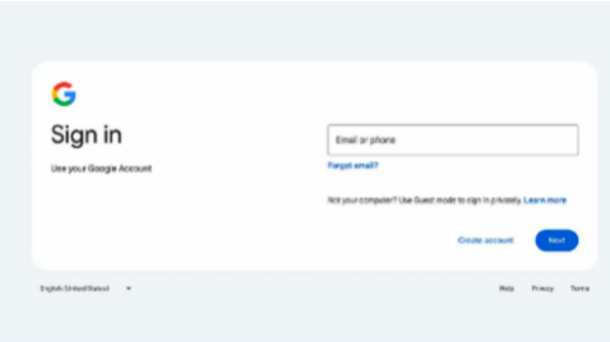
Web3 基礎架構系列 | 身分在 Web3 基礎架構中的作用

自網路誕生以來，線上身分主要依賴帳戶為基礎的體系，如電子郵件、使用者名稱、密碼及身分證號碼等。這些機製本質上是一種「存取許可」的驗證方式。

以Google帳號為例，用戶可以用其登入 Gmail、YouTube 或 Google Drive，但卻無法直接在 Apple、Facebook 或政府服務中使用。這些身分識別標識符雖然曾是創新之舉，但本質上是為封閉、孤立的系統設計的，難以跨平台遷移或互通。



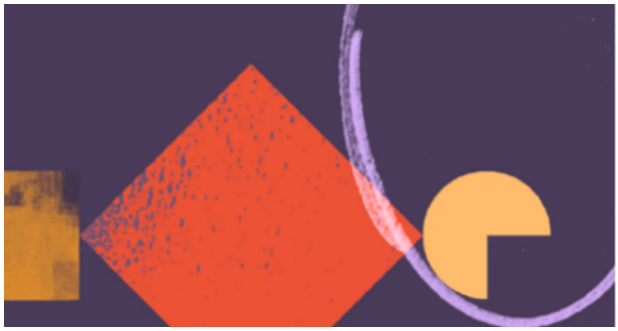
今天，大多數用戶依賴谷歌或蘋果等平台來管理登入資訊。然而，這種便利背後也隱藏著代價——這些平台掌控著使用者身分的創建、資料的共享方式以及應用程式的存取權限。

2018 年的「劍橋分析事件」揭示了這個系統的深層風險：使用者的身份資訊、行為偏好甚至心理畫像被平台未經授權地挖掘、打包並出售。這不是偶發漏洞，而是商業模式使然。

Web3 身分認證正是為解決這個結構性問題而提出的。它將身分控制權歸還給用戶，讓憑證不再由平台集中保管，而由用戶自主持有和管理。

Uptick 致力於打破平台鎖定，基於模組化、跨鏈的基礎設施，實現身分的可組合性與可移植性。有別於舊有系統造成的身份碎片化和訪問壁壘，Web3 的可編程身份系統為身份的未來帶來曙光。這不僅僅是數位護照的替代方案，或傳統 KYC 的簡單翻版，而是一個全新的、模組化的身份架構：它可在多個協議之間靈活調用用戶角色、訪問權限和憑證數據，且無需依賴中心化權威來協調。

這項轉變徹底重塑了存取控制、合規機制及使用者在多生態間的互動方式。在 Web3 世界中，身分認同不再是由平台發布和持有的資源，而是使用者自己攜帶、掌控、並在不同場景中自主使用的主權資產。



2017年，Equifax 遺失了1.47億人的數據，包括社保號碼和財務記錄，這深刻地提醒我們，身分中心化以及摩擦會造成系統性風險。相較之下，去中心化身分則完全消除了單點故障。

> Decentralized identity is a programmable layer that defines how users move, what they can access, and how they're trusted.

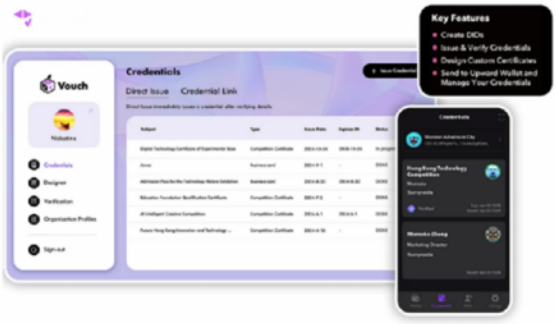
要實現模組化的 Web3 技術堆疊正常運行，身份認證必須具備三大核心特性：可移植性、可驗證性和隱私保護。這使得身分認證不僅僅是提供便利的前端功能或使用者體驗層，而是構成整個系統底層基礎架構的關鍵組成部分。

更重要的是，身分認證不應只是幫助使用者「登入」的工具，而應具備塑造系統運作邏輯與存取機制的能力，成為影響協定架構與生態協作方式的核心力量。

去中心化身分建立在三個核心元件之上：識別碼、憑證和證明。

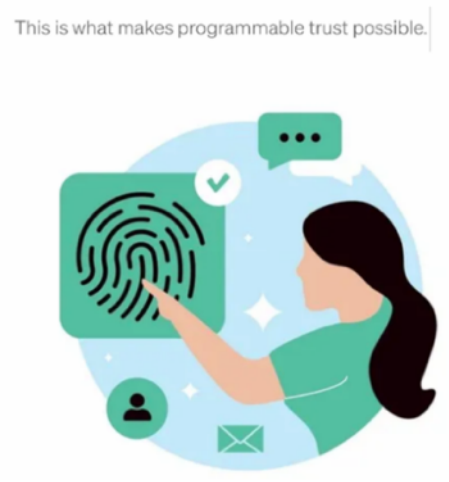
許多人仍然認為 Web3 身分是重新包裝的 KYC，但它的真正價值在於其靈活性和支援它的分層基礎設施。去中心化標識符充當憑證、屬性和證明的主權容器，這些憑證、屬性和證明可以在鏈上和鏈下進行頒發、更新或撤銷。其底層是 DID，它是身分的持久錨點。

除此之外，還有可驗證的憑證， 例如年齡、認證、會員資格或資格。這些憑證可以由機構、DAO、應用程式或其他使用者頒發，用於證明身分或資格，而無需洩露不必要的資料。



除此之外，還有證明，它們驗證了這些說法，但不會洩漏底層資料。

這種分層模型賦予身分識別巨大的靈活性，使其能夠適應各種用例，從內容存取和活動票務到借貸、治理和企業整合。因此，它更著重於建構一個適應不同情境的系統，而不是普通的全域登入。它應該支援可組合性，並且能夠在無許可和受監管的環境中運作。



Uptick 的 DID 系統符合 W3C 標準，並基於 Privado 的 Iden3。 Iden3 的設計充分考慮了可攜性，允許使用者跨平台攜帶已驗證的屬性，例如年齡、居住地或貢獻者身份，而無需暴露個人數據，同時還能適應他們所互動的應用程式或資產的邏輯。

此類憑證已可直接使用 Uptick 的即時 DID 和可驗證憑證平台 Vouch 進行頒發和管理。
Vouch 負責處理從 DID 建立到憑證設計和頒發的所有流程，並支援基於 DID 的直接分發和透過二維碼獲取可認領連結。 Vouch 還支援撤銷和到期功能，允許憑證隨著使用者角色或條件的變化而調整。

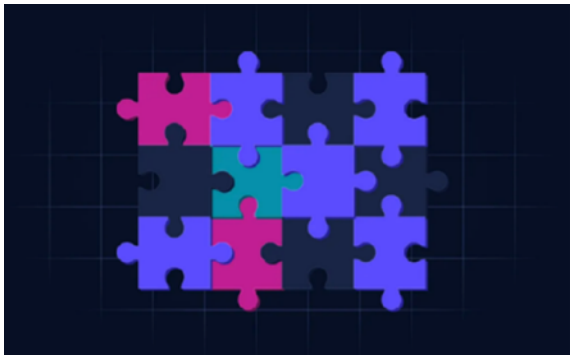
Vouch

與傳統的 Web2 模型相比，像 Vouch 這樣的平台將身分從完全固定的狀態轉變為模組化、可動態調整的狀態。用戶無需在每個應用程式中都重新開始，而是可以隨身攜帶自己的身份。

Composability is the core concept.

發行者決定共享什麼、何時分享以及與誰分享。一個憑證可能用於證明資產的年齡， 而另一個憑證可能用於解鎖對私人 NFT 代幣的存取權限， 又一個憑證可能用於確認 DAO 成員資格。

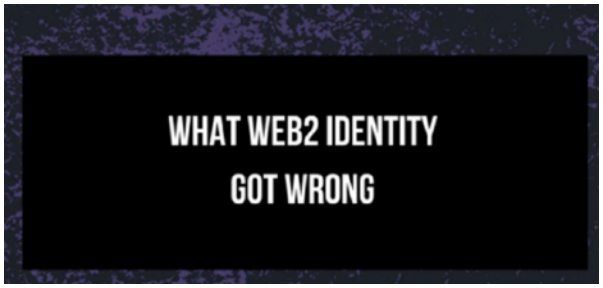
每個憑證都與具體情境相關，並會隨著使用者與資產狀況、 應用程式權限或治理邏輯的交互而演變。



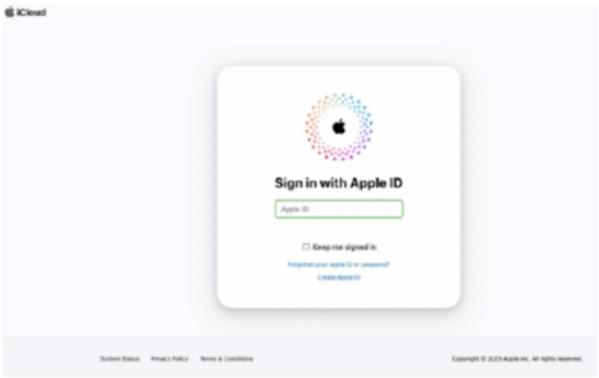
身分並非單一的檔案，而是由 一些可以協同運作的較小部分組成。

DID、憑證和證明各自服務於一個角色，它們可以單獨發布、選擇性地公開，並在需要時組合使用。這 解鎖了廣泛的用例，從社交聲譽、合規邏輯、鏈上憑證到基於角色的訪問， 所有這些都依賴相同的基礎架構。

身分成為使用者和應用程式之間的連結層，為互動添加上下文， 並幫助系統識別行為， 而不是依賴基本的存取控制。本質上，與可驗證身分相關的互動越多，網路就越有用，互通性就越強。



在 Web2 中，身分與帳戶綁定，並由平台控制。 你使用Google、Facebook 或電子郵件登錄， 平台保存你的數據，設定權限，並最終決定結果。這在封閉的環境中行得通，但在依賴共享上下文和分散式信任的生態系統中卻無法擴展。

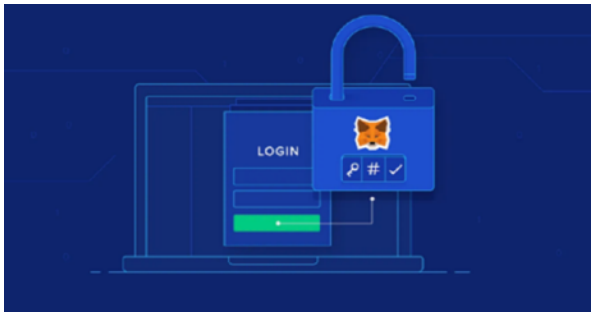


這種模式意味著使用者每次使用新應用程式時都必須重新建立信任。每個平台都建立了自己的“孤島”，彼此之間無法關聯身份或歷史記錄，因此每次用戶遷移，信任都會重置。這使其變成了商業資產，而不是用戶效用，而且由於資料無法隨用戶遷移，因此也會降低速度。

Web3 infrastructure can't just copy the same model.

正如我們在本文開頭所言， 身份應該是模組化、可移植且 可驗證的，無需依賴中間層， 並且應該與無需許可的訪問、 透明度和用戶控制保持一致。

簡單地在鏈上重建登入系統 錯失了重點。否則，我們最終會遇到同樣的問題，只是採用更酷的 Web3 格式。



去中心化身分顛覆了這種結構，因為使用者管理其憑證，應用程式驗證憑證，但實際上並沒有儲存憑證，從而隨著時間的推移建立起可信的互動。聲譽可以跨越生態系統，而無需鎖定於單一供應商，身分成為堆疊的一部分，而不是頂層服務。

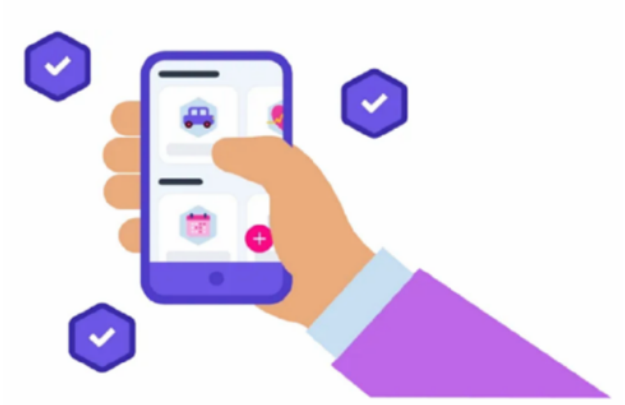
在錢包整合、存取流程或登入方法方面，身分通常被視為前端關注點，但身分在堆疊中的位置更深，支援資產級權限、基於角色的治理、委託授權和聲譽加權邏輯。

這定義了誰可以在什麼條件下採取行動，以及為什麼允許採取行動。 去中心化身分允許智慧合約在不依賴中心化監管的情況下強制執行合規性，從而無需儲存用戶資料即可存取代幣。它還將現實世界的憑證與數位互動連接起來，而不會破壞隱私或去中心化。這樣，身分就成為了在運行時強制執行邏輯的可程式系統的基礎層。

Uptick 在協議層面整合了 DID 模組，這意味著身分認同是核心基礎設施的一部分，每個身分都被設計為直接與資產邏輯、授權系統和應用層連接，因此它被視為一個經過深思熟慮的設計元件。

每個 DID 都錨定了一組可驗證的憑證，這些憑證可以定義資產存取權限、觸發合規性檢查或支援跨應用程式的聲譽系統。這樣，我們就能夠在資產層面強制執行憑證規則，例如，某種代幣可能需要居住證明，而另一種代幣可能只允許經過驗證的貢獻者存取。

每種資產都可以定義自己的條件，並在互動時根據具體情況應用，從而避免瓶頸，並允許在不影響整體靈活性的情況下進行許可。



RWA 可能需要居住證明， 而另一個可能需要投資者認證，或者 DAO 投票可能僅限於經過驗證的貢獻者。特定於資產的規則提供了 精確度，但不會造成中心化的 瓶頸。

這些是模組化的憑證檢查，應用於 交互點。

Uptick 的 DID 結構旨在充當一個權限層，在整個資產生命週期中隨資產一起移動。可驗證的憑證始終保持關聯，因此 所有權和資格可以在任何地方進行檢查，無需中心化協調或 重置。

憑藉跨鏈功能和內置的 零知識證明支持， 允許用戶在不洩露個人資料的情況下驗證聲明，這種基礎設施設計 實現了身份可移植性，無需鎖定，也無需監控即可實現合規性。

聲譽是身分的長期體現，它反映了賦予身分權重的 行動、驗證和關係。在荷馬史詩傳統中，這被稱為 kleos，即透過 行為而非頭銜贏得的榮耀。

從某種意義上說，Web3 建立在 同樣的理念之上，將行為轉化為系統能夠辨識的 持久訊號。Web3 聲譽正在開始取代信用評分、信任評級和靜態用戶資料， 而無需中心化存儲或固定身份，從而實現透過參與而增長的分散式信任。這也為信用委託、DAO 治理和創建者激勵開闢了新的模式，人們可以擁有貢獻者徽章、 已驗證的交付歷史記錄或一系列憑證，這些憑證可以塑造用戶與系統的交互方式。

Access, risk levels, and voting power can all adjust dynamically based on reputation inputs.

聲譽還能提供抗女巫攻擊的能力，而無需實名，因為它允許系統根據行為而不是身份披露來評估用戶，這對於任何希望保持無需許可的開放網絡來說都至關重要，因為它可以過濾掉垃圾郵件和欺詐行為，使信任變得與環境相關，是贏得的，而不是被賦予的。

Uptick 正在建立一個模型，其中聲譽 作為一個可移植、可驗證的層存在，透過參與獲得，並在應用程式邏輯中與資產層和身分層一起直接引用。去中心化客戶關係管理 (DCRM) 可以追蹤已驗證的操作、貢獻歷史記錄和情境回饋，而無需在中心化服務中聚合使用者數據，因此應用程式無需個人資訊或永久識別碼即可識別行為。

這意味著每個操作都可以為更廣泛的使用者畫像做出貢獻，而無需中心化實體進行聚合。

一個有效的識別系統應該優先考慮隱私。

這並不意味著隱藏所有訊息， 而只是意味著讓用戶自主決定何時披露哪些資訊。當憑證包含法律地位、病史或財務資訊等方面時，這一點尤其重要，因為這些資料一旦洩露，可能會被濫用。

Without privacy, composability loses its value.

零知識證明在協議層面強制執行，允許用戶在不洩露底層資料的情況下證明自身資格。選擇性揭露是指在不完全存取的情況下進行部分驗證，而加密的元資料即使在公共網路上使用也能確保憑證的隱私性。

這為可程式信任建立了一個安全的基礎，讓使用者可以控制顯示的內容、時間和物件。資格取代身份，因此您無需姓名或護照號碼即可鑄造代幣或在 DAO 中投票，只需證明滿足條件即可。

這就是去中心化身分的魅力所在， 無需暴露即可進行驗證。

隱私權保護身分是實現受監管的 DeFi、企業治理和機構資產發行的關鍵。如果沒有它，Web3 將會受到很大限制，甚至會倒退到中心化。然而，有了它，所有類型的用戶和用例都可以存在於鏈上並跨境運行。

Uptick 的憑證平台 Vouch 支援選擇性揭露、過期和撤銷，確保憑證在各個系統之間可用且相關。作為其持續發展路線圖的一部分，它還支援零知識證明發行路徑。這使得憑證持有者可以在與 dApp、DAO 或資產系統互動時選擇性地披露數據，所有這些都透過一個錨定在 Uptick 基礎設施上的 DID 進行，然後方便地儲存在 Upward 錢包中。

本質上，它充當一個安全憑證庫，並在 dApp 或 DAO 使用期間提供基於 ZK 的互動介面。

有人可能會認為去中心化身分只是使用者的一個基本概念，但它實際上是一個系統層級元件，在模組化的 Web3 堆疊中，身分是將一切連結在一起的關鍵。

> Decentralized identity allows open systems to apply rules.

存取控制、資產管理、合規性、治理和社區參與都依賴它。身分連結模組、產品和生態系統，賦予系統脈絡、連續性和精確性。

這為使用者提供了跨應用程式的一致性，開發者可以定義權限邏輯而無需設定障礙。 機構可以在不損失監管清晰度或可用性的情況下進入 Web3，因此，身分使結構化參與成為可能，而無需為每個應用程式建立新的信任模型。

Uptick 將身分視為核心基礎設施元件，與資產生命週期引擎、資料服務和治理模組協同工作。身分賦予資產意義，資產定義交互，資料連結兩者。當這些部分可組合時，基礎設施將變得更加適應性，這使其能夠支援。

身分正在從基於帳戶的系統轉向可驗證、可組合的憑證。隨著這種轉變，信任源自於行為而非平台分配，互動也變得具有情境性、預設私密性，並且跨網路相容。身分將與代幣、錢包和資料饋送並列，成為 Web3 堆疊的核心層。這種轉變改變了開發者處理存取控制的方式，因此他們無需為每個新應用程式重建身分邏輯，而是可以使用隨使用者移動的憑證，直接在資產或應用程式層級定義權限規則。然而，支援這種模型需要將身分視為堆疊一部分的基礎設施。

Uptick 提供了這一基礎，因為該協議包含一個去中心化身份 (DID) 系統、模組化憑證邏輯，以及對基於零知識的驗證的內置支持，所有這些都與資產邏輯、訪問控制和治理模組集成在一起。 Uptick 的識別系統支援選擇性揭露，而像 Vouch 這樣的平台（已整合在 Uptick 堆疊中）允許這些憑證一次簽發並跨不同系統使用，從而使開發人員無需直接管理使用者資料即可執行權限規則。憑證能夠在不暴露底層資料的情況下證明資格，並且由於零知識支援是該架構的一部分，使用者可以在不洩露個人資訊的情況下滿足條件。這使得從隱私投票、受監管的資產存取到開放系統內的合規性檢查等各種應用成為可能。 前路漫漫，但隨著身份的不斷發展，它正在成為定義跨網路系統的信任、存取和協調的基礎層，它在設計上是可編

程和可移植的，並且旨在將控制權掌握在用戶手中。

 hello@uptickproject.com

 @Uptickproject

 @Uptickproject

 Uptick Network

 Uptick Network