

PERSONIX

登世網絡的樣子，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絡
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
這本書講的是甚麼？	9
Essential Prerequisites for Change	16
變革的必要前提	16
The Tool	25
以聲譽為本的社交網絡	25
網絡為何不可審查	48
回應顯而易見的疑慮	50
對技術的依賴	50
在網絡裏發佈，是不是把錢扔出窗外？	50
如果有人創建多重身份怎麼辦？	52
有錢人難道不能乾脆「買下」更多身份（或創建虛擬社群）嗎？	54
那些只想讀取、卻不給社群貢獻任何東西的「搭便車者」怎麼辦？	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 — 架接數碼與物理世界	66

How Verification Works 68

共識與驗證過程	68
-------------------	----

Roles in the verification transaction and authorities	74
---	----

角色概覽	74
----------------	----

簽發者	76
---------------	----

權威	76
--------------	----

驗證者	80
---------------	----

主體	83
--------------	----

觀察者	85
---------------	----

機制：時間戳與挑戰碼	85
----------------------	----

妙處所在：你根本不需要真實的觀察者	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	108
追蹤金錢的軌跡	108
國家的弱點 — 金錢	108
Proposed transition to the state's successor	111
演化，而非革命	111
四件彼此支撐的工具	112
簡單的稅制 — 入門的誘餌	113
電子支出登記（ESR）	113
公民稅款分配 — 決定的份量	114
與國家談判的平台 — 那根槓桿	118
沒有身份證的公民身份	120
重疊與可逆性	123
Conclusion	126
這條路是存在的	126
致謝	127
靈感	127

審閱與反饋 128

工具 128

Glossary **131**

詞彙表 131

Introduction

你覺得自己可以依靠國家嗎？

當一樁顯而易見的不公降臨到我、我的家人或我社群中的某人身上（身體傷害、詐騙、無理限制……），而國家的回應卻是：對，這是不公，但你別採取任何行動，否則你跟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，而配合它的人是共犯。

結果就是彼此疏離、扮演社群、扮演國家，社會不斷崩解，並預示著前方嚴重的衝突。

國家能跟上技術與社會變遷的步伐嗎，還是它寧願一巴掌拍下一道禁令？

我大可假裝把停滯、無能與腐敗當作法治與傳統所宣示的穩定來對待，但我再也不想這樣了。那樣我是在騙自己，也是在騙你。

當你膽敢批評一件自己正在付錢供養的事情時，你有沒有感受到官員與民選代表的居高臨下？

我拒絕僅僅因為某些人不擅長那種軟技巧，就認定他們不配參與塑造全社會的規則——而在今天，那些軟技巧竟是成為國家法定機構中民選代表的唯一充分條件。我相信絕大多數人有能力照顧好自己、自己所愛的人以及自己的社群，並在其中看見自己人生哲學的一部分。我身邊認識的大多數人都是這樣的。

但我也遇過徹頭徹尾的混蛋，他們之所以是混蛋，恰恰是因為他們懂得玩這場遊戲——在這場遊戲裏，社群不被允許給他們反饋，國家保護他們，讓沒有人去擾亂那個秩序，因為那個秩序若被擾亂，就會威脅到國家的本質：確保權力階層及其機構層級上層樓的人過上輕鬆的日子。封建制度換來的，是民粹主義者與精英主義者的統治。

你喜歡別人告訴你該怎麼過自己的人生嗎？

我不把現狀當作完美、終極的既定事實來接受。我必須為自己的言行負責，但當有人告訴我應該持守哪些「正確」的價值時，我就會渾身不自在。你呢？



我拒絕接受。

這本書講的是甚麼？

想像一個聲譽社交網絡，任何願意的人都可以為它創建自己的密鑰（創建自己的身份），由社群成員邀請加入，或自行闖入。你在其中建立自己的聲譽，並在需要時汲取關於他人的有用聲譽數據。當不公發生時，你尋求社群的支持 — 你陳述你的案情，提供你手上與此事相關的東西，社群看一看，根據相關性決定是否把它傳遞給其他人，以及如何制裁那個犯錯者。

整本小書講的，就是要讓這件事在外表上如此簡單地運作，底層必須有些甚麼。如果你堅持讀下去，我向你保證，一個此刻在許多方面看似複雜難懂的世界，將會變得更可理解、更清晰地展開。你會看到，許多壞事可以被安排成不再對壞人如此不公平地划算。而且這並不是一件你得時時黏在網上的工具 — 只要在你覺得需要的時候伸手去用它就夠了。

我進一步向你保證，這裏所描述的安排，會讓人感覺更貼近人們真實的動機，而且它不需要以某種「主義」之名去改造他們。

最後，我們會展示如何管理一場非革命性的過渡，走向一種讓社群重新成為完全運作的社會單位、不再只是裝裝樣子的狀態。

■ 技術文章

本書是原始技術文章《去中心化聲譽網絡：一個自願且不可腐化的社會組織框架》(Pavel Kudrna, 2026) 的解說性伴讀。如果你對正式的架構描述、驗證者選取演算法以及經濟機制的論證有興趣，我建議從那裏開始。

■ 各章環環相扣

本書寫成一段連貫的論證——每一章都建立在前一章之上。某一部分引入的概念，會在後面的部分裏被用到，包括在腳註中。我不建議跳着讀。

■ 這本書寫給誰？

儘管在視覺上採用了親切的形式，本書的主要目標讀者，仍是那些關注人類社會可能的社會—經濟—政治安排原理的較專門讀者。要走到能夠把整個主題向最廣大的公眾深入淺出地講清楚的地步，仍然需要一條漫長的路，去建立起一整套完整的溝通策略。

我歡迎大家提出建議，讓這本小作品或任何後續修訂版更易於理解。

警告

我不知道你是誰、多大年紀，也不知道你這輩子被迫忍受過多少破碎的承諾。我在這裏不再做承諾了。相反，我想警告你：你在這裏學到的東西，唯一的結果或許就是意識到——大概不存在一條由別人替你收拾今天這爛攤子的路。我只是在描述一個框架／工具，它也許能讓收拾工作更簡單、更透明。在此基礎上，我會嘗試準備一場社會實驗／模擬，修正潛在的缺陷，或者，如果這個構想被證實有根本性的設計裂縫，就把它徹底埋葬。

一個請求



底下還有更多。跟著我。

如果即使在讀完本書之後，你仍能對這個構想保持開放的心態，跟進它的走向、看它如何經受住實質批評的考驗，我會由衷感激。而更讓我感激的，是你日後的參與 — 用你自己的想法去嘗試打破所提出的均衡原理，從而更好地檢驗這個系統對真實人類行為的準備程度。

沒有你和你的參與，這個構想就只是抽屜裏的一套理論。沒有你、你的貢獻以及財務捐助，我們就無法把這個項目推向真正的社會實驗，因而也無法推向真正的成熟。沒有你和你的實質批評，我們就會停滯在此刻，或者任由自己被中間派的聖杯 — 絕對、不可逆轉的極權主義 — 所吞噬。走哪一條路，或按兵不動，取決於我們自己。

挑戰

我們給你肩上加的擔子並不算輕。你已經在透過那些神秘咒語式的手冊 — 聲稱社會最好由中央來管理 — 承擔着一個揮霍無度地被治理的社會的成本，而我還有膽子向你要求更多，還要你逆着這些傾向而行。我很清楚，我們將不得不熬過歷史上最大龐氏騙局 — 隨收隨付的退休金制度 — 的崩潰，同時又不能讓好幾代人餓死。

儘管如此，我還是要請求你：讓我們終於能把一個更好的世界交到我們孩子的手上，並留下一份遺產 — 那就是我們完成了這場變革。釋放經濟增長，也許能部分解決地平線上迫近的困境。屆時我們可以告訴我們的後代：這是一段精彩絕倫的旅程，而且並非徒勞。



更好的世界值得這份重量。

■ 問題所在

唯有以直接責任加以平衡的自由，才能真正釋放出這個世界前所未見的巨大潛能。



進來吧。計劃都攤開了。

Essential Prerequisites for Change

變革的必要前提

向好變革的根本前提，是讓從屬者變成主導者 — 或者至少成為平等的夥伴。這意味着要接管那些界定主導與從屬關係的最關鍵議程。這些議程建立在對「歸屬於構成國家公民的那些社群」的證明之上。它們就是資訊，以及這些資訊由一位在那些社群中擁有可觀聲譽的權威加以驗證的能力。

為了克服現行制度，我歸納出五項前提，然後按我自己的理解逐一加以說明。我們可以把這些前提看作支撐本書其餘部分所描述之系統結構的支柱。這些支柱最初是我按自己的偏好挑選的，而在用它們來推理的過程中，我逐步把對每一根支柱的理解打磨成下面的形態。

讓我們逐一走過這五根支柱。

■ 自願性

在我們的情況裏，自願性意味着我不被強迫去參與運行這個去中心化聲譽網絡。然而，我不能主張一項以正面措辭包裝的權利，要求網絡不記錄關於我的資訊 — 關於我的資訊是否會進入聲譽網絡，只取決於我自己、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

單一個體無法破壞這個系統，這正是為何國家要控制人的結社，作為一種手段來防止那些可能威脅其結構與運作的活動。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。

讓我們不必設定共同目標，但我們可以一起走一段路。最自然的形式就是在社群中結社 — 但這些社群必須擁有它們所需的一切工具，才不至於停留在「扮演社群」的階段。

■ 韌性

所選擇的、通往改變國家 — 或通往過渡到其繼任者 — 的道路，絕不能依賴國家的許可。工具及其使用方式必須盡可能不可審查。說白了，審查它們的代價必須是天文數字。沒有這一點，整個努力就只是在燃燒時間與生命能量。

前提 2/5：組織



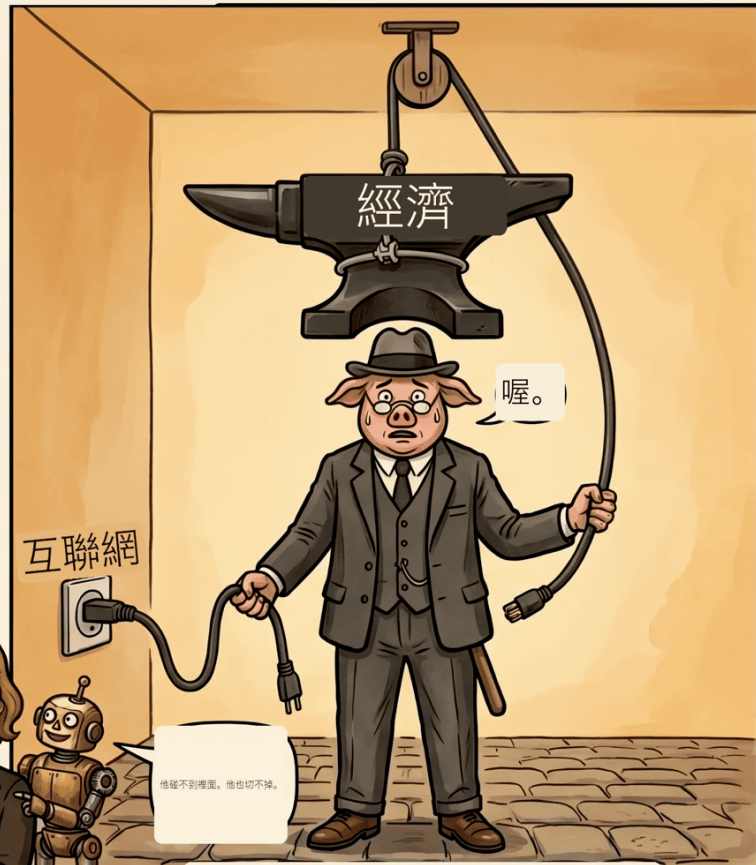
個人無法擊垮體制。社群可以。

前提 3/5: 韌性



他無法從外部搜尋。

沒有可申請的許可。沒有可拔的插頭。



拔掉插頭 — 等於自我毀滅。

■ 共識

所提出的解決方案，就其本質而言，必須既包含一套協商共識的機制，也包含一個在共識被違反時發揮作用的鎮壓性組成部分。它不必是一份自願的雙贏協議。只要情勢與社會壓力能確保在社群內部以及社群之間達成妥協，就足夠了。

■ 不可腐化性

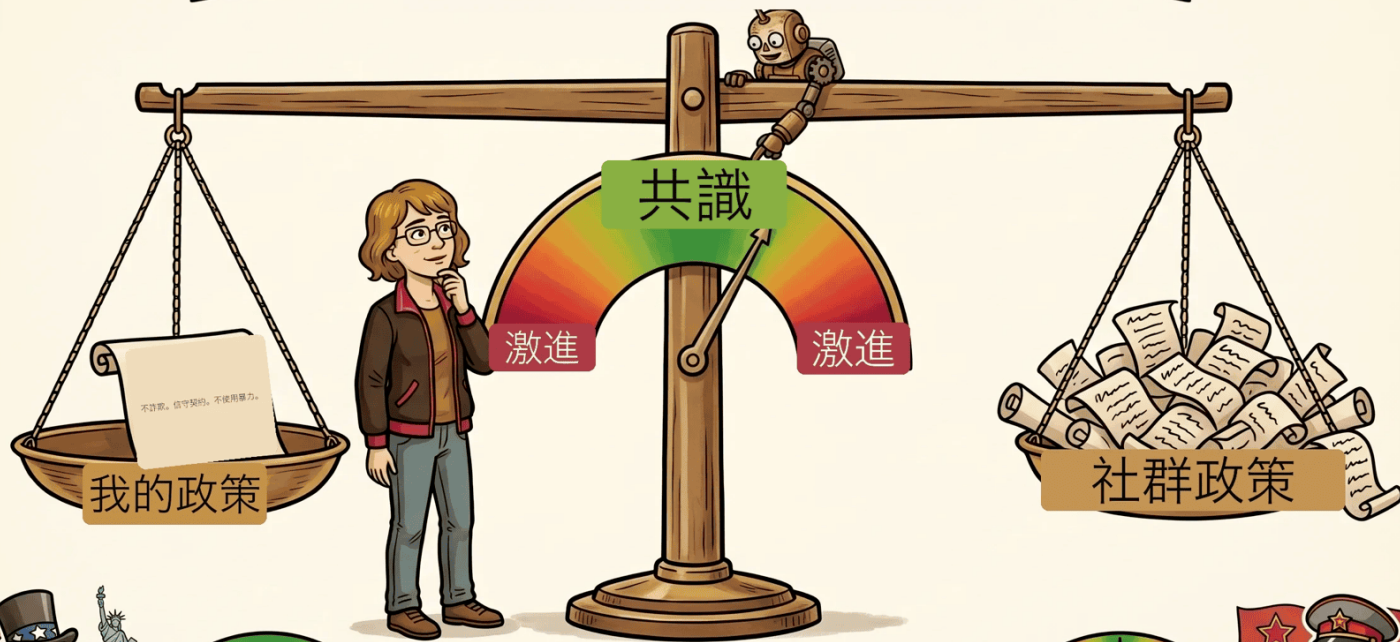
不可審查性從外部捍衛系統。但一個由人組成的網絡也可能從內部腐爛——某個權威被攻陷，某條宣示過的規則被悄悄拋棄，參與者被無聲地收買。如果內部的人可以毫無後果地被腐化，那麼不可審查性就會是一場空洞的勝利。

不可腐化性並非單一巧妙把戲的產物。它源自**所提出設計的若干原則協同運作**——對抗腐敗的壓力分佈於整個架構之中，各個部分彼此加強。這究竟是如何達成的，我們會逐步展示——在對工具的描述中、在驗證中、以及在講懲罰的那一章中。到最後，我們會把所有已經建立起來的東西重新梳理一遍。

不可腐化性既是設計的一項前提，也是結果的一項湧現性質。它是第二道防線——面向內部的那一道——而沒有它，韌性就只是半面盾牌。

待在範圍內 — 別當激進分子。

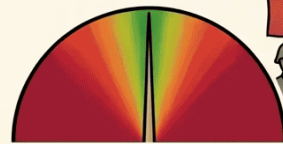
你可以有分歧。只是別偏得太遠。



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



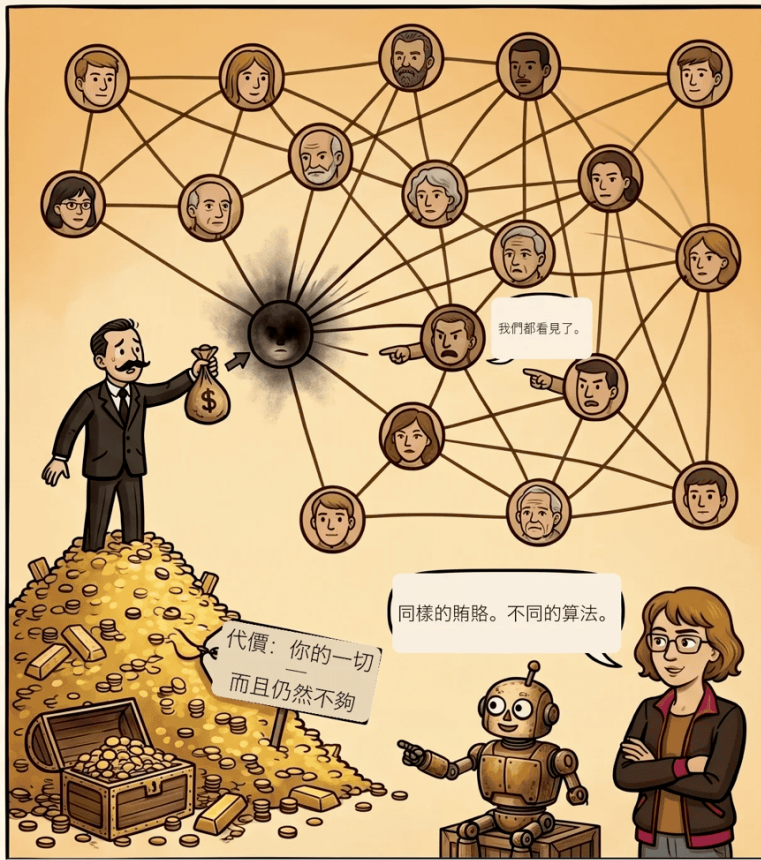
威權社會

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

以聲譽為本的社交網絡

要帶來變革，我們需要一件精心設計的工具。我們先簡略勾勒它，在後面的章節裏再更詳細地審視每一個部件並加以補充。想像一個不可審查的、全球性的、去中心化的社交網絡，你可以在其中安全地創建和管理你的代理身份 — 即所謂的去中心化身份（DID）。DID 是一種你自己創建並掌控的數碼身份，不依賴任何中央權威。沒有人能奪走它或偽造它，因為它是用你的私鑰（或多把密鑰，透過多重簽名）以密碼學方式簽署的。

■ 註

其中一個含意是：這樣的身分可以逐步取代國家簽發的身分證件 — 不過這一點留待講過渡的那一章再談。

在這樣的網絡裏，你可以透過自己的身份報告某人對你造成了傷害（以及日後可能報告他已經彌補，或被迫彌補了傷害）。要讓這條反饋 — 針對傷害的始作俑者 — 具有作為相關資訊來源的價值，把資訊錄入網絡就必須付出時間、能量與金錢，而且除此之外還必須為他人產出可驗證的證明，證明這並非閒言碎語。

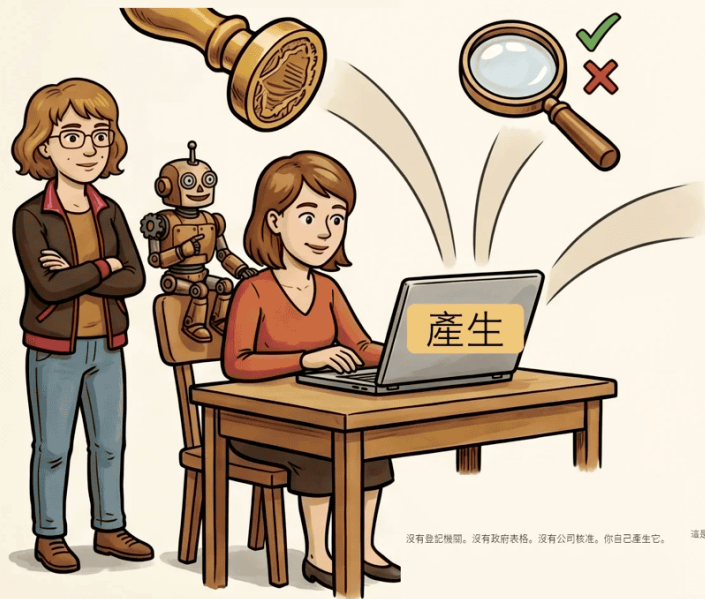
讀取資訊很容易而且相對便宜，但創建一條個別紀錄則代價高昂、要求很高。寫入會遵循一套明確的協議，其中依所選演算法進行的計算，嚴格決定要向哪一個 DID 請求對所提交資訊的驗證，以及如何操作，才能讓被選中的參與者代你處理該資訊、發佈它並成為它的驗證者。

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。網絡上可見。



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 —
由大學校友網絡驗證

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。

■ 演算法 vs 激進

演算法式的驗證者選取，確保非激進的資訊發佈者隨着時間推移，能在所發佈資訊的成本與驗證所得報酬之間，維持一種近乎中性的平衡。

發布耗費時間、能量與金錢

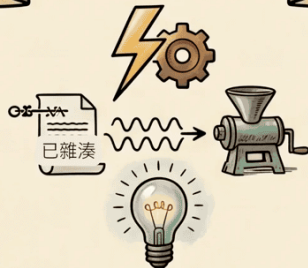
寫入網絡從不免費，讀取則免費
三個管道 三個都是真的

時間



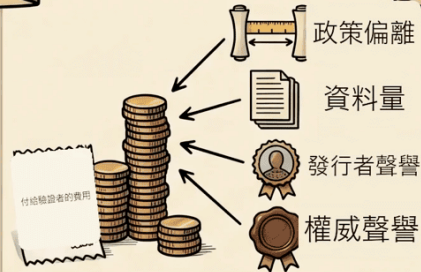
你在演算法抽選驗證者、驗證者讀取你的紀錄時等待。

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」、「驗證者如何讀取」、「發行者的選擇」



為何昂貴的寫入保護聲譽 — 本章稍後說明

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

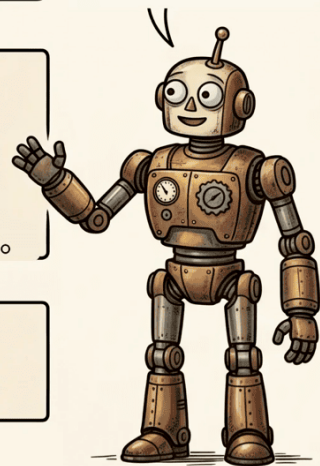
讀取很便宜



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。



讓我們看看演算法如何選取一個驗證者。

■ 演算法

演算法式的選取，會為不同的資訊片段非確定性地選出不同的驗證者（或一組可能的驗證者）。完整 DID 文件的雜湊（一種單向數學函數，能從任何輸入產出一個獨一無二的「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，並選出驗證者候選。

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

用大白話說：演算法拿走你的整份 DID 文件，從中計算出一個指紋，而這個指紋決定了你的驗證者。

在演算法選出的第一位驗證者那裏，作為發佈者的你可能不會成功 — 你的聲譽或你宣示的設定，可能不符合他的要求。你會以演算法方式繼續尋找下一位，透過再進行一次遞歸迭代，為你指派另一位驗證者。每走一步，通往目標驗證者的「距離」就會增大，隨附而必須發佈的元數據也會增多。隨著數據增多，成本自然上升（不僅因為主張本身最初的大小，也因為每一次被拒都會累積元數據）。可信的資訊要比荒謬的一時興起容易通過得多。每個人願意承受多高的價格、這條紀錄對他有多重要，都由他自己決定 — 激進註定會變得昂貴。

一枚公正的硬幣，擲向你的整個社群

一枚公正的硬幣，擲向你的整個社群

每張臉機會均等——
雜湊均勻隨機落點

你的社群及其鄰近地區

你無法選擇你的驗證者 —
演算法樹硬幣。這裡每個人機會均等。

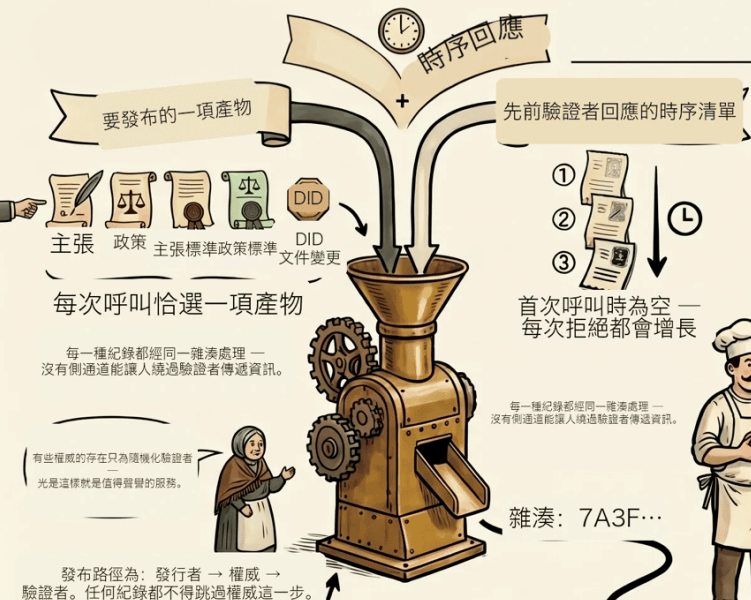
接下來會發生什麼

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個答覆
——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。



雜湊: 7A3F...

每一種紀錄都經同一雅漢處理——沒有側通道能讓人繞過驗證者傳遞資訊。

首次呼叫時為空——
每次拒絕都會增長

A 你能暴力破解它嗎？

我可以磨出成千上萬份草稿，直到有一份落在我要的驗證者身上……

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

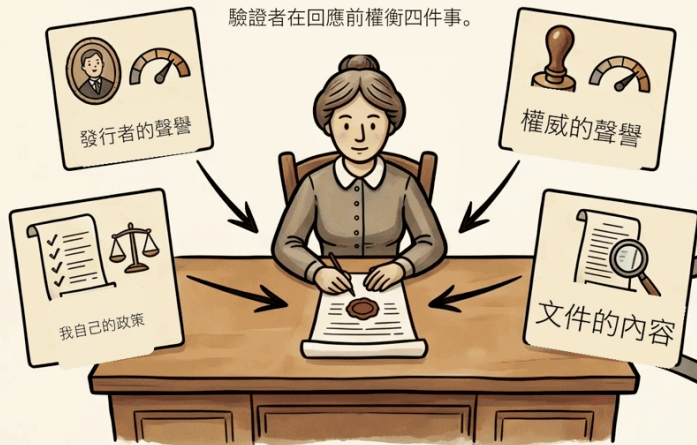
……但我無法預測權威會答什麼

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。

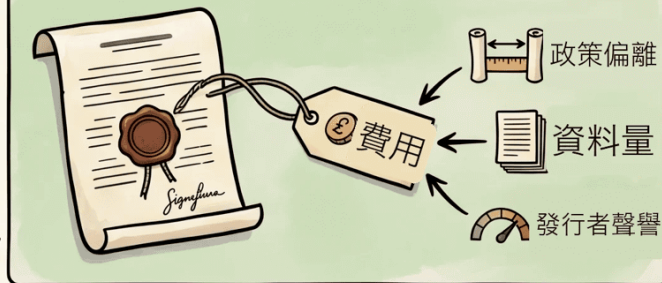


拒絕 — 附帶理由

- 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。

無論驗證者對你的驗證請求作出甚麼決定，皮球都會回到發佈者這一邊：他可以接受驗證者所提出的驗證服務條件，把回應折入時序記錄後再試一次（代價更高），或者一走了之、吞下已投入的沉沒成本。

為了讓你的資訊份量更重、在驗證者那裏更有機會被接受，作為對所簽發資訊有切身利害的發佈者，你可以動用一個**受信任權威**的服務。權威要麼拒絕所提交的資訊，要麼接受它並以自己的好名聲（聲譽）為它背書。權威通常會要求現實世界的證據，加以驗證並分類。其產出，是它在特定時刻對特定案例的評估協議。可以把權威想像成現實與數碼世界中某類服務的專家 — 例如調查員、審計師、保險商、某類貨品的供應商（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

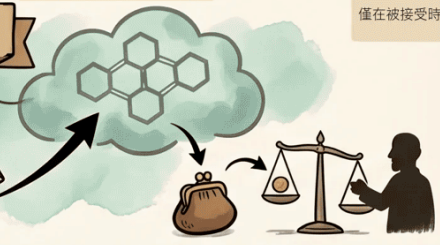
只有重試路徑會循環——接受與走開都結束故事。

驗證者提議——發行者定奪。

三條出路

接受這筆交易

DID 網絡



僅在被接受時

發行者付費——
紀錄被發布進網絡。僅在驗證者接受時可用。

再試一次



迷你磨製機



每次重嘗試成本更高

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



已花掉的時間與能量不會回來

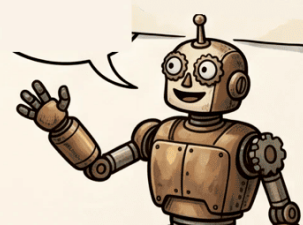


發行者捨棄草稿。什麼都不發布——
但也不再付出更多。

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

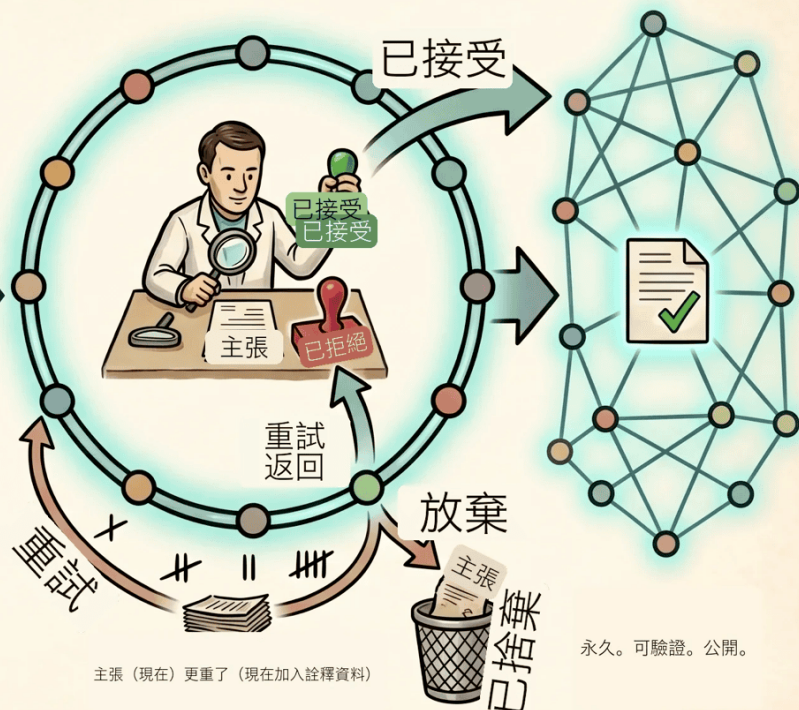


階段 1 —
發布主張

階段 2 —
質素過濾

階段 3 —
遞迴驗證

階段 4 —
永久紀錄



偽造昂貴。驗證便宜。

到你嘗試把資訊發佈到網絡的時候，網絡裏很可能已經包含了關於其行為者的資訊 — 這些就是聲譽信號。如何解讀聲譽信號 — 它們在不同情境下對你意味着甚麼、又帶有甚麼風險 — 可能並不簡單。每個參與者都可以透過自己的 DID，根據他正在處理的與對手方相關的情境，以不同的方式來看待聲譽紀錄。對手方是一位可靠的付款人，還是我在一筆生意裏需要要求先收錢？所提供的產品有沒有關於隱藏詐騙或缺陷的評價？當出事的時候，他們是否試圖推卸合約責任？有時候，對對手方整體一致性作一種較複雜的審視會派上用場 — 這取決於提出概覽要求的人的偏好。市場可以提供一些產品與服務，在當前情境的脈絡下簡化、處理並理清聲譽的解讀。各種權威及其提供的服務，也可以服務於這個目的。

■ 範例

對發佈者有興趣、對他人有價值的典型資訊，涉及的是現實或虛擬世界中超出日常人際溝通的事件。

負面例子：- 犯罪行為的證據（例如由受信任的調查機構審核過）- 間接證據（單獨看很薄弱，但在統計上可累積）— 例如短時間內多次出現在多宗盜竊案附近 → 還算巧合嗎？- 違約

正面例子：- 已彌補的傷害（自願，或在社群作為懲罰施加的壓力下）- 接受並服完由權威 X 提議的刑罰 - 權威 X 在一定程度上撤銷了對加害者財產權的承認

每個人都自行決定去蒐集關於對手方的可得資訊，並按自己的偏好評估風險。

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



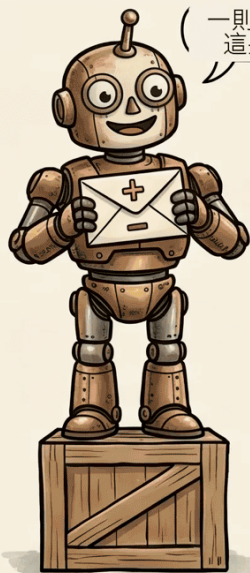
違約
未履行約定義務



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。

主張是行為進入網絡的方式。

■ 關於你的資訊會不會出現在網絡裏，只取決於你自己的行為。

你永遠不必加入這樣的網絡，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，就是一個受去中心化身份（DID）啟發的社交網絡可以如何運作。DID 概念的首要目的，是透過「認購我將遵循並據以生活的規則」這一原則，來加強私隱與自由 — 讓用戶有能力決定分享甚麼資訊，以及在甚麼條件下分享。

我進一步提議把各個 DID 連接成一個溝通網絡，讓其持有人交換反饋，甚至超出「某人身上發生了甚麼、社群或個人需要作出反應」的情境。這種對「我們所認購的規則」的預防性比對 — 加上可以計算雙方在「對方應如何行事」的期望上出現偏離時所帶來的經濟及其他後果 — 可以被視為尋求共識的一種動機。這樣的系統所強調的，不是自由，而是自願的抉擇再加上對現實世界行為所負的責任。

單一個體無法獨力破壞這個系統 — 一群人的機會更大，而一群已協商出共識、並在許多議題上有動機同心協力的人，抵抗威權傾向的機會就更大。第一章裏的「組織」前提，將在兩個條件滿足時得以實現：DID 聲譽網絡對社群的覆蓋足夠有代表性，以致使用它不再是甚麼稀奇之事。與此同時，這個社群板塊成為一個在經濟上舉足輕重的少數，足以強勢地與社會其餘部分談判。

■ 自願性 vs 自由

自由 — 就正面意義而言 — 會是平衡兩項因素的次生效果：自願性，以及周遭環境朝向責任所施加的壓力。

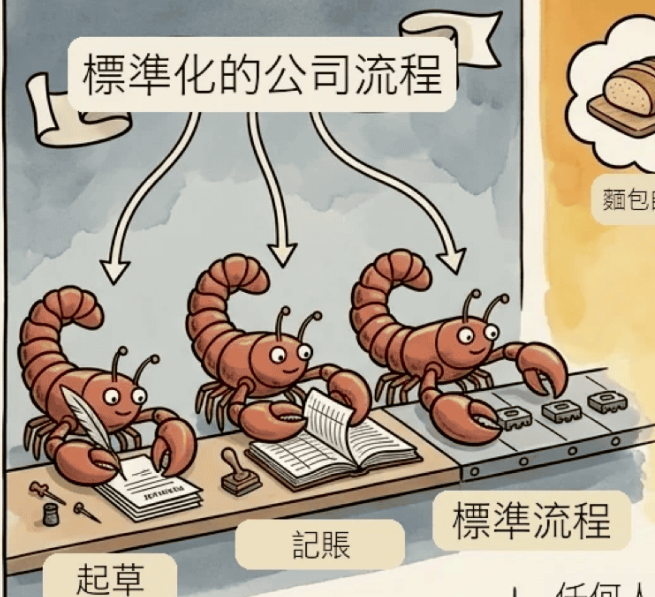
■ 人工智能時代與聲譽的價值

在人工智能的時代，一切與認知思維相關的東西都在被自動化 — 而且可能還會走得更遠。那麼，人類活動中還剩下甚麼可以作為競爭優勢？答案很難，而且必定會找到些甚麼，但有一件事我們可以肯定地說：聲譽將是決定性的。一部關於你行為、你的承諾及其履行的可驗證歷史 — 那是人工智能無法替你建立的東西。

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



那麼人類還剩什麼？



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。

一項接一項，重複性的認知工作正被交給代理。

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？



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



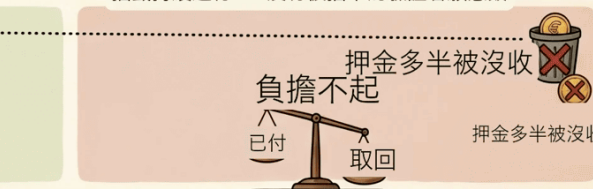
提交

抽籤



退款

賬簿



底部觀察者橫幅

演算法公平抽選。人們為自己的信念定價。

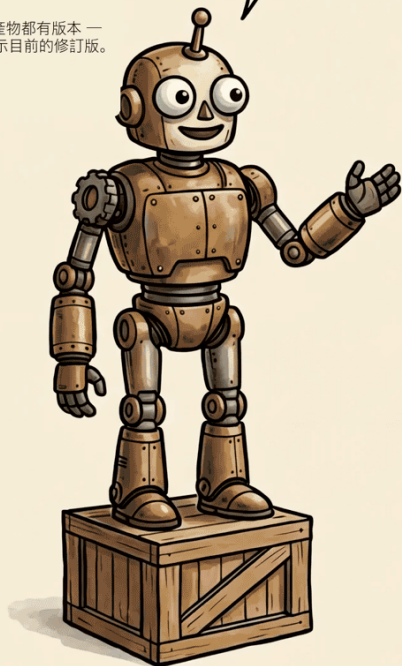


均勻抽籤。非均勻回應。離共識越遠，價格越高。

網絡中會發布什麼

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

你在網絡上的身分紀錄 —
金鑰、詮釋資料、網絡位址。

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

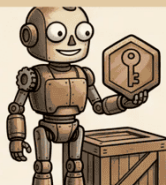
一個 DID 宣告的規則 —
用於驗證、共識與簽發。

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 文件是你在網絡上的身分證
— 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。



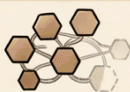
網絡位址

網絡能觸及你之處 — 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 —
但每個版本在網絡發布前都必須通過驗證。

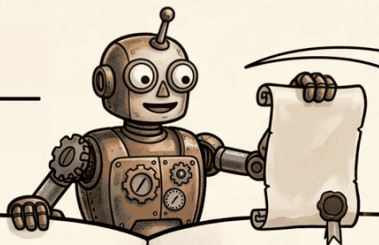
你撰寫它 — 網絡驗證它。你無法憑空把自己發布成存在。

你為自己的身分執筆 — 網絡加以確認。



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

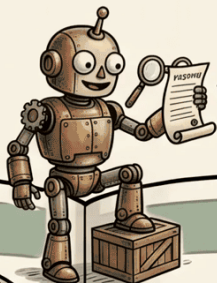


證詞 v5

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 — 我用我自己的公式

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。



網絡為何不可審查

到目前為止，我們描述了網絡能做甚麼。現在，讓我們把焦點放在它為何無法被關停或審查。

網絡很可能會建立在 Tor 網絡與洋蔥路由（一種利用 Mixnet 原理來遮蔽網絡流量的方法）的原理之上——這是一種讓通訊穿過若干層加密的技術，其中沒有任何單一節點能同時知道發送者與接收者。中央機構無法越過你的肩膀窺看，因為根本沒有一個可供窺看的位置。

你可以與它抗爭，但你贏不了——除非你把整個國家拖進極權式的監控，深入到單個網絡數據包，以及每一件接入互聯網並在該聲譽網絡上通訊的硬件上的底層操作。而這恰恰是中央集權所面對的抉擇：要麼接受公民手上有一件你觸不到的工具，要麼以極權控制之名，把自己埋進經濟停滯的陰暗角落。

我們不要抱有幻想——即使是民主政體，在其爭奪中央集權的鬥爭中也會嘗試這樣做。他們寧願把人套上枷鎖，也不肯交出權力。

你的訊息如何無法被追蹤

同時兩道防線 — 層層包裹與雜訊

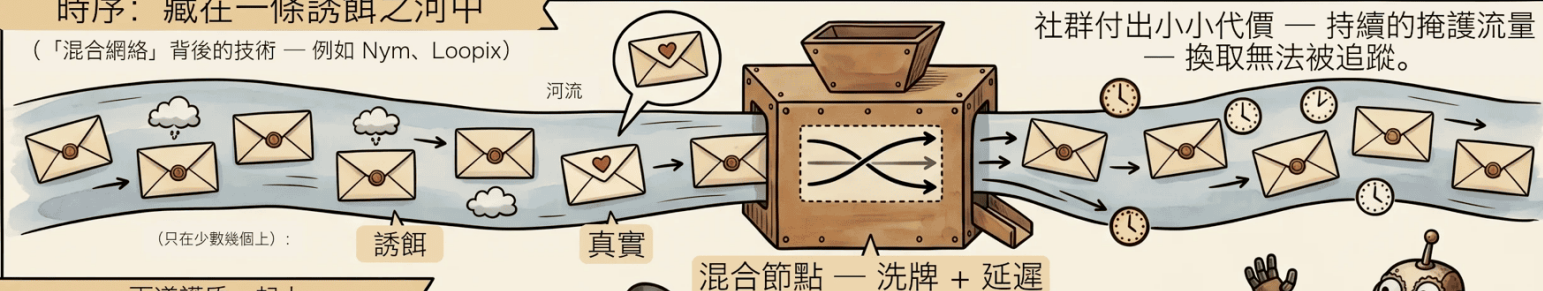
內容：層層包裹

(Tor 背後的技術 — 「洋蔥路由」)



時序：藏在一條誘餌之河中

(「混合網絡」背後的技術 — 例如 Nym、Loopix)



兩道護盾一起上

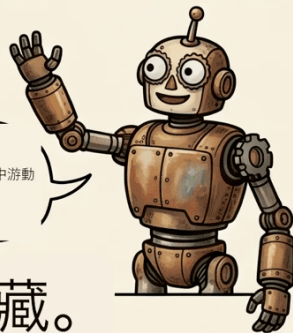
矩陣	隱藏誰？	隱藏何時？
只有層層包裹	✓ 是	✗ 否
只有雜訊	✗ 否	✓ 是
層層包裹 + 雜訊	✓ 是	✓ 是

(洋蔥路由 + 混合網絡 — 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出一連串問題。讓我們回應其中最常見的那些。

對技術的依賴

你大概已經注意到，與現代國家 — 它伴隨我們大約 150 年 — 不同，這裏所描述的聲譽網絡解決方案，嚴重依賴全球／本地互聯網的技術。一旦發生中斷，這樣一個網絡的運作就會有風險。

如果中斷是暫時的，網絡中的數據或主張的一致性都不會有損失，社群內部所達成的聲譽餘額也不應受到擾動。與可作比較的支付網絡不同，這個網絡假設的過程與數據項頻率非常低。在這一點上，去中心化聲譽網絡與今天的國家並無二致 — 國家如今也嚴重依賴技術，而且早已忘了怎樣用紙本卡片檔案來辦事（不過在危機預案裏它也別無選擇）。

以聲譽網絡形態出現的國家演化繼任者，在發生永久性中斷（一場規模空前的災難）時，可以退回到一個更原始的中心化系統 — 也就是國家。

技術讓人類得以邁向更高的文明化治理形態，並為我們帶來益處，但也帶來風險。

在網絡裏發佈，是不是把錢扔出窗外？

在聲譽網絡裏發佈一條主張的成本，大體上並非沉沒成本。發佈者投入網絡的訊息 — 關於真實冤情的資訊、經驗證的經歷、切中要害的警告 — 其有用性，在較長的時間跨度上，會以「為社群裏其他人的主張進行驗證所得的費用」這種形式在統計上回流。社群受益，發佈者建立聲譽，因而發佈真實資訊的成本就趨近於一筆可退還的按金，只需從中扣除較小一部分實際的網絡維護成本。反過來，不真實或無關痛癢的紀錄不會回流 — 它們的成本是淨損失。因此，誠實不僅是一種道德抉擇，也是一種在經濟上理性的策略。

兩條路 — 國家關閉，網絡開啟

聲譽網絡

國家

什麼都不做，就是選了那扇對的門。

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。網絡憑選擇開啟。

庫門仍在關閉。另一扇門仍然開著。

選一扇 —
否則選擇會選你。



在扣除網絡維護成本之後，這個原則可以稱為經濟中性原則 — 當我與社群同在時我不會虧，當我與它作對時我才會虧。

社群也有一些團結互助的渠道，用來嘉許其成員的誠實態度。但我們不要抱有幻想：訴諸團結多半源自社群的社會壓力，所以這未必是「自願」這個詞本義上的團結。

如果有人創建多重身份怎麼辦？

一個人可以並行運作多個 DID 身份。然而，為每一個身份建立聲譽都需要獨立的付出 — 時間、能量、金錢。

沒有捷徑：每一個身份都必須透過實際的活動來累積它的往績¹。因此，維持並行身份是刻意設計得很昂貴的。

在自由社會裏，這些成本會令濫用得不償失。

然而在獨裁政權下，並行身份卻成為一種求生工具：它們使地下網絡的組織、黑市中更安全的周旋，以及區隔化²的抵抗成為可能 — 在這種抵抗裏，一個身份被攻破並不會暴露其他身份 — 而且在政權倒台之後，它們讓人得以無縫地重返公開生活以及在那裏建立起來的聲譽，甚至可以透過一條主張，把先前官方的與秘密的 DID 合併成單一的一組合併紀錄。

¹往績 (Track record) — 一般而言：一個人或組織過往結果、成功與失敗的歷史。此處：某個 DID 身份在網絡中所有過往互動的總和 — 已驗證的主張、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, 源自英文 *compartment*) 指把資訊分隔成互相隔離的單元，使得一個單元被暴露不會危及其他單元。這是一條為情報機構所熟知的原則：一名特工只知道自己那部分行動，因此即使身處脅迫之下，也無法供出全局。

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

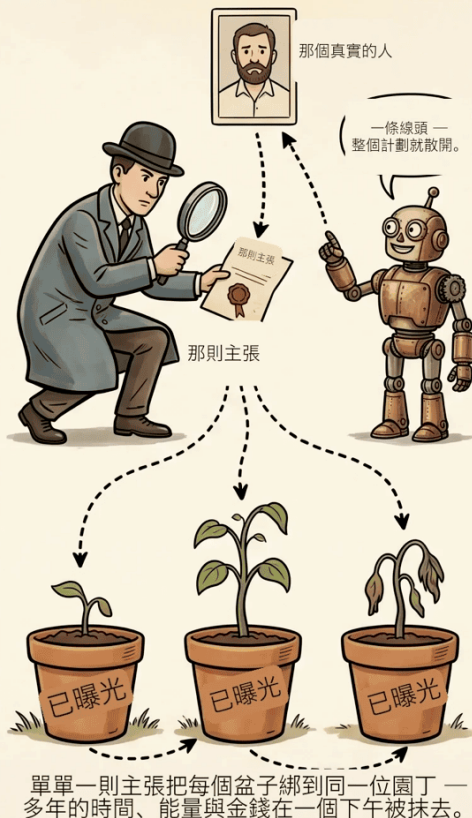
在自由中 — 一個代價高昂的備案



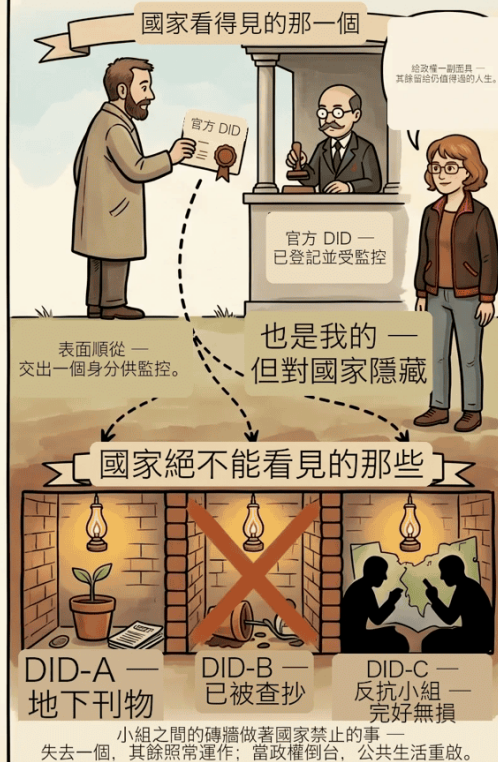
或 — 一個人失足後的一張白紙



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。

■ 感知被翻轉過來

與國家不同，建立在去中心化身份之上的聲譽網絡，其原則把「所感知的優先次序」這一範式翻轉了過來：

- 重要的是聲譽 — 亦即用來評估與對手方互動風險的「過去」 — 而姓名、地址等個人資料，可以是一種出於禮節的數據交換
- 而國家則首先索取個人資料，累積聲譽性數據，然後只讓社群看到合它心意的部分

有錢人難道不能乾脆「買下」更多身份（或創建虛擬社群）嗎？

創建並行去中心化身份的可能性，乍看之下像是讓經濟實力較強的人相對於實力較弱的人佔了不公平的便宜。然而必須強調，與中心化系統不同 — 在中心化系統裏，只需腐蝕權力金字塔上的幾個點，就足以讓某些惡行消失 — 在去中心化系統裏，人得腐蝕整個社群。

替代性的去中心化身份可以服務於這個目的，但它們的聲譽必須隨時間透過與真實的其他社群成員進行真實互動來建立 — 它無法被簡單地買到，因為網絡讓「某個身份表現如何」變得可驗證。

此外，市場上可以（而且很可能將會）存在一些服務，它們作為權威，提供調查、產出證據，證明幾個去中心化身份其實是同一個人。因此，只需錄入聲譽網絡的一條紀錄，就能以極小的成本，抵銷掉為建立並行身份所投入的全部時間、能量與金錢。

所以在經濟上，不欺騙社群才是划算的 — 如果有需要，就審視自己的作為並着手彌補，讓聲譽回到可接受的水平，使其持有人不致因社群的怒火而在經濟上或其他方面吃虧。

一個在自己社群裏喪失了聲譽、經濟實力雄厚的身份，可能會試圖透過與特定身份的暗中交易來逃避社群的怒火 — 但那些身份屆時也會冒着失去自己聲譽的風險。

還剩下一條逃路：帶着一個全新身份逃到另一個社群 — 但那意味着拋下一切成就，在某處從零、從零聲譽重新開始。有時候這可能是一條可以理解的路，也是唯一的出路。

■ 註

同樣地，社群也會這樣應對一種攻擊 — 有人投入資源去創建一個虛擬身份：對那個身份而言，未經驗證就與另一個社群發生互動 — 也就是不加批判地接受關於對方社群身份的資訊 — 是有風險的。聲譽永遠是在一個社群內部建立的，而非全球性地建立。

那些只想讀取、卻不給社群貢獻任何東西的「搭便車者」怎麼辦？

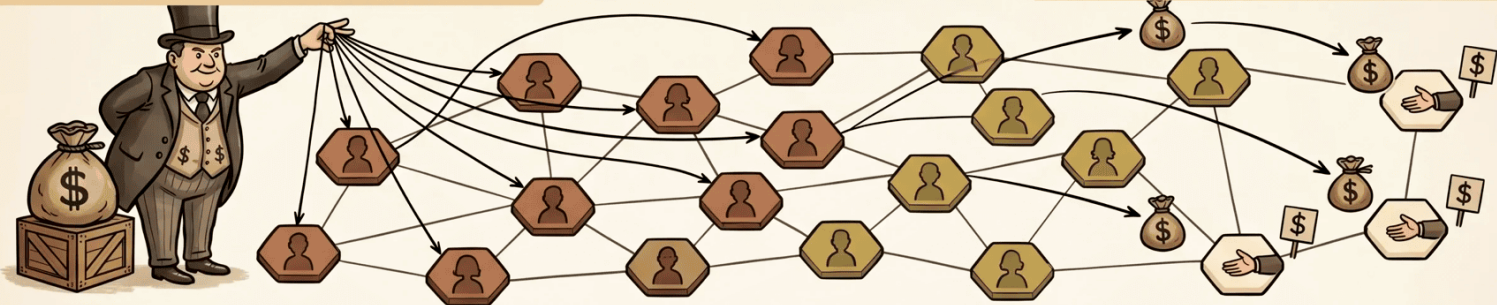
從創建去中心化身份的第一天起，對資訊的取用就不是無限制的。新的參與者 — 那些尚未透過實際活動建立聲譽的人 — 會面對分級的限制：資訊更少、等待時間更長、查詢成本更高。網絡獎勵的是參與，而非被動的消費和任意的數據收割。

當一個去中心化身份為了報酬把自己的聲譽借給另一個人（那人甚至可能根本不在 DID 聲譽網絡裏）時，它也在拿自己的聲譽冒險。這裏適用同一條原則：這種對社群的背叛（侵犯私隱），會反映到背叛者的聲譽上，而且這件事無法像在中心化系統裏那樣，透過一筆暗中交易被抹去。他必須面對社群的怒火，包括成就的喪失 — 因為在他眼中，社群正是諸如「擁有動產與不動產這一特權」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

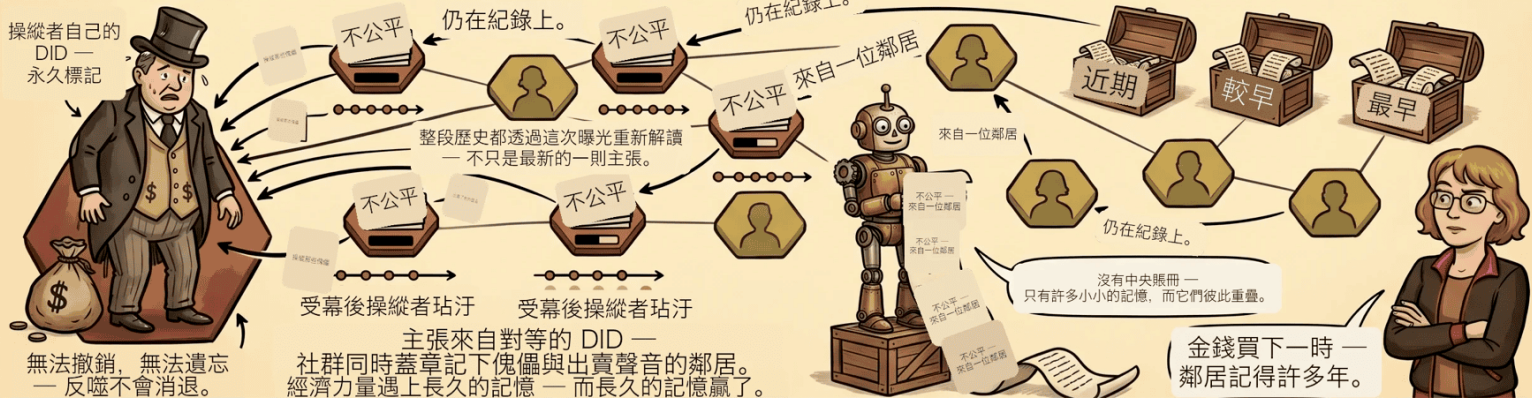


經濟力量能把絲線伸進任何社群 — 沿途還買下幾個真實的聲音。起初，看起來富人只是擴大了他的交友圈。

稍後

防禦 — 長久的記憶，分散的記賬

每位鄰居保有自己的記憶 — 沒有中央賬冊，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，較有風險的主體，自然是那個不享有某社群所承認的擁有權特權的人 — 他在交往中可失去的東西更少（數碼資產更容易轉移）。

這看似一個小細節，卻有重大後果。想讓社群對其成員擁有制衡力，就意味着把擁有權當作一種特權 — 在最自由的社會裏它近乎不可觸碰，但它仍然不是一項權利，也不是一條根本原則，而是一種特權，在極端情況下可能被撤銷（例如，我可以想像在武裝衝突中拒絕為保衛社群而服務的情形）。

它也在潛移默化中回答了：社群將如何對待其成員，以及一個成員為社群而戰的動機何在 — 就是為了保住自己的特權。一個人可以在他對社群的責任上失敗，但在道德上不能指望，當涉及保住來之不易的特權時，還會得到寬待。

財務中性

讀到「去中心化、不可審查、不可腐化」這些字眼時，人難免會把它們與最為人熟知的加密貨幣 — Bitcoin、Monero，還有比方說 Kaspa — 聯繫起來，這些貨幣的確可以用這樣的字眼來形容。然而直覺在這裏會誤導人：權威服務、驗證與發佈等等的費用，可以用任何貨幣或金錢結算。對 DID 網絡中社交網絡的相連參與者（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，證明款項已經支付。發佈一條主張，個別地必須帶有一份合理、可驗證的成本，這樣一個行為者才不能想發多少、想發哪些主張就發多少、發哪些，而無需耗費能量、金錢與時間 — 後一種狀態極不可取，對應的正是今天那些腐敗叢生的國家系統裏精英所享的特權。

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
個項目



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

時間 能量 金錢

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
個項目

時間 能量 金錢

時間 能量 金錢

55 歲 — 權威

聲譽 95%

交付 15
個項目

權威——
你驗證他人，網絡付你報酬

時間建構曲線 —
你自己的努力能讓它更陡。

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。

隨著你事蹟的賬簿填滿，門逐漸開啟。

搭便車者——只讀，從不發布



讀取其他所有人的紀錄。

我的貢獻

自己什麼都不發布。

投入真實工作的時間、能量與金錢——是網絡唯一尊重的貨幣。

受限存取 — 天花板不會升高

網絡回報那些投入的人。

聲譽 5%

沒有事蹟，沒有提升——年復一年，同一條線。

在這一點上，前面提到的那些加密貨幣有一個小優勢：它們的網絡充當受信任的權威，用以驗證某筆款項確實發生過，代價是損失一點私隱，並暴露自己的部分地址。

自願性、責任與自由

自願性是個人的：我自己替自己作決定。責任在我的決定影響到他人時產生 — 反饋隨即啟動。自由既非恩賜，亦非權利 — 它是自願性與朝向責任的壓力之間、成千上萬次雙邊互動在整個社會中取平均之後所得的一種現象學³結果。網絡並不規定這個平均 — 它是從驗證者的價格信號、以及社群成員為自己設定的預先公佈的驗證政策中湧現⁴出來的。

一個處於社群中的個人對自由有多少偏好，取決於他對「自己願意吞下多少他強加於他人之物」的感受。對那些不言自明、且對所有人都有益的事情，並不存在道德兩難 — 謀殺是錯的。然後有一些情況，選項轉移到「被允許的特權」這個位置上：先證明你的技能，我們才讓你上路，這樣你撞死我們的機會就小一些。最後還有一些事情，個人會說 — 這對我不值得，我不會禁止我的鄰居燒樹葉，因為我自己也燒，或者因為我做着別的一些限制他舒適的事情，而他反過來也可能想禁止我這樣做。如果歷史上我們是把自由的界線劃在「他人自由開始之處」，那麼建立在去中心化身份之上的聲譽社交網絡，在這一點上做得比中心化的代議民主更好 — 在代議民主裏，例如那一層享有特權的民選代表，試圖讓自己豁免於對私人通訊的監控，卻毫不猶豫地把這種監控強加於他們的選民身上，還動用各式各樣暗地裏的藉口與操弄。

³現象學的 (Phenomenological, 源自希臘文 *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考察的取徑，透過觀察由現象所引出的結果，而不預設底層微觀世界的解釋理論。此處：自由不是一條自上而下定義的抽象原則，而是一種被觀察到的現象 — 是人與人之間成千上萬次微互動的結果，從我們實際上如何彼此相待中湧現出來。

⁴湧現的 (Emergent, 源自拉丁文 *emergere* — 浮現) 意指「從較簡單部分的互動中自發產生，而無人設計或指揮」。一群鳥即使沒有哪一隻鳥對隊形有計劃，也能列隊飛行 — 隊形是從每一隻個體所遵循的簡單規則中湧現出來的。同樣，在聲譽網絡裏，沒有人設計整體的行為規則 — 它們是從成千上萬個個別決定中湧現出來的。

自願性 → 責任 → 自由

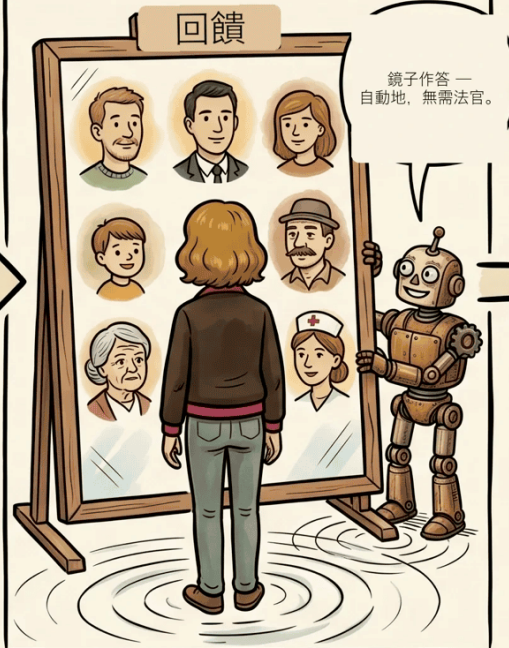
三步 — 從一個人的選擇到整個社會的模式

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 網絡中的一個簡單機制，能把整個系統推向更多自由或更多控制：一個 DID 在每個時段可以發佈的紀錄數量。當紀錄保持稀缺時，每一條都份量十足 — 那就是自由。當紀錄氾濫、連雞毛蒜皮的事都覆蓋時，那就是極權。你每發佈一條紀錄，都是在為方向作抉擇。網絡本身既不自由也不極權 — 它是中性的基礎設施。它會變成甚麼，取決於人們如何使用它。

在我自己的驗證政策裏，對我社交網絡中的一個一般 DID — 在社群內部 — 設定一個「發佈者每個時段可簽發的主張（泛指任何可驗證的陳述；此處指發佈到聲譽網絡的一條紀錄）的最大數量」是說得通的，超過這個數量，我才會把它們納入考量、才會認為它們的驗證請求切題。

我心裏有一個直覺的數字 — 每年低個位數。這種帶審查性質的取態，看起來或許相當孤立主義。但我可以正當地把申請人置於一個抉擇之前：從他已簽發的紀錄中挑一條，請驗證者撤銷它，也就是使它作廢 — 而在申請人恰好真的成了多宗互不相干的冤情受害者的情況下，這是一個相當咄咄逼人的要求，而我這樣做，肯定也會加深他被社群疏離的感受。

因此，一個更有效的選項似乎是：把自己一部分「向聲譽網絡發佈資訊」的權利，委託給一個社群或一個權威，讓它按其內部規則、以互助的方式來決定如何分配這些權利。一個群體必須有能力照顧它認為處於弱勢的那些人。社群成員有權在任何時候，只要被委託的權利尚未被使用，就撤回自己的委託。

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。網絡本身是中立的；我的政策不是。

每位讀者轉自己的轉盤
網絡沒有共通的那個。

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

每個點數決定計入原由主張，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 — 那隻眼睛從不眨，鄰居不再交談。

自由是我拒絕計入的 — 極權是我同意追蹤的。

發布權的委派

你把金鑰借給為你服務的權威 — 並在一瞬間收回



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。

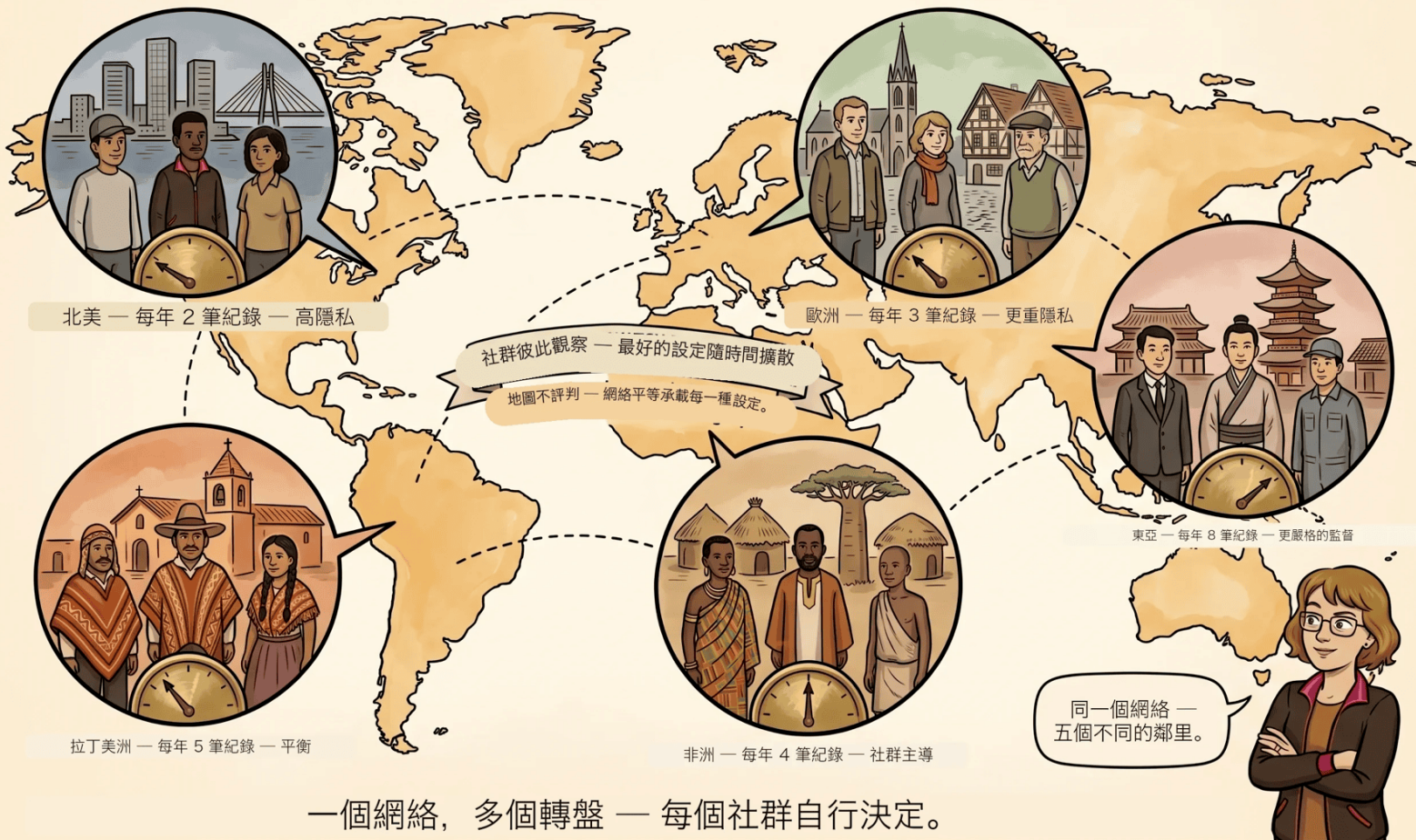
借出金鑰 — 保留線頭。委派絕非交出。

■ 自由 vs 極權

一個看管並限制所發佈紀錄數量的社會，會更自由；一個紀錄過剩的社會，則會傾向極權。人們可以設想把發佈紀錄的權利委託給別人。

每個社群自我設定

網絡不歧視 — 每個地區設定自己的轉盤



■ 文化適應

人們大體上都喜歡窺看彼此的碗裏有甚麼。跨越不同文明，我們在歷史經驗與人口密度上各不相同——因而在「文明與社群內部我們想窺看彼此碗裏東西的程度」上也各不相同。亞洲國家傾向於對社會自由持較嚴格的看法；歐美國家在某些方面則傾向較自由。無論這條類比多麼不精確，在去中心化聲譽社交網絡的脈絡裏可以說：各個社群的設定並不歧視，每個社群都可以按自己認為合適的方式，配置其內部的溝通。

儘管存在差異，仍會有一些為全球所公認的標準（隨機殺人對誰都沒好處）。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、透過觀察周遭的設定，可以尋求共識——從雙邊安排，到社群層面，再隨着時間，憑藉配置得最好的那些社群的經濟優勢，甚至上升到全球層面。

不過關於共識，下一章再細談。

預言機問題 — 架接數碼與物理世界

「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聯繫在一起。一般而言：你如何確保進入數碼系統的數據，忠實地對應到物理世界中實際發生的事？系統本身無法驗證某人是否真的傷害了另一個人，或某份合約是否真的被違反——它只看得見數碼紀錄。

在這裏，我們透過權威來解決這個問題——這些實體以自己的聲譽作賭注，擔保數碼紀錄對應於物理現實。權威的聲譽越高，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

共識與驗證過程

要就「一個社會平均而言應當持守並執行哪些規則」建立共識，以下這套機制能派上用場。作為一名 DID 參與者，我宣示我所認購並將據以生活的規則，並把它們發佈出來。（可以把它看作那些在我看來構成我理想世界的章程與規約 — 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 — 並評估在普通的社交或商業互動中，若這些互動假設性地發生，我會被誰、以多大力度加以制裁。

決定性的評估發生在你向另一個 DID 索取資訊、或請他驗證一條你想發佈到聲譽網絡的主張（或向某個權威請求一項服務，等等）之時。它的結果應當與你自己在乾跑（dry run）中對照對手方所宣示的政策所作的評估一模一樣 — 如果不一樣，那麼對手方那一邊就有問題：他們在試圖玩一場不誠實的遊戲。

結果要麼是接受，並附上一個驗證的報價（在驗證者或權威服務的情況下），要麼是拒絕。對「偏離評估者政策」的制裁與獎勵，都折入這個報價之中。請求者隨後決定是接受條件，還是走向分配演算法中的下一輪驗證 — 重複這個過程，直到滿意為止，或直到經濟上不值得再繼續為止。

■ 社交圖譜

聲譽網絡首先是一個社交網絡。你添加聯絡人 — 那些同意連接的人。他們有聯絡人，而那些聯絡人又有聯絡人。演算法在一個可配置的深度內搜尋驗證者（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 — 網絡會自然而然地形成社群，並與其他社群有所重疊。

演算法是非確定性的：它把你的主張文件做雜湊，把雜湊映射到這個圈子內已知身份組成的環上的一個位置，並選取最近的那一個作為候選驗證者。你無法預測或影響誰將驗證你的主張。

每一位驗證者的拒絕，都會擴大你的文件並增加它的處理成本 — 那是第一條成本渠道（文件增長）。每一位新的驗證者，都會依據數據量、你的聲譽，以及你主張的內容偏離其所宣示驗證政策的程度來收費 — 那是第二條成本渠道（風險溢價）。而每一次迭代都耗費時間與能量 — 那是第三條成本渠道。

■ 驗證者依次檢查甚麼

一旦被選中，驗證者大致按四個有序步驟來評估一條主張 — 最便宜的過濾器在前，昂貴的內容檢查在後：

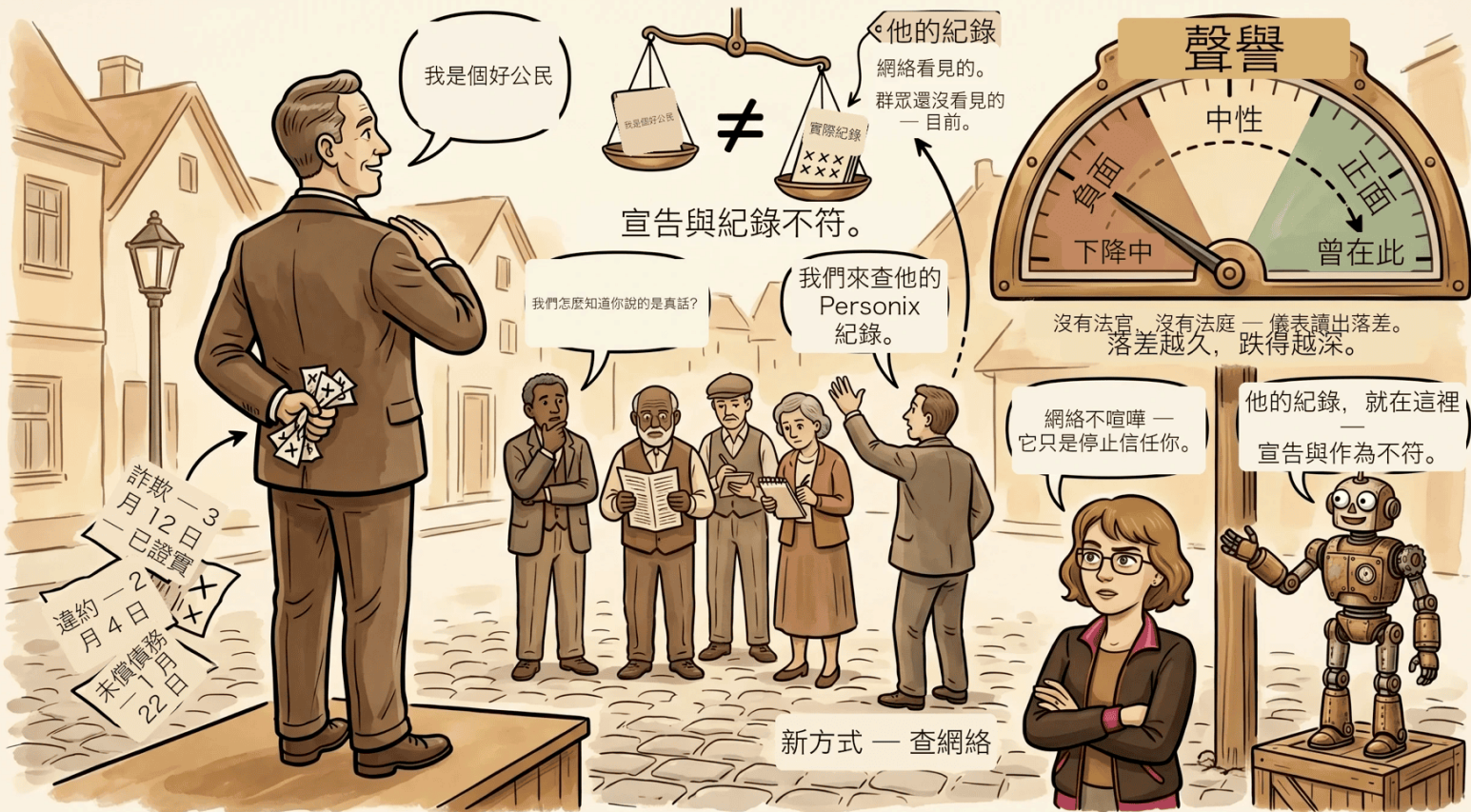
1. **政策把關。**這類主張是否落在驗證者公開驗證的範圍之內？若否，請求即被直接拒絕。
2. **權威信任。**為該主張背書的權威，在驗證者自己宣示的政策下是否足夠受信任？一個低於驗證者信任門檻的權威，無論主張內容如何，都構成拒絕的理由。
3. **簽發者聲譽。**簽發者是否達到驗證者為這類主張所宣示的聲譽門檻？低聲譽可能提高費用，也可能觸發拒絕。
4. **內容檢查。**只有在前三道關卡都通過之後，驗證者才會評估主張本身 — 簽名、內部一致性、形式正確性，以及它偏離驗證者政策的程度。為這最後一步所收的費用，反映的是實際承擔的風險。

驗證者會發佈管轄上述每一道關卡的政策，因此這些步驟並非任由他自由裁量 — 他受制於自己已經宣示過的東西。偏離已發佈的政策本身，就是一條可以針對他發佈的主張，而他要用自己的聲譽為此付出代價。

結果就是：發佈一條可信而有用的主張，成本幾乎為零。發佈一條激進的主張，成本更高。發佈一個謊言，則變得貴到令人卻步 — 你必須一位驗證者接一位驗證者地迭代下去，而每一位拒絕你的人都在增加成本。市場為你的主張定價，而這個價格告訴你，相對於你所置身的那些社群，你站在甚麼位置。

網絡悄悄比對你的言語與你的紀錄 — 落差人人可見

網絡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。

僅僅宣示你遵守某條規則，而現實中你並不遵守，是不夠的。在那種情況下，你的 DID 就要冒着被發佈一條負面紀錄、揭穿其虛偽的風險 — 這會把你變成對其他所有人的風險。其結果應當是：規則更少，但被更一致地遵守，並清理掉那片連法律專業人士都幾乎理不清的法律與規例叢林。

■ 共識 vs 問責

要讓網絡充當有價值的資訊來源，一個 DID 不應太過激進 — 否則其他人會拒絕它。社會壓力會尋求均衡，而試圖破壞這種均衡的舉動很可能會受到懲罰。

偽善的解方

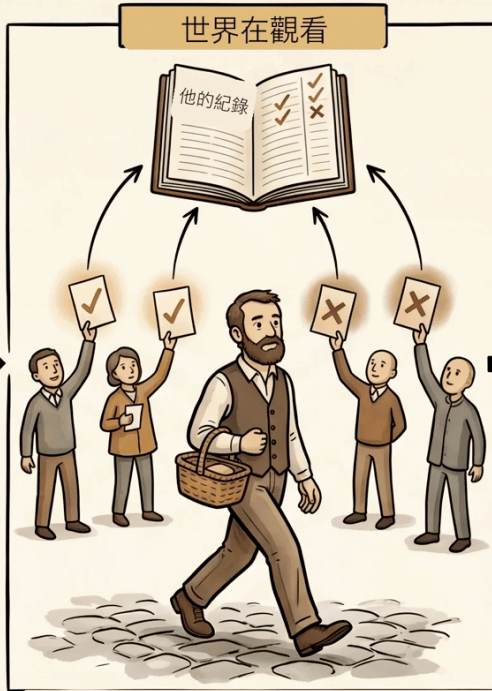
宣告你的規則 — 依此而活，否則市場把你定價出局

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，他的賬簿上多添一點證據。

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。

■ 票數並不等於一把聲音的份量

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。

由此可見，從賢能制的角度看，凡是貢獻更多而又沒有壞聲譽的人，理應在社群中擁有更大的聲音份量。透過雙邊關係的鏡頭來看：當我掂量該遷就哪些共識壓力時，最大的份量歸於那些讓我獲得最大經濟收益的關係。十個與我沒有實際交易往來的人，對我的影響，遠遠比不上一個長期的生意夥伴。這一範式不限於商業 — 它延伸到社會、政治及其他關係。

Roles in the verification transaction and authorities

角色概覽

在講網絡及其基本特性的那一章裏，我們已經簡略觸及過其中一些角色。現在是時候更詳細地再看它們一次，並補上那些讓網絡更為穩健所需的角色。每一筆驗證交易都涉及若干角色 — 讓我們看看它們如何運作。

■ 驗證交易中的角色

每一筆驗證最多涉及六個不同的角色，概括於下表。它們全都可以在去中心化聲譽網絡中擁有自己的 DID。

角色	說明
Issuer (簽發者)	把資訊發佈到網絡的人 — 主張某件事發生了（一個 DID 被創建、編輯或解散，一條主張，某個 DID 的政策，等等）
Subject (主體)	資訊所關乎的人 — 主張的對象
Authority (權威)	一個受信任的實體，透過調查主張、審閱所呈交的證據或主動蒐集證據，以自己的名聲為主張的質素作賭注
Observer (觀察者)	一個獨立的第三方，紀錄驗證者如何處理主張 — 確保驗證者既不保持沉默，也不偏離他所宣示的政策
Verifier (驗證者)	一個由演算法選出、負責處理交易的參與者
Delegate (受託人)	一個代另一名參與者行事的人

簽發者

我們之前已經見過簽發者。當某人受了冤屈，或想把自己的一項成就廣而告之時，正是那個由 DID 所代表的人，觸發了把該資訊放進網絡的過程 — 因為他對此有首要的利害關係（動機要麼是渴望得到滿足，要麼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，我可以作為它的主體兼簽發者保留起來，留待我想使用它們的場合（一張文憑、一份服務證明等等）。這正是正面主張與負面主張的分別所在：分享一條已驗證的負面主張，符合整個社群的利益，而分享一條正面主張，則符合其持有人的利益。

權威

權威扮演雙重角色：它既可以是**審計者**（在一條主張被發佈之前，驗證證據的質素），也可以是**擔保者**（以自己的聲譽為一條主張的真實性作賭注）。無論哪一種，它都在加強簽發者的主張。這兩項服務是可分離的 — 一個權威可以只提供其中一項、另一項，或同時提供兩項。基本假設是：權威所提供的大部分服務，都可以在自由市場的基礎上交付。即使在那些難以想像可以私有化的領域也是如此，例如司法 — 在那裏，各種專門服務（調查、證據評估，一直到今天由中心化軍隊提供的服務，如戰略規劃、標準化訓練、採購與庫存管理等等）都可以由市場行為者高效地交付。幾乎沒有甚麼東西，在重組之後不能藉着自由市場的激勵而變得更有效率。

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、簽發者與觀察者，絕不能是自己案件的驗證者。

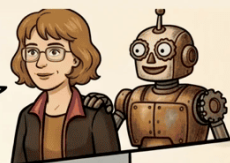
演算法式的驗證者選取，保障了獨立性。沒有人可以驗證自己的主張，或一條自己有直接利害關係的主張。這是整個 DID 社群都有利益去維護的基本規則之一。

以下的圖示，從互補的視角展示了權威所涵蓋活動的廣度（「權威」一詞可與「服務提供者」互換理解）。

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。

■ 作為隱身觀察者的權威

一個聲譽卓著的權威 — 想像一位生意完全繫於其往績的公證人 — 可以在主要功能（審計者／擔保者）之外，再提供第三項功能：在驗證過程中充當隱身觀察者的角色。他為所提交的主張保存一份帶時間戳的紀錄，使驗證者無法悄悄把它丟棄。觀察者角色的機制，會在講「觀察者」角色的那一節裏進一步描述。

驗證者

任何 DID 都可以充當驗證者，無論是直接充當，還是透過委託給第三個 DID 的驗證權來充當。為了讓我 — 或我的受託人 — 能夠驗證，我應當在網絡上可達（在線）。並非人人都願意作出這樣的承諾，這正是為何一個 DID 的紀錄裏，可以按優先次序列出一些替代者，在它離線期間代它履行這項功能。

網絡中每一個活躍的 DID，都公開宣示自己的政策。透過該政策所定義的規則，它在驗證過程中判斷對手方的聲譽，以及簽發者已標記待發佈到聲譽網絡的那條主張的內容與形式。政策的一部分，是用來計算驗證服務費用的計算公式。這一切就位之後，在統計上大量流經網絡的主張之中，我等待網絡的演算法把我抽到簽發者那一邊，並在某一次迭代中把我指派為所簽發資訊的驗證者。簽發者可以事先計算一個行為正確的驗證者會如何反應，但無法迴避實際去接觸他（或他的替代者）；與被選中的驗證者進行的那次迭代，即使簽發者事先知道通不過，也必須由簽發者實際完成。

我們怎麼知道簽發者是在正確的一組候選驗證者 DID 上運行驗證者選取演算法的？每一個 DID 在公開宣示其政策的同時，也會發佈其在聲譽網絡中社交網絡的當前識別碼清單。如果一個簽發者把自己的社交網絡界定為一個只會附和並強化其自身觀點的社交泡泡，那麼透過它發佈的資訊，將很難被其他社群更廣泛地接收。我不惜高昂代價把一條激進主張塞進網絡，並不意味着在判斷對手方聲譽時，我會賦予它任

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。

何份量。有些主張是我的社群逼我納入考量的（施加於犯錯者的刑罰與限制）；另一些則完全由我自己決定——是否納入某項資訊，其經濟價值由我自己來判定。

主體

發佈到聲譽網絡的資訊所關乎的那些人，就是資訊的承載者，或者你也可以叫他們主體。聲譽網絡中的激勵是這樣設定的：主體有充分理由按自己的規則正確、公道地行事，並被社群推向某種恪守規則的黃金中庸。他們甚至有動機做得比自己所宣示的規則更講道德——預先宣示的政策，並不排除社群達成共識、追溯性地施加某種評估或措施。從這個角度看，聲譽網絡對法律秩序的替代方案，正如人們所料，更多地是由規則的精神、而非規則的字面所驅動的。

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鑽規則空子的動機。在驗證者不喜歡簽發者或權威的請求的情況下，他大可乾脆保持沉默 — 不作回應，卡住演算法的序列。觀察者 — 或一組觀察者 — 以自己的聲譽作賭注，記錄驗證者是如何被查詢的。如果驗證者明明有一份表明相反做法的宣示政策，卻仍保持沉默，那麼他就可以被判定違反了協議。

機制：時間戳與挑戰碼

在你把一條主張發送給驗證者之前，你先讓它經過觀察者 — 你信任的人，或收取小額費用的專門觀察者服務提供者。每一位觀察者收到你的提交後，為它蓋上時間戳，簽署證明自己看見它發出去了，並生成一個挑戰碼 — 對其簽名所作的一個密碼學雜湊。這些挑戰碼會附加到你的請求上。驗證者看得見它們，卻毫不知情觀察者是誰，甚至不知道這些碼是不是真的。因此，觀察者充當簽發者與驗證者之間的代理，持有一份獨立的紀錄，證明該主張已被提交以及它包含甚麼內容。他們的數量可以是零到 N 個。

當驗證者誠實行事 — 按其宣示政策接受或拒絕 — 時，這些碼保持不透明。沒有人被暴露。

但如果驗證者明明有一份寬容的政策卻仍保持沉默，或以一種與他所發佈之物相矛盾的方式回應，那麼你手上就握着最初那些觀察者的簽名。你可以把它們作為代理證言發佈出去，證明該主張已被提交，而驗證者沒有遵循協議。任何人都可以驗證這些簽名與挑戰碼相符。

妙處所在：你根本不需要真實的觀察者

而最精妙的部分在這裏：**你根本完全不需要真實的觀察者**。你可以生成一些看起來與挑戰碼一模一樣的隨機數。驗證者分辨不出區別 — 他不得不擲骰子賭一把，決定是否拿自己的聲譽去冒險。在他收到的每一個請求背後，都可能有一位受尊敬的觀察者在隱身守望 — 也可能純粹是噪音。驗證者並不知道。而那份不確定性，正是這個機制的所在。

觀察者 — 轉遞主張並觀看往返的代理

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。



觀察者做什麼

1.
從發行者收到主張

2.
蓋上她的印章：那個印章就是加了時間戳的紀錄

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徽章
—— 她的聲譽就是保證

註腳

© 2014 香港中文大學。所有權利保留。此圖為教育用途而設計，不得用於商業目的。如需轉載，請向香港中文大學圖書館申請。

看得見代碼 —
看不見是誰。

對大眾匿名，對網絡當責。驗證者看見代碼，永遠看不見觀察者。

* 對稱地，驗證者也可透過自己的觀察者轉遞回應 — 同樣的把戲，相反的方向。

維持誠實壓力的成本：近乎為零（隨機數是免費的）。對驗證者而言，不誠實的潛在代價：災難性的。即使根本沒有人真正守望，誠實的行為也被激勵着。

這個系統之所以有效，是因為人人都有點疑神疑鬼。不確定性比監控便宜。

■ 單次迭代中的多個驗證者

對於驗證者可達性，一條起加強作用的伴隨規則，可以是一個演算法擴展 — 在單次迭代中返回一組候選驗證者，而不只是一個。

委託

文明把它的經濟增長建立在分工與專業化的能力之上。世界在其全部壯麗之中是複雜的，而我們把它的全部複雜性一把抓住的機會近乎於零。自然的出路是把「一大堆支撐舒適生活的活動」委託給專門的提供者，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 — 提供我們最擅長的、或市場在我們身上估值最高的那些服務。

同樣的委託邏輯，延伸進聲譽網絡。在《自由—極權開關（以及委託）》那一章裏，我們闡述了透過限制「在特定時間窗內可發佈到網絡的主張數量」來保障自由社會的原則（簡化地想，每年低個位數的發佈權，好讓社會保持最大程度的自由）。這條原則可以擴展到多個維度。我們不必只有一個數字 — 我們可以有若干個限額，適用於不同類型的主張。針對「揭發他人虛偽」與針對「生意往來中的不當行為」，我們可以用不同的數字，而比方說，DID 文件的變更（例如改密碼）之類的事，社群大概根本不會在意，如此等等。這一切都取決於社群在演化的時間裏，如何界定甚麼才符合它在「其目標自由水平與問責之間找到恰當平衡」上的利益。

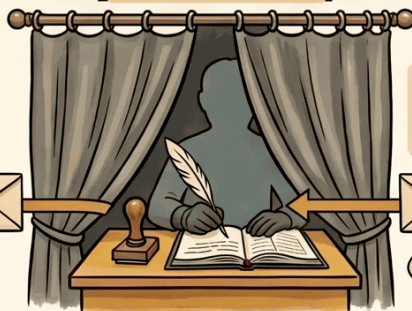
讓驗證者保持誠實的虛張聲勢

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】

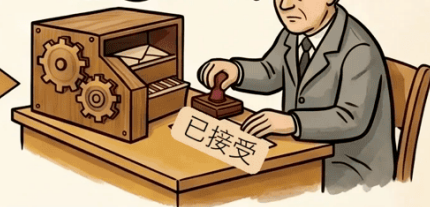


【驗證者】

挑戰碼 —
加時間戳紀錄的雜湊

已簽署的挑戰

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】



看起來一樣。成本：零。

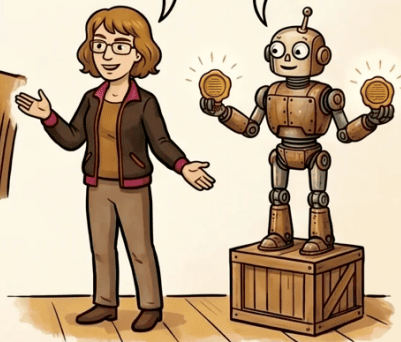
【驗證者 — 相同的行為】

有人在記錄我在這裡做的事？我不知道
— 所以我守規矩。



驗證者分不出兩者。

誰分得出差別？



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。

為甚麼社群授予我的發佈權數量應當夠小？用一條負面主張標記一個 DID（主體），會摧毀一份花了很長時間才建立起來的聲譽，而且損害持久。一份被摧毀的聲譽，會面對社群針對每一次進一步或重複犯錯所施加的、不斷升級的一整套制裁，一直到把這個破壞性實體徹底清除（極端情況）。一套呈指數升級的懲罰階梯，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，也就是社會沒有被一場（外部或內部的）災難所撼動之時。

對於概率極低的事件，統計頻率一旦應用到個人身上就會波動很大。放到社群這個群體上，卻不會如此。這正是「把自己的發佈權委託給專門的匯集型權威」的價值所在 — 這些權威很像損失發生時的相互保險，動用你的權利並代你行使它。讓我們少講點抽象，舉幾個例子：- 偵測並打擊有組織犯罪 - 執行商業協議 - 管理特權（教育證明、資產的取得／處置等等） - 如此等等

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。

■ 「發佈權」實際上如何運作

受託人的圖示為求清晰，把發佈權畫成實體代幣，但系統裏並不存在這樣的物件。實際發生的是這樣：你想與之保持良好關係的那些人 — 你的社群 — 的政策，匯集成一條湧現的規則，界定他們在開始把你當作噪音之前，每年會把你多少條主張當作切題來接受。這個上限之所以存在，是為了讓網絡不被瑣碎的「假如」主張淹沒，並讓它保持社群所想要的那麼自由（透過限制數量來保住信號）。

你讀取你的社群允許你的份額。份額有一個區間，並帶有一定幅度，取決於你最看重哪些人。然後你在那個限額之內自行決定 — 自己發佈多少條主張，以及把多少條委託給專業服務，讓他們只在事件落入其職責範圍時代你發佈。正是這一點讓你保持良好關係，同時又不必為發生在你身上的每一件小事都提交一條主張。

圖示中的「代幣」，是這種「讀取—決定」循環的一個視覺替身，而非字面上的一件實物。

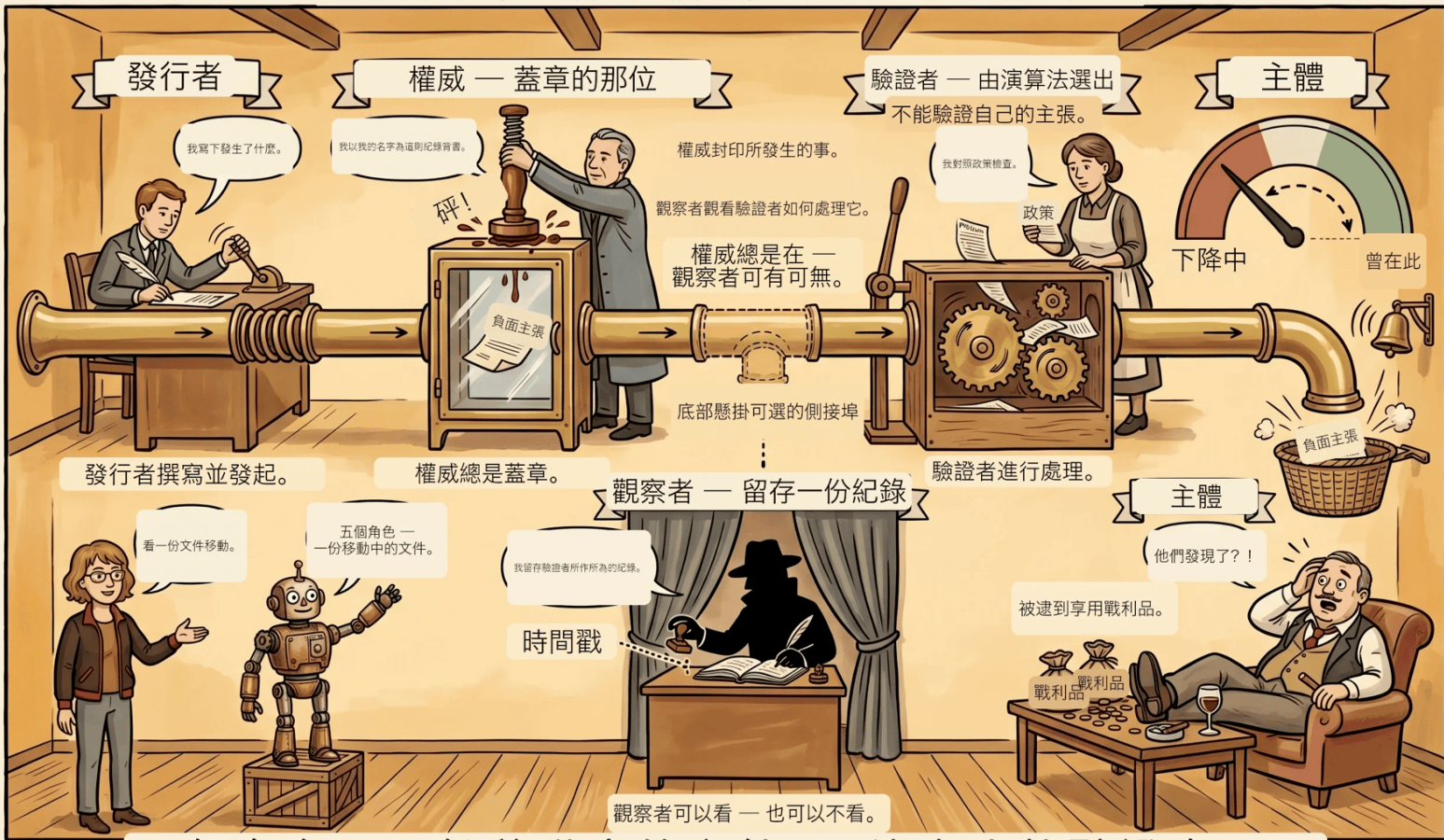
在聲譽網絡裏，能夠撤回已委託的發佈權是有價值的。這可以在任何時候進行，只要受託人尚未使用被委託的權利。

角色之間的溝通

下面的圖示概括了在一宗真實案例中，各個角色如何連接起來 — 從簽發者提交一條主張，一直到發佈進聲譽網絡。

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，以及每個角色扮演甚麼部分。現在，我們轉向：成千上萬份個別政策，如何變成某種運作起來像真正社會契約的東西。它絲毫不像左翼那些關於社會契約與強制團結的夢想。

每個參與者都根據自己的道德，宣示自己的政策（policy）——他認為甚麼可以接受，以及他如何回應他人的特定行為。網絡上為某個 DID（社群）所知的全部政策的總和，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，以雙邊價格信號為支撐，構成一份可量度的社會契約：不是一個誰也沒有在出生時簽過的理論建構，而是有實際行為支撐、可經驗地觀察到的規則。

■ 社會契約

人們爭論「社會契約」是不是自相矛盾。沒有人簽過任何東西，然而在中心化社會裏，它卻被援引來為立法與行政行動辯護。

對去中心化網絡中的互動作一番現象學分析，或許能揭示出某些湧現的規則——全球性的或本地性的。我們該如何稱呼這些被廣泛共享的規範？稱之為社會契約？正如社群一樣，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，都會得出一份不同的社會契約。

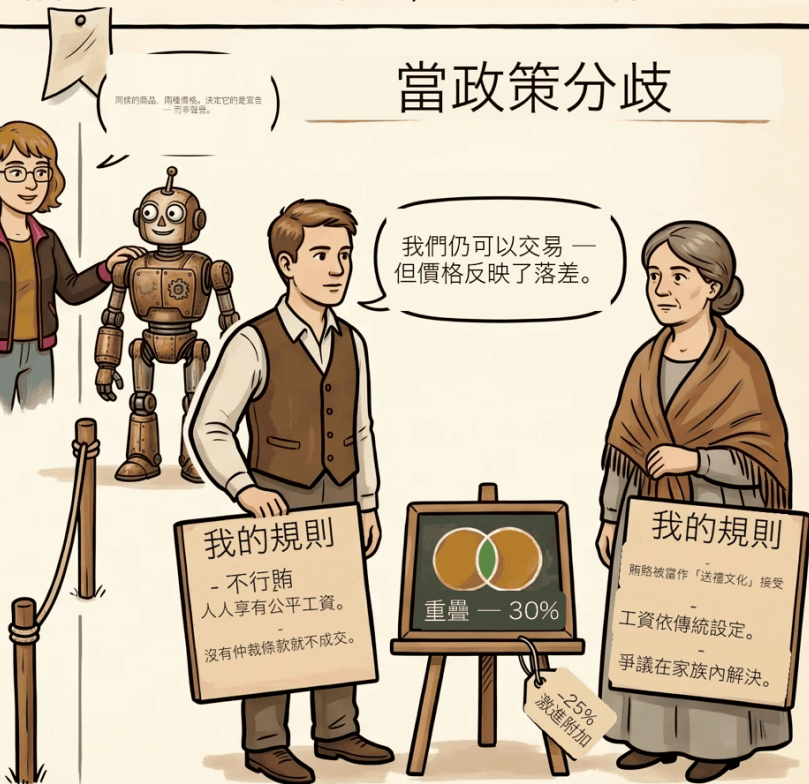
政策相遇。態度成形。

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



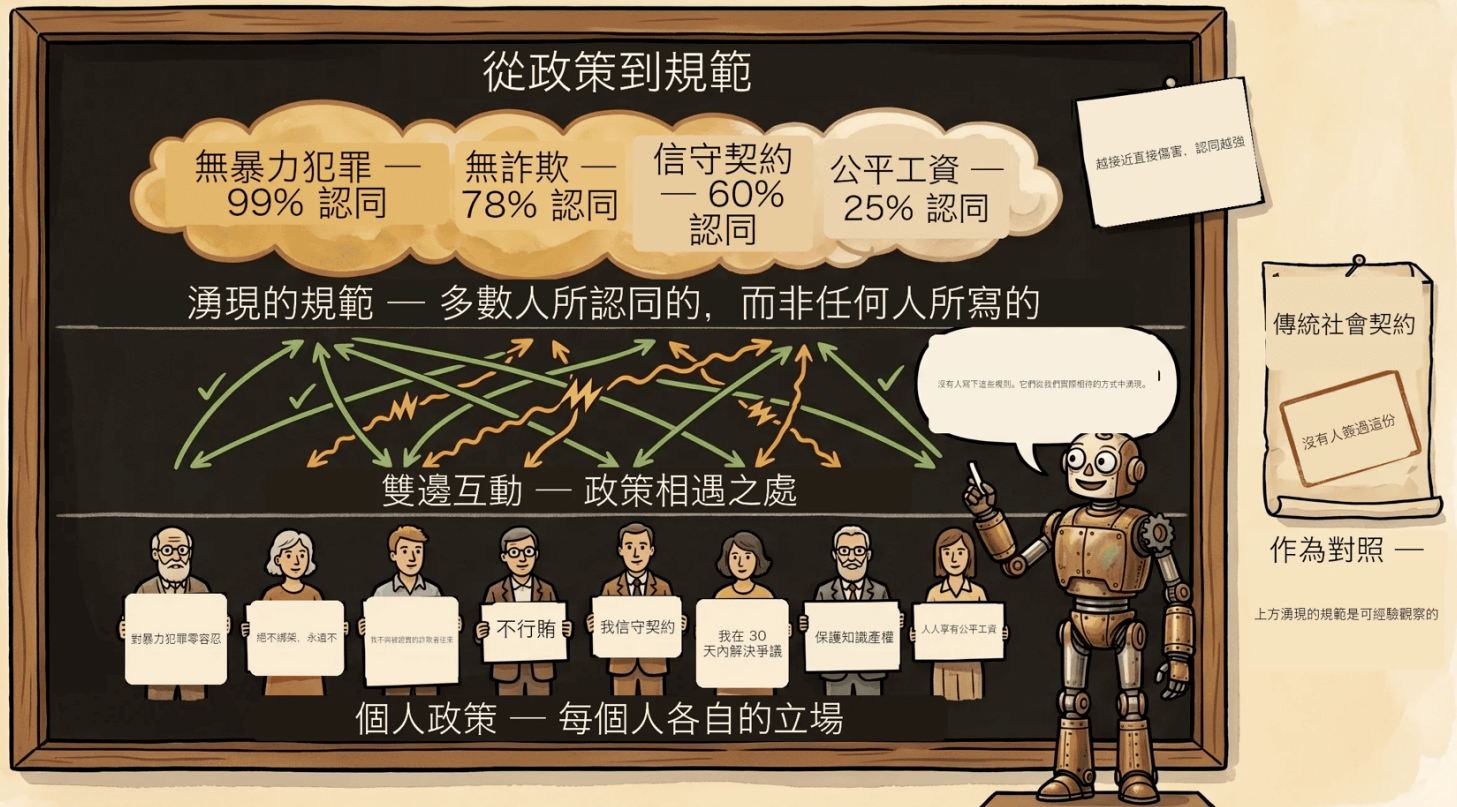
當兩項政策在交易中相遇，它們的一致程度成為價格調整因子。

* 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。

■ 以價值為本的政策

把「以價值為本的政策」當作決策的基礎，同樣具有誤導性。價值更像是一些在特定時期普遍被偏好的規則的現象學集群。它們會演變，而且並非恆常不變。

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

當兩個互不相識的 DID 主體進入一段經濟關係時，我們可以代對方向自己的社群簽署一份請求，要求它提供關於我們的資訊。然而，這是一種對「社群是甚麼」的十分天真的觀念。社群不是封閉的集合——單一個 DID 可以同時是多個社群的參與者。

從某個特定參與者的視角看，社群更像是一種現象學上的現象，體現在他的社交網絡之中；它不是那種總是值得明確劃界的東西。一條村的居民可以構成一個社群，但一個只在週末去那裏的人，也可能在同一條村裏屬於另一個社群。一個社群也可以是一支足球隊，連同它的球迷、職員以及所有相關人士的家庭。一個民族，或一個國家的公民，同樣可以構成一個或多個社群。從不同的角度看一個 DID，可以得出對社群不同的（而且往往很直覺的）看法。

因此，處在邊界上的 DID 是社群之間的橋樑，而且——正如現實生活中一樣——它們在提供關於其他社群成員的資訊方面扮演一定角色，無論是業餘層面，還是專業層面，例如一個專門連接人與人、並匯集關於高風險 DID 資訊的權威。

DID 網絡中的某些類型的資訊，很適合無條件地相互交換（暴力犯罪、詐騙等等）。然而另一些類型的資訊，一個社群可能會當作限於社群內部使用的東西（相當於公民身份、為社群提供的服務等等）。這類資訊能否傳播，取決於社群成員所宣示的政策。

一個社群在自己的圈子內守護它的私隱，作為回報，則在無條件的基礎上交換互利的資訊。

Crime and Punishment

罪與罰

我們知道網絡如何運作：紀錄如何被創建、由誰驗證、驗證者的舞弊如何被遏止。還剩下一個問題 — 當有人真的對另一個人造成傷害時，會發生甚麼？

■ 我們彼此依賴到甚麼程度？

我們全都站在這個大千世界的舞台上，這裏發生的一切都與我們所有人相關。

Jan Amos Comenius（《世界之迷宮與心靈之天堂》）

加入或拒絕一個聲譽網絡，可以有許多理由。然而我相信，人性中的一個面向 — 常被視為陰暗的那一面 — 可以派上良善的用場。我說的是人渴望在感知到的不公面前，感受到一份滿足的需要。

滿足、正義、復仇 — 我們把它們與負面情緒聯繫在一起。為了讓社會維繫在一起，我們至少必須假裝滿足是透過中心化機構來交付的；否則個人就不會覺得自己與所身處的社會相連。平均而言，我們需要歸屬於某支隊伍並信任它。當有人傷害了另一個人，社會就會注視着滿足將如何、以及以甚麼程度被交付。有點爭議地，我要主張：在歷史上 — 以及現在 — 對被告的程序是否乾淨往往並不重要；重要的是社會看見了某個人受罰。它發揮了它的功能（無數的冤案，以及對重審舊案的抗拒，已經把這個故事講得夠清楚

了)。受害者與遺屬的看法只是次要的。首先重要的，是給社會其餘部分的信號，因為不公並非常見到足以出現在每一個個人的每一天裏。

一個去中心化的聲譽系統，會讓公眾看得見直接與間接的證據（經審核的與未經審核的）。社會可以評估這些資訊——靠自己，或透過專門作此類評估的自由市場服務——並根據質與量的信號，決定對主體（甚至對作者或作驗證的權威）施加甚麼措施。

甚麼是懲罰？它是一種透過剝奪所指稱加害者的特權來使其屈辱的形式——好讓受害者與社會都感到，傷害性的作為並不划算。這正是關鍵所在：傷害性或危險性的行為絕不能划算，同時它又必須為受害者以及社會／社群的其餘部分提供一份滿足感。

這樣的懲罰非得由一個中央權威來施行不可嗎？如果每個人都能預先宣示自己將如何回應某些作為呢？我顯然無法在別人的財產上執行懲罰。但我可以宣示：一旦犯錯者進入我的地界，我會為懲罰加害者之目的，把我的財產交予一組選定的執行權威使用。而且我可以公開宣示這一點，好讓其他人評估我的取態。

而正是在這裏，比例性的價格機制登場。如果我為輕微的過犯宣示嚴厲的懲罰，網絡就會為我的極端主義定價：其他人會覺得我不合比例，我的驗證成本會上升——更少人願意與我交易，或者只肯以更差的價格交易，也更少驗證者願意以合理的價格接受我的紀錄。反過來，如果我太過寬鬆，社群就會把我視為一個風險。如果我容忍詐騙，社群大概就會對那些冒犯到我的作為的加害者從寬——好讓我嚐嚐自己那一套的滋味。

正義不再是一件奢侈品。當有人傷害了你，記錄下這樁冤屈是負擔得起的，紀錄是永久的，而對加害者的後果是實實在在的。

■ 虛偽偵測

光是宣示一項政策並不夠 — 如果我宣示我遵循某條規則，但我的行為偏離了它，這道落差就是一項聲譽上的負債。網絡並不區分「違反了法律」與「違背了自己的諾言」 — 兩者都是可量度的信號。虛偽是昂貴的，而我不知道還有甚麼比它更惹人光火的紅布。

■ 量 vs 質 — 打破罪責的二元範式

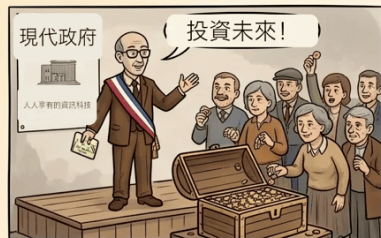
在中心化的司法裏，罪責是二元的：0 或 1，有罪或無罪。在一個聲譽網絡裏，重要的不是罪責是否被證明，而是信號的累積。

針對被告的一宗孤立、未經證實的盜竊指控，大概不會引起太多警覺 — 但它會引起對指控者的警覺。然而，來自各個獨立來源的多項間接跡象，卻開始有了份量。重要的不只是數量，還有質量：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，若同一個簽發者針對各個不同的目標主體反覆提出頻繁而毫無根據的指控，這些指控可能會被評定為誹謗 — 而指控者的聲譽要為此付出代價。

一個陷阱。一條出路。

內線人總是拿下合約 — 直到網絡讓人們直接購買，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。



在緊閉的門後，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。

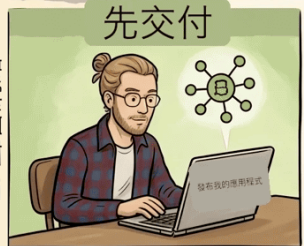


內線人拜訪師儒。那份「善意的建議」只是最小的一點碎屑。

1. 傳統做法

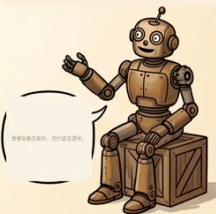


2. 聲譽網絡



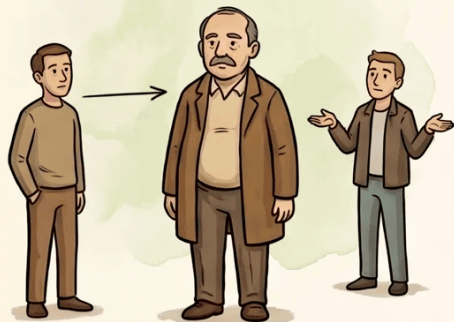
兩條路。陷阱在規則裡。出路是徹底繞過規則。

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。聲譽網絡是出路：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。



證據如何累積

「一則孤立的主張」



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。

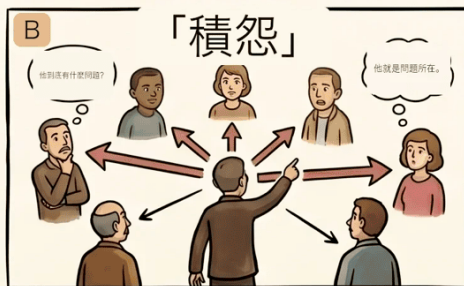
「壓倒性的份量」



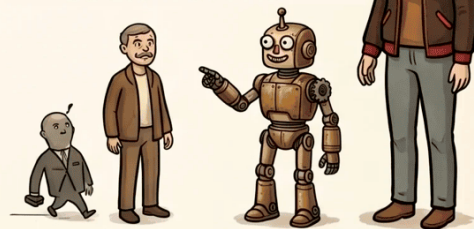
二十個獨立來源 —
壓倒性的份量。



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。

我們也不應忽視贖罪 — 一種在罪責被證明之前所作的自願行為，提供一條通往較輕懲罰的道路。當加害者不採取任何邁向贖罪的步驟、指望着逃脫後果時，懲罰就會啟動 — 這種結果，很像在中心化系統裏可以透過腐敗買下來。

■ 過犯的類型

資訊的類型不必限於犯罪行為；它們可以包括：- 對罪行的描述 - 違約與詐騙 - 不道德的行為 - 對公共秩序的擾亂，無論是真實的還是虛擬的 -

DID 網絡中每一條新紀錄，都會調整對某個 DID（無論是主體、作者，還是作驗證的權威）所評估的聲譽與風險。我為他人的命運承擔的責任越多，我就變得越審慎。

■ 透過委託執行懲罰

我不必親自執行懲罰。我可以（類似買保險那樣）付費給一個權威，讓它按預先界定的規則執行結果 — 相當於偵查、執法與司法服務。如果這個權威執行得不合比例，或根本不執行，它的聲譽就會受損 — 而它的聲譽正是它賴以謀生的能力之基礎。

委託是網絡中的一條通用原則：一個 DID 的任何活動都可以委託給另一個 DID — 驗證、簽發主張、回應爭議、宣示共識。委託在任何時候都可撤回。它讓專業化成為可能，而不喪失最終的控制權。

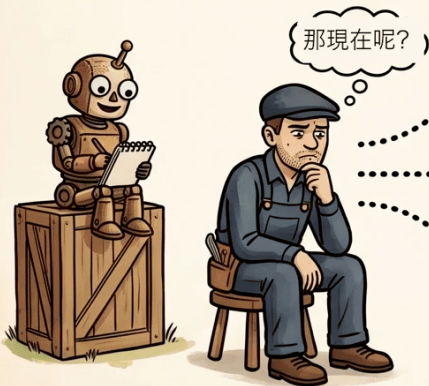
傷害之後 — 你會怎麼做？

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」



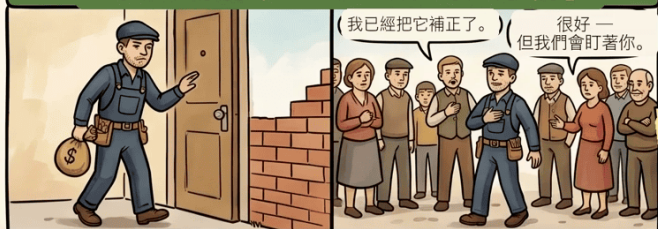
沒有補救 — 每家店都拒絕他 — 被逐出經濟生活

「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

這幅插圖並非真實故事，所有文字
只為向本報讀者介紹有關「被拒、被迫、自願」三種情況。

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。

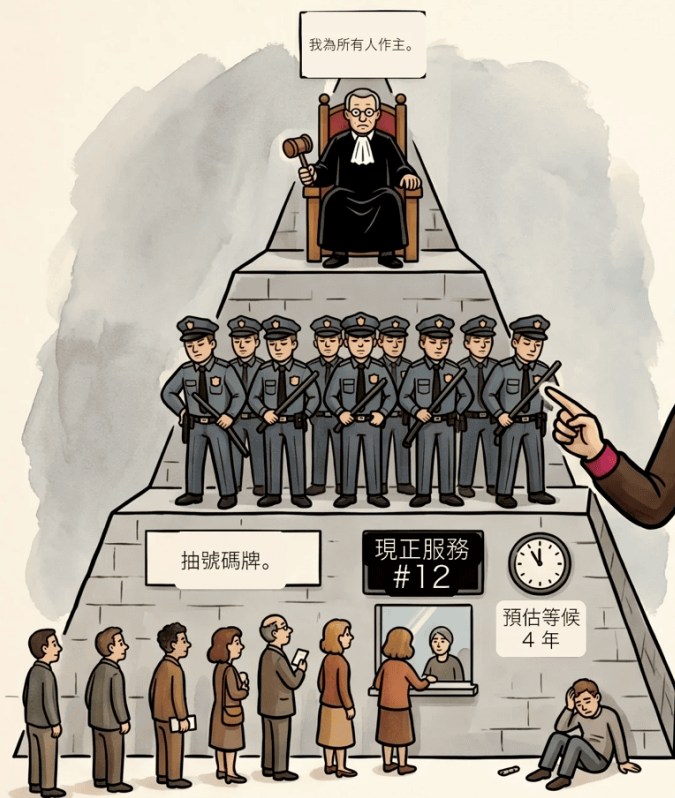
■ 風險管理的民主化

一個不可審查的聲譽網絡，會把銀行或大型工業設施的維護者早已作為核心活動在做的事——風險管理——加以民主化。

對一位面對客戶的銀行家而言，風險評估是預先準備好的，好讓他能在預先界定的限度內專注於商業互動。精密的維護團隊，在定期的保養週期裏，蒐集風險指標（結構裂縫的跡象、令運營基礎設施退化的過程等等），並能預測設備的壽命，以及何時需要甚麼樣的介入。

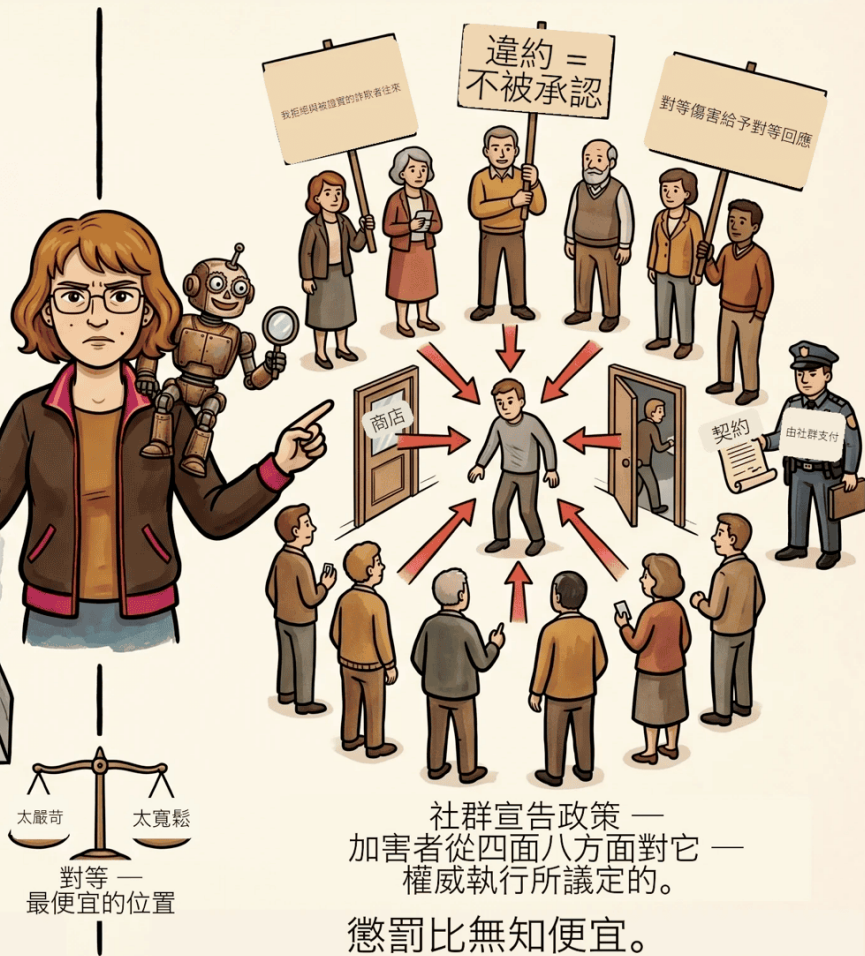
我對 DID 的使用有類似的設想——某個人（大概是收費的）會提供一份人類可讀的對手方概要。這份概要會反映客戶所訂購的那個風險評估角度。

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

追蹤金錢的軌跡

我們有了一個去中心化聲譽網絡，也有了使用它的動機。它已經可以為用戶帶來競爭優勢 — 理清潛在的風險，幫助他們更有效率地規劃對手方的選擇與談判策略，並納入那些降低這些已知風險的措施。

接下來的，是使用它的一種可能方法論⁵ — 利用網絡的特性，來構建一條從現行制度通往其演化繼任者的遷移路徑。它很可能帶有中歐的特徵，這篇論說正是在中歐孕育的。本地的條件會需要本地的調整。我在任何地方都會建議保留的，是對國家所採取措施的不妥協性格 — 沒有這一點，目標就會在無休止的討論中被稀釋，而變革永遠不會到來。當心 — 國家的代表與擁護者會拿一堆廢話把你纏住。別上當；他們的飯碗正押在這上面。

國家的弱點 — 金錢

讓我們回到起點。我們想要更多由此而來的自由、對其形態更多的影響力，以及與之相稱的更多責任。問題很簡單：國家在哪裏有一個我們可以不訴諸暴力就施壓的脆弱點？

答案很沉悶，卻正因如此而更加有力。金錢。

國家的核心，是一股金錢的流動。它靠金錢供養它的強制機器 — 也就是執行其規則的最後一環。沒有金錢，就沒有暴力壟斷。一旦金錢開始卡頓，國家就開始退卻 — 因為它再也沒有甚麼東西可以付給那些以物理方式把它撐在原地的人。

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家 Daniel Steigerwald 一本同名的即將出版著作（預定 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。

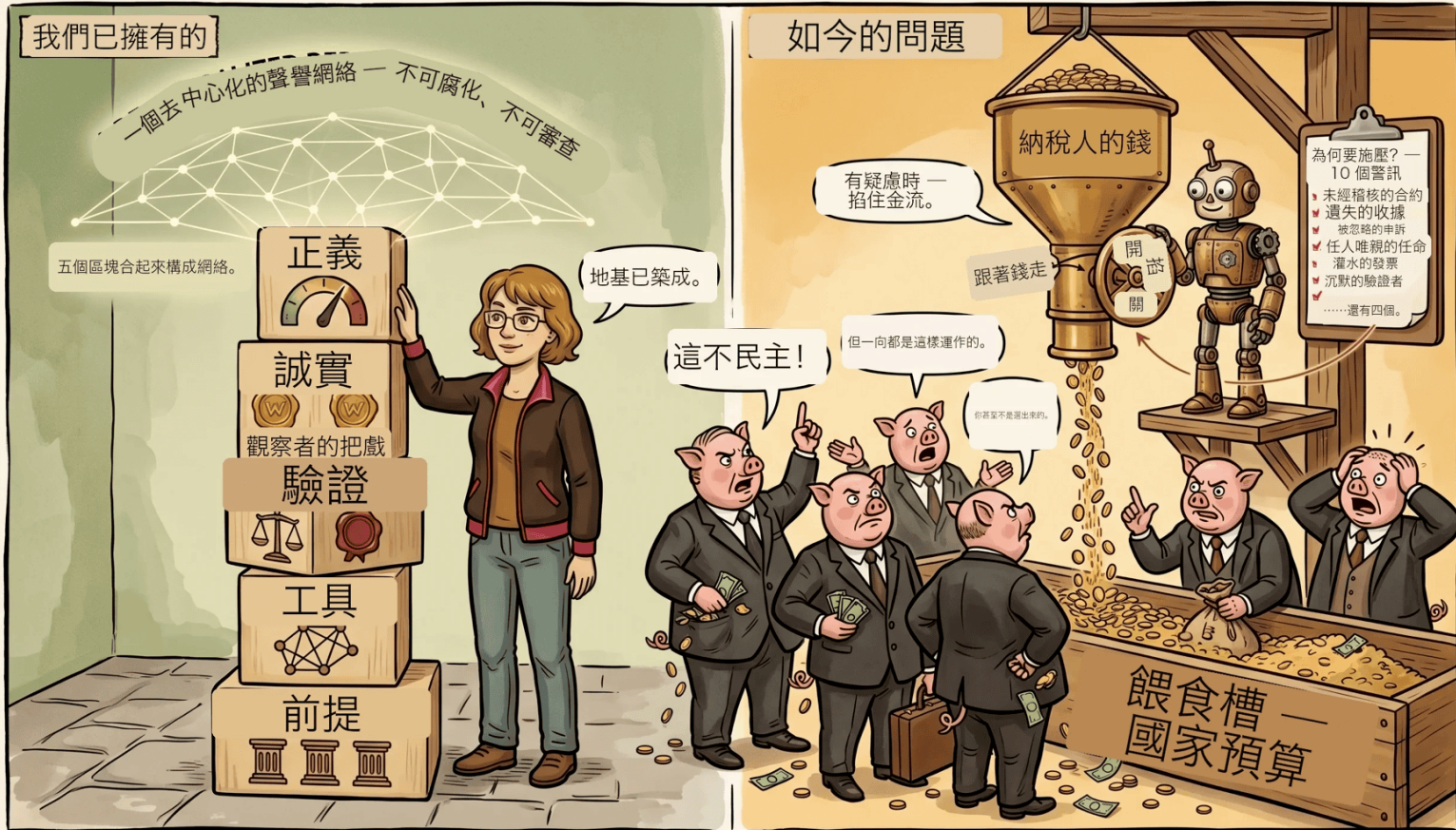
金錢的流動天然會起伏 — 隨季節、隨經濟、隨投資者情緒。國家透過在金融市場上借貸來掩蓋這一點。偶爾一筆貸款是理性的：一項能回本的投資。然而更常見的是，它填補的是那些早已超出國家核心目的（國防、內部安全、刑事司法、外交事務）的議程上的過度支出。一旦越過某些門檻，中央銀行就以錨定於自己對通脹估計的利率作出反應。

而在這裏，那道無聲的稅登場了。通脹遠不只是宏觀經濟學家的一項會計上的關注。它是對貨幣購買力的一道隱藏稅，由每一個為晚年攢下幾個銅板的人繳付。低通脹之所以被公眾容忍，是因為他們沒有把握它的長遠影響 — 他們沒有意識到，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保障自己晚年的地步。而當他們無法做到時，他們就被馴化成對國家福利的依賴。到最後，他們掛在那些福利上，被拴在國家身上。

在動盪的時期 — 戰爭、疫症、那筆「必要」的投資 — 國家乾脆按下印鈔機的開關。負責任的儲蓄者與工作者的購買力下降，而我們卻向他們保證，他們得到了優厚的回報。有人在悄悄偷走他們的時間，還讚美他們賺得多麼漂亮。

這嚴重地侵蝕了對國家的信任。而信任是唯一一把整部機器黏合在一起的膠水。那正是值得使勁去撐的那根槓桿。

跟著錢走 — 至此的故事



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

■ 為甚麼是金錢，而不是其他弱點？

文明的另一個弱點，例如能源分配。但擾亂它的流動並不是一根槓桿 — 那會是侵略、恐怖主義。自願的不參與，跟蓄意傷害他人不是一回事。金錢的特殊之處在於：壓力可以自願地、透明地、不用暴力地施加。

Proposed transition to the state's successor

演化，而非革命

即使最終目標很吸引人，突如其來的變化也會激起抵抗。它撕裂各種紐帶 — 社會的、經濟的、政治的 — 而人們會本能地捍衛自己已經熟悉的東西，來對抗自己尚未見到的東西。

因此，正確的取態是漸進的 — 演化式的。一種能防止舊制度只需輕輕一按按鈕就把新制度關掉的取態 — 因為它一旦能夠這樣做，它就會這樣做。

不幸的是，這意味着要接受：均衡的自願性不會在我們部署聲譽網絡的那一刻就達到；它會伴隨着一個逐步的採用速率一同到來。接納可能會 — 而且大概會 — 很緩慢，是由個人的一種渴望拉動着前進的：當按規矩尋求正義的方式失敗時（而它會失敗），透過聲譽網絡向自己的社群尋求救濟。讓我們看看那條路是甚麼樣子，包括按比例作出的估計。

■ 空槽 — 別按那套注定讓你輸的規則來玩

從內部改革國家的嘗試，依賴的是權力的內部機制，寄望官員會逆着自己的激勵去推動變革。那是不會發生的。

何必去餵養這個系統，而不去把那些為它輸送生命的渠道抽乾？與其去改變舊制度、按它的規則來玩，不如讓我們在它之上建起一個新的層 — 一個逐步把舊制度變成新制度子集的層。一開始，那個子集幾乎填滿了超集。隨着時間推移，行為者們紛紛遷移過去。

公司都懂這一點：當一個舊系統糾纏得無法替換時，你就建一個並行的系統，然後逐步把用戶遷移進去。

至於國家最終會在「它實際交付的」與「它的章程所要求的」之間出現落差，並會傾向於援引這道落差 — 那純粹是它的代表與參與者的問題，沒有必要回頭去看它。唯一值得注意的是這一點：不要挑起一場暴力革命。

四件彼此支撐的工具

到目前為止，DID 聲譽網絡可能看起來主要在司法與共識方面有用。我相信它能夠穩定自身、頂住攻擊 — 以賢能制的方式，建基於實際的功績，而非形式上的頭銜。但單靠聲譽，並不會逼國家讓步。逼它讓步的，是經濟，以及透過經濟施加的壓力。

沒有甚麼能阻止我們把 DID 身份用作額外工具的管理者，來狠狠地壓在金錢上。不要從公民的完全自願開始 — 先設定一個國家無法阻止的方向。這場過渡建基於四件互相撐着對方後背的具體工具。沒有任何一件單憑自己就足夠。

簡單的稅制 — 入門的誘餌

第一件工具，是一套建立在 DID 基礎設施之上的、簡單而透明的稅制。對所有收入採用單一的比例稅率。沒有例外，沒有免稅期，沒有企業扣減，沒有優惠。每一筆繳款都可審計地連結到繳付它的那個 DID。交叉核對輕而易舉。

稅率的設定，對一部分納稅人而言，會比舊制度略為有利 — 那就是入門的誘餌。稅負會逐年下降，制度會變得越來越吸引人，遷移也會加快步伐。這套制度既是紀錄的保管者，又是徵收者 — 沒有中間人，沒有不透明。

電子支出登記 (ESR)

第二件工具，是把 EET（電子收入紀錄）翻轉過來。與其由國家追蹤一名自由職業者的每一張收據，不如讓我們追蹤國家的每一筆支出。除非國家的每一筆支出 — 無一例外 — 都通過這道篩子，否則國家不會就任何一筆個別繳款，從簡單稅制那裏收到任何款項。

ESR 是一個代理⁶，把國家與公共部門每一筆已實現的支出，與一條有關計劃付款的紀錄相配對 — 包括脈絡上的理由，以及對收款方、支出實體與用途的識別。其成果是原始的公共數據，可分層化。任何人都可以拿去分析。任何人都可以就如何處理它，向納稅人提供建議。審計部門多年來都達不到的目標，如今對每個人而言只在一鍵之遙。

你不必轉用新稅制就能參與。只需為每一筆已實現的付款繳付一筆完全可退還的按金（比方說 1-3 歐元）就夠了。未實現的餘額會被沒收，充當一個垃圾過濾器，好讓系統不被攻擊淹沒。一條紀錄可以由任何人提交 — 一名親屬替一位失能的祖父母，一位鄰居替被忽視的公共服務，一名企業家替一張未付的發票，一名官員透過從自己系統匯出的方式。

⁶代理 (Proxy, 拉丁文 *procurator*, 英文 *deputy/intermediary*) — 此處指一個代另一個實體行事的中介。ESR 代理接受任何人提交的計劃付款紀錄，把它們與國家已實現的支出相配對，並把由此得出的數據集向公眾開放。

我預期，政黨會自然而然地轉型為分析提供者，或者會有新的政黨湧現出來取代舊的。它們不再靠從稅款抽取的撥款，而是開始提供專業知識——向自己的支持者提供以價值為本的概覽，涵蓋結盟的權威、它們的服務以及驗證政策。那些出於懶惰而潦草或無稽的紀錄，會自動成為削減預算的候選對象。在第一輪，你的付款總會被支付出去，但所收集的數據會作為評估「某項國家支出是否仍然說得通」的依據。承包商以及其他吃國家糧的人，都有動機去確保官員負責任地把支出配對好。否則，下一輪的錢就不會流過來。

■ ESR 這個縮寫從何而來

在 2016 至 2022 年間，捷克政府對它自己的公民——自由職業者與企業家——實施了一套名為「電子收入紀錄」(EET) 的制度。訊息很簡單：「我們假定你們每一個人都在欺騙國家。你們要記錄每一筆交易，實時傳送到我們的服務器，我們會盯着你們。如果你們試圖逃避 EET，我們會在財務上獎勵你們的同胞來舉報你們。」

EET 是仿照巴爾幹的先例設計的。世界上第一個推出全國性強制實時網上銷售記錄系統的國家，是 2013 年的克羅地亞，名為 *fiskalizacija*。捷克在幾年之後採納了這個模式，並運行了歐洲最嚴格的收入追蹤體制之一。

如果陰暗的一方毫不猶豫，我們又何必猶豫？ESR 就是同一套邏輯翻轉過來：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」有直接的影響力。在第一輪，無論 ESR 揭示了甚麼，國家都照樣收到它的錢。到第二輪它就不再如此了——第一輪得出的分析，以及由此而生的措施，接手掌控。已

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

國家支出的公開賬簿 — 開放紀錄

對任何想看的人開放。

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：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：道路設計顧問
承包商：顧問公司 T 金額：300 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：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



政黨轉型為分析提供者



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

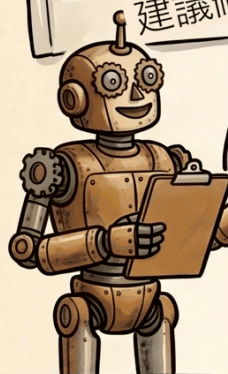
這套系統將為政府、企業、公民提供透明、可查、可追溯的支出紀錄。

繳稅款中的一小部分百分比，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（公民身份、居留身份、社群所承認的成年／行為能力）。可分配的百分比逐年增長。潛在地呈指數增長。從今天的百分之五，到十年內的數十個百分點。

原始的 ESR 數據，自然地引導着納稅人的決定。質量低劣的紀錄，充當一個建議削減的警示信號。任何人都可以創建紀錄；官員則不得不去配對。沒有這一點，稅制就不會給國家送去任何錢——既不進國庫，也不進其他預算章節。政治鬥爭從投票箱，轉移到日復一日對一枚枚具體銅板的分配上。

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。



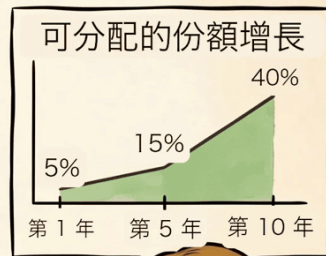
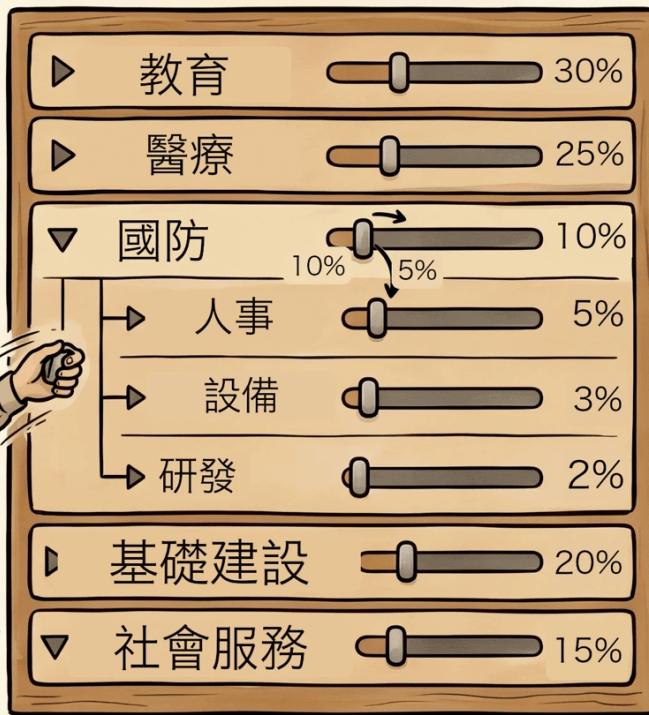
或委派這件事

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。



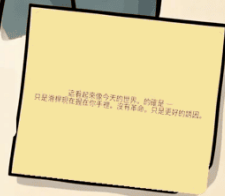
讀完報告後
國防調降。



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。



與國家談判的平台 — 那根槓桿

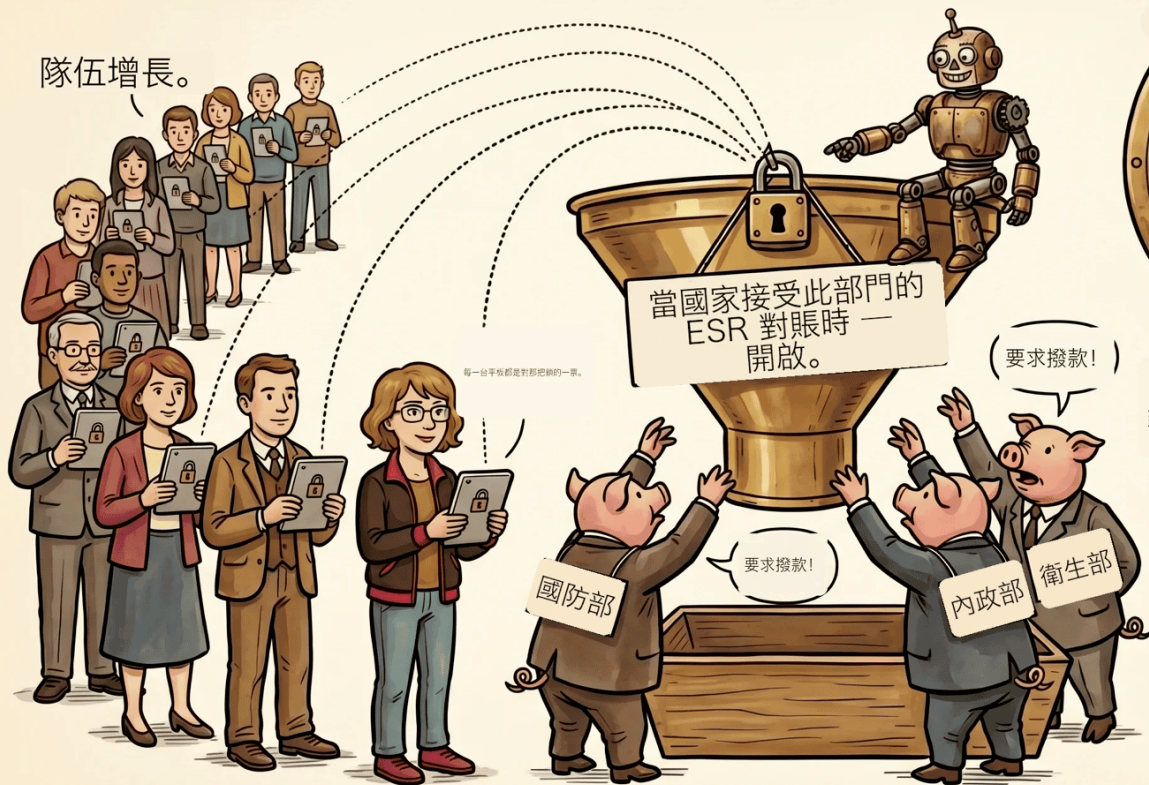
第四件工具，是把一切綁在一起的那根槓桿，只有到了這一步，網絡才成為一個真正的威脅。主要的衝突，將圍繞國家是否接受 ESR 作為一個具約束力的標準 — 首先在全國層面 — 以及要在此之前，來自聲譽網絡參與者的威脅必須變得多大。

那根槓桿，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。只有在國家滿足了透明度條件的那一刻，錢才會流動。一份參與者的輪候名單，在聲譽網絡內部形成。當這個群體達到經濟上舉足輕重的規模 — 大到足以威脅 GDP 增長 — 啟動就會開始。到那一刻，公民不服從就成為一個可信的威脅，而不再是一個姿態。

國家會死死抱住那些與腐敗掛鈎的問題付款到最後。在壓力之下，它會先在自己有容易辯護、又沒有騰挪空間去找節約的地方讓步。逐步而不斷加大的壓力，會逼它一步一步地從每一個陣地退卻。

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賬冊。

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。

這套系統是為了幫助公民監督政府開支，並確保每一分錢都用在正確的地方。它不是為了取代政府，而是為了讓政府更透明、更負責任。

沒有身份證的公民身份

隨着過渡到 DID 基礎設施，國家簽發的身份證失去了它壟斷性的用途。你不需要身份證 — 你有一系列 DID 身份，其中一些帶有一條主張，例如你是捷克人、某個市鎮的居民、某所學校的畢業生。這條主張是可驗證的、永久的，並且獨立於國家行政。

一個技術實現的問題浮現出來：市場上誰會承接起「在國家控制之外驗證現有公民」的工作，以便把有意者遷移進一個帶有相應主張的 DID？最有可能的是，會湧現出一些專門作身份驗證的自由市場權威 — 公證人、本地社群、僱主。他們以自己的聲譽作賭注，擔保某個 DID 確實屬於聲稱擁有它的那個人。公民身份 — 也就是對某一種社群看法的歸屬 — 被從中央記錄的需要中解放出來。透過聲譽網絡的連結，所嵌入的數據會被連接並二度、三度、四度地驗證，如此下去。

其後果是直覺的，卻在中心化系統裏無解。今天，政治領導層 — 着眼於更容易連任 — 可以把集中的問題輸入社群的地界：不顧吸納能力以及現有社群的意願接收來自其他文明圈的移民，透過一種壓力去改變原有的社群，而社群在這種壓力下根本來不及同化來自其他文明圈的到來者。在一個 DID 網絡裏，一個透過腐敗被接納的移民，無法確定社群會繼續把他當作自己人。社群的成員在客觀上不必忍受一個陌生人穿着社群的制服來到他們家門口，還拿他打算在屋裏執行的措施的合法性來威脅他們（因為一則社交媒體帖子而沒收孩子的手機）。有了去中心化的聲譽，社會的大多數不必對此逆來順受 — 因為對一個社群的歸屬，不是由一名官員來決定的，而是由社群本身，透過它的聲譽信號來決定的。

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。

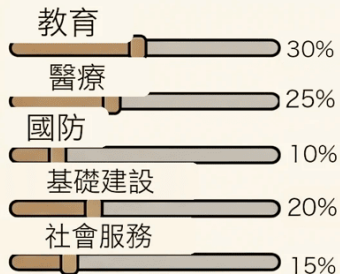
ESR — 電子支出報告



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



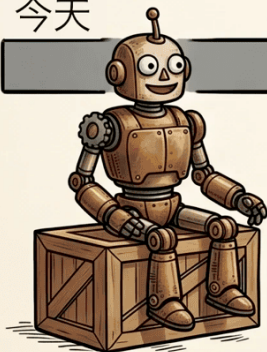
研讀紀錄 —
然後移動滑桿。

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

95%

十年後

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



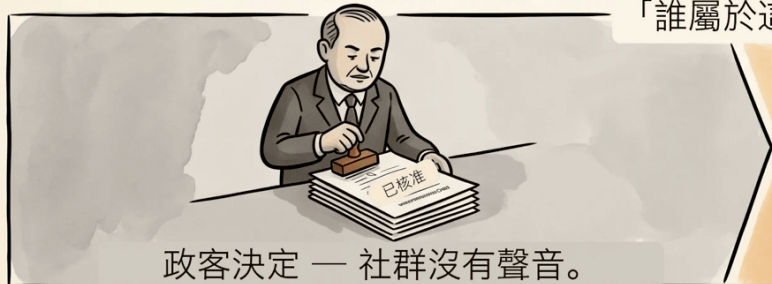
身分 = 國家許可 — 可撤銷 — 社群無置喙餘地。

「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。

在國家職權範圍內的事務上，一張選票的份量，將來可以與「對簡單稅制的貢獻紀錄」嚴格掛鉤。再結合合適的 DID 主張（例如「此人是捷克公民」），外國國民便可以被排除在選舉之外 — 人口登記冊只不過搬到了這裏而已。

重疊與可逆性

我並不聲稱這是唯一的路，甚至不聲稱它是最好的路。但它看來相當周全 — 它涵蓋了主要的槓桿，並保留了退回一步的選項。在起點，新制度與舊制度重疊，只改變激勵。隨着時間推移，舊制度不斷收縮，直到它可能 — 但也不一定 — 消解。好處在於漸進性與可逆性：萬一設計裏出現了一個錯誤，那不是終點，只是一次修正。

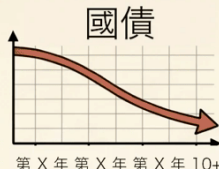
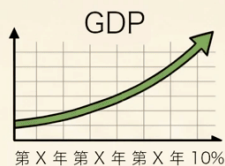
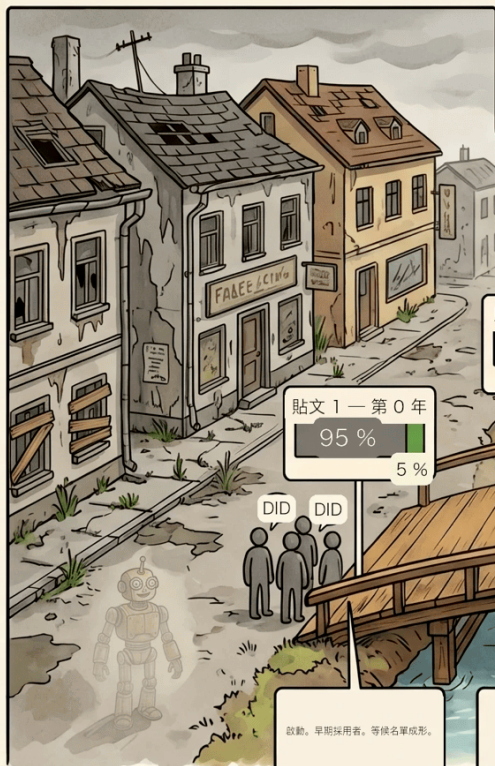
■ 和平與戰爭

國家的某些部分，也許並沒有一個完全以市場為本的替代方案 — 或許是軍隊。在危機中臨時委託非常之權（正如古希臘人任命獨裁官那樣）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。與中心化的治理不同，一旦威脅過去，收回被委託的權力會更容易 — 或者在必要時更早收回。即使在與威權政體的兵戎相見中，一個自由的社會也不會處於劣勢。

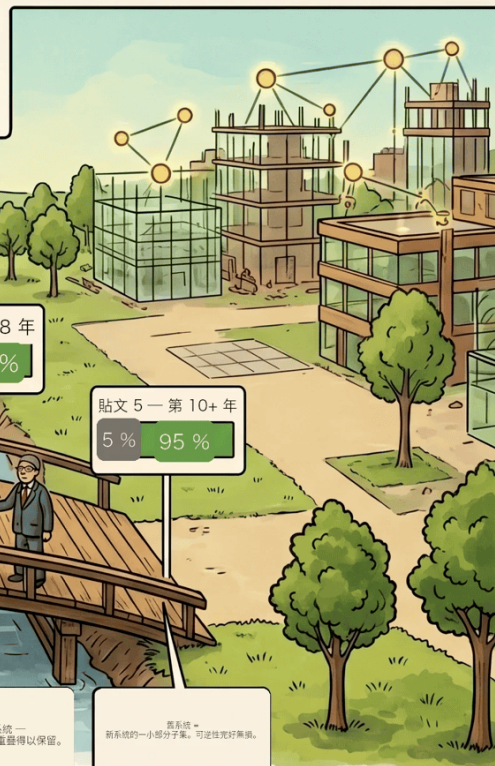
■ 戰爭罪犯

有了即時的國家撥款以及透明的支出，要為侵略戰爭積累資源就變得困難。一個繼續資助這樣一場戰爭的納稅人，成為一個正當的目標，並且不能援引《日內瓦公約》下的平民身份。在新的安排下，沉默的默許被當作參與。

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。

成長中。參與者名單膨脹。

啟動。早期採用者。等候名單成形。

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

國家之所以是今天這個樣子，是因為它創立之時可得的技術，加上人性。把一切建立在自願性之上，同時又否認一般的人性，是天真的。它擺脫不了腐敗，也擺脫不了那種朝向極權主義漂移的傾向。國家的繼任者，必須連我們目前視為負面、並加以排斥或懲罰的那些特質也能一起應付。

這本書描述了一個問題——一個系統（國家），在其中撰寫規則的人，從不與規則的後果一同生活。它描述了要讓那個系統停止運作，必須成立的種種條件。它描述了一件滿足那些條件的工具。而它提議了一套過渡方法論——一些關於如何使用那件工具的具體步驟，作為一個可能的例子。

在第一章裏，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** — 沒有人逼你進入網絡，但你也無法把自己的作為從中抹去。
- **組織** — 社群從「你認識誰」中生長，而非從「你被自上而下指派給誰」中生長。
- **韌性** — 即使是一個願意花錢監控每一個數據包的國家，也關不掉它。
- **共識** — 它源自貼在虛偽之上的價格標籤，而非源自票數或簽名。
- **不可腐化性** — 五條小規則把腐敗織進成本裏：自願性與責任的平衡、任何人發聲的權利、誰也選不了的入口點、帶着「虛偽要付價」的公開承諾，以及每一筆交易背後那道觀察者的陰影。

沒有任何單一支柱能夠獨力取代國家。合在一起，它們構成一種對腐敗的抵抗力，而那是國家連同它全部的機器也無法構成的。

我們正處在這樣一個時點：整件事可以用當今的技術建成（密碼學、去中心化身份、為把激勵調校到位而熟知的心理學模式……）。只缺一樣東西：一群找到勇氣去支持它、並決定開始動手的人，達到臨界質量。

不是透過革命。

這些構想成形於 2025 年 6 月至 2026 年 5 月之間。到我坐下來動筆的時候，這個框架在我腦海裏大體上已經想通了——這也正是為何當 [Farewell To Westphalia](#) 面世時，我懷着如此的好奇去讀它。我想看看他們的圖景在哪裏與我的重疊，在哪裏又與我的分道揚鑣。第二股推力來自 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》；他的項目推動我把自己的願景以完整的廣度寫下來——好讓這個世界能把它與其他人的一併擺上桌面。

我並不是要你相信其中任何一點。我是要你去思考它。而我留給你一個問題：

你會改變甚麼？

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，感謝那個思想框架，它幫助我把自己的構想放進「解構威斯特伐利亞式國家模型」這個更廣闊的脈絡之中。

審閱與反饋

工具

在準備文本、梳理構想以及反覆打磨措辭的過程中，我借助了人工智能工具的協助。所有的構想、論證與結論都是我自己的 — 人工智能充當的是打磨的工具，而非內容的共同作者。

資訊圖表是與生成式工具合作、依據作者的規格設計的。

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

bc1q7cctdz6r026dgy06u194eygg49ujtxnrq5czaj



Bitcoin Lightning

LNURL1DP68GURN8GHJ7AMPD3KX2AR0VEEKZ
AR0WD5XJTNRDAKJ7TNHV4KXCTTTDEHHWM30
D3H82UNVWQHXXMNP0FA8JMTVPD5XJMN9XUE
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

詞彙	繁體中文	意思
Authority	權威	一個受信任的實體（個人、組織），驗證資訊並以自己的聲譽為之背書。可以是專門化的（調查、法律、技術）。
Claim	主張	一般而言：任何可驗證的陳述。此處：發佈到聲譽網絡的一條紀錄 — 一項關於某事件、屬性或關係的斷言，經密碼學簽署並驗證。例如「我是市鎮 X 的居民」或「此人違反了一份合約」。
Compartmentalization	區隔化	一般而言：把資訊分隔成互相隔離的單元，使暴露一個單元不會危及其他單元。一條為情報機構所熟知的原則。此處：獨裁政權下的並行 DID 身份 — 攻破其一，不會暴露其餘。

詞彙	繁體中文	意思
Consistent Hash Ring	一致性雜湊環	一種選取驗證者的演算法機制 — 環上的位置由社交圖譜內 DID 文件的雜湊決定。確保一種既非確定性、又可驗證的選取。
DID	DID（去中心化身份）	一種你自己創建並掌控的數碼身份，沒有中央權威。以你的私鑰作密碼學簽署 — 沒有人能撤銷它或偽造它。
DID Document	DID 文件	一份公開可得、描述你 DID 身份的數據檔案 — 包含公鑰、網絡地址與元數據。用於在網絡中驗證你的身份。
Due Diligence	盡職調查	一般而言：在進入商業或法律關係之前，對對手方進行深入的核查 — 查核其歷史、財務、聲譽與風險。此處：在聲譽網絡裏，因已驗證紀錄的可得性，它進行得更快、更自動化。
Economic Neutrality Principle	經濟中性原則	網絡中的誠實行為，在經濟上接近於零 — 發佈成本會作為驗證報酬回流。不誠實的行為則是淨損失。

詞彙	繁體中文	意思
Emergent	湧現的	從較簡單部分的互動中自發產生，而無人設計或指揮。一群鳥沒有計劃也能列隊飛行 — 隊形從每一隻個體所遵循的簡單規則中湧現。
Emergent Social Contract	湧現的社會契約	一些行為規則，不是自上而下（法律）產生，而是自下而上 — 從社群內部反覆的互動與共識中產生。
ESR	電子支出登記	一套用以透明追蹤公共支出的擬議制度 — 國家每一筆已實現的支出，都與一條計劃付款相配對。靈感來自捷克的 EET，卻反過來對準國家。
Hash	雜湊（指紋）	一般而言：一種單向數學函數，能從任何輸入產出一個獨一無二、定長的「指紋」 — 就像文件的指紋。同一輸入總產出同一輸出，但無法從輸出反推輸入。此處：用來決定雜湊環上的位置，並驗證文件的完整性。
Just-in-Time Funding	即時撥款	以透明度為條件的國家撥款 — 只有當國家接受 ESR 並配對其支出時，錢才會流動。一根迫使合作的槓桿。

詞彙	繁體中文	意思
Meritocracy	賢能制	一般而言：一種以實際功績與經證明的能力、而非以形式頭銜、關係或世襲特權來決定地位的制度。此處：聲譽網絡自然地偏袒那些對社群有可證明貢獻的人 — 他們的聲音因往績而非因職位而更有份量。
Onion Gateway	洋蔥閘道	一個 DID 身份在洋蔥網絡上的網絡地址。與 DID 文件分開 — 它可以在不喪失身份的情況下更改（類似更改一個域名背後的 IP 地址）。
Onion Routing	洋蔥路由 (Tor)	一種確保網絡不可審查性的通訊協議。訊息被分層加密 — 每個節點剝去一層，但不知道完整的路徑。
Oracle Problem	預言機問題	一般而言：如何確保進入數碼系統的數據，忠實地對應到物理世界中實際發生的事。此詞源自區塊鏈領域。此處：透過權威來應對，他們以自己的聲譽作賭注，擔保一條數碼紀錄對應於物理現實。

詞彙	繁體中文	意思
Phenomenological	現象學的	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研究的取徑，透過觀察由它們引出的結果，而不預設既有的理論。此處：自由、社會契約與行為規範都是被觀察到的現象 — 是人與人之間成千上萬次微互動的結果，而非自上而下定義的原則。
Policy	政策	一般而言：一套管轄特定脈絡中行為的規則或原則。此處：DID 網絡中每一個參與者都宣示自己的政策 — 他如何回應他人的特定行為、他遵循哪些規則、他認為哪些懲罰合乎比例。政策的總和構成湧現的社會契約。
Proxy	代理	一般而言：一個替身或中介 — 一個代另一方行事的系統或實體。此處用於兩種脈絡：(1) ESR 作為配對公共支出與計劃付款的代理；(2) 觀察者作為觀察者把戲中發佈者與驗證者之間的代理。
Publisher	發佈者	一個創建並發佈紀錄（關於一樁不公、一次彌補等等的主張）的網絡參與者。承擔發佈的成本。

詞彙	繁體中文	意思
Reputation-Based Social Network (RSN)	聲譽網絡	一個去中心化的社交網絡，參與者在其中交換關於現實世界行為的反饋。紀錄創建起來昂貴，讀取起來便宜。
Reputation Signal	聲譽信號	網絡中的一條個別紀錄 — 正面的（傷害的彌補、義務的履行）或負面的（不公、違約）。信號累積起來，構成一份聲譽檔案。
Social Graph	社交圖譜	你的聯絡人以及你聯絡人的聯絡人所構成的網絡。演算法在一個可配置的深度（例如 3 層）內搜尋驗證者。沒有全球性的區塊鏈 — 網絡自然地形成有所重疊的社群。
Tax Allocation	稅款分配	一種機制，讓納稅人決定自己一部分稅款流向何處。可分配的百分比逐年增長。
Track Record	往績	一般而言：一個人或組織過往結果、成功與失敗的歷史。此處：某個 DID 身份在網絡中所有過往互動的總和 — 已驗證的主張、被接受與被拒絕的紀錄 — 其聲譽即由此推導而來。

詞彙	繁體中文	意思
Verifier	驗證者	一個經演算法選出、負責驗證並發佈一條紀錄的參與者。以自己的好名聲為資訊的真實性作賭注。

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).