比特幣把中央銀行變不見了！

區塊鏈應用的挑戰與機會

中央銀行的機制已存在世界上846年，你曾想過這個已經存活8個世紀的銀行、也有派不上用場的一天嗎？而區塊鏈的存在，證明這一天極有可能到來。

撰文／陳愛君

什麼是區塊鏈？工研院資訊與通訊研究所所長闕志克表示，簡單來說，區塊鏈就是去中心化的資料庫。在區塊鏈的設計中，帳簿管理人分散在世界各地，不用記名，對帳簿管理也沒有所謂的權利和義務，如此分散的管理機制，如何確保帳簿的交易資料不被竄改，也不致發生雙重支付（Double Spending），是件相當困難的事。

客戶、挖礦者與參與者是區塊鏈靈魂人物

在區塊鏈裡存在三個靈魂人物，第一個是專門產生交易記錄的人——客戶（Client），其次是現在最紅的挖礦者（Miner），負責將資料庫的交易記錄以事先設定好的欄位與格式儲存起來，並使用「條件雜湊（Conditional hash）」，計算出小於困難指數（Difficulty）的雜湊值（Hash value），所有的挖礦者比賽誰先算出雜湊值，只要先算出雜湊值就可得到區塊鏈獎勵——比特幣。挖礦者找到新區塊的雜湊值後，就可以數值送交給參與者（Participants）來驗證，以維護區塊鏈的正確性。

為了讓所有的區塊串起來，挖礦者算出新區塊的內涵還不夠，新算出來雜湊值的內涵，必須隱含上一個區塊的雜湊值，這樣才有可能將所有的區塊全都串起來，形成真正的區塊鏈。一旦有人想修改某個區塊內容，其他區塊也須同步異動，使得更改區塊鏈上的任一個內容，變得極為困難。

獎勵與表決機制推進區塊鏈發展

形成區塊鏈中有二個重要機制，第一是獎勵，提供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，才能促使挖礦者持續投入挖礦，這誘因就是比特幣；另一個機制是民主表決（Voting）。闕志克強調，儘管多數的區塊鏈都朝線性發展，但有時也會出現分枝，不過分枝一般不會持續太久，時間一拉長，挖礦者就會往多數

隨著區塊鏈應用逐漸成熟，區塊鏈的型態也愈來愈多元，除了公有鏈、私有鏈外，混合鏈也會應運而生。

工研院資訊與通訊研究所所長 闕志克

的方向聚集，因為在挖礦過程中，愈多人去算就能夠愈早解謎，愈有可能贏。一般來說，一個新的區塊如果後面可以順利再接上兩個區塊，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挖礦者民主表決的結果。

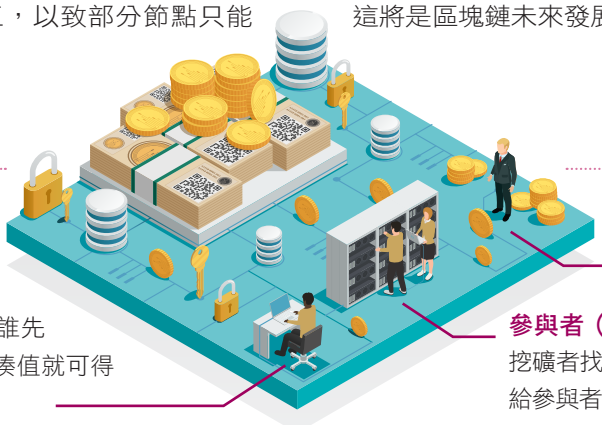
闕志克預言，隨著區塊鏈應用逐漸成熟，區塊鏈的型態也愈來愈多元，除了公有鏈、私有鏈外，混合鏈也會應運而生。所謂公有鏈，指的是任何人都進行讀取、並隨意發送交易資料，一切運作端賴信任機制運行，不過因為從交易完成到交易紀錄被存取必須經過很多關卡，較不具效率，現行的比特幣採行的就是公有鏈。而私有鏈則全然相反，限定特定個人可以參與，私有鏈的成員在參與前就已經通過身分認證，所以在交易時就可以免除掉一些認證手續，資訊處理速度相對較快，不過缺點是不夠開放。

未來公、私有鏈之間的界限也會愈來愈模糊，不再是所有節點都擁有一樣的權限，而會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，僅有小部分的節點可以下載完整的區塊鏈數據，進而產生全新的混合鏈。

闕志克舉例，如果有5個人各自享擁有不同資料來源，卻不想對外分享內容，但如果可以將5個人的資料整合形成混合鏈，就能產生全新的經濟效益，此時可以透過第三方安全精算（Secure Multi Party Computation）機制，既可以讓所有人保有資料的私密性，又可以透過資訊整合產生綜效，這種「所有權保留的合併（Ownership-preserving Data Amalgamation）是工研院現正研究的新模式。

區塊鏈目前最大的考驗就是處理效能太慢，因為要完成每筆帳本記錄需要經過好幾道流程，以致存放資料的速度，遠比傳統資料庫要慢上許多。另一個問題是挖礦者必須花費很多時間和電力去做驗證系統，並不環保。

再者，區塊鏈的資料正確性（Data Veracity）也存在著盲點。闕志克指出，雖然可以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，但無法驗證一開始輸入的資料是否正確，而這將是區塊鏈未來發展可能會面臨的阻礙。■



挖礦者（Miner）
將資料庫的交易紀錄以事先設定好的欄位與格式儲存起來，所有的挖礦者比賽誰先算出雜湊值，只要先算出雜湊值就可得到區塊鏈獎勵——比特幣。

客戶（Client）
專門產生交易記錄的人。

參與者（Participants）
挖礦者找到新區塊的雜湊值後，將數值送交給參與者驗證，以維護區塊鏈的正確性。