# 善用「混合鏈」應用 加速金融革新

台灣雲端物聯網產業協會秘書長/闕志克

何謂區塊鏈？簡單來說，就是去中心化的資料庫。值得注意的是，在區塊鏈的設計中，所謂的帳簿管理人，分散在世界各地，不用記名，彼此也互不相識，且對帳簿管理也沒有所謂的權利和義務，在這麼分散的管理機制下，如何確保帳簿的交易資料不會被竄改，也不致發生雙重支付（double spending）的情事，是件很困難的事。

在形成區塊鏈中有二個機制很重要，第一個機制就是獎勵，就是要給花很多時間和電力去「驗證系統」(proof-of-work)的挖礦者足夠的誘因，才能誘使挖礦者源源不絕地投入挖礦，而區塊鏈中的獎勵指的就是比特幣，另一個機制則是民主表決（voting），儘管多數的區塊鏈都朝線性發展，但有時也會出現分枝，這種狀況在區塊鏈中是被允許的，不過，分枝的狀況一般不會持續太久，因為時間一拉長，挖礦者就會往多數的方向聚集，因為在挖礦的過程中，愈多人去算，就能夠愈早解謎，愈有可能贏，而這就是區塊鏈中所謂的民主表決（voting）。一般來說，一個新的區塊如果後面可以順利再接上二個區塊，就意味著這個新區塊已獲得確認，而在區塊鏈形成的過程中，到底接下來哪一個區塊才是正主？全憑挖礦者的自由意志決定，也就是說區塊鏈的形成每一個步驟都是透過挖礦者民主表決的結果。

區塊鏈被視為啟動金融產業變革的金鑰，近年在金融領域應用形態也會愈來愈多元，除了公有鏈、私有鏈外，「混合鏈」也將應運而生。

「公有鏈」指的是全世界任何人可進行讀取、並隨意發送交易資料，一切運作端賴信任機制運行的區塊鏈，但因經過很多關卡，效能較差，比如現行的比特幣採行的就是公有鏈；「私有鏈」只限定特定個人可參與，由於成員參與前已通過身分認證，交易時可免除認證的繁複手續，資訊處理速度相對較快；缺點是不夠開放，信任機制就沒公有鏈高。然對特定產業來說，例如銀行產業就偏好私有鏈。

公有鏈和私有鏈各有利弊，未來兩者界限會更加模糊，不再是所有節點都擁有一樣的權限；而是針對不同的節點做不同的分工，以致部分節點只能查看部分區塊鏈數據，僅有小部分節點可下載完整區塊鏈數據，成為整合兩者優勢的「混合鏈」應運而生。

「混合鏈」既可讓所有人保有資料私密性，又可透過資訊整合，產生綜效，也是工研院當前研究的重要方向，將幫助產業找出更多的應用機會。

目前區塊鏈最大的考驗在於處理效能太慢，完成每筆帳本紀錄需要經過好幾道流程，以致區塊鏈存放資料的速度過於緩慢，每筆資料要更新時，遠比傳統資料庫要慢約一千倍。

其次，區塊鏈的資料正確性也存在著盲點。雖然區塊鏈可以靠著數學演算法驗證資訊的正確性，確保寫入的資料日後不會遭到竄改，但卻無法驗證一開始輸入的資料是否都正確無誤，這既是技術的優點，也同是缺點。儘管現階段區塊鏈實質應用仍不多見，如何透過區塊鏈加速金融業的革新？甚至帶動其他產業的創新應用，則是產、官、學、研各界的共同目標。

(本文亦刊登於聯合報財經觀點專欄)