Web3 基礎設施系列 | 打破驗證中間人陷阱

每一份工作申請、公寓租賃和專業執照申請都需要你再次證明你之前已經向頒發機構證明過的資格。

例如，大學在你畢業時會確認你的學位，但雇主仍然需要支付 15 到 20 美元，透過像美國國家學生資訊交換中心 (National Student Clearinghouse) 這樣的第三方服務機構再次驗證，而且通常還會捆綁背景調查費用，導致成本更高。專業委員會在頒發執照時會確認你的執照，但客戶需要支付驗證費來確認你持有該執照。

此外，還有一些背景調查公司會收取 30 美元來驗證你之前的雇主已經在系統中記錄的工作經驗。

事實上，這種模式在你的職業生涯中會重複數千次，因為每個新的雇主、房東、認證機構或客戶都會要求你重新驗證那些自最初頒發機構頒發以來從未更改過的資格證書。 2015年獲得的學士學位，在2018年換工作時需要重新驗證，2020年申請研究生院時需要再次驗證，2022年租房時需要再次驗證，2024年申請專業資格認證時需要再次驗證，儘管證書本身在每次驗證中都完全相同。

傳統的學歷認證透過集中式中介機構運作，每次有人需要證明自己已獲得的資格時，這些機構都會收取費用，從而形成了一個基於重複驗證的數十億美元產業。同樣的學位、執照或工作記錄，即使在頒發數十年後，仍然能夠持續產生收入。美國國家學生資訊交換中心（National Student Clearinghouse）每年在其約3600家機構的網絡中處理數百萬次學歷認證，作為一家非營利機構，其每年僅從這些認證服務中獲得的收入就超過1億美元。

這些服務之所以連結在一起，是因為它們都基於一種機構間脫節的商業模式：大學、雇主和執照頒發機構拒絕頒發其係統已驗證的可移植證書，迫使證書持有者反覆購買驗證服務，而不是提供他們真正能夠掌控的選項。大學在你畢業時確認你的學位已存在於他們的資料庫中，但他們沒有提供任何機制讓你在不付費給中間人的情況下向第三方證明這一點，而這些中間人查詢的資料庫正是你的畢業證書所引用的資料庫。

Web3 基礎設施徹底瓦解了這種資訊提取方式。機構只需頒發一次可驗證的證書，證書上的加密證明便永久有效，驗證過程透過數學上的確定性而非資料庫查詢來實現。此外，隱私保護型證明允許選擇性地披露信息，而不會將底層數據暴露給那些利用你的個人信息牟利的驗證服務機構。

大學擁有一套名為註冊系統的系統，用於追蹤每個學位的授予情況，並將畢業記錄儲存在資料庫中。當學位持有者需要驗證學歷以用於就業、繼續深造或申請專業執照時，大學會查閱這些資料庫。這些記錄在初始資料輸入後幾乎無需大學維護，它們作為永久性數位檔案存在，學位授予後便不再更改。

問題在於，大學沒有為畢業生提供獨立驗證學歷的機制，而是要求驗證請求者直接聯繫註冊辦公室或使用指定的第三方服務，例如全國學生資訊交換中心（National Student Clearinghouse）。畢業生在求職時會向潛在雇主提供學位信息，但雇主無法輕易相信畢業生的說法，因此他們不得不付費請驗證服務機構查詢大學數據庫，以確認學位是否如畢業生所述真實存在。

這就形成了一種持續的收入來源：同一個學位會在畢業生的整個職業生涯中產生數十次驗證費用，因為每個新的雇主、研究生課程或專業認證機構都需要獨立的驗證資訊。 2020 年的學士學位在未來十年內可能需要被五家雇主驗證、三個不同的專業認證課程驗證、兩次研究生申請驗證，以及各種公寓租賃或安全許可的背景調查驗證，總共會產生超過 500 美元的驗證費用，而大學在頒發學位證書時只確認過一次。

美國國家學生資訊交換中心 (NSC) 在學歷認證領域幾乎處於壟斷地位，為超過 3600 所院校處理學歷認證，涵蓋了高達 97% 的美國學生。大學將認證工作外包給 NSC 是為了避免接聽雇主電話帶來的行政壓力，但 NSC 對每次驗證查詢都收取費用，從基本的入學確認 4.95 美

元到學位驗證 14.95 至 19.95 美元不等，從大學免費提供給 NSC 的數據中榨取利潤。

這種經濟模式造成了一種反常的激勵機制：大學沒有動力頒發可攜帶的學歷證書，因為驗證過程不會產生任何成本。雇主支付驗證費用，畢業生忍受等待確認的漫長過程，而國家安全委員會（NSC）則透過介入院校和驗證請求者之間來獲取收入。

大學將行政工作外包，並且沒有壓力去改變那些在他們看來運作良好的系統。

這種驗證流程違反了基本的資料所有權原則：畢業生透過多年的學術努力和學費支付獲得了學歷證書，但卻沒有任何獨立的成就證明可以在不經過院校或其指定驗證機構的情況下出示。事實上，文憑除了紙面上的內容之外，沒有任何實際意義，因為任何人都可以花100美元在網上購買假文憑，如果沒有數據庫驗證，這張紙質文憑就毫無價值，而數據庫驗證只能由大學或其授權機構提供。

Uptick 的 DID 基礎設施透過符合 W3C 標準的去中心化識別碼解決了這個問題，使院校能夠頒發可驗證的證書，這些證書以加密簽署數位證書的形式存在，畢業生可以將其儲存在個人錢包中。

當大學授予學位時，他們可以頒發一份使用院校私鑰進行加密簽名的可驗證證書，其中包含學位詳情的結構化數據，畢業生可以將這些數據存儲在自主身份錢包中，而無需依賴院校數據庫或紙質文憑。目前，機構已經可以透過 Vouch 等平台實現這種憑證授權模式的部分功能。在 Vouch 等平台上，任何人都可以使用持有者的 DID 直接頒發證書，或者生成畢業生訪問的聲明鏈接，以便獲取其可驗證的學位。這表明，加密證書的頒發無需大學開發定制的 Web3 基礎設施即可實現。

當畢業生需要向雇主證明其學歷時，他們只需從錢包中出示可驗證證書，雇主即可透過數學方法驗證大學的加密簽名，而無需聯繫大學或支付驗證服務費用。簽名證明證書來自大學，頒發給出示證書的特定畢業生，並且自頒發以來未被篡改，從而提供絕對的數學確定性，無需數據庫查詢或第三方驗證服務。

其工作原理基於公鑰加密技術。大學維護公鑰，並透過可驗證的鏈上註冊表發布，將機構身分映射到加密地址，允許任何人引用和驗證簽名，但只有大學持有簽署證書所需的私鑰。偽造的證書會立即無法透過簽名驗證，因為造假者無法在沒有大學私鑰的情況下產生有效簽名，這使得偽造在計算上不可行，而不僅僅是難以透過人工驗證流程檢測。

Uptick 的可程式 NFT 協議旨在將這些證書作為不可轉讓的代幣，綁定到具有靈魂綁定特徵的特定 DID，從而防止證書欺詐，即個人購買或租用他們未獲得的證書。該證書以 NFT 的形式存在，並透過智能合約與畢業生的 DID 綁定。

智慧合約可防止證書轉移到其他帳戶，因為嘗試轉移證書會失敗，接收帳戶無法提供加密證明，證明其與證書所代表的學位相關。

背景調查公司透過核實前雇主已記錄在其內部系統中的工作經驗來賺取巨額收入。 Checkr、HireRight 和 Sterling 主導著全球價值約 120 億美元的背景調查行業，它們對每位候選人收取 30 至 100 美元的費用，以核實雇主人力資源資料庫中已有的工作日期、職位和薪資資訊。

核實流程是透過背景調查服務直接聯繫候選人的前雇主，要求確認候選人是否曾在所聲稱的日期和職位上工作過。這需要大量的人工，因為人力資源部門需要處理核實請求、交叉核對內部記錄，並向背景調查服務提供書面確認，而背景調查服務再將結果轉發給潛在雇主。

每次工作變動都會觸發這個核實循環，即使基本事實沒有改變，相同的工作記錄也需要重新核實。這意味著，某人在2018年至2022年間曾在A公司工作，但當他2022年加入B公司時，其在A公司的工作經歷需要再次驗證；2024年加入C公司時，需要再次驗證；2025年申請專業認證時，又需要再次驗證。即使在A公司的工作經驗始終是不變的歷史事實，且已被多次確認。

前雇主承擔了處理驗證請求的行政成本，但他們沒有動力簽發可轉移的就業證明，因為驗證過程中的摩擦對他們來說並非負擔。背景調查公司透過介入需要確認的雇主和持有記錄的前雇主之間來收取驗證費用，而潛在雇主則承擔了這些成本，因為如果僱用未經驗證的候選人，一旦就業聲明被證實為欺詐，他們將承擔法律責任。

最終，我們陷入了這樣一種境地：員工無法獨立證明自己的工作經歷，除非聯繫前雇主或付費請背景調查公司聯繫他們。 W-2稅表可以證明收入，但無法證明職位或職責；錄取通知書可以證明初始工作，但無法證明工作時長；工資單可以證明特定時期的工作，但無法證明完整的就業歷史。

目前尚無任何便攜式證據表明，員工可以控制展示其完整的職業發展軌跡，而無需前雇主對資料庫查詢作出回應。

Uptick 的可驗證憑證框架旨在幫助雇主在員工離職時頒發加密簽名的僱傭憑證，記錄員工的僱用日期、職位、職責和績效指標等結構化數

據，這些數據由員工儲存在他們控制的 DID 錢包中。

當員工申請新職位時，他們可以提供先前雇主的僱傭憑證，潛在雇主無需聯繫前雇主或支付背景調查費用，即可透過數學方式驗證簽名。

該框架採用與學術證書相同的公鑰加密技術：前雇主使用私鑰對僱傭記錄進行簽名，員工將簽名憑證儲存在錢包中，潛在雇主使用公鑰驗證簽名，從而證明憑證來自所聲稱的雇主，而無需直接聯繫或查詢資料庫。加密簽名提供了僱傭記錄真實且自頒發以來未被篡改的數學證明，從而無需電話、電子郵件確認或背景調查服務。

透過零知識證明，員工無需透露完整的僱傭記錄即可證明特定的僱傭關係，從而實現保護隱私的驗證。員工無需透露特定日期、薪資資訊或離職原因，即可證明其在特定公司擔任特定職位超過兩年，從而滿足驗證要求並保護個人資訊免遭不必要的洩露。

這種選擇性揭露機制已在生產環境中應用。憑證持有者提交多屬性憑證，但可以選擇驗證者可以訪問哪些特定屬性，例如僅披露“高級經理，2020-2024”，而將績效評估和薪酬詳情保密。加密簽章用於確認所揭露屬性的真實性，而無需暴露完整的僱用記錄。

Uptick 的 DID 基礎設施透過零知識證明協議來實現此功能。在該協議中，員工產生加密證明，證明其僱傭憑證符合特定標準，而無需洩露底層資料；驗證者則透過數學方法確認這些證明，而無需存取完整的憑證。例如，要求求職者提供五年管理經驗證明的潛在雇主，無需了解候選人的具體工作時間、薪資增長情況或曾就職的具體公司，即可驗證其工作經歷是否符合要求，只需確認其總體經驗即可。

專業執照在職業生涯的多個階段都需要驗證，例如醫生、律師、會計師、工程師和技術工人需要向雇主、客戶、保險公司和監管機構證明其資格。各州執照委員會維護追蹤每位持證專業人士的資料庫，儲存確認個人已完成所需教育、通過考試並透過繼續教育維持有效執照狀態的記錄。

然而，執照委員會並未提供專業人士可以獨立出示的便攜式證明，而是要求驗證請求者直接查詢州資料庫或使用專門的驗證服務。醫療執照驗證服務每次向醫院收取 50 至 150 美元的費用，以確認醫生在特定州持有有效執照；法律名錄向律師事務所收取訂閱費，以提供律師資格驗證服務；工程委員會則要求對每位需要驗證資格的專業人士進行人工驗證。

這造成了驗證方面的繁瑣流程，持證專業人士每次加入新機構、接納新客戶、申請醫療事故保險或跨州工作時，都需要進行資格驗證。一位在三個州獲得執業資格的醫生，由於獲得醫院執業資格、加入醫療集團、與保險網絡簽約以及出差從事臨時執業等原因，其執業資格每年可能需要驗證五次，即使其執業資格全年保

持有效且未發生變化，驗證費用累計也可能超過 500 美元。

對於持有多個認證的專業人士而言，驗證問題會更加複雜，因為除了基本執業資格之外，其他專業資格也需要單獨驗證。例如，一位擁有三個專科認證的醫生，除了持有州級執業資格外，還持有來自不同委員會的專科認證，這使得驗證過程更加複雜。醫院在核查資質時，必須查詢州級資料庫以確認其執業資格，並聯繫專科委員會確認其專科認證狀態，從而增加了行政管理和驗證成本。

專業執業資格委員會往往不願意頒發可攜帶的執業資格證書，因為驗證收入是委員會運營的資金來源，這些收入包括資料庫存取費、列印驗證信函費和線上驗證服務費。特別是醫療委員會，由於醫院、保險公司和資格認證機構需要支付定期費用來確認醫生的執業資格，而這些費用實際上在頒發和續簽執業資格時，委員會已經驗證過這些資格，因此醫療委員會從驗證服務中獲得了可觀的收入。

Uptick 的基础设施使执照颁发机构能够颁发可验证的证书，这些证书以加密签名的形式存储在 DID 钱包中。智能合约会自动更新证书状态，反映续期、继续教育完成情况或纪律处分等信息，而无需专业人员获取新的证书。

当医生续签行医执照时，执照颁发机构会通过执行智能合约更新链上证书的状态。任何验证证书的人都能看到反映最新续期的当前状态，而无需联系机构或支付验证费用。医疗委员会可以选择实施此方案：在医生通过考试后颁发初始执照作为可验证的证书，然后在满足继续教育要求后通过智能合约更新元数据。医院可以通过医生提供的二维码验证证书，而无需等待数天时间等待验证服务查询州数据库并返回确认信息。

该方案通过可编程证书实现：初始颁发会创建一个与专业人员 DID 绑定的基础证书，后续的机构操作会更新链上元数据，供验证者在检查证书时参考。医院在验证医生执照时，首先通过数学方法确认执照证书上委员会的签名，然后查询链上数据，根据委员会最新的续期信息确认当前的有效状态，从而无需直接查询数据库或通过验证服务机构进行验证。

选择性披露使专业人士能够在不公开完整监管记录的情况下证明其执照状态。除非出于验证目的需要，否则纪律处分、投诉或之前的状态变更等信息均保持私密。简而言之，这意味着医生可以在不披露过去曾被调查但最终未采取纪律处分的投诉的情况下，证明其持有有效的、不受限制的行医执照，从而满足验证要求并保护未导致限制的监管事项的隐私。

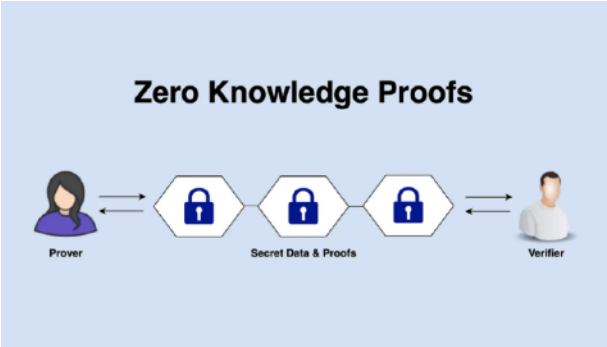
目前的驗證流程意味著，持證人需要披露超出驗證要求所需的個人信息，從而造成隱私洩露，而驗證服務機構則透過資料聚合從中牟利。

當雇主要求進行背景調查時，員工授權驗證服務機構訪問完整的就業歷史、成績單、全面的犯罪記錄和詳細的信用報告，儘管雇主可能只需要確認特定信息，例如學位完成情況或無犯罪記錄。

一份工作申請可能只需要確認是否擁有學士學位，但學歷驗證服務機構卻被授權存取完整的成績單，包括成績、所修課程、學業警告記錄和所獲榮譽。就業驗證也類似地提供了完整的就業歷史，包括離職原因、是否符合再次聘用條件以及主管評價，而雇主可能只需要確認工作日期和職位。

這種過度揭露的現像源於驗證流程採用二元授權模式：員工要麼授予完全存取權限，要麼完全阻止驗證，缺乏選擇性披露機制，無法在不洩露底層資料的情況下證明特定資訊。候選人若不公開GPA就無法證明自己已畢業，若不披露薪資歷史就無法核實工作經歷，若不披露完整的監管記錄（包括從未導致紀律處分的投訴）就無法確認執照狀態。

零知識證明協議透過加密技術解決了這些問題，使證書持有者能夠在不洩露底層資料的情況下證明其證書的特定聲明。這意味著，員工無需透露特定院校、畢業日期、專業或GPA，即可證明自己擁有認可大學的學士學位，既滿足了基本的學位要求，又避免了詳細的學術記錄被不必要地洩露。



Uptick 的基礎設施透過零知識證明（ZK-proofs）來實現此功能，該證明產生加密證明，確保憑證符合特定標準，同時不洩漏憑證內容。當驗證者需要確認候選人是否持有相關學位時，候選人的錢包會產生一個零知識證明，證明其可驗證的憑證符合要求。驗證者無需存取包含畢業日期、具體院校、課程或成績的實際憑證，即可透過數學方式驗證該證明。

這使得各種細緻的驗證場景成為可能：例如，可以透過範圍證明來確認薪資要求，證明候選人之前的薪酬已超過閾值，而無需透露具體數字；可以在不洩露獲得日期或續期記錄的情況下驗證專業認證；可以在不披露安全許可級別或頒發機構的情況下確認安全許可狀態。

每次驗證僅披露滿足驗證目的所需的最低信息，從而保護隱私並確保被驗證聲明的數學確定性。

验证中间人陷阱依然存在，因为当前的基础设施将凭证所有权分散在持有者无法独立访问的机构数据库中，人为地造成了对查询这些数据库并将结果打包提供给验证请求者的服务的依赖。

大学维护学位记录，雇主维护雇佣记录，执照颁发机构维护证书状态，但这些机构都无法提供持有者可控制且无需中介即可提供的可移植证明。

改变这种现状需要一种基础设施，其中凭证以加密签名数字证书的形式存在，持有者将其存储在自主身份钱包中；验证通过数学签名确认而非数据库查询进行；选择性披露能够提供保护隐私的证明，仅披露验证所需的信息。

机构已经通过这种基础设施颁发凭证，而无需具备 Web3 专业知识。他们通过接口设计凭证，自动处理加密签名，并通过无需始终在线系统或专用硬件即可在物理空间中运行的方法实现验证。每个组件都通过消除集中式依赖关系来解决当前系统中的特定缺陷，从而避免信息提取。

Uptick 的 DID 基础设施提供身份层，使凭证能够通过去中心化标识符绑定到特定个人，这些标识符可在各个机构间通用，无需中央注册机构或凭证颁发机构之间的协调。

员工来自多所大学、雇主和执照颁发机构的专业凭证均可引用同一个 DID，从而创建一个统一的身份，将来自不同来源的凭证聚合到一个由员工通过加密密钥而非机构权限控制的钱包中。

通过 W3C 标准颁发的可验证凭证提供数据层，使机构能够对凭证进行加密签名，员工能够将凭证存储在他们控制的钱包中，验证者能够通过签名验证来确认凭证的真实性，而无需联系颁发机构。凭证以结构化的 JSON 文档形式存在，其中包含声明数据和证明颁发机构创建声明的加密签名，二者结合可提供凭证真实性的数学确定性。

智能合约提供逻辑层，支持动态更新证书状态。证书的续期、撤销或修改均通过链上交易完成，无需重新颁发证书。因此，作为可验证证书颁发的医疗执照在续期后不会失效，而是由许可机构更新链上状态以反映续期情况。验证者通过智能合约查询自动检查证书的当前状态。

零知识证明协议提供隐私层，支持选择性披露。工作者无需披露底层数据即可证明证书的特定声明，验证请求者只需了解所需信息。工作者在保护详细信息免遭不必要的披露的同时，仍能提供数学证明，证明其证书满足验证要求。

通过 Uptick 的跨链桥 (UCB) 和 IBC 协议实现的跨链互操作性，使得在不同 Web3 基础设施上颁发的证书能够无缝协作，避免了因大学使用基于以太坊的系统而颁发的证书与雇主使用基于 Cosmos 的基础设施而颁发的证书无法互操作的情况。这种可移植性使得工作者可以从任何发行方（无论选择何种区块链）获取凭证，并向验证者提供统一的凭证集，而无需考虑底层技术架构。

驗證中間人陷阱之所以持續存在，是因為製造這問題的機構無需承擔任何成本。大學、雇主和執照頒發機構維持著資料庫壟斷，它們之所以能從中獲取驗證收入，正是因為它們從不頒發可移植的證書。而任何有能力改變這種現狀的人都面臨著足夠的壓力。勞工承擔驗證費用，雇主承擔背景調查成本，而驗證中介機構則從交易雙方收取費用。如果憑證授權單位在核發憑證時直接對記錄進行加密簽名，那麼這筆交易原本無需中介。

可驗證證書改變的是驗證交易背後的經濟結構。因此，當大學在畢業生畢業時頒發加密簽名的證書後，未來所有驗證該證書的雇主都可以通過數學方式進行驗證，而無需中間機構查詢證書所引用的同一數據庫來獲取收入。 2015年獲得的學士學位在2018年、2020年、2022年和2024年將不再產生驗證費用，因為畢業生持有可移植的證書，無需訪問資料庫即可確認。

然而，機構採納問題才是真正的障礙。像Vouch這樣的平台已經表明，頒發加密證書並不需要大學構建定制的Web3基礎設施或發展深厚的技術專長，但經濟利益仍然阻礙著那些從驗證過程中獲利的機構採用加密證書。醫療委員會透過證書查詢獲得收入，國家安全委員會（NSC）從雇主驗證中收取費用，背景調查公司從就業確認中攫取數十億美元，所有這些收入來源一旦證書持有者擁有可進行數學驗證的便攜式證明，就會消失。

Uptick的基礎設施通過去中心化身份、可驗證的證書標準、可編程智能合約邏輯和零知識隱私，為這種轉變提供了技術基礎，從而創造了證書頒發機構停止通過數據庫訪問盈利，轉而開始頒發其記錄本身就支持的便攜式證明的條件。當競爭壓力、監管變化或證書持有者要求使用便攜式證明時，這種轉變就會發生，因為這些因素會改變目前從基於自身管理便利而非證書所代表的人員利益而建立的系統中獲利的機構的考慮。

Uptick Network

hello@uptickproject.com

@Uptickproject

@Uptickproject

Uptick Network

Uptick Network