【專題一】

區塊鏈發展趨勢

楊英伸（證交所專員）

壹、前言

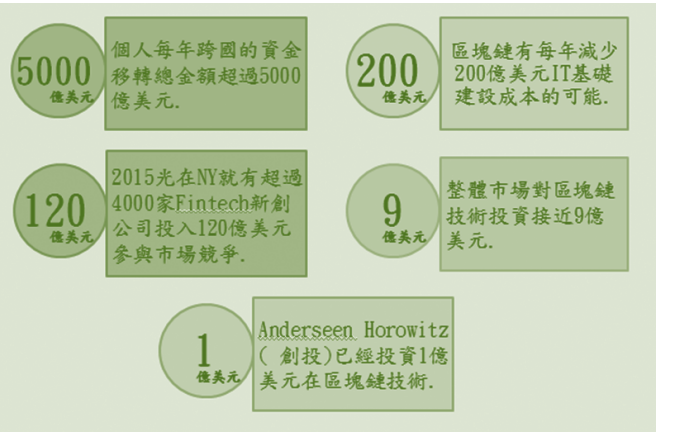
當中本聰於 2009 年基於前一年發表的理論基礎，釋出初版比特幣（Bitcoin）開放原始碼系統後，全球逐漸陷入了挖礦和爭論貨幣定位的狂熱，而當這股狂熱逐漸平息之餘，比特幣系統用以驗證資訊有效性和鏈成各個效性資訊的元件—區塊鏈（Blockchain）—卻成為研究與發展金融科技（FinTech）的顯學之一。

貳、全球競相研究以區塊鏈技術為核心的金融系統

以交易所及政府機關為例，納斯達克於 2015 年 10 月正式發佈用於私募股權市場的區塊鏈系統「Linq」，並在今（2016）年初宣佈愛沙尼亞塔林證券交易所的股東電子投票系統將基於區塊鏈技術進行研發；日本交易所於今年發表由 IBM、Intel、Cisco、倫敦交易所、JP Morgan、Wells Fargo 及 State Street 共同參與研發的區塊鏈專案；澳洲證券交易所於今年 2 月成為全球第一個將區塊鏈技術運用於證券結算交割系統的交易所；德國交易所不但參與區塊鏈公司 Digital Asset Holding 的融資案，也已著手將區塊鏈技術運用至證券交易業務中；歐洲央行更於今年 2 月份的報告中提及如何將區塊鏈技術應

用在歐盟的證券支付與結算系統中。

而在私人機構方面，由德國交易所、澳洲交易所、芝加哥商業交易所、荷蘭銀行、法國巴黎銀行、IBM 等金融及資訊公司投資的 Digital Asset Holdings，也針對貸款及結算交割等業務的區塊鏈系統進行研發及測試；JP Morgan 則邀請 2200 名客戶參與有關倫敦與東京間外幣匯款的區塊鏈系統測試；瑞穗金融集團著重區塊鏈技術於交易紀錄的安全機制；IBM 則與倫敦證交所及日本證交所合作，共同研討如何將區塊鏈技術帶入股票交易系統中；以協助各銀行發展區塊鏈技術為宗旨，R3 國際集團更是促成全球 45 個銀行共同合作。



圖表 1　2015 年全球區塊鏈的參與投入狀況

參、區塊鏈如何成為金融科技最受倚重的發展技術

為何區塊鏈技術能在金融科技的發展中佔有一席之地，得由其 4 大特性—密碼學機制、分散式帳本、共識決演算法及智慧合約談起：

一、密碼學機制（Cryptography）：

在比特幣理論中，每當交易產生時，都須要原本的擁有者進行數位簽章核准這筆交易，驗證中的交易資料會被打包至區塊中，並透過雜湊演算法進行記錄。數位簽章讓交易產生了不可否認性，雜湊演算法則提升了交易的偽造難度，也奠定了區塊鏈的安全基礎。

二、分散式帳本（Distiduted Ledgers）：

區塊鏈將所有的交易紀錄存放在多個節點，去中心化的資料留存方式讓買賣雙方得以隨時追溯交易歷史，提升資訊透明度，降低偽幣流通的風險。因此在區塊鏈的環境下，交易一旦驗證確認完成後，數據篡改的難度和代價將會相對龐大，資料更動的權限也不受單一組織控制，提升交易資料的可信任度。

三、共識決演算法（Consensus Algorithm）：

在集中式的管理環境中，交易的正確性皆由中央控管單位負責，而在分散式帳本的去中心化環境下，區塊鏈讓每個擁有交易紀錄的節點，以多數決的方式取得資料正確性的共識。共識決機制牽涉到每個節點的存放資料，就結果而言降低了中央控管單位因資安事故導致金融詐欺事件的風險。

四、智慧合約（Smart Contracts）：

結合了不可否認性、高資訊偽造難度、高資料可信任度及低詐欺風險等基礎特性後，買賣雙方甚至得以在這樣的交易環境中，預先設定好合約執行的條件，並將相關資訊儲存於區塊鏈中，並藉由電腦程式以全自動化方式進行驗證，判斷是否執行合約內容。

彙整區塊鏈特性後可以發現，區塊鏈的特性提供了讓買賣雙方在互不信任，且不存在中央控管單位的情況下，可以互相協作的資訊安全機制。英國經濟學人雜誌也因為這些區塊鏈天生帶有的特性，認為區塊鏈機制身為比特幣交易機制的其中一個元件，其價值遠遠超出比特幣帶來的效益，並稱區塊鏈是台「創造信任的機器」，這也成了引爆金融及資訊產業瘋狂投入研究區塊鏈技術應用的熱潮主因。

圖表 2　區塊鏈可應用的領域

肆、區塊鏈技術發展的隱憂

但在這股熱潮下，顧能公司（Gartner）在分析近年金融科技及區塊鏈技術的發展脈絡後，則認為區塊鏈技術正處在媒體及網路曝光的顛峰，但其應用可能尚未達到同等高度，呼籲現階段研究及採用區塊鏈技術的組織，要做好現有技術在未來 1 至 2 年內就會完全汰換的心理準備。這個呼籲隱含的當然是對區塊鏈技術的擔憂，而要細探這股擔憂，或許可由技術及治理兩方面來推敲。

一、技術面的瓶頸

在技術層面上，以證交所為例，為提高交易效率及增加市場流動性，證交所已於 2014 年 12 月將競價撮合循環秒數由現行的 10 秒調整至 5 秒，並持續推動逐筆撮合與國際制度逐步接軌。然而，以加密機制為基礎的區塊鏈技術，早期的比特幣案例完成一筆交易結算花費的平均時間為 10 分鐘，一天累積的交易量僅有 30 萬筆；而以目前國內台大金融科技暨區塊鏈中心研發的 G-coin 系統，每 15 秒就能形成一個區塊來看，仍無法滿足證券交易對於低延遲性的高頻交易需求。

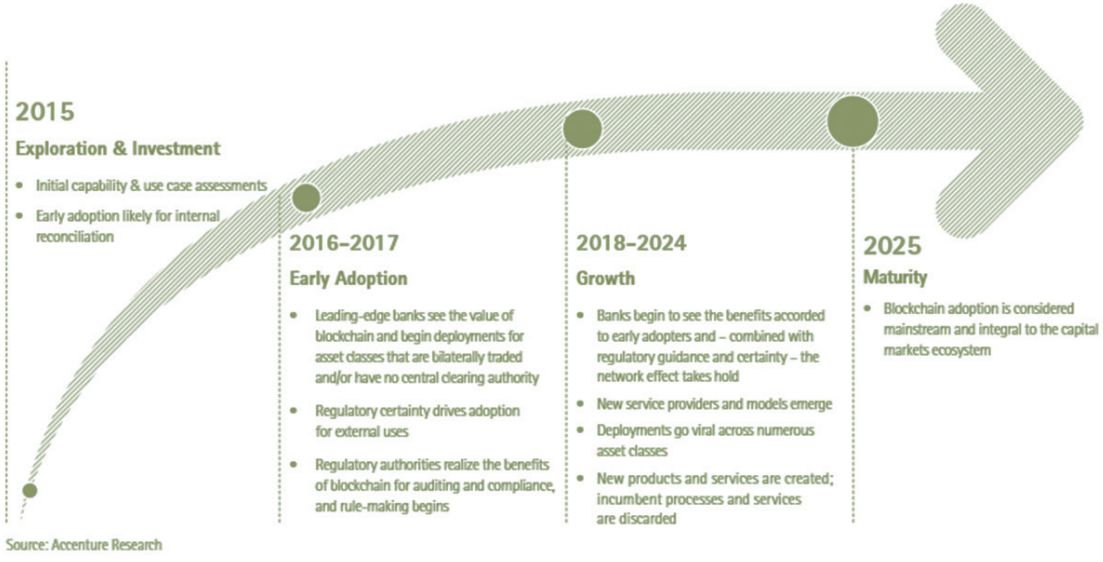
在資料傳輸面上，證交所與證券商透過交易網路專線進行資料傳輸，以確保交易資料的可靠性和正確性，目前每日的委託量約 1 千萬筆上下，套用區塊鏈的分散式共享帳本架構，龐大的交易資料量可能會造成傳輸量太大，使網路傳輸在日常營運時產生無法負荷的風險。

將視野放諸國際，為了能使區塊鏈技術應用於金融產業，相關實作已經從極端的完全開放自由的作業環境（公開區塊鏈），逐漸的朝向適度控管的環境（私有區塊鏈），這樣的演變恰恰說明了全球對此議題仍在尋求最佳實務運作，例如 IBM 知名的私有區塊鏈平台 Hyperledger 逐漸朝向實名制的憑證管理機制架構發展。另外如 I/O Digital、Sho Card 等公司則尋求提供依客戶的申請文件與識別資料掃描後產生公私鑰以使用於區塊鏈系統的服務，這樣持續出現的新型應用可以證明區塊鏈熱潮仍在蔓延，但也是全球仍在尋找最佳應用的闡述。

二、治理面的衝擊

然而，即使區塊鏈的「密碼學機制」與「共識決演算法」等特色導致了交易在有管理面需求時，執行取消、修改及調整交易紀錄等作業的難度，技術層面的問題終究能藉由研究分析及應用經驗的累積加以突破，但如何讓區塊鏈技術與現有的金融體系接軌，確保金融體系的治理運作，恐怕將會是更令人傷神的問題。

管理顧問公司 Oliver Wyman 及歐洲清算銀行 EuroClear 於 2016 年 2 月間共同提出的報告中提到，區塊鏈中的第一個區塊包含了金融交易細節，用於驗證訊息的有效性，並生成下一個區塊，這種「實際上一個區塊就包含全體資料」的數據，套用現今主流的集中保管機制，或許可以透過擴大解釋集中保管結算所的角色來完成治理面的協商，但這並非區塊鏈技術與既有金融治理面唯一的角力。區塊鏈技術的「分散式帳本」特色，讓採用區塊鏈技術的系統天生便具有將資料分散到所有資料儲存節點上的特性，然而許多國家都有相關的法令，要求資料數據必須實際存放在該國，這些法令與區塊鏈的天性背道而馳，在實際應用上限制了區塊鏈系統將資料散佈到世界各地驗證的能力，也等於扼止了區塊鏈系統的優勢。



圖表 3　Accenture 研究報告指出區塊鏈技術的應用仍須要 10 年左右的時間熟成

因此，不論是要將區塊鏈技術作為市場基礎設施的一部分，或是建構一套國際共通的遵循標準，都須要一套新的監管原則進行管理。目前集中保管結算的體系仍是大多數市場的標準，也是交易最終被確認，及款券交割的地方，但假設這樣的系統要納入區塊鏈技術，結算最終性（Finality of Settlement）的法律定義甚至需要被重新解讀或是修改。另外，區塊鏈將資料分散到系統各個節點，並透過共識決機制議定資料效性的機制，因此在講究資料一致性的金融系統中，便須要釐清或重新定義維持一致性的權責單位。更進一步思考，由於區塊鏈系統的不可否認性，當產生交易爭議或法律判決需介入時，可能會產生監管機關無法接受的系統性問題。

伍、結論

區塊鏈技術是劃時代的金融創新技術，讓記帳從原先的集中式管理轉化為分散式網路信任機制，達成去中心化的運作。因此現今的金融機構，多著墨於以破壞式的重新思考方式，摸索如何因應區塊鏈技術的發展。臺灣證券交易所目前為因應區塊鏈技術之發展，已成立專案小組，持續觀察各國交易所對於區塊鏈技術之應用及審慎評估，於適當時機推廣此項技術應用於我國證券市場，盼我國證券市場透過金融創新與世界接軌，現階段臺灣證券交易所或相關周邊單位不會因區塊鏈之發展而逐漸失去市場中介者之功能與角色，反之，將協助臺灣證券市場觀察區塊鏈技術的成熟度，在共同標準、系統可擴展性及監管制度逐漸成熟時，帶領證券市場預為因應。