從「幣圈」到「鏈圈」，加密貨幣意外成就區塊鏈上位

■文：任芸萍


照片人物：PUNDI X Labs 副總裁 Peko Wan

對於一個新技術或新應用來說，「創生」成敗絕對是後勢強弱關鍵！總部位於新加坡的 PUNDI X Labs 是區塊鏈 (Blockchain) 裝置的先驅開發者 (包括專用 POS 系統和區塊鏈手機 XPhone)，並為開發人員、數位資產發行人和企業創建 PUNDI X 開放交易平台及發行自有虛擬代幣。

PUNDI X Labs 一手包辦終端機、APP 和支付卡

PUNDI X Labs 副總裁 Peko Wan 認為，加密貨幣之所以尚未被大量採用可歸因於：使用者體驗差勁、確認費時與價格波動；為此，他們致力於降低交易費用、提高流動性，以吸引、留住顧客並創造有利可圖的收入來源，讓任何商店都能輕鬆加值並接受加密貨幣。透過 XPOS 終端機 (獲 FCC / CE / KC TRA 認證) 連接 XWallet APP 和 XPass 卡片，可立即與各式電子錢包連線確認；當獲得轉移許可後，便可做支付及加值。XPOS 目前已出貨至 30 多個國家，深受全球商店支持，截至今年第一季已完成 390 萬美元交易，XWallet APP 有 20 萬名使用者註冊。

Wan 指出，早期社群網路皆是集權式營運、各自為政，區塊鏈的興起將打破這些框架，改以使用者為中心。藉由 XPOS、XPASS 和 XWallet 技術，為使用者提供多種虛擬貨幣交易，換個角度，包括餐廳、咖啡館、購物中心、診所、

圖 1：使用 XPOS 對實體店進行數位化——XPASS 卡片只需輕輕一按即可交易，支援 PUNDI X 的電子錢包可以購買、支付和接受數位貨幣

資料來源：https://pundix.com/TheScopeOfBusinessOfPundixTrademark/

智能公寓、酒店和數據中心在內的任何參與商家，都可接受虛擬貨幣。XPOS 在幣圈具有中立地位，廣受 BTC、ETH、BNB、NPXS 等虛擬貨幣認可為首選代幣，但商家仍可選擇以法定貨幣進行結算；而 XPASS 是可加值所有主要虛擬貨幣的實體錢包卡片，連結 XPOS 在不到 0.5 秒的時間內就能即時完成交易。

PUNDI X 還允許客製化，經銷商可在卡片嵌入自有設計並發行專屬代幣，催生全新經濟圈。雖然目前 PUNDI X 的活動尚未經包括新加坡金融管理局 (MAS) 在內之許多司法管轄區的金融監管機構監管或許可，然而，借助全球經銷網路，PUNDI X 正迅速擴張市場。杜拜官方信貸局用以實施「全球首個公部門區塊鏈數位支付」，將 XPOS 佈建至全市數百個店面，供消費者支付帳單、學費及使用數位貨幣的公用事業費用。柬埔寨亦與新加坡智慧城市開發商 Limestone Network 合作，以 XPOS 即時分析居民生活和移動數據，期達成最佳能源生產、營造便利生活。

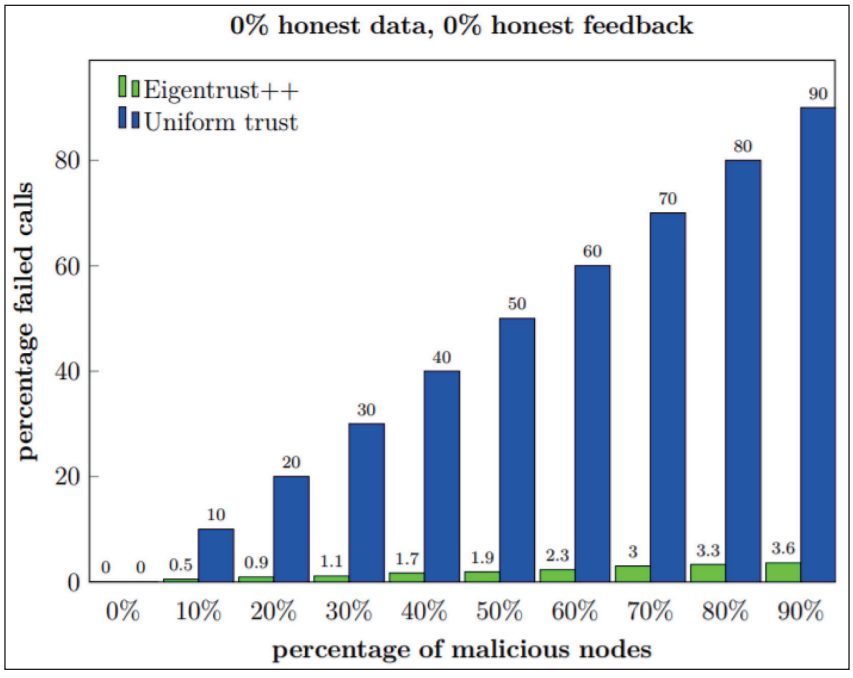
NEM 首以「聲譽系統」評比節點並倡導「重要性證明」

在網路世界，信任感是最可貴的東西，節點 (Node) 之間最怕遇到心懷不軌或拖後腿的壞鄰居，「聲譽系統」或許是個好主意，而 NEM (新經幣 NewEconomyMovement) 是採用節點聲譽措施的虛擬貨幣鼻祖。基於 Eigentrust ++ 安全叢集的演算法，可監視網路中節點的既往行為並使節點能在叢集中為其鄰居提供聲譽，以確保點對點 (P2P) 連接的可靠性並最佳化網路負載平衡。Eigentrust ++ 聲譽管理器將對等網路中的每個對等點或節點視為真實、可信、非惡意和有效；若節點順利運作，則意謂該節點受到信任且不會出現惡意進程。

最初的 Eigentrust ++ 文件建議使用額外措施來限制信任在誠實和不誠實的節點之間傳播，但如此一來，不完整的數據 (文件的一部分) 仍會被共享、而不能檢查有效性，即使誠實的節點也可能分發惡意數據。NEM 的改良作法是：能將網路中的節點始終完整下載並驗證它們，減少惡意節點存在的可能。此外，有鑑於工作證明 (PoW) 和權益證明 (PoS) 的缺失，NEM 另行提出「重要性證明」(PoI) 替代概念。上述三者皆是演算法，用於加密貨幣有助維持選擇區塊的順序，避免雙重支付 (double-spending，又稱「雙花攻擊」) 等弊端。

NEM 基金會暨 LuxTag 公司共同創辦人 Jeff McDonald 表示，「區塊鏈最令人讚嘆的突破不是你能做什麼，而是：什麼是不能做的？」例如，雙重支付就是不被允許的。那麼，PoI、PoW、PoS 究竟有何差異？PoW 是由比特幣所帶頭發起的第一個系統，欲賺取這些加密貨幣者，須使用電腦開採硬幣 (挖礦)，機器功率越大、獲得的機會就越大；如此大費周章，讓區塊鏈的攻擊成本大幅提高。然不

圖 2：NEM 增強版 Eigentrust ++ 之數據分發完整性模擬——沒有額外信任傳播措施的結果更佳



資料來源：https://nem.io/wp-content/themes/nem/files/NEM_techRef.pdf


照片人物：NEM 基金會暨 LuxTag 公司共同創辦人 Jeff McDonald

久後人們就意識到：這種挖礦動作 (將運算力用於製造新區塊的過程) 對普羅大眾而言，太過耗費時間、資源且幾乎毫無賺頭！

「智能資產系統」可快速建構並客製化區塊鏈

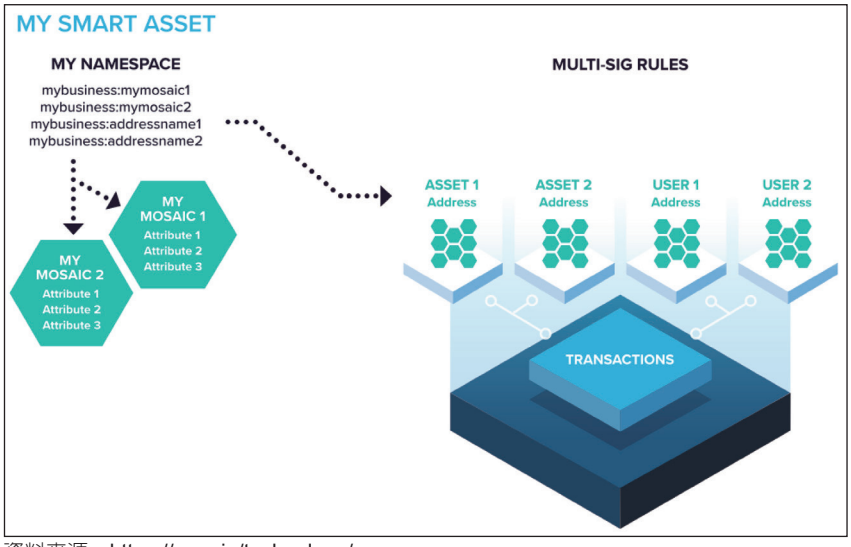
因為以 CPU 進行挖掘無法與 ASIC (專用晶片) 競爭，只會讓負擔得起昂貴 ASIC 的富人變得越來越富裕；根據 NEM 的說法，從 2014 年開始有 80% 比特幣財富是掌握在前 1% 持有者手中！於是，另一著名的加密貨幣 Peercoin 力主以 PoS，要求參與者證明他們的「所有權」或擁有多少 Peercoin。雖然改善了運算耗能，但「富者越富」的積弊卻有增無減。反觀 NEM 的 PoI 意在獎勵擁有大量帳戶餘額的人，且將與他人交易的次數及交易者納入考量，每個用戶都有一個信任分數，數值越高、所獲得獎勵的機會就越大，有助於財富分配更加均衡。

任何貢獻者都可獲得額外的 XEM (NEM 網路的貨幣)，人人皆平權。McDonald 介紹，NEM 是利用插件 (plugins) 設置區塊鏈「資料庫」，開發者可基於「智能資產系統」建構並客製化使用區塊鏈，不必從零開始編寫智能合約代碼、也不必被迫使用封閉式區塊鏈 (私有鏈) 定義資產，只要透過應用程式介面 (API) 即可訪問一組可測試、安全、開放的資料庫。他強調，「去中心化」不等同雜亂無章！統整 NEM 智能資產由四大部分組成：

1. 地址：它是智能資產的「容器」，且是唯一、可更新的單一物件，意指要遞交的包裹、房屋契約或公證文件，可在多方之間以各種方式共享所有權；
2. 固定的「馬賽克」(mosaic) 智能資產：可代表一組不變的多個相同事務，可以是簡單代幣，也可以是積分獎勵、股票份額、簽章等專業資產，每種馬賽克可包含多種屬性，如：名稱、描述、數量、可分割性、可轉移性等，可使用 NEM API 在地址之間傳遞；
3. 個性化命名空間：類似互聯網域名，可在 NEM 區塊鏈上為業務和資產定義唯一標識，以便易於使用且可信賴；
4. 交易：在地址之間傳輸馬賽克或配置所有權 (包括「多重簽名」規則)、發送消息等，NEM 區塊鏈包括一個內置共同驅動的時間維持機制，可為交易自動準確地加上時間戳記。

2015 年發佈的「馬賽克」是 NEM 最負盛名的技術——在公有鏈上，任何人都可自訂帳戶與命名空間、並發佈區塊鏈資產，為異質資產在 NEM 區塊鏈的寄存和傳輸提供有效途徑。McDonald 以 NEM 投票平台為例，它允許任何人創建和投票儲存在 NEM 區塊鏈上的民意調查，模組的數據結構有

圖 3：NEM 用於應用程式就像 RESTful JSON API 一樣簡單，允許開發者配置自己的「智能資產」並使用 NEM 區塊鏈平台作為快速、安全和可擴展的解決方案



資料來源：https://nem.io/technology/

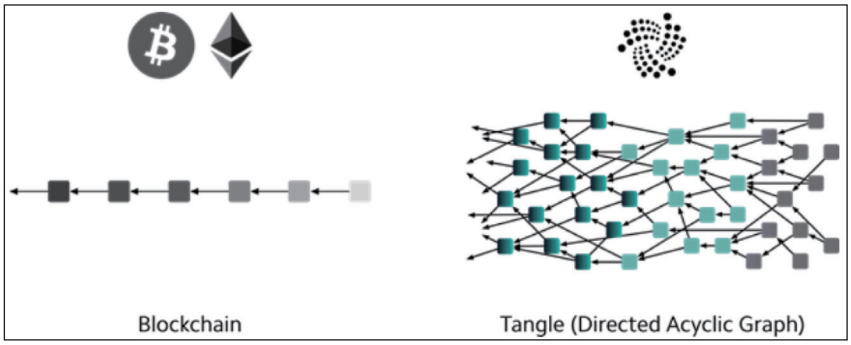
四大元素：投票指數帳戶 (PI)、民意調查帳戶 (PA)、期權帳戶 (OA) 和選民帳戶 (V)；NEM 再新增馬賽克加權投票方式，例如，企業內部投票可創建馬賽克並進行分發，甚至可向公司重要人物發送更多馬賽克，也可使用 XEM 作為馬賽克計算權益證明。

No Block、No Chain！DAG 讓 IOTA Tangle 可無限擴展

照片人物：IOTA 創辦人 Dominik Schiener

另一個正在進行概念驗證 (POC) 的專案是瞄準土地和財產登記需求的 Landstead，讓政府和公民共同創建一個開放的區塊鏈系統，供相關人士徵信和諮詢。McDonald 補充，著眼於防盜和防偽需求，他們新創的 LuxTag 公司 (https://github.com/luxtagofficial) 即致力於查核區塊鏈內容的所有權認證，確保它們是可更新、可轉移和真實可靠的。「數位世界，

圖 4：區塊鏈 (左) vs. IOTA Tangle 網路 (右) 的區別在於——圖左是順序塊鏈，每個區塊的引用皆依時間順序排列前導，包含多項事務且多以常規離散時間間隔添加；圖右以「單一事務」為單位、而非一個區塊，形成一個複雜的網狀組織 (Web) 結構，允許同時發佈交易



資料來源：https://www.iota.org/get-started/faqs

信任正在崩解中」，IOTA 創辦人 Dominik Schiener 也深感信任的不易。他直言，未來是機器對機器 (M2M) 時代，所謂的「信任」應包括：可被信賴的資料、即時交易與安全存取控制。

Schiener 舉例，惡意軟體「Mirai」(未來) 只需對互聯網開放 Telnet 通訊埠進行大範圍掃描並嘗試以預設密碼登入，就能堂而皇之主宰不安全的物聯網 (IoT) 設備、聚積殭屍網路 (botnet) 大軍，讓「受駭者」付出慘痛代價。有別於傳統加密貨幣的區塊鏈架構，2017 年底在德國柏林成立、聚焦加密貨幣和「分散式帳本技術」(Distributed Ledger Technology, DLT) 的 IOTA，採用「有向無環圖」(Directed Acyclic Graph, DAG) 原理開發名為「Tangle」(糾結) 的獨特網路——使用拓樸排序的有向圖形數據結構，非環狀、不走回頭路、不斷向前進、可無限擴展為特點。

不過，它仍跳脫不了須依賴「中心協調機制」對節點層層把關以確認交易有效性、效率不彰的宿命。為消弭技術熱衷者 vs. 夢想家，以及實用主義者 vs. 保守派 vs. 懷疑論者之間的斷層，IOTA 計劃以名為「Shimmer」的去中心化共識系統，試圖在安全性、可擴展性和去中心化三者之間取得平衡。比特幣為首的 PoW 乃利用礦機運算解決複雜的數學問題，在將挖得之新區塊向外廣播到網路前添加交易內容並永久驗證；一旦網路使用量大，會導致時間延遲和費用攀升——多數區塊鏈網路是依時間順序處理交易，若想加速驗證須支付更高的網路費用。

「Shimmer」加入聲譽排名，用最少步驟達成網路共識

再者，既有「中心協調機制」有遭受「51% 攻擊」的風險 (參閱：《沒有密碼學，就沒有比特幣》http://compotechasia.com/a/opportunity/2018/1102/40278.html 一文)。雖然有人主張改用「權益證明」(PoS) 能達到獎勵代幣／令牌持有者與提高攻擊成本的目的，

但仍無法防堵「大股東」濫權惡意製造衝突或另闢秘密通道；而IOTA新一代「Shimmer」解方是：令牌持有者可依據節點在IOTA生態系統中的表現好壞，透過投票建立聲譽排名且可隨時撤銷或重新表態。這些訊息會在所有IOTA網路節點共享、並發送至對應系統，以求用最少步驟達成網路共識。

Shimmer仿效蜜蜂、螞蟻、魚群等自發性「同步」參與集體行動，只關心非常小的節點子集意見、而非試圖重建每個節點的意見；若遇衝突，節點會迭代交換偏好、直到最終達成共識。當中節點可綜觀「Tangle」網路全局，在某些時候，節點可進一步將其決定標記為已完成，意味著它將停止參與投票且永遠不會再次偏離定案，即使有壓倒性的意見變動也不例外，可有效抵禦惡意攻擊造成「翻盤」。節點會拒絕同時「更喜歡」兩個衝突子細胞的投票，違反規則的劈腿節點可能會被忽略並遭永久刪除。細究操作手法有「細胞共識」與「快速概率共識」兩種。

前者只需五行代碼就能實現一致性演算法，增加節點數雖會影響網路傳播時間、但不會影響達成共識的時間。無論有多少節點參與，決策都是在本地並行，而結合聲譽能增加安全性；惟很難用數學方法建模是最大缺點。因此，IOTA一改鄰居異步投票，將投票過程分為不同輪次；在每一輪中，每個節點會選擇其他節點的新隨機子集並徵詢當前意見，再根據多數回饋意見形成節點意見、從隨機數序列得出決策閾值，而非50%固定閾值，為想要推遲達成共識的攻擊增添難度。「Shimmer」還將此共識機制模組化，使作業更靈活、也更方便日後創新或升級。CTA

圖5：「Shimmer」旨在讓網路節點自主、「有機地」形成共識

資料來源：https://coordicide.iota.org/module5.1