區塊鏈可望成爲 IoT 落地的突破口

■文：任芷萍


照片人物：BiiLabs 共同創辦人暨技術長黃敬群

台灣已有奉行 IOTA Tangle「有向無環圖」(Directed Acyclic Graph, DAG) 的新創團隊出現。2017 年成立的 BiiLabs，主攻智能合約引擎的「分散式帳本技術」(Distributed Ledger Technology, DLT) 開發——它們只是簡單的常規法律合約，條款會被儲存在分散式帳本、且可被機器讀取及自動驗證。共同創辦人暨技術長黃敬群表示，他們成員從事物聯網 (IoT) 嵌入式系統的軟、硬體開發多年，發現缺乏新技術很難催生新的經濟活動，而區塊鏈 (Blockchain) 將是一個新的切入點。例如，將家戶用電數據賣給物流公司，以便依據用電狀況判斷收貨人是否在家。

為何以往做不到？黃敬群認為主要受限於取得成本太高所致，而資料也不能保證不會被竄改。因此，BiiLabs 多方參與開放原始碼等國際組織，基於 DLT 區塊鏈架構、以人為本投入去中心化識別工作，之後再逐步擴展至人與機器、機器與機器應用；追隨領導廠商腳步、從團隊多年累積人脈著手，以保險、能源、電子憑證為敲門磚，提供包括數位身份證、分類帳和結算、小額支付、數位取證等在內的沙盒測試服務，亦有能力包裝成客製化的應用程式介面 (API) 和閘道器 (Gateway) 裝置，並將實作成果開放出來。

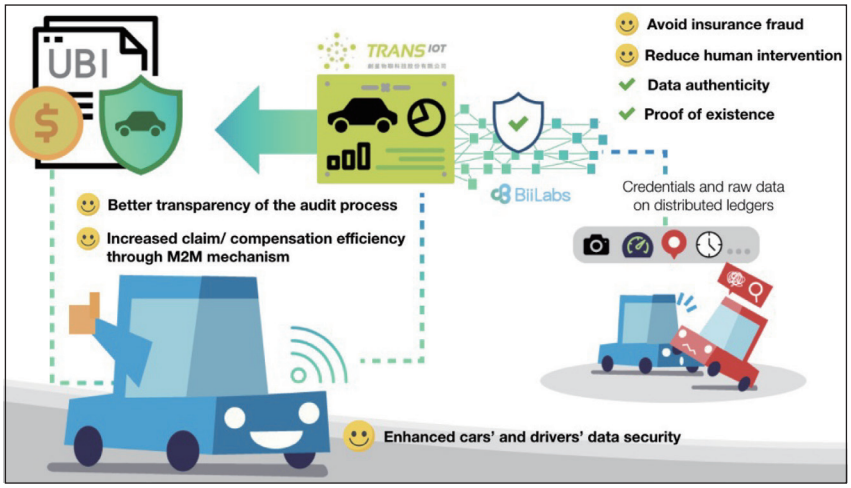
「幣圈」投機氣氛盛，「鏈圈」應用才是長久之道

借助 DLT 記錄微交易／奈米交易，並為開發者提供創新的物聯網應用工具，為市場提供各式電動產品或運算資源的租賃服務，亦協助企業和政府通過 DLT 監控水質數據。本身也是知名 Linux 核心開發高手的黃敬群指出，區塊鏈已存在超過十年，是承襲密碼學、網路、資料庫等脈絡而來，當中許多專利已過期，也意味著足夠成熟，設法將其整合、開創新的經濟活動是今後必須思考的方向。當這些元素全數到位，現在就是發展區塊鏈最好的時機。他坦言，當下區塊鏈應用以交易所和幣圈投機為大宗，但其餘看似小眾的利基市場才是更長遠的議題。

黃敬群提到，尤其歐盟《通用資料保護法規》(GDPR) 的實施極具正面助益，促使 IP 和看待資訊結構的方式發生改變，對於資料交付流向、副本存續時限及被遺忘權的關注正式浮上檯面。「資料的建立與轉移皆有貨幣價值，一旦去識別化，存在區塊鏈上的資料就只是憑證，且可供追溯」，他舉例，依使用量調整費用的 UBI 保險 (駕駛行為計費) 雖立意良善，但卻有資料難以使用且不被信任的疑慮。如何將車載診斷系統 (OBD) 資料交付保險公司或數據分析機構？是否經過變造？其間資料流並非單向，怎麼進行第三方監管或解析、又不會「侵犯」到原始資源？

每一層，都是設計思維上的關卡。導入區塊鏈技術或是解方，因為每筆資料都能被追蹤，借助

圖 1：BiiLabs 正在將區塊鏈技術推向 UBI 保險，具備存在證明和數據真實性避免保險詐欺並減少人為干預。



資料來源：https://biilabs.io/#

網路通訊還能實施「零知識證明」(zero-knowledge proofs)——不用看到本人就能清楚他的某些特質或屬性。如此可自源頭建立信任，確保從電子、電機底層通訊開始的一連串原始資料格式，以及資訊載具的身份識別皆是可信，以建立「信任根」(Root of Trust, RoT) 經濟模型。一個設想的應用情境是：菸酒銷售商判斷消費者是否成年？黃敬群主張，領域知識是如何建立商模邏輯的關鍵，而當中傳遞的數據即是數位資產，須秉持「最小資訊揭露權」原則。

P2P 網路可有效降低成本和資料傳輸延遲

它們要能被交換、識別，但不應揭露過多個人資訊，據悉 W3C CCG (Credentials Community Group，認證社群團體) 已擬於明年針對「去中心化身份識別」推出相關規範。藉著 BiiLabs 今年出席《AWS Summit Taipei 年度高峰會》的場合，黃敬群也談到區塊鏈與雲端服務的連結。由於各種憑證的讀寫頻繁度不同，例如：保單屬於寫多讀少、但畢業證書等資格文件卻是讀多寫少，若以傳統計價方式會失去彈性，點對點 (P2P) 網路可有效降低成本和資料傳輸延遲。目前已有很多節點 (Node) 是建構在雲端主機上，長期而言也是必然走向。

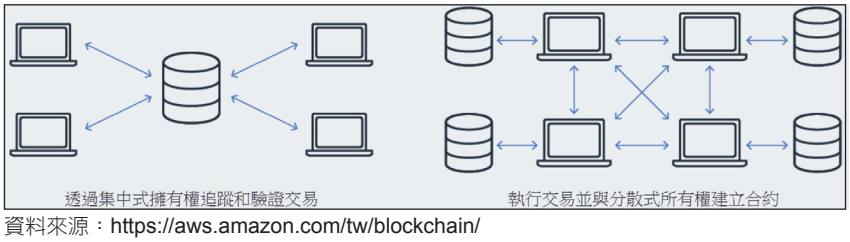
「差別在於：不同規模需要不同的雲端基礎建設支持以建立最適邏輯」，黃敬群說。雲端服務業者亞馬遜 AWS 觀察，區塊鏈技術通常用於解決兩種類型的客戶需求，並推出用於建立可擴展區塊鏈網路和總帳應用程式，進而締結智能合約和交易，且 AWS 對於資料落地與區域性法規已有妥善處理。第一種是「集中式」，透過受信任的授權單位完整維護可驗證的交易記錄，例如，某位零售商客戶可經由集中式總帳與供應商建立聯繫，維護產品動態及歷史資訊。一般而言，實作總帳應用程式通常是利用關聯式資料庫中建立的自訂稽核表或稽核追蹤。

這種舊式實作需自訂開發，非常耗時、容易出現人為錯誤，且關聯式資料庫本身並非固定不變，難以追蹤、驗證資料的意外變更 AWS 名為 QLDB (Quantum Ledger Database) 的「總帳資料庫」全託管服務可為授權單位記錄經濟和財務活動歷史，提供透明、不可變、以密碼編譯驗證的交易日誌，追蹤單一及所有應用程式的資料變更，並於一段時間內維護完整且可驗證的變更記錄，無須實作建立複雜的稽核表或設定區塊鏈網路；另無伺服器 (Serverless) 的強項是可自動擴展支援程式需求，無須管理或設定讀寫限制，僅需按實際用量付費。

AWS 全託管區塊鏈服務上架，公有鏈、私有鏈須視情況而定

雖然坊間 Hyperledger Fabric

圖 2：集中式 vs. 分散式區塊鏈連結形態



資料來源：https://aws.amazon.com/tw/blockchain/

(超級帳本) 和 Ethereum (以太坊) 等區塊鏈架構也可當作總帳使用，但需設定包括多個節點的整個區塊鏈網路、管理相關基礎設施，且節點須事先對每筆交易進行驗證才能歸戶至總帳，複雜度較高。Amazon QLDB 的好處是：為開發者提供熟悉且與 SQL 類似的 API、靈活的文件資料模型及完整的交易支援。第二種是「分散式」，例如，銀行財團和出口公司希望相互之間執行信用狀等跨境資產轉移，無須作為聯絡人的中央授權單位，AWS 亦有「Amazon Managed Blockchain」可擴展的全託管區塊鏈服務備選。

開發者可使用常見的開放原始碼架構 Hyperledger Fabric 和 Ethereum (即將推出) 輕鬆建立、管理可擴展的區塊鏈網路，省去建立網路的開銷並自動擴展，以因應執行百萬筆交易之數千個應用程式所需。待網路建立妥當並執行後，也易於管理和維護。藉由憑證管理，使用者可輕鬆邀請新成員加入區塊鏈網路並追蹤操作指標，如：運算使用量、記憶體和儲存資源。當問到私有鏈 (Private Blockchain) 是否會因節點太少而不實用？黃敬群的看法是：不能單一論之，要視應用定位、功能屬性和營運成本而定，例如，單向讀取的數位憑證只需兩個節點就夠。

另一個質疑是：標榜「去中心化」的區塊鏈要大力拓展，恐免不了大卡司領頭、無形中又趨於集中的自相矛盾 (參閱：《從幣圈入 Dao，區塊鏈格局大不同！》一文 http://compotechasia.com/a/feature/2018/0716/39418.html)，導致企業傾向觀望；黃敬群的解決之道是：為企業創造動機和誘因。BiiLabs 共同創辦人與執行長朱宜振補充，早期投入者或許無法守得雲開見月明，所以，不少台灣企業素來習慣做「快老二」——待風向已定再全速急起直追；然而，趨勢一旦形成就不易改變，新創的價值就是勇於嘗試，不是嗎？

表：集中式所有權總帳 vs. 分散式所有權區塊鏈網路

具有中央所有權的總帳功能	具有分散所有權的區塊鏈網路功能
集中式 集中式、受信任的授權單位擁有並管理總帳，且與相互合作的任何方分享	分散式 多方可以彼此進行交易，不必互相了解或彼此信任。各方即成員擁有網路中的對等節點
不可變 使用僅附加日誌，其將每一項交易儲存至區塊中。區塊以密碼編譯方式連結在序列中，且中央擁有者或任何其他實體均無法刪除或修改。	不可變 進行的交易儲存於區塊中，並以密碼編譯方式連結在一起且無法修改。交易進行後，它會在所有成員中重複，因此無法變更或刪除。
可驗證 使用密碼建立變更歷史記錄的簡潔摘要。此安全摘要也稱為摘要檔，可用於以密碼編譯方式驗證總帳中的資料歷程。	可驗證 每位成員儲存一份本機總帳副本，可獨立驗證並確保總帳內容準確無誤。若做出任何變更，網路中的成員需要驗證新的交易，確保所有對等交易中的資料保持一致
透明 整個資料歷史記錄可輕鬆查詢，提供完整、透明的資訊日誌。	透明 所有進行的交易都歸屬於一或多個實體，提供完整、透明的資訊給所有成員。許可的區塊鏈架構，例如 Hyperledger Fabric，透明度可設定為僅指定的對等群組可存取資訊。
快速 集中式、受信任的總帳不需要執行分散式一致性，允許其輕鬆擴展並執行交易，相比常見區塊鏈架構中的總帳更快捷。	移除中繼點 每個對等組織可使用編碼應用程式邏輯開始新的交易。交易開始後，它會在網路中的所有對等間重複，允許多方存取並驗證該資訊。無須中繼點用作成員間的聯絡人，使複雜的交易更高效、更實惠。

資料來源：https://aws.amazon.com/tw/blockchain/

「六域鏈聯盟」制訂全球首個 IoT + Blockchain 國際標準

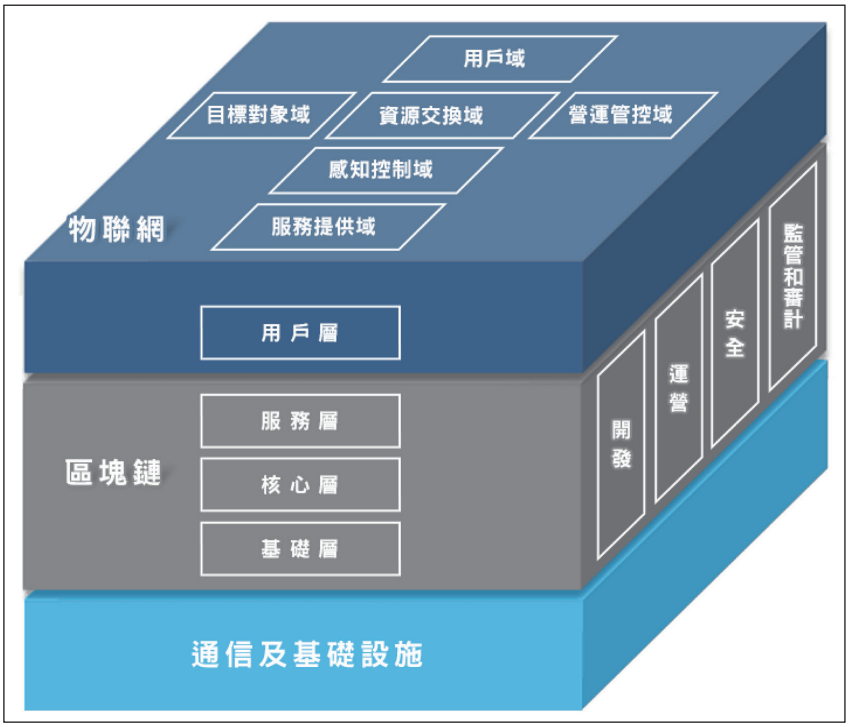
同樣押寶物聯網＋區塊鏈雙效合一，加拿大非營利組織「六域鏈聯盟」(SDChain Alliance) 更率先為兩者建立融合框架、制訂全球首個國際標準 ISO / IEC 30141；其技術商轉的「鏈圈」新創公司——台灣六域鏈 (SDChain IoT)，於去年中正式推出商業激勵模式的公有鏈服務，以企業用戶市場為核心，開發區塊鏈產品並部署全球代理商通路。乍看之下，總不免令人對其命名感到好奇；根據官方說法，所謂的六域包括：感知控制、目標對象、維運管控、資源交換、服務提供及用戶域，矢志成為創造物聯網資料價值的啓動者。那麼，為何有此一說？

SDChain IoT 強調，物聯網應用的高併發性和高度差異化特性，使區塊鏈的「共識機制」不能直接延續以發行數位貨幣為主、缺乏實際應用的現有區塊鏈共識演算法；於是，他們提出 SDFT (Six-Domain Fault Tolerance，六域容錯) 演算法，融合高度一致性的 RAFT(資源聚合容錯) 及高併發性的 PBFT (實用拜占庭容錯) 兩種共識演算法，同時滿足安全性、高性能及信任性。此外，為平衡大量物聯網的接入請求負載，SDFT 採取分層架構系統，將節點區分成主節點 (Master Node) 和驗證用節點

(Validate Node) 兩大類。

前者可以有一個或多個，由改進的 RAFT 演算法投票產生，依據交易記帳成功率賦予權重以平衡用戶端的訪問請求負載，或作為驗證伺服器與外部網路之間的代理人；後者為一般驗證節點，採用改進後的 PBFT 演算法，增加帳本的堅固性和網路公正性，節點數量無上限。特別一提的是，考慮到物聯網應用場景的高併發性及高業務量，加上許多應用的設備客戶都是按照代理模式批次性接入，故在一般共識激勵的基礎上設置「Charge 模式」，以實現運行客戶代理的節點分享、底層共識和節點激勵收益，以兼顧業務和共識。

圖 3：SDChain 六域架構，期許全面保護物聯網的信用體系和價值體系



資料來源：http://sdchain-iot.com/whySdchain.html

國際發聲，搶產業標準話語權

誠如 SDChain IoT 點評，應用服務提供商正面臨一些重大挑戰：在各種生態系統之間建立業務夥伴關係、在多個實體之間協調數據，並為這些數據建立信用和價值傳遞，區塊鏈將是最佳解；而他們的應用案例已拓展至漁業水產品溯源、農業生產履歷、醫療器具流向追蹤與知識產權／版權歸屬。統整 SDChain 的優勢在於：綜合多方考量的共識機制、原生支援多資產和資產交易、系統資源運用更有效，這或許就是他們能一馬當先、成功在國際發聲的原因；從自身人脈創建生態固然是新創出線的好方法，但若能在產業標準取得話語權，將更如虎添翼。CTA

圖 4：SDChain vs. 同業之技術路線比較

技術路線	比特幣	以太坊	超級帳本	SDChain
共識機制	POW	POW+POS	插件式	改進 PBFT
多資產	不支援	合約方式	合約方式	原生支援
資產交易	不支援	合約方式	合約方式	原生支援
智能合約	不支援	支援	支援	支援
系統性能	很弱	很弱	好	很好
節點數量	很多	較多	沒有公鏈	較多

資料來源：http://sdchain-iot.com/aboutSDChain.html