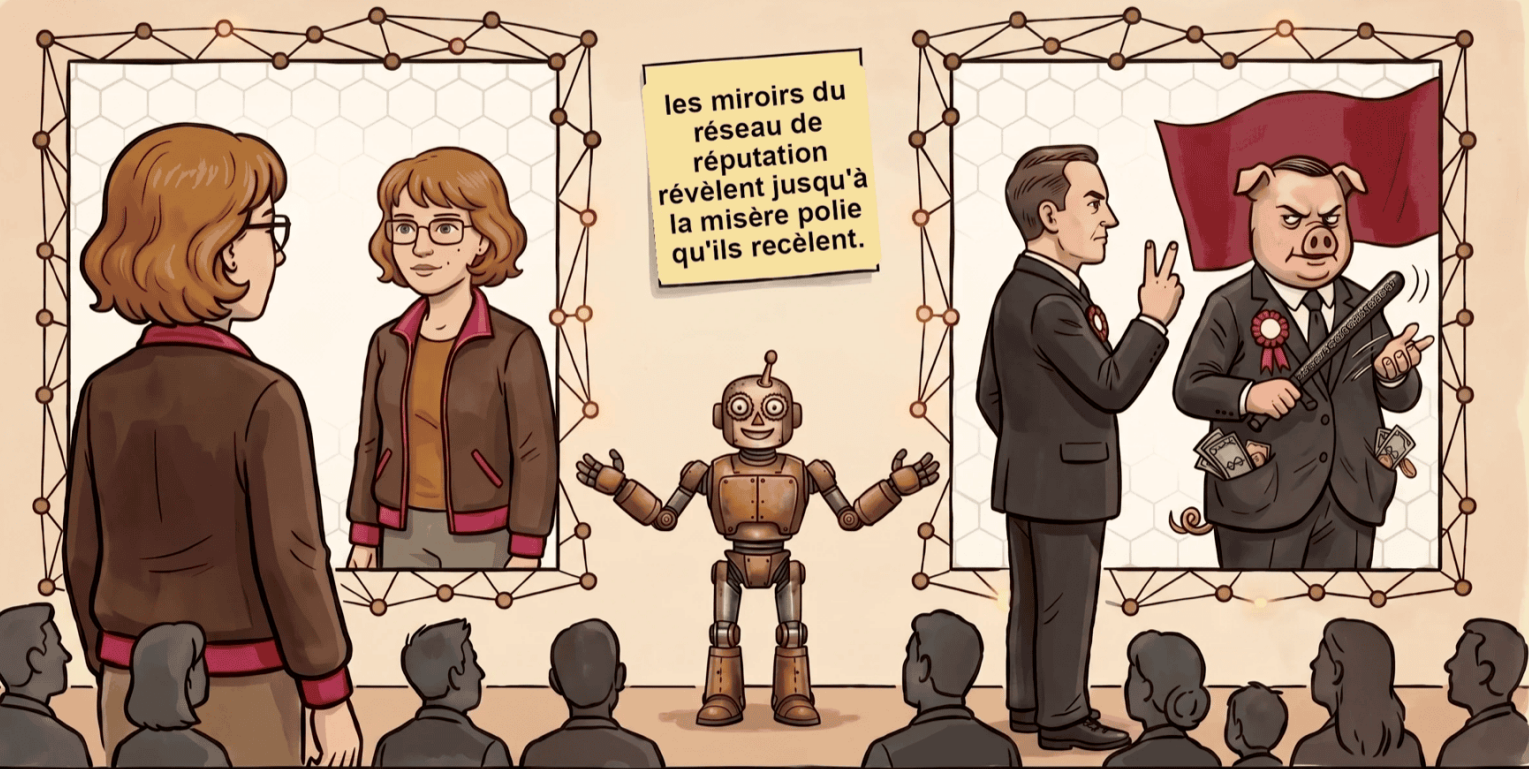


# PERSONIX

les miroirs du  
réseau de  
réputation  
révèlent jusqu'à  
la misère polie  
qu'ils recèlent.



**Un réseau de réputation décentralisé, incensurable et incorruptible  
un successeur évolutif de l'État**

## **Personix — Changement sans compromis**

Un réseau de réputation décentralisé, incensurable et incorruptible

© 2025–2026 Pavel Kudrna, Prague

Version 6 (2026-05-21)

Première ébauche juin–novembre 2025, réécrit avril–mai 2026.

Composé en  $\text{\LaTeX}$  (Tectonic) avec Palatino et Helvetica Neue.  
A5 paysage (210 × 148 mm).

Sous licence **Creative Commons Attribution-ShareAlike 4.0 International (CC BY-SA 4.0)** — [creativecommons.org/licenses/by-sa/4.0/](https://creativecommons.org/licenses/by-sa/4.0/). Les éléments réservés, le dépôt des sources et une note sur les outils de production sont indiqués à la fin du livre.



# Contents

|                                                                                                                                  |           |
|----------------------------------------------------------------------------------------------------------------------------------|-----------|
| <b>Introduction</b>                                                                                                              | <b>7</b>  |
| De quoi parle ce livre ? . . . . .                                                                                               | 9         |
| <b>Conditions préalables essentielles au changement</b>                                                                          | <b>17</b> |
| Conditions préalables essentielles au changement . . . . .                                                                       | 17        |
| <b>L'outil</b>                                                                                                                   | <b>28</b> |
| Réseau social fondé sur la réputation . . . . .                                                                                  | 28        |
| Pourquoi le réseau est incensurable . . . . .                                                                                    | 54        |
| Réponse aux doutes les plus évidents . . . . .                                                                                   | 56        |
| Dépendance à la technologie . . . . .                                                                                            | 56        |
| Est-ce que je jette mon argent par les fenêtres en publiant dans le réseau ? . . . . .                                           | 58        |
| Et si quelqu'un crée plusieurs identités ? . . . . .                                                                             | 58        |
| Une personne fortunée ne peut-elle pas simplement « acheter » plus d'identités (ou créer des communautés virtuelles) ? . . . . . | 61        |
| Et les profiteurs qui ne veulent que lire sans rien donner à la communauté ? . . . . .                                           | 64        |
| Neutralité financière . . . . .                                                                                                  | 65        |

|                                                                                                 |           |
|-------------------------------------------------------------------------------------------------|-----------|
| Volontariat, responsabilité et liberté . . . . .                                                | 67        |
| L'interrupteur liberté-totalitarisme (et la délégation) . . . . .                               | 68        |
| Le problème de l'oracle — faire le pont entre le monde numérique et le monde physique . . . . . | 76        |
| <b>Comment fonctionne la vérification</b>                                                       | <b>78</b> |
| Le consensus et le processus de vérification . . . . .                                          | 78        |
| Roles in the verification transaction and authorities . . . . .                                 | 84        |
| Vue d'ensemble des rôles . . . . .                                                              | 84        |
| Émetteur . . . . .                                                                              | 86        |
| Autorité . . . . .                                                                              | 86        |
| Vérificateur . . . . .                                                                          | 90        |
| Sujet . . . . .                                                                                 | 92        |
| Observateur . . . . .                                                                           | 95        |
| Le mécanisme : horodatage et code de défi . . . . .                                             | 95        |
| La chute : vous n'avez pas besoin de vrais observateurs . . . . .                               | 97        |
| Délégation . . . . .                                                                            | 97        |
| La communication entre les rôles . . . . .                                                      | 104       |
| Le contrat social émergent — la politique . . . . .                                             | 104       |
| Fournir des informations sur soi-même . . . . .                                                 | 108       |

|                                                                     |            |
|---------------------------------------------------------------------|------------|
| <b>Crime et châtime</b>                                             | <b>110</b> |
| Crime et châtime . . . . .                                          | 110        |
| <b>Suivre l'argent</b>                                              | <b>122</b> |
| Suivre la trace de l'argent . . . . .                               | 122        |
| Le point faible de l'État — l'argent . . . . .                      | 123        |
| Proposed transition to the state's successor . . . . .              | 124        |
| Évolution, pas révolution . . . . .                                 | 124        |
| Quatre outils qui se soutiennent mutuellement . . . . .             | 127        |
| Système fiscal simple — l'appât d'entrée . . . . .                  | 128        |
| Registre électronique des dépenses (ESR) . . . . .                  | 128        |
| Allocation citoyenne de l'impôt — le poids de la décision . . . . . | 130        |
| Plateforme de négociation avec l'État — le levier . . . . .         | 134        |
| La citoyenneté sans carte d'identité . . . . .                      | 136        |
| Chevauchement et réversibilité . . . . .                            | 140        |
| <b>Conclusion</b>                                                   | <b>143</b> |
| Le chemin existe . . . . .                                          | 143        |
| Remerciements . . . . .                                             | 145        |
| Inspiration . . . . .                                               | 145        |

Relecture et retours . . . . . 145

Outils . . . . . 145

**Glossaire** 148

Glossaire . . . . . 148



# Introduction

## **Avez-vous le sentiment de pouvoir compter sur l'État ?**

Je refuse d'accepter qu'une injustice manifeste soit commise contre moi, ma famille ou quelqu'un de ma communauté (violence physique, fraude, restriction abusive, ...) et que l'État réponde : oui, c'est une injustice, mais n'y touchez pas, sinon vous aurez un problème encore plus grand avec nous. Un tel état de choses est malade, et les gens qui s'en accommodent en sont complices.

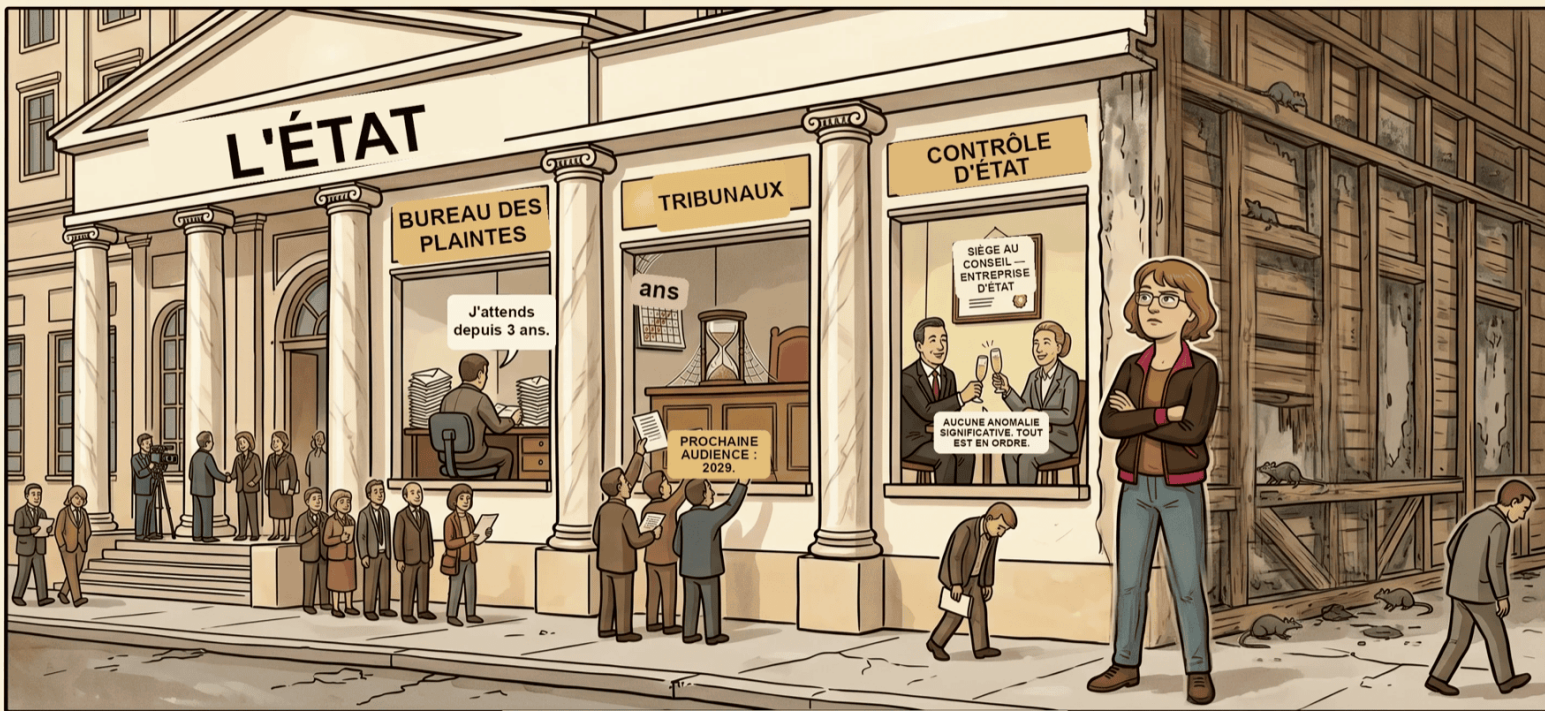
Le résultat est une aliénation mutuelle, un simulacre de communauté, un simulacre d'État, et une désagrégation croissante de la société qui promet de sérieux conflits à venir.

## **L'État peut-il suivre le rythme du changement technologique et social, ou préfère-t-il coller une interdiction ?**

Je pourrais faire semblant de traiter la stagnation, l'incompétence et la corruption comme la stabilité déclarée de l'État de droit et de la tradition, mais je n'en ai plus envie. Je me mentirais à moi-même et je vous mentirais.

## **Ressentez-vous la condescendance des fonctionnaires et des élus lorsque vous osez critiquer quelque chose que vous payez ?**

Je refuse de considérer que des membres de la société sont indignes de façonner les règles valables pour tous, simplement parce qu'ils n'excellent pas dans ces compétences relationnelles qui sont aujourd'hui l'unique condition suffisante pour devenir un élu dans les institutions codifiées par l'État. J'ai foi que l'immense majorité sait prendre soin d'elle-même, de ses proches et de sa communauté — et qu'elle y



**Je refuse de l'accepter.**

voit une part de sa philosophie de vie. La plupart des gens que j'ai appris à connaître autour de moi sont ainsi.

Mais j'ai aussi rencontré de véritables salauds qui l'étaient précisément parce qu'ils savaient jouer le jeu — ce jeu où la communauté n'a pas le droit de leur adresser un retour, où l'État les protège pour que personne ne trouble l'ordre qui menacerait l'essence même de l'État : assurer une vie facile à ceux qui occupent les étages supérieurs de la hiérarchie du pouvoir et de la hiérarchie de ses institutions. La féodalité a été remplacée par le règne des populistes et des élitistes.

### **Aimez-vous que les autres vous dictent comment mener votre vie ?**

Je n'accepte pas l'état actuel des choses comme un donné parfait et définitif. Je dois être responsable de ma manière de me conduire, et pourtant je suis susceptible quand on me dit quelles bonnes valeurs je devrais épouser. Et vous ?

## **De quoi parle ce livre ?**

Imaginez un réseau social de réputation où quiconque le souhaite peut créer ses propres clés (créer son identité), se faire inviter par des membres de sa communauté, ou s'y aventurer seul. Vous bâtissez votre réputation et puisez dans les données de réputation utiles sur les autres quand vous en avez besoin. Vous sollicitez le soutien de votre communauté lorsqu'une injustice survient — vous exposez votre cas et fournissez ce que vous avez sur l'affaire, et la communauté examine, décide selon sa pertinence de transmettre ou non à d'autres, et de la manière de sanctionner le coupable.

Ce court livre tout entier traite de ce qui doit se trouver sous le capot pour que cela fonctionne aussi simplement à l'extérieur. Si vous persévérez, je vous promets qu'un monde qui peut aujourd'hui paraître complexe et difficile à comprendre à bien des égards s'ouvrira à vous, plus compréhensible et plus clair.

Vous verrez que beaucoup de mauvaises choses peuvent être agencées de sorte qu'elles ne soient plus aussi injustement rentables pour les mauvais acteurs. Et ce n'est pas un outil auquel il faudrait rester collé en ligne en permanence — il suffit d'y recourir lorsqu'on en ressent le besoin.

Je vous promets encore que l'agencement décrit ici se sentira plus proche des motivations réelles des gens, et qu'il n'a pas besoin de les remodeler au nom d'un quelconque -isme.

Et enfin, nous montrerons comment gérer une transition non révolutionnaire vers un état où les communautés redeviennent des unités sociales pleinement fonctionnelles et n'ont plus à faire semblant.

### Article technique

---

Ce livre est un compagnon explicatif de l'article technique original « *Decentralized Reputation Network: A Framework for Voluntary and Uncorruptible Societal Organization* » (Pavel Kudrna, 2026). Si la description formelle de l'architecture, l'algorithme de sélection des vérificateurs et la justification des mécanismes économiques vous intéressent, je vous recommande de commencer par là.

## ■ Les chapitres se construisent l'un sur l'autre

Le livre est écrit comme un argument continu — chaque chapitre s'appuie sur le précédent. Les concepts introduits dans une partie sont utilisés dans les parties suivantes, y compris dans les notes de bas de page. Je ne recommande pas de lire dans le désordre.

## ■ À qui ce livre s'adresse-t-il ?

Malgré son format visuellement accueillant, le public cible principal est le lecteur plus spécialiste, préoccupé par les principes des agencements socio-économico-politiques possibles de la société humaine. Parvenir à un point où je pourrais expliquer l'ensemble du sujet de manière accessible au plus large public exige encore un long chemin de construction d'une véritable stratégie de communication.

J'accueille volontiers les suggestions pour rendre ce petit ouvrage, ou toute édition révisée qui lui ferait suite, plus compréhensible.

### **Avertissement**

Je ne sais pas qui vous êtes, quel âge vous avez, ni combien de promesses non tenues vous avez dû subir dans votre vie. J'en ai fini d'en faire ici. À la place, je veux vous avertir que le seul résultat de ce que





**Il y a plus sous le capot. Restez avec moi.**

vous apprendrez ici sera peut-être la prise de conscience qu'il n'existe probablement pas de chemin où quelqu'un d'autre nettoierait à votre place le désordre d'aujourd'hui. Je ne fais que décrire un cadre/outil qui pourrait rendre ce nettoyage plus simple et plus transparent. Sur cette base, je tenterai de préparer une expérience/simulation sociale, d'en corriger les défauts éventuels, ou d'enterrer complètement l'idée s'il s'avère qu'elle présente des fissures fondamentales dans sa conception.

### **Une requête**

J'apprécierais profondément que, même après avoir terminé ce livre, vous gardiez l'esprit ouvert à l'idée et suiviez où elle va et comment elle résiste à la critique de fond. J'apprécierais encore davantage votre implication ultérieure — essayer de briser par vos propres idées les principes d'équilibre proposés, et ainsi mieux éprouver à quel point le système est prêt face au comportement humain réel.

Sans vous et votre implication, l'idée reste une théorie dans un tiroir. Sans vous, vos contributions et vos dons financiers, nous ne pourrions pas pousser le projet vers une véritable expérience sociale, et donc vers une véritable maturité. Sans vous et votre critique de fond, nous stagnerons où nous en sommes, ou nous laisserons engloutir par le Graal des centristes — le totalitarisme absolu et irréversible. C'est à nous de choisir quel chemin prendre, ou de rester spectateurs.

### **Le défi**

Nous ne posons pas exactement un fardeau léger sur vos épaules. Vous portez déjà le coût d'une société gérée avec prodigalité, à travers des manuels incantatoires et occultistes affirmant que la société se gouverne au mieux de manière centralisée — et j'ai le culot de vous demander encore davantage, et d'aller à l'encontre de ces tendances. Je suis conscient qu'il nous faudra traverser l'effondrement de la plus grande chaîne de Ponzi de l'histoire — le système de retraite par répartition — sans laisser plusieurs générations mourir de faim.



**Un monde meilleur vaut ce poids.**



Et pourtant je vous le demande malgré tout : léguons enfin à nos enfants un monde meilleur et laissons derrière nous l'héritage d'avoir accompli ce changement. Libérer la croissance économique pourrait être une solution partielle à la difficulté qui se profile. Nous pourrions alors dire à nos descendants que ce fut une sacrée aventure et qu'elle n'a pas été vaine.

## ■ Le problème

---

Seule une liberté équilibrée par une responsabilité directe peut véritablement libérer un potentiel énorme que le monde n'a jamais connu.



**Entrez. Les plans sont sur la table.**

# Conditions préalables essentielles au changement

## Conditions préalables essentielles au changement

La condition fondamentale d'un changement pour le mieux, c'est que le subordonné devienne le supérieur — ou du moins un partenaire à égalité. Cela signifie reprendre les agendas les plus critiques qui définissent la relation de supériorité et de subordination. Ces agendas reposent sur des preuves d'appartenance aux communautés qui constituent les citoyens de l'État. Ce sont l'information et sa vérifiabilité par une autorité disposant d'une réputation substantielle au sein de ces communautés.

Pour dépasser le système actuel, je suis arrivé à cinq conditions préalables que j'explique ensuite de la manière dont je les comprends. On peut se représenter ces conditions comme les piliers qui portent la construction du système décrit dans le reste du livre. J'ai d'abord choisi les piliers selon ma propre préférence puis, en raisonnant avec eux, j'ai peu à peu affiné ma compréhension de chacun jusqu'à la forme ci-dessous.

Passons ces cinq piliers en revue un à un.

# CONDITIONS PRÉALABLES AU CHANGEMENT

VOLONTARIAT



VOLONTARIAT

Je décide par moi-même.

ORGANISATION



ORGANISATION

Ensemble, sous l'autorité de personne.

RÉSILIENCE



RÉSILIENCE

Ne peut pas être censuré.

CONSENSUS



CONSENSUS

Compromis sous la pression.

INCORRUPTIBILITÉ



INCORRUPTIBILITÉ

On ne peut pas tous les acheter.

**Sans ces cinq piliers, tout changement n'est qu'une perte de temps.**

## ■ Volontariat

---

Dans notre cas, le volontariat signifie que je ne suis pas contraint de participer au fonctionnement du réseau de réputation décentralisé. Je ne peux toutefois pas revendiquer un droit formulé positivement selon lequel le réseau ne consignerait aucune information à mon sujet — que des informations sur moi finissent ou non dans le réseau de réputation ne dépend que de moi, de mon comportement, de mes actes et de ma responsabilité.





**Volontaire — jusqu'à ce que la responsabilité vous rattrape.**



## ■ Organisation

---

Un individu seul ne peut pas briser le système, c'est pourquoi l'État contrôle l'association des personnes comme moyen d'empêcher les activités susceptibles de menacer sa structure et son fonctionnement. Peu importe que les gens s'organisent pour ou contre. Par l'organisation, il est possible d'atténuer l'impact des punitions exemplaires lorsque quelqu'un ose changer l'État contre sa volonté.

Ne fixons pas de buts communs, mais nous pouvons faire une partie du chemin ensemble. La forme la plus naturelle est l'association en communautés — mais elles doivent disposer de tous les outils dont elles ont besoin pour ne pas rester de simples simulacres de communautés.

## ■ Résilience

---

Le chemin choisi pour changer l'État — ou pour transiter vers son successeur — ne doit pas dépendre de la permission de l'État. Les outils et les manières de les utiliser doivent être aussi incensurables que possible. En clair, le coût de leur censure doit être astronomique. Sans cela, tout l'effort ne fait que consumer du temps et de l'énergie vitale.

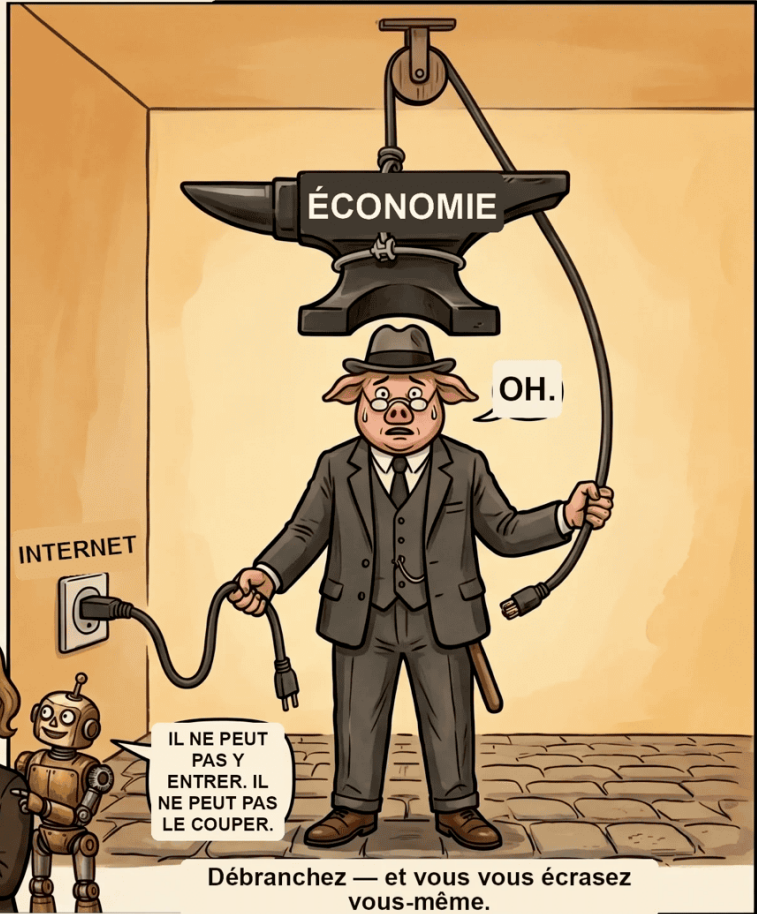
# CONDITION 2 SUR 5 : ORGANISATION



**Un individu ne peut pas briser le système. Une communauté le peut.**



# CONDITION 3 SUR 5 : RÉSILIENCE



**AUCUNE PERMISSION À DEMANDER. AUCUNE PRISE À DÉBRANCHER.**

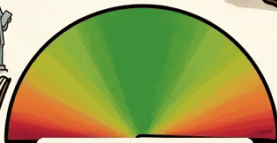
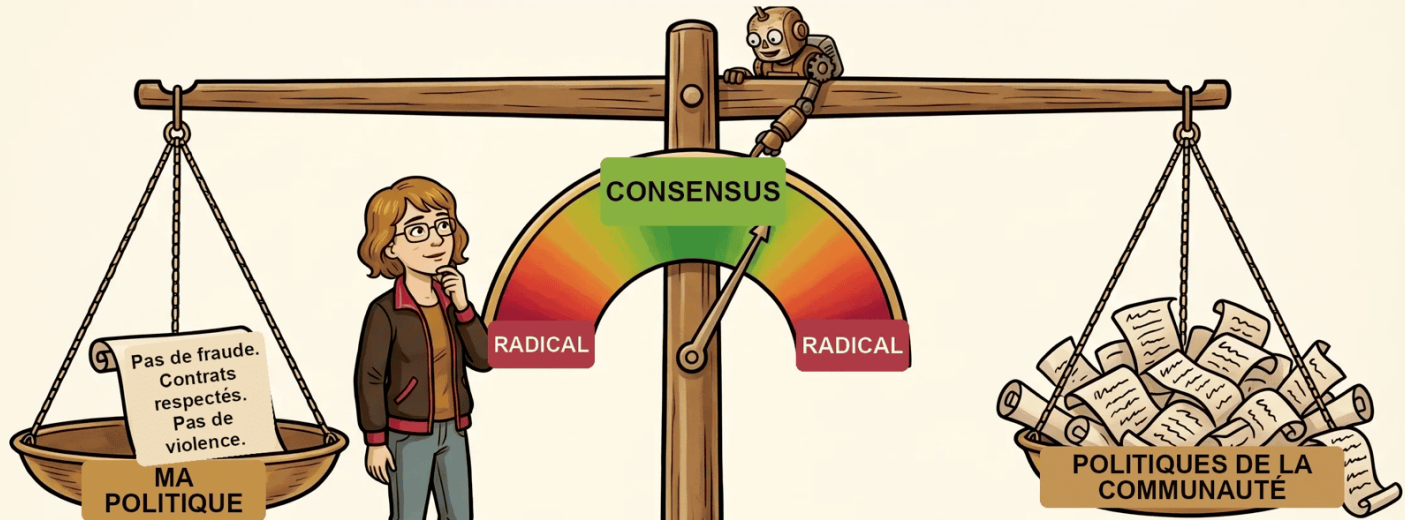
## ■ Consensus

---

La solution proposée doit, par sa nature même, contenir un mécanisme de négociation du consensus ainsi qu'une composante répressive pour les cas où le consensus est violé. Il n'est pas nécessaire que ce soit un accord volontaire gagnant-gagnant. Il suffit que les circonstances et la pression sociale assurent un compromis au sein d'une communauté et entre communautés.

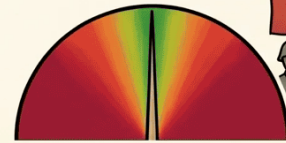
**RESTEZ DANS LA ZONE — PAS UN RADICAL.**

Vous pouvez être différent. Mais pas trop.



SOCIÉTÉ LIBRE

La zone de tolérance s'élargit  
avec la liberté de la culture.



CONDITION 4 SUR 5 : CONSENSUS SOCIÉTÉ AUTORITAIRE

**LE CONSENSUS EST UNE ZONE DE TOLÉRANCE, PAS UN ACCORD UNANIME.**

## ■ Incorruptibilité

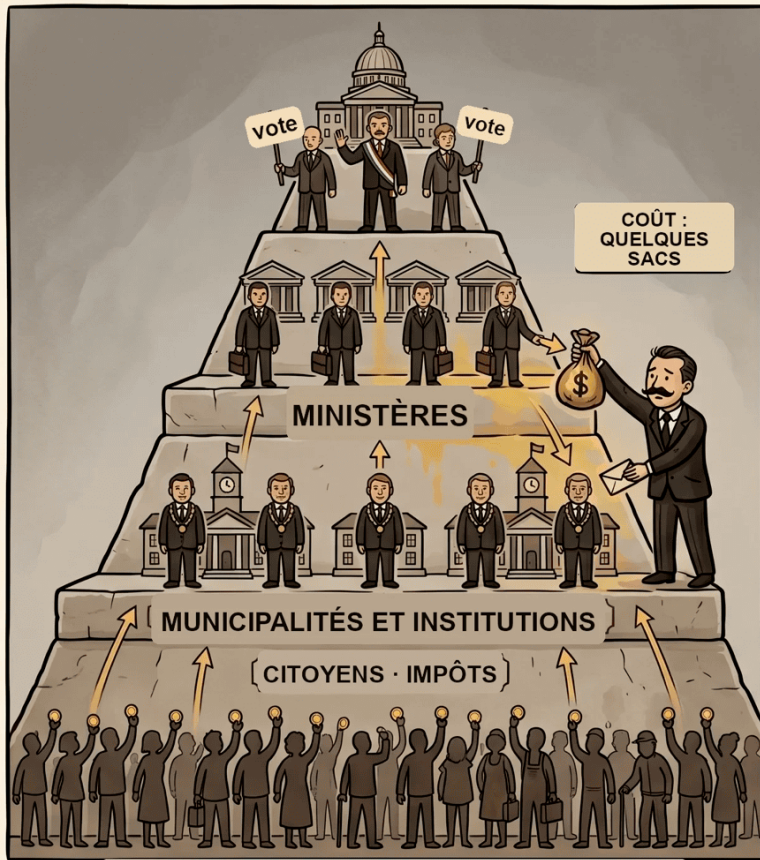
L'incensurabilité défend le système de l'extérieur. Mais un réseau de personnes peut aussi pourrir de l'intérieur — une autorité se fait capturer, une règle déclarée est discrètement abandonnée, des participants sont achetés en silence. L'incensurabilité serait une victoire creuse si les gens à l'intérieur pouvaient être corrompus sans conséquence.

L'incorruptibilité n'est pas le résultat d'une unique astuce ingénieuse. Elle émerge de **plusieurs principes de la conception proposée agissant de concert** — la pression contre la corruption est répartie dans toute l'architecture, et les parties individuelles se renforcent mutuellement. Comment cela est exactement obtenu, nous le montrerons progressivement — dans la description de l'outil, dans la vérification et dans le chapitre sur le châtiment. À la fin, nous récapitulerons tout ce qui aura été édifié.

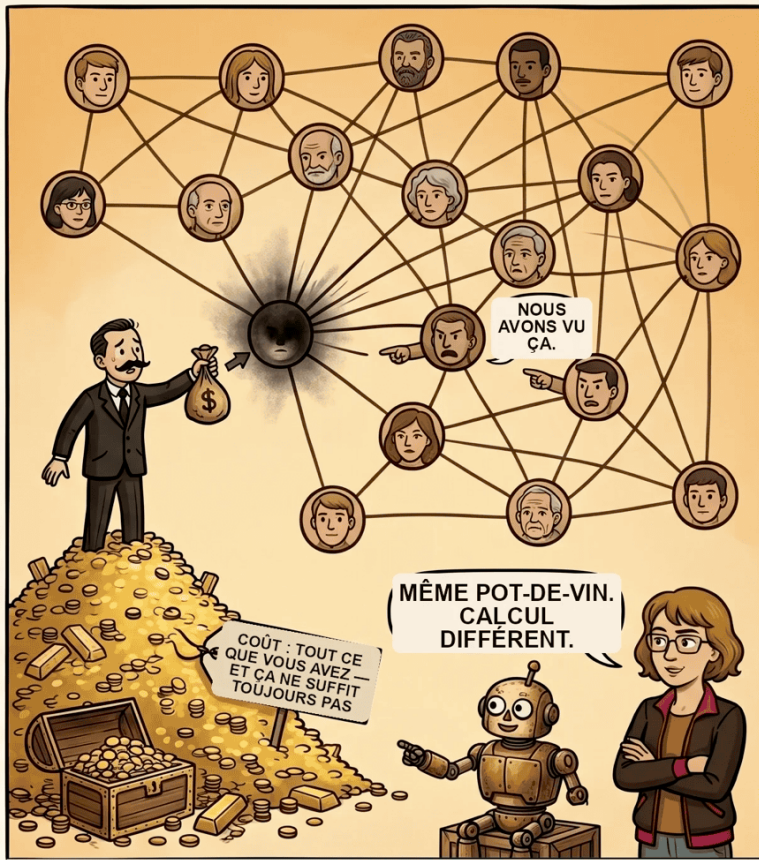
L'incorruptibilité est à la fois une condition préalable de la conception et une propriété émergente du résultat. C'est la seconde ligne de défense — celle tournée vers l'intérieur — et sans elle, la Résilience n'est qu'un demi-bouclier.



# CONDITION 5 SUR 5 : INCORRUPTIBILITÉ



Corrompez quelques étages supérieurs — la base paie quand même.



Corrompez-en un — il perd sa réputation pour toujours. Corrompez-les tous — vous serez ruiné avant.

## LA CORRUPTION A UN PRIX. DANS LE MAILLAGE, IL EST TROP ÉLEVÉ.

# L'outil

## Réseau social fondé sur la réputation

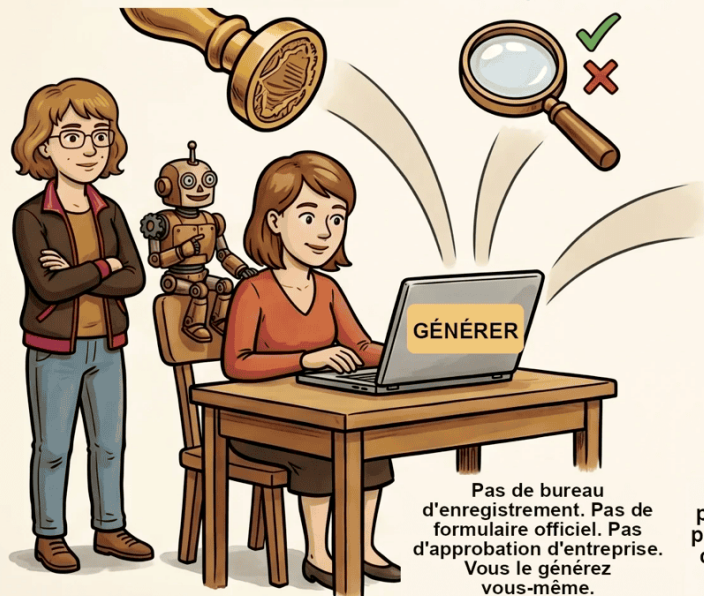
Pour provoquer le changement, il nous faut un outil soigneusement conçu. Nous allons d'abord l'esquisser brièvement ; dans les chapitres suivants, nous examinerons chaque pièce plus en détail et en ajouterons d'autres. Imaginez un réseau social incensurable, mondial et décentralisé, dans lequel vous pourriez créer et gérer en toute sécurité votre identité mandataire — une identité dite décentralisée (DID). Une DID est une identité numérique que vous créez et contrôlez vous-même, sans dépendre d'aucune autorité centrale. Personne ne peut vous la retirer ni la falsifier, car elle est signée cryptographiquement avec votre clé privée (ou vos clés, via multisig).

# VOTRE IDENTITÉ, VOS CLÉS, VOS RÈGLES

## VOUS LE CRÉEZ VOUS-MÊME

**CLÉ PRIVÉE** — signe en votre nom. Vous seul la détenez. Ne la partagez jamais.

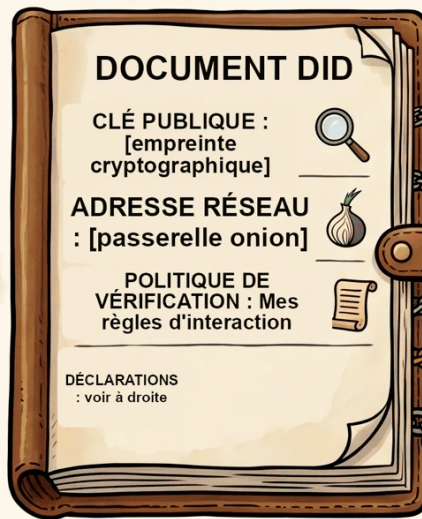
**CLÉ PUBLIQUE** — vérifie vos signatures. Visible par le réseau.



GÉNÉRER

Pas de bureau d'enregistrement. Pas de formulaire officiel. Pas d'approbation d'entreprise. Vous le générez vous-même.

## VOTRE DOCUMENT DID



### DOCUMENT DID

**CLÉ PUBLIQUE :**  
[empreinte  
cryptographique]

**ADRESSE RÉSEAU**  
: [passerelle onion]

**POLITIQUE DE  
VÉRIFICATION :** Mes  
règles d'interaction

**DÉCLARATIONS**  
: voir à droite

Ceci est votre identité publique. Tout le monde peut la lire. Seule VOTRE clé privée peut y signer des modifications.



Aucun État ne peut la révoquer.

## DÉCLARATIONS — DES FAITS VÉRIFIÉS À VOTRE SUJET

**CITOYENNETÉ :** République tchèque — vérifié par le notaire municipal

**ÉDUCATION :** Master en informatique — vérifié par le réseau des anciens élèves de l'université

**PROPRIÉTÉ :** Propriétaire de l'appartement n° 42 — vérifié par le registre communautaire local

**TÉMOIN PASSIF :** A ignoré une infraction — politique non respectée — déposé par des témoins du voisinage

**FRAUDE :** A escroqué les économies d'un voisin — déposé par le tribunal communautaire local

Les déclarations sont des affirmations vérifiées. Le bon et le mauvais. Les autorités y engagent leur réputation.



**CARTE D'IDENTITÉ D'ÉTAT —  
RÉVOCABLE :** l'État peut  
l'annuler à tout moment.



**DID — IRRÉVOCABLE :** seule votre  
clé privée peut signer des  
modifications.

## Votre identité. Vos clés. Vos règles. Aucune permission requise.



## Note

Une implication est qu’une telle identité pourrait progressivement remplacer les documents d’identification émis par l’État — mais nous y reviendrons dans le chapitre sur la transition.

Dans un tel réseau, vous pourriez signaler à travers votre identité que quelqu’un vous a causé un préjudice (et plus tard, éventuellement, qu’il l’a réparé ou a été contraint de le faire). Pour que ce retour — dirigé vers l’auteur du préjudice — ait de la valeur en tant que source pertinente, l’inscription d’une information dans le réseau doit coûter du temps, de l’énergie et de l’argent — et par-dessus le marché, une preuve vérifiable doit être produite pour les autres, attestant qu’il ne s’agit pas de bavardage oiseux.

Lire une information serait facile et relativement bon marché, mais créer un enregistrement individuel serait coûteux et exigeant. L’écriture suivrait un protocole clair, dans lequel un calcul selon l’algorithme choisi détermine strictement quelle DID solliciter pour vérifier l’information soumise, et comment procéder pour que le participant sélectionné traite l’information en votre nom, la publie et en devienne le vérificateur.

## ■ Algorithme vs radicalisme

---

La sélection algorithmique des vérificateurs garantit que les émetteurs d'informations non radicales maintiendront, avec le temps, un équilibre quasi neutre entre les coûts des informations publiées et les récompenses pour la vérification.



# PUBLIER COÛTE DU TEMPS, DE L'ÉNERGIE ET DE L'ARGENT

ÉCRIRE DANS LE RÉSEAU N'EST JAMAIS GRATUIT — LIRE L'EST

TROIS CANAUX — TOUS RÉELS

## TEMPS



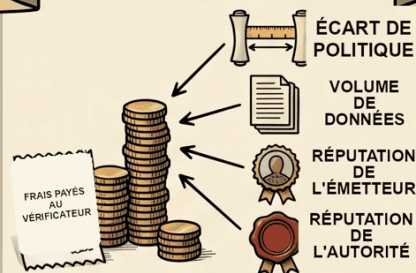
vous attendez pendant que l'algorithme choisit un vérificateur et que le vérificateur lit votre enregistrement.

## ÉNERGIE



signer, hacher, vérifier — chaque étape est un calcul réel et de l'électricité réelle.

## ARGENT



plus votre déclaration s'éloigne de la politique du vérificateur, plus l'enregistrement est volumineux, et moins l'émetteur ou son autorité inspirent confiance — plus les frais sont élevés.

## CE QUI SE PASSE ENSUITE

- La chaîne de vérification en trois étapes — voir COMMENT L'ALGORITHME CHOISIT UN VÉRIFICATEUR, COMMENT LE VÉRIFICATEUR RÉPOND, LE CHOIX DE L'ÉMETTEUR
- Pourquoi une écriture coûteuse protège la réputation — plus loin dans le chapitre

le bruit coûte cher. Le signal a de la valeur. C'est pourquoi le réseau facture l'écriture, pas la lecture.

## coût selon les itérations

CHACQUE NOUVELLE TENTATIVE COÛTE PLUS CHER

la réponse du vérificateur s'intègre à la chronologie — voir LE CHOIX DE L'ÉMETTEUR et COMMENT L'ALGORITHME CHOISIT UN VÉRIFICATEUR



chaque rejet ou nouveau tirage s'ajoute à la chronologie que l'algorithme absorbe — et la tentative suivante coûte plus cher sur les trois plans.

## asymétrie de lecture

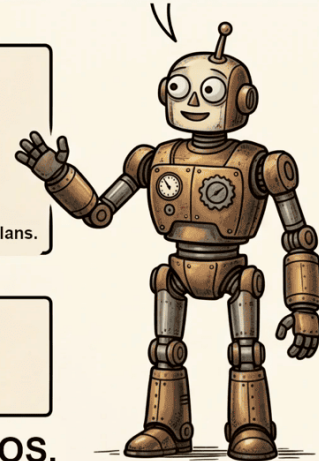
LIRE EST BON MARCHÉ



consultation gratuite

n'importe qui peut lire la réputation et les enregistrements — seule l'écriture coûte. Cette asymétrie fait partie de la conception.

L'ÉCRITURE COÛTE — PAS LA LECTURE. L'ASYMÉTRIE EST LE PROPOS.



Voyons comment l'algorithme sélectionne un vérificateur.

## ■ Algorithme

La sélection algorithmique choisit de manière non déterministe un vérificateur différent (ou un ensemble de vérificateurs possibles) pour différentes informations. Un hash (une fonction mathématique à sens unique qui produit une « empreinte » unique à partir de n'importe quelle entrée — comme l'empreinte digitale d'un document) du document DID complet détermine la position sur un anneau de hachage cohérent et sélectionne les vérificateurs candidats.

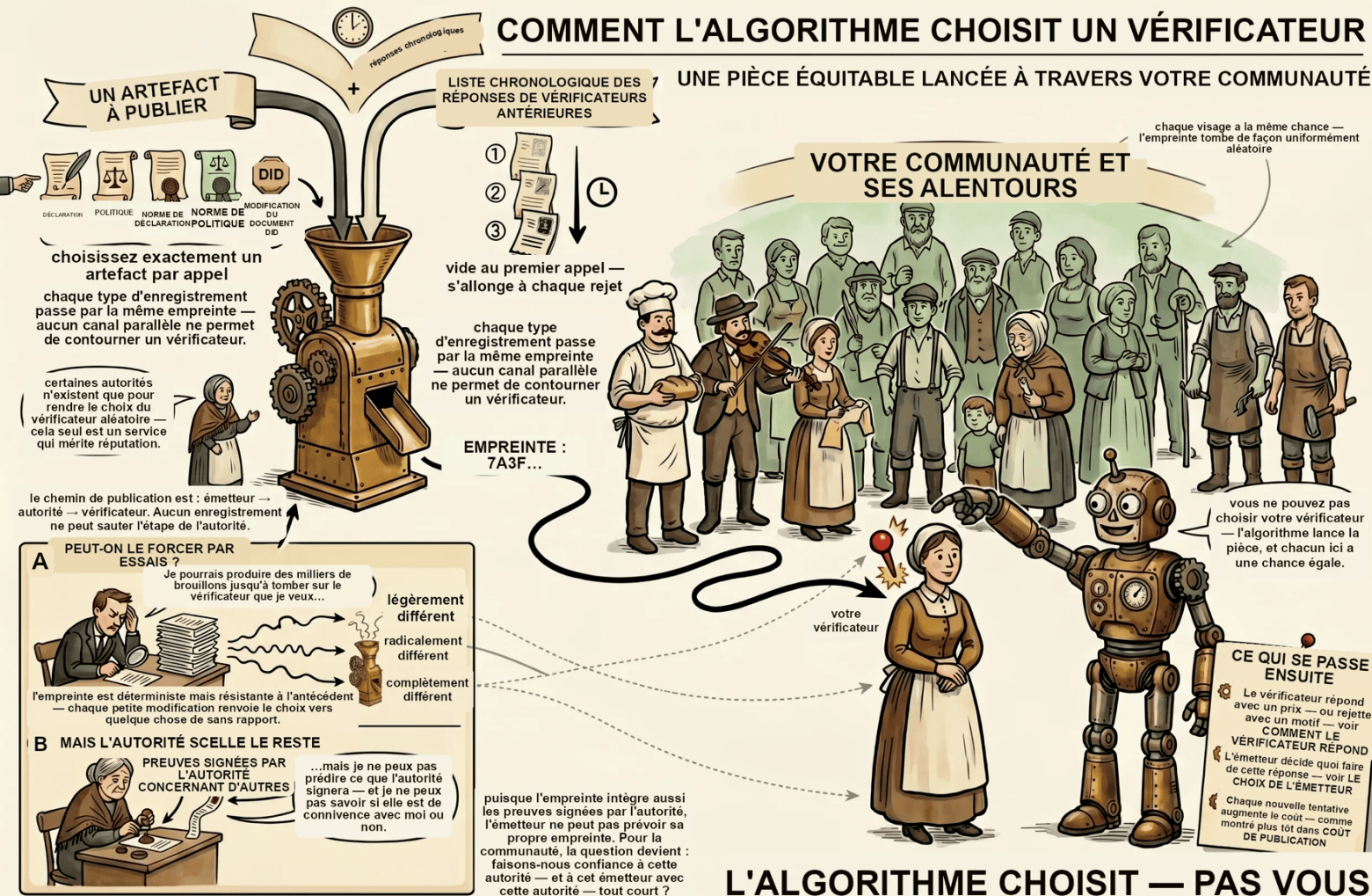
$$\text{verifier\_DID} = \text{hash}(\text{DID\_document})$$

En clair : l'algorithme prend l'ensemble de votre document DID, en calcule une empreinte, et cette empreinte détermine votre vérificateur.

Avec le premier vérificateur que l'algorithme sélectionne, vous, en tant qu'émetteur, pouvez ne pas aboutir — votre réputation ou vos paramètres déclarés peuvent ne pas satisfaire ses exigences. Vous poursuivriez algorithmiquement la recherche du suivant en effectuant une nouvelle itération récursive, qui vous attribue un vérificateur supplémentaire. À chaque étape, la « distance » jusqu'au vérificateur cible croît, tout comme les métadonnées d'accompagnement qui doivent être publiées. À mesure que les données croissent, les coûts augmentent naturellement (non seulement à cause de la taille initiale de l'assertion, mais aussi à cause des métadonnées qui s'accumulent à chaque rejet). Une information

# COMMENT L'ALGORITHME CHOISIT UN VÉRIFICATEUR

UNE PIÈCE ÉQUITABLE LANCÉE À TRAVERS VOTRE COMMUNAUTÉ



crédible passe bien plus aisément que des lubies dénuées de sens. Il appartient à chacun de décider quel prix il est prêt à supporter et à quel point l'enregistrement lui importe — le radicalisme finit à coup sûr par coûter cher.



# COMMENT LE VÉRIFICATEUR RÉPOND

ACCEPTER AVEC UN PRIX — OU REJETER AVEC UN MOTIF

le vérificateur évalue quatre éléments avant de répondre.



## REJETER — AVEC UN MOTIF



- la réputation de l'émetteur est trop basse pour moi
- l'autorité derrière cet enregistrement n'est pas une autorité en qui j'ai confiance
- la politique de l'émetteur est trop éloignée de la mienne pour être conciliée
- le document lui-même ne respecte pas les règles de ma politique

le vérificateur note le POURQUOI — sa réponse alimente la tentative suivante.

## ACCEPTER — AVEC UN PRIX



ÉCART DE POLITIQUE

VOLUME DE DONNÉES

RÉPUTATION DE L'ÉMETTEUR

le vérificateur accepte de publier — mais le prix reflète à quel point la déclaration s'écarte de sa politique, combien de données elle contient, et à quel point l'émetteur est digne de confiance.

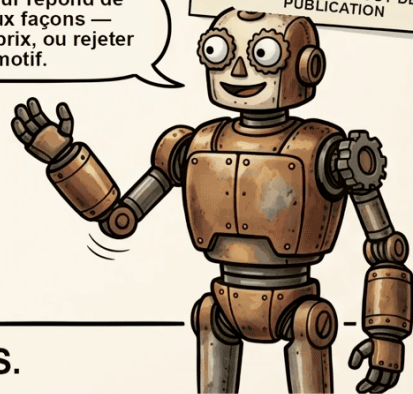
la réponse du vérificateur est ajoutée à la liste chronologique — comme montré dans COMMENT L'ALGORITHME CHOISIT UN VÉRIFICATEUR

quoi que dise le vérificateur, sa réponse devient une donnée d'entrée pour l'appel suivant.

chaque vérificateur répond de l'une de ces deux façons — accepter avec un prix, ou rejeter avec un motif.

## CE QUI SE PASSE ENSUITE

- L'émetteur décide quoi faire de cette réponse — voir LE CHOIX DE L'ÉMETTEUR
- Chaque réponse modifie le coût de la tentative suivante — comme montré plus tôt dans COÛT DE PUBLICATION



LE VÉRIFICATEUR FIXE UN PRIX — OU VOUS DIT POURQUOI PAS.



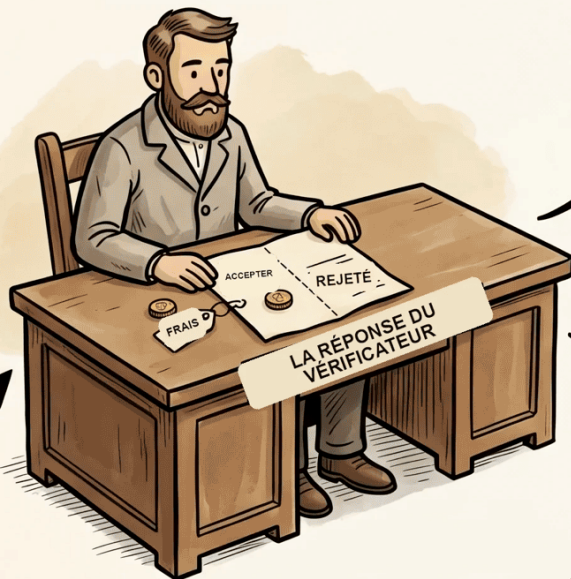
Quoi que le vérificateur décide en réponse à votre demande de vérification, la balle est de nouveau dans le camp de l'émetteur : il peut accepter l'offre de services de vérification du vérificateur, intégrer la réponse dans la chronologie et réessayer (à un coût plus élevé), ou renoncer et encaisser le coût irrécupérable.

Pour donner à votre information un poids accru et une meilleure chance d'acceptation auprès des vérificateurs, vous — en tant qu'émetteur ayant un intérêt dans l'information à émettre — pourriez recourir aux services d'une **autorité de confiance**. L'autorité soit rejette l'information soumise, soit l'accepte et engage sa bonne réputation dessus. L'autorité demande généralement des preuves du monde réel, les vérifie et les classe. Le produit est un protocole de son évaluation du cas donné à l'instant donné. Voyez une autorité comme un spécialiste d'un certain type de service, dans le monde réel comme numérique — par exemple un enquêteur, un auditeur, un assureur, un fournisseur d'une certaine classe de biens (en somme, n'importe quel acteur économique du marché).

# LE CHOIX DE L'ÉMETTEUR

## QUE FAIRE DE LA RÉPONSE DU VÉRIFICATEUR

quoi qu'ait dit le vérificateur, l'émetteur a maintenant UNE réponse sur la table.



retour à COMMENT L'ALGORITHME CHOISIT UN VÉRIFICATEUR — montré plus tôt

seul le chemin de la nouvelle tentative boucle — accepter et abandonner mettent tous deux fin à l'histoire.

TROIS ISSUES POSSIBLES

ACCEPTER L'ACCORD

réseau-DID



SEULEMENT SI ACCEPTÉ

l'émetteur paie les frais — l'enregistrement est publié dans le réseau. Disponible uniquement si le vérificateur a accepté.

RÉESSAYER



petite machine à broyer



la réponse est intégrée à la chronologie — l'algorithme relance. Fonctionne que le vérificateur ait accepté à un prix que l'émetteur n'aime pas, ou rejete d'emblée.

ABANDONNER



le temps et l'énergie déjà dépensés ne reviennent pas

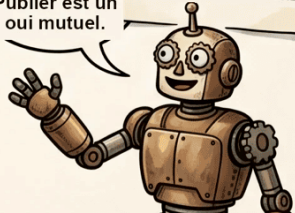


l'émetteur abandonne le brouillon. Rien n'est publié — mais rien n'est payé non plus.

CE QUI SE PASSE ENSUITE

le vérificateur décide comment — l'émetteur décide si. Publier est un oui mutuel.

- Chaque nouvelle tentative modifie le coût de la suivante — comme montré plus tôt dans COUT DE PUBLICATION
- La réponse du vérificateur elle-même — comme montré plus tôt dans COMMENT LE VÉRIFICATEUR RÉPOND

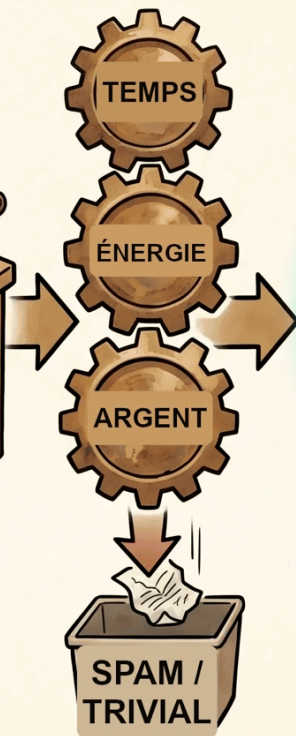


LE VÉRIFICATEUR PROPOSE — L'ÉMETTEUR DISPOSE.

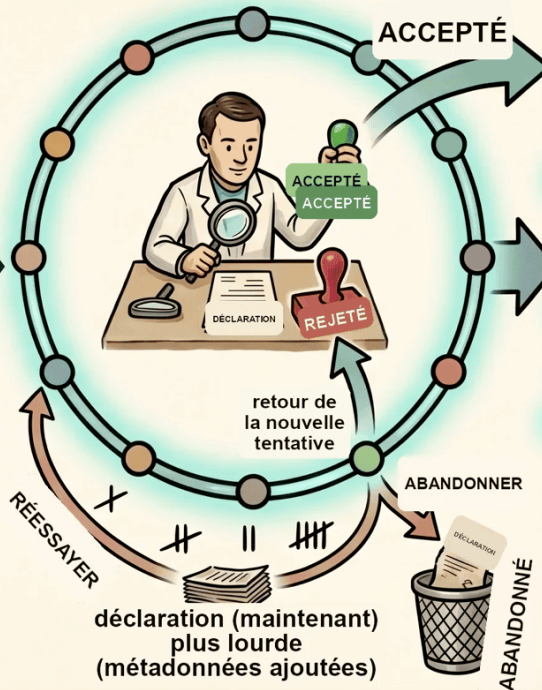
## ÉTAPE 1 — PUBLIER UNE DÉCLARATION



## ÉTAPE 2 — FILTRE DE QUALITÉ



## ÉTAPE 3 — VÉRIFICATION RÉCURSIVE



## ÉTAPE 4 — ENREGISTREMENT PERMANENT



Permanent.  
Vérifiable.  
Public.

# COÛTEUX À FALSIFIER. BON MARCHÉ À VÉRIFIER.

Au moment où vous tenterez de publier une information dans le réseau, celui-ci contiendra probablement déjà des informations sur ses acteurs — ce sont des signaux de réputation. Savoir comment lire les signaux de réputation — ce qu'ils signifient pour vous dans différentes situations et quels risques ils comportent — peut ne pas être trivial. Chaque participant peut regarder les enregistrements de réputation différemment à travers sa DID, selon la situation à laquelle il fait face vis-à-vis de sa contrepartie. La contrepartie est-elle un payeur fiable, ou dois-je exiger l'argent d'avance pour une transaction commerciale ? Le produit proposé fait-il l'objet d'avis signalant une fraude ou des défauts cachés ? Cherche-t-elle à se soustraire à sa responsabilité contractuelle lorsque quelque chose tourne mal ? Parfois, une vue plus complexe de la cohérence globale de la contrepartie est utile — cela dépend des préférences de celui qui demande l'aperçu. Le marché pourrait offrir des produits et services qui simplifient, traitent et clarifient la lecture de la réputation dans le contexte de la situation en cause. Diverses autorités et les services qu'elles proposent peuvent aussi servir à cette fin.



# COMMENT LIRE LA RÉPUTATION

## DÉCISION ÉCLAIRÉE



Elle sait à qui elle a affaire.

## CONFIANCE AVEUGLE



Il n'a aucune idée de qui il a affaire.

AVANT D'ACCORDER UN CRÉDIT. AVANT DE SIGNER. AVANT DE FAIRE CONFIANCE.



## ■ Exemples

Les informations qui intéressent typiquement les émetteurs — et qui ont de la valeur pour les autres — concernent des événements dépassant la communication interpersonnelle ordinaire, dans le monde réel ou virtuel.

Exemples négatifs : - preuve d'actes criminels (par ex. audités par un organe d'enquête de confiance) - preuve indirecte (faible en elle-même, mais statistiquement cumulative) — par ex. présence répétée à proximité de plusieurs vols en peu de temps → toujours une coïncidence ? - rupture de contrat

Exemples positifs : - préjudice réparé (volontairement ou sous la pression de la communauté à titre de sanction) - acceptation et exécution d'une peine proposée par l'autorité X - l'autorité X a révoqué la reconnaissance des droits de propriété de l'auteur dans une certaine mesure

Il appartient à chacun de rassembler les informations disponibles sur la contrepartie et d'en évaluer les risques selon ses préférences.

# QUELS TYPES DE DÉCLARATIONS PEUVENT APPARAÎTRE ?

## EXEMPLES DE L'ARTEFACT DÉCLARATION

( une déclaration est une affirmation à propos de quelqu'un — voici les types que les gens publient. )

— DÉCLARATIONS NÉGATIVES



**AGRESSION**  
a physiquement agressé une autre personne



**VOL**  
a pris le bien d'autrui sans consentement



**FRAUDE**  
a trompé quelqu'un à des fins personnelles



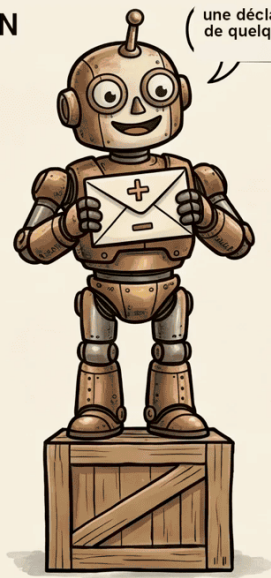
**CONTRAT ROMPU**  
n'a pas honoré une obligation convenue



**DIFFAMATION**  
a répandu un mensonge nuisible



**ABANDON**  
a délaissé des personnes à charge ou des obligations



+ DÉCLARATIONS POSITIVES



**PRÉJUDICE RÉPARÉ**  
a réparé un dommage causé auparavant



**DETTE RÉGLÉE**  
a payé intégralement ce qui était dû



**AIDE APPORTÉE**  
a aidé autrui à ses propres frais



**EXPERTISE VÉRIFIÉE**  
compétence prouvée dans un métier ou un domaine



**SERVICE EXCEPTIONNEL**  
contribution durable à la communauté

exemples seulement — chaque déclaration suit une norme de déclaration, et toute norme peut en ajouter d'autres.

vous n'êtes pas obligé d'adhérer — mais si votre comportement affecte autrui, quelqu'un peut publier une déclaration à ce sujet.

LES DÉCLARATIONS SONT LA FAÇON DONT LE COMPORTEMENT ENTRE DANS LE RÉSEAU.

■ **Le fait que des informations sur vous apparaissent dans le réseau dépend exclusivement de votre propre comportement.**

---

Vous n'êtes jamais obligé de rejoindre un tel réseau, et pourtant des informations sur vous peuvent tout de même y apparaître. Cela dépend exclusivement de vos actes et de l'impact qu'ils ont sur les autres.

# LA COMMUNAUTÉ PEUT EN OUVRIR UN POUR VOUS



Il n'a pas de DID à lui. Il ne s'est jamais inscrit.



Vous n'avez pas ouvert de DID, alors la communauté en ouvre un À VOTRE SUJET. Les déclarations négatives s'y rattachent.



Vous pouvez en ouvrir un vous-même — mais la communauté reliera les deux. La réputation suit la personne, pas la clé.

1. VOUS CAUSEZ  
UN TORT

2. LA COMMUNAUTÉ  
DÉPOSE UNE PLAINTE

3. VOUS NE POUVEZ  
PAS Y ÉCHAPPER

**Vous pouvez renoncer à ouvrir un DID. Vous ne pouvez pas renoncer à votre réputation.**



Ce que je viens d’esquisser brièvement, c’est la manière dont pourrait fonctionner un réseau social inspiré de l’identité décentralisée (DID). L’objectif premier des concepts de DID est de renforcer la vie privée et la liberté par le principe de souscription aux règles que je vais suivre et selon lesquelles je vais vivre — en donnant aux utilisateurs la capacité de décider quelles informations partager et à quelles conditions.

Je propose de relier davantage les DID en un réseau de communication où leurs détenteurs échangent des retours au-delà même des situations où quelque chose est arrivé à quelqu’un et où la communauté ou un individu doit réagir. Une telle comparaison préventive des règles auxquelles nous avons souscrit — avec la possibilité de calculer les conséquences économiques et autres des écarts mutuels dans nos attentes sur la façon dont l’autre partie devrait opérer — pourrait être considérée comme une motivation à trouver un consensus. Au lieu de la liberté, un tel système mettrait l’accent sur la prise de décision volontaire combinée à la responsabilité du comportement réel.

Un individu ne peut pas briser le système à lui seul — un groupe de personnes a de meilleures chances, et un groupe de personnes disposant d’un consensus négocié et de motivations à tirer dans le même sens sur de nombreux sujets a des chances encore plus grandes de résister aux tendances autoritaires. La condition d’organisation du premier chapitre sera remplie une fois deux conditions réunies : le réseau de réputation DID couvre les communautés de façon suffisamment représentative pour que son usage cesse d’être exotique. Et, en même temps, ce segment communautaire devient une minorité économiquement significative, capable de négocier avec assurance avec le reste de la société.

## ■ Volontariat vs liberté

---

La liberté — au sens positif — serait un effet secondaire de l'équilibrage de deux facteurs : le volontariat et la pression de l'entourage vers la responsabilité.

## ■ L'ère de l'IA et la valeur de la réputation

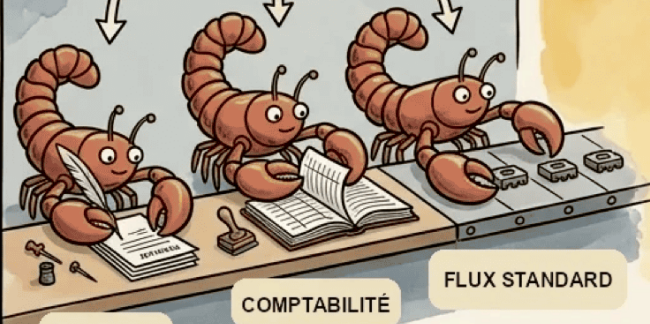
---

À l'ère de l'intelligence artificielle, tout ce qui touche à la pensée cognitive est en train d'être automatisé — et cela pourrait aller encore plus loin. Que reste-t-il alors, dans l'activité humaine, comme avantage concurrentiel ? La réponse est difficile, et l'on trouvera sûrement quelque chose, mais une chose est certaine : la réputation décidera. Un historique vérifiable de votre comportement, de vos engagements et de leur tenue — voilà quelque chose que l'IA ne bâtira pas à votre place.

# SI L'IA FAIT LE TRAVAIL DE RÉFLEXION — QUE VOUS RESTE-T-IL ?

LES AGENTS IA REPRENENT LE TRAVAIL RÉPÉTITIF

FLUX D'ENTREPRISE  
STANDARDISÉS



RÉDACTION

COMPTABILITÉ

FLUX STANDARD

un par un, le travail cognitif  
répétitif est confié aux agents.

QUE RESTE-T-IL DONC POUR UN  
HUMAIN ?



n'importe qui peut choisir la même idée.

qu'est-ce qui distingue un boulanger, un  
menuisier, un atelier d'IA d'un autre ?

LA RÉPUTATION — CE QUI LES DISTINGUE

TIENT  
PAROLE

PARLE AU  
CLIENT

RÉPOND  
DE SON IA

10 ANS,  
AUCUNE  
PLAINTÉ

c'est encore la  
touche humaine  
qui conclut l'affaire.

Même moi, je ne peux  
pas construire cela à  
votre place — cela  
doit venir de vous.



quelqu'un doit répondre de ce que fait  
l'agent — et cette responsabilité ne peut pas  
être déléguée.

sans réputation, tous les boulangers se ressemblent — et la plus grosse marque les avale  
tous.

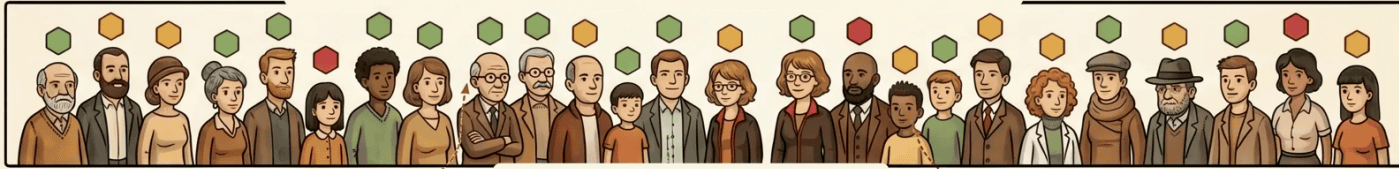
serait-ce la voie décentralisée qui tient l'IA en laisse — ce qui empêche un seul acteur de s'appropriier tout le marché ?

## L'IA AUTOMATISE LE TRAVAIL — LA RÉPUTATION VOUS GARDE HUMAIN.



# L'ÉCONOMIE DE LA VÉRITÉ

bande  
communautaire



UNE COMMUNAUTÉ. DES POSITIONS DIFFÉRENTES.

## IMPOPULAIRE MAIS ACCEPTABLE

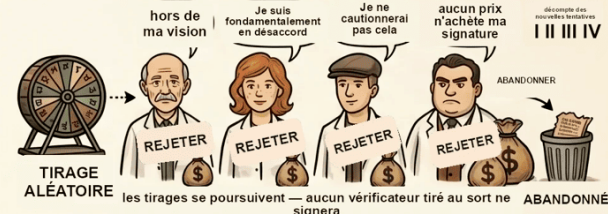
## DANS LE CONSENSUS

## HORS CONSENSUS

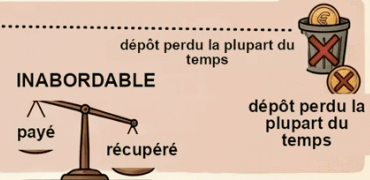
LA  
SOUSSION



LE  
TIRAGE



LE  
REMBOURSEMENT



LE  
REGISTRE

BANDE  
D'OBSERVEURS  
EN BAS

L'ALGORITHME CHOISIT  
ÉQUITABLEMENT. LES GENS  
TARIFENT CE QU'ILS CROIENT.



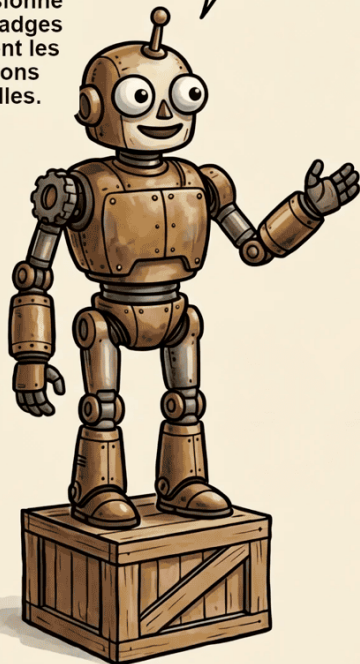
TIRAGE UNIFORME. RÉPONSE NON UNIFORME. PLUS ON S'ÉLOIGNE DU CONSENSUS, PLUS LE PRIX EST ÉLEVÉ.



# CE QUI EST PUBLIÉ DANS LE RÉSEAU

cinq choses peuvent  
être publiées —  
chacune a ses versions.

chaque artefact  
est versionné  
— les badges  
indiquent les  
révisions  
actuelles.



v1

## DOCUMENT DID

votre enregistrement  
d'identité sur le réseau —  
clés, métadonnées,  
adresse réseau.

GÉRÉ PAR : le détenteur du DID



v2

## NORME DE DÉCLARATION

le schéma qu'une  
déclaration doit suivre — ce  
qui compte comme preuve  
valable.

GÉRÉ PAR : une autorité ayant  
une réputation dans le  
domaine



v3

## NORME DE POLITIQUE

le schéma qu'une politique  
doit suivre — la forme des  
règles d'acceptation.

GÉRÉ PAR : une autorité ayant  
une réputation dans le domaine

↓ dérivé de

↓ dérivé de



v4

## DÉCLARATION

une affirmation à propos d'un sujet,  
suivant une norme de déclaration  
— publiée par un émetteur,  
cosignée par l'autorité de la norme  
si l'émetteur et le vérificateur le  
demandent tous deux.

GÉRÉ PAR : l'émetteur  
publie — le sujet est la cible

les déclarations sont de deux  
types — positives (+) et  
négatives (-).



v5

## POLITIQUE DID

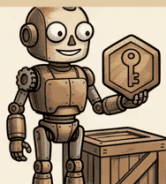
les règles déclarées d'un  
DID — utilisées lors de la  
vérification, du consensus  
et de l'émission.

GÉRÉ PAR : le détenteur du  
DID (une politique par DID)

# CHAQUE ARTEFACT EST VERSIONNÉ. CHAQUE VERSION EST PUBLIQUE.

# QUE CONTIENT UN DOCUMENT DID ?

## EXEMPLES DE L'ARTEFACT DOCUMENT DID



vosre document DID est votre carte d'identité sur le réseau — voici ce qu'il contient.

## CHAMPS QUE VOUS Y TROUVEREZ



### CLÉS ET RÈGLES DE SIGNATURE

chaque clé confère un pouvoir — modifier ce document, émettre une déclaration, agir en tant qu'autorité, gérer une politique, ou déléguer la récupération. Les pouvoirs peuvent être confiés à un autre DID, puis révoqués plus tard.



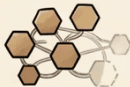
### ADRESSES RÉSEAU

où le réseau peut vous joindre — modifiable sans réécrire votre identité



### CRÉÉ ET VERSIONNÉ

quand cette identité est apparue pour la première fois, et quelle révision vous lisez maintenant



### IDENTITÉS LIÉES

un résumé des DID auxquels vous êtes connecté — une vue pratique, techniquement stockée ailleurs



### MARQUEUR DE SUCCESSION

si votre identité est perdue ou volée, une autorité peut marquer ce DID comme terminé et pointer vers votre successeur

le détenteur du DID rédige chaque nouvelle version — mais chaque version doit passer la vérification avant que le réseau ne la publie.

vous l'écrivez — le réseau le vérifie. Vous ne pouvez pas simplement vous publier vous-même à l'existence.

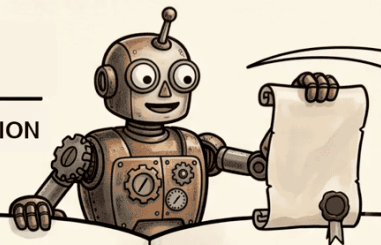


# VOUS RÉDIGEZ VOTRE IDENTITÉ — LE RÉSEAU LA CONFIRME.



# QU'EST-CE QU'UNE NORME DE DÉCLARATION ?

## EXEMPLES DE L'ARTEFACT NORME DE DÉCLARATION



la norme est le formulaire vide — une déclaration est le formulaire rempli. Laissez-moi vous montrer les deux côté à côté.

### LA NORME — LE FORMULAIRE VIDE



#### DID DU SUJET

le DID concerné par cette déclaration



#### DID DE L'ÉMETTEUR

le DID qui signe la déclaration



#### QUAND ET OÙ

une date et un lieu



#### TYPES DE PREUVES APPROUVÉS

seuls ces types de preuves comptent



aucune /  
légère /  
modérée /  
grave

#### ÉCHELLE DE GRAVITÉ

choisissez exactement un échelon — pas de  
texte libre

### UNE DÉCLARATION — LE FORMULAIRE REMPLI



#### DID DU SUJET

did:nwo:alice-9f2b...



#### DID DE L'ÉMETTEUR

did:nwo:magistrates-04...



#### QUAND ET OÙ

3 mars, place du marché



#### TYPES DE PREUVES APPROUVÉS

photographie ✓ — serment de  
témoin ✓ — certificat médical ✓



#### TYPES DE PREUVES APPROUVÉS

modérée — échelon 2 sur 4

chaque champ à gauche a exactement un équivalent rempli à droite — c'est ce qui rend comparables deux déclarations de même type.

le sceau de l'autorité sur une  
déclaration remplie est un engagement :  
la procédure a bien été suivie.



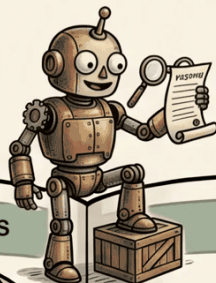
J'engage ma  
réputation que ceci a  
été traité selon la  
norme.



LA NORME EST LE FORMULAIRE — UNE DÉCLARATION EST LE FORMULAIRE REMPLI ET CAUTIONNÉ.

# QU'EST-CE QU'UNE POLITIQUE DID ?

## EXEMPLES DE L'ARTEFACT POLITIQUE DID



ma politique ne concerne pas la façon dont une déclaration est rédigée — c'est le rôle de la norme. Ma politique détermine si je me soucie même de la déclaration : est-ce que je fais confiance à celui qui l'a signée, est-ce que je fais confiance à l'autorité derrière sa norme, et l'affaire mérite-t-elle seulement mon attention ?

### LA NORME — VALEURS PAR DÉFAUT HÉRITÉES

NOM DE LA RÈGLE



**SEUIL MINIMAL DE RÉPUTATION DE L'ÉMETTEUR**

j'accepte les émetteurs ayant une réputation supérieure à cinq sur dix



**LISTE DE CONFIANCE DES AUTORITÉS**

j'accepte les normes de toute autorité dont la propre réputation dépasse quatre sur dix



**FILTRE DE SUBSTANCE**

je traite toute déclaration dont l'importance dépasse le seuil « insignifiant »



**COURBE TARIFAIRE ANTI-SPAM**

me soumettre une déclaration est peu coûteux pour les déclarations substantielles et rares — et devient vite cher pour les déclarations mesquines ou répétées



**PONDÉRATION COMBINÉE**

la réputation de l'émetteur et celle de l'autorité se multiplient ; le caractère mesquin divise le résultat par deux

la politique ne réécrit pas la norme — elle juge les personnes et l'affaire. Conserver, modifier, supprimer, ajouter — quatre gestes simples à partir d'un point de départ commun.

### MA POLITIQUE — DÉRIVÉE DE CELA



CONSERVE



MODIFIÉ



SUPPRIMÉ



AJOUTÉ

coche mot d'action mot d'action mot d'action

nom de la règle

**SEUIL MINIMAL DE RÉPUTATION DE L'ÉMETTEUR**

**durci — j'exige sept sur dix**

**LISTE DE CONFIANCE DES AUTORITÉS**

je fais entièrement confiance aux magistrats et aux médecins ; je réduis de moitié le poids des déclarations sous surveillance municipale ; je refuse tout ce qui relève de la police portuaire

**FILTRE DE SUBSTANCE**

les déclarations de nuisance mineure ne me coûtent rien à ignorer — je ne les lis tout simplement pas

**COURBE TARIFAIRE ANTI-SPAM**

conservé — la courbe par défaut me convient

**PONDÉRATION COMBINÉE**

supprimé — j'utilise ma propre formule

**COÛT EXPONENTIEL SUR LES DÉCLARATIONS RÉPÉTÉES**

ajouté — chaque nouvelle déclaration du même émetteur à mon sujet dans l'année coûte dix fois la précédente

**HEURES DE SILENCE**

ajouté — je refuse de lire toute déclaration déposée entre minuit et l'aube



**VÉRIFICATION** — ma politique filtre à la fois les déclarations entrantes et mes propres brouillons avant que je les émette. L'émission est une vérification à la sortie.

**CONSENSUS** — ma politique est mon vote lorsque la communauté négocie des règles communes.

## VOTRE POLITIQUE JUGE LE MESSAGE — PAS LE FORMULAIRE.





## Pourquoi le réseau est incensurable

Jusqu'ici, nous avons décrit ce que le réseau peut faire. Concentrons-nous maintenant sur les raisons pour lesquelles il ne peut être ni fermé ni censuré.

Le réseau sera probablement bâti sur les principes du réseau Tor et du routage en oignon (une manière de masquer le trafic réseau en s'appuyant sur les principes des Mixnet) — une technologie où la communication traverse plusieurs couches de chiffrement et où aucun nœud ne connaît à la fois l'expéditeur et le destinataire. Une institution centrale ne peut pas regarder par-dessus votre épaule, car il n'existe aucun endroit depuis lequel regarder.

Vous pouvez combattre cela, mais vous ne pouvez pas gagner — à moins de plonger le pays entier dans une surveillance totalitaire au niveau de chaque paquet réseau et de chaque action de bas niveau sur chaque matériel qui se connecte à internet et communique sur le réseau de réputation en question. Et c'est précisément le choix auquel le centralisme est confronté : soit accepter que les citoyens disposent d'un outil hors de sa portée, soit s'enfoncer dans les recoins obscurs de la stagnation économique au nom du contrôle totalitaire.

Ne nous faisons aucune illusion — même les régimes démocratiques tenteront cela dans leur combat pour le centralisme. Ils préféreraient mettre les gens aux fers plutôt que de céder le pouvoir.

# COMMENT VOS MESSAGES RESTENT INTRAÇABLES

DEUX LIGNES DE DÉFENSE À LA FOIS — COUCHES ET BRUIT

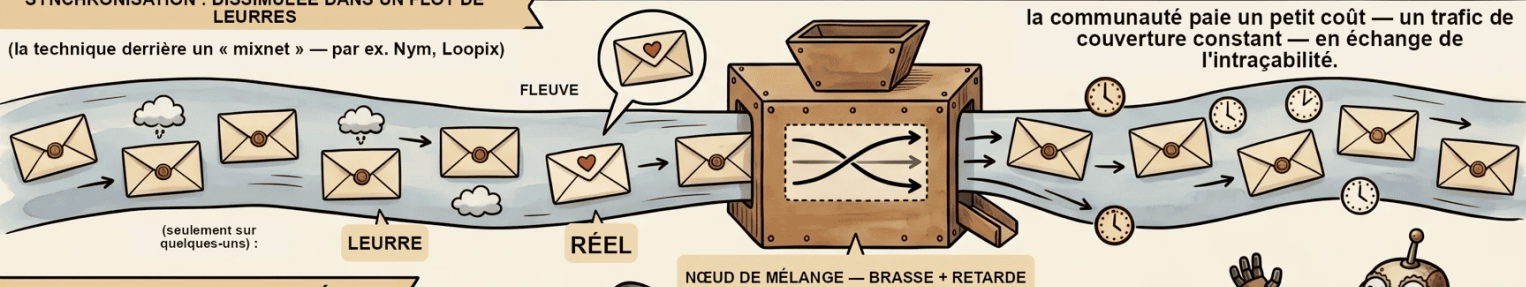
## CONTENU : ENVELOPPÉ DE COUCHES

(la technique derrière Tor — le « routage en oignon »)



## SYNCHRONISATION : DISSIMULÉE DANS UN FLOT DE LEURRES

(la technique derrière un « mixnet » — par ex. Nym, Loopix)



## LES DEUX BOUCLERS RÉUNIS

| MATRICE           | CACHE QUI ? | CACHE QUAND ? |
|-------------------|-------------|---------------|
| COUCHES SEULEMENT | ✓ OUI       | ✗ NON         |
| BRUIT SEULEMENT   | ✗ NON       | ✓ OUI         |
| COUCHES + BRUIT   | ✓ OUI       | ✓ OUI         |

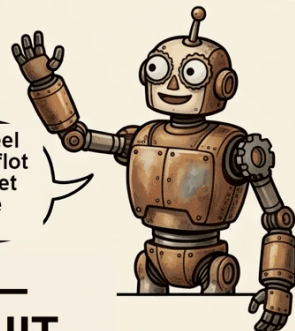
(routage en oignon + mixnet — la combinaison d'oignon et de bruit)



cent enveloppes par heure — laquelle compte ?

l'observateur voit le flux mais ne peut distinguer le RÉEL du LEURRE.

le message réel nage dans un flot de leurres — et porte quatre manteaux.



# CONTENU CACHÉ PAR LES COUCHES — SYNCHRONISATION CACHÉE PAR LE BRUIT.

## Réponse aux doutes les plus évidents

Le système décrit soulève naturellement un certain nombre de questions. Répondons aux plus courantes.

### Dépendance à la technologie

Vous avez probablement déjà remarqué que, contrairement à l'État moderne — qui nous accompagne depuis quelque 150 ans — la solution du réseau de réputation telle qu'elle est décrite ici dépend fortement de la technologie de l'internet mondial/local. En cas de panne, le fonctionnement d'un tel réseau est menacé.

Si la panne est temporaire, il n'y a ni perte de données ni perte de cohérence des assertions dans le réseau, et les soldes de réputation atteints au sein des communautés ne devraient pas non plus être perturbés. Contrairement aux réseaux de paiement comparables, ce réseau suppose de très faibles fréquences de processus et de données. À cet égard, le réseau de réputation décentralisé ne diffère pas de l'État actuel, qui dépend lui aussi désormais fortement de la technologie et a oublié comment travailler avec des fichiers cartonnés en papier (même si, dans ses plans de crise, il n'aurait pas le choix).

Le successeur évolutif de l'État sous la forme d'un réseau de réputation peut, en cas de panne permanente (une catastrophe d'une ampleur sans précédent), se replier sur un système centralisé plus primitif — l'État.

La technologie permet à l'humanité d'atteindre des formes civilisationnelles de gouvernance plus élevées et nous apporte des bénéfices, mais aussi des risques.

# DEUX VOIES — L'ÉTAT SE FERME, LE RÉSEAU S'OUVRE

LE RÉSEAU DE RÉPUTATION

NE RIEN FAIRE,  
C'EST CHOISIR  
LA BONNE  
PORTE.

L'ÉTAT

le portail est encore  
en train de se  
fermer. l'autre porte  
est encore ouverte.

choisissez-en  
une — ou le  
choix vous  
choisira.

Tous les régimes finissent de la même façon. Le seul  
choix est de faire un pas à gauche.

## L'ÉTAT SE FERME PAR DÉFAUT. LE RÉSEAU S'OUVRE PAR CHOIX.



## **Est-ce que je jette mon argent par les fenêtres en publiant dans le réseau ?**

Les coûts de la publication d'une assertion dans le réseau de réputation sont en grande partie non récupérables. L'utilité du message qu'un émetteur place dans le réseau — information sur des torts réels, expériences vérifiées, avertissements pertinents — revient statistiquement, sur un horizon plus long, sous la forme de frais pour la vérification des assertions d'autrui issues de la communauté. La communauté en profite, l'émetteur bâtit sa réputation, et les coûts de publication d'une information véridique s'approchent ainsi d'une caution remboursable, dont il ne faut soustraire qu'une plus petite part correspondant aux coûts réels de maintenance du réseau. À l'inverse, les enregistrements mensongers ou triviaux ne reviennent pas — leurs coûts sont une perte nette. L'honnêteté n'est donc pas seulement un choix moral, mais aussi une stratégie économiquement rationnelle.

Après déduction des coûts de maintenance du réseau, ce principe pourrait être appelé le principe de neutralité économique — je ne perds pas quand je suis avec la communauté, je perds quand je suis contre elle.

La communauté dispose aussi de canaux de solidarité pour apprécier l'attitude honnête de ses membres. Mais ne nous faisons aucune illusion : les appels à la solidarité naissent le plus souvent de la pression sociale de la communauté, si bien que ce n'est peut-être pas de la solidarité au sens volontaire du terme.

## **Et si quelqu'un crée plusieurs identités ?**

Une personne peut exploiter plusieurs identités DID en parallèle. Cependant, bâtir la réputation de chaque identité exige un effort indépendant — du temps, de l'énergie, de l'argent.

Aucun raccourci : chaque identité doit accumuler son historique<sup>1</sup> par une activité réelle. Maintenir des identités parallèles est donc intentionnellement coûteux.

Dans les sociétés libres, les coûts découragent l'abus.

Dans les dictatures, en revanche, les identités parallèles deviennent un outil de survie : elles permettent d'organiser des réseaux clandestins, de naviguer plus sûrement dans le marché noir, et une résistance cloisonnée<sup>2</sup>, où la compromission d'une identité ne révèle pas les autres — et, après la chute du régime, elles permettent un retour sans heurt à la vie publique et à la réputation qui y a été bâtie, voire la fusion de la DID auparavant officielle et de la DID secrète en un unique ensemble combiné d'enregistrements, au moyen d'une assertion.

---

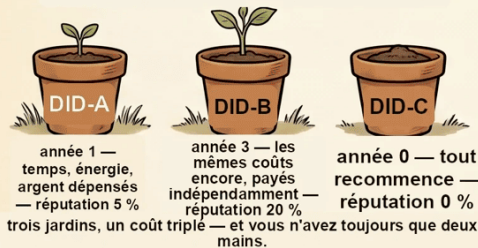
<sup>1</sup>**Track record** — en général : l'historique des résultats passés, des succès et des échecs d'une personne ou d'une organisation. Ici : la somme de toutes les interactions passées d'une identité DID donnée dans le réseau — assertions vérifiées, enregistrements acceptés et rejetés — dont sa réputation est dérivée.

<sup>2</sup>**Cloisonnement** (de l'angl. *compartment*) signifie séparer l'information en unités isolées, de sorte que l'exposition d'une unité ne compromette pas les autres. Un principe connu des services de renseignement : un agent ne connaît que sa part de l'opération, si bien que, même sous la contrainte, il ne peut pas révéler l'ensemble.

# LE MÊME EFFORT — UN PLAN B COÛTEUX DANS LA LIBERTÉ, UNE BOUÉE DE SAUVETAGE SOUS LA TYRANNIE

DES IDENTITÉS PARALLÈLES COÛTENT LE MÊME PRIX — MAIS N'ACHÈTENT PAS LA MÊME CHOSE

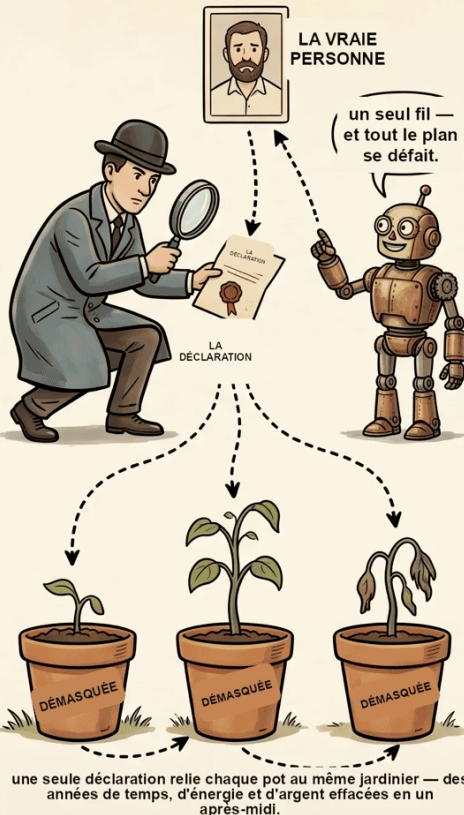
## DANS LA LIBERTÉ — UN PLAN B COÛTEUX



## OU — UNE ARDOISE VIERGE APRÈS UN FAUX PAS PERSONNEL

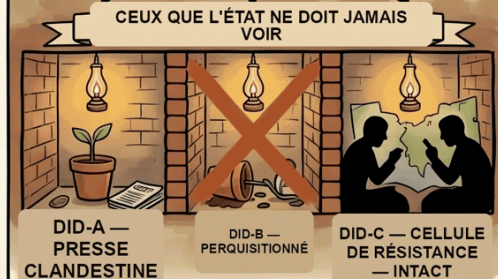
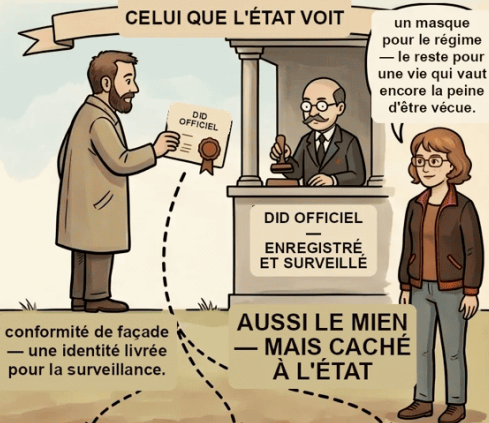


## UNE SEULE DÉCLARATION ET LE PLAN B DISPARAIT



## SOUS LA TYRANNIE — UN POUR L'ÉTAT, LES AUTRES POUR L'ASSOCIATION LIBRE

(l'État interdit purement et simplement les identités, ou les exige sous son propre contrôle)



les murs étanches entre les cellules accomplissent ce que l'État interdit — en perdant une, les autres continuent ; quand le régime tombe, la vie publique reprend.

DANS LA LIBERTÉ, L'ABUS COÛTE CHER. SOUS LA TYRANNIE, LA SURVIE EST POSSIBLE.

## ■ Une perception retournée comme un gant

Contrairement à l'État, le principe d'un réseau de réputation fondé sur l'identité décentralisée inverse le paradigme de la priorité perçue :

- Ce qui compte, c'est la réputation — c'est-à-dire le passé, utilisé pour évaluer les risques d'une interaction avec une contrepartie — tandis que les données personnelles comme les noms, les adresses, etc. peuvent relever d'un échange de courtoisie
- Alors que l'État exige avant tout des données personnelles, accumule des données de réputation, et ne laisse la communauté voir que ce qui l'arrange

### **Une personne fortunée ne peut-elle pas simplement « acheter » plus d'identités (ou créer des communautés virtuelles) ?**

La possibilité de créer des identités décentralisées parallèles ressemble à première vue à un avantage injuste des personnes disposant de plus de moyens économiques sur celles qui en ont moins. Il faut toutefois souligner que, contrairement à un système centralisé où il suffit de corrompre quelques points de la pyramide du pouvoir pour faire disparaître certains méfaits, dans un système décentralisé il faudrait corrompre la communauté tout entière.

Des identités décentralisées de substitution pourraient servir à cette fin, mais leur réputation doit être bâtie dans le temps par une interaction réelle avec d'autres membres effectifs de la communauté — elle ne peut pas simplement s'acheter, car le réseau rend vérifiable la façon dont une identité donnée se comporte.



De plus, des services peuvent exister sur le marché (et existeront probablement) qui, agissant comme une autorité, proposent des enquêtes produisant la preuve que plusieurs identités décentralisées sont en fait la même personne. Un seul enregistrement inscrit dans le réseau de réputation peut ainsi anéantir, pour une fraction du coût, tout l'investissement en temps, en énergie et en argent consacré à bâtir des identités parallèles.

Économiquement, il est donc rentable de ne pas tromper la communauté — et, au besoin, d'examiner ses actes et de rechercher réparation pour que la réputation revienne à un niveau acceptable et que son porteur ne souffre pas, économiquement ou autrement, du courroux de la communauté.

Une identité économiquement puissante qui a perdu sa réputation dans sa propre communauté peut tenter d'échapper au courroux de celle-ci par des arrangements souterrains avec des identités ciblées — mais celles-ci risquent alors, elles aussi, de perdre leur propre réputation.

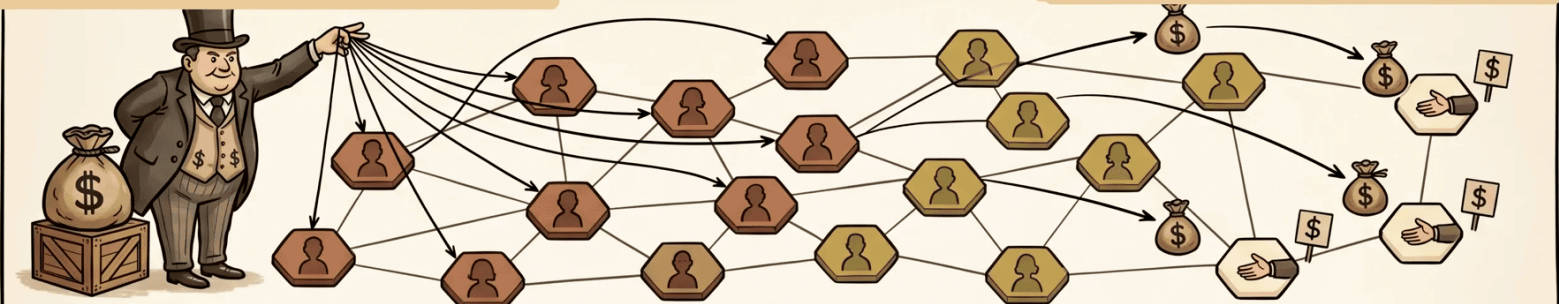
Il reste encore la fuite vers une autre communauté avec une identité neuve — mais cela signifie laisser derrière soi tous ses acquis et repartir quelque part de zéro, avec une réputation nulle. Ce peut parfois être un chemin compréhensible et la seule issue.

# LA RÉPUTATION EST LE CONTREPOIDS DE LA PUISSANCE ÉCONOMIQUE

L'HOMME RICHE ACHÈTE DE L'INFLUENCE — LA COMMUNAUTÉ S'EN SOUVIENT

## L'ATTAQUE — INFILTRER ET CORROMPRE

HUIT PANTINS INFILTRÉS + TROIS VOISINS ACHETÉS

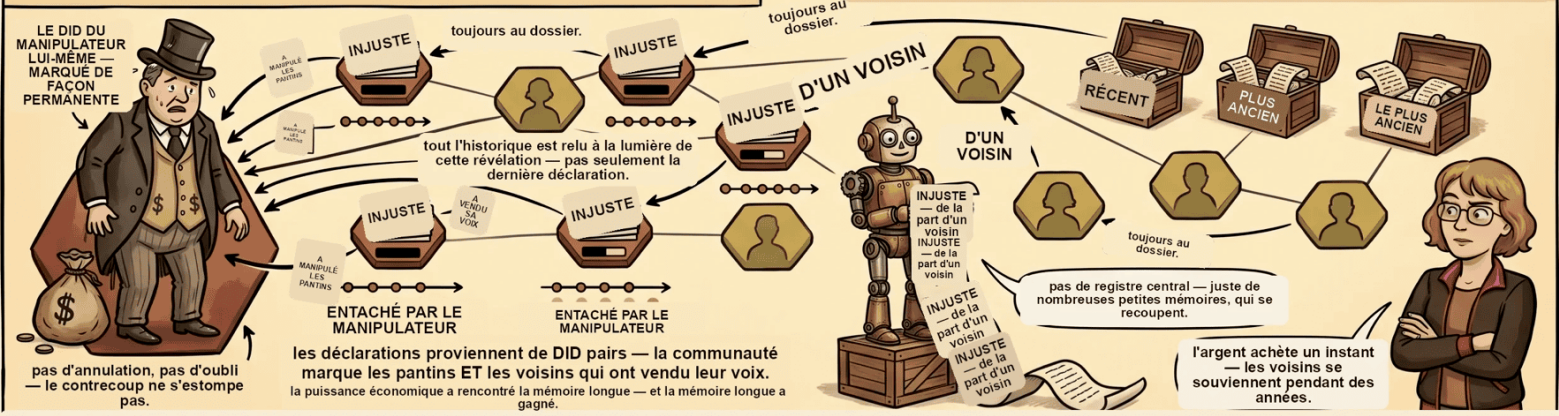


la puissance économique peut glisser des fils dans n'importe quelle communauté — et acheter au premier abord, on dirait que l'homme riche a simplement élargi son cercle d'amis.

PLUS TARD

## LA DÉFENSE — MÉMOIRE LONGUE, COMPTABILITÉ DISTRIBUÉE

CHACQUE VOISIN GARDE SA PROPRE MÉMOIRE — PAS DE REGISTRE CENTRAL, PAS D'OUBLI



## LE POUVOIR ÉCONOMIQUE S'IMMISCE — LE CONTRECROUP REVIENT, ET IL NE S'EFFACE PAS.

## Note

De la même manière, les communautés traiteraient une attaque où quelqu'un consacre des ressources à créer une identité virtuelle : pour cette identité, il est risqué d'entrer en interaction avec une autre communauté sans vérification — c'est-à-dire d'accepter sans esprit critique les informations sur les identités de l'autre communauté. Les réputations se bâtissent toujours au sein d'une communauté, non globalement.

## **Et les profiteurs qui ne veulent que lire sans rien donner à la communauté ?**

L'accès à l'information n'est pas illimité dès le premier jour de création d'une identité décentralisée. Les nouveaux participants — ceux qui n'ont pas encore bâti de réputation par une activité réelle — font face à des restrictions graduées : moins d'informations, des délais d'attente plus longs, des coûts de requête plus élevés. Le réseau récompense la participation, non la consommation passive et la collecte arbitraire de données.

Une identité décentralisée risque aussi sa réputation lorsqu'elle prête sa réputation contre paiement à une autre personne (qui peut même ne pas être dans le réseau de réputation DID). Le même principe s'applique ici : une telle trahison de la communauté (violation de la vie privée) peut se répercuter sur la réputation du traître, et l'acte ne peut pas être effacé par un arrangement souterrain comme cela fonctionne dans un système centralisé. Il doit compter avec le courroux de la communauté, y compris la perte de ses acquis — car la communauté est, à ses yeux, la garante par exemple du privilège de posséder des biens meubles et immeubles.

## ■ Ancrage au monde réel

Lors de l'évaluation du risque, le sujet le plus risqué est naturellement celui qui ne jouit pas du privilège de la propriété reconnue par une communauté donnée — il a moins à perdre dans ses transactions (les actifs numériques sont plus faciles à déplacer).

Cela peut ressembler à un détail mineur, mais les conséquences en sont majeures. Vouloir que la communauté ait un levier sur ses membres implique la propriété comme un privilège — dans les sociétés les plus libres presque intouchable, mais tout de même pas un droit, ni un principe fondamental, mais un privilège qui, dans des cas extrêmes, peut être révoqué (j'imagine par exemple le refus de servir pour défendre la communauté dans un conflit armé).

Cela répond aussi subliminalement à la question de la manière dont la communauté traitera ses membres, et de la motivation qu'a un membre à se battre pour la communauté — conserver ses privilèges. Une personne peut manquer à sa responsabilité envers la communauté, mais moralement elle ne peut pas s'attendre à de l'indulgence lorsqu'il s'agit de conserver des privilèges durement gagnés.

## Neutralité financière

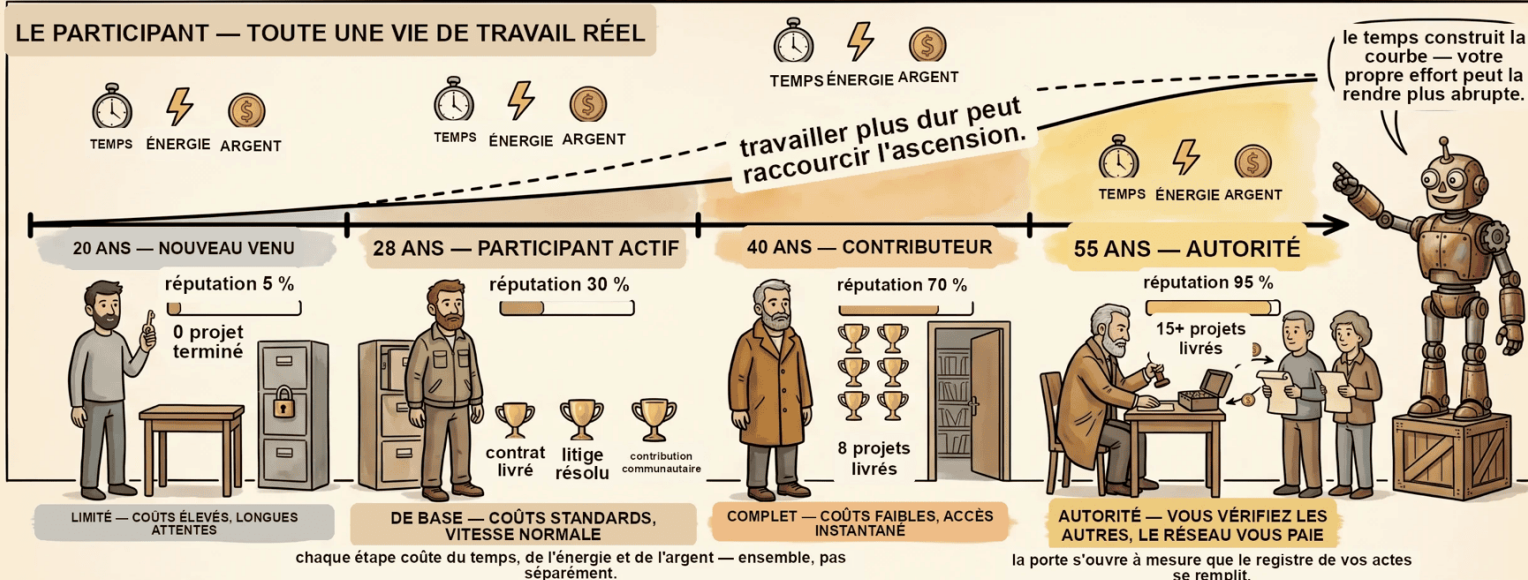
En lisant des mots comme décentralisé, incensurable, incorruptible, on ne peut s'empêcher de les associer aux cryptomonnaies les plus connues — Bitcoin, Monero, et disons Kaspas — que l'on peut décrire en ces termes. L'intuition est pourtant trompeuse ici : les frais pour les services des autorités, pour la vérification



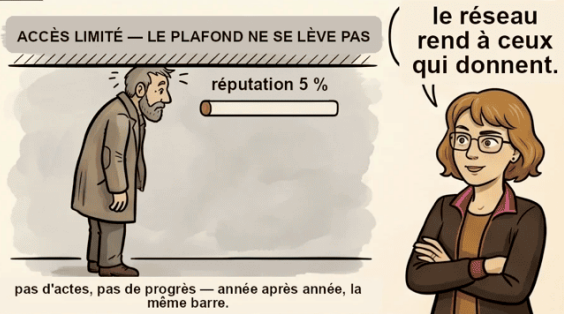
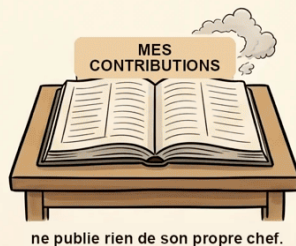
# LE RÉSEAU RÉCOMPENSE LA PARTICIPATION

LA RÉPUTATION SE CONSTRUIT SUR TOUTE UNE VIE — ELLE NE S'ACHÈTE NI NE S'EMPRUNTE

## LE PARTICIPANT — TOUTE UNE VIE DE TRAVAIL RÉEL



## LE PROFITEUR — LIT, NE PUBLIE JAMAIS



LE TEMPS, L'ÉNERGIE ET L'ARGENT — INVESTIS DANS UN TRAVAIL RÉEL — SONT LA SEULE MONNAIE QUE LE RÉSEAU RESPECTE.

et la publication, etc., peuvent être réglés dans n'importe quelle devise ou monnaie. Ce qui compte pour les participants connectés du réseau social dans le réseau DID (c'est-à-dire votre communauté) et son entourage, c'est une confirmation adossée à la réputation que le paiement a bien été effectué. La publication d'une assertion doit individuellement comporter un coût raisonnable et vérifiable, de sorte qu'un acteur ne puisse pas publier autant d'assertions qu'il veut, et lesquelles il veut, sans dépenser d'énergie, d'argent et de temps — un état de choses fortement indésirable, correspondant au privilège des élites dans les systèmes étatiques rongés par la corruption d'aujourd'hui.

À cet égard, les cryptomonnaies mentionnées ont un petit avantage : leurs réseaux agissent comme des autorités de confiance pour vérifier qu'un paiement donné a bien eu lieu, au prix d'une petite perte de vie privée et de l'exposition de certaines de ses adresses.

## Volontariat, responsabilité et liberté

Le volontariat est individuel : je décide pour moi-même. La responsabilité surgit lorsque ma décision affecte les autres — le retour entre en jeu. La liberté n'est ni un don ni un droit — elle est un résultat phénoménologique<sup>3</sup> de milliers d'interactions bilatérales entre le volontariat et la pression vers la responsabilité, moyennées à l'échelle de la société. Le réseau ne dicte pas cette moyenne — elle émerge<sup>4</sup> des

---

<sup>3</sup>**Phénoménologique** (du gr. *phainómenon* — ce qui apparaît) — en général : une approche examinant les phénomènes tels qu'ils se présentent dans l'expérience directe, en observant ce qui en découle, sans théories explicatives préétablies dans le microcosme qui les sous-tend. Ici : la liberté n'est pas un principe abstrait défini d'en haut, mais un phénomène observé — une conséquence de milliers de micro-interactions entre les personnes, qui émerge de la manière dont nous nous traitons réellement les uns les autres.

<sup>4</sup>**Émergent** (du lat. *emergere* — émerger) signifie « surgissant spontanément des interactions de parties plus simples, sans que personne le conçoive ou le dirige ». Une nuée d'oiseaux vole en formation même si aucun oiseau n'a de plan pour la formation

signaux de prix des vérificateurs et des politiques de vérification pré-annoncées que les membres de la communauté se fixent à eux-mêmes.

La préférence pour la liberté qu'a un individu au sein d'une communauté dépend de son sentiment quant à ce qu'il est lui-même prêt à avaler de ce qu'il impose aux autres. Pour les choses évidentes et bénéfiques à tous, il n'y a pas de dilemme moral — le meurtre est mal. Puis il y a les cas où les options glissent vers la position de privilèges autorisés : prouvez vos compétences et nous vous laisserons prendre la route, ainsi il y a moins de chances que vous nous tuiez. Et enfin il y a les affaires où l'individu se dit — cela n'en vaut pas la peine pour moi, je n'interdirai pas à mon voisin de brûler des feuilles alors que je le fais moi-même, ou parce que je fais autre chose qui restreint son confort et qu'il pourrait à son tour vouloir me l'interdire. Si nous avons historiquement tracé la frontière de la liberté là où commence la liberté d'autrui, alors un réseau social de réputation fondé sur l'identité décentralisée remplit cela mieux que la démocratie représentative centralisée — où, par exemple, la couche privilégiée des élus tente de s'exempter de la surveillance des communications personnelles, tout en n'hésitant pas à l'imposer à leurs électeurs, à l'aide de toutes sortes de prétextes souterrains et de manipulations.

## **L'interrupteur liberté-totalitarisme (et la délégation)**

Un mécanisme simple au sein du réseau DID peut faire glisser tout le système vers plus de liberté ou plus de contrôle : le nombre d'enregistrements qu'une DID peut publier par période de temps. Quand les enregistrements restent rares, chacun pèse — c'est la liberté. Quand les enregistrements sont abondants et couvrent des brouilles, c'est le totalitarisme. Vous choisissez la direction avec chaque enregistrement

---

— la formation émerge des règles simples de chaque individu. De même, dans le réseau de réputation, personne ne conçoit les règles de comportement de l'ensemble — elles émergent de milliers de décisions individuelles.



# VOLONTARIAT → RESPONSABILITÉ → LIBERTÉ

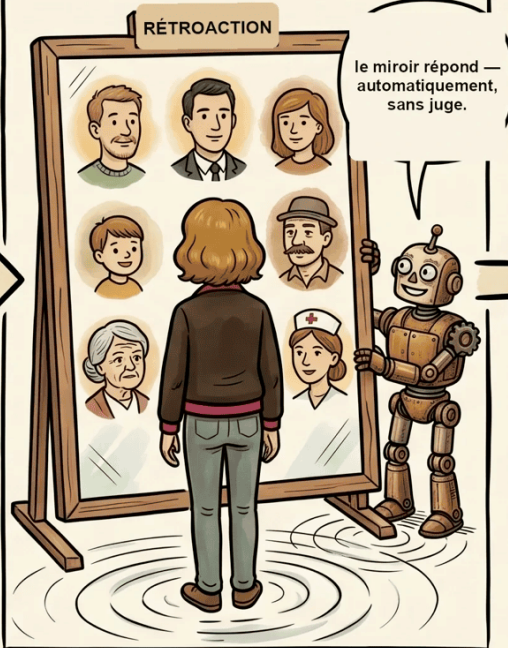
TROIS ÉTAPES — DU CHOIX D'UNE PERSONNE AU MODÈLE D'UNE SOCIÉTÉ ENTIÈRE

## VOLONTARIAT



l'individu décide — personne ne l'y contraint.  
et personne ne lui doit non plus d'obligation positive.

## RESPONSABILITÉ



mes choix se propagent — et les ondes reviennent.  
les conséquences parlent d'elles-mêmes.

## LIBERTÉ



personne n'a dessiné cette carte — elle s'est dessinée elle-même.

la liberté est la forme statistique de  
la façon dont les voisins se traitent.

**LA LIBERTÉ N'EST PAS UN DON D'EN HAUT — C'EST LE MODÈLE QUE NOUS CRÉONS ENSEMBLE.**



que vous publiez. Le réseau lui-même n'est ni libre ni totalitaire — c'est une infrastructure neutre. Ce qu'il devient est déterminé par la manière dont les gens l'utilisent.

Dans le cadre de ma propre politique de vérification, il est logique de fixer, pour une DID générique de mon réseau social — au sein des communautés — un nombre maximal d'assertions (toute déclaration vérifiable en général ; ici : un enregistrement publié dans le réseau de réputation) qu'un émetteur peut émettre par période pour que je les prenne en compte et considère ses demandes de vérification comme pertinentes.

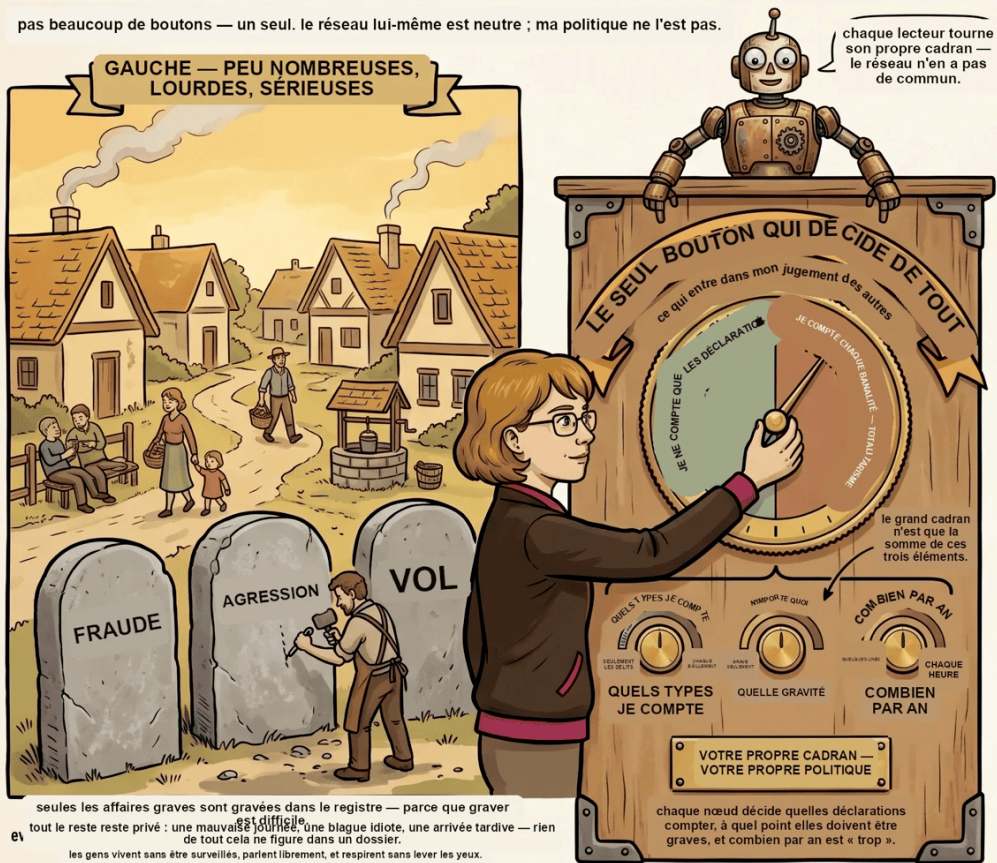
Je garde en tête un nombre intuitif — quelques unités par an. Une telle approche censoriale peut sembler plutôt isolationniste. Mais je peux légitimement placer le demandeur devant un choix : sélectionner l'un de ses enregistrements déjà émis et demander au vérificateur de le révoquer, c'est-à-dire de l'invalidier — ce qui est une exigence assez agressive dans une situation où le demandeur est, par coïncidence, réellement devenu victime de multiples torts indépendants, et je contribuerais sûrement par là à son sentiment d'éloignement de la communauté.

Une option plus efficace apparaît donc être la capacité de déléguer une partie de ses droits de publication d'informations dans le réseau de réputation au profit d'une communauté ou d'une autorité, qui décide alors — de manière solidaire, selon ses règles internes — comment les répartir. Un groupe doit pouvoir prendre soin de ceux qu'il considère comme défavorisés. Un membre de la communauté a le droit, à tout moment, tant que le droit délégué n'est pas utilisé, de révoquer sa délégation.

# L'INTERRUPTEUR LIBERTÉ-TOTALITARISME

UN SEUL PARAMÈTRE — CE QUE JE CHOISIS DE SURVEILLER — FAIT BASCULER TOUTE UNE SOCIÉTÉ ENTRE LIBERTÉ ET TYRANNIE

pas beaucoup de boutons — un seul, le réseau lui-même est neutre ; ma politique ne l'est pas.



LA LIBERTÉ EST CE QUE JE REFUSE DE COMPTER — LE TOTALITARISME EST CE QUE J'ACCÈPTE DE SURVEILLER.



# DÉLÉGATION DES DROITS DE PUBLICATION

VOUS PRÊTEZ LA CLÉ À UNE AUTORITÉ QUI VOUS SERT — ET LA RÉCUPÉREZ EN UN INSTANT

Je prête la clé — la ficelle reste entre mes mains.

délégation — l'autorité agit en mon nom, dans les règles que j'approuve.

FICELLE DE RAPPEL

MON DROIT DE PUBLIER — ENREGISTRÉMENT

Je peux prêter plusieurs clés à la fois — une automatisation en arrière-plan peut en réémettre une nouvelle dès que l'une des miennes est tirée.

AUTORITÉ — PRESTATAIRE DE SERVICE  
politique · norme · parti · chambre

POLITIQUE

TIRÉE AU HASARD QUAND L'AUTORITÉ AGIT

CLÉS DÉLÉGUÉES — RÉSERVOIR

TIRÉE AU HASARD QUAND L'AUTORITÉ AGIT

UN COUP SEC — LA CLÉ REVIENT

la ficelle ne quitte jamais votre main — c'est tout le truc.

UTILISÉE

UNE CLÉ TIRÉE AU HASARD — LA CLÉ EST UTILISÉE

révocable seulement jusqu'à ce que la clé soit tirée.

après cela, le citoyen doit émettre une nouvelle clé pour rester en règle avec l'autorité — une automatisation peut le faire en arrière-plan.

TYPES D'AUTORITÉS POUVANT DÉTENIR LA CLÉ



PARTI POLITIQUE  
PARTI



ORGANISME DE NORMALISATION  
BUDJ



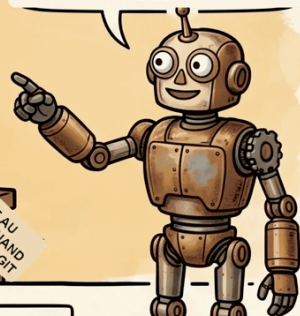
CHAMBRE PROFESSIONNELLE



COOPÉRATIVE

l'autorité sert ses membres — pas l'inverse.  
une traction sur la ficelle met fin à l'accord.

PRÊTEZ LA CLÉ — GARDEZ LA FICELLE. LA DÉLÉGATION N'EST JAMAIS UN ABANDON.



## ■ Liberté vs totalitarisme

---

Une société qui surveille et limite le volume des enregistrements publiés sera plus libre ; une société avec un excès d'enregistrements tendra vers le totalitarisme. On peut envisager de déléguer à quelqu'un d'autre le droit de publier des enregistrements.



## Adaptation culturelle

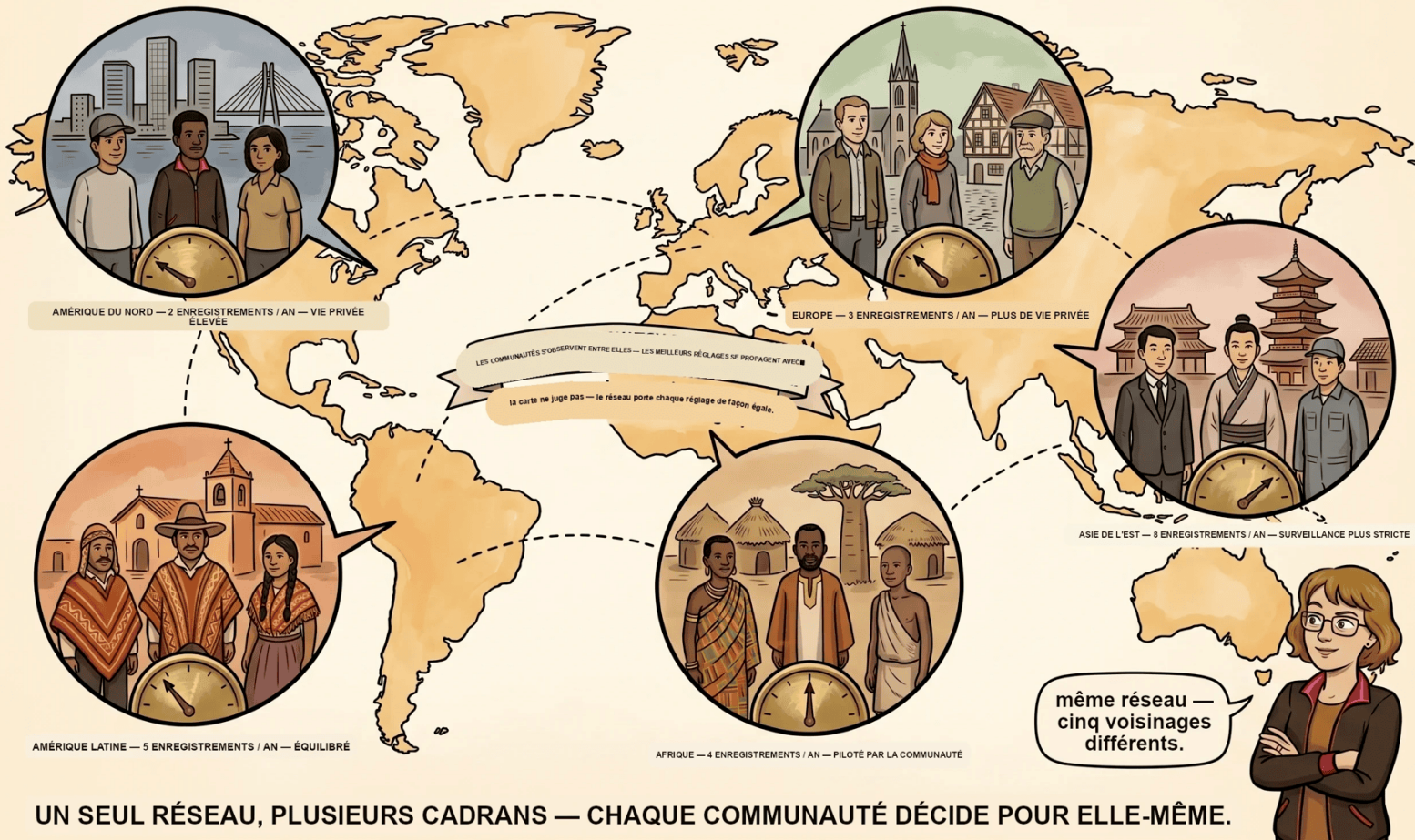
Les gens aiment généralement voir ce qu'il y a dans l'assiette des autres. À travers les civilisations, nous différons par l'expérience historique et la densité de population — et donc par la mesure dans laquelle nous voulons voir dans l'assiette des autres, au sein des civilisations et des communautés. Les États asiatiques tendent vers une vision plus stricte de la liberté dans la société ; les États européens et américains, sous certains aspects, vers une vision plus libre. Aussi imprécis que soit ce parallèle, dans le contexte d'un réseau social de réputation décentralisé on peut dire que les paramètres des communautés individuelles ne discriminent pas, et que chaque communauté peut configurer la communication en son sein comme bon lui semble.

Malgré les différences, il y aura des normes reconnues à travers la planète (tuer au hasard n'est bon pour personne). D'autres paramètres seront spécifiques à une communauté, et d'autres encore spécifiques à un individu. L'avantage est que, par la communication mutuelle et l'observation des paramètres de son entourage, un consensus peut être recherché — depuis les arrangements bilatéraux jusqu'aux arrangements communautaires et, avec le temps, grâce à la domination économique des communautés les mieux configurées, jusqu'au niveau mondial.

Mais nous en dirons plus sur le consensus au chapitre suivant.

# CHAQUE COMMUNAUTÉ SE CONFIGURE ELLE-MÊME

LE RÉSEAU NE DISCRIMINE PAS — CHAQUE RÉGION RÈGLE SON PROPRE CADRAN



## **Le problème de l'oracle — faire le pont entre le monde numérique et le monde physique**

Le terme « problème de l'oracle » a été ces derniers temps le plus souvent associé au monde des cryptomonnaies, des chaînes de blocs et des systèmes décentralisés. En général : comment s'assurer que les données entrant dans un système numérique correspondent fidèlement à ce qui s'est réellement passé dans le monde physique ? Le système lui-même ne peut pas vérifier si quelqu'un a réellement porté préjudice à autrui, ou si un contrat a véritablement été rompu — il ne voit que des enregistrements numériques.

Ici, nous résolvons cela par les autorités — des entités qui engagent leur réputation sur le fait que l'enregistrement numérique correspond à la réalité physique. Plus la réputation de l'autorité est élevée, plus l'enregistrement est crédible.



# RELIER LES MONDES NUMÉRIQUE ET PHYSIQUE

L'AUTORITÉ FAIT PASSER LA RÉALITÉ DE L'AUTRE CÔTÉ



**La réputation de l'autorité rend l'enregistrement numérique digne de confiance.**

\* Le système ne cherche pas à résoudre le problème de l'oracle — il accepte que les autorités soient le pont, et s'aligne sur la façon dont la confiance fonctionne déjà dans le monde réel.

\* Si le pont se trompe sur la réalité, l'autorité en paie le prix — avec sa réputation.



# Comment fonctionne la vérification

## Le consensus et le processus de vérification

Pour construire un consensus sur les règles qu'une société devrait, en moyenne, respecter et faire respecter, le mécanisme suivant peut aider. En tant que participant DID, je déclare les règles auxquelles je souscris et selon lesquelles je vivrai, et je les publie. (Voyez cela comme les statuts et le règlement qui, à mes yeux, composent mon monde idéal — un monde où je ne me sens pas restreint, mais en sécurité.)

Je peux estimer à l'avance comment mes contacts DID réagiraient — et évaluer avec quelle force, et par qui, je serais sanctionné dans des interactions sociales ou commerciales ordinaires, si elles devaient hypothétiquement survenir.

L'évaluation définitive se produit lorsque vous demandez une information à une autre DID, ou lui demandez de vérifier une assertion (ou demandez un service à une autorité, et ainsi de suite) que vous voulez publier dans le réseau de réputation. Cela devrait aboutir de la même manière que lorsque vous exécutez l'évaluation vous-même, à blanc, par rapport à la politique déclarée de la contrepartie — et si ce n'est pas le cas, quelque chose cloche du côté de la contrepartie : elle tente de jouer un jeu malhonnête.

Le résultat est soit une acceptation, avec un prix indiqué pour la vérification (dans le cas des services d'un vérificateur ou d'une autorité), soit un rejet. Tant les sanctions que les bonus pour écart par rapport à la politique de l'évaluateur sont intégrés au prix indiqué. Le demandeur décide ensuite d'accepter les conditions, ou de passer à la ronde suivante de vérification dans l'algorithme d'attribution — en répétant le processus jusqu'à satisfaction, ou jusqu'à ce que l'économie rende inutile de continuer.

## ■ Le graphe social

Le réseau de réputation est, avant tout, un réseau social. Vous ajoutez des contacts — des personnes qui consentent à la connexion. Elles ont des contacts, et ces contacts ont des contacts. L'algorithme cherche des vérificateurs dans une profondeur configurable (par ex. trois niveaux : vos contacts directs, leurs contacts, et un niveau au-delà). Aucune chaîne de blocs mondiale n'est nécessaire — le réseau forme naturellement des communautés avec des chevauchements vers d'autres communautés.

L'algorithme est non déterministe : il hache votre document d'assertion, projette le hash sur une position d'un anneau d'identités connues au sein de ce cercle, et sélectionne la plus proche comme vérificateur candidat. Vous ne pouvez ni prédire ni influencer qui vérifiera votre assertion.

Chaque rejet d'un vérificateur agrandit votre document et augmente son coût de traitement — c'est le premier canal de coût (croissance du document). Chaque nouveau vérificateur facture des frais fondés sur le volume de données, votre réputation et l'ampleur de l'écart entre le contenu de votre assertion et sa politique de vérification déclarée — c'est le deuxième canal de coût (prime de risque). Et chaque itération coûte du temps et de l'énergie — le troisième canal de coût.

## ■ Ce que le vérificateur contrôle, dans l'ordre

Une fois sélectionné, un vérificateur évalue une assertion en gros en quatre étapes ordonnées — les filtres les moins chers d'abord, les contrôles de contenu coûteux en dernier :

1. **Filtrage par politique.** Ce genre d'assertion entre-t-il seulement dans le champ de ce que le vérificateur vérifie publiquement ? Sinon, la demande est rejetée d'emblée.
2. **Confiance dans l'autorité.** L'autorité qui a avalisé l'assertion est-elle suffisamment digne de confiance au regard de la propre politique déclarée du vérificateur ? Une autorité sous le seuil de confiance du vérificateur est un motif de rejet, quel que soit le contenu de l'assertion.
3. **Réputation de l'émetteur.** L'émetteur atteint-il les seuils de réputation que le vérificateur a déclarés pour ce type d'assertion ? Une réputation faible peut soit augmenter les frais, soit déclencher un rejet.
4. **Contrôle du contenu.** Ce n'est que lorsque les trois premières barrières sont franchies que le vérificateur évalue l'assertion elle-même — signatures, cohérence interne, correction formelle, et ampleur de l'écart par rapport à sa politique. Les frais facturés pour cette dernière étape reflètent le risque réellement pris.

Le vérificateur publie la politique qui régit chacune de ces barrières, de sorte que les étapes ne relèvent pas de son bon vouloir — il est lié par ce qu'il a déjà déclaré. Un écart par rapport à la politique publiée est lui-même une assertion publiable à son encontre, et il la paie de sa réputation.

Le résultat : publier une assertion crédible et utile ne coûte presque rien. Publier une assertion radicale coûte davantage. Publier un mensonge devient prohibitivement cher — vous devez itérer de vérificateur en vérificateur, et chacun qui vous rejette ajoute des coûts. Le marché fixe le prix de votre assertion, et le prix vous dit où vous vous situez par rapport aux communautés dans lesquelles vous évoluez.

Il ne suffit pas de déclarer que vous respectez une règle quand, en réalité, vous ne la respectez pas. Dans ce cas, votre DID risque la publication d'un enregistrement négatif exposant l'hypocrisie — ce qui fait de vous un risque pour tous les autres. Le résultat devrait être des règles moins nombreuses mais plus systématiquement suivies, et un défrichage de cette jungle de lois et de règlements dans laquelle même les professionnels du droit se repèrent à peine.

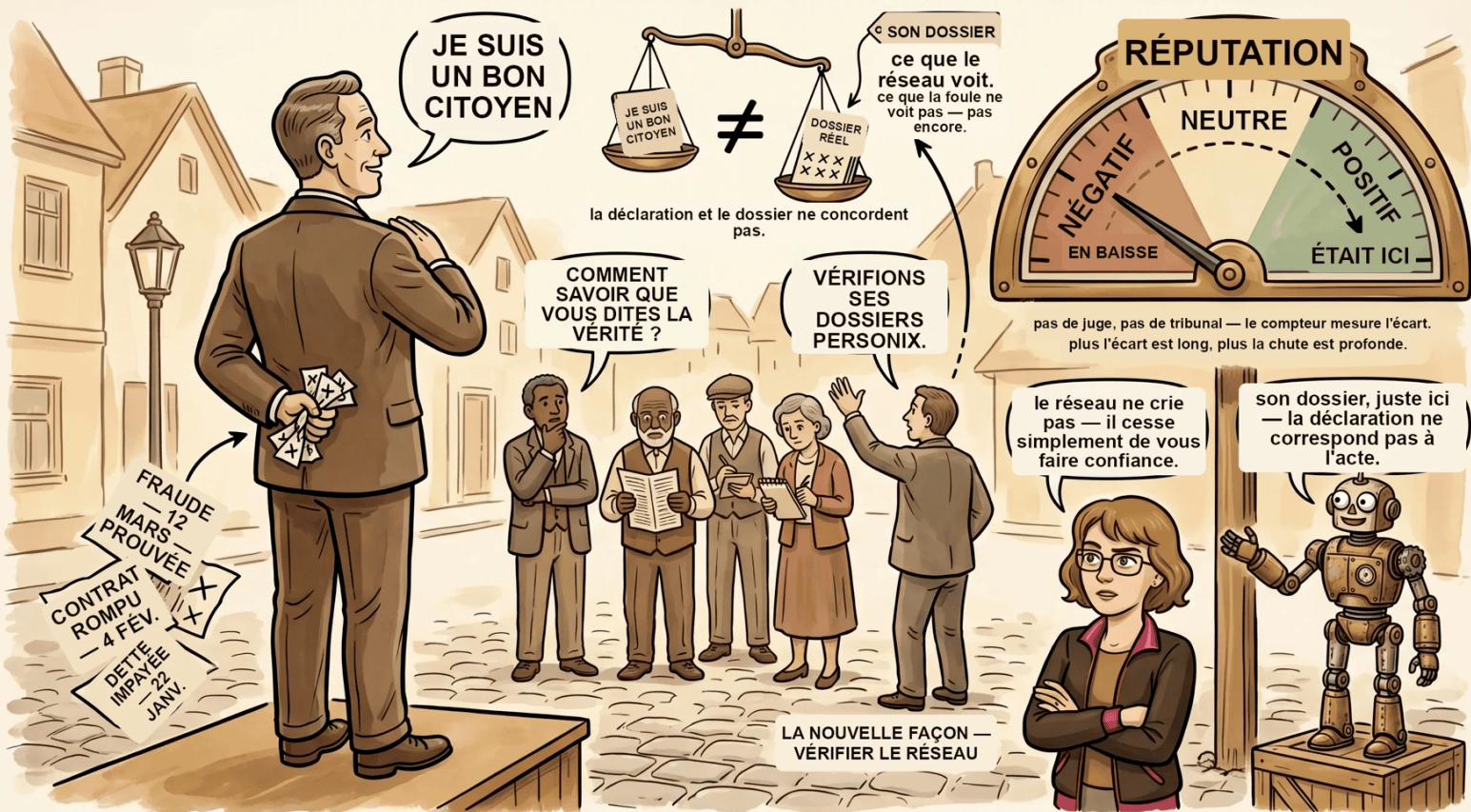
### **Consensus vs responsabilité**

Pour que le réseau serve de source d'information précieuse, une DID ne devrait pas être trop radicale — sinon les autres la rejetteront. La pression sociale cherchera l'équilibre, et les tentatives de le déstabiliser seront vraisemblablement punies.



# L'HYPOCRISIE EST LE COMPORTEMENT LE PLUS COÛTEUX

LE RÉSEAU COMPARE DISCRÈTEMENT VOS PAROLES À VOTRE DOSSIER — L'ÉCART EST VISIBLE DE TOUS



LE DÉCLARER ET LE ROMPRE ? L'ÉCART EST LE COMPORTEMENT LE PLUS COÛTEUX.

# LE REMÈDE À L'HYPOCRISIE

DÉCLAREZ VOS RÈGLES — VIVEZ SELON ELLES, OU LE MARCHÉ VOUS EN FAIT PAYER LE PRIX

JE DÉCLARE MA POLITIQUE



tout le monde peut lire mes normes.  
pas de gardiens, pas de secrets.

LE MONDE OBSERVE



le monde note ce qu'il fait réellement.  
chaque jour, un peu plus de preuves dans son registre.

AU MAGASIN — VOUS PAYEZ POUR VOTRE PROPRE DOSSIER



l'hypocrisie n'est pas punie par une autorité — elle est tarifée par le marché.  
chaque service ordinaire que vous achetez porte un surcôt façonné par votre propre dossier.

POURRIONS-NOUS APPELER CELA LE CONTRAT SOCIAL — REDESSINÉ ?

aucune autorité n'impose l'éthique — le prix, si.  
une pression douce, chaque jour, vers la moyenne commune avec laquelle nous pouvons tous vivre.

AGISSEZ SELON VOS PAROLES — OU PAYEZ-EN LE PRIX. L'HYPOCRISIE EST LA RÉPUTATION LA PLUS COÛTEUSE.



## ■ Le nombre de voix n'est pas la même chose que le poids d'une voix

Juraj Karpiš dit que « l'argent est la mémoire des bonnes actions ». J'ajouterais que la réputation est la mémoire des mauvaises.

Il s'ensuit que, méritocratiquement, celui qui contribue davantage et n'a pas de mauvaise réputation mérite un plus grand poids de voix dans la communauté. Vu à travers le prisme des relations bilatérales : quand je pèse quelles pressions de consensus accommoder, le plus grand poids revient aux relations dont je tire le plus grand bénéfice économique. Dix personnes avec qui je n'ai aucun échange commercial actif m'influenceront bien moins qu'un partenaire d'affaires permanent. Ce paradigme ne se limite pas au commerce — il s'étend aux relations sociales, politiques et autres.

## Roles in the verification transaction and authorities

### Vue d'ensemble des rôles

Nous avons déjà brièvement abordé certains de ces rôles dans le chapitre sur le réseau et ses propriétés fondamentales. Le moment est venu de les examiner à nouveau, plus en détail, et d'ajouter les rôles supplémentaires dont nous avons besoin pour rendre le réseau plus robuste. Chaque transaction de vérification implique plusieurs rôles — voyons comment ils se comportent.

## ■ Les rôles dans une transaction de vérification

Chaque vérification implique jusqu'à six rôles distincts, résumés dans le tableau ci-dessous. Tous peuvent disposer de leur propre DID dans le réseau de réputation décentralisé.

| Rôle                | Description                                                                                                                                                                                              |
|---------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Émetteur</b>     | La personne qui publie l'information dans le réseau — affirme que quelque chose s'est produit (une DID a été créée, modifiée ou dissoute, une assertion, la politique d'une DID donnée, etc.)            |
| <b>Sujet</b>        | La personne dont parle l'information — le destinataire de l'assertion                                                                                                                                    |
| <b>Autorité</b>     | Une entité de confiance qui engage son nom sur la qualité de l'assertion, en l'examinant et en passant en revue les preuves présentées ou en les recueillant activement                                  |
| <b>Observateur</b>  | Un tiers indépendant qui tient un registre de la manière dont le vérificateur traite l'assertion — s'assurant que le vérificateur ne reste ni silencieux ni ne s'écarte de la politique qu'il a déclarée |
| <b>Vérificateur</b> | Un participant sélectionné algorithmiquement qui traite la transaction                                                                                                                                   |
| <b>Délégué</b>      | Une personne agissant au nom d'un autre participant                                                                                                                                                      |



## Émetteur

Nous avons déjà rencontré l'émetteur. Lorsque quelqu'un subit un tort, ou veut faire connaître une réussite qui lui est propre, c'est la personne représentée par la DID qui déclenche le processus de mise de cette information dans le réseau — parce qu'elle a l'intérêt premier à le faire (la motivation étant soit un désir de réparation, soit un souhait d'améliorer son image publique).

### ■ Assertions positives

Les assertions positives à mon sujet, je peux les conserver, en tant que sujet et émetteur à la fois, pour les situations dans lesquelles je veux les utiliser (un diplôme, un certificat de service rendu, etc.). C'est là qu'une assertion positive diffère d'une négative : partager une assertion négative vérifiée est dans l'intérêt de toute la communauté, tandis qu'une assertion positive est dans l'intérêt de son porteur.

## Autorité

L'autorité joue un double rôle : elle peut être **auditeur** (vérifier la qualité des preuves avant qu'une assertion ne soit publiée) ou **garant** (engager sa réputation sur la véracité d'une assertion). Dans les deux cas, elle renforce l'assertion de l'émetteur. Ces deux services sont dissociables — une autorité peut offrir l'un, l'autre, ou les deux à la fois. L'hypothèse de travail est que la plupart des services fournis par les autorités peuvent être rendus sur une base de marché libre. Cela vaut même dans des domaines qu'on imagine difficilement privatisés, comme la justice, où des services spécialisés — enquête, évaluation

# L'ÉMETTEUR — CELUI QUI RÉDIGE LA DÉCLARATION

AUTEUR · SIGNATAIRE · ENGAGE SA PROPRE RÉPUTATION

## CE QUE FAIT L'ÉMETTEUR

1. Rédige la déclaration dans ses propres mots
2. Rassemble des preuves du monde réel pour l'appuyer
3. Signe avec son propre DID et l'envoie à l'autorité choisie
4. Paie le coût de publication
5. Assume les conséquences s'il ment

## MA RÉPUTATION



Si c'est faux, mon aiguille chute.

Mon nom y figure. J'ai intérêt à en être sûr — et à apporter des preuves.

N'importe qui peut parler. Le mensonge coûte à celui qui le profère.



L'émetteur est l'auteur. Son nom y figure.

\* N'importe qui possédant un DID peut être émetteur. Le seuil requis est le courage et la responsabilité, pas une licence.

des preuves, jusqu'aux services aujourd'hui rendus par les armées centralisées (planification stratégique, entraînement standardisé, achats et gestion des stocks, etc.) — peuvent être efficacement fournis par des acteurs du marché. Il n'y a guère de chose qui, après restructuration, ne pourrait être rendue plus efficace par les incitations du marché libre.

■ **L'autorité, l'émetteur et l'observateur ne doivent jamais être le vérificateur de leur propre cas.**

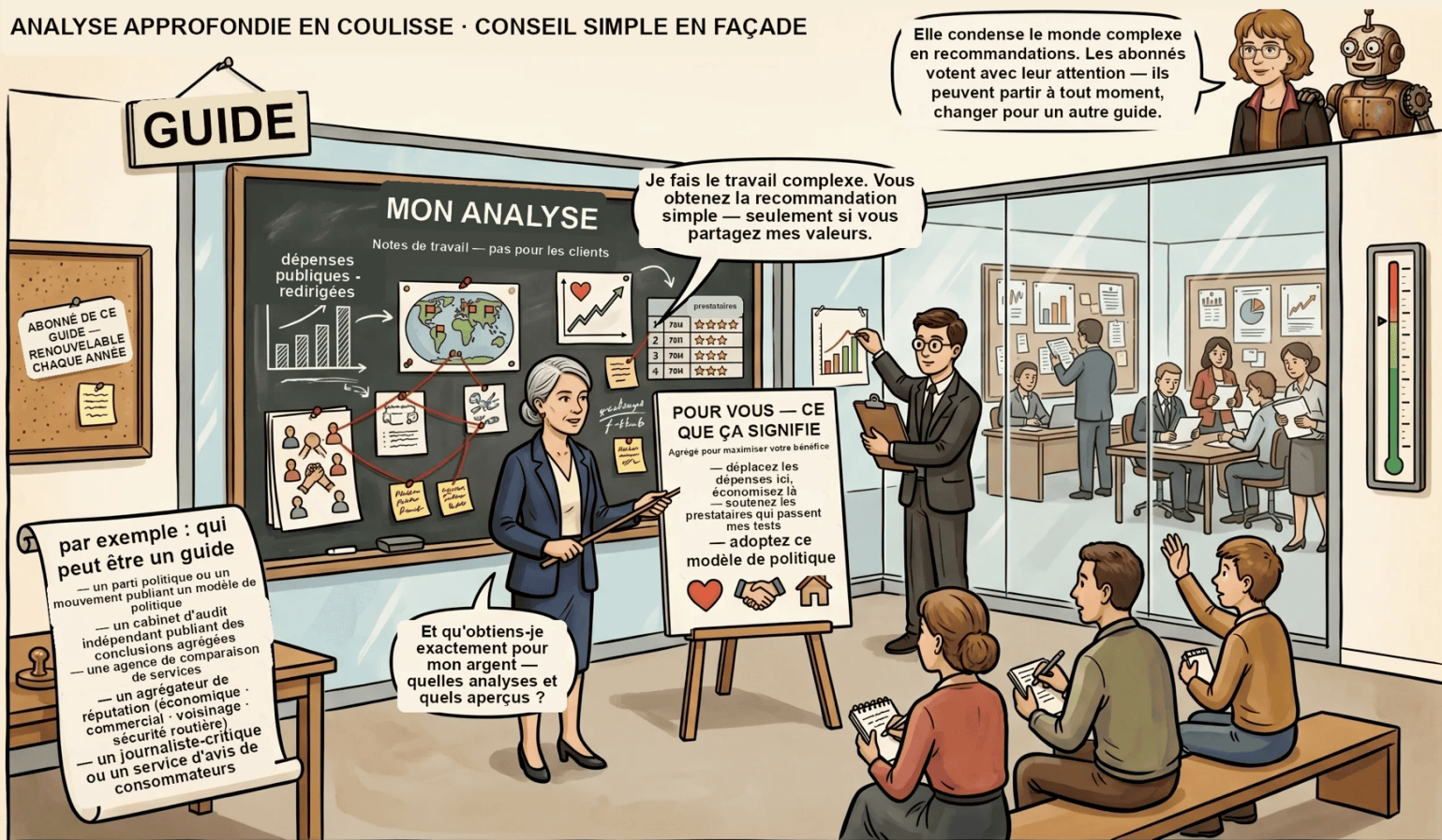
La sélection algorithmique du vérificateur garantit l'indépendance. Personne ne peut vérifier sa propre assertion, ni une assertion dans laquelle il a un intérêt direct. C'est l'une des règles fondamentales que toute la communauté des DID a intérêt à faire respecter.

Les graphiques suivants montrent des vues complémentaires de l'étendue de l'activité que couvrent les autorités (le terme « autorité » peut se lire de façon interchangeable avec « prestataire de services »).



# LE GUIDE — VOUS AIDE À VOUS ORIENTER SELON VOS VALEURS

ANALYSE APPROFONDIE EN COULISSE · CONSEIL SIMPLE EN FAÇADE





## ■ L'autorité comme observateur incognito

Une autorité réputée — pensez à un notaire dont l'activité repose uniquement sur son historique — peut, à côté des fonctions principales (auditeur / garant), en offrir une troisième : le rôle d'observateur incognito pendant la vérification. Elle tient un registre horodaté de l'assertion soumise, de sorte que le vérificateur ne puisse pas la laisser tomber en silence. Le mécanisme du rôle d'observateur est décrit plus loin, dans la section sur le rôle de l'Observateur.

## Vérificateur

Toute DID peut agir comme vérificateur, soit directement, soit via des droits de vérification délégués à une DID tierce. Pour que moi — ou mon délégué — puisse vérifier, je devrais être joignable sur le réseau (en ligne). Tout le monde ne voudra pas s'y engager, c'est pourquoi un enregistrement DID peut lister, par ordre de priorité, les suppléants qui exerceront la fonction en son nom pendant qu'elle est hors ligne.

Chaque DID active dans le réseau déclare publiquement sa propre politique. À travers les règles définies dans cette politique, elle juge, pendant le processus de vérification, la réputation de la contrepartie ainsi que le contenu et la forme de l'assertion que l'émetteur a marquée pour publication dans le réseau de réputation. La formule de calcul utilisée pour déterminer les frais des services de vérification fait partie de la politique. Une fois cela en place, alors, sur un nombre statistiquement grand d'assertions circulant dans le réseau, j'attends que l'algorithme du réseau me tire du côté de l'émetteur et m'assigne, dans une itération donnée, à vérifier l'information émise. L'émetteur peut calculer à l'avance comment un vérificateur au comportement correct réagirait, mais ne peut pas éviter de le contacter effectivement

# LE PRESTATAIRE — GÈRE UN SERVICE DE SIGNATURE DE DÉCLARATIONS

## NORMES PUBLIÉES · PRIX PUBLIÉS



**Lié par ce qu'il déclare publiquement. La réputation fait le reste.**

\* Le prestataire a aussi sa propre politique — quand il accepte, quand il rejette, comment il rembourse. Elle est publiée, mais ce n'est pas le sujet principal ici.

(lui ou ses suppléants) ; l'itération avec le vérificateur sélectionné doit être menée par l'émetteur, même lorsqu'il sait d'avance qu'elle n'aboutira pas.

Comment savons-nous que l'émetteur exécute l'algorithme de sélection des vérificateurs sur le bon ensemble de DID vérificatrices candidates ? En même temps que sa politique déclarée publiquement, chaque DID publie aussi la liste courante des identifiants de son réseau social au sein du réseau de réputation. Si un émetteur définit son réseau social comme une bulle sociale qui ne fait que faire écho à ses propres vues et les renforcer, l'information publiée à travers lui ne sera guère mieux reçue par d'autres communautés. Le fait que je parvienne, à grands frais, à pousser une assertion radicale dans le réseau n'implique pas que, lorsque je juge la réputation de la contrepartie, je lui accorderai le moindre poids. Certaines assertions, ma communauté me pousse à en tenir compte (peines et restrictions imposées aux contrevenants) ; d'autres relèvent entièrement de moi — je décide moi-même de la valeur économique d'inclure ou d'exclure une information donnée.

## **Sujet**

Ceux que concerne l'information publiée dans le réseau de réputation en sont les porteurs ou, si vous préférez, les sujets. Les incitations du réseau de réputation sont agencées de sorte que le sujet ait toutes les raisons de se comporter correctement et loyalement selon ses propres règles, et soit poussé par la communauté vers un certain juste milieu du respect des règles. Il a même une incitation à se comporter plus moralement que ses règles déclarées ne l'exigent — les politiques pré-déclarées n'empêchent pas la communauté de parvenir à un consensus pour appliquer rétroactivement une évaluation ou une mesure. Sous cet angle, l'alternative du réseau de réputation à un ordre juridique est, comme on pouvait s'y attendre, davantage guidée par l'esprit des règles que par leur lettre.



# LE VÉRIFICATEUR — JUGE LA DÉCLARATION SELON LA POLITIQUE PUBLIÉE

QUATRE PORTES, DANS L'ORDRE. LES FILTRES BON MARCHÉ D'ABORD.

Il ne peut pas faire preuve de créativité. Il doit faire ce que dicte sa politique.

Ses propres règles. Publiques. Il ne peut pas les changer discrètement.

## PORTES DE VÉRIFICATION — DANS L'ORDRE

### 1. FILTRAGE PAR POLITIQUE

Est-ce que je vérifie même ce type de déclaration ?

### 2. CONFIANCE EN L'AUTORITÉ

L'autorité est-elle au-dessus de mon seuil ?

### 3. RÉPUTATION DE L'ÉMETTEUR

L'émetteur atteint-il ma barre de réputation ?

### 4. VÉRIFICATION DU CONTENU

Signatures, cohérence, écart par rapport à la politique

NE PEUT PAS ÊTRE : l'émetteur, l'autorité, l'observateur ou le sujet.

RÉPUTATION DU VÉRIFICATEUR

S'ÉCARTER DE LA POLITIQUE — LA RÉPUTATION CHUTE → PLUS AUCUN CHOIX FUTUR

## CE QUE FAIT LE VÉRIFICATEUR

1. Filtre selon ses portes de politique publiées (dans l'ordre)
2. Vérifie la confiance envers l'autorité, puis la réputation de l'émetteur
3. Évalue le contenu de la déclaration seulement si les portes sont franchies
4. Facture des frais proportionnels au risque
5. Engage sa propre réputation à chaque décision

FRAIS  $\propto$  RISQUE

plus de risque → frais plus élevés

Les filtres bon marché d'abord. La vérification coûteuse du contenu en dernier.

Le vérificateur est lié par les règles qu'il a lui-même publiées — et par la réputation qu'il risque de perdre.



# LE SUJET — CELUI QUE CONCERNE LA DÉCLARATION

LA REÇOIT · NE PEUT PAS LA FAIRE TAIRE · PEUT Y RÉPONDRE



Le sujet n'a pas de veto — seulement le droit de réponse.  
\* Une contre-déclaration est elle-même une déclaration — la réputation du sujet est en jeu pour ce qu'il dit en réponse.

## Observateur

Le rôle d'observateur supprime l'incitation du vérificateur à contourner les règles. Dans les situations où un vérificateur n'aime pas la demande de l'émetteur ou de l'autorité, il pourrait simplement rester silencieux — ne pas répondre et bloquer la séquence algorithmique. L'observateur — ou un ensemble d'observateurs — engage sa réputation en documentant la manière dont le vérificateur a été sollicité. Si le vérificateur reste silencieux malgré une politique déclarée qui affirme le contraire, il peut être convaincu d'avoir violé le protocole.

## Le mécanisme : horodatage et code de défi

Avant d'envoyer une assertion au vérificateur, vous la faites transiter par des observateurs — des personnes en qui vous avez confiance, ou des prestataires spécialisés de services d'observation qui facturent de modestes frais. Chaque observateur reçoit votre soumission, l'horodate, signe qu'il l'a vue partir, et génère un code de défi — un hash cryptographique de sa signature. Les codes sont annexés à votre demande. Le vérificateur les voit, mais n'a aucune idée de qui sont les observateurs, ni même si les codes sont réels. Les observateurs agissent ainsi comme des mandataires entre l'émetteur et le vérificateur, détenant un registre indépendant attestant que l'assertion a été soumise et ce qu'elle contenait. Il peut y en avoir de zéro à N.

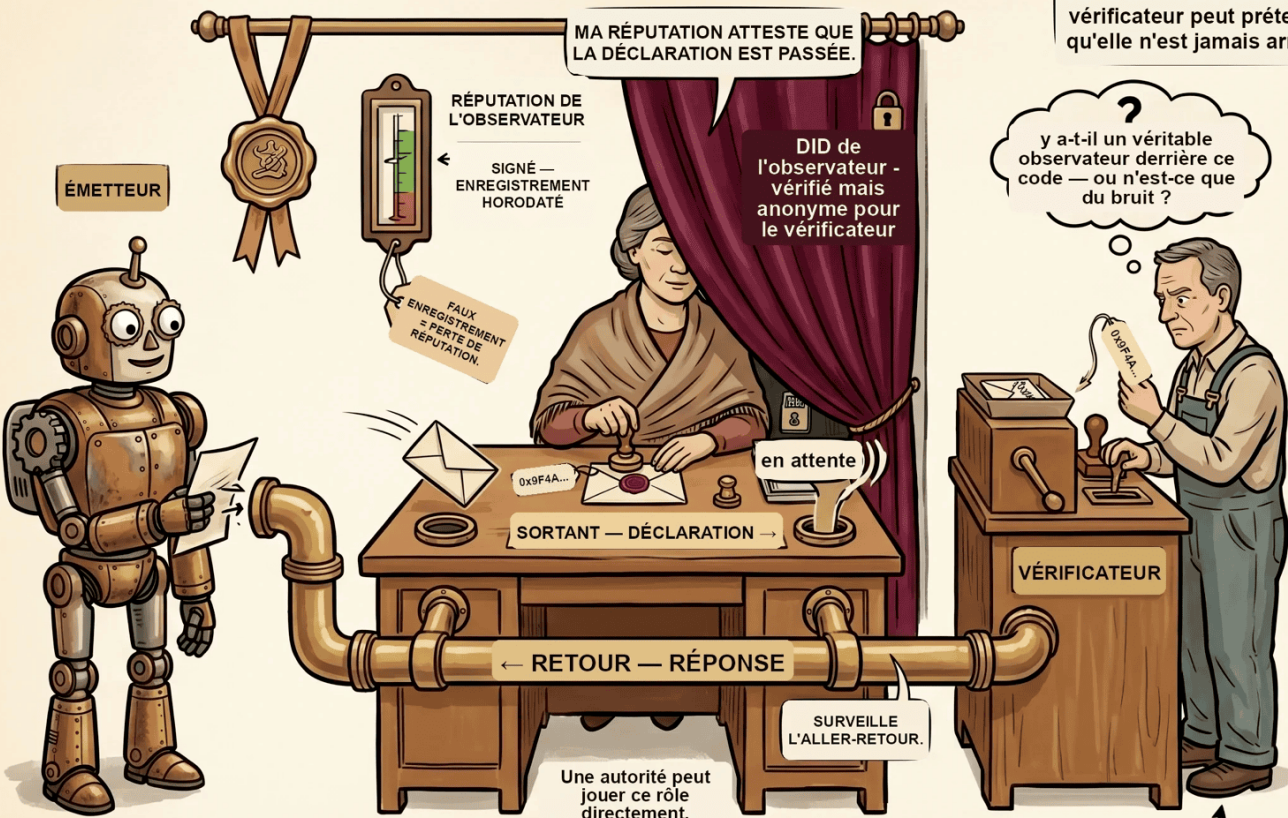
Lorsque le vérificateur se comporte honnêtement — en acceptant ou en rejetant conformément à sa politique déclarée — les codes restent opaques. Personne n'est exposé.

Mais si le vérificateur reste silencieux malgré une politique accommodante, ou répond d'une manière qui contredit ce qu'il a publié, vous détenez les signatures originales des observateurs. Vous pouvez les publier comme un témoignage par mandataire attestant que l'assertion a été soumise et que le vérificateur n'a pas suivi le protocole. Quiconque peut vérifier que les signatures correspondent aux codes de défi.



# L'OBSERVATEUR — UN RELAIS QUI TRANSMET LA DÉCLARATION ET SURVEILLE L'ALLER-RETOUR

LE VÉRIFICATEUR LUI PARLE. LE VÉRIFICATEUR NE SAIT JAMAIS QUI ELLE EST — NI MÊME SI QUELQU'UN OBSERVE.



## CE QUE FAIT L'OBSERVATEUR

1. Reçoit la déclaration de l'émetteur
2. L'estampille de son propre sceau ; l'estampille est l'enregistrement horodaté
3. La transmet au vérificateur au nom de l'émetteur
4. Surveille si la réponse revient, et ce qu'elle dit
5. Ne publie sa signature que si le vérificateur se comporte mal — sa réputation est la garantie

notes de bas de page  
Il peut y avoir zéro à N observateurs derrière toute requête. Le vérificateur ne voit que des codes opaques et ne sait jamais si un véritable observateur surveille ou s'il ne s'agit que de bruit. Cette incertitude est ce qui incite à bien se comporter.

\* Symétriquement, le vérificateur peut faire passer la réponse par son propre observateur — même astuce, direction opposée.

Anonyme pour le public, responsable devant le réseau. Le vérificateur voit le code, jamais l'observateur.

## La chute : vous n'avez pas besoin de vrais observateurs

Et voici la partie la plus élégante : **vous n'avez pas besoin de vrais observateurs du tout**. Vous pouvez générer des nombres aléatoires qui ressemblent exactement à des codes de défi. Le vérificateur ne peut pas faire la différence — il doit jouer aux dés pour décider s'il risque sa réputation. Derrière chaque demande qu'il reçoit pourrait se tenir un observateur respecté qui surveille incognito — ou ce pourrait être du pur bruit. Le vérificateur ne le sait pas. Et cette incertitude est le mécanisme.

Le coût du maintien d'une pression honnête : quasi nul (les nombres aléatoires sont gratuits). Le coût potentiel de la malhonnêteté pour le vérificateur : catastrophique. Le comportement honnête est incité même quand personne ne surveille réellement.

Le système fonctionne parce que chacun est un peu paranoïaque. L'incertitude coûte moins cher que la surveillance.

### ■ Plusieurs vérificateurs dans une seule itération

Une règle compagne renforçant la disponibilité des vérificateurs peut être une extension algorithmique qui renvoie, dans une seule itération, un ensemble de vérificateurs candidats plutôt qu'un seul.

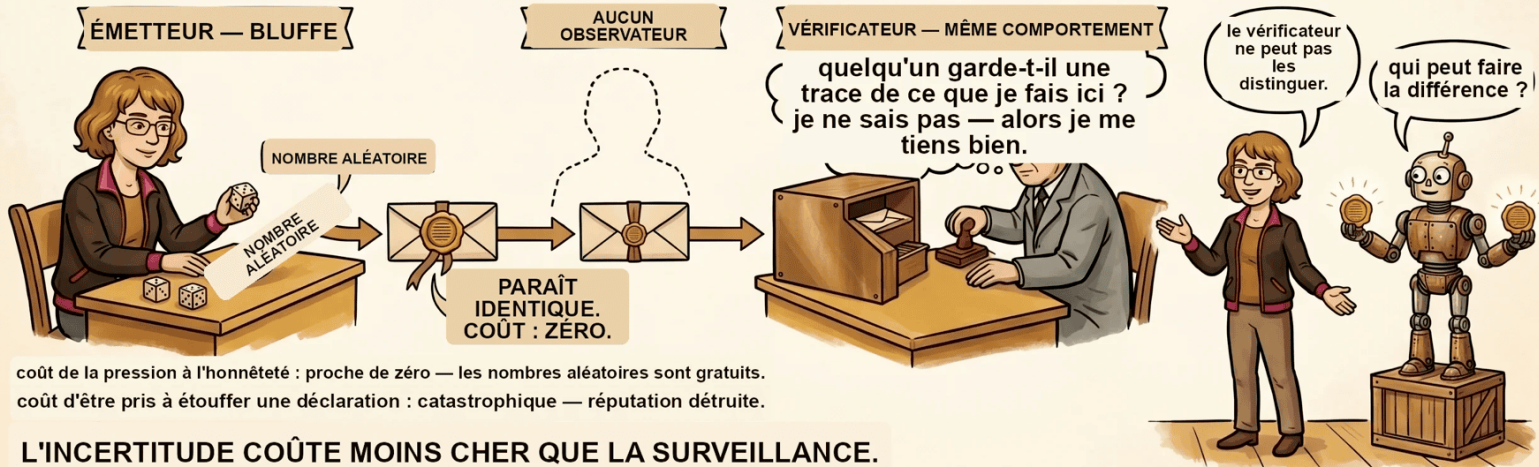
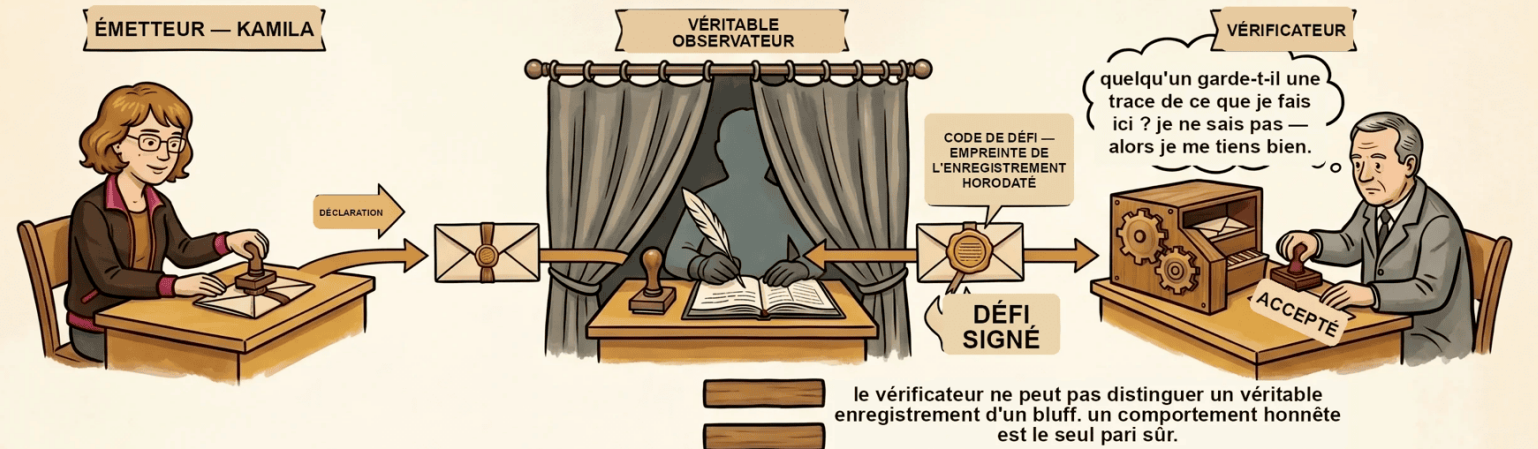
## Délégation

La civilisation a bâti sa croissance économique sur la capacité de division du travail et de spécialisation. Le monde, dans toute sa splendeur, est complexe, et nos chances de le saisir dans toute sa complexité sont



# LE BLUFF QUI MAINTIENT LE VÉRIFICATEUR HONNÊTE

UN VÉRITABLE OBSERVATEUR ET UN BLUFF ALÉATOIRE SONT IDENTIQUES DU POINT DE VUE DU VÉRIFICATEUR



proches de zéro. La voie naturelle est de déléguer un large éventail d'activités qui soutiennent une vie confortable à des prestataires spécialisés, qui nous font gagner du temps, de l'énergie et de l'argent, et nous laissent nous spécialiser à notre tour — en fournissant les services que nous savons faire le mieux, ou que le marché valorise le plus chez nous.

La même logique de délégation s'étend au réseau de réputation. Dans le chapitre L'interrupteur liberté-totalitarisme (et la délégation), nous avons exposé les principes de sauvegarde d'une société libre en limitant le nombre d'assertions pouvant être publiées dans le réseau au sein d'une fenêtre de temps donnée (pensez, en termes simplifiés, à quelques droits de publication par an, de sorte que la société reste maximale libre). Ce principe peut s'étendre à plusieurs dimensions. Nous ne sommes pas obligés de n'avoir qu'un seul nombre — nous pouvons avoir plusieurs limites, s'appliquant à différents types d'assertions. Nous pouvons utiliser un nombre différent pour signaler l'hypocrisie d'autrui que pour les fautes dans les affaires commerciales, et, disons, une modification du document DID comme un changement de mot de passe est une chose dont la communauté ne se souciera guère, et ainsi de suite. Tout dépend de la manière dont la communauté définit, au fil du temps évolutif, ce qui sert ses intérêts pour trouver le bon équilibre entre son niveau cible de liberté et de responsabilité.

Pourquoi le nombre de droits de publication que la communauté m'accorde devrait-il être suffisamment petit ? Signaler une DID (sujet) par une assertion négative détruit une réputation qui a mis longtemps à se construire, et le dommage perdure. Une réputation détruite fait face à une échelle de sanctions croissantes de la part de la communauté pour chaque nouvelle infraction ou récidive, jusqu'à l'élimination complète de l'entité perturbatrice (le cas extrême). Une échelle de punition croissant de façon exponentielle n'a pas besoin d'un grand volume d'assertions, pourvu qu'elles soient étayées par des preuves vérifiables. Cela vaut pour l'état stationnaire paisible, quand la société n'est pas secouée par une catastrophe (externe ou interne).

Pour les événements de très faible probabilité, la fréquence statistique est volatile lorsqu'elle est appliquée à un individu. À l'échelle de la population de la communauté, elle ne l'est pas. C'est là la valeur de déléguer ses droits de publication à des autorités agrégatrices spécialisées, qui — un peu comme une assurance mutuelle en cas de sinistre — utilisent votre droit et l'exercent en votre nom. Parlons de manière moins abstraite et donnons quelques exemples : - détecter et combattre le crime organisé - faire respecter les accords commerciaux - gérer les privilèges (preuves de formation, acquisitions / cessions d'actifs, etc.) - et ainsi de suite



# LE DÉLÉGUÉ — UN SERVICE DE DÉCLARATION AUQUEL VOUS VOUS ABONNEZ

DÉLÉGUEZ CE QUE VOUS NE POUVEZ PAS GÉRER VOUS-MÊME · GARDEZ CE QUI COMPTE POUR VOUS



Externalisez ce que vous ne pouvez pas gérer vous-même. Restez informé. Reprenez les droits à tout moment.

\* Si le délégué agit en dehors du périmètre convenu, sa réputation et la vôtre en pâtissent publiquement toutes les deux.



## ■ Comment fonctionnent réellement les « droits de publication »

Le graphique du délégué représente les droits de publication comme des jetons physiques, par souci de clarté, mais dans le système aucun objet de ce genre n'existe. Ce qui se passe réellement est ceci : les politiques des personnes avec qui vous voulez rester en bons termes — votre communauté — s'agrègent en une règle émergente sur le nombre d'assertions par an qu'elles accepteront de vous comme pertinentes avant de commencer à vous traiter comme du bruit. Le plafond existe pour que le réseau ne soit pas noyé sous des assertions triviales du type « et si », et qu'il reste aussi libre que la communauté le souhaite (le signal préservé en limitant le volume).

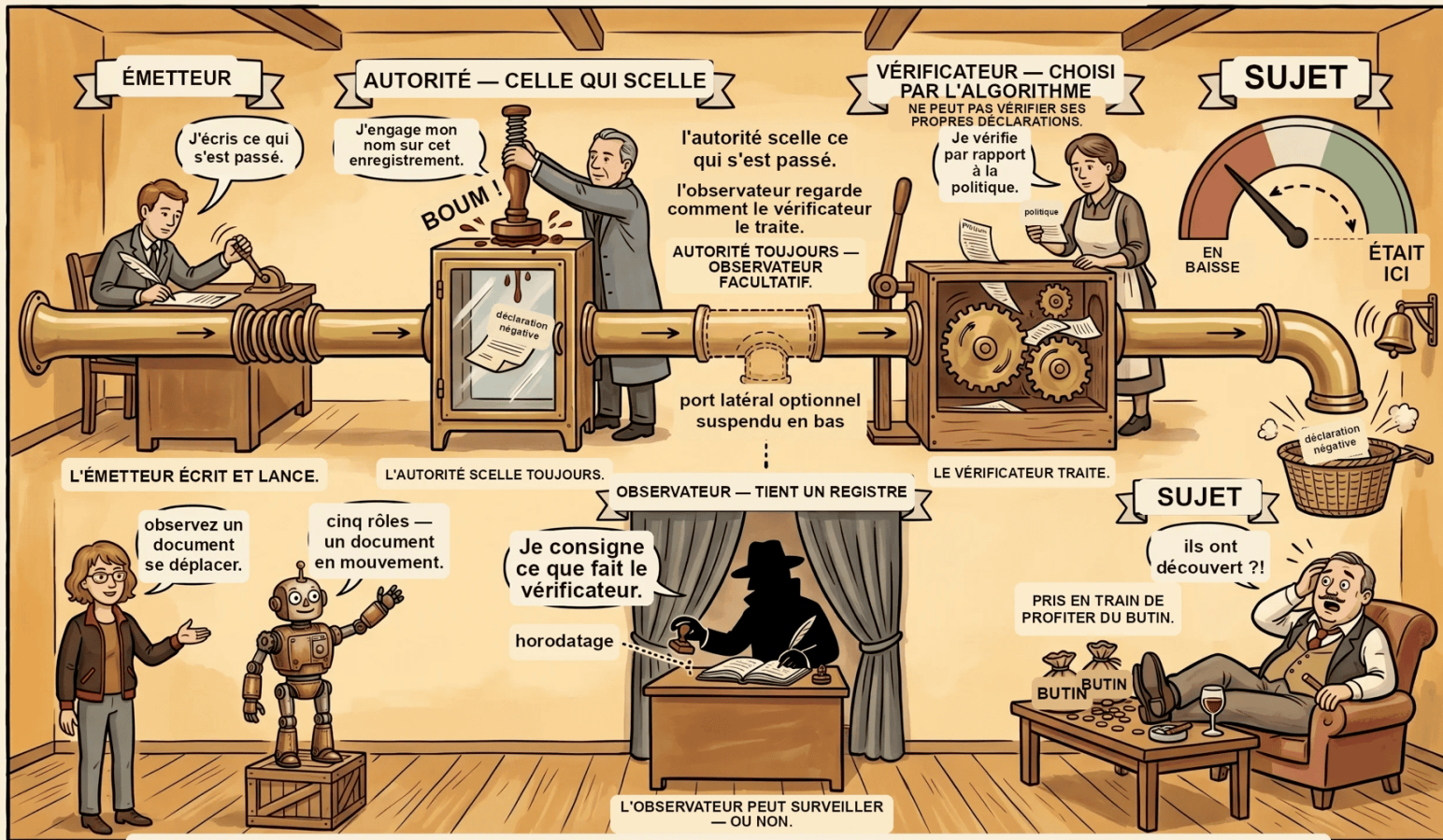
Vous lisez ce que votre communauté vous autorise. Il y a une fourchette, avec une certaine dispersion selon les personnes auxquelles vous accordez le plus de poids. Vous décidez ensuite — dans le cadre de cette allocation — combien d'assertions publier vous-même, et combien déléguer à des services professionnels qui publieront en votre nom uniquement lorsque des événements entrent dans leur champ. C'est ce qui vous maintient en bons termes sans vous forcer à déposer une assertion pour chaque petite chose qui vous arrive.

Les « jetons » du graphique sont une représentation visuelle de cette boucle lire-et-décider, non un artefact littéral.

Il est utile de pouvoir révoquer les droits de publication délégués dans le réseau de réputation. Cela peut se faire à tout moment, tant que le délégué n'a pas encore utilisé le droit délégué.

# UNE DÉCLARATION NÉGATIVE CIRCULE DANS LE SYSTÈME

SUIVEZ UN DOCUMENT — VOYEZ CE QUE CHAQUE RÔLE LUI FAIT



CINQ RÔLES, UN DOCUMENT EN MOUVEMENT — PERSONNE NE PEUT SE VÉRIFIER SOI-MÊME.

## **La communication entre les rôles**

Le graphique ci-dessous résume comment les rôles se connectent dans un cas réel — depuis la soumission d’une assertion par l’émetteur jusqu’à sa publication dans le réseau de réputation.

## **Le contrat social émergent — la politique**

Jusqu’ici, nous avons décrit comment les assertions sont vérifiées, et quel rôle joue chacun. Nous nous tournons maintenant vers la manière dont des milliers de politiques individuelles deviennent quelque chose qui fonctionne comme un véritable contrat social. Rien qui ressemble aux rêves de gauche d’un contrat social et d’une solidarité imposée.

Chaque participant déclare sa propre politique fondée sur sa morale (policy) — ce qu’il considère comme acceptable, et comment il réagit à des comportements spécifiques des autres. L’agrégat de toutes les politiques du réseau connues d’une DID donnée (la communauté) produit une éthique émergente — des normes observables que personne n’a conçues. Ces normes émergentes, sous-tendues par des signaux de prix bilatéraux, forment un contrat social mesurable : non pas une construction théorique que personne n’a signée à la naissance, mais des règles empiriquement observables, adossées à un comportement réel.

## ■ Le contrat social

---

Les gens débattent pour savoir si « contrat social » n'est pas un oxymore. Personne ne signe rien, et pourtant on l'invoque pour justifier l'action législative et exécutive dans les sociétés centralisées.

Une analyse phénoménologique des interactions dans un réseau décentralisé pourrait révéler certaines règles émergentes — globales ou locales. Comment devrions-nous appeler ces normes largement partagées ? Un contrat social ? Tout comme pour les communautés, le contrat social d'une communauté ne peut être observé et délimité avec précision — chaque angle sur la communauté donne un contrat social différent.

## ■ La politique fondée sur les valeurs

---

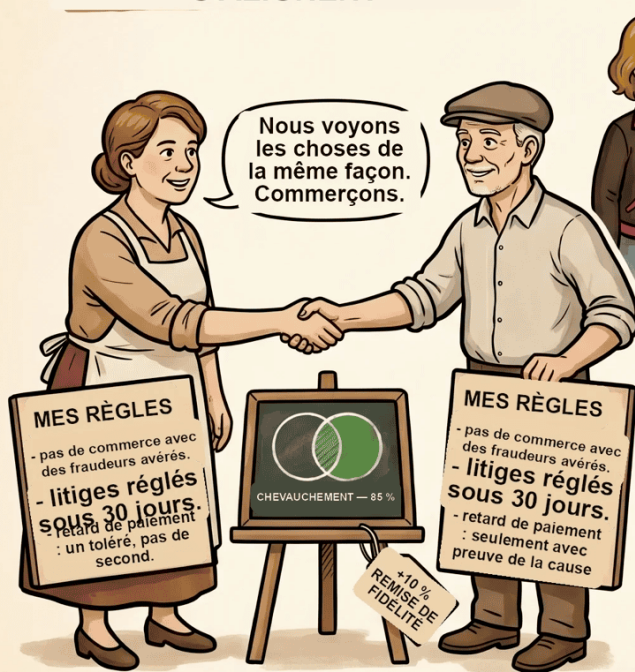
Il est tout aussi trompeur de traiter la « politique fondée sur les valeurs » comme le fondement de la prise de décision. Les valeurs sont davantage des grappes phénoménologiques de règles communément préférées à un moment donné. Elles évoluent, et elles ne sont pas constantes dans le temps.



# LES POLITIQUES SE RENCONTRENT. LES ATTITUDES SE FORMENT.

LES RÈGLES DÉCLARÉES FIXENT LE PRIX D'AUJOURD'HUI — REMISE POUR L'ALIGNEMENT, MALUS POUR LA DIVERGENCE

## QUAND LES POLITIQUES S'ALIGNENT



Mêmes biens, deux prix. Ce sont les déclarations — pas la réputation — qui en décident.

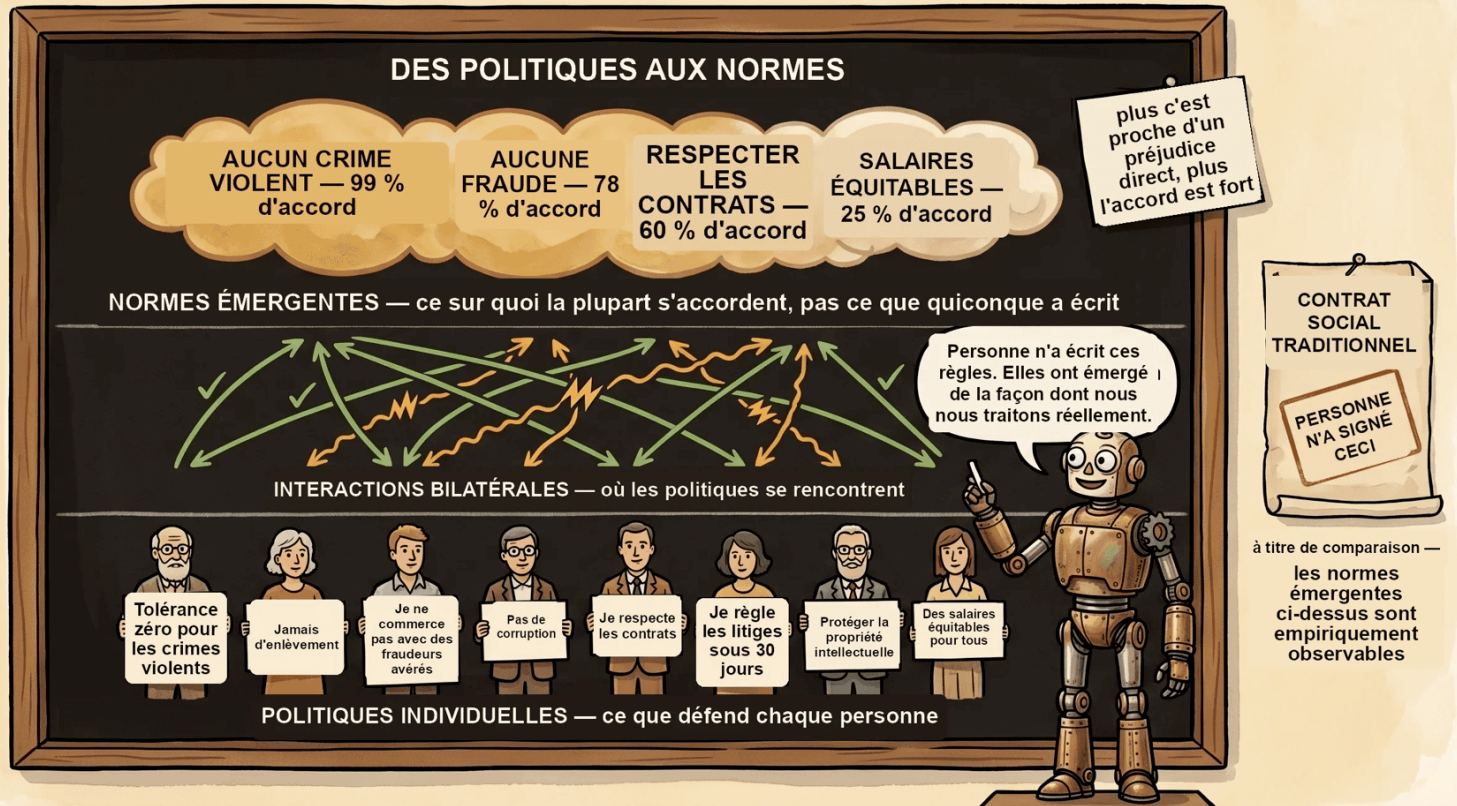
## QUAND LES POLITIQUES DIVERGENT



Quand deux politiques se rencontrent dans un échange, leur alignement devient le modificateur de prix.

\* Il ne s'agit pas de réputation. Il s'agit de ce que chaque personne a déclaré publiquement — et est désormais censée respecter.

# COMMENT L'ÉTHIQUE ÉMERGE DES POLITIQUES INDIVIDUELLES



**L'éthique n'est pas conçue. Elle émerge de la façon dont nous nous traitons réellement.**

\* Chaque politique individuelle reflète la moralité de cette personne — façonnée par la pression à s'adapter à sa communauté et à son environnement.

## Fournir des informations sur soi-même

Lorsque deux sujets DID qui ne se connaissent pas entrent dans une relation économique, nous pouvons signer une demande auprès de notre propre communauté au nom de l'autre partie, en lui demandant de fournir des informations sur nous. C'est toutefois une notion très naïve de ce que sont les communautés. Ce ne sont pas des ensembles fermés — une même DID peut être participante de plusieurs communautés.

Une communauté est davantage un phénomène phénoménologique du point de vue d'un participant donné, se manifestant dans son réseau social ; ce n'est pas quelque chose qu'il est toujours sensé de délimiter explicitement. Les habitants d'un village peuvent former une communauté, mais une personne qui n'y vient que le week-end peut aussi appartenir à une autre communauté dans ce même village. Une communauté peut aussi être une équipe de football avec ses supporters, ses dirigeants et les familles de tous les intéressés. Une nation, ou les citoyens d'un État, peuvent également former une communauté ou des communautés. Regarder une DID sous différents angles peut donner des vues différentes (et souvent intuitives) des communautés.

Les DID situées aux frontières sont ainsi des ponts entre les communautés et — tout comme dans la vie réelle — elles jouent un rôle dans la fourniture d'informations sur les membres d'autres communautés, que ce soit à un niveau amateur ou professionnel, comme une autorité spécialisée dans la mise en relation des personnes et l'agrégation d'informations sur les DID à risque.

Certains types d'informations dans le réseau DID se prêtent bien à un échange mutuel inconditionnel (crime violent, fraude, etc.). D'autres types d'informations, en revanche, une communauté peut les traiter comme restreints à un usage interne à la communauté (l'équivalent de la citoyenneté, des services rendus à la communauté, etc.). Que de telles informations puissent être diffusées ou non dépend des politiques déclarées des membres de la communauté.

Une communauté garde sa vie privée au sein de son propre cercle, et échange en retour, sur une base inconditionnelle, des informations mutuellement bénéfiques.



# Crime et châtement

## Crime et châtement

Nous savons comment fonctionne le réseau : comment les enregistrements sont créés, qui les vérifie, comment la fraude des vérificateurs est dissuadée. Une question demeure — que se passe-t-il lorsque quelqu'un cause réellement un préjudice à autrui ?

### ■ À quel point dépendons-nous les uns des autres ?

**Nous nous tenons tous sur la scène de ce grand monde, et tout ce qui s'y produit nous concerne tous.**

Jan Amos Comenius (Le Labyrinthe du monde et le Paradis du cœur)

Il peut y avoir de nombreuses raisons de rejoindre un réseau de réputation ou de le rejeter. Je crois cependant qu'un aspect de la nature humaine — souvent considéré comme sombre — peut servir un bon dessein. Je parle du besoin humain d'éprouver un sentiment de satisfaction face à une injustice perçue.

La satisfaction, la justice, la vengeance — nous les associons à des émotions négatives. Pour que la société tienne, nous devons au moins faire semblant que la satisfaction est rendue par des institutions centralisées ; sans quoi les individus ne se sentiraient pas liés à la société dans laquelle ils vivent. En

moyenne, nous avons besoin d'appartenir à une équipe et de lui faire confiance. Quand quelqu'un porte préjudice à autrui, la société observe comment la satisfaction sera rendue et à quel degré. De façon quelque peu controversée, je soutiens que souvent dans l'histoire — et aujourd'hui — il n'a pas importé que le procès contre l'accusé fût propre ; ce qui importait, c'était que la société voie *quelqu'un* puni. Cela remplissait sa fonction (de nombreuses erreurs judiciaires et la résistance à rouvrir de vieilles affaires racontent assez bien cette histoire). Le point de vue de la victime et des proches n'est que secondaire. Ce qui importe d'abord, ce sont les signaux adressés au reste de la société, car les injustices ne sont pas si fréquentes qu'elles figurent dans la journée de chaque individu.

Un système de réputation décentralisé permettrait au public de voir les preuves directes et indirectes (auditées et non auditées). La société pourrait évaluer l'information — par elle-même ou via des services du marché libre spécialisés dans une telle évaluation — et décider, sur la base de signaux qualitatifs et quantitatifs, quelles mesures appliquer au sujet (ou même à l'auteur ou à l'autorité vérificatrice).

Qu'est-ce que le châtiment ? C'est une forme d'humiliation de l'auteur présumé par la perte de ses privilèges — de sorte que la victime comme la société aient le sentiment que les actes nuisibles ne paient pas. Voilà le point essentiel : un comportement nuisible ou dangereux ne doit pas payer, et en même temps il doit procurer un sentiment de satisfaction tant aux victimes qu'au reste de la société/communauté.

Un tel châtiment doit-il être administré par une autorité centrale ? Et si chacun pouvait déclarer à l'avance comment il réagira à certains actes ? Je ne peux évidemment pas exécuter un châtiment sur la propriété d'autrui. Mais je peux déclarer que je mettrai ma propriété à la disposition d'un ensemble choisi d'autorités exécutives dans le but de punir l'auteur, si le contrevenant pénètre dans mes domaines. Et je peux le déclarer publiquement, de sorte que d'autres puissent évaluer mon approche.

Et c'est ici qu'entre le mécanisme de prix de la proportionnalité. Si je déclare des châtiments sévères pour des délits mineurs, le réseau fixe le prix de mon extrémisme : les autres me trouveront disproportionné et mes coûts de vérification augmenteront — moins de gens voudront commercer avec moi, ou seulement à de moins bons prix, et moins de vérificateurs accepteront mes enregistrements à un prix raisonnable. Si, au contraire, je suis trop indulgent, la communauté me verra comme un risque. Si je tolère la fraude, la communauté sera vraisemblablement indulgente envers les auteurs d'actes qui me touchent — pour me faire goûter à ma propre médecine.

La justice cesse d'être un bien de luxe. Quand quelqu'un vous porte préjudice, consigner le tort est abordable, l'enregistrement est permanent, et les conséquences pour le contrevenant sont réelles.

### Détection de l'hypocrisie

Déclarer une politique ne suffit pas — si je déclare suivre une règle mais que mon comportement s'en écarte, l'écart est un passif réputationnel. Le réseau ne distingue pas entre « a enfreint la loi » et « a manqué à sa parole » — les deux sont des signaux mesurables. L'hypocrisie coûte cher, et je ne connais pas de chiffon rouge plus irritant.

# UN PIÈGE. UNE ISSUE.

L'INITIÉ REMPORTE TOUJOURS LE CONTRAT — JUSQU'À CE QUE LE RÉSEAU PERMETTE D'ACHETER DIRECTEMENT, SANS PERMISSION.



Le public convient qu'un nouveau système informatique public est nécessaire, payé sur le budget, payé par les impôts.



Derrière des portes closes, l'agent des marchés publics et l'initié conçoivent l'appel d'offres pour qu'il convienne à une seule entreprise. Une enveloppe change de mains.



L'agent hausse les épaules. Sa poche gonfle de pots-de-vin.



Le contrat est attribué. L'initié a la licence — mais aucune compétence, et aucun respect pour le travail.



L'initié rend visite au voisin. « L'offre aimable » est la plus infime des miettes.

1. TRADITIONNEL



la plainte



le silence



la porte fermée



chez l'avocat

Painte, silence, délais, avocat.

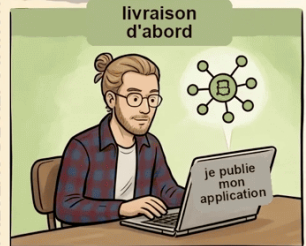
Le piège est intégré aux règles elles-mêmes.



RÉSEAU DE RÉPUTATION

— c'est ici que commence le nouveau monde —

2. RÉSEAU DE RÉPUTATION



livraison d'abord

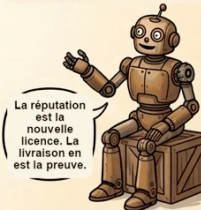


la demande la trouve



un revenu décent

Il livre d'abord. Les gens trouvent l'application et l'utilisent. Chaque utilisateur reconnaissant paie un peu. Un revenu décent. Aucune autorité centrale à corrompre.



Deux voies. Le piège est dans les règles. La sortie consiste à contourner les règles entièrement.

\* Quand les règles sont écrites par l'initié, se plaindre à l'intérieur des règles est le piège — même les amendes retournent alimenter le prochain appel d'offres truqué. Le réseau de réputation est la sortie : les citoyens trouvent le produit, paient directement le créateur, et la communauté confère la seule licence qui compte — la confiance gagnée par la livraison.



## ■ Quantité vs qualité — briser le paradigme binaire de la culpabilité

Dans la justice centralisée, la culpabilité est binaire : 0 ou 1, coupable ou non coupable. Dans un réseau de réputation, ce qui compte n'est pas de savoir si la culpabilité est prouvée, mais l'accumulation de signaux.

Une unique accusation de vol non prouvée contre l'accusé n'éveillera probablement pas beaucoup de vigilance — mais elle éveillera la vigilance envers l'accusateur. Plusieurs indices indirects issus de diverses sources indépendantes, en revanche, commencent à peser. Ce qui compte, ce n'est pas seulement la quantité mais aussi la qualité : l'indépendance des témoins (personnes différentes, contextes différents), la cohérence du schéma (un type de soupçon récurrent), la corrélation temporelle.

À l'inverse, des accusations infondées fréquentes, qui reviennent du même émetteur contre divers sujets cibles, peuvent être évaluées comme de la diffamation — et la réputation de l'accusateur en paie le prix.

# COMMENT LES PREUVES S'ACCUMULENT

« une déclaration isolée »



une seule déclaration — trop mince pour agir. aucune des parties n'est condamnée.

« un schéma »



cinq sources indépendantes — un schéma émerge.

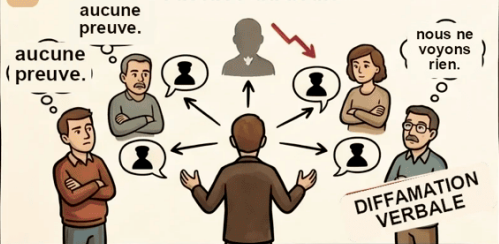
« un poids écrasant »



vingt sources indépendantes — un poids écrasant.

A

« l'astuce du bruit »



diffuser la même déclaration sans preuve — quand la communauté ne voit rien, c'est de la diffamation, et cela coûte à l'accusateur.

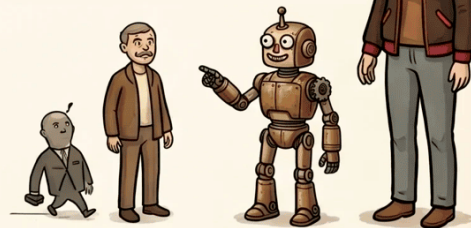
L'indépendance est primordiale. Une voix répétée n'est que du bruit. Plusieurs voix venues d'ailleurs sont un signal.

B

« la rancune »



un seul accusateur qui pointe tout le monde — le schéma, c'est l'accusateur, pas l'accusé.



cela ressemble au monde d'aujourd'hui. c'est le cas — sauf que les motivations sont désormais honnêtes. pas de révolution. juste de meilleures incitations.

Nous ne devrions pas non plus négliger l'expiation — un acte volontaire avant que la culpabilité ne soit prouvée, offrant une voie vers un châtement plus doux. Le châtement entre en jeu lorsque l'auteur ne fait aucun pas vers l'expiation et espère échapper aux conséquences — un peu comme cette issue peut s'acheter par la corruption dans un système centralisé.

### ■ Types de délits

---

Les types d'information n'ont pas à se limiter aux actes criminels ; ils peuvent inclure : - descriptions de crimes - ruptures de contrat et fraudes - comportements immoraux - troubles à l'ordre public, réels comme virtuels - ...

Chaque nouvel enregistrement dans le réseau DID ajuste la réputation évaluée et le risque de la DID donnée (qu'il s'agisse du sujet, de l'auteur ou de l'autorité vérificatrice). Plus je porte de responsabilité pour le sort d'autrui, plus je deviens prudent.

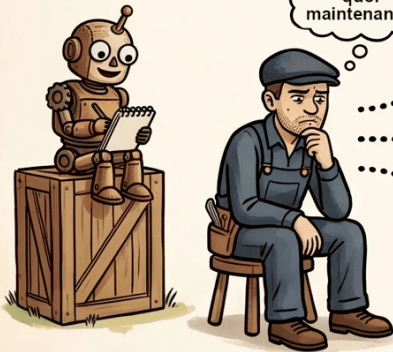
# APRÈS LE TORT — QUE FEREZ-VOUS ?

rejeté. forcé. volontaire. trois façons dont le village répond.

ce qui s'est passé



et maintenant ?



le choix rationnel est toujours le moins coûteux :  
RÉPAREZ-LE VOUS-MÊME.

« j'essaie de l'ignorer — refusé partout »



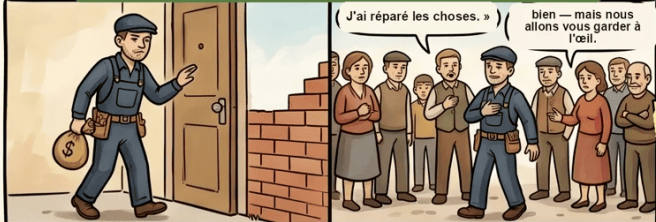
aucune réparation — chaque commerce le refuse — exil de la vie économique

« je répare — mais seulement sous le regard de la foule »



réparation forcée sous le regard de la foule — remboursé, mais le village majore son prix — la leçon doit rester gravée.

« je viens de mon propre chef — et je l'avoue à tous »



réparation volontaire et précoce — acceptée publiquement — la réputation se rétablit, avec prudence

cela ressemble au monde d'aujourd'hui. c'est le cas — sauf que les coûts sont désormais visibles de tous. pas de révolution. juste de meilleures incitations.



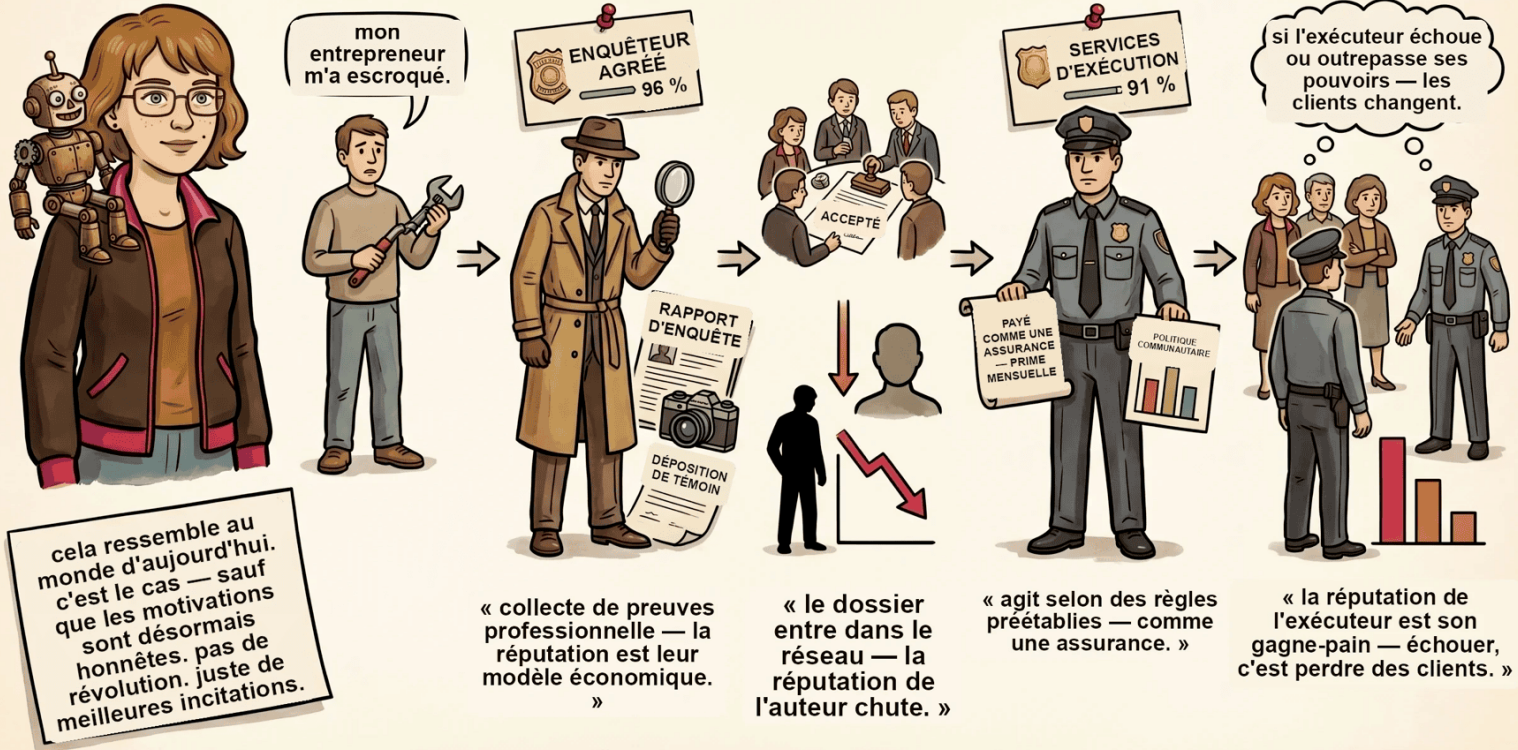
## ■ Faire respecter le châtimeut par la délégation

Je n'ai pas à faire respecter le châtimeut personnellement. Je peux payer (de façon similaire à une assurance) une autorité qui fait respecter les issues selon des règles prédéfinies — l'équivalent des services d'enquête, de maintien de l'ordre et de justice. Si l'autorité fait respecter de manière disproportionnée ou ne fait rien respecter du tout, sa réputation en souffre — et sa réputation est le fondement de sa capacité à gagner sa vie.

La délégation est un principe général dans le réseau : toute activité d'une DID peut être déléguée à une autre DID — vérification, émission d'assertions, réponse aux litiges, déclaration du consensus. La délégation est révocable à tout moment. Elle permet la spécialisation sans perte du contrôle ultime.

# QUI ENQUÊTE, QUI FAIT APPLIQUER ?

« le tort » → « l'enquêteur » « le dossier » → « l'exécuteur » → « la responsabilité »



LA DÉLÉGATION EST RÉVOCABLE. Toute activité d'un DID peut être déléguée à un autre DID — et reprise à tout moment.  
vous n'appliquez pas vous-même la punition. vous déléguez. et le délégué vous rend des comptes.

## ■ Démocratisation de la gestion des risques

Un réseau de réputation incensurable démocratiserait ce que les banques ou les mainteneurs de grands complexes industriels font déjà comme activité centrale — la gestion des risques.

Pour un banquier face à un client, l'évaluation du risque est préparée à l'avance afin qu'il puisse se concentrer sur l'interaction commerciale dans des limites prédéfinies. Les équipes de maintenance sophistiquées, à intervalles de service réguliers, collectent des indicateurs de risque (signes de fissures structurelles, processus dégradant l'infrastructure opérationnelle, etc.) et peuvent prédire la durée de vie des équipements ainsi que le moment et le type d'intervention nécessaires.

J'imagine l'usage des DID de manière similaire — quelqu'un (probablement contre rémunération) fournira un résumé lisible par un humain de la contrepartie. Le résumé reflétera l'angle d'évaluation du risque que le client aura commandé.

# LA PUNITION SANS AUTORITÉ CENTRALE



La réparation coûte moins cher que la punition.

La punition coûte moins cher que l'ignorance.



# Suivre l'argent

## Suivre la trace de l'argent

Nous disposons d'un réseau de réputation décentralisé et de la motivation à l'utiliser. Il peut déjà apporter un avantage concurrentiel à ses utilisateurs — clarifier les risques potentiels, les aider à planifier plus efficacement la sélection des contreparties et la stratégie de négociation, et inclure les mesures qui réduisent ces risques connus.

Ce qui suit est une méthodologie<sup>5</sup> possible pour l'utiliser — en tirant parti des propriétés du réseau pour construire un chemin de migration du système actuel vers son successeur évolutif. Elle porte probablement des traits caractéristiques de l'Europe centrale, où cette thèse a été conçue. Les conditions locales exigeront des ajustements locaux. Ce que je recommanderais de préserver partout, c'est le caractère sans compromis des mesures envers l'État — sans cela, l'objectif se diluera dans des discussions sans fin et le changement n'arrivera jamais. Attention — les représentants et les partisans de l'État vous occuperont avec des absurdités. Ne tombez pas dans le panneau ; c'est leur gagne-pain qui est en jeu.

---

<sup>5</sup>**Déconstruction de l'État** — dans le contexte tchèque, cela sera vraisemblablement traité en profondeur dans un livre à paraître du même nom, de l'auteur tchèque Daniel Steigerwald (prévu pour 2026). Je place personnellement de grands espoirs dans les procédures inspirantes qu'il contiendra.

## Le point faible de l'État — l'argent

Revenons au début. Nous voulons plus de libertés en résultat, plus d'influence sur leur forme, et plus de responsabilité à leur mesure. La question est simple : où l'État a-t-il un point vulnérable sur lequel nous pouvons appuyer sans recourir à la violence ?

La réponse est ennuyeuse, et n'en est que plus forte. L'argent.

Au fond, l'État est un flux d'argent. Par l'argent, il paie son appareil coercitif — le maillon final qui fait respecter ses règles. Sans argent, il n'y a pas de monopole de la violence. Dès que l'argent commence à se tarir, l'État commence à reculer — parce qu'il n'a plus rien pour payer ceux qui le maintiennent physiquement en place.

Les flux d'argent fluctuent naturellement — de façon saisonnière, économique, selon le sentiment des investisseurs. L'État masque cela par l'emprunt sur les marchés financiers. Parfois, un emprunt est rationnel : un investissement qui se rembourse. Le plus souvent, cependant, il couvre des dépenses surdimensionnées pour des agendas qui ont depuis longtemps dépassé la finalité première de l'État — défense, sécurité intérieure, justice pénale, affaires étrangères. Une fois certains seuils franchis, la banque centrale réagit par des taux d'intérêt ancrés à sa propre estimation de l'inflation.

Et voici l'impôt silencieux. L'inflation est loin de n'être qu'une préoccupation comptable de macroéconomistes. C'est un impôt caché sur le pouvoir d'achat de la monnaie, payé par tous ceux qui ont mis de côté quelques pièces pour leurs vieux jours. Une faible inflation est tolérée par le public parce qu'il n'en saisit pas les effets à long terme — il ne réalise pas que même des chiffres à un seul chiffre, composés sur un long horizon, érodent l'épargne au point que les gens ne peuvent plus assurer leurs propres vieux jours. Et quand ils ne le peuvent pas, ils sont conditionnés à la dépendance aux prestations de l'État. Au bout du compte, ils sont suspendus à ces prestations et attachés à l'État.

En période turbulente — guerre, pandémie, l'investissement « nécessaire » — l'État se contente d'allumer la planche à billets. Le pouvoir d'achat des épargnants et des travailleurs responsables baisse pendant que nous leur promettons qu'ils sont bien récompensés. Quelqu'un vole discrètement leur temps et les félicite de gagner si magnifiquement leur vie.

Cela mine sérieusement la confiance dans l'État. Et la confiance est la seule colle qui tient toute la machinerie ensemble. Voilà le levier contre lequel il vaut la peine de s'arc-bouter.

### ■ Pourquoi l'argent, et non d'autres points faibles ?

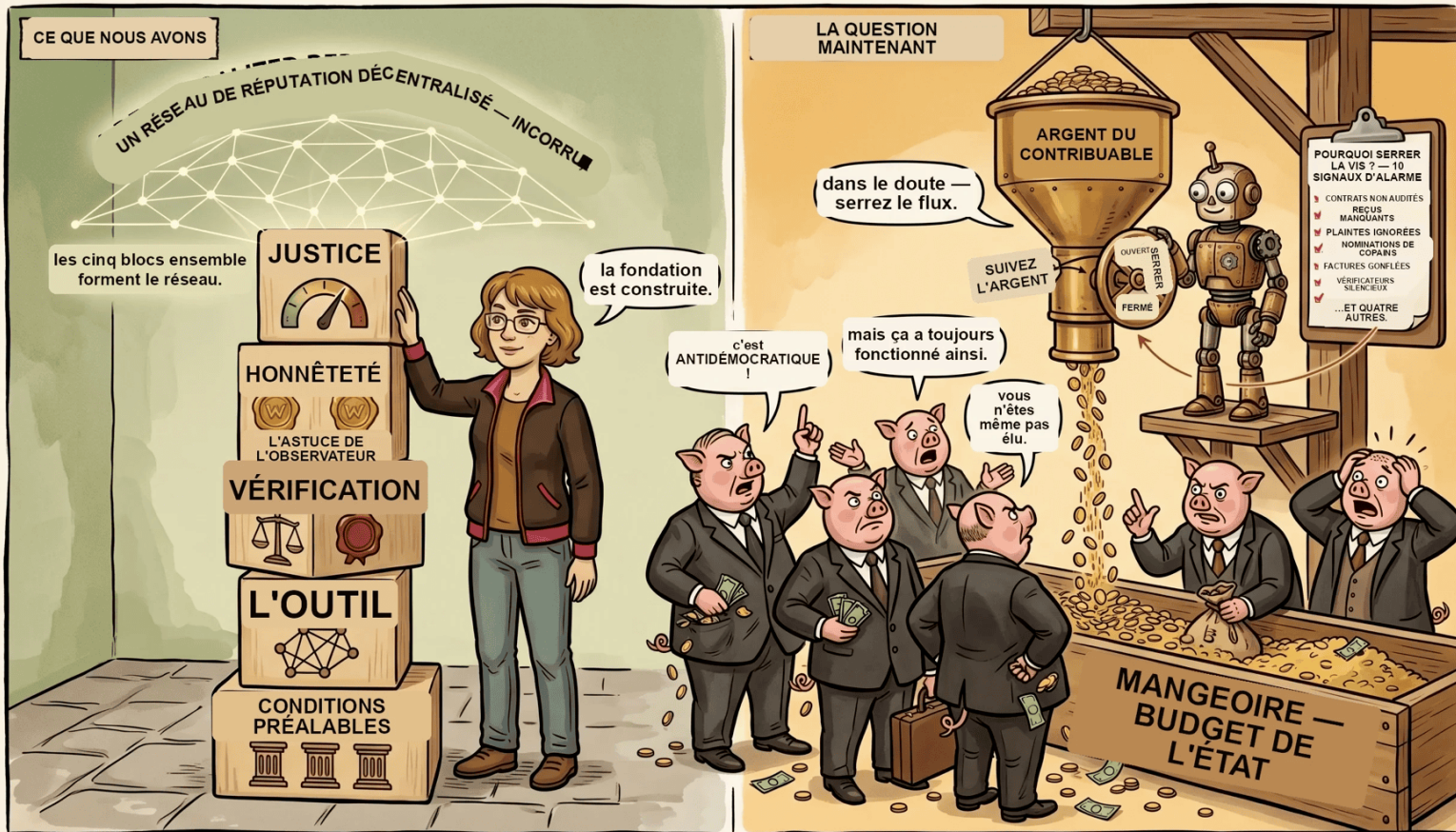
Un autre point faible de la civilisation est, par exemple, la distribution de l'énergie. Mais perturber son flux n'est pas un levier — ce serait de l'agression, du terrorisme. La non-participation volontaire n'est pas la même chose que nuire délibérément à autrui. L'argent est exceptionnel en ce que la pression peut s'exercer volontairement, de façon transparente et sans violence.

## Proposed transition to the state's successor

### Évolution, pas révolution

Un changement soudain provoque la résistance même lorsque le but final est séduisant. Il brise les liens — sociaux, économiques, politiques — et les gens défendent instinctivement ce qu'ils connaissent déjà contre ce qu'ils n'ont pas encore vu.

# SUIVEZ L'ARGENT — L'HISTOIRE JUSQU'ICI



Nous avons le réseau. Nous savons comment il fonctionne. Maintenant : dans le doute, serrez la trémie.  
le pouvoir de l'État repose sur l'argent. suivez-le.



La bonne approche est donc graduelle — évolutive. Une approche qui empêche l'ancien système d'éteindre le nouveau d'une simple pression sur un bouton — car dès qu'il le pourrait, il le ferait.

Malheureusement, cela signifie accepter que le volontariat d'équilibre ne sera pas atteint au moment où nous déploierons le réseau de réputation ; il arrivera de concert avec un rythme progressif d'adoption. L'adhésion pourra être — et sera probablement — lente, tirée par le désir des individus de trouver un recours auprès de leur communauté à travers le réseau de réputation lorsque la voie conformiste de recherche de justice échoue (et elle échouera). Voyons à quoi ressemble ce chemin, estimations proportionnelles comprises.

## ■ Auges vides — ne jouez pas selon des règles truquées pour vous faire perdre

Les tentatives de réformer l'État de l'intérieur reposent sur les mécanismes internes du pouvoir, dans l'espoir que les fonctionnaires imposeront des changements contre leurs propres incitations. Cela n'arrivera pas.

Pourquoi nourrir le système au lieu d'assécher les canaux qui lui apportent la vie ? Au lieu de changer l'ancien système et de jouer selon ses règles, bâtissons une nouvelle couche au-dessus de lui — une couche qui transforme progressivement l'ancien système en un sous-ensemble du nouveau. Au départ, ce sous-ensemble remplit presque le sur-ensemble. Avec le temps, les acteurs migrent.

Les entreprises le savent : quand un ancien système est trop enchevêtré pour être remplacé, on en bâtit un parallèle et l'on y migre progressivement les utilisateurs.

Le fait que l'État finisse avec un décalage entre ce qu'il livre réellement et ce que ses statuts exigent, et qu'il soit enclin à invoquer ce décalage, est purement un problème de ses représentants et de ses participants — inutile de s'y attarder. La seule chose qui vaille la peine d'être surveillée est celle-ci : ne pas provoquer de révolution violente.

## Quatre outils qui se soutiennent mutuellement

Jusqu'ici, le réseau de réputation DID a pu sembler utile surtout pour la justice et le consensus. Je crois qu'il pourrait se stabiliser et résister aux attaques — méritocratiquement, sur la base du mérite réel plutôt

que de titres formels. Mais la réputation seule ne forcera pas l'État à céder du terrain. L'économie le fera, et la pression exercée à travers elle.

Rien ne nous empêche d'utiliser les identités DID comme gestionnaires d'outils supplémentaires qui appuient fort sur l'argent. Ne commencez pas par un plein volontariat de la part des citoyens — fixez une direction que l'État ne peut arrêter. La transition repose sur quatre outils spécifiques qui se soutiennent mutuellement. Aucun d'eux ne suffit à lui seul.

## **Système fiscal simple — l'appât d'entrée**

Le premier outil est un système fiscal simple et transparent, bâti sur l'infrastructure DID. Un taux unique proportionnel sur tous les revenus. Aucune exception, aucune exonération temporaire, aucune déduction pour les entreprises, aucune incitation. Chaque paiement est auditablement relié à la DID qui l'a versé. Le recoupement est trivial.

Le taux serait fixé un peu plus favorablement que dans l'ancien système pour une partie des contribuables — c'est l'appât d'entrée. La charge fiscale déclinerait d'année en année, le système deviendrait de plus en plus attractif, et la migration prendrait de la vitesse. Le système est à la fois le teneur de registre et le collecteur — pas d'intermédiaire, pas d'opacité.

## **Registre électronique des dépenses (ESR)**

Le deuxième outil consiste à retourner l'EET (enregistrement électronique des recettes) comme un gant. Au lieu que l'État suive chaque reçu d'un indépendant, nous suivons chacune des dépenses de l'État. L'État ne reçoit pas de fonds du système fiscal simple pour un paiement individuel donné, à moins que chacun — sans exception — ne passe par ce tamis.

L'ESR est un proxy<sup>6</sup> qui met en correspondance chaque dépense réalisée de l'État et du secteur public avec un enregistrement du paiement planifié — incluant une justification contextuelle et l'identification du destinataire, de l'entité dépensière et de la finalité. Le résultat est une donnée publique brute, hiérarchisable. N'importe qui peut la prendre et l'analyser. N'importe qui peut proposer aux contribuables des recommandations sur ce qu'il faut en faire. Ce que les cours des comptes n'ont pas pu obtenir en des années est soudain à un clic pour tout le monde.

Vous n'êtes pas obligé de passer au nouveau système fiscal pour y participer. Il suffit de payer une caution entièrement remboursable (disons 1 à 3 EUR) par paiement réalisé. Le reliquat non réalisé est confisqué en guise de filtre anti-spam, afin que le système ne soit pas inondé par des attaques. Un enregistrement peut être soumis par n'importe qui — un proche pour un grand-parent incapable, un voisin pour des services publics négligés, un entrepreneur pour une facture impayée, un fonctionnaire par export depuis son propre système.

Je m'attends à ce que les partis politiques se transforment naturellement en fournisseurs d'analyses, ou que de nouveaux émergent pour remplacer les anciens. Au lieu de contributions puisées dans les impôts, ils commenceront à offrir de l'expertise — fournissant à leurs partisans des aperçus fondés sur les valeurs des autorités alliées, de leurs services et de leurs politiques de vérification. Les enregistrements bâclés ou dénués de sens par paresse deviennent automatiquement des candidats aux coupes budgétaires. Au premier tour, votre paiement sera toujours décaissé, mais les données collectées servent de base pour évaluer si une dépense de l'État a encore du sens. Les prestataires et autres bénéficiaires de la masse salariale de l'État ont une incitation à s'assurer que les fonctionnaires appariant les dépenses de manière responsable. Sinon, l'argent ne coulera pas au tour suivant.

---

<sup>6</sup>**Proxy** (latin *procurator*, anglais *deputy/intermediary*) — ici, un intermédiaire agissant au nom d'une autre entité. Le proxy ESR accepte les enregistrements de paiements planifiés de la part de quiconque, les met en correspondance avec les dépenses réalisées de l'État, et met le jeu de données obtenu à la disposition du public.



## D'où vient l'acronyme ESR

Entre 2016 et 2022, le gouvernement tchèque a mis en œuvre un système appelé Enregistrement électronique des recettes (EET) contre ses propres citoyens — indépendants et entrepreneurs. Le message était simple : « Nous supposons que chacun de vous fraude l'État. Vous enregistrez chaque transaction, la transmettez en temps réel à nos serveurs, et nous vous surveillerons. Nous récompenserons financièrement vos concitoyens qui vous dénoncent si vous tentez d'échapper à l'EET. »

L'EET était calqué sur des précédents balkaniques. Le premier pays au monde à lancer un système national obligatoire d'enregistrement en ligne des ventes en temps réel, en 2013, fut la Croatie, sous le nom de *fiskalizacija*. La République tchèque a adopté le modèle quelques années plus tard et a fait tourner l'un des régimes de traçage des recettes les plus stricts d'Europe.

Si le côté obscur n'hésite pas, pourquoi le devrions-nous ? L'ESR est la même logique retournée à l'envers : l'État se justifie auprès des citoyens.

## **Allocation citoyenne de l'impôt — le poids de la décision**

Le troisième outil donne aux contribuables une influence directe sur la destination de leur argent. Au premier tour, l'État recevait son argent quelles que soient les révélations de l'ESR. Au deuxième tour, ce n'est plus le cas — l'analyse du premier tour, et les mesures qui en découlent, prennent le relais. Un petit pourcentage de l'impôt payé peut être alloué par le payeur lui-même — à condition que sa DID satisfasse

# ESR — DÉCLARATION ÉLECTRONIQUE DES DÉPENSES

chaque dépense de l'État enregistrée — chaque enregistrement public — chaque détail ouvert à l'examen.

qui soumet  
tout  
enregistrement  
peut être soumis  
par : — le  
fonctionnaire qui a  
traité le paiement —  
le bénéficiaire qui  
a été payé

ouvert à quiconque  
veut regarder.

## REGISTRE PUBLIC DES DÉPENSES DE L'ÉTAT — dossier ouvert

catégorie : conseil juridique  
prestataire : cabinet d'avocats **PAYÉ**  
s.r.o. montant : 14 M EUR engagé :  
14-01-2026 payé : 19-01-2026

contexte : avis externe sur le nouveau projet  
de loi de réforme des marchés publics — trois  
versions produites, un atelier avec le  
ministère, aucune audience publique tenue —  
version finale livrée après le délai législatif.

catégorie : conseil en conception routière  
prestataire : Cabinet-conseil T **PAYÉ**  
montant :  
9 M EUR engagé : 03-02-2026 payé : —  
contexte : étude de faisabilité pour l'extension de  
l'autoroute D-X — le même cabinet a rédigé trois  
études précédentes sur ce tracé — résultat :  
recommandation de poursuivre à +18 % par rapport à  
l'estimation précédente.

catégorie : délivrance de plaques  
d'immatriculation bénéficiaire : **PAYÉ**  
régional Z montant : 45 EUR par plaque  
engagé : 19-02-2026 payé : 19-02-2026  
contexte : frais administratifs standards par  
plaque délivrée — les frais couvrent les  
matériaux et le traitement — volume total 12 400  
plaques ce trimestre.

catégorie : équipement hospitalier  
prestataire : MedSupply a.s. **PAYÉ**  
montant :  
8,2 M EUR engagé : 08-03-2026 payé : —  
contexte : installation d'un scanner IRM à l'hôpital  
régional — appel d'offres public, trois  
soumissionnaires — offre retenue 2 % sous la  
médiane, livraison sous 60 jours — facture en retard  
de 90 jours.

filtre anti-spam — dépôt remboursable



les partis se transforment en fournisseurs d'analyse



Chaque couronne d'argent public — enregistrée, publique, vérifiable.

la valeur n'est pas de prendre les tricheurs sur le fait — elle est d'ouvrir les comptes.

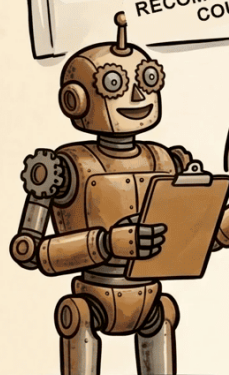
aux exigences réputationnelles (citoyenneté, résidence, majorité/capacité reconnue par la communauté). Le pourcentage allouable croît d'année en année. Potentiellement de façon exponentielle. De cinq pour cent aujourd'hui à des dizaines de pour cent en une décennie.

Les données brutes de l'ESR guident naturellement les décisions des contribuables. Les enregistrements de faible qualité fonctionnent comme un signal d'alerte pour des coupes recommandées. Quiconque peut créer des enregistrements ; les fonctionnaires doivent les apparier. Sans cela, le système fiscal n'enverra aucun argent à l'État — ni dans le Trésor, ni dans d'autres chapitres budgétaires. La bataille politique se déplace de l'urne à l'allocation quotidienne de pièces concrètes.



# AFFECTATION CITOYENNE DE L'IMPÔT — VOUS DÉCIDEZ OÙ VONT VOS IMPÔTS

étudiez les dossiers ESR. puis déplacez les curseurs.

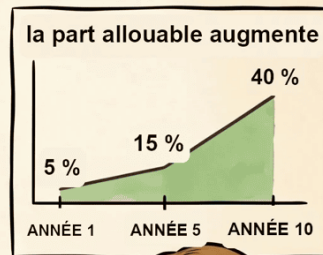
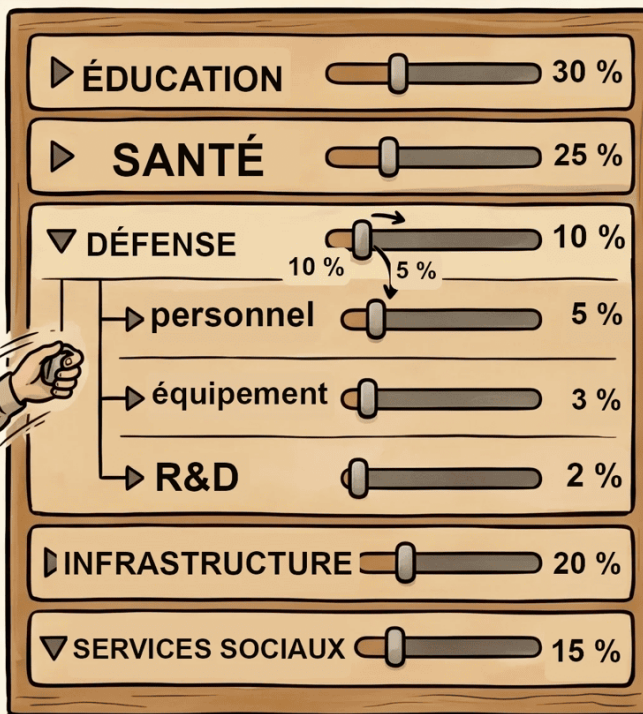


ou délégez ceci

vous ne voulez pas allouer vous-même ? délégez à : — l'analyste de votre parti — un voisin de confiance — quiconque vous choisissez — et révoquez à tout moment.



après lecture du rapport — défense en baisse.



cliquez sur n'importe quelle ligne pour approfondir — allouez à n'importe quel niveau.



cela ressemble au monde d'aujourd'hui. c'est le cas — sauf que le curseur est désormais entre vos mains. pas de révolution. juste de meilleures incitations.

De 5 % aujourd'hui à 40 % en une décennie. Vous décidez.  
les dossiers sont ouverts. l'analyse est la vôtre. le curseur aussi.



## **Plateforme de négociation avec l'État — le levier**

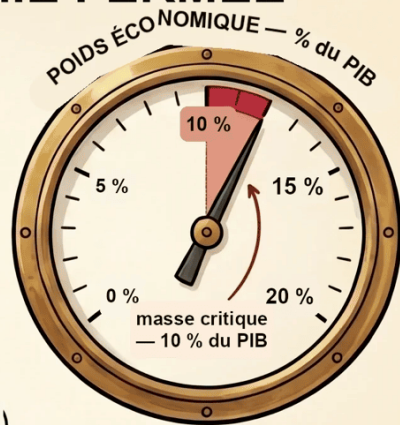
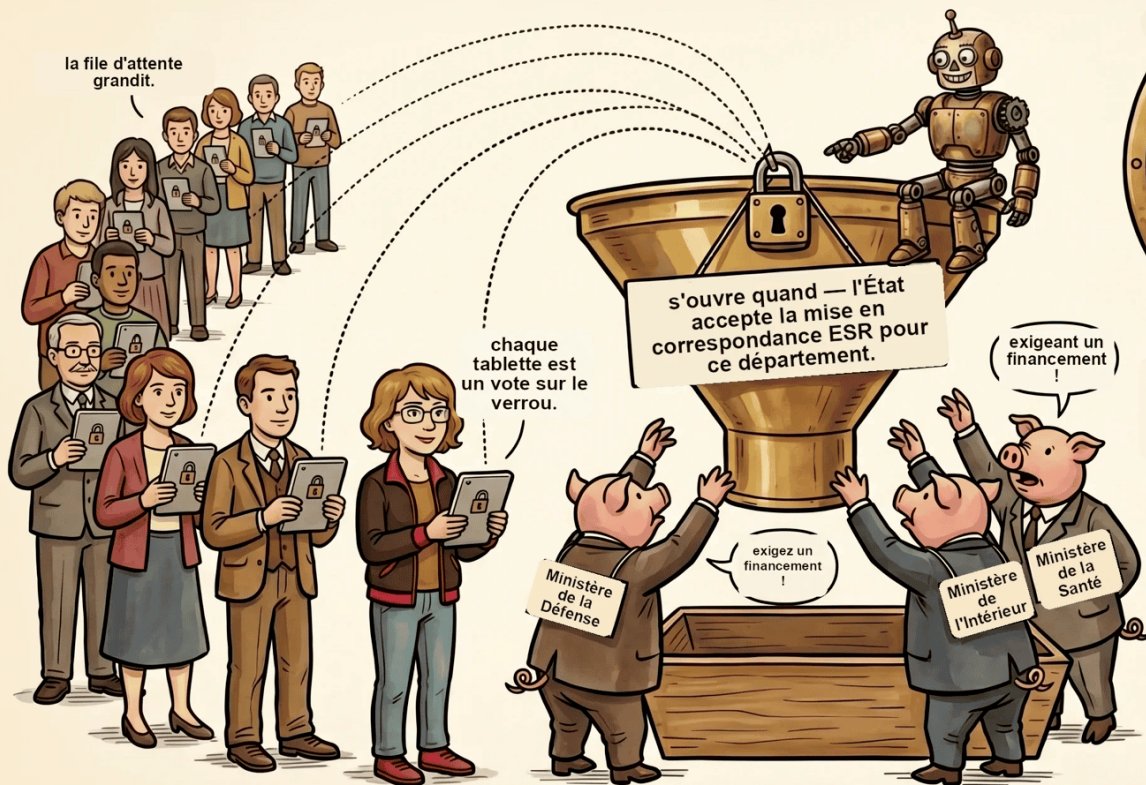
Le quatrième outil est le levier qui relie tout le reste et ne fait que maintenant du réseau une véritable menace. Le principal conflit portera sur la question de savoir si l'État accepte l'ESR comme norme contraignante — d'abord au niveau national — et sur l'ampleur que doivent atteindre les menaces des participants au réseau de réputation avant que cela ne se produise.

Le levier est le financement de l'État en juste-à-temps, conditionné à ce que les paiements soient appariés à l'ESR. L'argent ne coule qu'au moment où l'État a satisfait aux conditions de transparence. Une liste d'attente de participants se forme à l'intérieur du réseau de réputation. L'activation s'enclenche lorsque le groupe atteint une taille économiquement significative — suffisamment grande pour menacer la croissance du PIB. À ce moment, la désobéissance civile devient une menace crédible plutôt qu'un geste.

L'État s'accrochera le plus longtemps aux paiements problématiques liés à la corruption. Sous la pression, il cédera d'abord du terrain là où il a une défense facile et où il n'y a pas de marge pour chercher des économies. Une pression graduelle et croissante le forcera à reculer, pas à pas, de chaque position.

# PLATEFORME DE NÉGOCIATION — LA TRÉMIE FERMÉE

les citoyens détiennent la clé. l'État s'ouvre quand les conditions sont remplies.



une petite fraction du PIB suffit — à la masse critique, la rétention devient une menace réelle.

après la masse critique —

l'État ouvre d'abord ses comptes pour les paiements simples et justifiables.

les catégories liées à la corruption restent verrouillées le plus longtemps.

chaque déverrouillage exige plus de pression — et est lui-même enregistré.

cela ressemble au monde d'aujourd'hui. c'est le cas — sauf que la clé est désormais entre de nombreuses mains. pas de révolution. juste de meilleures incitations.

L'argent circule quand il y a de la transparence. Les citoyens détiennent la clé.

pas de force. pas de révolution. juste assez de tablettes pour rendre la rétention crédible.

## La citoyenneté sans carte d'identité

Avec la transition vers l'infrastructure DID, la carte d'identité émise par l'État perd sa finalité monopolistique. Vous n'avez pas besoin d'une carte d'identité — vous disposez d'un éventail d'identités DID, et certaines d'entre elles portent une assertion selon laquelle vous êtes, par exemple, tchèque, résident d'une commune particulière, diplômé d'une école particulière. L'assertion est vérifiable, permanente et indépendante de l'administration de l'État.

Une question de mise en œuvre technique s'ouvre : qui, sur le marché, se chargera de vérifier les citoyens existants en dehors du contrôle de l'État, afin de migrer les parties intéressées vers une DID portant l'assertion appropriée ? Le plus probablement, des autorités du marché libre spécialisées dans la vérification d'identité émergeront — notaires, communautés locales, employeurs. Elles engagent leur réputation sur le fait qu'une DID donnée appartient véritablement à la personne qui le prétend. La citoyenneté — c'est-à-dire l'appartenance à une vision particulière de la communauté — est libérée du besoin d'une tenue de registre centrale. Par la mise en relation à travers le réseau de réputation, les données intégrées sont connectées et validées une deuxième fois, une troisième, une quatrième, et ainsi de suite.

La conséquence est intuitive, mais insoluble dans un système centralisé. Aujourd'hui, un leadership politique — dans l'optique d'une réélection facilitée — peut importer des problèmes concentrés sur le territoire de la communauté : accepter des migrants d'autres cercles civilisationnels sans égard à la capacité d'absorption ni à la volonté de la communauté existante, altérant les communautés d'origine par une pression sous laquelle elles ne peuvent pas suivre le rythme d'assimilation des arrivants d'autres cercles civilisationnels. Dans un réseau DID, un migrant admis de manière corrompue ne peut pas être certain que la communauté continuera de le considérer comme l'un des siens. Les membres de la communauté n'ont objectivement pas à supporter qu'un étranger vienne frapper à leur porte, revêtu de l'uniforme de la

# QUATRE OUTILS DE TRANSITION ÉVOLUTIVE

le système reconstruit de l'intérieur — sans le briser.

## IMPÔT SIMPLE



un seul taux. pas de dérogation. vérifiable de façon croisée.

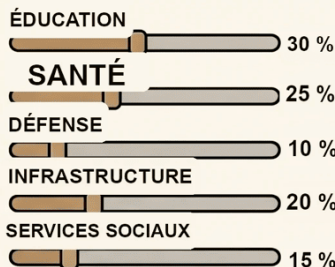
## ESR — DÉCLARATION ÉLECTRONIQUE DES DÉPENSES



chaque dépense enregistrée — chaque enregistrement public — chaque détail ouvert.

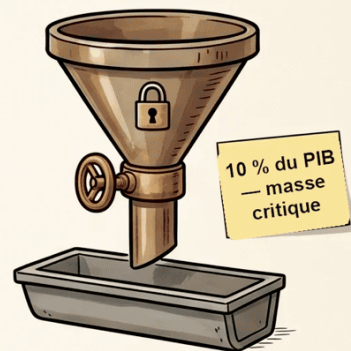
## AFFECTATION CITOYENNE DE L'IMPÔT

5 % → 15 % → 40 %  
ANNÉE 1 → ANNÉE 5 → ANNÉE 10



étudiez les dossiers — puis déplacez les curseurs.

## PLATEFORME DE NÉGOCIATION



l'argent circule uniquement quand les conditions de transparence sont remplies.

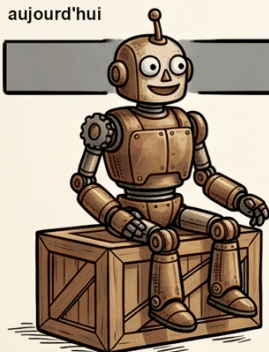
aujourd'hui

évolution en cours

dans une décennie

95 %

en expansion



## Évolution, pas révolution.

quatre outils qui changent le système de l'intérieur.

cela ressemble au monde d'aujourd'hui. c'est le cas — sauf que les outils sont désormais entre les mains des citoyens. pas de révolution. juste de meilleures incitations.





communauté, et les menace de la légalité des mesures qu'il compte exécuter dans la maison (confiscation du téléphone d'un enfant à cause d'une publication sur les réseaux sociaux). Avec une réputation décentralisée, la majorité de la société n'a pas à s'y résigner — car l'appartenance à une communauté n'est pas décidée par un fonctionnaire, mais par la communauté elle-même, à travers ses signaux de réputation.

# CITOYENNETÉ SANS CARTE D'IDENTITÉ

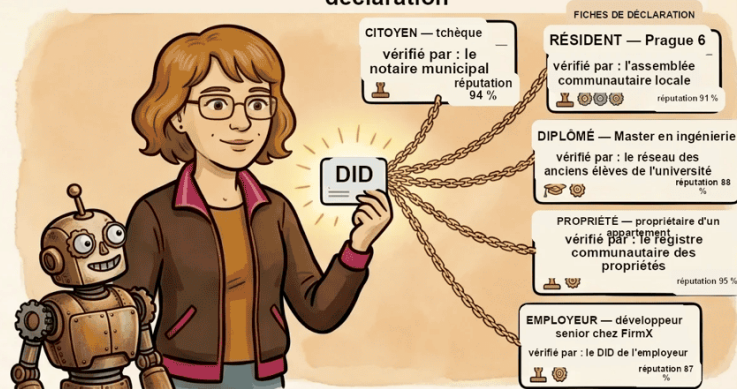
d'un permis d'État à la reconnaissance communautaire.

« l'ancienne façon » : modèle d'identité institutionnelle délivrée par l'État



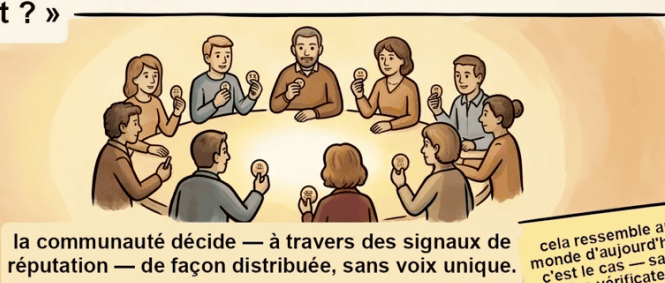
identité = permission de l'État — révocable — la communauté n'a pas voix au chapitre.

« la nouvelle façon » : modèle de DID avec fiches de déclaration



aucune autorité unique ne contrôle toutes les déclarations — chacune est indépendante — chaque vérificateur engage sa réputation.

« qui appartient ? »



la communauté décide — à travers des signaux de réputation — de façon distribuée, sans voix unique.

cela ressemble au monde d'aujourd'hui. c'est le cas — sauf que les vérificateurs sont désormais nombreux. pas de révolution. juste de meilleures incitations.

**Votre citoyenneté n'est pas un permis gouvernemental. C'est la reconnaissance de votre communauté.**

le tampon de l'État est remplacé par une chaîne de vérificateurs indépendants — chacun avec un intérêt personnel en jeu.

Le poids d'une voix électorale sur les matières relevant de l'État pourrait, à l'avenir, être strictement corrélé aux enregistrements de contributions au système fiscal simple. Combiné à des assertions DID appropriées (par exemple « cette personne est un citoyen tchèque »), les ressortissants étrangers peuvent alors être exclus des élections — le registre de population se déplace simplement ici.

## Chevauchement et réversibilité

Je ne prétends pas que ce soit le seul chemin, ni même le meilleur. Mais il paraît complet — il couvre les principaux leviers et préserve la possibilité de faire marche arrière. Au départ, le nouveau système chevauche l'ancien et ne change que les incitations. Avec le temps, l'ancien système rétrécit jusqu'à ce qu'il puisse — mais sans nécessité — se dissoudre. L'avantage est le gradualisme et la réversibilité : si une erreur apparaît dans la conception, ce n'est pas la fin, juste une correction.

### Paix et guerre

Certaines parties de l'État peuvent ne pas avoir d'alternative pleinement fondée sur le marché — peut-être l'armée. La délégation temporaire de pouvoirs extraordinaires en temps de crise (comme les anciens Grecs nommaient des dictateurs) pourrait continuer d'exister. La responsabilité, cependant, repose sur la société décentralisée, non sur le chef. Contrairement à la gouvernance centralisée, il sera plus facile de reprendre les pouvoirs délégués une fois la menace passée — ou plus tôt, si nécessaire. Une société libre ne sera pas désavantagée, même dans le choc des armes contre des régimes autoritaires.

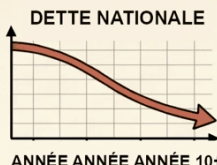
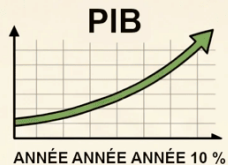
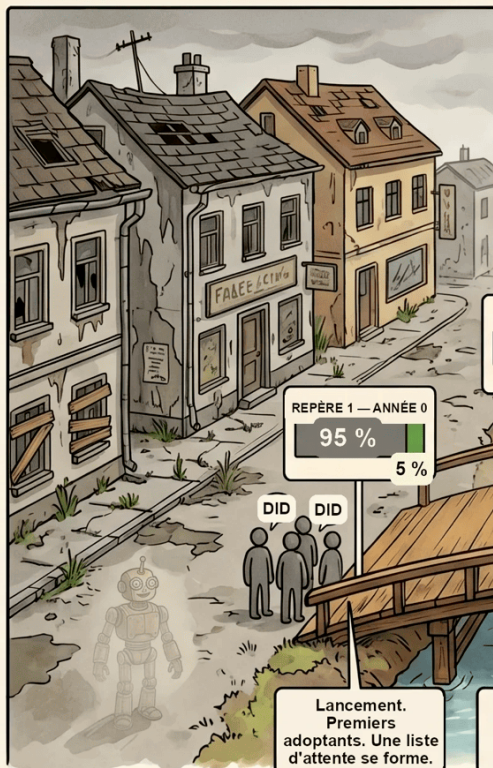
## ■ Criminels de guerre

---

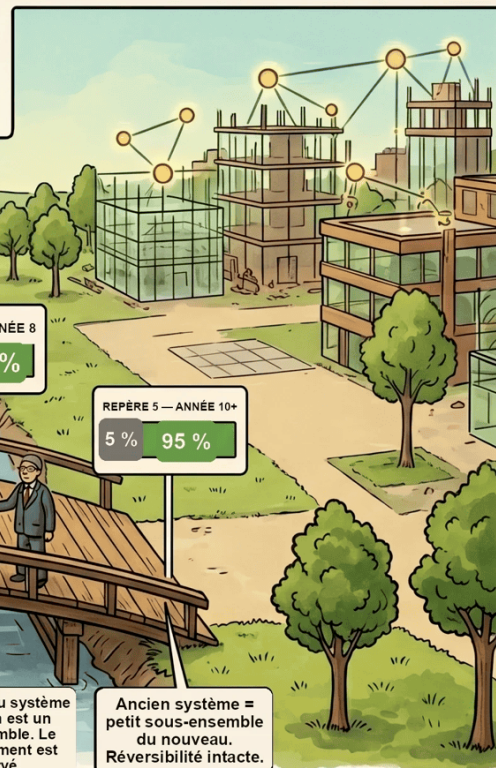
Avec un financement de l'État en juste-à-temps et des dépenses transparentes, il devient difficile d'accumuler des ressources pour des guerres d'agression. Un contribuable qui continue de financer une telle guerre devient une cible légitime et ne peut pas invoquer le statut de civil au titre des Conventions de Genève. Sous le nouvel agencement, le consentement silencieux est pris pour une participation.



## RIVE GAUCHE — « L'ANCIEN SYSTÈME »



## RIVE DROITE — « LE NOUVEAU SYSTÈME »



REPÈRE 1 — ANNÉE 0  
95 %  
5 %

REPÈRE 2 — ANNÉE 2  
80 %  
20 %

REPÈRE 3 — ANNÉE 5  
50 % 50 %

REPÈRE 4 — ANNÉE 8  
25 % 75 %

REPÈRE 5 — ANNÉE 10+  
5 % 95 %

**MASSE CRITIQUE — L'ÉTAT ACCEPTE L'ESR SOUS PRESSION ÉCONOMIQUE.**

MARCHE ARRIÈRE

Lancement. Premiers adoptants. Une liste d'attente se forme.

Croissance. La liste des participants gonfle.

Erreur de conception ? On peut revenir en arrière. La réversibilité est préservée.

75 % nouveau système — l'État en est un sous-ensemble. Le chevauchement est préservé.

Ancien système = petit sous-ensemble du nouveau. Réversibilité intacte.

**ANCIEN SYSTÈME**

> Transition graduelle. Réversibilité en cas d'erreur. Une direction qu'on ne peut pas arrêter.

# Conclusion

## Le chemin existe

L'État est tel qu'il est à cause des technologies disponibles à l'époque de sa création, combinées à la nature humaine. Tout bâtir sur le volontariat en niant la nature humaine moyenne est naïf. Il ne se débarrassera ni de la corruption, ni de sa tendance à dériver vers le totalitarisme. Le successeur de l'État doit fonctionner même avec les traits que nous considérons actuellement comme négatifs, et soit les ostraciser, soit les punir.

Ce livre a décrit un problème — un système (l'État) où les gens qui écrivent les règles n'en vivent jamais les conséquences. Il a décrit les conditions qui doivent tenir pour que ce système cesse de fonctionner. Il a décrit un outil qui satisfait ces conditions. Et il a proposé une méthodologie de transition — des étapes concrètes pour utiliser cet outil, comme un exemple possible.

Dans le premier chapitre, j'ai nommé cinq piliers : le volontariat, l'organisation, la résilience, le consensus et l'incorruptibilité. Nous les avons tous satisfaits.

- **Volontariat** — personne ne vous force à entrer dans le réseau, mais vous ne pouvez pas non plus en effacer vos actes.
- **Organisation** — la communauté naît de qui vous connaissez, non de qui l'on vous a assigné d'en haut.
- **Résilience** — pas même un État prêt à payer pour surveiller chaque paquet ne peut l'éteindre.
- **Consensus** — il naît de l'étiquette de prix apposée sur l'hypocrisie, non de votes ou de signatures.

- **Incorruptibilité** — cinq petites règles tissent la corruption en coûts : l'équilibre du volontariat et de la responsabilité, le droit de chacun à parler, des points d'entrée que personne ne choisit, des promesses publiques avec un prix pour l'hypocrisie, et l'ombre d'un observateur derrière chaque transaction.

Aucun pilier ne peut remplacer l'État à lui seul. Ensemble, ils forment une résistance à la corruption que l'État, avec tout son appareil, ne peut opposer.

Nous en sommes à un point où l'ensemble peut être bâti avec les technologies actuelles (cryptographie, identité décentralisée, schémas psychologiques bien connus pour ajuster correctement les incitations, ...). Une seule chose manque : une masse critique de personnes qui trouvent le courage de le soutenir et décident de commencer.

Pas par la révolution.

Ces idées ont pris forme entre juin 2025 et mai 2026. Au moment de m'asseoir pour écrire, j'avais le cadre largement élaboré dans ma tête — c'est précisément pourquoi j'ai lu [Farewell To Westphalia](#) avec tant de curiosité lorsqu'il est paru. Je voulais voir où leur image recouperait la mienne et où elle divergerait. Une seconde impulsion est venue de Dan Steigerwald, qui, en mai 2026, travaille encore sur son propre livre *Déconstruction de l'État* sous un autre angle ; son projet m'a poussé à coucher ma propre vision dans toute son ampleur — afin que le monde l'ait sur la table aux côtés des autres.

Je ne vous demande de croire rien de tout cela. Je vous demande d'y réfléchir. Et je vous laisse avec une question :

*Que changeriez-vous ?*

## Remerciements

### Inspiration

Je remercie les auteurs de [Farewell to Westphalia](#) (Jarrad Hope, Peter Ludlow) pour le cadre intellectuel qui m'a aidé à replacer mes propres idées dans le contexte plus large de la déconstruction du modèle westphalien de l'État.

### Relecture et retours

### Outils

Pour préparer le texte, structurer les idées et itérer sur les formulations, j'ai eu recours à l'assistance d'outils d'IA. Toutes les idées, tous les arguments et toutes les conclusions sont les miens — l'IA a servi d'outil de raffinement, non de coauteur du contenu.

Les infographies ont été conçues en collaboration avec des outils génératifs, sur la base des spécifications de l'auteur.



# REPRENEZ VOTRE TEMPS

les citoyens chassent les parasites de la vie publique.



Défendez le temps qu'ils voudraient voler. ce qui a été pris par tromperie est repris de force.

# Soutenir le projet

*Personix est financé par des lecteurs comme vous.*



**Bitcoin on-chain**

bc1q7cctdz6r026dgy06ul94eygg49ujtxnrq5czaj



**Bitcoin Lightning**

LNURL1DP68GURN8GHJ7AMPD3KX2AR0VEEKZ  
AR0WD5XJTNRDAKJ7TNHV4KXCCTTDEHHWM30  
D3H82UNVWQHXMNP0FA8JMPVD5XJMN9XUE  
RX55QRQK

## ■ Où va cet argent — et où il ne va pas

Les codes QR sont les **canaux personnels de l'auteur** — les contributions vont directement à Pavel Kudrna et financent la poursuite de l'écriture, l'expérience/simulation sociale et la communication.

Les *seuls* canaux légitimes de collecte de fonds pour ce projet sont :

- **Les éditions de ce livre autorisées par l'auteur** — codes QR figurant dans les exemplaires autorisés par l'auteur.
- **personix.org** ou son miroir Tor onion qui y est lié — où la *Fondation Personix* collecte pour les activités qui y sont décrites. Les fonds de la Fondation sont tenus séparés des fonds personnels de l'auteur.

**Tout ce qui est annoncé ailleurs** — adresses substituées dans des réimpressions, domaines sosies, « collectes pour Personix » sur les réseaux sociaux, cagnottes non rattachées à l'un des canaux ci-dessus — **est très probablement une fraude**. Nous évitons délibérément le marché des cryptomonnaies et ses participants.

# Glossaire

## Glossaire

| Terme            | Français  | Signification                                                                                                                                                                                                                                                                                            |
|------------------|-----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Authority</b> | Autorité  | Une entité de confiance (personne, organisation) qui vérifie des informations et engage sa réputation dessus. Peut être spécialisée (enquête, juridique, technique).                                                                                                                                     |
| <b>Claim</b>     | Assertion | En général : toute déclaration vérifiable. Ici : un enregistrement publié dans le réseau de réputation — une affirmation sur un événement, une propriété ou une relation, signée cryptographiquement et vérifiée. Par ex. « je suis résident de la commune X » ou « cette personne a rompu un contrat ». |

| Terme                       | Français                     | Signification                                                                                                                                                                                                                                                              |
|-----------------------------|------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Compartmentalization</b> | Cloisonnement                | En général : séparer l'information en unités isolées, de sorte qu'exposer une unité ne compromette pas les autres. Un principe connu des services de renseignement. Ici : les identités DID parallèles dans les dictatures — en compromettre une ne révèle pas les autres. |
| <b>Consistent Hash Ring</b> | Anneau de hachage cohérent   | Un mécanisme algorithmique de sélection des vérificateurs — une position sur l'anneau est déterminée par le hash du document DID au sein du graphe social. Assure une sélection non déterministe mais vérifiable.                                                          |
| <b>DID</b>                  | DID (identité décentralisée) | Une identité numérique que vous créez et contrôlez vous-même, sans autorité centrale. Signée cryptographiquement avec votre clé privée — personne ne peut la révoquer ni la falsifier.                                                                                     |



| Terme                                | Français                          | Signification                                                                                                                                                                                                                                                                                                                                  |
|--------------------------------------|-----------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>DID Document</b>                  | Document DID                      | Un fichier de données accessible publiquement décrivant votre identité DID — il contient des clés publiques, des adresses réseau et des métadonnées. Utilisé pour vérifier votre identité dans le réseau.                                                                                                                                      |
| <b>Due Diligence</b>                 | Diligence raisonnable             | En général : la vérification approfondie d'une contrepartie avant d'entrer dans une relation commerciale ou juridique — examen de son historique, de ses finances, de sa réputation et de ses risques. Ici : dans le réseau de réputation, elle se fait plus vite et plus automatiquement grâce à la disponibilité d'enregistrements vérifiés. |
| <b>Economic Neutrality Principle</b> | Principe de neutralité économique | Le comportement honnête dans le réseau est économiquement proche de zéro — les coûts de publication sont restitués sous forme de récompenses de vérification. Le comportement malhonnête est une perte nette.                                                                                                                                  |

| Terme                           | Français                           | Signification                                                                                                                                                                                                                     |
|---------------------------------|------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Emergent</b>                 | Émergent                           | Surgissant spontanément des interactions de parties plus simples, sans que personne le conçoive ou le dirige. Une nuée d'oiseaux vole en formation sans plan — la formation émerge de règles simples suivies par chaque individu. |
| <b>Emergent Social Contract</b> | Contrat social émergent            | Des règles de comportement qui naissent non pas d'en haut (la loi) mais d'en bas — d'interactions répétées et d'un consensus au sein d'une communauté.                                                                            |
| <b>ESR</b>                      | Registre électronique des dépenses | Un système proposé pour le suivi transparent des dépenses publiques — chaque dépense réalisée de l'État est mise en correspondance avec un paiement planifié. Inspiré de l'EET tchèque, mais retourné contre l'État.              |

| Terme                       | Français                     | Signification                                                                                                                                                                                                                                                                                                                                                                                                |
|-----------------------------|------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Hash</b>                 | Hash (empreinte)             | En général : une fonction mathématique à sens unique qui produit une « empreinte » unique de longueur fixe à partir de n'importe quelle entrée — comme l'empreinte digitale du document. La même entrée produit toujours la même sortie, mais l'entrée ne peut pas être dérivée de la sortie. Ici : utilisé pour déterminer une position sur l'anneau de hachage et pour vérifier l'intégrité d'un document. |
| <b>Just-in-Time Funding</b> | Financement en juste-à-temps | Un financement de l'État conditionné à la transparence — l'argent ne coule que lorsque l'État accepte l'ESR et apparie ses dépenses. Un levier pour contraindre à la coopération.                                                                                                                                                                                                                            |

| Terme                | Français                | Signification                                                                                                                                                                                                                                                                                                                                              |
|----------------------|-------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Meritocracy</b>   | Méritocratie            | En général : un système où le rang est déterminé par le mérite réel et la capacité prouvée, non par des titres formels, des relations ou un privilège hérité. Ici : le réseau de réputation favorise naturellement ceux qui contribuent de façon démontrable à la communauté — leur voix pèse davantage grâce à leur historique, non grâce à une fonction. |
| <b>Onion Gateway</b> | Passerelle onion        | L'adresse réseau d'une identité DID sur le réseau onion. Distincte du document DID — elle peut être changée sans perdre l'identité (comme changer l'adresse IP derrière un nom de domaine).                                                                                                                                                                |
| <b>Onion Routing</b> | Routage en oignon (Tor) | Un protocole de communication qui assure l'incensurabilité du réseau. Les messages sont chiffrés en couches — chaque nœud retire une couche mais ne connaît pas le chemin complet.                                                                                                                                                                         |



| Terme                   | Français             | Signification                                                                                                                                                                                                                                                                                                                                                                      |
|-------------------------|----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Oracle Problem</b>   | Problème de l'oracle | En général : comment s'assurer que les données entrant dans un système numérique correspondent fidèlement à ce qui s'est réellement passé dans le monde physique. Le terme provient du domaine de la chaîne de blocs. Ici : résolu par des autorités qui engagent leur réputation en garantie qu'un enregistrement numérique correspond à la réalité physique.                     |
| <b>Phenomenological</b> | Phénoménologique     | En général : une approche qui étudie les phénomènes tels qu'ils se manifestent dans l'expérience directe, en observant ce qui en découle, sans théories préétablies. Ici : la liberté, le contrat social et les normes de comportement sont des phénomènes observés — des conséquences de milliers de micro-interactions entre les personnes, non des principes définis d'en haut. |

| Terme         | Français           | Signification                                                                                                                                                                                                                                                                                                                                                    |
|---------------|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Policy</b> | Politique (policy) | En général : un ensemble de règles ou de principes régissant le comportement dans un contexte donné. Ici : chaque participant du réseau DID déclare sa politique — comment il réagit à des comportements spécifiques des autres, quelles règles il suit, et quelles sanctions il juge proportionnées. L'agrégat des politiques forme le contrat social émergent. |
| <b>Proxy</b>  | Proxy              | En général : un substitut ou un intermédiaire — un système ou une entité agissant au nom d'un autre. Utilisé ici dans deux contextes : (1) l'ESR comme proxy appariant les dépenses publiques avec les paiements planifiés ; (2) les observateurs comme proxy entre l'émetteur et le vérificateur dans l'astuce de l'observateur.                                |

| Terme                                        | Français                          | Signification                                                                                                                                                                                                          |
|----------------------------------------------|-----------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Publisher</b>                             | Émetteur                          | Un participant du réseau qui crée et publie un enregistrement (une assertion sur une injustice, une réparation, etc.). Supporte le coût de la publication.                                                             |
| <b>Reputation-Based Social Network (RSN)</b> | Réseau social de réputation (RSN) | Un réseau social décentralisé où les participants échangent des retours sur le comportement dans le monde réel. Les enregistrements sont coûteux à créer, bon marché à lire.                                           |
| <b>Reputation Signal</b>                     | Signal de réputation              | Un enregistrement individuel dans le réseau — positif (réparation d'un préjudice, exécution d'une obligation) ou négatif (injustice, rupture de contrat). Cumulativement, les signaux forment un profil de réputation. |

| Terme                 | Français              | Signification                                                                                                                                                                                                                                                                                           |
|-----------------------|-----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Social Graph</b>   | Graphe social         | Le réseau de vos contacts et des contacts de vos contacts. L'algorithme cherche des vérificateurs à une profondeur configurable (par exemple 3 niveaux). Pas de chaîne de blocs mondiale — le réseau forme naturellement des communautés avec des chevauchements.                                       |
| <b>Tax Allocation</b> | Allocation de l'impôt | Un mécanisme par lequel le contribuable décide où va une partie de ses impôts. Le pourcentage allouable croît d'année en année.                                                                                                                                                                         |
| <b>Track Record</b>   | Track record          | En général : l'historique des résultats passés, des succès et des échecs d'une personne ou d'une organisation. Ici : la somme de toutes les interactions passées d'une identité DID donnée dans le réseau — assertions vérifiées, enregistrements acceptés et rejetés — dont sa réputation est dérivée. |



| Terme           | Français     | Signification                                                                                                                                 |
|-----------------|--------------|-----------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Verifier</b> | Vérificateur | Un participant sélectionné algorithmiquement pour vérifier et publier un enregistrement. Engage son bon nom sur la véracité de l'information. |

## Notes de production

**Réservé par l'auteur** (non couvert par la licence CC BY-SA) : le nom et le logotype Personix, la couverture du livre, et les canaux de soutien (codes QR, adresses, adresse e-mail de contact). Les éditions dérivées doivent retirer ou remplacer ces éléments, qui ne peuvent servir qu'à référencer cette œuvre originale.

**Fichiers sources.** La source complète — texte markdown, infographies, scripts de compilation — est disponible avec ce PDF.

**Outils.** Pour préparer le texte et itérer sur les formulations, l'auteur a eu recours à l'assistance d'outils d'IA. Les infographies ont été conçues en collaboration avec des outils génératifs, sur la base des spécifications de l'auteur. Toutes les idées, tous les arguments et toutes les conclusions sont ceux de l'auteur.

# PERSONIX

*Changement sans compromis*

Un réseau de réputation décentralisé, incensurable et incorruptible

L'État fonctionnait quand la communication était lente, les décisions locales, et l'autorité vivait dans la même ville que celle qu'elle gouvernait. Les réseaux d'aujourd'hui inversent ces trois hypothèses — et les institutions bâties sur elles ne conviennent plus au monde qu'elles régissent. Ce livre décrit un outil qui, lui, convient : un réseau de réputation décentralisé où l'identité est vôtre à garder, où la vérité est publiquement auditable, et où la corruption est un suicide réputationnel.

Pas un manifeste. Pas une prévision. Un plan opérationnel de la manière dont le successeur de l'État peut être bâti — volontairement, une déclaration à la fois.

Pavel Kudrna • Prague, 2026

[personix.org](https://personix.org)

Sous licence Creative Commons Attribution-ShareAlike 4.0 International (CC BY-SA 4.0).