

超越密碼：區塊鏈驅動的身份驗證

文／蔡孟凌

區塊鏈在這幾年被廣泛運用在各個領域，我們過去也介紹過各種產業的應用場景，這次要來跟大家分享近期很常被拿出來討論的「使用區塊鏈技術來驗證身份」。

這部分主要分成兩類，一個是將實體的文件透過演算法轉換成 hash 後寫入到區塊鏈上，另一種則是透過代幣綁定個別持有者來進行身份驗證。接下來我們就來看看這兩種類型的使用場景和差異。

一、數位憑證

數位憑證在近年來學術界、培訓機構以及其他需要發放和驗證證書的場合中越來越受歡迎。這不僅可以減少偽變造證書的可能性，也可以使證書的驗證過程更為迅速和簡單。我們可將數位憑證分為兩類，除了數位證書外，還有數位徽章的發行。

II (一) 數位證書 (Digital Certificate)

我們先來看目前應用範圍較多的數位證書，目前國內外有許多大學已經將傳統實體文憑無縫轉換為數位證書。數位證書可以由發證單位控制，例如當發現有人用不正當的方式取得大學學位時，該大學希望可以使該學生先前取得的畢業證書作廢時，需要取得實體證書正副本並銷毀，然而此舉動並不能避免該學生將該證書放在其履歷中，若第三方未能直接與學校驗證證書真偽，也不太可能知道該證書已經失效。相比之下，數位證書可以透過一鍵驗證的方式，即可確認該證書是否為真、證書期限、是否已被



圖 1 證書驗證圖示 (圖片來源：圖靈鏈)

發證機構撤回等。

圖 1 是台灣新創圖靈鏈 (Turing Certs) 所提供數位證書服務上鏈後的驗證畫面，只要在數位證書上方點擊「驗證」，即會自動執行驗證程序，對第三方要驗證證書真偽非常便利。

由此可見，我們可以保存的數位資產不只是加密貨幣、NFT 的代幣類型，這種基於發證者和收證者的相互信任，還有第三方針對該數位憑證的驗證性，讓我們可以看見此類需求正在迅速增長。尤其在疫情期間，數位學習取代實體學習，許多教育訓練機構透過網路進行培訓、發放微型證書來填補傳統教育的技能差距。當數位證書持續累積後，這些就會是我們的個人履歷、記錄個人的學習歷程。

II (二) 數位徽章 (Digital Badge)

在很多行業都會看到數位徽章的應用，例如在

教育系統中，數位徽章可以代表持有者具有某種特定技能、成就、學習成果。它通常包含有關這項技能或成就的具體資訊、發行者身份、如何獲得等，因此數位徽章不只是一個圖示或標示，並且具備驗證機制，已確認其真實性和有效性。

在數位學習的世代，隨著技術和教育界的發展，尤其在職業發展和終身學習的背景下，相信數位徽章會越來越受到重視。

二、身份驗證

在現在 AI 普遍應用的時代，可以看到像是 deep fake 深偽技術等非真人的身份出現在網路世界中，若單就影像或視訊、AI 演算法已經無法區分對象是否為真人。另外，當我們進入 Web 3.0 的世界時，會面臨到支付等商業行為需要驗證身份，過去我們可能會使用第三方支付、刷卡等形式在網路

世界進行轉帳或付款行為，然而還是有許多人並沒有銀行帳戶可供驗證，因此數位身管理（Digital identity management）成為了一個新的商機。例如 IBM 有基於區塊鏈的數位憑證服務，近期最受關注的則是 Worldcoin 的基於虹膜掃描技術的加密貨幣項目，目前已經收集超過百萬以上的用戶的視網膜掃描。

人格證明是 Worldcoin 主要核心理念之一，除了透過 Orb 裝置（圖 2）辨識人別身份外，更重要的是確保一個人只能註冊一次，讓區塊鏈網路中能公平分發其代幣，避免目前網路世界中假帳號、一個人持有多組帳號的問題，也就是一個能夠向網路證明該人實際上是網路中的唯一性，打造網路信任模型（Web of Trust）。從該項目的白皮書可以看出



圖 2 生物識別設備 Orb（圖片來源：worldcoin.org）

Worldcoin 未來的應用場景有：數位資產的持有與轉移、數位身份識別、代幣治理。

在數位身份識別的部分，我們可以想像當全世界的人都已經掃過虹膜、建立個人數位身份後，這樣的資料庫就可以讓我們在各種網路上的服務需要驗證身份時派上用場，例如「Login with World ID」。

Worldcoin 產生數位身分的流程如下：

1. 使用者透過下載 World APP 並親自出現在 Orb 裝置前。
2. 點選「立即驗證」，將會生成兩對金鑰儲存在其手機中，一個是以太坊錢包金鑰對，一個是身份錢包金鑰對。
3. 驗證時，使用者向裝置顯示公鑰，透過 Orb 掃描該虹膜的唯一編碼透過神經網路計算後，再用私鑰簽名，接著傳送到後端伺服器進行校驗（圖 3）。
4. 當用戶之後使用 World ID 時，則是透過零知識證明（zero-knowledge proof）來證明這個公鑰已經被包含在使用者的集合中，因此在各種生態系統中都可以使用這個作為證明身份的方式，而且不會洩露任何個人資訊（圖 4）。

有人認為 Worldcoin 將可以打造世界級的數位

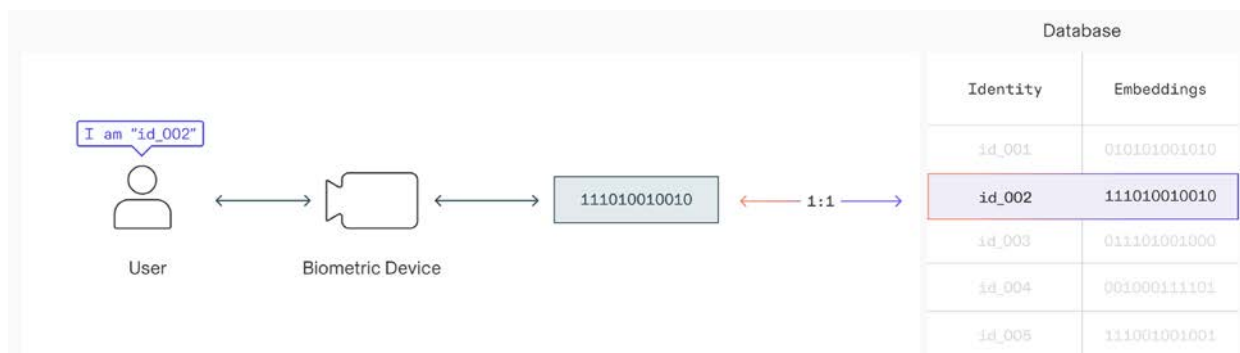


圖 3 World ID 驗證流程（圖片來源：worldcoin.org）

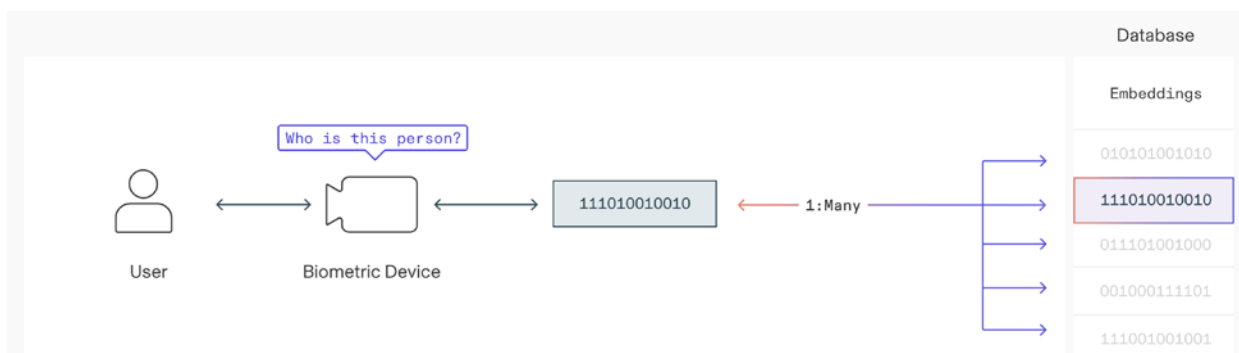


圖 4 World ID 識別流程 (圖片來源: worldcoin.org)

貨幣實現金融普惠，縱使該專案不斷強調沒有隱私問題，然而透過搜集敏感的生物資料建立身份識別的模式，仍不免讓許多政府或個人感到疑慮，並可能踩到世界各國的「數據保護法」的紅線，這可能也是 Worldcoin 團隊一開始選擇香港作為出發，而非歐美國家的原因之一。另外，虹膜儀的普及率也會影響該專案的觸及率。

不論如何，以太坊的創辦人 Vitalik 也認同透過身份驗證專案可以想像到的應用場景很多，例如在 DAO 投票、平方投票、融資、基於真實用戶的代幣空投、作為防止 Dos 攻擊的驗證替代方案、防範社群媒體中的機器人、女巫攻擊等。只是該如何避免違背去中心化的初衷，變相成為另一種第三方的中心化。

整體而言，數位證書的出現讓學歷和證書的驗證更加迅速與簡單。這使得在畢業證書等被誤用或遺失的情況下，進行認證或撤銷的流程更加方便。此外，數位徽章也作為一種身份和能力的驗證，在職業發展和終身學習中佔有越來越重要的地位。但是，除了上述的身份驗證方式外，Worldcoin 提出了一種基於虹膜掃描技術的數位身份驗證方法，使得身份驗證更加精確且難以被冒用。但這同時也引起了對隱私保護的議論，特別是在虹膜資料的收集和

使用方面。我們可以看到區塊鏈技術在身份驗證領域的應用展示了巨大的潛力，但也伴隨著許多技術和倫理的挑戰，這需要我們更加謹慎地考慮其影響和應用方式。



作者蔡孟凌現為睿科金融科技有限公司創辦人兼執行長，曾任知名外商科技業法務、臺灣加密貨幣交易所犯罪預防專員與法律顧問、法務部調查局資通安全委員、刑事司法單位教育訓練的講師，專長是協助加密貨幣金流分析與數位資產託管，並擅長橫向資源整合以共同面對 Web 3.0 的產業新革命，樂於跨領域學習並建立系統與架構。