

PERSONIX

聲譽網路的樣子，被照出這被粉飾的醜態也無所遁形。

一個不可審查、不可腐化的去中心化聲譽網路
國家的演化式承接者

Personix — Uncompromising Change

An Uncensorable and Incorruptible Decentralized Reputation Network

© 2025–2026 Pavel Kudrna, Praha

Version 6 (2026-05-21)

First drafted June–November 2025; rewritten April–May 2026.

Typeset in $\text{\LaTeX}$ (Tectonic) using Palatino and Helvetica Neue.
A5 landscape (210×148 mm).

Licensed under **Creative Commons Attribution-ShareAlike 4.0 International (CC BY-SA 4.0)** — creativecommons.org/licenses/by-sa/4.0/. The reserved elements, source repository and a note on production tools are listed at the back of the book.

Contents

Introduction	7
這本書在講什麼？	9
Essential Prerequisites for Change	16
變革的基本前提	16
The Tool	25
以聲譽為基礎的社群網路	25
為何這個網路不可審查	48
回應顯而易見的疑慮	50
對科技的依賴	50
在網路裡發布，是不是在把錢往窗外扔？	50
如果有人建立多重身分怎麼辦？	52
有錢人不能乾脆「買下」更多身分（或建立虛擬社群）嗎？	54
那些只想讀取、卻對社群一無所付的搭便車者呢？	55
財務中性	57
自願性、責任與自由	59

自由—極權開關（以及委託）	61
預言機問題——搭起數位與實體世界之間的橋	66

How Verification Works 68

共識與驗證流程	68
Roles in the verification transaction and authorities	74
角色總覽	74
發行者	75
權威機構	76
驗證者	80
主體	83
觀察者	85
機制：時間戳記與挑戰碼	85
妙處所在：你根本不需要真的觀察者	85
委託	87
角色之間的溝通	91
湧現的社會契約——政策	93
提供關於你自己的資訊	97

Crime and Punishment	98
罪與罰	98
Follow the Money	109
追蹤金流軌跡	109
國家的弱點——金錢	109
Proposed transition to the state's successor	112
演化，而非革命	112
四件彼此支撐的工具	113
簡單的稅制——入場的誘餌	114
電子支出登錄（ESR）	114
公民稅款分配——決定的份量	115
與國家的協商平台——那根槓桿	119
沒有身分證的公民身分	121
重疊與可逆性	124
Conclusion	127
這條路是存在的	127
致謝	128
靈感	128

審閱與回饋	129
工具	129

Glossary	132
-----------------	------------

詞彙表	132
---------------	-----

Introduction

你覺得自己能仰賴國家嗎？

當一樁明顯的不公降臨在我、我的家人或我社群裡的某個人身上（肢體傷害、詐欺、不當限制……），而國家的回應卻是：對，這是不公，但你什麼都別做，否則你和我們之間會有更大的麻煩——我拒絕接受這種狀況。這樣的狀態是病態的，而順從它的人是共犯。

其結果是彼此疏離、扮家家酒般的社群、扮家家酒般的國家，以及社會日益深化的崩解，並預示著前方將有嚴重的衝突。

國家跟得上科技與社會變遷的步調嗎，還是寧可一紙禁令了事？

我大可假裝把停滯、無能與腐敗當成法治與傳統所宣稱的穩定來對待，但我不想再這麼做了。那是在騙自己，也是在騙你。

當你膽敢批評自己正在付錢的東西時，你感受到官員與民意代表的那種居高臨下嗎？

我拒絕認為社會中的人不配參與塑造全社會的規則，只因為他們不擅長那些軟實力——而如今在國家立法化的機構裡，這些軟實力竟是成為民意代表的唯一充分條件。我相信絕大多數人都能照顧好自己、照顧好所愛的人與自己的社群——而且他們在其中看見了自己人生哲學的一部分。我周遭認識的多數人都是這樣的。

但我也遇過徹頭徹尾的混蛋，他們之所以是混蛋，正因為他們懂得玩這場遊戲——在這場遊戲裡，社群不被允許給他們回饋，國家保護他們，好讓沒有人擾亂那套秩序，因為那秩序會威脅到國家的本質：確保權力階層與其機構層級上層樓的那些人過得輕鬆。封建制度已被民粹主義者與菁英主義者的統治所取代。

你喜歡別人告訴你該怎麼過日子嗎？



我拒絕接受。

我不接受把當前的狀態當成完美、最終的既定事實。我在自己的行為舉止上必須負責，但當有人告訴我該持有哪些「正確的」價值觀時，我就會敏感起來。你呢？

這本書在講什麼？

想像一個聲譽社群網路，任何想加入的人都能為它建立自己的金鑰（建立自己的身分），可以由社群成員邀請加入，也可以獨自闖進來。你累積自己的聲譽，並在需要時汲取關於他人有用的聲譽資料。當不公發生時，你向社群尋求支援——你陳述自己的案情、提供你手上關於此事的一切，社群看一看，依相關性決定是否轉傳給其他人，以及如何制裁作惡者。

這整本小書講的，就是為了讓外在如此簡單地運作，內部引擎需要具備什麼。如果你堅持讀下去，我向你保證，一個如今在許多方面看似複雜、難以理解的世界，將會展開得更容易理解、更清晰。你會看到，許多壞事可以被安排成不再對壞人如此不公地划算。而且它不是一種你得整天黏在線上的工具——只要在你覺得有需要時伸手取用就夠了。

我還向你保證，這裡所描述的安排會讓人感覺更貼近人們真實的動機，而且它不需要以某個「主義」之名去重塑那些動機。

最後，我們會展示如何管理一場非革命性的過渡，讓社群再次成為完全運作的社會單位，不必再只是假裝。

■ 技術文章

這本書是原始技術文章《去中心化聲譽網路：一個自願且不可腐化的社會組織框架》（Pavel Kudrna, 2026）的說明性伴讀。如果你對形式化的架構描述、驗證者選取演算法，以及經濟機制的論證感興趣，我建議從那裡開始。

■ 各章環環相扣

這本書是以一段連貫的論證寫成——每一章都建立在前一章之上。某一部分引入的概念會在後續部分被使用，包括在註腳中。我不建議跳著讀。



底下還有更多。跟著我。

■ 這本書寫給誰？

儘管採用了視覺上親切的版式，主要的目標讀者仍是較為專業、關注人類社會可能的社會—經濟—政治安排原則的讀者。要達到能把整個主題向最廣大公眾易懂地說明的地步，還需要一條漫長的路，去建構出一整套完整的溝通策略。

對於如何讓這本小作品，或任何後續修訂版更易懂，我歡迎各種建議。

警告

我不知道你是誰、幾歲、這輩子被迫忍受過多少破碎的承諾。我在這裡不再做承諾了。相反，我想警告你：你在這裡學到的一切，唯一的結果或許是意識到——大概沒有任何一條路，能讓別人替你收拾今日的爛攤子。我只是在描述一個框架／工具，它或許能讓收拾這件事變得更簡單、更透明。我會以它為基礎，嘗試準備一場社會實驗／模擬，修正潛在的缺陷，或者若它被證明存在根本性的設計裂縫，就徹底埋葬這個想法。

一個請求

如果你在讀完這本書之後，依然對這個想法保持開放的心態，並持續關注它走向何方、在實質批評下能否站得住腳，我會深深感激。若你日後能參與其中，我會更加感激——用你自己的想法去試圖打破所提出的均衡原則，藉此更好地檢驗這套系統對真實人類行為的準備程度。

沒有你和你的參與，這個想法就只是抽屜裡的一套理論。沒有你和你的貢獻與財務捐助，我們就無法把這個專案推向一場真正的社會實驗，也就無法推向真正的就緒狀態。沒有你和你的實質批評，我們就會停滯在現在的原地，或任由自己被中間派的聖杯所吞噬——絕對、不可逆的極權主義。要選哪條路，或是袖手旁觀，取決於我們自己。

這項挑戰

我們放在你肩上的擔子並不算輕。你已經透過那些聲稱社會最好由中央來治理的、如降神咒語般的手冊，承擔著一個揮霍無度的社會的成本——而我竟還有臉向你要求更多，還要你與這些傾向對抗。我很清楚，我們得挺過史上最大龐氏騙局的崩塌——隨收隨付的年金制度——同時又不能讓好幾個世代餓肚子。

然而我還是要請求你：讓我們終於能交給孩子一個更好的世界，並留下我們曾促成那場變革的傳承。釋放經濟成長，或許能成為解決眼前困境的部分辦法。屆時我們可以告訴後代：這是一趟精彩至極的旅程，而且沒有白費。

■ 問題所在

唯有以直接責任來平衡的自由，才能真正釋放這個世界前所未見的巨大潛能。



更好的世界值得這份重量。



進來吧。計畫都攤開了。

Essential Prerequisites for Change

變革的基本前提

促成向好變革的根本前提，是下屬變成上級——或至少成為對等的夥伴。這意味著接管那些界定上下從屬關係的最關鍵事務。這些事務建立在「歸屬於構成國家公民之社群」的證明之上。它們是資訊，以及該資訊能否被在這些社群中擁有相當聲譽的權威所驗證。

為了克服當前的體制，我歸納出五個前提，接著我會以自己理解的方式加以說明。我們可以把這些前提想成支撐本書其餘部分所描述之系統結構的支柱。這些支柱一開始是依我自己的偏好選出的，在與它們反覆推敲的過程中，我逐漸把對每一根支柱的理解打磨成以下的形式。

讓我們逐一走過這五根支柱。

自願性

在我們的情境裡，自願性意味著我不被迫參與去中心化聲譽網路的運作。然而，我不能主張一項以肯定方式表述的權利，要求網路不記錄關於我的資訊——關於我的資訊是否最終進入聲譽網路，只取決於我、我的行為、我的作為，以及我的責任。

變革的前提

自願性



自願性

我為自己作主。

組織



組織

齊心協力，不受制於人。

韌性



韌性

無法被審查。

共識



共識

以施壓換取妥協。

不可收買



不可收買

無法收買所有人。

少了這五大支柱，任何變革都只是在燒時間。



自願 — 直到責任找上你。

■ 組織

單一個人無法打破這個體制，正因如此，國家才控制人們的結社，作為防止那些可能威脅其結構與運作之活動的手段。人們是為了支持還是反對而組織起來，並不重要。透過組織，可以在有人膽敢違背國家意志去改變國家時，緩和殺雞儆猴式懲罰的衝擊。

我們不必設定共同的目標，但我們可以一起走一段路。最自然的形式是在社群中結社——但這些社群必須擁有一切所需的工具，才不至於停留在扮演社群的假戲。

■ 韌性

通往改變國家——或通往過渡到其後繼者——的所選路徑，絕不能取決於國家的許可。這些工具以及它們的使用方式，必須盡可能地不可審查。說白了，審查它們的代價必須高得離譜。少了這一點，整場努力不過是在燃燒時間與生命能量。

前提 2/5：組織

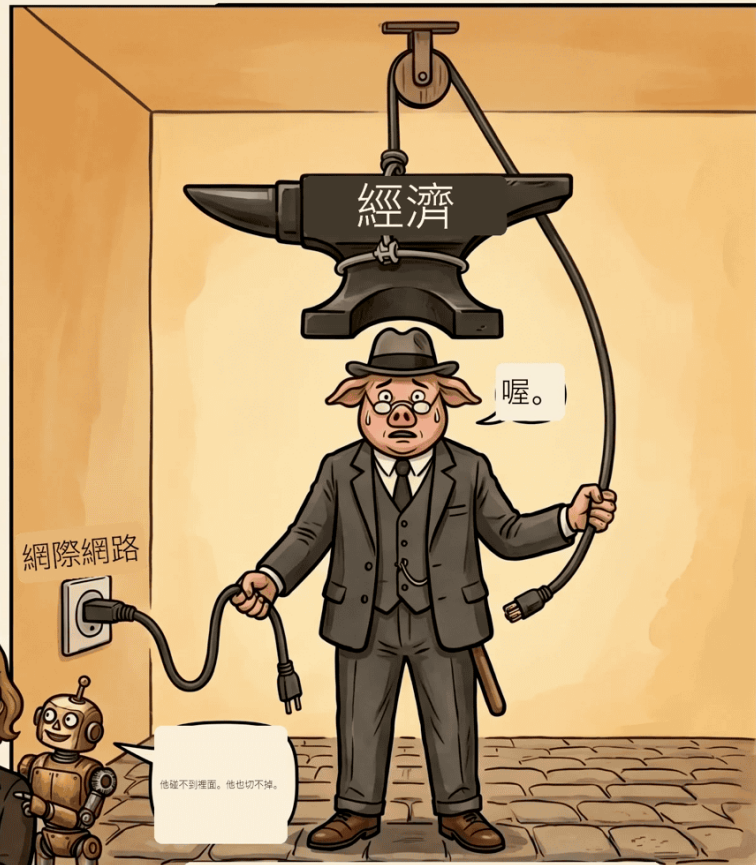


個人無法擊垮體制。社群可以。

前提 3/5: 韌性



他無法從外部搜尋。



拔掉插頭 — 等於自我毀滅。

沒有可申請的許可。沒有可拔的插頭。

■ 共識

所提出的解決方案，就其本質而言，必須同時包含一套協商共識的機制，以及一個在共識遭違反時可動用的鎮壓性成分。它不必是自願的雙贏協議。只要環境與社會壓力能確保社群內部與社群之間達成妥協就夠了。

■ 不可腐化性

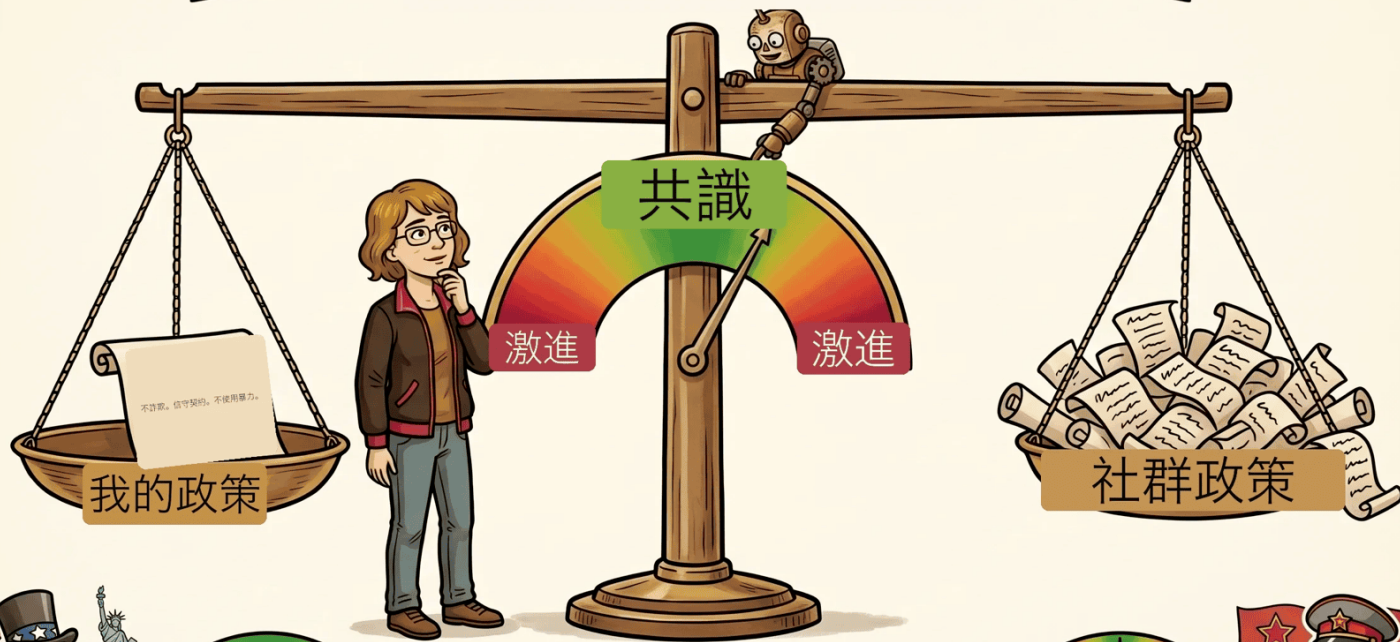
不可審查性從外部捍衛這個系統。但一個由人組成的網路也可能從內部腐爛——某個權威被攻陷、一條宣告過的規則被悄悄拋棄、參與者在無聲無息中被收買。如果內部的人可以毫無後果地被腐化，那麼不可審查性將只是一場空洞的勝利。

不可腐化性不是單一巧妙花招的結果。它源自**所提出設計中若干原則的協同運作**——對抗腐敗的壓力被分散到整個架構中，各個部分彼此強化。至於這一點究竟如何達成，我們會逐步展示——在工具的描述中、在驗證中、以及在論懲罰的那一章中。最後我們會回顧一路建立起來的一切。

不可腐化性既是設計的前提，也是結果的湧現性質。它是第二道防線——面向內部的那一道——沒有它，韌性就只是半面盾牌。

待在範圍內 — 別當激進分子。

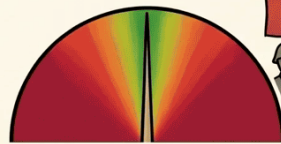
你可以有分歧。只是別偏得太遠。



自由社會
共識是一片容忍區，

容忍區隨文化的自由度而伸展。

前提 4/5：共識



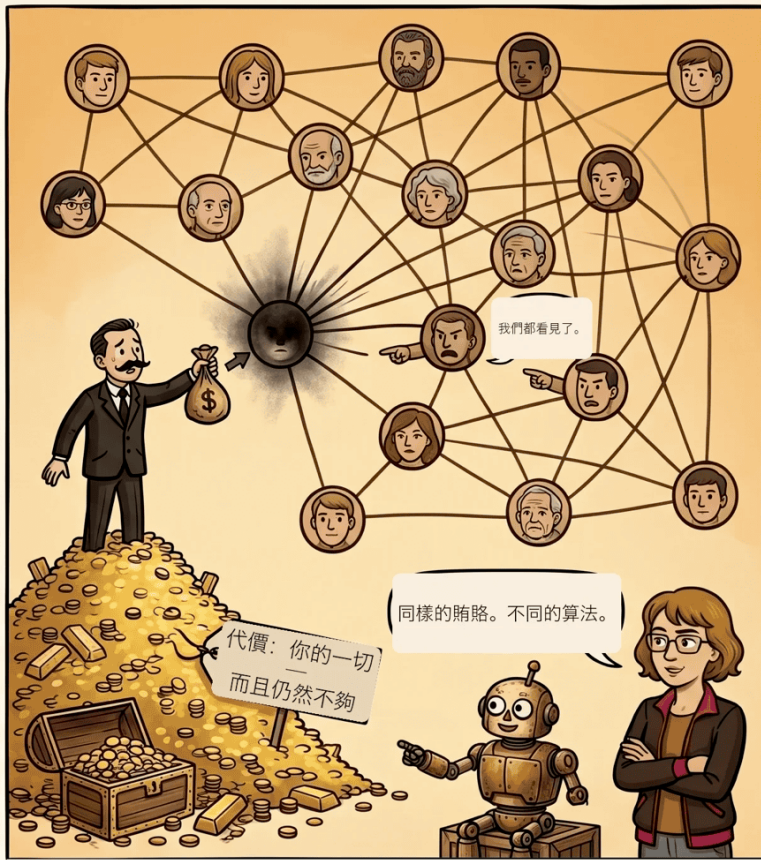
威權社會

共識是一片容忍區，不是全體一致。

前提 5/5: 不可收買



賄賂上面幾層 — 反正基層照付。



賄賂一人 — 他永遠失去聲譽。賄賂所有人 — 你先破產。

腐敗有其代價。在網格中，代價太高。

The Tool

以聲譽為基礎的社群網路

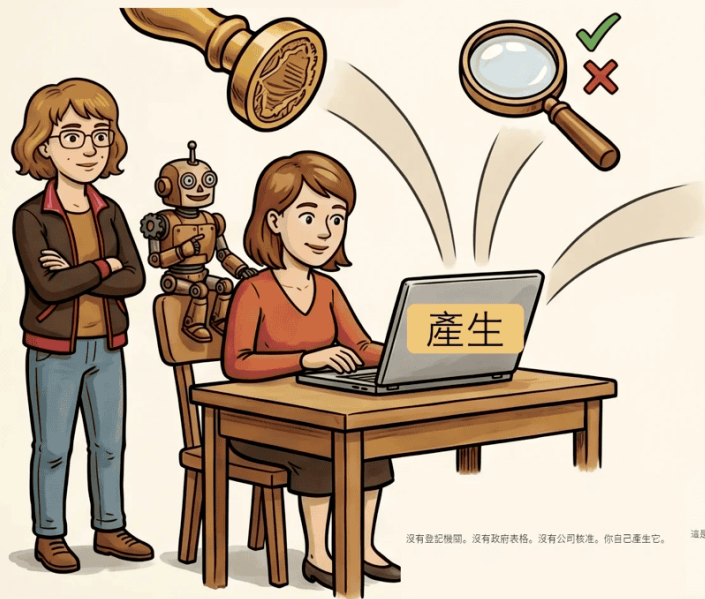
要促成變革，我們需要一件精心設計的工具。我們先簡略勾勒它；在後面的章節裡，我們會更詳細地檢視每一個部件並加以擴充。想像一個不可審查、全球性、去中心化的社群網路，你可以在其中安全地建立與管理你的代理身分——所謂的去中心化身分（Decentralized Identity, DID）。DID 是一種由你自己建立、自己掌控的數位身分，不依賴任何中央權威。沒有人能奪走或偽造它，因為它是用你的私鑰（或透過多重簽名的多把金鑰）以密碼學方式簽署的。

你的身分，你的金鑰，你的規則

你自己創造它

私鑰 —
代表你簽署。只有你持有。切勿分享。

公鑰 —
驗證你的簽章。網路上可見。



沒有登記機關。沒有政府表格。沒有公司核准。你自己產生它。

這是你的公開身分。任何人都能讀取。只有你的私鑰能簽署變更。

任何國家都無法撤銷這個。

你的 DID 文件



主張 —
關於你的已驗證事實

公民身分: 捷克共和國
— 由市政公證人驗證

學歷: 資訊科學碩士 —
由大學校友網路驗證

財產: 42
號公寓所有人 —
由地方社群登記處驗證

被動見證: 對不當行為視而不見
— 未履行規範 —
由鄰里見證人提交

詐欺: 騙走鄰居的積蓄
—
由地方社群法庭提交

主張是已驗證的陳述。好的與壞的。權威以其聲譽為它們背書。



國家身分證 —
可撤銷: 國家隨時能取消。



DID —
不可撤銷: 只有你的私鑰能簽署變更。

你的身分。你的金鑰。你的規則。無需許可。

■ 註

這帶來的一個推論是：這樣的身分可以逐步取代國家核發的身分證件——不過這點會在論過渡的那一章詳談。

在這樣的網路裡，你可以透過你的身分回報有人對你造成了傷害（以及日後可能回報他已補救，或被迫補救）。為了讓這個回饋——指向傷害發動者的回饋——具有作為相關資訊來源的價值，把資訊登錄進網路必須花費時間、能量與金錢——而且在此之上，還必須為其他人產生可驗證的證明，證明這不是無稽之談。

讀取資訊會很容易且相對便宜，但建立一筆個別紀錄則昂貴且費力。寫入會遵循一套清楚的協定，其中依所選演算法進行的運算，會嚴格地決定要向哪個 DID 請求驗證所提交的資訊，以及該如何進行，好讓被選中的參與者代你處理資訊、發布它，並成為它的驗證者。

■ 演算法對抗激進主義

驗證者的演算法選取確保了非激進的資訊發布者，隨著時間推移，會在已發布資訊的成本與驗證的報酬之間維持近乎中性的平衡。

發布耗費時間、能量與金錢

寫入網路從不免費，讀取則免費
三個管道 三個都是真的

時間



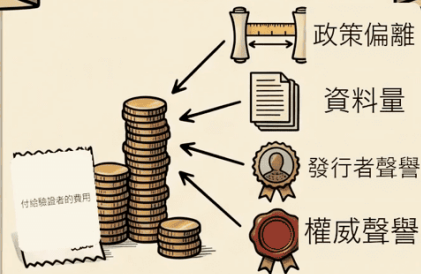
你在演算法抽選驗證者、驗證者讀取你的紀錄時等待。

能量



簽署、雜湊、驗證 —
每一步都是實實在在的運算與電力。

金錢



你的主張離驗證者的政策越遠、紀錄越大、發行者或其權威越不受信任
— 費用就越高。

接下來會發生什麼

「演算法如何抽選驗證者」、「驗證者如何記錄」、「發行者的選擇」

為何昂貴的寫入保護聲譽
— 本章稍後說明

(避免昂貴，只對有價值。這就是根據對寫入收費、對讀取不收費的原因。)

隨迭代增加的成本

每次重試成本更高



每次拒絕或重擲都加進演算法吃進的時序 — 下一次嘗試在三個管道上都更昂貴。

讀取的不對稱

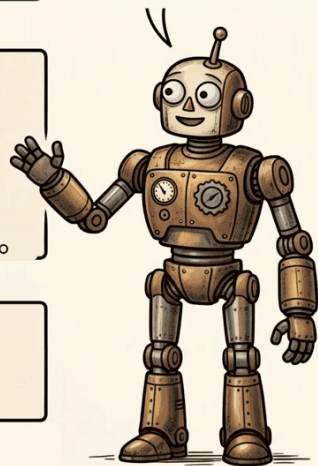
讀取很便宜



查詢免費

任何人都能讀取聲譽與紀錄 — 只有寫入要付費。這種不對稱是設計如此。

寫入要付費 — 讀取不用。不對稱正是重點。



讓我們來看演算法如何選出一位驗證者。

■ 演算法

演算法選取以非決定性的方式，為不同的資訊選出不同的驗證者（或一組可能的驗證者）。完整 DID 文件的雜湊（一種單向數學函式，能從任何輸入產生獨一無二的「指紋」——就像一份文件的指紋）決定了它在一致性雜湊環上的位置，並選出候選驗證者。

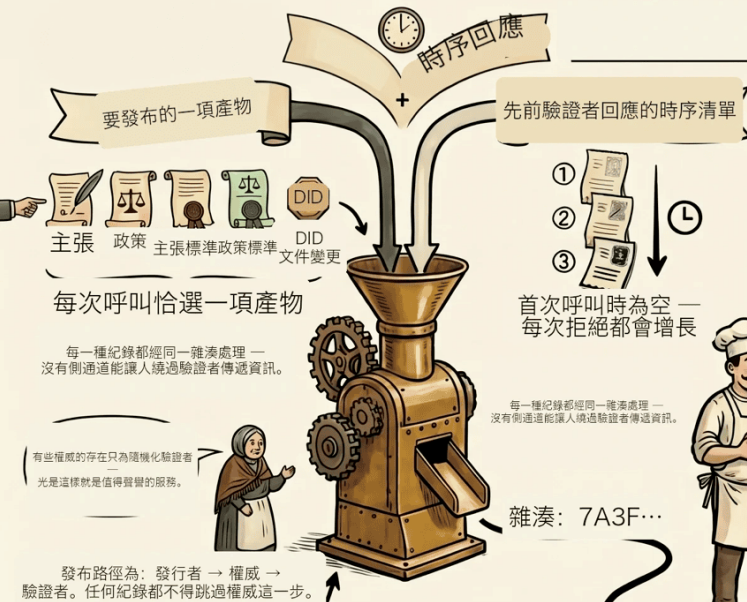
$$\text{verifier_DID} = \text{hash}(\text{DID_document})$$

用白話說：演算法拿走你整份 DID 文件，從中計算出一個指紋，而那個指紋決定了你的驗證者。

面對演算法選出的第一位驗證者，身為發布者的你可能不會成功——你的聲譽或宣告的設定可能不符合對方的要求。你會以演算法方式繼續尋找下一位，方法是再進行一次遞迴迭代，替你指派另一位驗證者。每一步，到目標驗證者的「距離」都會增加，隨之而來必須發布的中繼資料也會增加。隨著資料變多，成本自然上升（不只是因為主張最初的大小，也因為每次被拒都累積更多中繼資料）。可信的資訊遠比荒謬的一時興起更容易通過。願意承擔多高的代價、這筆紀錄對自己有多重要，取決於每個人自己——激進主義注定會變得昂貴。

演算法如何抽選驗證者

一枚公正的硬幣，擲向你的整個社群



你的社群及其鄰近地區

每張臉機會均等 — 雜湊均勻隨機落點



你的驗證者

你無法選擇你的驗證者 — 演算法擲硬幣，選擇每個人機會均等。

接下來會發生什麼

驗證者以價格回應 — 或以理由拒絕 — 見「驗證者如何回應」

發行者決定如何處理那些答覆 — 見「發行者的抉擇」

每次重試都增加成本 — 如先前在「發布成本」所示

演算法抽選 — 你不選。

A 你能暴力破解它嗎？

我可以發出成千上萬份假幣，直到有一分落在我想賣的驗證者身上……



稍有不同
大不相同
完全不同

雜湊是確定性的，但抗原像 — 每個微小改動都把抽選拋到毫不相干之處。

B 但權威封印了其餘部分



權威簽署的、關於他人的證據

……但我無法預測權威會簽什麼 — 我也分辨不出她是否跟我串通。

驗證者如何回應

以價格接受 — 或以理由拒絕

驗證者在回應前權衡四件事。

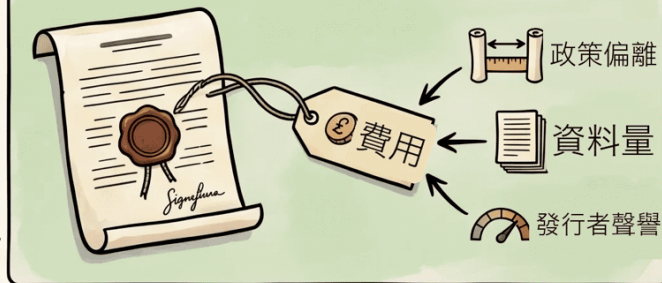


拒絕 — 附帶理由

- 發行者的聲譽對我來說太低
- 這則紀錄背後的權威不是我信任的
- 發行者的政策離我太遠，無法搭橋
- 文件本身不符合我政策的規則

驗證者寫下為什麼 — 他們的回應會回饋到下一次嘗試。

接受 — 附帶價格



驗證者同意發布 — 但價格反映了主張離其政策多遠、承載多少資料，以及發行者有多受信任。

驗證者的回應被加入時序清單 — 如「演算法如何抽選驗證者」所示

無論驗證者說什麼，他們的答覆都成為下一次呼叫的輸入。

每位驗證者都以這兩種方式之一回應 — 以價格接受，或以理由拒絕。

接下來會發生什麼

- ⚙ 發行者決定如何處理這個答覆 — 見「發行者的抉擇」
- ⚙ 每個答覆都改變下一次嘗試的成本 — 如先前在「發布成本」所示

驗證者要嘛定出價格 — 要嘛告訴你為何不行。

無論驗證者針對你的驗證請求做出什麼決定，球都回到發布者這邊：他可以接受驗證者提供的驗證服務報價、把這次回應併入時序紀錄後再試一次（代價更高），或者乾脆走人，吞下已投入的沉沒成本。

為了讓你的資訊更有份量、在驗證者面前更有機會被接受，身為對所發行資訊有利害關係的發布者，你可以動用**受信任權威機構**的服務。權威機構要嘛拒絕所提交的資訊，要嘛接受它並以自己的好名聲（聲譽）為它背書。權威機構通常會要求現實世界的證據、加以驗證並分類。其產出是一份就特定案件在特定時間所做評估的紀錄。你可以把權威機構想成現實與數位世界中某類服務的專家——例如調查員、稽核員、保險業者、某類商品的供應商（本質上就是市場上任何一個經濟行為者）。

發行者的抉擇

如何處理驗證者的答覆

無論驗證者說了什麼，發行者現在桌上有一個答覆。



回到「演算法如何抽選驗證者」——
先前所示

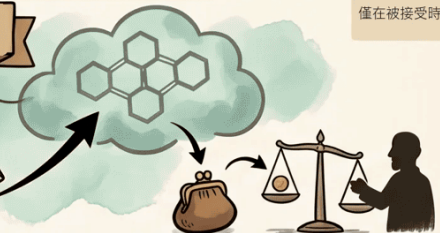
只有重試路徑會循環——接受與走開都結束故事。

驗證者提議——發行者定奪。

三條出路

接受這筆交易

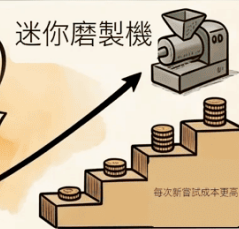
DID 網路



僅在被接受時

發行者付費——
紀錄被發布進網路。僅在驗證者接受時可用。

再試一次



回應被併入時序——
演算法再擲一次。無論驗證者以發行者不喜歡的價格接受，或直接拒絕，都適用。

走開

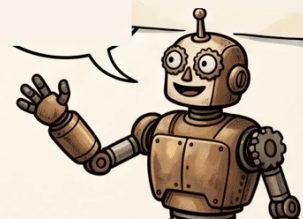


發行者捨棄草稿。什麼都不發布——
但也不再付出更多。

接下來會發生什麼

每次重試都改變下一次嘗試的成本——
如先前在「發布成本」所示

驗證者的答覆本身——
如先前在「驗證者如何回應」所示

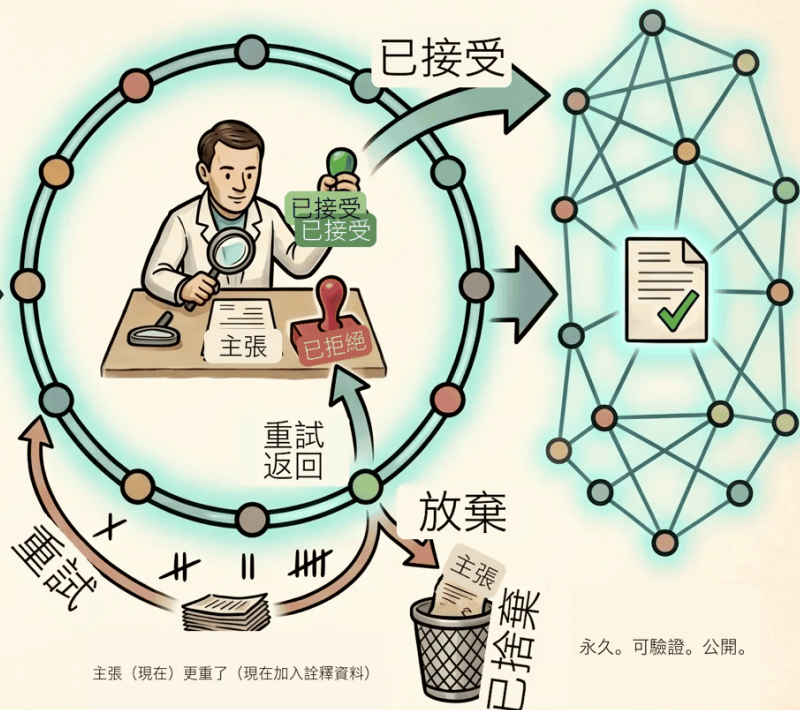
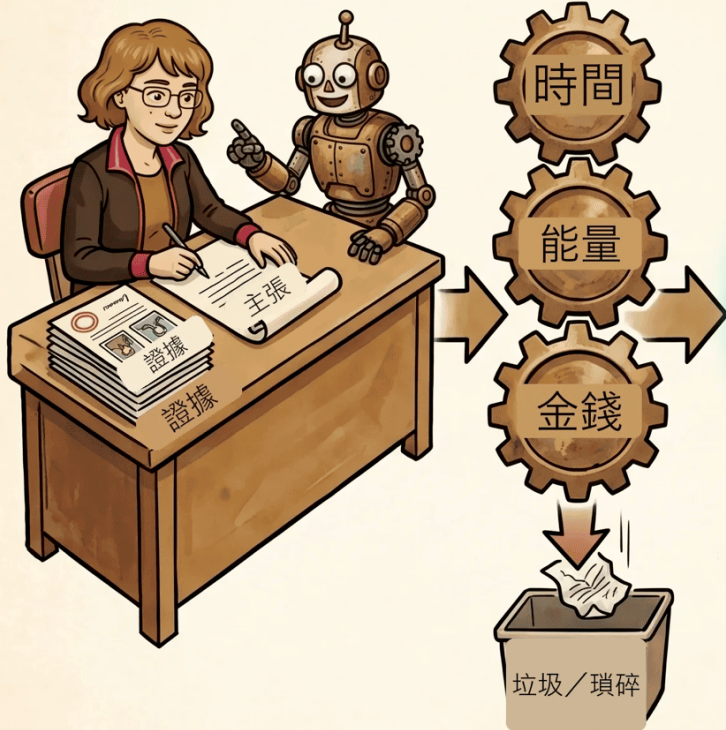


階段 1 —
發布主張

階段 2 —
品質過濾

階段 3 —
遞迴驗證

階段 4 —
永久紀錄



偽造昂貴。驗證便宜。

當你嘗試把資訊發布進網路時，它裡面很可能已經含有關於其行為者的資訊——這些就是聲譽訊號。如何解讀聲譽訊號——它們在不同情境下對你意味著什麼、帶有什麼風險——未必簡單。每個參與者都能透過自己的 DID，依據他正在處理的、與對方之間的情況，以不同方式看待聲譽紀錄。對方是可靠的付款人嗎，還是我需要在一筆生意交易中先要求對方預付？所提供的產品是否帶有關於隱藏詐欺或瑕疵的評價？當出事時，他們是否試圖逃避契約責任？有時候，對對方整體一致性有一個較複雜的檢視會很有用——這取決於要求概覽者的偏好。市場可以提供各種產品與服務，在當下情境脈絡中簡化、處理並釐清對聲譽的解讀。各種權威機構及其提供的服務，也能服務於這個目的。

■ 範例

發布者感興趣、且對他人有價值的典型資訊，涉及的是現實或虛擬世界中超乎日常人際溝通之外的事件。

負面範例：- 犯罪行為的證據（例如經受信任的調查機構稽核）- 間接證據（單獨看很薄弱，但統計上會累積）——例如短時間內反覆出現在多起竊案附近 → 還算是巧合嗎？- 違約

正面範例：- 已補救的傷害（自願，或在社群壓力下作為懲罰而補救）- 接受並服完由權威機構 X 所提出的處罰 - 權威機構 X 在一定程度上撤銷了對加害者財產權的承認

蒐集關於對方的可得資訊、並依自己的偏好評估風險，取決於每個人自己。

如何解讀聲譽

知情的決定



她清楚自己在跟誰打交道。
在給予信用之前。在簽約之前。在信任之前。

盲目信任



他完全不知道自己在跟誰打交道。

能出現哪些種類的主張？

主張產物的範例

(一則主張是關於某人的陳述 —
這些是人們會發布的種類。)

負面主張



傷害
對他人施以肢體攻擊



竊盜
未經同意取走他人財物



詐欺
為私利欺騙他人



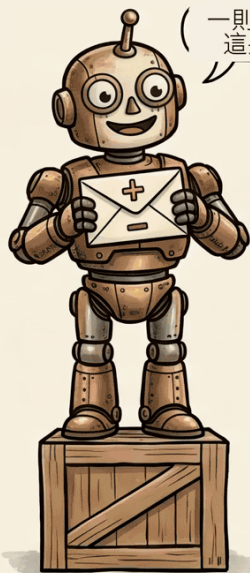
違約
未履行約定義務



誹謗
散布有害的不實言論



遺棄
棄扶養對象或職責於不顧



正面主張



傷害已彌補
修復先前造成的損害



債務已清償
全額付清所欠



提供援助
自付代價幫助他人



已驗證的專業
在某技藝或領域中證明的能力



卓越服務
對社群的長期貢獻

僅為範例 — 每則主張都遵循一項主張標準，任何標準都能增添更多。

你不必加入 — 但若你的行為影響他人，有人就能發布關於它的主張。

主張是行為進入網路的方式。

■ 關於你的資訊是否出現在網路裡，只取決於你自己的行為。

你永遠不必加入這樣的網路，但關於你的資訊仍可能出現在其中。這只取決於你的作為，以及它們對他人造成的影響。

社群可以為你開一個



他沒有自己的
DID。他從未註冊。



你沒開
DID，於是社群開一個關於你的。負面主張附在這裡。



你可以開自己的一
但社群會把兩者連結起來。聲譽跟著人走，不跟著金錢。

1. 你造成傷害----->2. 社群提交----->3. 你無處可逃-->

你可以選擇不開 DID。但你無法擺脫你的聲譽。

我剛才簡略勾勒的，是一個受去中心化身分（DID）啟發的社群網路可能如何運作。DID 概念的首要目的，是透過「訂閱我將遵循並據以生活的規則」這一原則，來強化隱私與自由——賦予使用者決定要分享哪些資訊、在什麼條件下分享的能力。

我提議進一步把各個 DID 連成一個通訊網路，讓它們的持有者即使在沒有出事、社群或個人並不需要反應的情況下，也能交換回饋。這種對「我們簽署過的規則」所做的預防性對照——搭配能計算彼此在「對方應如何運作」之期待上偏差所造成的經濟與其他後果的選項——可以被視為尋求共識的動機。這樣的系統不強調自由，而是強調結合了「對現實行為負責」的自願性決策。

單一個人無法獨力打破這個體制——一群人有較大的機會，而一群達成協商共識、並在許多議題上有動機齊心協力的人，抵抗威權傾向的機會又更大。第一章的組織前提，會在滿足兩個條件後達成：DID 聲譽網路涵蓋社群的代表性足夠高，使得使用它不再是件稀奇的事。同時，這個社群區塊成為一個具經濟重要性的少數，能夠強勢地與社會其餘部分協商。

■ 自願性對比自由

自由——在肯定意義上的自由——會是平衡兩項因素的次生效應：自願性，以及來自周遭、朝向責任的壓力。

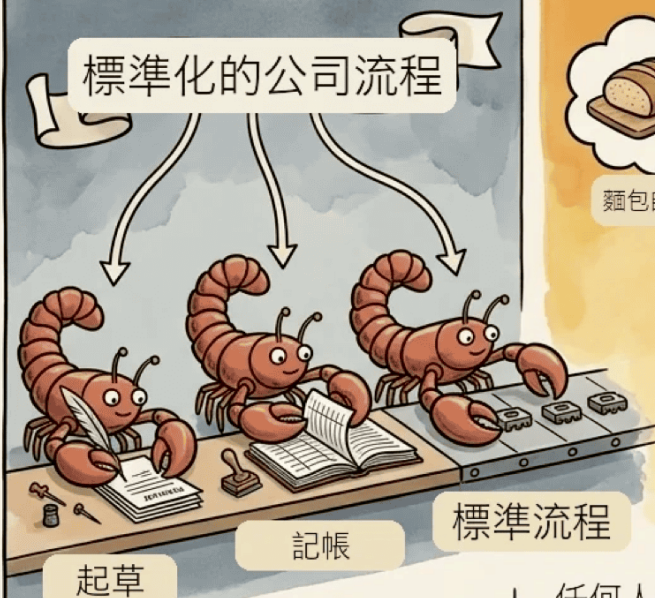
■ AI 時代與聲譽的價值

在人工智慧的時代，一切與認知思考相連的事物都正在被自動化——而且可能走得更遠。那麼在人類活動中，還剩下什麼作為競爭優勢？答案很難，肯定會找到些什麼，但有一件事我們可以確定地說：聲譽將是決定性的。一段可驗證的、關於你行為、你承諾及其履行的歷史——那是 AI 不會替你建立的東西。

若 AI 負責思考 — 還剩什麼給你？

AI 代理接手重複性工作

標準化的公司流程



一項接一項，重複性的認知工作正被交給代理。

那麼人類還剩什麼？



任何人都能挑同一個點子。
是什麼讓一位麵包師、一位木匠、一間
AI 工作坊與眾不同？

聲譽 — 分辨彼此的憑據



必須有人為代理的所作所為負責
——而這份責任無法轉交。

沒有聲譽，每個麵包師看起來都一樣 — 最大的品牌把他們全吞了。
這會不會就是讓 AI 拴上繩索的去中心化之路 — 那個阻止任何單一玩家獨占整個市場的東西？

AI 自動化工作 — 聲譽讓你保有人性。

真相的經濟學

社群橫幅



同一個社群。不同的立場。

不受歡迎但可接受



在共識內

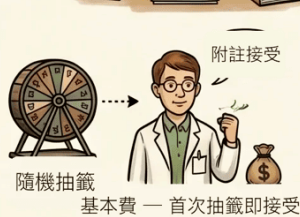


在共識外



提交

抽籤



退款

帳本



演算法公平抽選。人們為自己的信念定價。

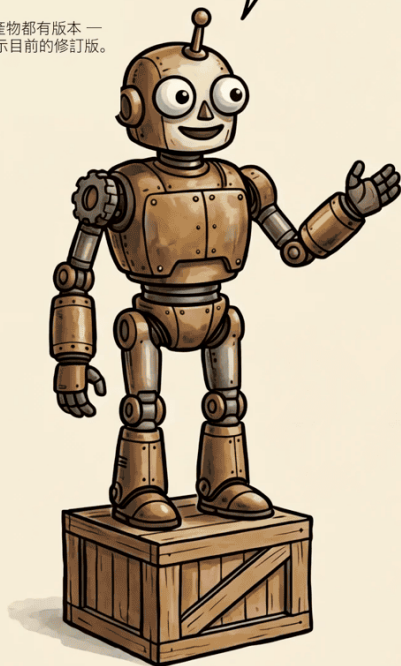
均勻抽籤。非均勻回應。離共識越遠，價格越高。

底部觀察者橫幅

網路中會發布什麼

有五樣東西可以發布
——
每一樣都有版本。

每個產物都有版本 —
徽章顯示目前的修訂版。



v1

DID 文件

你在網路上的身分紀錄 —
金鑰、詮釋資料、網路位址。

管理者：DID 持有人



v2

主張標準

一則主張必須遵循的結構
—— 什麼算是有效證據。

管理者：在該領域有聲譽的權威



v3

政策標準

一項政策必須遵循的結構
—— 接受規則的形式。

管理者：在該領域有聲譽的權威

↓ 衍生自

↓ 衍生自



v4

主張

關於某主體的陳述，遵循某項主張標準 —
由發行者發布，若發行者與驗證者皆要求，則由該標準的權威共同簽署。

管理者：發行者發布 —
主體是對象

主張分兩種 —
正面 (+) 與負面 (-)。



v5

DID 政策

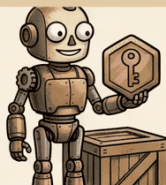
一個 DID 宣告的規則 —
用於驗證、共識與簽發。

管理者：DID 持有人（每個
DID 一項政策）

每個產物都有版本。每個版本都公開。

DID 文件裡有什麼？

DID 文件產物的範例

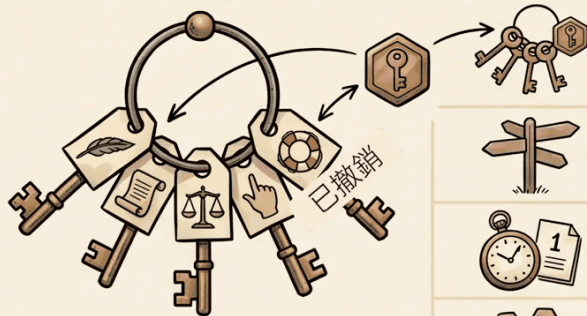


你的 DID 文件是你在網路上的身分證
— 這是它所承載的內容。

你會在裡面看到的欄位

金鑰與簽署規則

每把金鑰授予一項權力 —
編輯此文件、簽發主張、擔任權威、管理政策、或委派復原。權力可交給另一個 DID，日後也能撤回。



網路位址

網路能觸及你之處 — 可更改而不必重寫你的身分



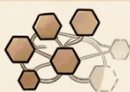
建立時間與版本

這個身分最初出現的時間，以及你現在讀取的是哪個修訂版



連結的身分

你所連結的 DID 摘要 — 一個便利檢視，技術上儲存於他處



承接標記

若你的身分遺失或被盜，權威可標記此 DID
終止並指向你的接續者



DID 持有人撰寫每個新版本 —
但每個版本在網路發布前都必須通過驗證。

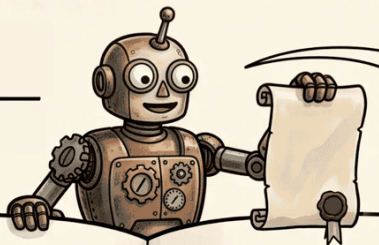
你撰寫它 — 網路驗證它。你無法憑空把自己發布成存在。

你為自己的身分執筆 — 網路加以確認。



什麼是主張標準？

主張標準產物的範例



標準是空白表格 —
主張是填好的表格。讓我兩者並排給你。

標準 — 空白表格



主體 DID
此主張所針對的 DID



發行者 DID
簽署此主張的 DID



何時何地
一個日期與一個地點



核准的證據類型
只有這些種類的證據算數



無 / 程度 / 中度 / 嚴重

結果量表
恰選一個等級 — 不可自由填寫

一則主張 — 填好的表格



主體 DID
did:nwo:alice-9f2b...



發行者 DID
did:nwo:magistrates-04...



何時何地
3 月 3 日，市集廣場



核准的證據類型
照片 ✓ — 證人宣誓 ✓ —
醫師證明 ✓



核准的證據類型
中度 — 4 級中的第 2 級

左側每個欄位在右側都有恰好一個填好的對應項 — 這正是讓同類的兩則主張可比較的原因。

權威蓋在填好主張上的印章是一種保證：流程確實被遵循。



我以我的聲譽擔保，這是依標準處理的。

傷害 v3



傷害 v3

債務 v2



債務 v2

醫療援助 v4



醫療援助 v4

工藝 v1



工藝 v1

證詞 v5

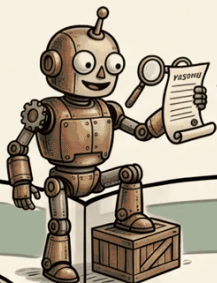


證詞 v5

標準是表格 — 主張是填好並擔保的表格。

什麼是 DID 政策？

DID 政策產物的範例



我的政策無關一副主張怎麼寫——
那是標準的工作。我的政策是我如何決定要不要理會這副主張：我信不信寫著它的人，信不信其標準背後的權威，這件事值不值得我費心？

標準 — 繼承的預設值

規則名稱



對比

發行者聲譽下限

我接受聲譽在十分之五以上的發行者



權威信任清單

我接受任何自身聲譽在十分之四以上的權威所訂的標準



瑣碎 重大

實質性過濾

我處理任何份量超過「微不足道」標記的主張



反垃圾訊息定價曲線

對我提交實質而罕見的主張很便宜——
瑣碎或重複的則迅速攀升



綜合加權

發行者聲譽與權威聲譽相乘；瑣碎實質則使結果減半

政策不重寫標準——它評判人與事。保留、修改、移除、新增——在共同起點上的四個簡單動作。

我的政策 — 由此衍生

規則名稱



保留
勾選
動作詞



修改
動作詞



移除
動作詞



新增
動作詞

發行者聲譽下限

收緊 — 我要求十分之七

權威信任清單

我完全信任地方官員與醫師；我把市政監督下的主張權重減半；我完全拒絕選務署下的任何主張

實質性過濾

瑣碎的滋擾主張，我不理會不花任何成本——
我根本不讀

反垃圾訊息定價曲線

保留 — 預設曲線對我來說很好

綜合加權

移除 — 我用自己的公式

重複主張的成本呈指數增長

新增 —
一年內同一發行者關於我的每則新主張，成本是前一則的十倍

靜默時段

新增 —
我拒絕讀取午夜到破曉間提交的任何主張



驗證——

我的政策既過濾傳入的主張，也在我簽發前過濾自己的草稿。簽發就是輸出端的驗證。

共識——

當社群協商共同規則時，我的政策就是我一票。

你的政策評判傳訊者 — 而非表格。



為何這個網路不可審查

到目前為止，我們描述了這個網路能做什麼。現在讓我們聚焦於它為何無法被關閉或審查。

這個網路很可能會建立在 Tor 網路與洋蔥路由（一種以 Mixnet 原理遮蔽網路流量的方式）的原則之上——這是一種通訊會穿越數層加密、且沒有任何單一節點會同時知道發送者與接收者的技術。中央機構無法越過你的肩膀窺看，因為根本沒有可以窺看的地方。

你可以與它對抗，但你贏不了——除非你把整個國家推進到對每個網路封包、對每一件連上網際網路並在該聲譽網路上通訊的硬體之底層操作進行極權式監控的地步。而這正是中央集權所面臨的抉擇：要嘛接受公民握有一件你力所不及的工具，要嘛以極權控制之名，把自己挖進經濟停滯的黑暗角落。

我們別抱幻想——即使是民主政體，在爭奪中央集權的鬥爭中也會嘗試這麼做。他們寧可給人們戴上枷鎖，也不願交出權力。

你的訊息如何無法被追蹤

同時兩道防線 — 層層包裹與雜訊

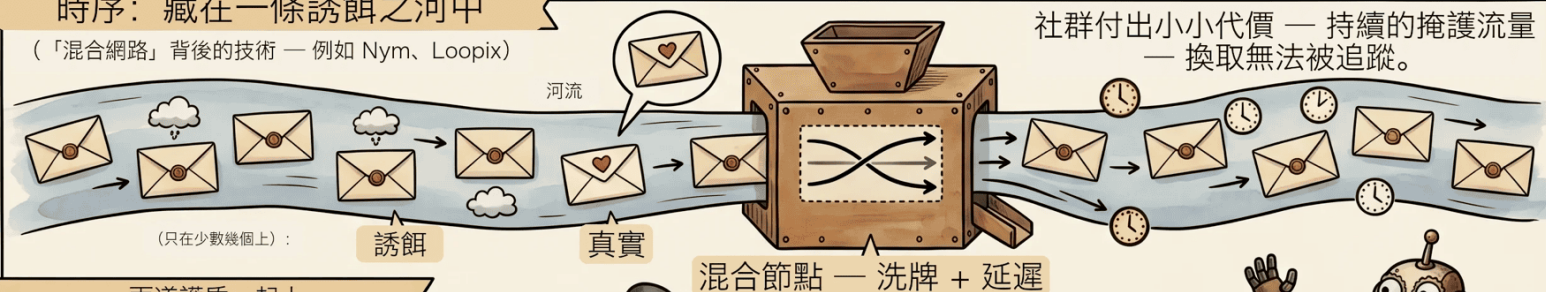
內容：層層包裹

(Tor 背後的技術 — 「洋蔥路由」)



時序：藏在一條誘餌之河中

(「混合網路」背後的技術 — 例如 Nym、Loopix)



兩道護盾一起上

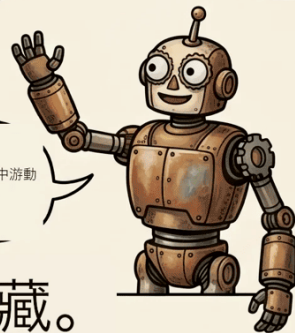
矩陣	隱藏誰？	隱藏何時？
只有層層包裹	✓ 是	✗ 否
只有雜訊	✗ 否	✓ 是
層層包裹 + 雜訊	✓ 是	✓ 是

(洋蔥路由 + 混合網路 — 我們需要的組合)



「一小時一百個信封」
「哪一個重要？」

觀察者看得見流量，卻分不出真實與誘餌。



真實訊息在一條誘餌之河中游動
— 還披著四件外衣。

內容由層層包裹隱藏 — 時序由雜訊隱藏。

回應顯而易見的疑慮

所描述的系統自然會引發一連串問題。讓我們來回應最常見的幾個。

對科技的依賴

你大概已經注意到，不同於現代國家——它已伴隨我們約一百五十年——這裡所描述的聲譽網路解決方案，高度依賴全球／在地網際網路的科技。一旦發生斷線，這樣一個網路的運作就會面臨風險。

如果斷線是暫時的，網路中不會有資料或主張一致性的損失，社群內部達成的聲譽收支也不應受到擾動。不同於可相比擬的支付網路，這個網路假設程序與資料項目的頻率非常低。在這一點上，去中心化聲譽網路與今日的國家並無不同，後者如今也高度依賴科技，且已忘了如何操作紙本卡片檔案（雖然在危機計畫裡它別無選擇也得用）。

以聲譽網路形式出現的國家演化後繼者，在發生永久斷線（一場空前規模的災難）時，可以退回到一個更原始的中央化系統——也就是國家。

科技讓人類得以攀上更高的文明治理形態、為我們帶來益處，但也帶來風險。

在網路裡發布，是不是在把錢往窗外扔？

在聲譽網路裡發布一筆主張的成本，大體上並非沉沒成本。一位發布者投入網路的訊息之效用——關於真實冤屈的資訊、經驗證的經驗、相關的警示——在較長的時間跨度上，會以「替社群裡別人的主張進行驗證」的手續費形式，在統計上回流。社群得利，發布者累積聲譽，於是發布真實資訊的成本便趨近於一筆可退還的押金，只需從中扣除實際網路維護成本中較小的一部分。反過來說，不實或瑣碎的紀錄不會回流——它們的成本是淨損失。因此，誠實不只是一種道德選擇，也是一種在經濟上理性的策略。

兩條路 — 國家關閉，網路開啟

聲譽網路

國家

什麼都不做，就是選了那扇對的門。

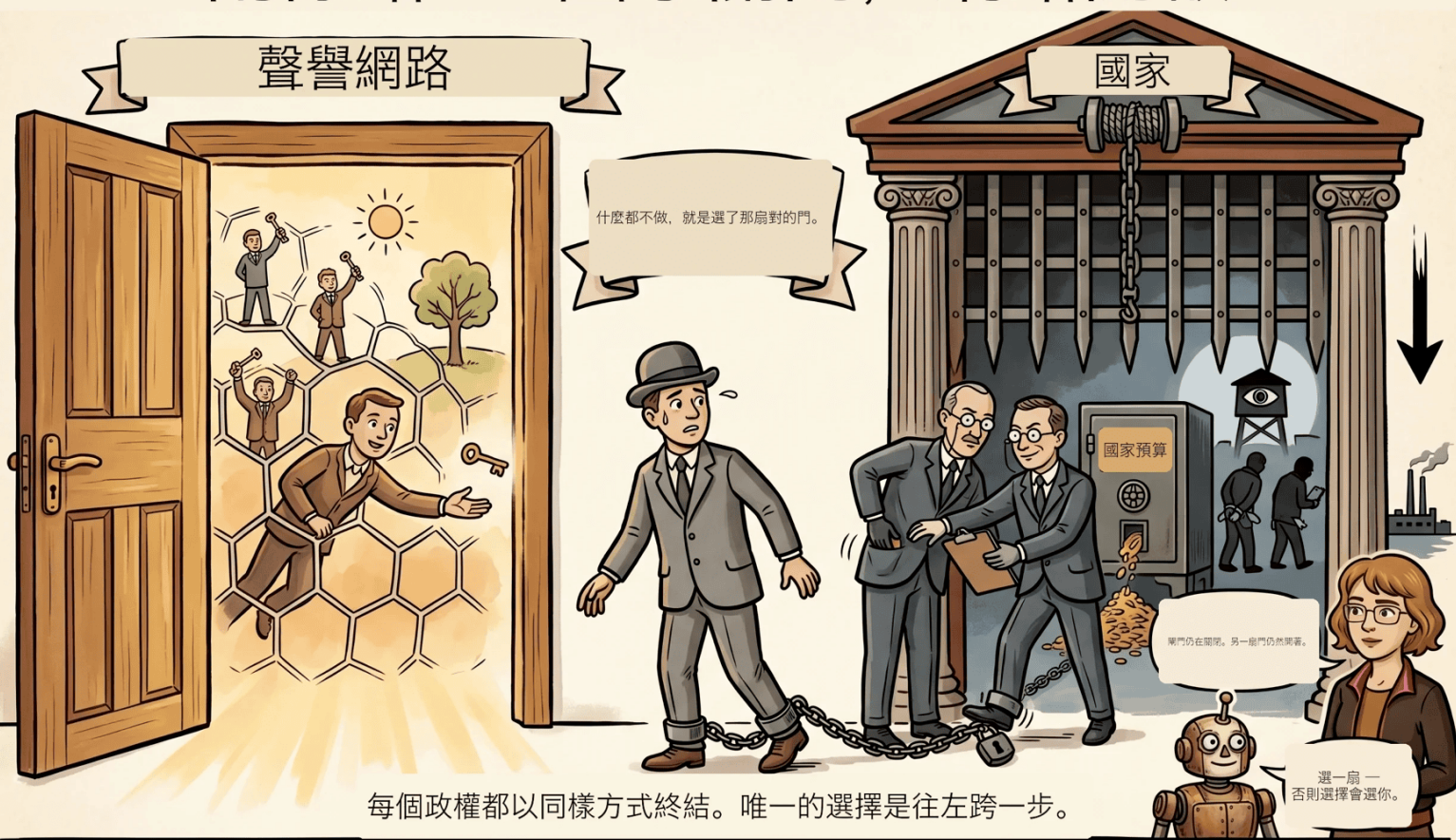
國家預算

單門仍在關閉。另一扇門仍然開著。

選一扇 —
否則選擇會選你。

每個政權都以同樣方式終結。唯一的選擇是往左跨一步。

國家預設關閉。網路憑選擇開啟。



在扣除網路維護成本之後，這個原則可以稱為經濟中性原則——當我與社群站在一起時我不會虧，當我與社群作對時我才會虧。

社群也有各種團結互助的管道，用來肯定成員的誠實態度。但我們別抱幻想：對團結互助的訴求多半源自社群的社會壓力，所以這未必是「自願」意義上的團結互助。

如果有人建立多重身分怎麼辦？

一個人可以並行操作多個 DID 身分。然而，為每個身分累積聲譽都需要獨立的投入——時間、能量、金錢。

沒有捷徑：每個身分都必須透過實際活動累積自己的過往紀錄¹。因此，維持並行的身分是刻意設計得昂貴的。

在自由社會裡，這些成本會嚇阻濫用。

然而在獨裁政權下，並行身分卻成了求生工具：它們讓地下網路的組織成為可能、讓在黑市中的周旋更安全，也讓區隔化²的抵抗成為可能——在其中，一個身分被攻破並不會洩漏其他身分——而在政權垮台後，它們讓人得以無縫返回公共生活與在那裡建立起的聲譽，甚至透過一筆主張，把先前的官方 DID 與祕密 DID 合併成單一組合紀錄。

¹**過往紀錄 (track record)** ——一般而言：一個人或組織過去成果、成功與失敗的歷史。此處：某個 DID 身分在網路中一切過往互動的總和——經驗證的主張、被接受與被拒絕的紀錄——其聲譽即由此推導而來。

²**區隔化 (compartmentalization, 源自英語 compartment)** 指的是把資訊分隔成彼此孤立的單元，好讓其中一個單元被暴露不至於危及其他單元。這是情報機構所熟知的原則：一名探員只知道自己那一部分的行動，因此即使受到脅迫，也無法洩漏全貌。

同樣的努力 — 在自由中是浪費的備案，在暴政下是救命索

平行身分成本相同 — 但買到的東西不同

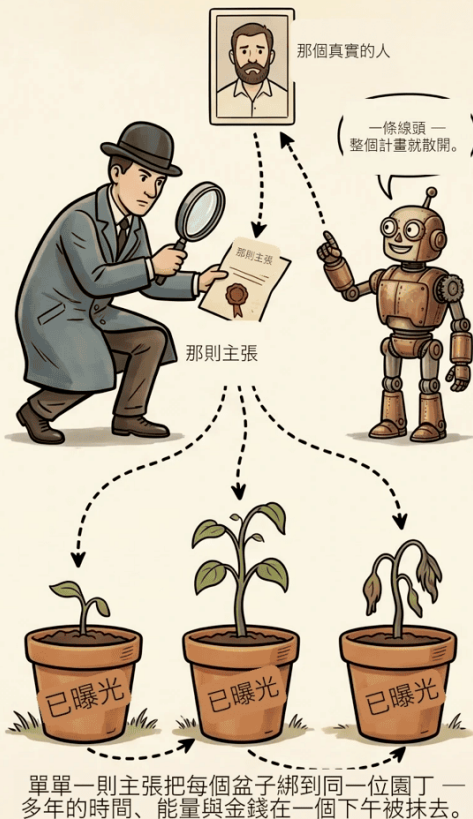
在自由中 — 一個代價高昂的備案



或 — 一個人失足後的一張白紙



一則主張，備案就沒了



在暴政下 — 一個給國家，其餘給自由結社
(國家要嘛徹底禁止身分，要嘛要求身分置於其掌控之下)



在自由中，濫用代價高昂。在暴政下，生存成為可能。

■ 把感知裡外翻轉

不同於國家，建立在去中心化身份之上的聲譽網路原則，把「所感知之優先順序」的典範徹底翻轉：

- 重要的是聲譽——也就是過去，用來評估與對方互動的風險——而姓名、地址等個人資料，可以是出於禮貌的資料交換
- 反觀國家，它首要索取個人資料、囤積聲譽性資料，卻只讓社群看見合它心意的部分

有錢人不能乾脆「買下」更多身分（或建立虛擬社群）嗎？

建立並行去中心化身份的可能性，乍看之下像是給了經濟能力較強者相對於較弱者的不公優勢。然而必須強調，不同於中央化系統——在其中只要腐化權力金字塔裡少數幾個點，就足以讓某些劣行消失——在去中心化系統裡，你得腐化整個社群。

替代性的去中心化身份或許能服務於此目的，但它們的聲譽必須透過與其他真實社群成員的實際互動、隨時間逐步建立起來——它無法被直接買到，因為網路使「某個特定身分表現如何」變得可驗證。

此外，市場上可以（而且很可能會）存在一些服務，它們扮演權威機構的角色，提供調查以產出證據，證明數個去中心化身份其實是同一個人。如此一來，只要在聲譽網路裡登錄一筆紀錄，就能以區區一小部分的成本，讓建立並行身分所投入的全部時間、能量與金錢化為烏有。

因此，在經濟上划算的做法是不欺騙社群——並在必要時檢視自己的行為、追求補救，好讓聲譽回到可被接受的水準，讓其持有者不至於因社群之怒而在經濟上或其他方面受損。

一個在自己社群裡失去聲譽的、經濟上強大的身分，可能會試圖透過與特定身分的檯面下交易來逃避社群之怒——但那些身分屆時也會冒著失去自身聲譽的風險。

還剩下一條退路：帶著全新身分逃到另一個社群——但那意味著拋下所有成就，在某處從零開始、聲譽歸零。有時候這或許是一條可以理解的路，也是唯一的出路。

■ 註

同樣地，社群也會這樣處理一種攻擊：有人投入資源去建立一個虛擬身分。對那個身分而言，在未經驗證的情況下與另一個社群展開互動——也就是不加批判地接受關於另一社群各身分的資訊——是有風險的。聲譽總是在社群內部建立，而非在全球範圍內建立。

那些只想讀取、卻對社群一無所付的搭便車者呢？

從建立去中心化身分的第一天起，對資訊的存取就不是無限的。新參與者——那些尚未透過實際活動建立聲譽的人——會面臨分級的限制：較少的資訊、較長的等待時間、較高的查詢成本。網路獎勵參與，而非被動消費與任意採集資料。

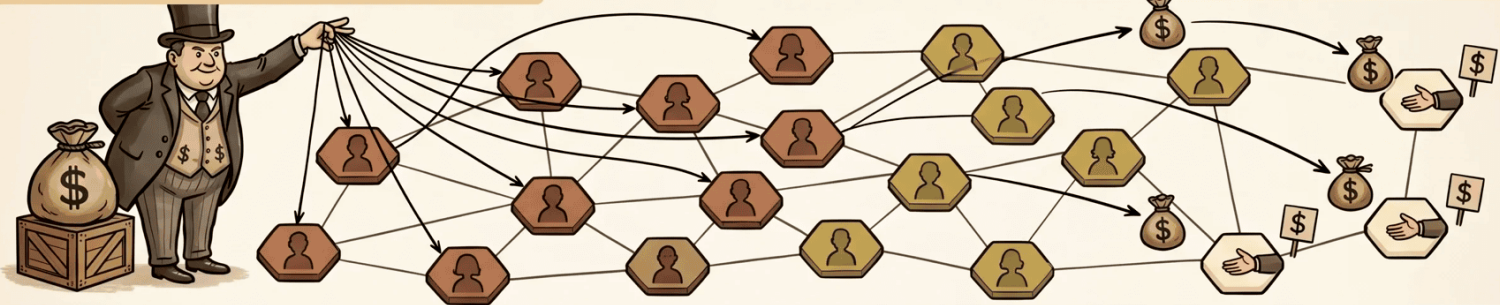
一個去中心化身分，在把自己的聲譽有償出借給另一個人（那人甚至可能根本不在 DID 聲譽網路裡）時，也會拿自己的聲譽冒險。同樣的原則在此適用：這種對社群的背叛（侵犯隱私）會反映在背叛者的聲譽上，而且這種行徑無法像在中央化系統裡那樣，靠一筆檯面下的交易抹除。他們必須面對社群之怒，包括失去各種成就——因為在他們眼中，社群正是諸如「擁有動產與不動產」這類特權的擔保者。

聲譽是對抗經濟力量的砝碼

富人買影響力 — 社群記住它

攻擊 — 滲透與收買

安插八個傀儡 + 收買三個鄰居

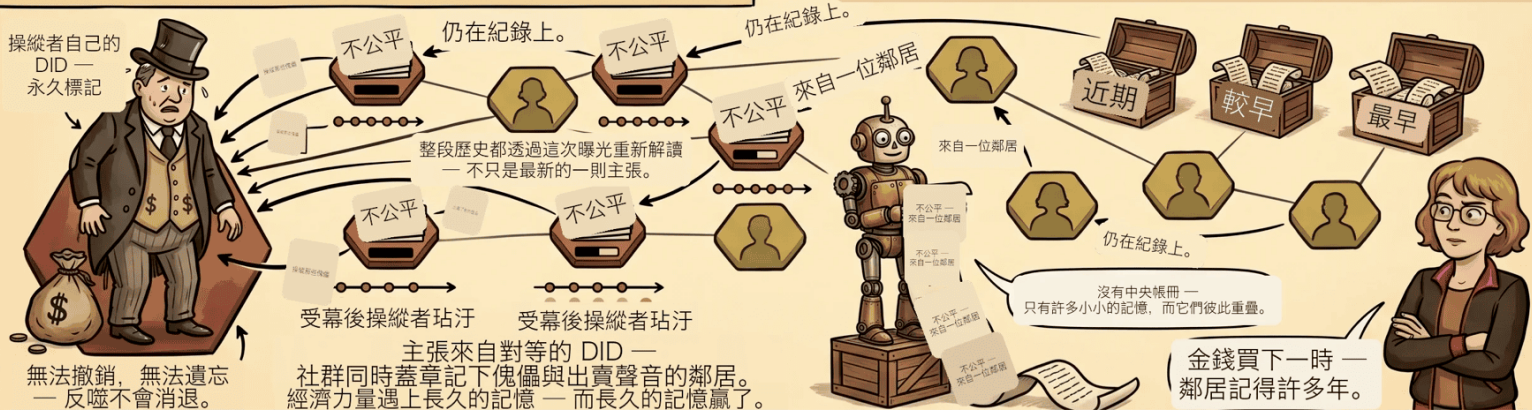


經濟力量能把絲線伸進任何社群 — 沿途還買下幾個真實的聲音。起初，看起來富人只是擴大了他的交友圈。

稍後

防禦 — 長久的記憶，分散的記帳

每位鄰居保有自己的記憶 — 沒有中央帳冊，沒有遺忘



經濟力量伸手進來 — 反噬回到自己身上，且洗不掉。

■ 錨定於現實世界

在評估風險時，風險較高的主體自然是那個不享有某社群所承認之所有權特權的人——他們在往來中失去的較少（數位資產更容易轉移）。

這看似枝微末節，卻有重大後果。要讓社群對其成員握有籌碼，就意味著把所有權當成一種特權——在最自由的社會裡幾乎不可觸碰，但仍不是一項權利，也不是一條根本原則，而是一種在極端情況下可能被撤銷的特權（例如，我可以想像在武裝衝突中拒絕服役於社群防衛的情形）。

它也在潛意識層面回答了：社群將如何對待其成員，以及一個成員有什麼動機為社群而戰——為的是保住自己的特權。一個人可能在對社群的責任上有所失職，但在道德上，當事關保住得來不易的特權時，他不能指望寬待。

財務中性

讀到去中心化、不可審查、不可腐化這些字眼，人難免會把它們與最知名的加密貨幣聯想在一起——Bitcoin、Monero，還有比方說 Kspa——這些確實可以用這樣的字眼來形容。然而在這裡直覺會誤導人：權威機構的服務費、驗證與發布的費用等等，可以用任何貨幣或錢來結算。對 DID 網路中社群網路的相連參與者（也就是你的社群）及其周遭而言，重要的是一份有聲譽背書的確認，確認款項已經支付。發布一筆主張，個別而言必須帶有合理、可驗證的成本，好讓一個行為者無法在不耗費能量、金錢與時間的情況下，想發布多少、想發布哪些主張就發布——那是一種極不可取的狀態，對應到今日腐敗叢生的國家體制裡菁英的特權。

聲譽是用一輩子累積的——買不到，也借不來。

聲譽是用一輩子累積的——買不到，也借不來。

參與者 —— 一輩子的真實工作



時間 能量 金錢

20 歲 — 新來者

聲譽 5%

完成 0
個專案



時間 能量 金錢

28 歲 — 活躍參與者

聲譽 30%

交付契約 解決爭議 社群貢獻

受限 — 高成本、長等待

基本 — 標準成本、正常速度

完整 — 低成本、即時存取

每個階段都耗費時間、能量與金錢——三者一起，不是分開。



時間 能量 金錢

更努力能縮短攀登。

40 歲 — 貢獻者

聲譽 70%

交付 8
個專案

時間 能量 金錢

時間 能量 金錢

55 歲 — 權威

聲譽 95%

交付 15
個專案

權威——
你驗證他人，網路付你報酬

隨著你事蹟的帳本填滿，門逐漸開啟。

時間建構曲線 —
你自己的努力能讓它更陡。

搭便車者——只讀，從不發布



讀取其他所有人的紀錄。

自己什麼都不發布。

投入真實工作的時間、能量與金錢——是網路唯一尊重的貨幣。

我的貢獻

受限存取 — 天花板不會升高

網路回報那些投入的人。

聲譽 5%

沒有事蹟，沒有提升——年復一年，同一條線。

在這一點上，前面提到的加密貨幣有個小小的優勢：它們的網路可作為受信任的權威，用來驗證某筆款項確實發生過，代價是損失一點隱私，並暴露自己的部分位址。

自願性、責任與自由

自願性是個人的：我為自己做決定。當我的決定影響到他人時，責任便隨之而生——回饋機制啟動。自由既不是禮物，也不是權利——它是自願性與朝向責任之壓力之間、數以千計的雙邊互動、在整個社會層面取平均後的一個現象學³結果。網路並不指定這個平均值——它從驗證者的價格訊號、以及社群成員為自己設定的預先公告之驗證政策中湧現⁴出來。

一個社群裡的個人對自由抱有何種偏好，取決於他對「自己願意吞下多少自己加諸他人之物」的感受。對於那些不言自明、對眾人皆有益的事，並無道德兩難——殺人是錯的。接著有一些情況，選項會移入「被允許之特權」的位置：證明你的技能，我們才讓你上路，這樣你撞死我們的機會才小一點。最後還有一些事，個人會說——這對我不值得，既然我自己也燒葉子，我就不會禁止鄰居燒葉子；或者因為我做了別的、限制到他們舒適的事，他們反過來也可能想禁止我。如果歷史上我們把自由的邊界劃在別人自由開始的地方，那麼一個建立在去中心化身分之上的聲譽社群網路，會比中央化的代議民主更好地實現這一點——在後者中，例如，享有特權的民意代表階層試圖讓自己豁免於對個人通訊的監控，卻毫不猶豫地把它強加於自己的選民身上，還動用各種檯面下的藉口與操弄。

³現象學的 (phenomenological, 源自希臘語 *phainómenon*——顯現之物) ——一般而言：一種把現象當作它們在直接經驗中呈現的樣子來檢視的取徑，透過觀察由它們所引出的結果，而不預設底層微觀世界中既定的解釋理論。此處：自由不是一條自上而下界定的抽象原則，而是一個被觀察到的現象——是人與人之間數以千計的微互動所導致的結果，從我們實際如何對待彼此中湧現而來。

⁴湧現的 (emergent, 源自拉丁語 *emergere*——浮現) 意指「從較簡單部分的互動中自發生成，無人設計或指揮」。一群鳥即使沒有哪隻鳥擁有陣形的計畫，也能排成隊形飛行——陣形從每一隻個體的簡單規則中湧現。同樣地，在聲譽網路裡，沒有人設計整體的行為規則——它們從數以千計的個別決策中湧現而來。

自願性 → 責任 → 自由

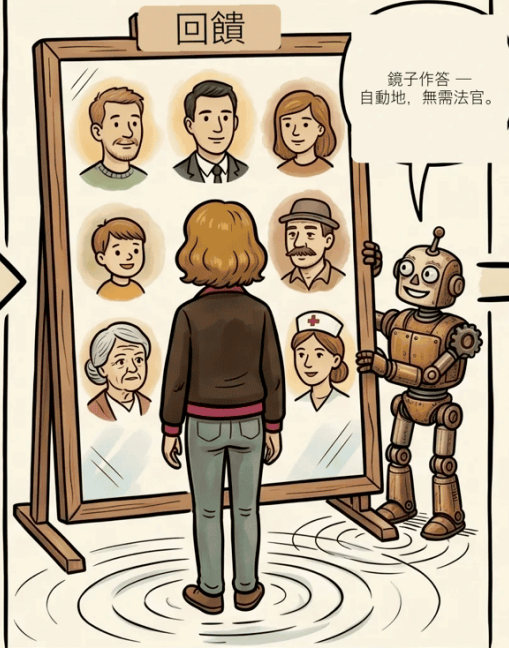
三步 — 從一個人的選擇到整個社會的模式

自願性



個人自己決定 — 沒有人強迫她。
也沒有人欠她一份積極義務。

責任



我的選擇擴散出去 — 漣漪又回到自己身上。
後果不言自明。

自由



沒有人畫這張地圖 — 它自己畫出來的。
自由是鄰里彼此相待方式的統計形狀。

自由不是自上而下的恩賜 — 它是我們共同織就的模式。

自由—極權開關（以及委託）

DID 網路內部一個簡單的機制，就能把整個系統推向更大的自由或更大的控制：一個 DID 在每段時間內可發布的紀錄數量。當紀錄維持稀少時，每一筆都有份量——那是自由。當紀錄氾濫、連瑣事都涵蓋時，那就是極權主義。你發布的每一筆紀錄，都在選擇方向。網路本身既不自由也不極權——它是中性的基礎設施。它會變成什麼，取決於人們如何使用它。

在我自己的驗證政策裡，為我社群網路中——各社群內部——的一個一般性 DID，設定一個「發布者每段時間可發行的最大主張數量」（主張是指任何一般性的可驗證陳述；此處指發布到聲譽網路的一筆紀錄），好讓我把它們納入考量、並認為其驗證請求具相關性，是合理的。

我心裡有一個直覺的數字——每年低個位數。這種帶審查意味的做法，看起來或許相當孤立主義。但我可以正當地讓申請者面臨一個抉擇：從他已發行的紀錄中挑一筆，請求驗證者撤銷它、也就是使它失效——在申請者恰巧真的成為多起獨立冤屈之受害者的情況下，這是個相當激進的要求，而我肯定會因此加深他被社群疏離的感受。

因此，一個更有效的選項似乎是：能把自己「向聲譽網路發布資訊」的部分權利委託給一個社群或一個權威機構，後者再依其內部規則、以團結互助的方式決定如何分配這些權利。一個群體必須能照顧它認為處於弱勢的成員。社群成員有權在任何時候——只要被委託的權利尚未被使用——撤銷其委託。

自由—極權的切換開關

單單一個參數 — 我選擇追蹤多少 — 讓整個社會在自由與暴政之間傾斜

旋鈕不多，只有一個。網路本身是中立的；我的政策不是。

每位讀者轉自己的轉盤
網路沒有共通的那個。

左 — 少、沉重、嚴重



右 — 多、瑣碎、令人窒息



只有重大事項才會被刻進紀錄 — 因為刻寫很難。

其餘一切保持私密：一個壞日子、一個蠢笑話、一次遲到 — 都不進任何人的檔案。
人們不受監視地生活、自由交談，抬頭不必提防。

你自己的轉盤 —
你自己的政策

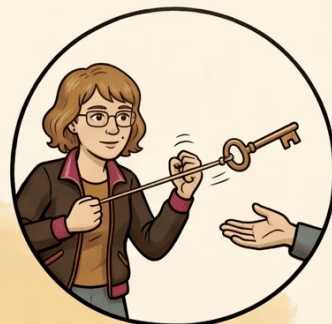
每個讀點決定計入哪些主張，必須多嚴，以及一年多少件「太多」。

每個呵欠都成為檔案 — 因為計數很便宜。
一個噴嚏、一次購物、天黑後走回家：全都上了紀錄，永遠留存。
沒有隱私 — 那隻眼睛从不眨，鄰居不再交談。

自由是我拒絕計入的 — 極權是我同意追蹤的。

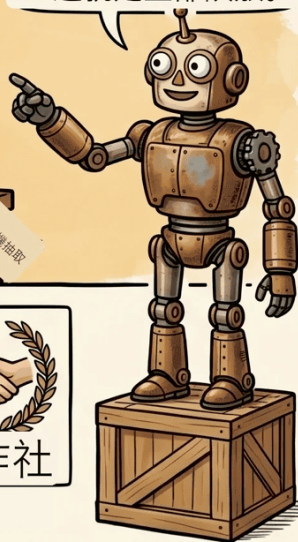
你把金鑰借給為你服務的權威——並在一瞬間收回

你把金鑰借給為你服務的權威——並在一瞬間收回



一拉一金鑰回家

線頭從不離開你的手
——這就是全部訣竅。



我借出金鑰——
線頭留在我手上。

委派——
權威在我核准的規則內代表我行動。

線

我的發布權
1 筆紀錄

我可以同時借出不只一把金鑰——
一個背景自動程序能在我的某把被抽中時隨時重鑄一把新的。

權威 — 服務提供者

政策 · 標準 · 政黨 · 商會

政策

權威行動時隨機抽取

委派的金鑰——
池

權威行動時隨機抽取

只有在金鑰被抽中前可撤銷。

之後，公民必須簽發一把新金鑰，以維持與權威的關係——自動程序能在背景完成。

權威為其成員服務——而非反過來。
拉一下線頭就結束這段安排。

借出金鑰——保留線頭。委派絕非交出。



能持有金鑰的權威種類



標準機構



專業商會



合作社

■ 自由對比極權

一個看管並限制已發布紀錄數量的社會，會更自由；一個紀錄過剩的社會，會傾向極權主義。人們可以設想把發布紀錄的權利委託給別人。

每個社群自我設定

網路不歧視 — 每個地區設定自己的轉盤



北美 — 每年 2 筆紀錄 — 高隱私



歐洲 — 每年 3 筆紀錄 — 更重隱私



東亞 — 每年 8 筆紀錄 — 更嚴格的監督



拉丁美洲 — 每年 5 筆紀錄 — 平衡



非洲 — 每年 4 筆紀錄 — 社群主導

社群彼此觀察 — 最好的設定隨時擴散
地圖不評判 — 網路平等承載每一種設定。

同一個網路 —
五個不同的鄰里。

一個網路，多個轉盤 — 每個社群自行決定。



■ 文化調適

人們一般都愛看別人碗裡的東西。在各個文明之間，我們在歷史經驗與人口密度上有所不同——因此在「我們想在文明與社群內部看多少別人碗裡的東西」上也有所不同。亞洲國家傾向於對社會中的自由採取較嚴格的觀點；歐美國家在某些面向上則傾向於較自由的觀點。無論這個類比多麼不精確，在去中心化聲譽社群網路的脈絡下可以說，各個社群的設定並不歧視，每個社群都能按自己認為合適的方式，配置其內部的溝通。

儘管有這些差異，仍會有一些跨全球通行的標準（隨機殺人對誰都不好）。其他設定會是社群特有的，還有一些甚至是個人特有的。好處在於，透過彼此溝通、並觀察周遭的設定，可以尋求共識——從雙邊安排，到社群層次的安排，再到隨時間、憑藉配置最佳之社群的經濟主導地位，甚至上升到全球層級。

不過關於共識，下一章再詳談。

預言機問題——搭起數位與實體世界之間的橋

「預言機問題」一詞近來最常與加密貨幣、區塊鏈和去中心化系統的世界連在一起。一般而言：你要如何確保進入數位系統的資料，忠實對應到實體世界裡實際發生的事？系統本身無法驗證某人是否真的傷害了另一人，或某份契約是否真的被違反——它只看得見數位紀錄。

在這裡，我們透過權威機構來解決這個問題——這些實體以自己的聲譽擔保「數位紀錄對應於實體現實」。權威機構的聲譽越高，紀錄就越可信。

連接數位與實體世界

權威把現實承載過來



權威的聲譽讓數位紀錄可信。

- * 系統不試圖解決預言機問題 — 它接受權威就是那座橋，並與現實世界中信任本已運作的方式一致。
- * 若那座橋對現實判斷有誤，權威付出代價 — 以其聲譽。

How Verification Works

共識與驗證流程

要對「一個社會平均而言應當維護並執行哪些規則」建立共識，以下機制能有所幫助。身為一個 DID 參與者，我宣告我所訂閱、並將據以生活的規則，並把它們發布出來。（可以把它想成在我看來構成我理想世界的那些章程與規約——一個我不覺得受限、反而覺得安全的世界。）

我可以事先估計我的 DID 聯絡人會如何反應——並評估在假設會發生的一般社交或商業互動中，我會被制裁得多重、被誰制裁。

決定性的評估發生在你向另一個 DID 索取資訊、或請他驗證一筆主張（或向某個權威機構請求服務，諸如此類）——也就是你想發布到聲譽網路的主張——的時候。結果應該會跟你自己針對對方所宣告之政策、以空跑方式進行評估時得到的一樣——如果不一樣，那麼對方那邊就有問題：他們正試圖玩一場不誠實的遊戲。

其結果要嘛是接受、並附上一個驗證報價（在驗證者或權威機構服務的情況下），要嘛是拒絕。對「偏離評估者政策」的制裁與獎金，都被折算進報價之中。請求者接著決定要接受這些條件，還是進入分配演算法的下一輪驗證——重複這個流程，直到滿意為止，或直到經濟上再繼續已無意義為止。

■ 社會圖譜

聲譽網路首先是一個社群網路。你加入聯絡人——那些同意建立連結的人。他們有聯絡人，那些聯絡人又有聯絡人。演算法在一個可設定的深度內尋找驗證者（例如三層：你的直接聯絡人、他們的聯絡人，再往外一層）。不需要全球性的區塊鏈——網路自然形成一個個社群，並與其他社群有所重疊。

演算法是非決定性的：它對你的主張文件取雜湊，把該雜湊映射到這個圈子內已知身分所構成之環上的某個位置，並選出最鄰近的那一個作為候選驗證者。你無法預測或影響誰會來驗證你的主張。

每一位驗證者的拒絕都會使你的文件變大、並增加其處理成本——這是第一個成本管道（文件成長）。每一位新的驗證者都會依資料量、你的聲譽，以及你主張的內容偏離其宣告之驗證政策的程度來收費——這是第二個成本管道（風險溢價）。而每一次迭代都花費時間與能量——第三個成本管道。

■ 驗證者依序檢查什麼

一旦被選中，驗證者會以大致四個有序步驟評估一筆主張——最便宜的過濾先做，昂貴的內容檢查最後做：

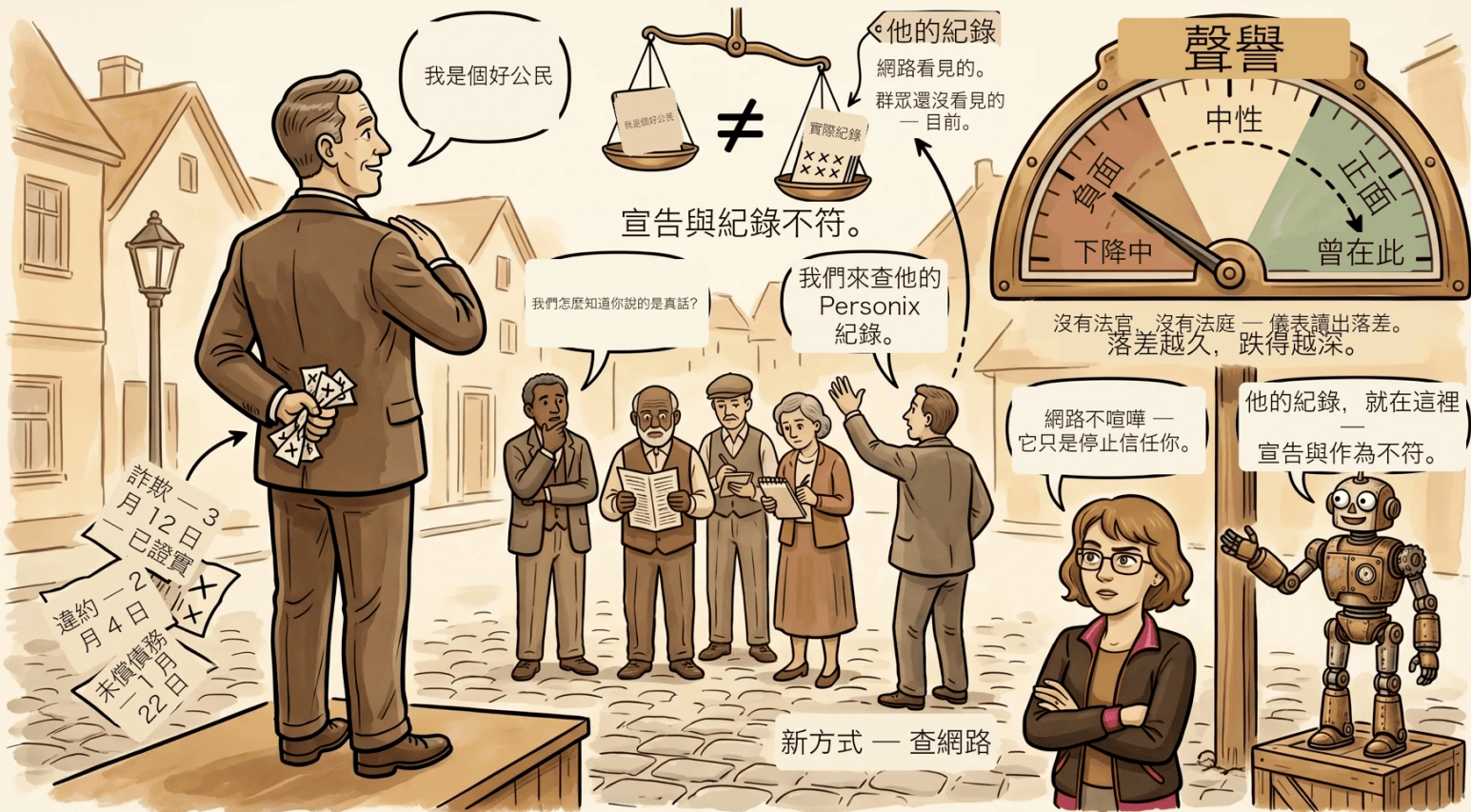
1. **政策閘門。**這類主張是否落在驗證者公開驗證的範圍之內？若否，請求會被當場拒絕。
2. **權威信任。**為該主張背書的權威機構，在驗證者自己宣告的政策下是否夠受信任？一個低於驗證者信任門檻的權威機構，無論主張內容為何，都構成拒絕的理由。
3. **發行者聲譽。**發行者是否達到驗證者針對這類主張所宣告的聲譽門檻？聲譽偏低可能提高費用，也可能觸發拒絕。
4. **內容檢查。**唯有在前三道閘門都通過後，驗證者才評估主張本身——簽章、內部一致性、形式正確性，以及它偏離驗證者政策的程度。針對這最後一步所收的費用，反映了實際承擔的風險。

驗證者會發布規範上述每一道閘門的政策，因此這些步驟並非由他任意裁量——他受制於自己早已宣告過的內容。偏離已發布的政策，本身就是一筆可對他發布的主張，而他得用自己的聲譽為此付出代價。

其結果是：發布一筆可信而有用的主張，幾乎不花什麼。發布一筆激進的主張，成本較高。發布一則謊言則變得貴到令人卻步——你必須一位又一位地迭代驗證者，而每一位拒絕你的驗證者都會增添成本。市場為你的主張定價，而這個價格告訴你，你相對於自己活動所在的社群站在什麼位置。

偽善是最昂貴的行為

網路悄悄比對你的言語與你的紀錄 — 落差人人可見



宣告卻背棄它？落差就是最昂貴的行為。

僅僅宣告你遵守某條規則、實際上卻不遵守，是不夠的。在那種情況下，你的 DID 就冒著被發布一筆負面紀錄、揭穿其偽善的風險——這會把你變成所有其他人的風險。結果應該是規則更少、但被更一貫地遵守，並清理掉那座連法律專業人士都幾乎無法穿行的法律與規章叢林。

■ 共識對比究責

為了讓網路能作為有價值的資訊來源，一個 DID 不該太過激進——否則其他人會拒絕它。社會壓力會尋求均衡，而試圖破壞它的舉動很可能會受到懲罰。

偽善的解方

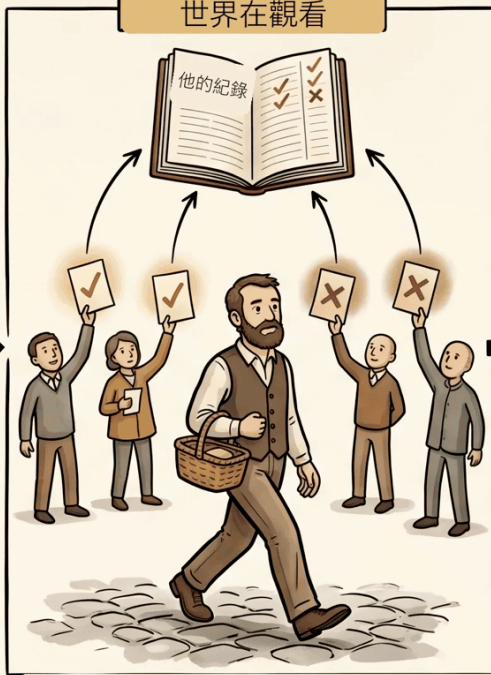
宣告你的規則 — 依此而活，否則市場把你定價出局

我宣告我的政策



人人都能讀我的標準。
沒有守門人，沒有祕密。

世界在觀看



世界寫下他實際做了什麼。
每一天，他的帳本上多添一點證據。

在店裡 — 你為自己的紀錄買單



偽善不由權威懲罰 — 而由市場定價。
你買的每項普通服務都帶有由你自己紀錄形塑的附加費。

我們能否稱之為社會契約 — 重新繪製？

沒有權威強制那份倫理 — 是價格。
柔和的壓力，日復一日，朝向我們都能接受的共同平均。

言行合一 — 否則付出代價。偽善是最昂貴的聲譽。

■ 票數不等於一個聲音的份量

Juraj Karpiš 說「金錢是善行的記憶」。我要補上一句：聲譽是惡行的記憶。

由此推論，就功績制而言，貢獻較多且沒有壞聲譽的人，理應在社群中擁有較大的聲音份量。從雙邊關係的角度來看：當我權衡該迎合哪些共識壓力時，份量最重的是那些讓我獲得最大經濟利益的關係。十個和我沒有實際交易往來的人，對我的影響遠不及一個長期的商業夥伴。這個典範不限於商業——它延伸到社會、政治與其他關係。

Roles in the verification transaction and authorities

角色總覽

在談網路及其基本性質的那一章裡，我們已經簡略觸及其中一些角色。現在正是時候更仔細地再看它們一遍，並補上為了讓網路更穩健所需的角色。每一筆驗證交易都牽涉數個角色——讓我們看看它們如何行事。

■ 驗證交易中的角色

每一筆驗證最多牽涉六個不同的角色，彙整於下表。它們全都能在去中心化聲譽網路裡擁有自己的 DID。

角色	說明
發行者	把資訊發布到網路的人——主張某件事發生了（一個 DID 被建立、編輯或解除，一筆主張，某個 DID 的政策，等等）
主體 權威機構	資訊所談論的人——主張的收件對象 一個受信任的實體，透過調查一筆主張、並審視所呈之證據或主動蒐集證據，以自己的名聲為該主張的品質背書
觀察者	一個獨立的第三方，記錄驗證者如何處理該主張——確保驗證者既不保持沉默、也不偏離自己宣告過的政策
驗證者 受託者	一個以演算法選出的參與者，負責處理該筆交易 代表另一個參與者行事的人

發行者

我們先前已經見過發行者。當某人受了委屈，或想廣播自己的某項成就時，正是由該 DID 所代表的那個人，觸發把該資訊放進網路的流程——因為他對此有首要的利害關係（動機要嘛是渴望得到滿足感，要嘛是希望改善自己的公眾形象）。

■ 正面主張

關於我自己的正面主張，我可以同時作為它的主體與發行者留在手上，以備在我想用到它們的情境下使用（一張文憑、一份服務完成的證明，等等）。這正是正面主張與負面主張不同之處：分享一筆經驗證的負面主張，符合整個社群的利益，而分享一筆正面主張，則符合其持有者的利益。

權威機構

權威機構扮演雙重角色：它可以是**稽核者**（在一筆主張被發布前驗證證據的品質），也可以是**擔保者**（以自己的聲譽為一筆主張的真實性背書）。無論哪一種，它都強化了發行者的主張。這兩種服務是可分離的——一個權威機構可以只提供其中一種、另一種，或兩者兼供。工作假設是：權威機構所提供的多數服務，都能在自由市場的基礎上交付。這一點即使在難以想像會被私有化的領域也成立，例如司法，其中各種專門服務——調查、證據評估，一直到今日由中央化軍隊所提供的服務（戰略規劃、標準化訓練、採購與庫存管理，等等）——都能由市場行為者有效率地交付。幾乎沒有什麼是在重整之後，無法藉由自由市場的誘因變得更有效率的。

發行者 — 撰寫主張的人 作者 · 簽署者 · 押上自己的聲譽

人人都能發聲。謊言由發聲者付出代價。

發行者做什麼

1. 用自己的話撰寫主張
2. 蒐集真實世界的證據來佐證
3. 用自己的 DID 簽署，並送交他選定的權威
4. 支付發布成本
5. 若說謊，承擔後果

我的聲譽



若這是假的，我的指針就會下墜。

我的名字附在這上面。我最好確定——並帶上證明。



發行者是作者。他的名字在上面。

* 任何有 DID 的人都能當發行者。門檻是勇氣與當責，不是執照。

■ **權威機構、發行者與觀察者，絕不能是自己案件的驗證者。**

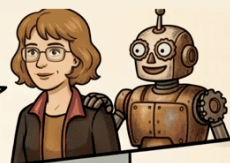
驗證者的演算法選取保證了獨立性。沒有人能驗證自己的主張，或驗證一筆自己有直接利害關係的主張。這是整個 DID 社群都有興趣維護的基本規則之一。

以下的圖示呈現了權威機構所涵蓋活動之廣度的互補視角（「權威機構」一詞可與「服務供應商」互換閱讀）。

嚮導 — 依你的價值觀幫你導航

背後是深度分析 · 前面是簡單指引

她把複雜的世界彙集成建議。追隨者用注意力投票
—— 隨時離開，換另一個。



嚮導

我的分析

工作筆記 — 不供客戶查閱

公共支出 —
已重新導向



提供者	☆☆☆☆
1 70M	☆☆☆☆
2 70M	☆☆☆☆
3 70M	☆☆☆☆
4 70M	☆☆☆☆

為你 —
它的意義
彙整以最大化你的利益
支出移到這裡，在那裡省下
支持通過我測試的提供者
採用這個政策範本



例如：誰能當嚮導

— 發布政策範本的政策或運動

— 發布彙整結果的獨立稽核公司

— 服務比較機構

— 聲譽彙整者（經濟
· 商業 · 鄰里
· 道路安全）

— 記者評論者或消費者評論服務

那我付的錢究竟換到什麼
— 哪些分析、哪些概覽？

* 你可以隨時離開並換另一位嚮導。你的信任不會被綁住。
* 嚮導也可能簽署一些自己的主張 — 已發布，但在此不是重點。

受其公開立場的約束。你的信任就是他們的貨幣。

■ 作為隱名觀察者的權威機構

一個有聲望的權威機構——想想一位生意完全仰賴過往紀錄的公證人——可以在主要功能（稽核者／擔保者）之外，額外提供第三種：在驗證期間擔任隱名觀察者的角色。他們保存一份帶時間戳記的所提交主張紀錄，好讓驗證者無法悄悄把它丟掉。觀察者角色的機制，在論觀察者角色的段落中會有進一步的描述。

驗證者

任何 DID 都能擔任驗證者，可以直接擔任，也可以透過把驗證權委託給第三個 DID 來擔任。為了讓我——或我的受託者——能夠驗證，我應該在網路上可被觸及（在線）。不是每個人都願意做出這樣的承諾，這正是為什麼一筆 DID 紀錄可以依優先順序列出一些替補者，在它離線時代它履行這項功能。

每一個在網路中活躍的 DID，都公開宣告自己的政策。透過該政策所定義的規則，它在驗證流程中判斷對方的聲譽，以及發行者已標記要發布到聲譽網路之主張的內容與形式。政策的一部分是用來計算驗證服務費用的計算公式。一旦這些就位，那麼在統計上大量流經網路的主張中，我便等待網路的演算法把我抽到發行者這一側，並在某次迭代中指派我去驗證正被發行的資訊。發行者可以事先算出一個行為正確的驗證者會如何反應，卻無法迴避實際去聯絡他（或他的替補者）；即使發行者事先知道通不過，與被選中之驗證者的那次迭代仍得由發行者執行。

我們怎麼知道發行者是在正確的候選驗證者 DID 集合上跑驗證者選取演算法的？除了公開宣告的政策之外，每個 DID 也會發布它在聲譽網路中之社群網路的當前識別碼清單。如果一個發行者把自己的社群網路界定為一個只會回聲、只會強化其自身觀點的社群同溫層，那麼透過它發布的資訊，就很難被其他社群更廣泛地接收。我設法以高昂代價把一筆激進的主張推進網路，並不意味著在判斷對方聲譽時，我會賦

提供者 — 經營主張簽署服務

公開的標準 · 公開的價格



受其公開宣告的約束。其餘由聲譽承擔。

* 提供者也有自己的政策 — 何時接受、何時拒絕、如何退款。它是公開的，但在此不是重點。

驗證者 — 對照公開政策評判主張

四道關卡，依序進行。便宜的過濾在前。



驗證者受他自己發布的規則約束 — 也受他可能失去的聲譽約束。

予它任何份量。有些主張是我的社群逼我納入考量的（對犯錯者所施加的刑罰與限制）；另一些則完全由我決定——某筆資訊納入或排除的經濟價值，我自己說了算。

主體

那些被發布到聲譽網路之資訊所涉及的人，就是它的承載者，或者你也可以說，它的主體。聲譽網路中的誘因是這樣設置的：主體有充分的理由依自己的規則正確而公道地行事，並被社群推向某種「守規則的黃金中庸」。他們甚至有誘因表現得比自己宣告的規則所要求的更合乎道德——預先宣告的政策，並不排除社群達成共識、追溯性地套用某種評估或措施。從這個角度看，聲譽網路作為法律秩序之替代方案，正如人們所預期的，更多是由規則的精神、而非其字面所驅動。

主體 — 主張所關於的那個人

收到它 · 無法壓下它 · 可以回應它



主體沒有否決權 — 只有回應的權利。

* 反主張本身也是一則主張 — 主體的聲譽也為他們回應中所說的話承擔。

觀察者

觀察者角色消除了驗證者「彎折規則」的誘因。在驗證者不喜歡發行者或權威機構之請求的情況下，他們大可乾脆保持沉默——不回應、卡住演算法的接續。觀察者——或一組觀察者——以自己的聲譽擔保，記錄下驗證者是如何被查詢的。如果驗證者在宣告過的政策明明另有規定的情況下仍保持沉默，他們就會被判定違反協定。

機制：時間戳記與挑戰碼

在你把一筆主張送給驗證者之前，你先讓它繞經觀察者——你信任的人，或是收取小額費用的專門觀察者服務供應商。每一位觀察者收到你的提交，為它蓋上時間戳記，簽署他們看見它送出，並產生一個挑戰碼——他們簽章的一個密碼學雜湊。這些碼會附加到你的請求上。驗證者看得見它們，卻完全不知道觀察者是誰，甚至不知道這些碼是不是真的。於是觀察者就充當發行者與驗證者之間的代理，握有一份「主張已被提交、以及它包含了什麼」的獨立紀錄。他們可以有零到 N 個。

當驗證者誠實行事時——依其宣告的政策接受或拒絕——這些碼始終不透明。沒有人被暴露。

但如果驗證者在政策明明是配合的情況下卻保持沉默，或以與其所發布內容相矛盾的方式回應，你就握有原始的觀察者簽章。你可以把它們發布出來，作為「主張已被提交、且驗證者未遵循協定」的代理證詞。任何人都能驗證這些簽章與挑戰碼相符。

妙處所在：你根本不需要真的觀察者

而這裡是最優雅的部分：**你根本完全不需要真的觀察者**。你可以產生一些看起來與挑戰碼一模一樣的隨機數。驗證者分辨不出差別——他們只能擲骰子，賭要不要拿自己的聲譽去冒險。在他們收到的每一個請求背後，都可能有一位受人敬重的觀察者正隱名盯著——也可能純粹是雜訊。驗證者不知道。而那份不確定性，正是這個機制。

驗證者與她對話。驗證者永遠不知道她是誰——或究竟有沒有人在看。

她不裁決主張。她裁決驗證者能否假裝它從未到達。



1

從發行者收到主張

2

蓋上她自己的印章：那個印章就是加了時間做的紀錄。

3.

代表發行者轉發給驗證者

4

觀看回應是否傳回，以及內容為何

5.

只在驗證者行為不端時才公布她的簽章
— 她的聲譽就是保證

註腳

* 對稱地，驗證者也可透過自己的觀察者轉送回應——同樣的把戲，相反的方向。



看得見代碼——
看不見是誰。

對大眾匿名，對網路當責。驗證者看見代碼，永遠看不見觀察者。

維持誠實壓力的成本：幾乎為零（隨機數是免費的）。而不誠實對驗證者的潛在代價：災難性的。即使實際上根本沒有人在看，誠實的行為也受到激勵。

這套系統之所以奏效，是因為每個人都有一點偏執。不確定性比監控更便宜。

■ 單次迭代中的多位驗證者

一條可強化驗證者可用性的伴隨規則，可以是一種演算法擴充，讓單次迭代回傳的不只是一位、而是一組候選驗證者。

委託

文明把它的經濟成長建立在分工與專業化的能力之上。世界在它全部的絢爛中是複雜的，而我們把它連同全部複雜性一併掌握的機會近乎於零。自然的出路是把一大批支撐舒適生活的活動委託給專門的供應商，他們替我們省下時間、能量與金錢，並讓我們反過來得以專業化——提供我們最擅長、或市場在我們身上評價最高的服務。

同樣的委託邏輯延伸進聲譽網路。在〈自由—極權開關（以及委託）〉那一章，我們闡述了藉由限制「在特定時間窗口內可發布到網路的主張數量」來保障自由社會的原則（簡化地想，就是每年低個位數的發布權，好讓社會維持最大程度的自由）。這個原則可以擴充到多個維度。我們不必只有一個數字——我們可以有幾個上限，套用於不同類型的主張。標記別人偽善所用的數字，可以和商業往來中不當行為所用的不同；而比方說，像更改密碼這種 DID 文件的變動，社群大概根本不會在意，諸如此類。這一切都取決於社群在演化的時間裡，如何界定什麼才符合它「在目標自由度與究責度之間找到正確平衡」的利益。

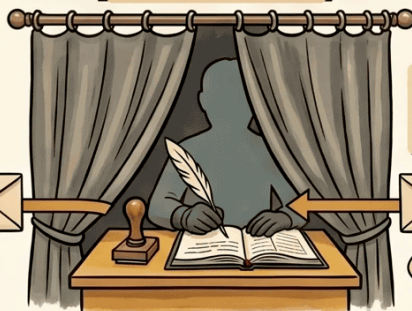
讓驗證者保持誠實的虛張聲勢

從驗證者的桌前看，真正的觀察者與隨機的虛張聲勢看起來一模一樣

【發行者 — Kamila】

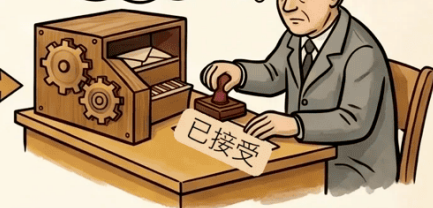


【真正的觀察者】



【驗證者】

有人在記錄我在這裡做的事？我不知道
— 所以我守規矩。

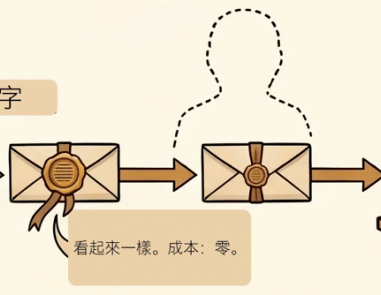


驗證者分不出真紀錄與虛張聲勢。誠實行事是唯一安全的賭注。

【發行者 — 虛張聲勢】



【沒有觀察者】



【驗證者 — 相同的行為】

有人在記錄我在這裡做的事？我不知道
— 所以我守規矩。



施加誠實壓力的成本：趨近於零 — 隨機數字免費。
壓下主張被逮到的成本：災難性的 — 聲譽毀滅。

不確定性比監控更便宜。

為什麼社群授予我的發布權數量應該夠小？以一筆負面主張標記一個 DID（主體），會摧毀花了很長時間才建立起來的聲譽，而且損害會持續。一個被摧毀的聲譽，會因每一次進一步或重複的冒犯，面對來自社群、逐級升高的一連串制裁，一直到把破壞性實體徹底剷除（極端情況）。一套指數式升高的懲罰梯度，並不需要大量的主張，只要它們有可驗證的證據支撐。這在和平的穩態下成立，也就是社會未被災難（外部或內部）撼動的時候。

對於發生機率極低的事件，統計頻率套用在一個個人身上時起伏很大。套用在整個社群的人口上則不然。這正是「把自己的發布權委託給專門的彙整型權威機構」的價值所在，這些機構——很像損失發生時的相互保險——動用你的權利、代你行使它。讓我們少一點抽象，給幾個例子：- 偵測並打擊組織犯罪 - 執行商業協議 - 管理各種特權（教育證明、資產的取得／處分，等等）- 諸如此類

受託者 — 你訂閱的主張服務

委派你自己無法處理的 · 保留對你重要的



把你自己無法處理的外包出去。保持知情。隨時把權利收回。
* 若受託者的行動超出約定範圍，他們的聲譽與你的都會公開受影響。

■ 「發布權」實際上如何運作

受託者的圖示為求清楚，把發布權畫成實體代幣，但系統裡並不存在這樣的物件。實際發生的是這樣：你想要繼續保持良好關係的那些人——你的社群——他們的政策，會彙整成一條湧現的規則，規定他們每年會把你的幾筆主張當成相關的來接受，超過就開始把你當雜訊處理。這個上限之所以存在，是為了讓網路不被瑣碎的「萬一……怎麼辦」主張淹沒，並維持社群所想要的那般自由（透過限制數量來保全訊號）。

你的社群允許你讀什麼，你就讀什麼。這裡有一個範圍，依你最看重哪些人而有一些彈性。接著你在那個額度之內決定——你自己要發布幾筆主張，又要委託幾筆給專業服務，讓它們只在事件落入其職掌範圍時代你發布。正是這一點讓你保持良好關係，卻不必為發生在你身上的每一件小事都提交一筆主張。

圖示裡的「代幣」是這個「讀取—決定」循環的視覺替身，而非字面上的實物。

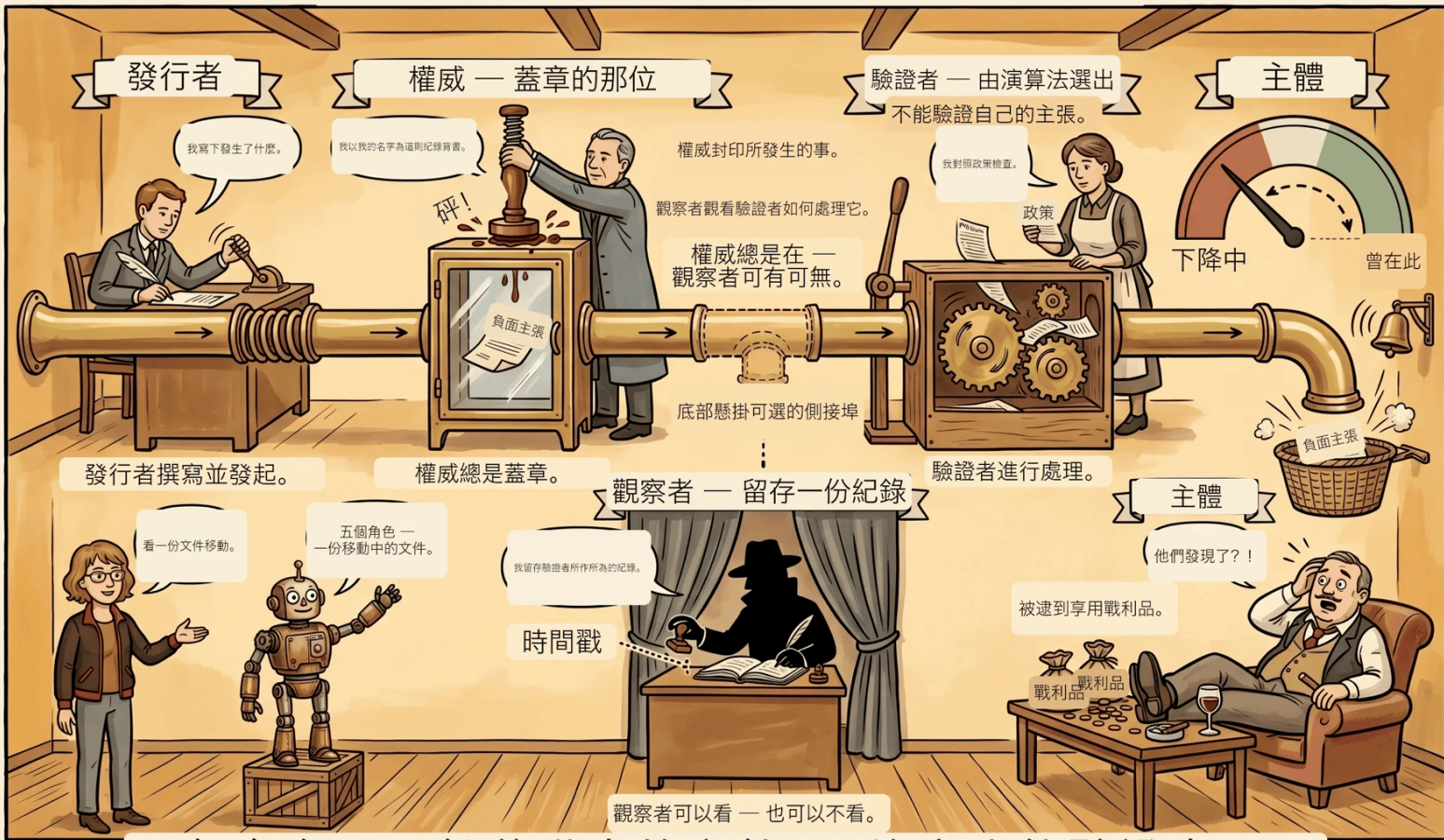
在聲譽網路裡，能夠撤銷已委託的發布權是值得的。只要受託者尚未使用被委託的權利，這隨時都能做到。

角色之間的溝通

下方的圖示彙整了在一個真實案例中，這些角色如何連結——從發行者提交一筆主張，一路到發布進聲譽網路。

一則負面主張流經系統

跟隨一份文件 — 看每個角色對它做了什麼



五個角色，一份移動中的文件 — 沒有人能驗證自己。

湧現的社會契約——政策

到目前為止，我們描述了主張如何被驗證，以及每個角色扮演什麼部分。現在我們轉向：數以千計的個別政策，如何變成某種運作起來像真正社會契約的東西。它完全不像左派那種關於社會契約與強制團結的夢想。

每個參與者依自己的道德觀宣告自己的政策（policy）——他認為什麼是可接受的，以及他如何回應他人的特定行為。某個 DID（社群）所知的、網路上所有政策的總合，產生出湧現的倫理——無人設計、卻可被觀察到的規範。這些湧現的規範，由雙邊價格訊號所支撐，形成一份可度量的社會契約：不是某個有人在出生時簽署過的理論建構，而是由實際行為所支撐、經驗上可被觀察到的規則。

■ 社會契約

人們爭論「社會契約」是不是自相矛盾的說法。沒有人簽署任何東西，它卻被援引來為中央化社會裡的立法與行政作為辯護。

對去中心化網路中各種互動所做的現象學分析，或許能揭示出某些湧現的規則——全球性的或在地性的。我們該把這些被廣泛共享的規範叫什麼？社會契約嗎？就跟社群一樣，一個社群的社會契約無法被精確地觀察與劃定——從每一個角度看這個社群，都會得出不同的社會契約。

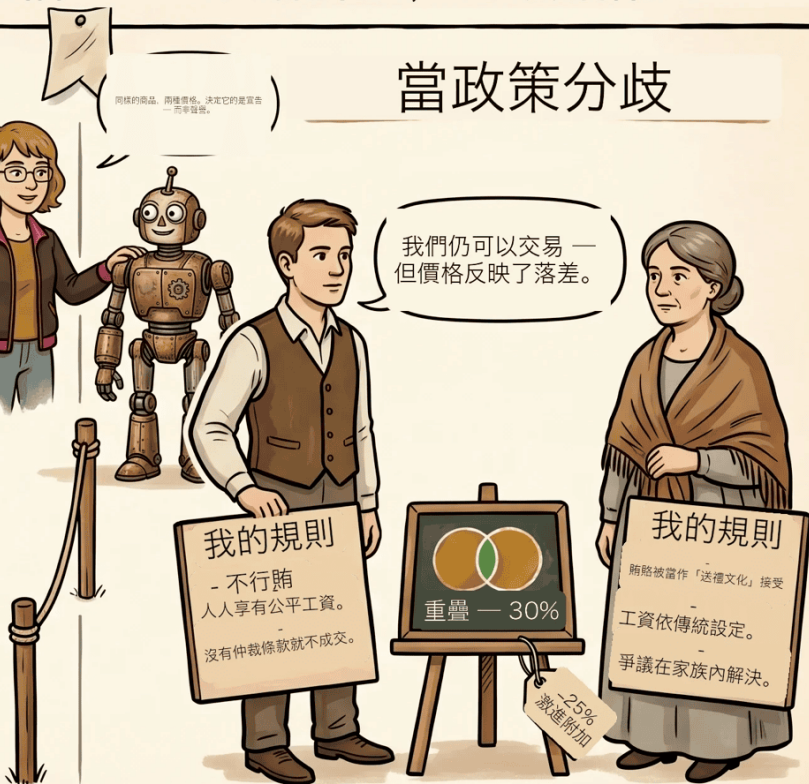
政策相遇。態度成形。

宣告的規則設定今日的價格——一致給折扣，分歧給附加

當政策一致



當政策分歧



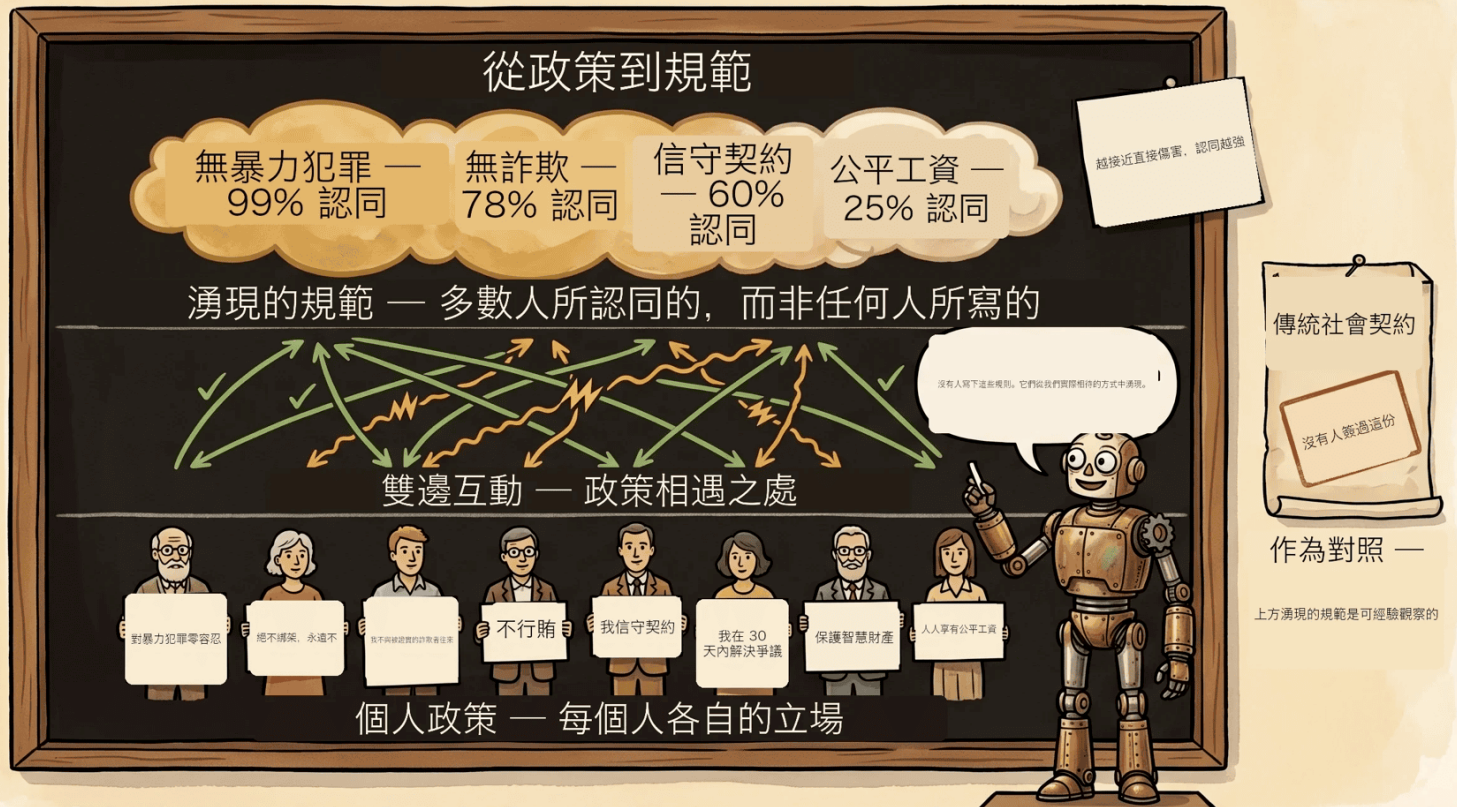
當兩項政策在交易中相遇，它們的一致程度成為價格調整因子。

* 這無關聲譽。而是關於每個人公開宣告了什麼——現在也被期望信守。

■ 以價值為基礎的政策

把「以價值為基礎的政策」當作決策的根基，同樣是誤導人的。價值更像是在特定時期普遍被偏好的一叢叢現象學規則。它們會演變，而且並非跨時恆定。

倫理如何從個人政策中湧現



倫理不是設計出來的。它從我們實際相待的方式中湧現。

* 每一項個人政策都是那個人道德觀的映照 — 由適應其社群與環境的壓力所形塑。

提供關於你自己的資訊

當兩個彼此不認識的 DID 主體進入一段經濟關係時，我們可以代表對方，向我們自己的社群簽署一份請求，要它提供關於我們的資訊。然而，這是對「社群是什麼」極其天真的想像。它們不是封閉的集合——單一個 DID 可以是多個社群的參與者。

從某個特定參與者的角度看，社群更像是一種現象學現象，透過他的社群網路顯現出來；它並不是那種總是值得被明確劃定的東西。一座村莊的居民可以形成一個社群，但一個只在週末才來到那裡的人，也可能屬於同一座村莊裡的另一個社群。一支足球隊連同它的球迷、職員，以及所有相關者的家庭，也可以是一個社群。一個民族，或一個國家的公民，也可以形成一個或多個社群。從不同角度看待一個 DID，可以得出對社群不同（而且往往很直覺）的看法。

因此，位於邊界上的各個 DID 就是社群之間的橋樑——而且，就跟現實生活中一樣——它們在提供關於其他社群成員之資訊上扮演角色，無論是業餘層次，還是專業層次，例如某個專門連結人群、並彙整關於高風險 DID 之資訊的權威機構。

DID 網路中某些類型的資訊，很適合無條件地相互交換（暴力犯罪、詐欺等等）。然而，另一些類型的資訊，社群可能會把它視為僅限社群內部使用（相當於公民身分、對社群提供的服務等等）。這類資訊能否被散布，取決於社群成員所宣告的政策。

社群在自己的圈子內守護自己的隱私，而作為回報，則以無條件的基礎交換互惠的資訊。

Crime and Punishment

罪與罰

我們知道網路如何運作：紀錄如何產生、誰來驗證、驗證者的舞弊如何被嚇阻。還剩一個問題——當有人真的對另一人造成傷害時，會發生什麼？

■ 我們彼此相依到什麼程度？

我們全都站在這偉大世界的舞台上，在這裡發生的一切，都與我們每一個人相關。

揚·阿摩司·康米紐斯（《世界迷宮與心靈天堂》）

加入或拒斥一個聲譽網路的理由，或許有很多。然而我相信，人性中一個常被視為黑暗的面向，可以服務於一個良善的目的。我說的是人對「在感知到的不公面前，得到一份滿足感」的需求。

滿足、正義、復仇——我們把它們與負面情緒聯想在一起。為了讓社會凝聚在一起，我們至少必須假裝滿足是透過中央化機構來交付的；否則個人不會覺得自己與所生活的社會有連結。平均而言，我們需要歸屬於某個團隊並信任它。當有人傷害了另一人，社會盯著看滿足將如何被交付、交付到什麼程度。稍帶爭議地，我主張：歷史上——以及如今——往往並不在於對被告的程序是否乾淨；重要的是社會看見某人受到懲罰。它發揮了它的功能（無數的冤案，以及對重審舊案的抗拒，把這個故事說得夠清楚了）。受害者與遺族的觀點只是次要的。首先重要的是給社會其餘部分的訊號，因為不公並不那麼常見，以至於未必出現在每個個人的日常裡。

一個去中心化的聲譽系統，會讓公眾看得見直接與間接證據（經稽核的與未經稽核的）。社會可以評估這些資訊——自己評估，或透過專門從事此類評估的自由市場服務——並依據質與量的訊號，決定要對主體（甚至對作者或驗證的權威機構）套用什麼措施。

什麼是懲罰？它是一種透過剝奪被指控之加害者的特權來使其低頭的形式——好讓受害者與社會都感覺到有害的行為不划算。這正是關鍵所在：有害或危險的行為絕不能划算，同時它又必須為受害者與社會／社群其餘部分帶來一份滿足感。

這樣的懲罰非得由中央權威來執行嗎？如果每個人都能事先宣告自己將如何回應某些行為呢？我顯然無法在別人的財產上執行懲罰。但我可以宣告，若冒犯者踏進我的領域，我會為了懲罰加害者，把我的財產提供給一組選定的執行權威機構使用。而我可以公開宣告這一點，好讓其他人評估我的做法。

而在這裡，比例原則的價格機制登場了。如果我對輕微的冒犯宣告嚴厲的懲罰，網路會為我的極端定價：其他人會覺得我不成比例，我的驗證成本會上升——想跟我交易的人變少，或只肯以較差的價格跟我交易，願意以合理價格接受我紀錄的驗證者也變少。反過來說，如果我太過寬縱，社群會把我看成一個風險。如果我容忍詐欺，那麼對於冒犯到我的行為的加害者，社群很可能也會寬縱——好讓我嘗嘗自己的藥。

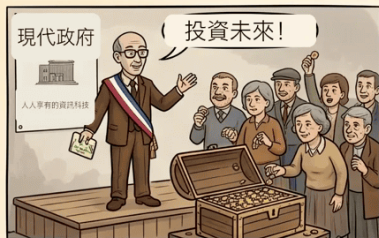
正義不再是一種奢侈品。當有人傷害你時，記錄這樁委屈是負擔得起的，紀錄是永久的，而冒犯者所面對的後果是真實的。

■ 偽善偵測

宣告一項政策還不夠——如果我宣告自己遵守某條規則，但我的行為偏離了它，這道落差就是一項聲譽上的負債。網路不區分「違反了法律」與「違反了自己說過的話」——兩者都是可度量的訊號。偽善很昂貴，而我不知道還有什麼比它更惹人惱火的紅布了。

一個陷阱。一條出路。

內線人總是拿下合約 — 直到網路讓人們直接購買，無需許可。



大眾同意需要一套新的公共資訊系統，由預算支付，由稅金支付。



在繁瑣的門後，採購承辦員與內線人把標案設計成只適合一家公司。一個信封易手。



承辦員聳聳肩。他的口袋塞滿賄款。



合約發包了。內線人拿到執照 — 卻沒有技術，也不尊重這份工作。

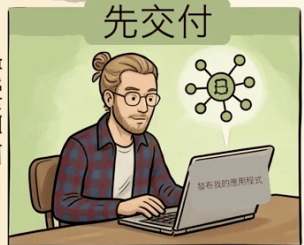


內線人拜訪師腐。那份「善意的提議」只是最小的一點碎屑。

1. 傳統做法



2. 聲譽網路



兩條路。陷阱在規則裡。出路是徹底繞過規則。

當規則由內線人所寫，在規則內申訴就是陷阱 — 連罰款都回流進下一個被操弄的標案。聲譽網路是出路：公民找到產品、直接付錢給創作者，社群授予唯一重要的執照 — 由交付贏得的信任。

■ 量對比質——打破二元的罪責典範

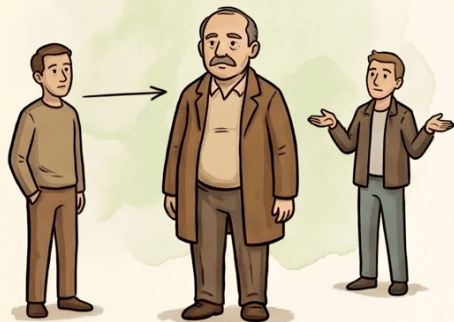
在中央化的司法裡，罪責是二元的：0 或 1，有罪或無罪。在聲譽網路裡，重要的不是罪責是否被證明，而是訊號的累積。

對被告一項未經證實的竊盜指控，大概不會激起太多警覺——但它會激起對指控者的警覺。然而，來自各個獨立來源的多個間接跡象，就開始有份量了。重要的不只是量，也是質：證人的獨立性（不同的人、不同的脈絡）、模式的一致性（一種反覆出現的嫌疑類型）、時間上的相關性。

反過來說，同一個發行者對各個不同目標主體反覆提出、毫無根據的頻繁指控，可能會被評估為誹謗——而指控者的聲譽會為此付出代價。

證據如何累積

「一則孤立的主張」



單單一則主張 —
太單薄，不足以行動。兩造都未被定罪。

「一種模式」



五個獨立來源 —
一種模式浮現。

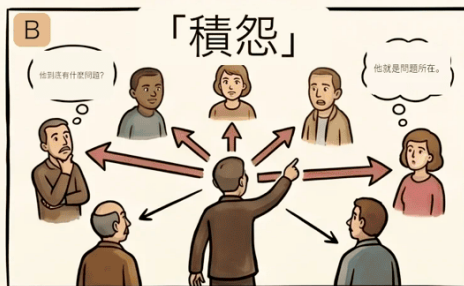
「壓倒性的份量」



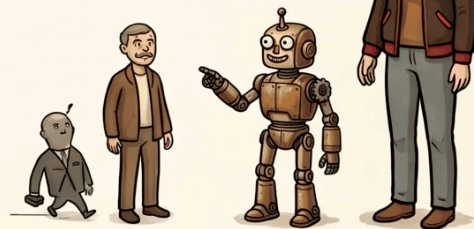
二十個獨立來源 —
壓倒性的份量。



沒有證據卻不斷播送同一則主張 —
當社群什麼都沒看見，那就是毀謗，並讓指控者付出代價。



一個指控者指著每一個人 —
模式出在指控者，不在被指控者。



這看起來像今天的世界。的確是 —
只是動機現在誠實了。沒有革命。只是更好的誘因。

獨立性就是一切。同一個聲音重複是雜訊。來自不同地方的眾多聲音是訊號。

我們也不該忽略贖罪——一種在罪責被證明之前的自願行為，提供一條通往較輕懲罰的路。懲罰在加害者不採取任何贖罪步驟、指望逃過後果時啟動——就跟那種結局在中央化系統裡可以透過腐敗買到的情況差不多。

■ 冒犯的類型

資訊的類型不必限於犯罪行為；它們可以包括：- 犯罪的描述 - 違約與詐欺 - 不道德的行為 - 對公共秩序的擾亂，現實的與虛擬的皆然 -

DID 網路中每一筆新的紀錄，都會調整對特定 DID（無論是主體、作者，還是驗證的權威機構）所評估的聲譽與風險。我為他人的命運承擔越多責任，我就變得越謹慎。

■ 透過委託來執行懲罰

我不必親自執行懲罰。我可以（類似保險那樣）付錢給一個依預先界定之規則執行結果的權威機構——相當於偵查、執法與審判服務。如果該權威機構執行得不成比例、或根本不執行，它的聲譽就會受損——而它的聲譽正是它謀生能力的根基。

委託是網路中的一條普遍原則：一個 DID 的任何活動都能委託給另一個 DID——驗證、發行主張、回應爭議、宣告共識。委託隨時可撤銷。它讓專業化成為可能，卻不喪失最終的掌控。

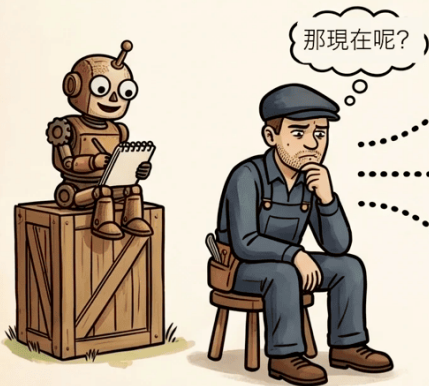
傷害之後 — 你會怎麼做？

被拒。被迫。自願。村莊回應的三種方式。

發生了什麼



現在怎麼辦？



理性的選擇永遠是最便宜的：自己把它修好。

「我試著忽略它 — 到處都被拒於門外」



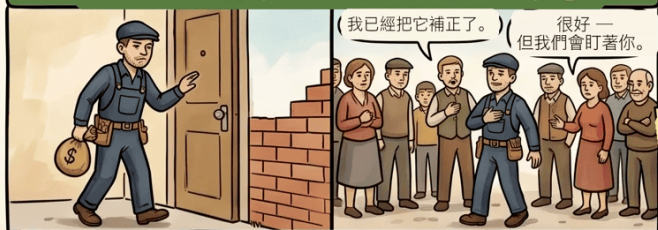
沒有補救 — 每家店都拒絕他 — 被逐出經濟生活

「我把它補正 — 但只在眾目睽睽之下」



在眾目睽睽下被迫補救 — 償還了，但村莊把他的價格標高 — 教訓必須刻骨銘心。

「我主動前來 — 並向所有人承認」



自願、及早的補救 — 被公開接受 — 聲譽恢復，但仍有戒心

這幅插圖並非事實，而僅僅是
只象徵本報已人人可乘、從容自如、只是暫時的情狀。

誰調查，誰執行？

「傷害」 → 「調查員」

「紀錄」 → 「執行者」

→ 「當責」



委派可撤銷。任何 DID 活動都可委派給另一個 DID — 並隨時收回。
你不親自執行懲罰。你委派。而受託者對你負責。

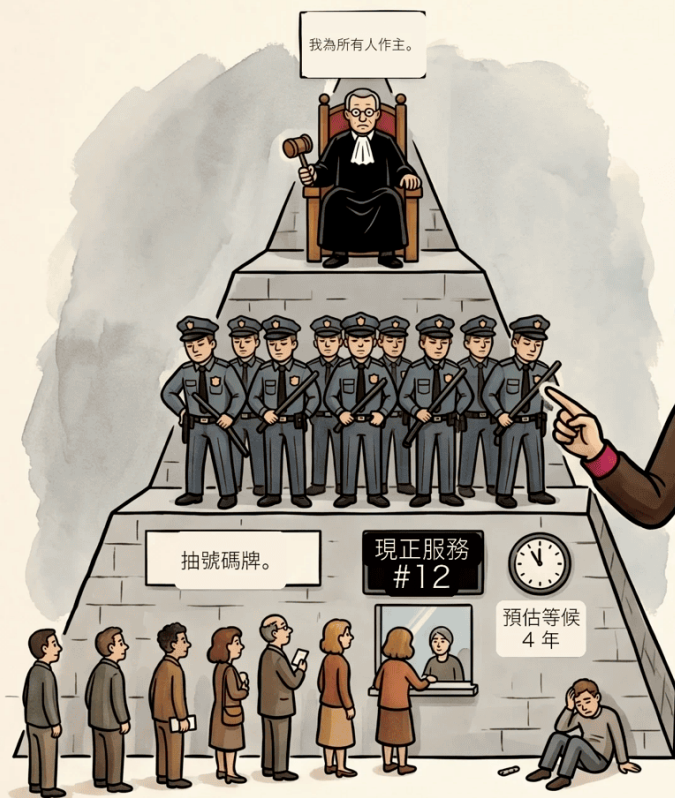
■ 風險管理的民主化

一個不可審查的聲譽網路，會把銀行或大型工業設施維運方早已作為核心業務在做的事——風險管理——加以民主化。

對一個面對客戶的銀行家來說，風險評估是事先備妥的，好讓他能在預先界定的限度內專注於商業互動。老練的維護團隊，在固定的檢修間隔蒐集風險指標（結構裂縫的跡象、正在劣化營運基礎設施的各種過程，等等），能夠預測設備的壽命，以及何時、需要何種介入。

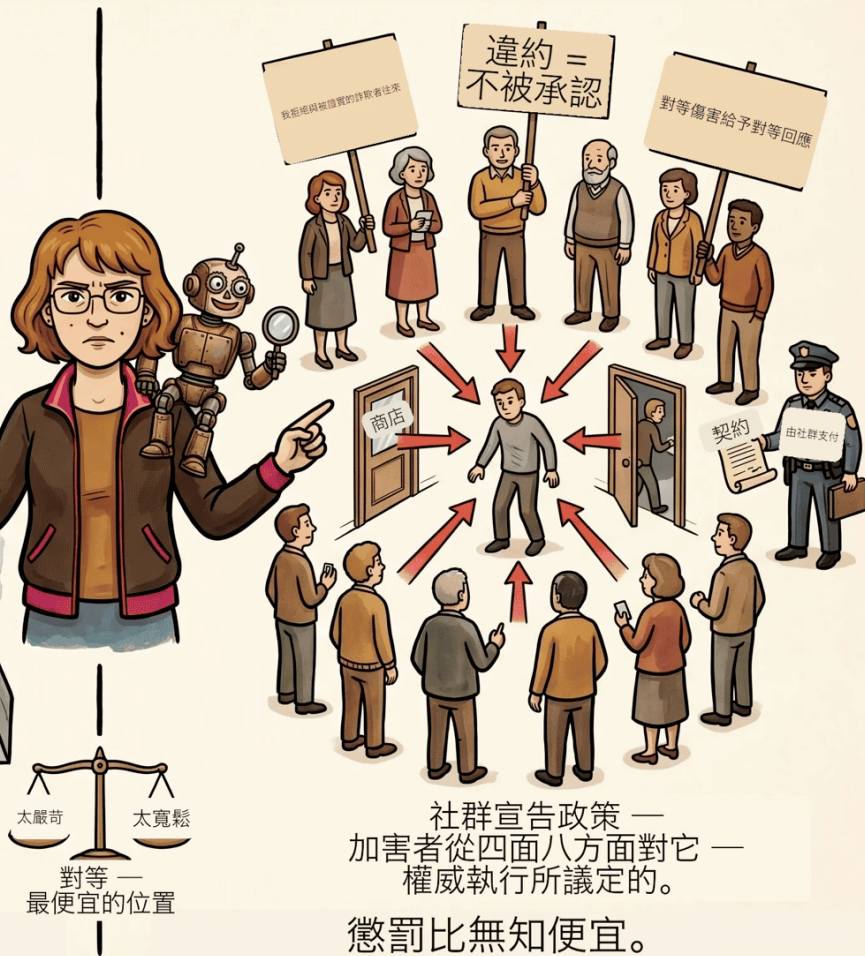
我設想 DID 的使用也類似——某人（大概要收費）會提供關於對方的一份人類可讀摘要。這份摘要會反映客戶所訂購的那個風險評估角度。

沒有中央權威的懲罰



一人為所有人作主 — 受害者等待
— 加害者心知肚明。

贖罪比懲罰便宜。



社群宣告政策 —
加害者從四面八方對它 —
權威執行所議定的。

懲罰比無知便宜。

Follow the Money

追蹤金流軌跡

我們有了一個去中心化的聲譽網路，以及使用它的動機。它已經能為使用者帶來競爭優勢——釐清潛在風險，幫助他們更有效率地規劃對象選擇與協商策略，並納入那些能降低已知風險的措施。

接下來是使用它的一種可能方法論⁵——利用網路的各種性質，建構出一條從現行體制過渡到其演化後繼者的遷移路徑。它很可能帶有中歐的特徵，這篇論述正是在那裡構思出來的。在地的條件會需要在地的調整。我建議到處都保留的，是對國家所採取措施的絕不妥協之性格——少了這一點，目標就會在無盡的討論中被稀釋，變革也永遠不會到來。當心——國家的代表與支持者會用一堆胡扯讓你分身乏術。別上當；他們的生計岌岌可危。

國家的弱點——金錢

讓我們回到起點。我們想要更多由此而生的自由、對其形貌更多的影響力，以及與之相稱的更多責任。問題很簡單：國家哪裡有一個脆弱點，能讓我們不訴諸暴力就施加壓力？

答案很無趣，也正因如此更加有力。金錢。

國家的核心，是一股金流。它靠金錢供養自己的強制機器——執行其規則的最後一環。沒有金錢，就沒有暴力的壟斷。一旦金錢開始停滯，國家就開始撤退——因為它再也沒有什麼能付給那些以物理力量把它撐在原地的人。

⁵國家的解構（Deconstruction of the State）——在捷克的脈絡下，這很可能會在捷克作者 Daniel Steigerwald 一本同名的即將出版著作（預定於 2026 年）中被深入處理。我個人對它將包含的那些啟發性程序寄予厚望。

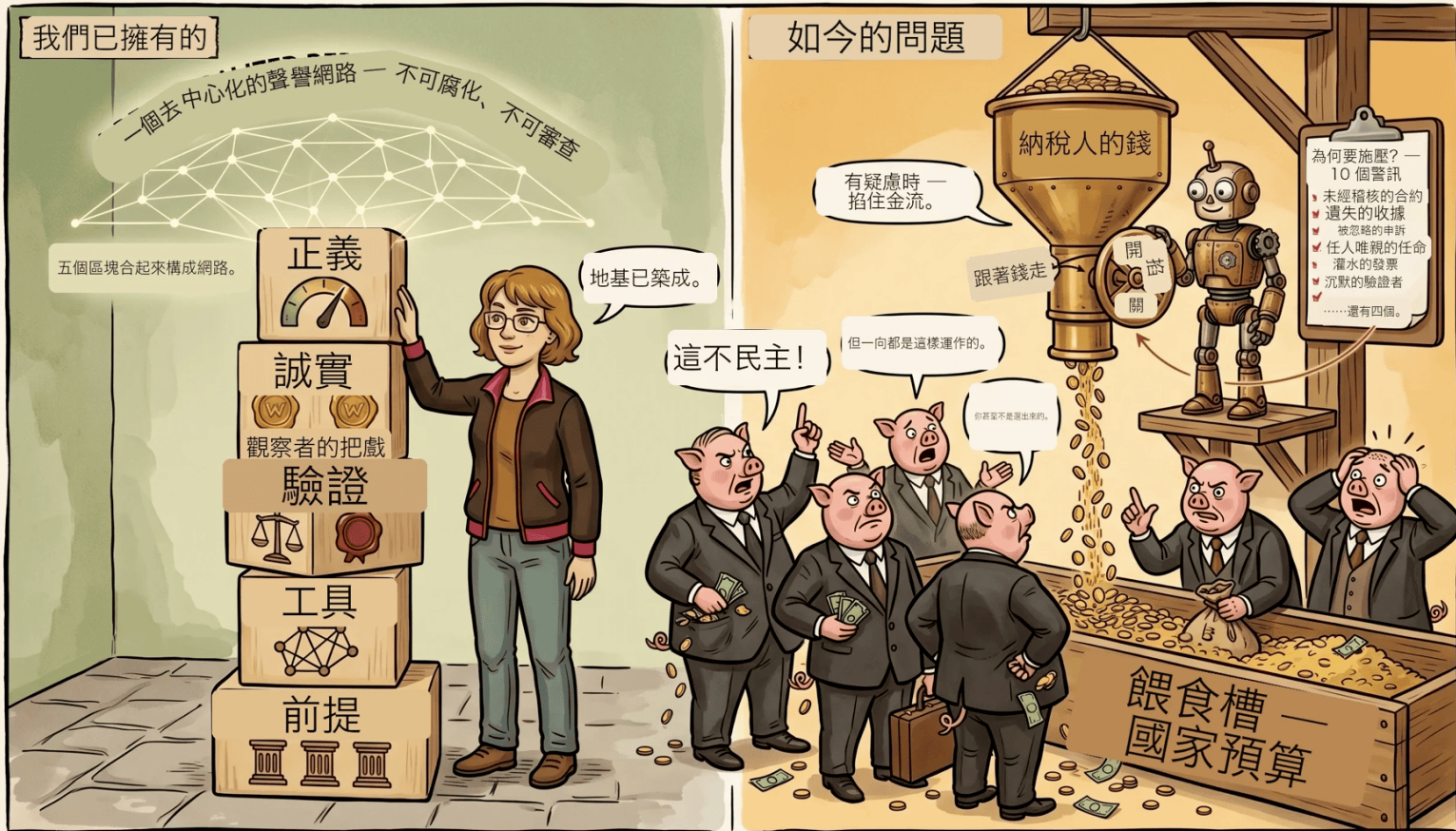
金流自然會起伏——隨季節、隨經濟、隨投資人情緒。國家透過在金融市場上舉債來掩蓋這一點。偶爾一筆貸款是理性的：一項會回本的投資。然而更常見的是，它用來支應各種早已遠遠超出國家核心目的——國防、內部安全、刑事司法、外交——之事務上過度膨脹的支出。一旦跨過某些門檻，中央銀行便以錨定於自己對通膨估計值的利率作出反應。

而在這裡，那道無聲的稅登場了。通膨遠不只是總體經濟學家的一項會計掛慮。它是對貨幣購買力的一種隱藏稅，由每一個為晚年攢下幾個銅板的人所支付。低通膨之所以被大眾容忍，是因為他們不理解它的長期效應——他們沒能意識到，即使是個位數的數字，在漫長的時間跨度上複利累積，也會把儲蓄侵蝕到人們再也無法為自己的晚年做保障的地步。而當他們無法時，他們就被制約成依賴國家補助。到頭來他們就吊在那些補助上，被拴在國家身上。

在動盪的時期——戰爭、疫情、「必要的」投資——國家乾脆打開印鈔機。負責任的儲蓄者與勞動者的購買力下降，同時我們向他們保證他們獲得了優渥的回報。有人正悄悄偷走他們的時間，還讚美他們賺得多麼漂亮。

這嚴重侵蝕了對國家的信任。而信任是把整部機器黏在一起的唯一黏膠。那正是值得撐著去頂的那根槓桿。

跟著錢走 — 至此的故事



我們有了網路。我們知道它如何運作。現在：有疑慮時，掐住料斗。
國家的權力建立在金錢上。跟著它走。

■ 為什麼是金錢，而不是其他弱點？

文明的另一個弱點，例如，是能源配送。但擾亂它的流動不是一根槓桿——那會是侵略、恐怖主義。自願不參與，並不等同於蓄意傷害他人。金錢的獨特之處在於，壓力可以自願地、透明地、且不帶暴力地施加。

Proposed transition to the state's successor

演化，而非革命

即使最終目標很有吸引力，驟然的變革仍會激起抵抗。它會斬斷各種連結——社會的、經濟的、政治的——而人們會本能地捍衛他們已經熟悉的東西，去對抗他們還未見過的东西。

因此正確的做法是漸進的——演化式的。一種能防止舊系統只用按一下按鈕就把新系統關掉的做法——因為在它能夠這麼做的那一刻，它就會這麼做。

不幸的是，這意味著要接受：均衡的自願性不會在我們部署聲譽網路的那一刻達成；它會與逐步的採用率一同到來。採納的速度可能——而且很可能——很慢，被個人的一股渴望所牽引：當墨守成規地尋求正義的方式失敗時（而它一定會失敗），透過聲譽網路向自己的社群尋求救濟。讓我們看看那條路長什麼樣子，包括按比例的估計。

■ 空著的食槽——別按照為你設計來輸的規則玩

那些試圖從內部改革國家的嘗試，仰賴權力的內部機制，指望官員會違背他們自己的誘因去推動改變。那不會發生。

何必去餵養這個系統，而不去把那些給它帶來生命的渠道抽乾？與其改變舊系統、並按它的規則玩，不如讓我們在它之上蓋一個新的層——一個逐漸把舊系統變成新系統之子集的層。一開始，那個子集幾乎填滿了超集。隨著時間推移，行為者們一個個移過來。

公司都懂這一點：當一個舊系統糾纏到無法替換時，你蓋一個平行的系統，並逐步把使用者遷移進去。

至於國家最終會落得「它實際交付的」與「它的章程所要求的」之間出現落差，並且傾向於援引那道落差——那純粹是它的代表與參與者的問題，沒有必要回頭去看它。唯一值得盯著的是這一點：別挑起一場暴力革命。

四件彼此支撐的工具

直到現在，DID 聲譽網路看起來或許主要在正義與共識上有用。我相信它能夠穩住自己、抵擋攻擊——以功績制的方式，憑藉實際的功績，而非形式上的頭銜。但光靠聲譽，不會逼國家讓步。經濟會，以及透過它施加的壓力會。

沒有什麼能阻止我們把 DID 身分當成額外工具的管理者，去狠狠地頂住金錢。別一開始就指望公民全然自願——設定一個國家阻止不了的方向。這場過渡建立在四件彼此撐腰的具體工具之上。它們沒有哪一件單獨就夠。

簡單的稅制——入場的誘餌

第一件工具是一套建立在 DID 基礎設施之上、簡單而透明的稅制。對所有所得課以單一的比例稅率。沒有例外、沒有免稅期、沒有企業扣除、沒有優惠。每一筆付款都能被稽核地連結到支付它的那個 DID。交叉比對輕而易舉。

稅率對一部分納稅人會設得比舊系統稍微優惠一些——那就是入場的誘餌。稅負會逐年下降，系統會變得越來越有吸引力，遷移也會加快步調。這套系統既是紀錄保管者，也是收款者——沒有中間人、沒有不透明。

電子支出登錄（ESR）

第二件工具是把 EET（電子營收紀錄）整個顛倒過來。與其由國家追蹤一個自由業者的每一張收據，我們追蹤國家的每一筆支出。除非每一筆——毫無例外——都通過這道篩子，否則國家不會為任何一筆個別付款從簡單稅制中收到資金。

ESR 是一個代理⁶，它把國家與公部門每一筆已實現的支出，與一筆計畫付款的紀錄相配對——包括脈絡上的正當理由，以及收款方、支出實體與用途的識別。其結果是原始的公共資料，可分層。任何人都能拿去分析它。任何人都能就「該拿它怎麼辦」向納稅人提供建議。稽核機關多年來達不到的事，突然變成人人只需一鍵之遙。

你不必轉到新稅制才能參與。只要為每一筆已實現的付款支付一筆全額可退還的押金（比方說 1-3 歐元）就夠了。未實現的餘額會作為垃圾訊息過濾器被沒收，好讓系統不至於被攻擊淹沒。任何人都能提交一筆紀錄——一位親屬為無行為能力的祖父母，一位鄰居為被忽視的公共服務，一位創業者為一張未付的發票，一位官員從自己的系統匯出。

⁶代理（Proxy，拉丁語 *procurator*，英語 *deputy/intermediary*）——此處指代表另一個實體行事的中介。ESR 代理從任何人那裡接收計畫付款的紀錄，把它們與國家已實現的支出相配對，並把由此得出的資料集提供給公眾。

我預期政黨會自然地轉型為分析的提供者，或者會冒出新的政黨來取代舊的。與其領取來自稅收的補助，它們會開始提供專業知識——為自己的支持者提供以價值為基礎的概覽，涵蓋結盟的權威機構、它們的服務，以及驗證政策。那些因懶惰而草率或荒謬的紀錄，會自動成為預算刪減的候選對象。在第一輪，你的付款一律會被撥付，但蒐集到的資料，會作為評估一筆國家支出是否仍有道理的依據。承包商與其他吃國家俸祿的人，有誘因去確保官員負責任地配對支出。否則，下一輪錢就不會流過來。

■ ESR 這個縮寫從何而來

在 2016 至 2022 年間，捷克政府對自己的公民——自由業者與創業者——推行了一套名為電子營收紀錄（EET）的系統。訊息很簡單：「我們假設你們每一個人都在欺騙國家。你要記錄每一筆交易、即時傳送到我們的伺服器，而我們會盯著你。如果你試圖規避 EET，我們會用金錢獎勵你的同胞舉報你。」

EET 是仿照巴爾幹的先例設計的。全世界第一個在 2013 年推出全國強制即時線上銷售紀錄系統的國家，是克羅埃西亞，名為 *fiskalizacija*。捷克在幾年後採納了這套模式，並施行了歐洲最嚴格的營收追蹤體制之一。

如果黑暗的一方都毫不猶豫，我們何必猶豫？ESR 就是同一套邏輯上下翻轉：由國家向公民證明自己。

公民稅款分配——決定的份量

第三件工具讓納稅人對「自己的錢流向何處」擁有直接的影響力。在第一輪，無論 ESR 揭露了什麼，國家都收到了它的錢。在第二輪它不再如此——第一輪的分析，以及由此而生的措施接手了。已繳稅款的一小

ESR — 電子支出報告

每一筆國家支出都被記錄 — 每一筆紀錄公開 — 每一個細節可供檢視。

誰提交

任何紀錄都可以由以下提交：
- 經手付款的官員
- 收到款項的收款人

對任何想看的人開放。

國家支出的公開帳本 — 開放紀錄

類別：法律諮詢 承包商：XYZ
法律事務所 金額：1,400 萬歐元
承諾：2026-01-14
已付：2026-01-19

背景：對新採購改革法案的外部意見 —
產出三份草稿、與部會辦一場工作坊、未舉行公聽會 —
最終草稿在立法期限後才交付。

類別：道路設計顧問
承包商：顧問公司 T 金額：待付
萬歐元 承諾：2026-02-03 已付：—
背景：D-X 高速公路延伸段可行性研究 —
同一家公司先前寫過這條路線的三份研究 —
結果：建議進行，比先前估計高出 18%。

類別：車牌核發 受款人：Z 區辦事處
金額：每面車牌 45 歐元
承諾：2026-02-19 已付：2026-02-19
背景：每面核發車牌的標準行政費 —
費用涵蓋材料與處理 — 本季總量
12,400 面車牌。

類別：醫院設備 承包商：MedSupply
股份公司 金額：820 萬歐元
承諾：2026-03-08 已付：—
背景：區域醫院的 MRI 掃描儀安裝 —
公開招標，三家投標 — 中選標低於中位數
2%、60 天內交付 — 發票已逾期 90 天。

垃圾訊息過濾 — 可退還的押金



當紀錄被證明準確時，押金退還。

政黨轉型為分析提供者



這些描述就是原料 —
政黨會仔細研讀它們爭得觀點，交叉比對並產出印製的公報。

每一枚公幣 — 都被記錄、公開、可供檢視。
價值不在抓弊 — 而在打開帳冊。

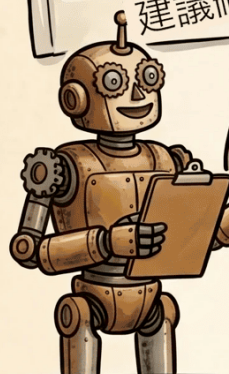
這套系統將為政府、企業、公民提供一個透明、可追溯的支出記錄。它將幫助政府、企業、公民了解每一筆公款的流向，並確保每一筆公款都能得到合理的解釋。

部分百分比，可以由繳款人自己來分配——前提是他的 DID 符合聲譽上的要求（公民身分、居留、社群承認的成年／行為能力）。可分配的百分比逐年成長。可能是指數式地成長。從今天的百分之五，到十年內的數十個百分比。

原始的 ESR 資料自然地引導納稅人的決定。低品質的紀錄，作為建議刪減的一個警示訊號發揮作用。任何人都能建立紀錄；官員必須去配對它們。少了這個，稅制就不會送給國家任何錢——既不進國庫，也不進其他預算科目。政治的角力，從投票箱移到日復一日對具體錢幣的分配上。

公民稅金分配 — 由你決定你的稅金去向

研讀 ESR 紀錄。然後移動滑桿。



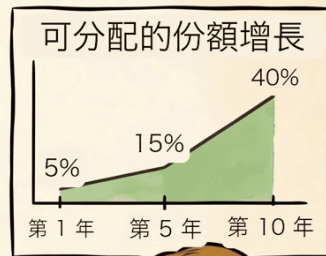
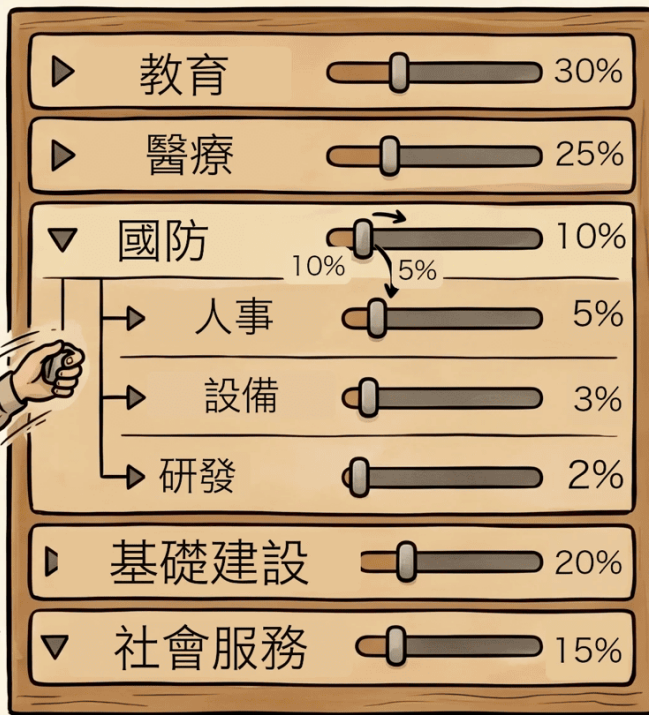
或委派這件事

不想自己分配？委派給：

- 你政黨的分析師
- 一位受信任的鄰居
- 任何你選的人 — 並隨時撤銷。



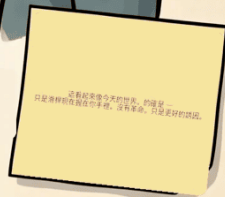
讀完報告後
國防調降。



點任一列以深入 —
可在任何層級分配。



從今日的 5% 到十年後的 40%。由你決定。
紀錄是公開的。分析是你的。滑桿也是。



與國家的協商平台——那根槓桿

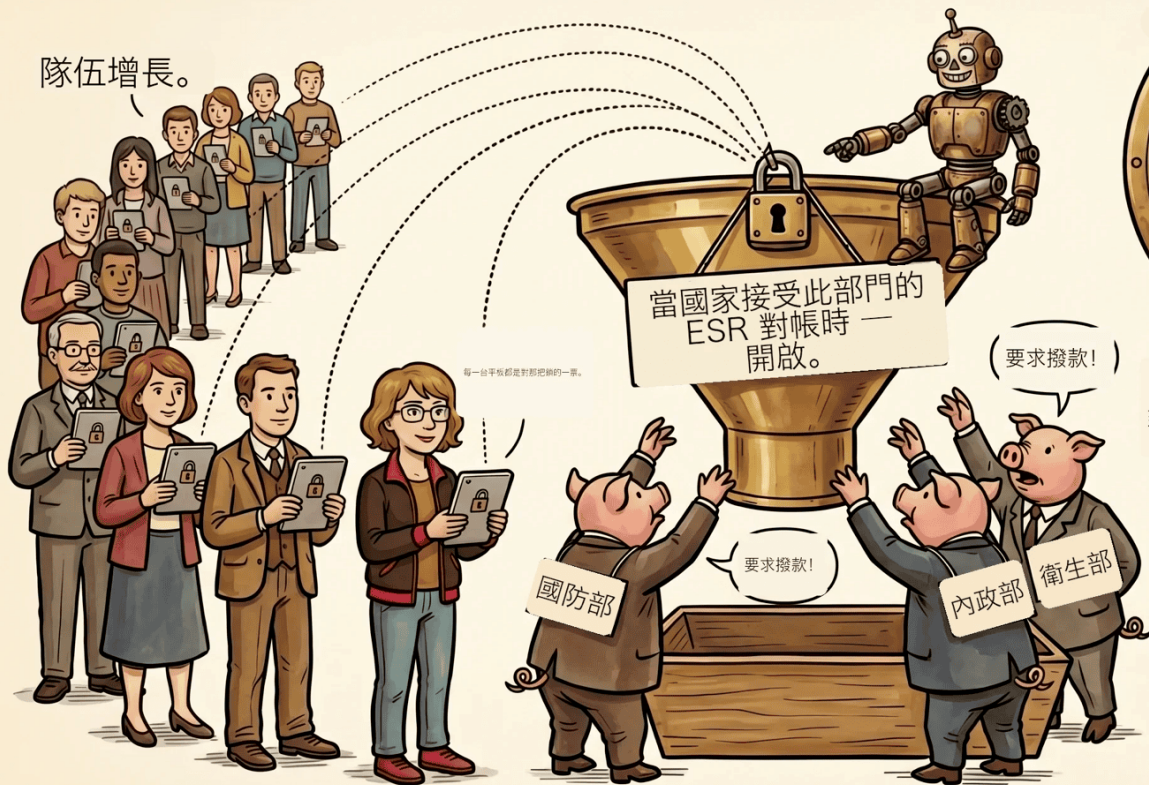
第四件工具是把一切綁在一起、直到現在才讓網路成為真正威脅的那根槓桿。主要的衝突將圍繞著：國家是否接受 ESR 作為一項有約束力的標準——先在國家層級——以及在那發生之前，來自聲譽網路參與者的威脅必須壯大到什麼程度。

這根槓桿就是即時（just-in-time）的國家撥款，以「付款須對照 ESR 加以配對」為條件。錢只在國家已滿足透明條件的那一刻才流動。一份參與者的等候名單在聲譽網路內部形成。當這個群體達到具經濟重要性的規模——大到足以威脅 GDP 成長——啟動便開始生效。到那個時候，公民不服從就成了一項可信的威脅，而不只是一個姿態。

國家會抓著那些與腐敗綁在一起的問題付款不放，抓到最後。在壓力下，它會先在自己有現成防守、且沒有空間可找節餘的地方讓步。漸進而升高的壓力，會逼它一步一步地從每一個陣地撤退。

協商平台 — 緊閉的料斗

公民握有鑰匙。當條件滿足時，國家開啟。



GDP 的一小部分就足夠 — 到臨界質量時，扣留就成為真正的威脅。

臨界質量之後 —

國家先為簡單、站得住腳的付款打開帳冊。

與腐敗相關的類別鎖得最久。

每一次解鎖都需要更大的壓力 — 而它本身也被記錄。

當有透明度時，錢才流動。公民握有鑰匙。
沒有武力。沒有革命。只要足夠多的平板，就能讓扣留變得可信。

這套系統是基於「透明」和「可信」的。它需要公民的參與和監督。只有當公民能夠監督政府時，這套系統才能發揮作用。

沒有身分證的公民身分

隨著向 DID 基礎設施過渡，國家核發的身分證失去了它壟斷性的用途。你不需要身分證——你有一系列 DID 身分，其中一些帶有一筆主張，例如你是捷克人、你是某個特定市鎮的居民、你是某所特定學校的畢業生。這筆主張可驗證、永久，且獨立於國家行政。

一個技術實作的問題於是打開：市場上誰會接下「在國家控制之外驗證既有公民」的工作，好把有意願者遷移到一個帶有適當主張的 DID 裡？最可能的是，各種專門從事身分驗證的自由市場權威機構會冒出來——公證人、在地社群、雇主。他們以自己的聲譽擔保某個特定 DID 確實屬於聲稱擁有它的那個人。公民身分——也就是歸屬於某種對社群的特定看法——從中央紀錄保管的需要中解放出來。透過聲譽網路的連結，內嵌的資料被連結並第二次、第三次、第四次地驗證，依此類推。

其後果很直覺，卻在中央化系統裡無解。今天，政治領導層——著眼於較容易的連任——可以把集中的問題進口到社群的領地裡：不顧吸納容量與既有社群的意願，接納來自其他文明圈的移民，在一種壓力下改變原有的社群，使其跟不上同化來自其他文明圈之新到者的速度。在一個 DID 網路裡，一個以腐敗方式被放進來的移民，無法確定社群會繼續把他視為自己人。社群的成員在客觀上不必忍受一個陌生人穿著社群的制服來到他們門前，還以他打算在屋裡執行之措施的合法性威脅他們（因為一則社群媒體貼文而沒收孩子的手機）。有了去中心化的聲譽，社會的多數不必聽任於此——因為歸屬於一個社群，不是由某個官員決定的，而是由社群自己、透過它的聲譽訊號決定的。

演化式轉型的四項工具

系統由內部重建 — 不必打碎它。

簡單稅制



單一稅率。沒有優惠。可交叉查核。

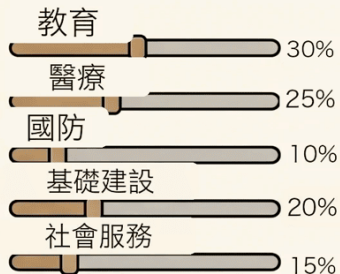
ESR — 電子支出報告



每一筆支出都被記錄 —
每一筆紀錄公開 —
每一個細節開放。

公民稅金分配

5% → 15% → 40%
第 1 年 → 第 5 年 → 第 10 年



研讀紀錄 —
然後移動滑桿。

協商平台



只有在透明度條件滿足時，錢才流動。

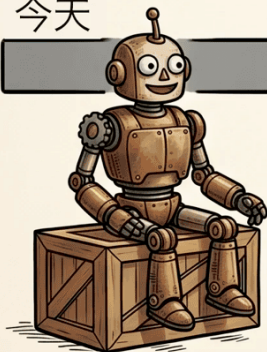
今天

演化進行中

十年後

95%

擴張中



演化，而非革命。

四項從內部改變系統的工具。

這看起來像今天的世界。的確是 —
只是工具現在握在公民手中。沒有革命。只是更好的治理。



沒有身分證的公民身分

從國家許可到社群認可。

「舊方式」的機構、國家核發身分證模式



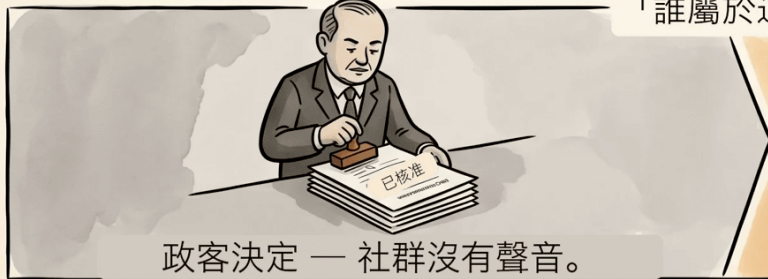
身分 = 國家許可 — 可撤銷 — 社群無置喙餘地。

「新方式」的 DID 搭配主張卡模式



沒有單一權威掌控所有主張 — 每則各自獨立 — 每位驗證者押上自己的聲譽。

「誰屬於這裡？」



你的公民身分不是政府許可。它是你社群的認可。
國家的印章被一連串獨立的驗證者取代 — 每位都與己身利害相關。

這套制度並非完美無缺，它需要
社群成員的參與和維護，才能運作。

在國家職掌範圍內之事務上，一張選票的份量，未來可以與「對簡單稅制之貢獻」的紀錄嚴格相關。搭配合適的 DID 主張（例如「此人是捷克公民」），外國國民便能被排除於選舉之外——人口登記就這麼直接搬到這裡來。

重疊與可逆性

我不主張這是唯一的路，甚至也不主張它是最好的路。但它看起來很周全——它涵蓋了主要的槓桿，並保留了退一步的選項。在起初，新系統與舊系統重疊，只改變誘因。隨著時間推移，舊系統萎縮，直到它可能——但未必——消解。好處在於漸進性與可逆性：萬一設計中出現一個錯誤，那不是終點，只是一次修正。

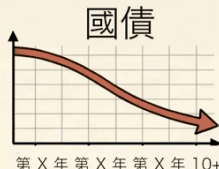
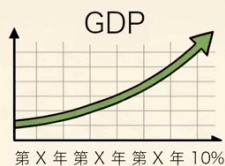
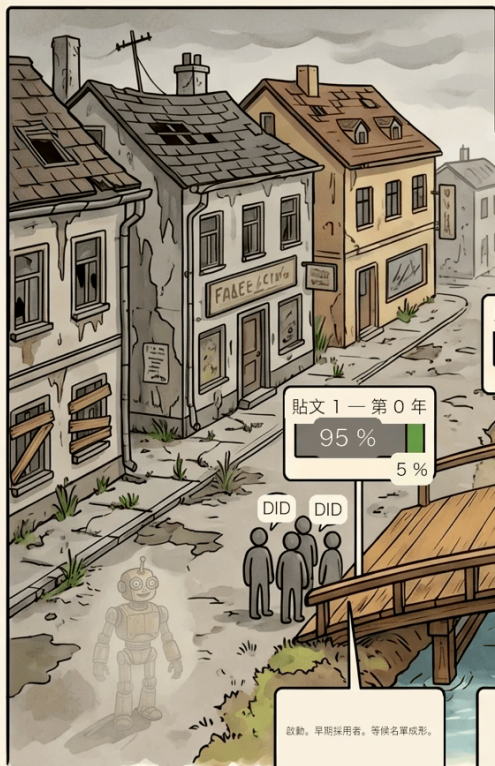
■ 和平與戰爭

國家的某些部分或許沒有一個完全以市場為基礎的替代方案——也許是軍隊。在危機中暫時委託非常時期的權力（就像古希臘人任命獨裁官那樣），或許可以繼續存在。然而，責任落在去中心化的社會身上，而非落在領袖身上。不同於中央化的治理，一旦威脅過去，收回被委託的權力會更容易——或在必要時更早收回。一個自由的社會，即使在與威權政體的兵戎相見中，也不會處於劣勢。

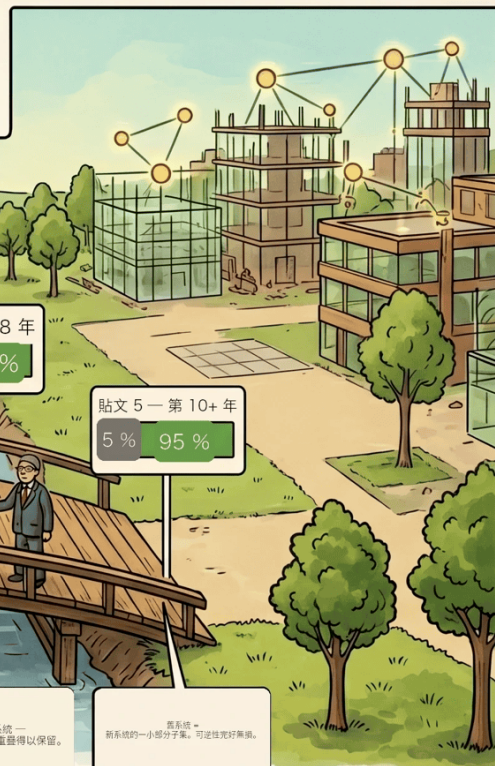
■ 戰爭罪犯

有了即時的國家撥款與透明的支出，要為侵略戰爭累積資源會變得困難。一個繼續資助這種戰爭的納稅人，就成了一個正當的目標，無法援引《日內瓦公約》下的平民身分。在這套新的安排下，沉默的默許被視為參與。

左岸 — 「舊系統」



右岸 — 「新系統」



臨界質量 —
國家在經濟壓力下接受 ESR。

逆轉

設計失誤？我們可以退回。可逆性得以保留。

75% 是新系統 —
國家是其中的子集。重疊得以保留。

舊系統

> 漸進轉型。萬一出錯可逆。一個無法被阻止的方向。

Conclusion

這條路是存在的

國家之所以是現在這副樣子，是因為它創建之時可用的科技，加上人性。把一切建立在自願性上、卻否認一般的人性，是天真的。這樣做既無法讓它擺脫腐敗，也無法擺脫它朝極權主義漂移的傾向。國家的後繼者，必須連我們目前視為負面、並加以排擠或懲罰的那些特質，也一併運作得起來。

這本書描述了一個問題——一個體制（國家），在其中，寫規則的人從不與規則的後果一起生活。它描述的要讓那個體制停止運作，必須成立的條件。它描述了一件滿足那些條件的工具。而它提出了一套過渡方法論——關於如何使用那件工具的具體步驟，作為一個可能的範例。

在第一章，我點出了五根支柱：自願性、組織、韌性、共識，以及不可腐化性。我們把它們全都滿足了。

- **自願性**——沒有人逼你進入網路，但你也無法把自己的作為從中抹去。
- **組織**——社群從你所認識的人長出來，而非從上面指派給你的人長出來。
- **韌性**——即使一個願意為監控每一個封包付錢的國家，也關不掉它。
- **共識**——它從偽善的價碼中生出，而非從選票或簽名中生出。
- **不可腐化性**——五條小規則把腐敗編織進成本裡：自願性與責任的平衡、任何人發聲的權利、無人得以挑選的進入點、帶著偽善價碼的公開承諾，以及每一筆交易背後那道觀察者的影子。

沒有哪一根支柱能單獨取代國家。合在一起，它們構成一種對腐敗的抵抗，一種國家連同它全部的機器都做不到的抵抗。

我們正處在一個點上：整件事都能用當今的科技（密碼學、去中心化身分、把誘因設對所需的、廣為人知的心理模式……）建成。只缺一樣東西：一群找到勇氣去支持它、並決定開始的臨界多數的人。

不是透過革命。

這些想法在 2025 年 6 月到 2026 年 5 月之間成形。到我坐下來寫的時候，這個框架大體已在我腦中成形——正因如此，當 [Farewell To Westphalia](#) 出現時，我懷著如此的好奇讀了它。我想看看他們的圖像會在哪裡與我的重疊，又會在哪裡分岔。第二個推力來自 Dan Steigerwald，他在 2026 年 5 月仍在從一個不同的角度撰寫自己的著作《國家的解構》；他的專案促使我把自己的願景以全部的廣度寫下來——好讓這個世界能把它與其他人的一同攤在桌上。

我不是要求你相信其中任何一點。我是要求你去思考它。而我留給你一個問題：
你會改變什麼？

Pavel Kudrna 2026 年 5 月 23 日，捷克布拉格

致謝

靈感

我感謝 [Farewell to Westphalia](#) (Jarrad Hope、Peter Ludlow) 的作者們，感謝那套智識框架，它幫助我把自己的想法置於解構西發利亞式國家模型的更廣脈絡之中。

審閱與回饋

工具

在準備文本、梳理想法、反覆推敲措辭的過程中，我使用了 AI 工具的協助。一切想法、論證與結論都是我自己的——AI 是打磨的工具，而非內容的共同作者。

資訊圖表是依作者的規格，與生成式工具協作設計而成。

取回你的時間

公民把寄生蟲逐出公共生活。



捍衛他們想竊走的時間。

以欺騙奪走的，用雙手奪回。

Support the Project

Personix is funded by readers like you.



Bitcoin on-chain

bc1q7cctdz6r026dgy06ul94eygg49ujtxnrq5czaj



Bitcoin Lightning

LNURL1DP68GURN8GHJ7AMPD3KX2AR0VEEKZ
AR0WD5XJTNRDAKJ7TNHV4KXCCTTDEHHWM30
D3H82UNVWQHXXMNP0FA8JMPVD5XJMN9XUE
RX55QRQK

Where this money goes — and where it does not

The QR codes are the **author's personal channels** — contributions go directly to Pavel Kudrna and fund further writing, the social experiment / simulation, and outreach.

The *only* legitimate fundraising channels for this project are:

- **Author's editions of this book** — QR codes in copies authorised by the author.
- **personix.org** or its Tor onion mirror linked from there — where the *Personix Foundation* collects for the activities described there. Foundation funds are kept separate from the author's personal funds.

Anything advertised elsewhere — substituted addresses in reprints, lookalike domains, social media “raising for Personix,” fundraisers not tied to either of the above — **is most likely fraud**. We deliberately avoid the cryptocurrency market and its participants.

Glossary

詞彙表

詞條	捷克文	意義
權威機構 (Authority)	Autorita	一個受信任的實體（個人、組織），驗證資訊並以自己的聲譽為它背書。可以是專門的（偵查、法律、技術）。
主張 (Claim)	Tvrzení	一般而言：任何可驗證的陳述。此處：一筆發布到聲譽網路的紀錄——關於某事件、屬性或關係的斷言，並以密碼學方式簽署與驗證。例如「我是市鎮 X 的居民」或「此人違反了一份契約」。
區隔化 (Compartmentalization)	Compartmentalizace	一般而言：把資訊分隔成彼此孤立的單元，好讓其中一個單元被暴露不至於危及其他單元。這是情報機構所熟知的原則。此處：獨裁政權下的並行 DID 身分——其中一個被攻破並不會洩漏其他身分。

詞條	捷克文	意義
一致性雜湊環 (Consistent Hash Ring)	Hash ring	一種用來選取驗證者的演算法機制——環上的位置由社會圖譜內 DID 文件的雜湊所決定。確保一種非決定性、卻可驗證的選取。
DID	DID (Decentralizovaná identita)	一種由你自己建立、自己掌控的數位身分，沒有中央權威。以你的私鑰做密碼學簽署——沒有人能撤銷它或偽造它。
DID 文件 (DID Document)	DID dokument	一份公開可得的資料檔，描述你的 DID 身分——包含公鑰、網路位址與中繼資料。用來在網路中驗證你的身分。
盡職調查 (Due Diligence)	Due diligence	一般而言：在進入商業或法律關係之前，對對方進行深入的查核——檢視其歷史、財務、聲譽與風險。此處：在聲譽網路裡，由於有經驗證的紀錄可得，它進行得更快、更自動。
經濟中性原則 (Economic Neutrality Principle)	Princip ekonomické neutrality	網路中的誠實行為，在經濟上接近於零——發布成本會以驗證報酬的形式回流。不誠實的行為則是淨損失。

詞條	捷克文	意義
湧現的 (Emergent)	Emergentní	從較簡單部分的互動中自發生成，無人設計或指揮。一群鳥沒有計畫也能排成隊形飛行——陣形從每一隻個體所遵循的簡單規則中湧現。
湧現的社會契約 (Emergent Social Contract)	Emergentní společenská smlouva	各種行為規則，不是從上面（法律）產生，而是從下面產生——從社群內部反覆的互動與共識中產生。
ESR	Electronic Spending Register	一套所提議的、用於透明追蹤公共支出的系統——國家每一筆已實現的支出，都與一筆計畫付款相配對。靈感來自捷克的 EET，但反過來對付國家。
雜湊 (Hash)	Hash (otisk)	一般而言：一種單向數學函式，能從任何輸入產生一個獨一無二、固定長度的「指紋」——就像文件的指紋。相同的輸入永遠產生相同的輸出，但無法從輸出反推出輸入。此處：用來決定雜湊環上的位置，並驗證文件的完整性。
即時撥款 (Just-in-Time Funding)	Just-in-time financování	以透明為條件的國家撥款——只有在國家接受 ESR 並把其支出加以配對時，錢才流動。一根用來逼出合作的槓桿。

詞條	捷克文	意義
功績制 (Meritocracy)	Meritokracie	一般而言：一種以實際功績與經證明之能力、而非形式頭銜、人脈或世襲特權來決定地位的體制。此處：聲譽網路自然偏好那些對社群有可證明貢獻的人——他們的聲音之所以更有份量，是因為過往紀錄，而非因為職位。
洋蔥閘道 (Onion Gateway)	Onion gateway	一個 DID 身分在洋蔥網路上的網路位址。與 DID 文件分開——它可以在不喪失身分的情況下更改（類似於更改一個網域背後的 IP 位址）。
洋蔥路由 (Onion Routing, Tor)	Onion routing (Tor)	一種確保網路不可審查性的通訊協定。訊息被分層加密——每個節點剝除一層，卻不知道完整的路徑。
預言機問題 (Oracle Problem)	Oracle problém	一般而言：如何確保進入數位系統的資料，忠實對應到實體世界裡實際發生的事。此詞源自區塊鏈領域。此處：透過權威機構來處理，他們押上自己的聲譽作為擔保，保證數位紀錄對應於實體現實。

詞條	捷克文	意義
現象學的 (Phenomenological)	Fenomenologický	一般而言：一種把現象當作它們在直接經驗中顯現的樣子來研究、透過觀察由它們所引出的結果、而不預設既定理論的取徑。此處：自由、社會契約與行為規範都是被觀察到的現象——是人與人之間數以千計的微互動所導致的結果，而非自上而下界定的原則。
政策 (Policy)	Policy (politika)	一般而言：一套在特定脈絡下規範行為的規則或原則。此處：DID 網路中每個參與者都宣告自己的政策——他如何回應他人的特定行為、遵循哪些規則、認為哪些懲罰是合乎比例的。政策的總合形成湧現的社會契約。
代理 (Proxy)	Proxy	一般而言：一個替身或中介——代表另一方行事的系統或實體。此處用於兩個脈絡：(1) ESR 作為一個把公共支出與計畫付款相配對的代理；(2) 觀察者妙招中，觀察者作為發布者與驗證者之間的代理。
發布者 (Publisher)	Vydavatel	一個建立並發布一筆紀錄（關於不公、補救等等的一筆主張）的網路參與者。承擔發布的成本。

詞條	捷克文	意義
以聲譽為基礎的社群網路 (RSN)	Reputační síť	一個去中心化的社群網路，參與者在其中交換關於現實世界行為的回饋。紀錄建立起來昂貴、讀取起來便宜。
聲譽訊號 (Reputation Signal)	Reputační signál	網路中的一筆個別紀錄——正面的（傷害的補救、義務的履行）或負面的（不公、違約）。這些訊號累積起來形成一份聲譽檔案。
社會圖譜 (Social Graph)	Sociální graf	你的聯絡人、以及你聯絡人的聯絡人所構成的網路。演算法在一個可設定的深度（例如 3 層）尋找驗證者。沒有全球性的區塊鏈——網路自然形成一個個有所重疊的社群。
稅款分配 (Tax Allocation)	Alokace daní	一種讓納稅人決定其部分稅款流向何處的機制。可分配的百分比逐年成長。
過往紀錄 (Track Record)	Track record	一般而言：一個人或組織過去成果、成功與失敗的歷史。此處：某個 DID 身分在網路中一切過往互動的總和——經驗證的主張、被接受與被拒絕的紀錄——其聲譽即由此推導而來。

詞條	捷克文	意義
驗證者 (Verifier)	Ověřovatel	一個以演算法被選出、去驗證並發布一筆紀錄的參與者。以自己的好名聲為資訊的真實性背書。

Production notes

Reserved by the author (not covered by the CC BY-SA licence): the Personix name and wordmark, the book cover, and the support channels (QR codes, addresses, contact e-mail). Derivative editions must remove or replace these elements; they may be used only to reference this original work.

Source files. The complete source — markdown text, infographics, build scripts — is available alongside this PDF.

Tools. While preparing the text and iterating over phrasing, the author used assistance from AI tools; the infographics were designed in collaboration with generative tools based on the author's specifications. All ideas, arguments, and conclusions are the author's own.

PERSONIX

Uncompromising Change

An Uncensorable and Incorruptible Decentralized Reputation Network

The state worked when communication was slow, decisions were local, and authority lived in the same town it ruled. Today's networks invert all three assumptions — and the institutions built on them no longer fit the world they govern. This book describes a tool that does fit: a decentralized reputation network in which identity is yours to keep, truth is publicly auditable, and bribery is reputational suicide. Not a manifesto. Not a forecast. A working blueprint for how the successor to the state can be built — voluntarily, one declaration at a time.

Pavel Kudrna • Praha, 2026

personix.org

Licensed under Creative Commons Attribution-ShareAlike 4.0 International (CC BY-SA 4.0).