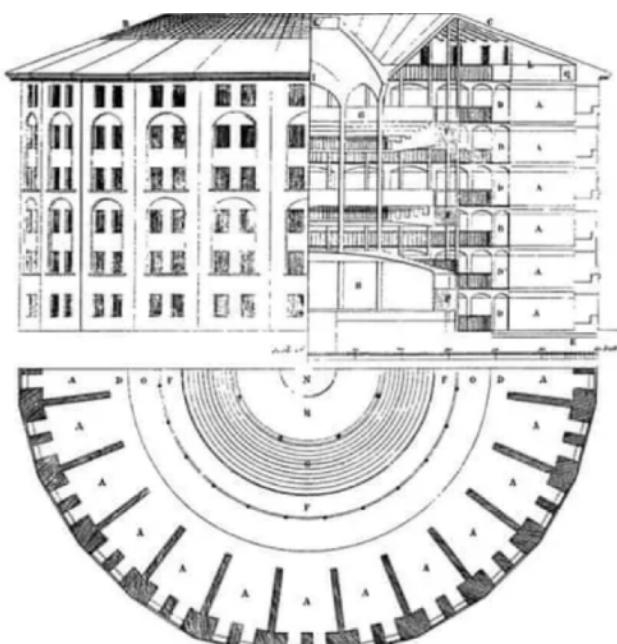


# Web3 基礎設施系列 | 監控國家降臨 英國 | 為什麼中心化數位身分是錯誤 的答案

1785年，英國哲學家傑里米·邊沁設計了一種完美的監獄，他稱之為「全景監獄」。其特點是中央設有瞭望塔，四周環繞著排列成圓形的牢房，一名獄警可以觀察每個囚犯，而囚犯卻渾然不知。這種設計對心理的影響非常深遠，囚犯會不斷調整自己的行為，即使沒有監視，也會假設自己受到了監視，從而形成一種持續的自我監控狀態，僅僅透過觀察就能實現控制。



240年後的今天，英國首相基爾·斯塔默宣布強制推行數位身分證，在全國範圍內建造了邊沁的圓形監獄。這標誌著公民與政府關係的根本轉變，他們用來之不易的隱私權換取了虛假的便利承諾。時機的選擇暴露了偽裝成進步的政治投機主義的本質：世界各國政府抓住危機時刻，將全面的人口監控常態化，而民粹主義在移民問題上的壓力，為監控基礎設施提供了便利的掩護，而這些基礎設施的用途遠遠超出了其既定的用途。

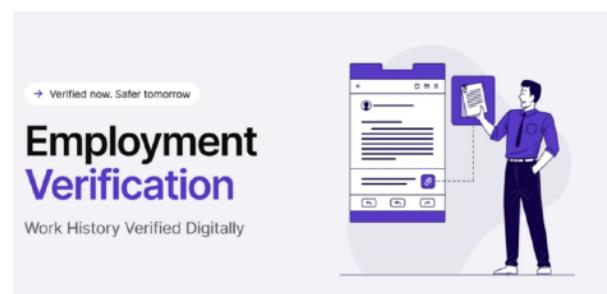


英國的這項計畫計劃於2029年實施，要求所有公民和合法居民持有基於智慧型手機的數位身分證件，用於就業驗證。儘管官員承諾這些身分證件無需每日攜帶，但正在建設的基礎設施卻為比移民管控更具侵略性的措施奠定了基礎。歷史告訴我們，監控系統一旦建立，其範圍永遠不會受到限制，而是演變成全面的社會控制工具，其最初的支持者會對此感到震驚。



政府的宣傳套路與專制政權的慣用伎倆如出一轍，承諾效率、安全和現代化，使數位身分證看起來像是必然的進步，而非潛在的越權行為。回想一下東德，史塔西（Stasi）將公民身份識別變成了一種無處不在的監控機制，以行政必要為幌子追蹤日常生活並控制行動。如今，愛沙尼亞、丹麥和澳洲等國家被視為數位身分系統帶來實際效益的成功案例，它們建構了一種技術進步的敘事，掩蓋了人們對權力和控制的更深層次的擔憂。

這種說法將監控基礎設施描繪成純粹的行政便利，掩蓋了政府監管力度空前的現實。



如果我們揭開行政效率的面紗，就會發現一幅更令人不安的景象：這些系統正以驚人的速度從用途有限的工具演變成全面險惡的監控基礎設施，今天的就業驗證將成為未來醫療、銀行、交通乃至公民生活方方面面的訪問控制。其技術架構揭示了真正的野心：中心化的數位身分系統創建了全面的檔案，即時追蹤用戶的行動、交易、關係和行為，因為每個驗證請求都將成為龐大政府資料庫中的資料點，建構公民活動的詳細地圖。

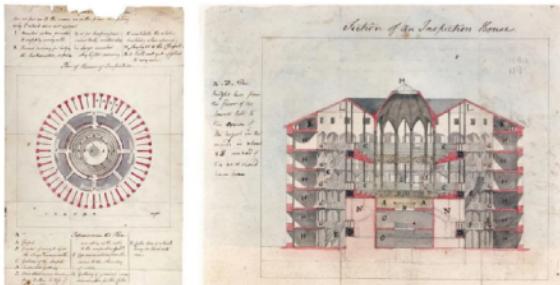
國際特赦組織英國分部的隱私倡導者警告稱，此類系統“存在巨大的身份盜竊風險，並為黑客和網絡犯罪分子提供誘餌”，但與政府積累大量

人口數據檔案所帶來的政治風險相比，網絡安全風險絕對微不足道。一旦這些基礎設施建成，擴大監控權力的誘惑就變得無法抗拒，將最初的行政便利轉變為社會和政治控制的工具，從根本上改變了個人自主權與國家權力之間的關係。

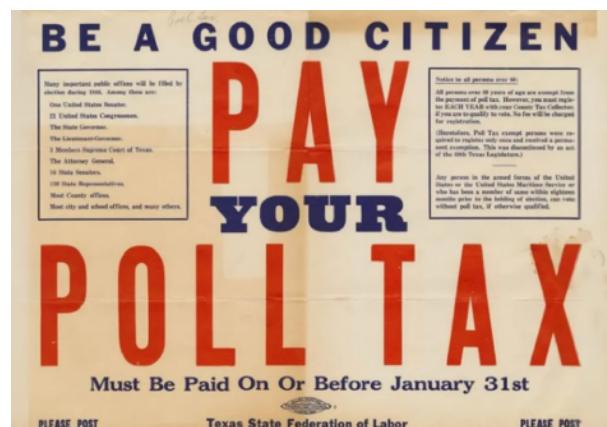


邊沁的圓形監獄在他有生之年從未真正建成，但其心理學原理自此便繚繞在監獄設計中，其天才之處在於行為矯正而非建築創新。19世紀英國維多利亞時代的濟貧院也採用了類似的監視機制，以機構照顧為幌子，透過嚴格的觀察和行動控制來監管窮人。當人們認為自己可能受到監視時，他們會自我監督，從而建立了一個透過監視的簡單可能性而非持續存在來運作的控制系統。

現代英國正在建造一個技術化的圓形監獄，公民們知道他們的每一次數位互動都可能被監控和記錄，這從根本上改變了個人自主權與國家權力的關係，其方式甚至會讓自由民主的締造者感到震驚。

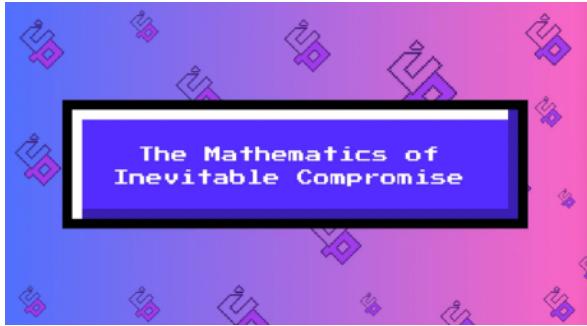


排斥效應加劇了這些監控擔憂，正如大赦國際指出的那樣，“許多老年人沒有智慧型手機或無法正確登記”，“有些人可能難以獲得服務”，從而造成系統性歧視，使技術合規成為獲得完全公民權的先決條件。歷史上，類似的官僚障礙，例如吉姆克勞時代的人頭稅和南非的通行證法，都利用證件要求剝奪社區的權利並進行隔離，這表明身份強制執行可以成為社會排斥的工具。



這實際上將社會劃分為能夠駕馭政府強制系統的人和無法駕馭系統的人，從而形成了一種雙重公民身份，基本權利取決於技術素養和智慧型手機擁有權，而非法律地位或民主參與。

想像一下，當就業等基本權利取決於維持有效的數位憑證時，會發生什麼事？政府獲得了前所未有的權力來控制個人行為，而那些反對政策、參與抗議或從事政治反對活動的公民可能會發現他們的數位身分特權受到限製或被徹底剝奪。經濟流放的基礎設施變得像更新資料庫條目一樣簡單，從而創建了一個系統，在這個系統中，政治上的一致性成為經濟生存的必要條件，而異議最終將面臨被社會數字排斥的懲罰。



1970年，電腦科學家詹姆斯·馬丁（James Martin）撰文探討了集中式資料系統的「魚缸效應」。他指出，資料儲存庫越大、價值越高，對攻擊者的吸引力就越大，因為他們可以專注於高價值目標，而不是分散的小型資料庫。集中式數位身分系統是這項原則的終極體現，它建構了包含數百萬人數位身分的儲存庫，為駭客創造了難以抗拒的目標，他們可以用最小的努力造成最大的破壞。

當這些系統被攻破時——數學上的確定性告訴我們它們會被攻破——損害會同時波及整個人群，相比之下，個人身份盜竊顯得微不足道，因為攻擊者獲得的是完整的個人資料，而不是孤立的信息片段。政府資料囤積造成了憲法學者所說的“道德風險”，權力的累積不可避免地導致濫用，因為全面的監控基礎設施變成了政治控製而非行政效率的工具。

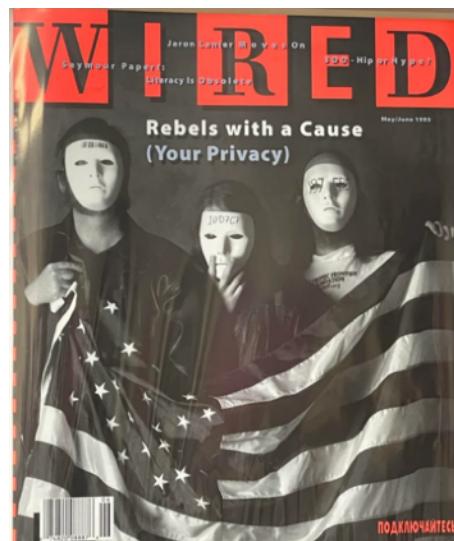


每個資料庫都面臨來自老練對手的持續攻擊，包括政府支持的、尋求情報的駭客、追求利益的犯罪組織，以及利用特權存取的不法內部人員。因此，問題不再是這些系統是否會被入侵，而是何時以及損害將蔓延到多大程度。

一旦攻擊者獲得政府精心匯總成便捷軟體包的個人資訊集中儲存庫的存取權限，入侵將影響到整個人口，而非個人帳戶，從而造成連鎖故障，同時危及所有人的安全。



1990年代，一群密碼學家和電腦科學家開始探索關於數位隱私和個人主權的激進理念，他們設想未來由數學而非法律或信託來保護個人隱私，使其免受政府過度幹預和企業監控。這些「密碼朋克」為現代區塊鏈技術奠定了基礎，並為我們當前的危機奠定了關鍵基礎，即去中心化身份系統，將控制權交還給個人，而不是將其集中在政府資料庫中。



其根本洞見依然有力，因為中心化數位身分的缺陷源自於中心化控製而非數位驗證本身。這表明，基於區塊鏈基礎設施建構的自主主權身分系統可以提供一種截然不同的方法，既能保留驗證優勢，又能消除監控風險。這些系統並非將控制權集中在政府資料庫中，以免成為駭客攻擊的目標和政治壓迫的工具，而是允許使用者維護自己的加密安全憑證，並決定在何種情況下與誰共享哪些資訊。

因此，個人資料將分佈在整個網路中，使用者對其資訊保持精細控制，從而創建無需資料收集和監控即可進行驗證的系統，而中心化系統的設計初衷正是如此。其技術基礎依賴成熟的加密技術，這些技術能夠實現無需披露即可進行驗證，使人們無需透露移民身份、國籍或地址即可證明其工作權利，無需向政府監控數據庫公開其完整的個人歷史記錄即可證明其服務資格。

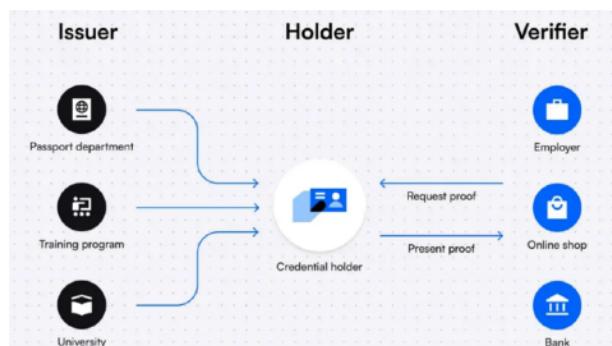
零知識證明透過數學突破實現了這一點，它允許在不洩露底層資料的情況下驗證特定聲明，因此人們可以在不透露確切出生日期的情況下證明自己已年滿 18 歲，或者在不透露簽證狀態或國籍的情況下證明工作許可。這些並非理論構想，而是經過驗證的數學工具，能夠提供比中心化系統更強大的安全保障，並保護個人隱私和自主權，透過數學確定性而非機構信任，實現無需監控的驗證。



密碼朋克願景需要的不僅僅是密碼學理論，還需要能夠滿足現實世界對安全性、可擴展性和用戶體驗需求的實用基礎設施，因為它彌合了理論可能性與實際應用之間的差距。像英國數位身分方案這樣的中心化系統中的每一個缺陷都指向了去中心化替代方案必須解決的特定技術要求，從防止政府監控到消除單點故障，再到維護用戶對個人資料的自主權。

在去中心化身分實作中，Uptick DID 展示如何將這些原則轉化為實用的基礎設施，透過成熟的技術架構來解決中心化系統的每個故障。

英國方案的根本弱點在於中心化，它創造了蜜罐，攻擊者只需一次入侵就能危及數百萬個身分。Uptick DID 是基於 Cosmos-SDK 所建構的分散式架構，旨在讓使用者透過私鑰對自己的憑證進行加密控制，從而減少身分資料在中心資料庫中的集中度。



政府鎖定是另一個重大失敗，因為受困於英國體系的公民，當他們的數位身分特權因政治原因或官僚錯誤而受到限制時，別無選擇。

Uptick DID 透過 Uptick 跨鏈橋和 IBC 協議在多個區塊鏈環境中運行，旨在跨以太坊、Cosmos、幣安智能鍊和 Polygon 等不同生態系統提供一致的身份管理，因此，即使政府頒

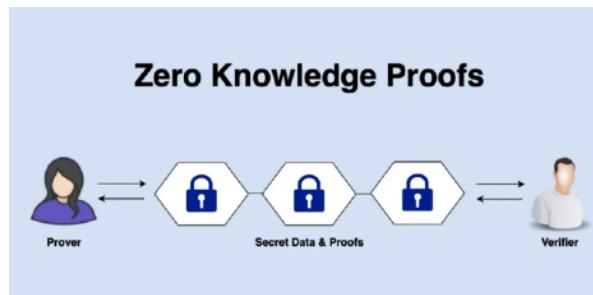
發的憑證受到限制的用戶，仍然可以通過超越政治界限且無法單方面撤銷的去中心化網絡驗證身份並訪問服務。

Get Uptick Network's stories in your inbox  
Join Medium for free to get updates from this writer.

Enter your email

Subscribe

嵌入在中心化數位身分系統中的監控架構會追蹤每項驗證請求，建構公民行為的全面檔案，從而實現政治控制。Uptick DID 透過可驗證憑證解決了這個問題，這些憑證透過零知識證明來證明身份，使用戶無需透露國籍、簽證狀態、工作經歷或任何超出特定憑證範圍的資訊即可證明其擁有工作授權。該架構旨在實現點對點驗證，透過加密簽章確認真實性，從而減少對監控中介機構的依賴。



資料持久性在中心化系統中會帶來額外的風險，因為如今收集的資訊會無限期地保存在政府資料庫中，並被用於公民從未授權或想像過的用途。Uptick 的基礎設施透過 IPFS 整合了 Uptick Storage，用於去中心化憑證存儲，創建了防篡改的記錄，無需依賴中心化伺服器即可存取。使用者可以控制自己持有的憑證、哪些驗證者可以存取這些憑證以及何時撤銷存取權

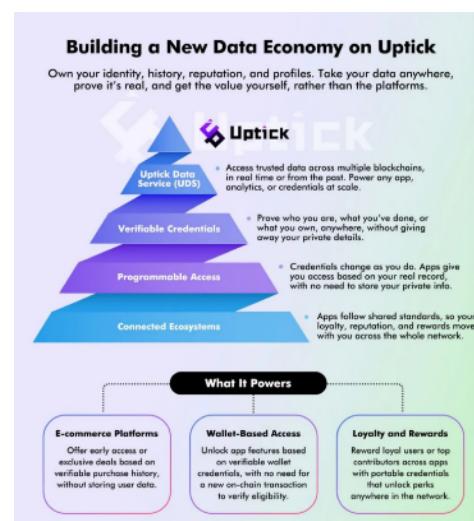
限，從而提供對數位身分的精細控制，而中心化系統在設計上是拒絕的。

英國將缺乏智慧型手機或技術素養的公民排除在外，揭示了中心化數位身分系統如何造成雙重公民身分。Uptick 透過用戶友好的設計解決了這個問題，使去中心化身份無需太多技術專業知識即可訪問，並通過加密安全的密鑰對系統和零知識證明將直觀的界面與全面的加密保護相結合，從而在無需機構監控的情況下提供機構級安全性。

Vouch 平台和 Upward Wallet 透過簡化的憑證管理實現了這種便捷的方法。持有者透過「發行者-持有者-驗證者」模型完全控制其憑證，發行者負責處理憑證創建的複雜性，驗證者可以快速確認其真實性。

或許最重要的是，當政府濫用權力、任意限制存取權限或將監控範圍擴大到超出既定目的時，中心化數位身分系統無法承擔責任。

Uptick 的去中心化資料服務旨在提供透明的追蹤，其中加密簽名保持真實性，並透過可審計的流程以不可篡改的方式記錄在鏈上，用數學證明取代機構承諾，使每個操作都完全可追溯，並防止了中心化監控系統特有的隱形濫用。



這種問題解決架構向我們展示了，透過 Uptick DID 實現的去中心化身分並非簡單地在區塊鏈基礎設施上複製中心化系統，而是從根本上重新構想了數位身分的運作方式，使其服務於使用者而非監視使用者。每項技術選擇都針對中心化方法中的特定缺陷，創造出無需監視的驗證、無需排斥的自主性以及無需集中權力（後者必然會導致腐敗）的安全性。



去中心化身分的經濟效益遠不止於成本節約，但考慮到不同數位身分管理方法的全生命週期成本和經濟效益，這些優勢就顯得尤為重要。英國的數位身分系統需要政府在基礎設施、持續維護成本以及行政和支援方面投入巨額資金，這些成本將給納稅人帶來負擔，無論他們是否選擇使用該系統，因為這會為擴大監控範圍創造經濟誘因。

像 Uptick 這樣的去中心化系統確實將成本分攤到整個生態系統，並消除了大部分行政管理成本，允許透過智慧合約進行點對點驗證，從而降低管理成本，並透過數學而非制度保障來提高安全性和隱私性。儘管去中心化系統需要在用戶教育和基礎設施建設方面進行初始投資，但消除持續的行政管理成本和中心化維護成本將帶來長期的經濟優勢，這種優勢會隨著網路效應降低每用戶成本而不斷累積。

Uptick 將去中心化身分與智慧合約自動化結合，可以簡化憑證驗證等用例。可驗證憑證使用戶無需依賴中心化服務即可證明其身分、資格或屬性，從而帶來效率提升，其效果不僅限於直接的成本節約，還涵蓋減少經濟交易中的摩擦。

這些經濟優勢形成了一個積極的回饋循環，鼓勵創新和應用。隨著越來越多的組織和個人加入 Uptick 的去中心化身分生態系統，並透過提升效率和自動化程度持續降低成本，網路效應將為所有參與者創造價值。最終形成了一個良性循環：更優的技術創造更優的經濟效益，進而推動更廣泛的應用和進一步的技術改進。與中心化替代方案相比，去中心化系統更具吸引力。中心化替代方案會為使用者帶來他們從未選擇承擔的監控成本，而其收益將集中在政府機構及其承包商手中。



去中心化身分認同系統最根本的面向或許在於其治理模式，它以數學確定性和社區共識取代了政治控制，從而消除了中心化系統中常見的腐敗和偏見。Uptick 的實施涵蓋了 DAO 功能，透過其社交 DAO 基礎設施，允許社區建立和維護治理標準和社區決策流程，從而提供能夠適應不同社區需求的治理，並透過透明、

可審計且不可篡改的鏈上流程，確保安全性和可靠性。

DAO 治理提供了政府系統通常缺乏的透明度和問責制，所有治理決策均記錄在鏈上，任何社區成員均可審計，從而確保身份驗證標準的一致和公平應用，避免了中心化系統中可能存在政治操縱或歧視性待遇。儘管 DAO 治理面臨著去中心化決策固有的協調挑戰，但鏈上流程的透明度和不可篡改性提供了中心化政治系統無法比擬的問責保障，從而對權力形成了數學而非機構上的約束。

去中心化治理模式允許在身分驗證方法上進行創新和試驗，讓不同的社區能夠測試各種方法，因為成功的創新是透過自願採用而非政治當局自上而下的強制要求傳播的。這創造了一個治理模式的市場，在大多數情況下，最佳方法的成功取決於自身能力而非政治權力，從而避免了中心化系統特有的監管俘虜和官僚僵化，因為它允許社區共同擁有和管理其身份驗證系統。

這種所有權促成了利害關係人的協調，鼓勵長期可持續性，而不是驅動政府政策的政治短視主義，從而形成服務於社區需求而非政治野心的治理體系。



英國的數位身分計劃是全球趨勢的一部分，即透過數位身分系統加強政府監控和控制。類似的項目正在世界各地實施，因為它們被人們熟知的安全、效率和防詐欺等論調所掩蓋，掩蓋了其作為人口監控基礎設施的真正目的。這一刻將定義數位社會的演變，決定我們是接受監控作為便利的代價，還是透過技術創新而非政治妥協，建構既能維護安全又能維護自由的替代方案。

透過 Uptick DID 等解決方案實現的去中心化身分識別，為抵制這種數位威權主義趨勢提供了一條途徑，因為它保留了數位身分識別所能提供的合法優勢，向世界展示了安全高效的身份驗證是可能的，而無需將控制權交給必然會濫用權力的中央集權機構。區塊鏈的全球性意味著去中心化身分識別系統可以透過 Uptick 的跨鏈協議跨越國界運行，即使在本國政府實施限制性數位身分識別方案的情況下，也能為個人提供身分驗證功能，因為它創造了超越政治控制的國際互通性。



隨著越來越多的個人和組織採用 Uptick 的去中心化身分基礎設施，他們給政府帶來了壓力，迫使政府放棄專制的數位身分方案，轉而採用尊重隱私的替代方案。去中心化系統的經濟和

效率優勢，為企業和機構提供了令人信服的理由，即使面臨政府的阻力，他們也要支持採用去中心化身分。儘管政府可能會透過支持中心化系統的法規或強制要求來抵制，但經濟和安全優勢創造了能夠克服政治阻力的激勵機制，因為企業和公民認識到被排除在跨轄區運營的去中心化生態系統之外的代價。

從本質上講，網絡效應為採用創造了強大的激勵機制，可以克服政治阻力，因為參與的收益會隨著網絡規模的擴大而增加，而被排除在 Uptick 等去中心化身份生態系統之外的代價對組織和個人來說都越來越明顯。



英國正處於傑里米·邊沁時代英格蘭的境地，正處於一種偽裝成進步的新型社會控制的門檻上。政府的數位身分方案建構了全面的監控基礎設施，將前所未有的權力集中在中央集權機構手中，同時也為公民的隱私和自主權帶來了巨大的漏洞。另一個選擇是走向像 Uptick DID 這樣的去中心化系統，它提供身份驗證的優勢，但又不帶有專制色彩，使用數學保證而非政治承諾來保護個人自由，同時保留了數位身份驗證的合法優勢。

如今，建構比中心化替代方案更安全、更私密、更有效率的去中心化身分系統的技術已經存在。Uptick 的 DID 基礎設施證明，這些系統

能夠滿足現實世界的需求，因為它們透過實際操作而非理論可能性來維護個人主權和民主價值觀。數位自由的基礎設施之所以存在，是因為經濟誘因機制傾向於選擇尊重隱私的解決方案而非監控系統，在政府數位身分方案根深蒂固、無法逆轉之前，只剩下選擇去中心化身分而非中心化控制的政治意願。



剩下的就是意識到，英國的經驗警示我們，當公民接受安全和便利的承諾，而不去審視潛在的權力結構，也不去考慮那些既能保障安全又能保障自由的替代方案時，民主社會會多麼迅速地接受專制技術。數位身分的未來取決於今天的選擇，這決定了我們是否接受英國政府關於強制實施數位身分方案的願景，將權力集中在中央集權機構手中，還是透過像 Uptick Network 這樣的平台來建立去中心化的替代方案，透過技術創新而非政治屈服來維護個人自權和隱私。

問題不在於我們是否擁有實現去中心化身分的技術，而是我們是否有智慧和勇氣在數位全景監獄變得像邊沁的實體版本所設想的那樣不可避免之前做出選擇。

在邊沁的時代，全景監獄仍然只是一個從未完全實現的理論構想，但今天的數位全景監獄沒有這樣的限制，這使得我們的選擇比以往任何一代人在自由與控制的鬥爭中所面臨的選擇都更加緊迫，也更加重要。



[hello@uptickproject.com](mailto:hello@uptickproject.com)



[@Uptickproject](https://twitter.com/Uptickproject)



[@Uptickproject](https://t.me/Uptickproject)



[Uptick Network](https://discord.com/invite/Uptick Network)



[Uptick Network](https://www.youtube.com/c/Uptick Network)