台北外匯市場發展基金會委託計畫

金融科技(區塊鏈)
對金融服務業之影響

研究人員*：陳珮為、王梓彥

日期： 中華民國一〇七年十二月

*中央銀行外匯局研究人員感謝任職單位長官與委託單位的指正與建議，本研究僅代表個人觀點，不代表中央銀行立場。

摘要

比特幣的崛起，讓區塊鏈承載許多希望。儘管區塊鏈技術未臻成熟，但已被嘗試應用在諸多領域，例如：支付、貿易融資、法律、通訊、投票和智能合約等。這些應用對於金融業現有業務和未來發展具有一定影響力－是機會，亦是挑戰。隨著區塊鏈相關專案的投資金額逐漸上升，可望推動技術進一步發展。區塊鏈有機會幫助金融機構降低平台成本、促進資訊傳遞、數據記錄及儲存管理方式轉型，也可能改變原有的監管模式，提供金融業更快速有效的運作模式。而目前看來，實名制和認許式區塊鏈或許是未來參考發向。另值得留意的是，有人開始將人工智慧演算法布署在區塊鏈上，避免同時掌握大數據和強大人工智慧的單位，對社會公平性構成威脅。

然另一方面，區塊鏈的發展也為金融和監管業者帶來諸多挑戰，例如：區塊鏈雖可降低交易成本，解決信用不足所產生的風險，但也可能弱化了金融中介或信用機構的功能；區塊鏈發展所帶動的新型 P2P 業務模式（如借貸等），可能分食銀行客源；由於部分區塊鏈係匿名機制，使得用戶的加密數位貨幣被盜後，將難以獲得保障。再者，區塊鏈技術對金融業現有法規和監管框架帶來新課題。譬如：歐盟一般資料保護規則（General Data Protection Regulation,GDPR）中所規定的「跨境傳輸原則禁止」與「被遺忘權（Right to be Forgotten）」與區塊鏈技術相衝突，且不同國家的法規、管理政策皆不盡相同。這些差異在跨國法規的融合及介接上亦會受影響。

儘管區塊鏈的發展之路並非一帆風順，但若各國產、官、學界持續相互合作與研究，依實際應用情況，建立適當、有效且相容的監管制度，以適用在全球化的區塊鏈金融服務，相信未來終將突破既有金融模式，帶來創新發展。

目　錄

圖表目錄

國際貨幣基金（International Monetary Fund, IMF）曾指出：「從人工智慧到分散式帳本，新興科技(金融科技，FinTech)正改變金融服務業之樣貌，為消費者、服務提供者和制定法規者，帶來機會與挑戰。這些科技可能提高金融業在支付、融資、投資、資產管理和保險領域之效能，但也為金融體系之穩定性和完整性構成風險，特別是在金融監管範疇之外。」

為因應席捲而來的金融科技浪潮，本文侷於篇幅，在眾多金融科技中選擇探討區塊鏈技術－分散式帳本技術（Distributed Ledger Technology, DLT），並針對其應用、發展、影響等議題進行分析。

壹、區塊鏈機制

一、何謂區塊鏈（Blockchain）

區塊鏈係加密型貨幣[1](以比特幣為例)背後的底層技術，透過「去中央處理」和「分散式帳本」機制為使用者進行點對點支付，從而創造一總帳本，記錄用戶之間的交易和資產移轉。茲詳述如下：

(一)何謂「去中央處理機制」

亦即「帳本共享」和「集體維護機制」。整個帳本的運作仍是依照創始者所撰寫的營運系統協定和軟體來運作，但整個交易過程不再需要中介機構協助結清算處理或管理交易紀錄，資料也不是由特定的中央控管機制處理後再分送資訊至各節點（node），而是由眾節點進行集體維護。

(二)何謂「分散式帳本」

資料的產生來自各節點，並由節點向終端使用者（end user）提供對外帳本服務。為了使記載在各節點上的帳本資料一致，每筆交易由發起方向的節點進行溢散式傳播（propagation casting），最後擴散到全網，使分散的各節點所記載之帳本一致。

---

[1]係指運用密碼學原理來確保交易安全及控制交易單位創造的交易媒介，屬於數位貨幣或虛擬貨幣的一種。

(三) 為何取名為「區塊鏈」

所謂「區塊」，係指透過 hash 機制，將交易相關資訊綁定和紀錄在特定格式和欄位[2]裡，而這一個一個資料區塊（block）即構成總帳簿；所謂「鏈」，則是指將不同區塊透過特殊機制鏈結（chain），以強化資料被竄改的難度。在交易過程中，為驗證交易身份和確保交易安全，另搭配「公開金鑰加密（Public Key Cryptography）」、「條件式雜湊函數計算（Conditional Hashing）」與「工作量驗證（Proof of Work, PoW）」等技術組合。交易過程中，為確定資產所有權和支配權是權利擁有人，故採用「公開金鑰加密技術（PKC-Public Key Cryptography）」；又為確保大帳本系統中所儲存的資料，不會被他人竄改，採用「區塊鏈機制」，配合上「條件式雜湊函數計算（Conditional Hashing）」來增加竄改交易訊息的難度，以及「工作量驗證（Proof of Work, PoW）[3]」來處理分岔問題[4]。

二、區塊鏈技術

(一)公開金鑰加密技術（或非對稱式加密技術）

每個使用者下載電子錢包時會產生一對金鑰，分別是公鑰（Public Key）與私鑰（Private Key）—公鑰能被廣泛地發布與流傳，而私鑰則須被妥善保存。訊息由一把金鑰加密後，必須由另一把金鑰解密。由於加密和解密需要兩個不同的密鑰，故亦被

---

[2]這些欄位包含：「時間戳記 」、「Hash 值」 、「前一個 hash 值（previous hash）」、「隨機值（Nonce）」和「困難值（Difficulty）」等。

[3]屬於共識決演算法其中一種，於本文第 4 頁會有更詳盡說明。

[4]所謂「分岔」問題係指，區塊傳送到不同節點所需時間不同，因此不同節點所擁有之區塊鏈，其資料不一定是處在完全一致狀態。再加上缺乏中央控管機制，故無從得知其他節點之挖礦進度。若某節點同時接受到來自節點甲和節點乙所製作的區塊，只能先將兩個區塊同時接上手中原本的區塊鏈，形成「分岔」現象。之後再以「共識決(consensus)」方式，決定保留哪一條區塊鏈分支。而比特幣所採用的共識機制為「工作量證明演算法（簡稱工作量證明，PoW）」。而之所以稱為「共識」，係因其中的信任機制是由各節點透過難以篡改的運算證明所達成的共識。

稱為非對稱加密（Asymmetric Cryptography）。它的優點在於，解決「對稱式加密技術」因為傳送方和接收方皆使用同一把密鑰，所產生的中間人攻擊風險[5]。然缺點是，私鑰須妥善保存，否則有被盜風險。再者，這種方法只能確認某筆交易訊息，的確是被該筆公私鑰擁有人所簽署（可驗證）。但因為這對鑰匙並未與使用者真實身分作連結（匿名制），故無法追蹤到底誰在進行這筆交易，也容易淪為不法人士洗錢、交付黑錢的管道。例如：Nick 想把 1 萬 Bitcoin 轉送給 Peter 來逃漏稅，或是支持其地下活動。Nick 本身就有一對公私鑰(即 N 公鑰與私鑰)。但他又另外產生一對「P 公鑰與私鑰」。然後，他透過 N 私鑰簽署該筆交易，將 1 萬 Bitcoin 轉入 P 公鑰所代表的帳號地址。Nick 再將 P 公鑰與私鑰，一併傳送給 Peter。之後 Peter 就可以透過 P 私鑰簽署該筆交易，動用這筆金額，或是藉由簽署另外一筆交易，將該筆錢兌換成其他資產，進而達到洗錢目的。

至於要如何改善上述風險，除妥善保管私鑰外，可驗證實名制或許是一可行方式。台灣網路認證公司董事長杜宏毅博士曾指出：「可驗證的實名制其實為電子憑證機制。依實作經驗，以區塊鏈平台介接目前所使用的電子憑證機制，似乎較為可行。」

(二)條件式雜湊函數計算

1.條件式雜湊函數：

在了解「條件式雜湊函數計算」前，需先了解何謂雜湊函數（hash functions）。所謂雜湊函數係一種數學演算法，將大量的資料或訊息壓縮成小量的亂數值。而為什麼 hash 機制可防止交易訊息被竄改呢？因 hash 機制的運作，係將數字化的交易訊息插入隨機值（nonce）後，透過特定 hash 演算法計算出 hash 值，再將 nonce 值和「計算出的 hash 值」回存進交易訊息裡，使得交易訊息、nonce 和 hash 值被綁定在一起。如果

[5]密鑰在傳送過程中，被中間人攔截且複製，再傳送給接受方，之後就能破解和竄改加密訊息。

有人竄改了交易訊息，在 nonce 值不變情況下，所產生的 hash 值就會與原本的不同。而比特幣創始者中本聰為了提高計算 hash 值難度，又加入了困難度指數條件，讓計算出的 hash 值，必須低於該指數[6]。

2.與「挖礦（mining）」之關係

這種不停地「設定 nonce 值、計算 hash 值」過程，就叫做挖礦。更詳細解釋，挖礦就是節點（俗稱礦工）運用礦機設備[7]計算認證每筆交易，而成功「計算出符合困難度指數條件的 hash 值」[8]，就可獲得記帳權和獎勵：最先計算出 hash 值的礦工，將計算出的 hash 值填入 block 以完成區塊的建立（記帳權），接著再把此消息傳送至其他節點，且為其他節點所接受，就會獲得一定數量的虛擬貨幣（如比特幣）作為報酬（回饋機制）。

3.然而，依照這種方法來製作一個區塊相當費時耗電[9]，因此也產生單位時間內處理交易量的「擴增能力（scalability）」問題。

(三)工作量驗證

然而，如果有兩個節點（以下簡稱甲、乙）同時計算出符合條件的 hash 值（都是正確答案但結果不同），由於欠缺中央控管機制，彼此並不知道對方的挖礦進度。在各自建立 block 後，向其他節點進行訊息傳遞。若某節點（以下簡稱丙）同時接收到甲與乙所計算出的 block，它應該如何作選擇？這時丙會產生兩條分支，讓甲 block 和乙 block 與其手中的區塊鏈分別作鏈結，形成「分岔現象」。等到又有新的 block 被傳遞到丙時，丙就會看哪條分支所「累積的困難度比較高」或「總工作量」比較大，來決

[6]整理自杜宏毅、宋倬榮（民107年）。《區塊鏈之書》，頁35-45。

[7]亦衍生出大量耗能耗電的問題。

[8]取自 https://www.inside.com.tw/article/13992-mining-miner-hash-ledger

[9]根據數位貨幣網站 Digiconomist 統計，全球比特幣礦工的年耗電量相當丹麥一國一年所需的電量。

定分支的去留。然而，這種「共識決」演算法的問題在於，難度比較低或被捨棄的分支，會讓原本被確認的交易又變回未確認狀態，形成「清算最終性（settlement finality）」問題。

三、區塊鏈類型

區塊鏈可依參與驗證及查閱帳本的授權，區分為不同類型。如果參與者須透過管理單位預先選定，僅限特定人才能參與驗證及查閱帳本，稱為認許式區塊鏈（Permissioned Blockchain）；反之，開放任何人均可參與驗證及查閱帳本，則屬於非認許式區塊鏈（Permissionless Blockchain）；另外，目前也有介於兩者之間的混合式區塊鏈（Hybrid Blockchain）（表 1）。

(一)認許式區塊鏈

認許式區塊鏈是一種不公開、需授權的區塊鏈，其透過可信任的中介管理單位來處理交易的驗證，因此不一定需要利用加密貨幣作為區塊鏈上驗證交易的報酬。認許式區塊鏈採行實名制，較能配合主管機關監管所需的反洗錢（Anti-Money Laundering, AML）與客戶身份驗證（Know Your Customer, KYC）規範。目前較為著名的例子：Opencoin 公司透過認許式區塊鏈來發行瑞波幣（Ripple, XRP）。

(二)非認許式區塊鏈

非認許式區塊鏈是一種公開的區塊鏈，開放所有人均可參與驗證，共識過程可使用密碼學等方式維護資料的安全，且不需要可信任的中介介入。非認許式區塊鏈採行匿名制，因此較不易監管且有價格波動度高等問題。目前市場上採用非認許式區塊鏈的例子，包括：比特幣（Bitcoin）及以太幣（Ether）。

(三)混合式區塊鏈

混合式區塊鏈主要係建立在非認許式區塊鏈的基礎架構上，同時為需授權或許可的網路提供技術，是目前市場上較多企業傾向提供的模式。其參與驗證的節點是預先選好的，區塊也不會隨意擴增，至於網路上的共識演算法則可以自行定義，目前市場上採用混合式區塊鏈的例子為 R3 聯盟[10]。

表 1 不同區塊鏈類型之特性

區塊鏈類型	認許式	混合式	非認許式
參與者	授權加入	特定入盟人群	任何人自由進出
記帳者	自訂	參與者協商決定	所有參與者
信任機制	中介	集體	工作量證明
激勵機制	不需要	可選擇	需要
中心化程度	中心化	多中心化	去中心化
特殊優勢	透明、可追溯	效率、降低成本	信用自行建立

四、區塊鏈之優缺點與相關建議

以下茲就原生型（比特幣型）區塊鏈進行探討。該區塊鏈雖具資料竄改不易、透明度高等特性，但尚存諸多缺點待克服。茲將其優劣勢與相關建議整理如下表：

表 2 原生型區塊鏈之優缺點與相關建議

技術組合	優點	缺點	建議
公開金鑰加密機制	解決對稱式加密技術所產生的中間人攻擊問題	1. 私鑰被盜風險 2. 若公私鑰擁有人之身分採匿名制，容易淪為洗錢或不法捐款的管道	1. 妥善保存私鑰 2. 可驗證實名制：杜宏毅博士曾指出，可考慮以區塊鏈平台介接目前所使用的電子憑證機制

[10] R3聯盟係於2015年成立，該聯盟成員多為跨國金融機構，其目標係為金融業提供合作探索區塊鏈技術的管道及建構以DLT為核心新技術平台。該聯盟目前擁有包括高盛及摩根士丹利等超過70個機構會員。

技術組合	優點	缺點	建議
條件式雜湊函數計算	1. 交易驗證與提高資料被竄改的難度 2. 由節點來挖礦，可節省中央控管機構之成本	1. 處理量的擴增能力（scalability of processing） 2. 51%攻擊風險 3. 耗費大量時間、運算力和電力	1. 不適合用於即時或高頻交易系統，但可考慮應用在跨境支付或跨國匯兌。另可採用私有鏈方式來擴大區塊包容交易筆數 2. 風險存在，但掌握51%運算力之成本相對高昂 3. 難以解決
共識決演算法─工作量驗證（PoW）	處理分岔問題	1. 清算最終性問題（Settlement Finality） 2. 耗費大量運算力和電力 3. 速度侷限性	1. 可採用其他共識決，例如：Paxos 演算法[11] 2. 難以解決（如果節點有限則電力成本會相對有限） 3. 認許式區塊鏈或其他共識決區塊鏈的處理速度，較非認許式區塊鏈之效率高
去中央控管之溢散式傳遞	成本由各節點分攤	1. 速度侷限性 2. 責任歸屬問題	1. 採用私有鏈，藉由調整區塊製作頻率，來提高速度 2. 基於究責問題，可考慮認許式區塊鏈
回饋機制	提供挖礦誘因	有發行量遞減問題，難以調節供給量。	不適合在法幣發行
分散式帳本	1. 每個參與者都能獲得完整備份數據，具不可取消之特性，有助提升資料透明度 2. 可提供事後稽核軌跡 3. 監管機關取得資料來源	資料透明的反面為隱私保障問題	透過認許式區塊鏈，讓資訊在不同主體間進行選擇性分享

[11]Paxos 係基於消息傳遞且具有高度容錯特性的一致性算法。《區塊鏈之書》曾指出，Paxos 演算法屬於「民主法治型」的共識決。它的特點在於，所有節點先依照某種既定的協定，選出製作區塊的節點。然後所有節點，再將交易傳送到此指定的節點。該節點再將製作好的區塊，傳送至其他節點。

貳、區塊鏈之發展與應用

一、區塊鏈發展

比特幣（一種數位加密貨幣）的風靡引發人類對區塊鏈的關注，開始探索其背後的運作機制，並有了後續的發展與應用。現今越來越多企業及個人運用該技術於加密貨幣交易及智能合約，同時展開各種 DLT 概念驗證項目，以評估應用在其他項目之優勢及功能。目前開發重點在強化交易處理效能、隱私保護及多功能應用等。專家 Melanie Swan[12]曾將區塊鏈的發展分為三個階段：區塊鏈 1.0、區塊鏈 2.0 和區塊鏈 3.0，茲介紹如下：

(一)區塊鏈 1.0：數位加密貨幣（以比特幣為代表）的應用（2008 年~2011 年）

有人說：「若互聯網的發明實現了信息的傳播，那麼區塊鏈的出現，則是實現價值的移轉」。2008 年中本聰發表比特幣白皮書「一個點對點的電子現金系統」，正是這波區塊鏈浪潮的濫觴。他的宗旨或許是在創造一個去中心化、自由、開放的價值移轉（交易和支付）世界，然比特幣型區塊鏈本身就存在限制性（如表 2 所提），且加密數位貨幣或虛擬貨幣[13]的安全性、穩定性和可信賴性仍待商榷。

(二)區塊鏈 2.0：可程式設計金融之應用（2012 年以來）

以 Ethereum 為代表的區塊鏈 2.0，實現了可程式設計[14]之金融應用。其應用加入了「智能合約（smart contract）」的概念，使得區塊鏈從最初的貨幣體系，拓展到股權、

---

[12]Swan, Melanie (2014), "Decentralized Money: Bitcoin 1.0, 2.0, and 3.0," *Institute For Ethics and Emerging Technologies*, Nov. 10.

[13]依據歐洲銀行業管理局的定義，虛擬貨幣係指以數位方式表示價值的貨幣，既非一定由央行或政府機構所發行，亦不一定與法定貨幣有所連結，但被自然人或法人所接受，作為支付、移轉、儲存或交易的媒介。

[14]可程式設計係指「通過預先設定的指令，完成複雜動作，並能通過判斷外部條件做出反應 」，取自於龔鳴（民106年）。《寫給未來社會的帳本》，頁37。

債權與產權的登記及轉讓，證券和金融合約的交易、執行，甚至防偽、虛擬貨幣首次公開發行（ICO, Initial Coin Offering）等金融領域。目前主要應用項目如下：

1.跨境支付、匯款和貿易結算；

2.股權、債券和財產權的登記和轉讓；

3.智能合約。

(三)區塊鏈 3.0：於其他領域之應用（未來）

區塊鏈 3.0 的應用，進一步使用較複雜的智能合約，旨在實現可程式設計的社會。此時區塊鏈是價值互聯網的核心，能夠對於每一個互聯網中代表價值的訊息進行產權確認、計量與存儲。區塊鏈 3.0 跳脫貨幣與金融領域，擴展到應用在法律、物聯和醫療等領域，進而到整個社會。

二、區塊鏈之應用與實例

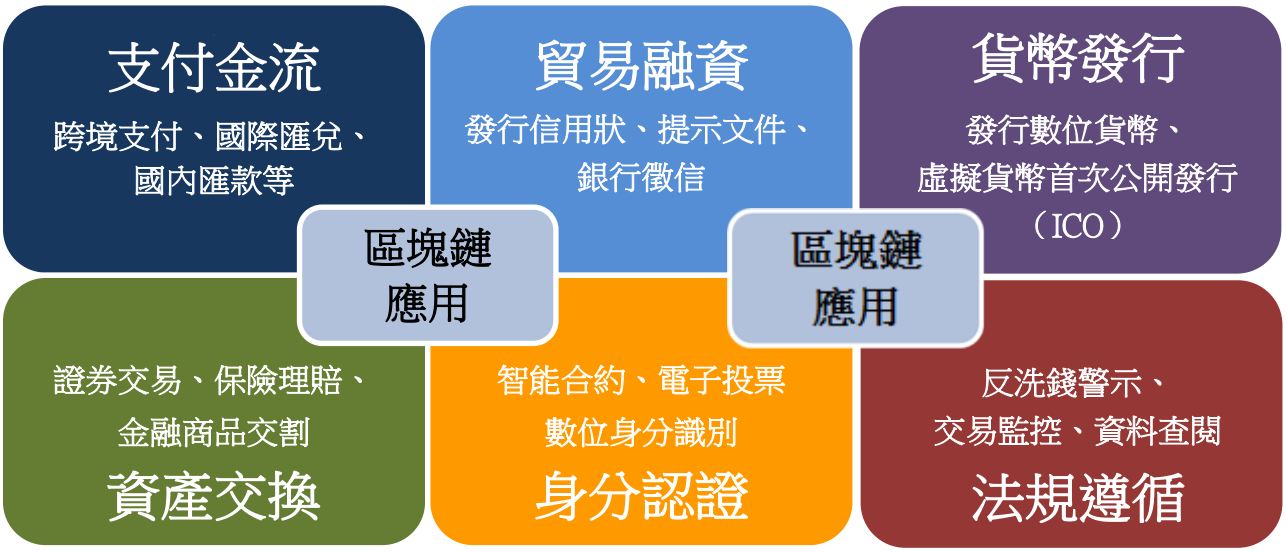
(一)區塊鏈於金融領域之應用

事實上，目前區塊鏈尚未出現成熟的應用解決方案，很多都還在開發、研究的階段。國際上許多金融機構、科技與新創公司透過聯盟合作開發區塊鏈專案，以實現更快速有效率的支付、結清算與交割、資產交換、貿易融資、身分認證與資訊安全等，甚至嘗試與主管機關合作，探討區塊鏈技術在貨幣發行及法規遵循方面的應用（圖 1）。以下茲就世界經濟論壇（World Economic Forum, WEF）[15]及國際貨幣基金（International Monetary Fund, IMF）[16]研究報告所提之區塊鏈金融應用作進一步介紹：

[15]World Economic Forum (2016), "The Future of Financial Infrastructure – An Ambitious Look at How Blockchain Can Reshape Financial Services," *World Economic Forum*, Aug.

[16]He, Dong et al. (2017), "Fintech and Financial Services：Initial Considerations," *IMF Staff Discussion Note,* June 19.

圖 1 區塊鏈於金融領域之各項應用



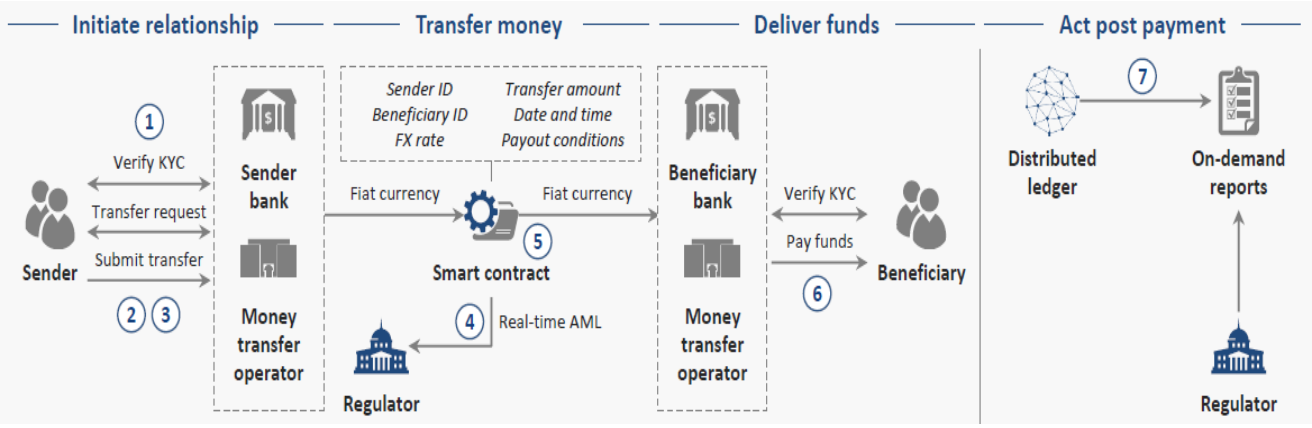
資料來源：綜合 WEF 及 IMF 報告資料整理

1.支付（以跨境支付為例）

目前跨境支付系統其實獨立於國內支付體系，兩者之間差異主要在於國內支付是透過國內銀行及央行結算，而跨境支付通常透過通匯銀行（中介行）或 SWIFT（Society for Worldwide Interbank Financial Telecommunication）來進行結清算。整個過程包括從一開始收取款項、傳遞訊息、資金結清算，到最後支付款項給收款人，所需耗費數天到一週以上不等（依照匯款地區及資料完整性等而有不同）。中介行收取之手續費亦不甚透明，但大多從十幾塊美金起跳，且若非全額到匯的匯款，並無法於一開始得知實際金額。

因此，透過科技創新，在跨境支付系統導入區塊鏈、DLT 與智能合約等技術，某程度上可改變現行支付架構，大幅降低相關費用，並使支付方式更快速有效率。此外，若將區塊鏈與其他技術結合應用（如：生物辨識、人工智慧），可發揮更大的效益。若應用在 KYC 及數位身分認證方面，將有助於訊息共享並降低法遵成本，亦有利於金融機構與主管機關進行反洗錢、反資恐及制裁等相關管控措施。茲將新型（應用 DLT）跨境支付的流程介紹如下（圖 2）：

圖 2 新型跨境支付流程



圖片來源：World Economic Forum

Step 1：匯款行可選擇透過驗證數位身分方式對匯款方進行 KYC。

Step 2、3：匯、收款方可透過智能合約確定彼此間資金移轉的權利義務關係。

Step 4：監理機關可透過智能合約收到反洗錢警告，並即時監控交易。

Step 5：透過智能合約可即時匯款，無須透過中介行或 SWIFT。

Step 6：完成收款方 KYC 後，智能合約將款項自動匯至收款方帳戶。

Step 7：歷史交易資訊均儲存在分散式帳本中，可供監理機關隨時查閱。

創新支付模式亦可應用區塊鏈與虛擬貨幣結合，如：以電子形式兌換虛擬貨幣，並以 DLT 為基礎網路（認許制或非認許制皆可），將帳戶資金移轉至虛擬貨幣體系。用戶可先透過 ATM、網路等方式將法定貨幣兌換成存於數位錢包中的虛擬貨幣，接著將虛擬貨幣透過其安全的網路移轉至國外收款人的數位錢包，最後由收款人將數位錢包中的虛擬貨幣兌換成國外法定貨幣。

相較於現行傳統支付系統，區塊鏈應用為跨境支付帶來許多新契機，如：身分確認、KYC 更為準確便利、降低匯款手續費、縮短匯款時程、隨時監控及減少作業疏失等，但也會帶來幣值不穩定、跨國法規遵循標準不一等問題（表 3）。另外，新技術導入對金融市場結構可能也會造成重大影響。如：未來交易訊息傳遞與資金結清算可能

將不再需要透過央行或通匯行；在款項收取及款項支付方面，虛擬貨幣交易所及數位錢包廠商恐將加入跨境支付市場爭奪客戶。

表 3 區塊鏈應用於跨境支付的優劣分析

傳統支付架構之優勢	區塊鏈架構之優勢
需透過繁複的作業流程確認客戶資訊，且各銀行規範不同，KYC 準確度受限	銀行可透過驗證分散式總帳中留存的數位身分資料對匯、收款方作 KYC
銀行需在存放國外同業帳戶中留存準備金，資金成本較高	透過智能合約，可將來自交易對手的匯款輕易地轉換成當地貨幣
跨國匯款手續費昂貴且費時	可即時匯款，且經手的機構較少可大幅降低交易手續費
為應對監理機關的要求，金融機構需付出較高的法遵成本	監理機關可透過智能合約即時收到異常警告，並可隨時從 DLT 中調閱歷史資料
交易需要多個機構經手，提高潛在錯誤機率，作業風險高	DLT 使匯款行與收款行可直接交易，且透過智能合約可減少作業疏失
傳統支付架構之劣勢	**區塊鏈架構之劣勢**
SWIFT 系統包含所有既有的金融機構	加密貨幣幣值波動度較高
可吸納大規模的國際資本	不易建置共同 KYC 及全體互通之標準
客戶較熟悉此模式，無轉換系統成本	各國法規複雜度不盡相同，須合作制定相關法規

資料來源：World Economic Forum

2.貿易融資[17]

根據 WEF 本(2018)年 9 月發布最新報告[18]，2017 年全球貿易融資缺口約 1.5 兆美元（主要為中小企業的資金障礙），占全球貿易量 10%，因此區塊鏈的出現對其影響尤深。由於傳統貿易融資多仰賴信用狀，除曠日廢時、手續繁雜且昂貴外，尚過度依賴紙本作業及人工流程。該報告指出，DLT 可帶來新的貿易模式，大幅降低貿易融資缺口，因而額外增加約 1.1 兆美元的貿易量，並使交易更有效、安全，有助於金融業者提高融資可信度並節省成本。茲將新型（應用 DLT）貿易融資的流程介紹如下（圖 3）：

圖 3 新型貿易融資流程

資料來源：World Economic Forum

Step 1：進口商透過智能合約，與進口銀行分享合約、商業發票等資訊。

Step 2：進口銀行進行文件審查，擬好信用狀條件後，傳送予出口銀行。

Step 3：出口銀行審查信用狀文件，核准後即產生一份智能合約以涵蓋信用狀條款。

Step 4：出口商在智能合約中對信用狀進行數位簽章後，開始裝船、運貨。

Step 5：貨物由第三方及原產國海關代理進行檢查（均以數位簽章核准）。

Step 6：進口商收到貨物前，貨物從 A 國運往 B 國，並由當地海關人員檢查。

Step 7：進口商以電子方式確認收到貨物，進口銀行透過智能合約付款給出口銀行。

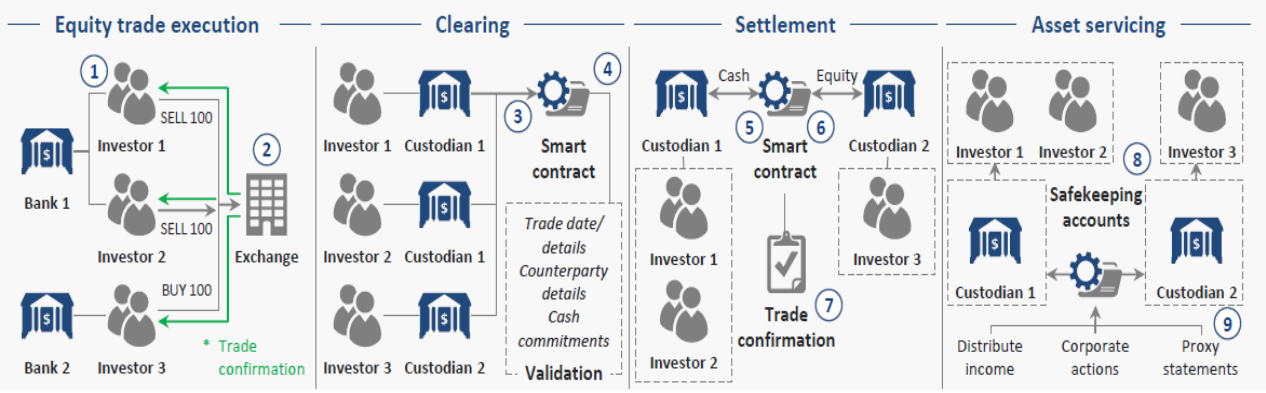
[17]貿易融資是進口商和出口商透過可信賴的金融中介機構來減輕貿易風險的授信過程。金融機構作為值得信賴的第三方中間人，向賣方提供保證、為買方承擔不確定性，並負責記錄、監督付款條件以及承擔進口商或出口商的風險。

[18]World Economic Forum (2018), "Trade Tech – A New Age for Trade and Supply Chain Finance," World Economic Forum, Sep.。

3.證券交易

證券業是區塊鏈相當適合的應用領域。相較於傳統證券交易需經過中央結算機構、保管銀行、證券公司及交易所相互協作，才能完成整個證券交易流程，效率低且成本高；區塊鏈則可獨立地完成一條龍式的證券服務，包括了股權、債券的轉讓、證券登記、結算交割等。區塊鏈應用在證券交易可自動化交易（縮短交易時間）、標準化數據（以提升清算效率）、降低交易對手風險、即時確認並降低證券帳戶的複雜度等。茲將新型（應用 DLT）證券交易流程如下（圖 4）：

圖 4 新型證券交易流程



資料來源：World Economic Forum

Step 1：投資人使用自己選擇的銀行，透過交易所下股票交易單。

Step 2：交易所負責撮合股票交易訂單，即時確認交易並啟動交割流程。

Step 3：保管銀行代投資人將其交易資訊透過 DLT 傳送。

Step 4：以智能合約驗證所有保管銀行提供的交易資訊，並即時撮合交易。

Step 5：撮合完所有交易後，透過智能合約確認淨交易量。

Step 6：以智能合約代表所有投資人，在保管銀行同時交付股票及現金。

Step 7：確認的交易資訊存在 DLT 中。

Step 8：資產轉移後，股票及現金皆存在保管銀行管理帳戶中。

Step 9：智能合約能在發生各項交易流程時，即時通知保管銀行及投資人。

4.數位貨幣發行

此非指央行發行另一種新型貨幣，而是以DLT運作機制為基礎，由央行發行法幣，大眾透過商業銀行或直接向央行進行兌換。BIS研究報告指出[19]，央行發行數位貨幣可區分為兩種類型：消費者支付使用之零售型數位貨幣，以及作為銀行間支付系統之批發型數位貨幣。

至於央行數位貨幣的形式，IMF[20]認為應會以與法幣相同之計價單位發行，成為央行的一種負債，並能跟央行其他非股權負債如現金或商業銀行準備金一比一兌換，且並無實體，須以電子方式兌換。至於數位貨幣的移轉方式，可使用現行「即時總額清算機制（Real-Time Gross Settlement, RTGS）」來移轉，但此方式較適合大額、制式化交易，並用於經認許的銀行，因現行結算系統有單點失誤風險，採用DLT(其擁有多個複本)可能更為安全。

央行發行的數位貨幣優點在於這種數位貨幣是由政府發行，因此較能被使用者信任，穩定的發行量也有助於維持虛擬貨幣匯率穩定，可解決虛擬貨幣價值不穩定與波動大的問題。然而，對於央行發行數位貨幣，需審慎考慮潛在的成本與風險，如平台的管理與整合，以及如何解決隱私權問題。另外，法定數位貨幣對金融體系監管的影響、貨幣政策制定及央行與商業銀行的角色，一直存在諸多疑問。

5.虛擬貨幣首次公開發行

虛擬貨幣首次公開發行（Initial Coin Offering, ICO）係由業者提出投資計畫，使用區塊鏈技術向社會大眾發行數位代幣（Token），並收取現金或虛擬貨幣（如比特幣、

[19] Bech, Morten and Rodney, Garratt (2017), "Central bank cryptocurrencies," BIS Quarterly Review, September。

[20] He, Dong et al. (2017), "Fintech and Financial Services：Initial Considerations," *IMF Staff Discussion Note,* June 19.

以太幣等）以進行籌資。由於性質類似發行證券或其他投資產品，概念與群眾募資相似，許多國家的監管機關因而將此業務納入現有證券法的範圍，以便管理。

ICO 既可做為一種融資機制，許多科技創新公司便透過加密貨幣或代幣進行籌資，而出資者也能透過購買加密貨幣或代幣來進行投資。然而，近來 ICO 詐騙、投機案件層出不窮，已引發各國主管機關關注，許多國家已強化針對 ICO 的監管，因應措施包括：將 ICO 納入現有證券法的範圍（如美國）[21]、納入監理沙盒進行創新實驗（英國），或是直接禁止（如中國大陸、韓國等）[22]。

（二）近期區塊鏈應用案例

近半年區塊鏈的應用專案正迅速發展，涵蓋：加密貨幣、跨境支付、證券交易、貿易融資、保險理賠、身分認證、資安、交易後手續甚至函證等領域，範圍廣泛。

表 4 近期區塊鏈應用案例

項　目	應 用 案 例
加密貨幣/數位錢包	1. 台灣活動平台 Accupass 活動通，已開通**加密貨幣支付功能**，目前得以**比特幣或以太幣**進行支付，而收到的加密貨幣款項會直接轉入活動舉辦方的帳戶（區塊鏈位址）中。 2. 投資平台 eToro 宣佈推出「**加密貨幣錢包**」，將支援用戶**存儲比特幣、比特現金、以太幣及萊特幣 4 種加密貨幣**。該錢包有多重簽名功能，讓用戶可更安全地持有加密貨幣資產。
跨境支付	Ripple 公司推出分散式帳本技術的服務「**xRapid**」，旨在加速進行**國際支付匯款**，且**不需事先在國外同業存款帳戶（Nostro Account）存入資金**。xRapid 採用瑞波幣（XRP）作為跨境支付的橋樑（共通）貨幣，可降低匯兌成本和提高支付效率。

[21] 2017年7月美國證券交易委員會(SEC)發布調查報告指出，判斷一特定交易是否涉及證券發行及銷售，取決於事實與情形，包括交易的經濟實質。其認定市場參與者利用分散式帳本或區塊鏈技術發行及銷售虛擬貨幣，適用聯邦證券法的規定。

[22] 中國人民銀行於2017年9月宣佈，由於許多 ICO 專案涉嫌從事非法金融活動，為保護投資者，故禁止各類代幣發行融資活動；隨後，韓國金融服務委員會（Financial Services Commission, FSC）於同月亦發布公告，禁止國內各種形式的 ICO 活動，此外並針對虛擬貨幣交易進行嚴格控管。

項　目	應 用 案 例
證券交易	新加坡金融管理局（MAS）與新加坡交易所（SGX）開發**款券同步交割（DvP）**功能，將用於不同**區塊鏈跨平台結算**，有助於簡化交易後流程並進一步縮短結算週期，並透過**智能合約**支援在不同區塊鏈平台間之**代幣資產結算**。
貿易融資	**中國信託**聯合 7 家國際外商銀行，透過區塊鏈聯盟 **R3** 所開發的 Corda 區塊鏈架構開發了名為 Voltron 的貿易融資解決方案，大幅**縮短信用狀作業流程**，在開放網路**直接發行信用狀與提示文件**，將過去紙本傳送的流程數位化，提高作業效率。
保險理賠	東京海上日動與 NTT 數據協作了一款獨特的**海事保險區塊鏈**，並採用「**概念驗證（Proof of Concept, PoC）**」，將過往繁雜耗時的**海事理賠作業（如貨櫃受損等）**，透過區塊鏈簡化，加速整個過程。其目標在 2019 年，使海事保險區塊鏈確實落地，進入實務應用。
身份驗證	台灣分散式帳本技術新創公司 BiiLabs，宣布啟動**符合歐盟「一般資料保護規範（GDPR）」標準的數位身份**開源專案，針對區塊鏈應用**安全與隱私保護**進行評估與測試。
資訊安全	R3 發布首個「**區塊鏈應用防火牆**」，展示其開源區塊鏈技術的 Corda，如何限制在不同環境中運行的**區塊鏈節點間的通信**，以及來自其網路的不同訊息需求。該防火牆**保護 Corda 節點免受外部影響，同時允許通過應該通過的訊息流量**。
交易後手續	新創公司 VAKT Global 將於本年底前啟用一新的區塊鏈平台，幫助能源產業進行交易後之繁雜手續，包括**交易完成後，雙方核對交易細節、執行轉收帳、更改交易物的所有權**等事宜，較複雜的交易甚至會在此階段，進行股權移轉。如此一來不僅可**降低交易後手續的成本**，還能**減少人工作業的失誤、降低風險**。
函證[23]	**財金公司**宣布「**金融區塊鏈函證服務**」將在本年 12 月正式商轉，該服務應用區塊鏈技術，並與金融機構與會計師事務所共同訂定統一資訊標準，並透過資訊自動化填列，減少金融機構在**提供企業財務資料**與會計師事務所**函證審計作業**所**耗費的人工查核時間**與**郵寄費用成本**，同時亦能**避免函證遺失、偽造及被竄改之風險**，進而提升整體作業效率及資料安全。

[23]上市櫃公司每年年初製作的財務報表，皆須委託會計師事務所辦理查核簽證財報的審計作業，此時會計師事務所必須先向金融機構取得函證，以證明企業的財報資訊是正確無誤的；目前參與該區塊鏈服務的金融機構有30家，至於會計師事務所則共有15家加入。

參、區塊鏈對金融服務業之影響評估及未來發展

一、區塊鏈對金融服務業之影響

(一)可能弱化了金融中介或信用機構的功能：

在探討區塊鏈對金融服務業影響之前，應先探討為何比特幣創始者中本聰採用區塊鏈機制。可能是因為他資本不足，故無力承擔建立各節點轉帳設備所需費用，而區塊鏈「節點共同維護特性」可有效降低中央控管成本。其次，中介機構未必願意幫一個陌生人擔任結清算角色。再者，各節點相互不識（亦即缺乏信用環境），而區塊鏈之「公開、共識機制、分散式帳本、不易竄改」特性，可以讓交易在眾節點之見證和共識下被完整記錄。因此，區塊鏈可降低交易成本，解決信用不足所產生的風險，但同時也可能弱化了金融中介或信用機構的功能。

(二)有助降低法遵成本

區塊鏈之「分散式帳本」和「溢散式傳播」特性，挑戰了傳統中心記帳的思維。而這種完整和分散式紀錄特性，有助提供事後稽核軌跡，有效降低法遵成本。

(三)實名制、認許式（聯盟式）區塊鏈，可能是未來參考方向

1.比特幣區塊鏈（非認許式、公開鏈）具諸多限制，包括：處理量擴增能力、清算最終性、速度侷限性、耗能耗電和究責問題。為釐清責任歸屬，可考慮「實名制」區塊鏈；如欲改善速度和處理量等其他問題，則可考慮認許式（聯盟式）區塊鏈。

2.認許式（聯盟式）區塊鏈的優點在於參與節點有限，故可加快交易和記帳速度，也可降低單位時間所需處理的交易量。加上許多認許式區塊鏈的本質就是利益共綁，存在一定信任或契約機制，因此無須提供挖擴等經濟誘因，也可降低因防偽或防竄需求，所耗費之大量運算資源和成本。

3.然認許式區塊鏈本身就存在一定信用基礎，與比特幣區塊鏈（非認許式、公開鏈）產生的前提—缺乏信用環境—相悖。況且現有機制本身即具有「可追蹤」、「不易竄改」等特性，如此，為何不沿襲現有中心化運作模式而要採用聯盟鏈模式？有人提出觀點如下[24]：

(1) 認許式區塊鏈之核心思想在於點對點的網路（peer-to-peer network），除改變了以伺服器為中心的主從式網路架構外，亦可讓資訊在不同主體間進行選擇性分享。

(2) 現有的中心化運作模式，參與者對所屬資料、資料存取方式和資訊系統建立，並無直接控制權；然認許式區塊鏈可以拿回主動權，並可透過聯盟鏈來執行智能合約，進行更深入的應用。

(四)智能合約之發展

過去即有「智能合約」的構想，讓資產或價值的移轉，變成可程式化和自動執行。然當時技術尚未成熟，且未出現一個合適平台來自動執行合約，一直到區塊鏈（平台）的出現，才實現了這個想法。另智能合約中的特色在於，參與者無須透過信任彼此來履行義務，因為合約是由代碼編寫、定義和強制執行，除可減少人工干預和人為判斷外，亦可降低監管成本、提高執行效率和減少資源浪費。目前可應用之金融領域包括：保險理賠、租賃服務等，甚至是 P2P 業務模式（如：P2P 借貸或群眾募資等，對金融服務業者構成一定挑戰）。

二、金融業者對區塊鏈應用之自我需求評估

金融業者在採納區塊鏈技術和執行相關應用時，可從「What」、「Why」、「Who」和「How」著手：

(一)What：工欲善其事，必先利其器。在應用區塊鏈前，需先瞭解其技術核心為何。

[24] Frank Lin（2017）。公共鏈 vs. 聯盟鏈 — 談區塊鏈的價值〔電子版〕。哈佛商業評論。取自 http://dweb.cjcu.edu.tw/ShepherdFiles/C0180/File/20180124115022861.pdf

(二)Why：思考為何要採用區塊鏈技術。相較於現行運作架構，它是否能帶來更多效益（如表 3 所示之優劣分析）。

(三)Who：參與對象為何？監管機關從中扮演的角色為何？

(四)How：如欲執行，可採納何種形式？如：認許式或非認許式區塊鏈等。

三、區塊鏈之未來展望

比特幣的崛起，讓區塊鏈承載許多希望。儘管區塊鏈技術未臻成熟，但已開始嘗試應用在諸多領域，例如：支付、貿易融資、法律、通訊、投票和智能合約等。這些應用對於金融業現有業務和未來發展具有一定影響力－是機會，亦是挑戰。

隨著區塊鏈相關專案的投資金額逐漸上升，可望推動技術進一步發展。區塊鏈有機會幫助金融機構降低平台成本、促進資訊傳遞、數據記錄及儲存管理方式轉型，也可能改變原有的監管模式，提供金融業更快速有效的運作模式。而目前看來，實名制和認許式區塊鏈或許是未來參考發向。另值得留意的是，開始有人將人工智慧演算法布署在區塊鏈上，避免同時掌握大數據和人工智慧的單位，對社會公平性造成威脅。

然另一方面，區塊鏈的發展也為金融和監管業者帶來諸多挑戰，例如：

（一）區塊鏈雖可降低交易成本，解決信用不足所產生的風險，但也可能弱化了金融中介或信用機構的功能。

（二）區塊鏈發展所帶動的新型 P2P 業務模式（如借貸等），可能分食銀行客源。

（三）區塊鏈仍存在網路犯罪之隱憂。由於部分區塊鏈係匿名機制，使得用戶的加密數位貨幣被盜後，將難以獲得保障。

（四）該技術將對金融業現有法規和監管框架帶來新課題。例如：歐盟一般資料保護規則（General Data Protection Regulation, GDPR）（2018 年 5 月 25 日生效）中

規定的「跨境傳輸原則禁止[25]」與「被遺忘權（Right to be Forgotten）[26]」與區塊鏈技術相衝突，且不同國家的法規、管理政策皆不盡相同。這些差異在跨國法規的融合及介接上亦會受影響。

儘管區塊鏈的發展之路並非一帆風順，但若各國產、官、學界持續相互合作與研究，依實際應用情況，建立適當、有效且相容的監管制度，以適用在全球化的區塊鏈金融服務，相信未來終將突破既有金融模式，帶來創新的發展。

[25] GDPR 中的「跨境傳輸原則禁止」，係指為保障歐盟公民的個資隱私，原則上禁止將個資傳輸至非歐盟的其他地區，以限制資料只能在隱私權高度保障的地區進行利用。然因區塊鏈的設計架構，分散式帳本會將資料儲存在世界各地的節點上，且非認許式區塊鏈無法限制誰能或不能成為節點，因此當鏈中兩個節點分別存在歐盟境內與境外時，恐產生違反 GDPR 的疑慮。

[26] GDPR 中的「被遺忘權」，係指當事人有權要求資料控制者刪除含有個人資料的網路連結。然區塊鏈因具有紀錄不可竄改、無法刪除的特性，因此區塊鏈技術與被遺忘權在涵義上並不相容。

參考文獻

1. Bech, Morten and Rodney, Garratt (2017), "Central Bank Cryptocurrencies," *BIS Quarterly Review,* September.
2. He, Dong et al. (2017), "Fintech and Financial Services：Initial Considerations," *IMF Staff Discussion Note*, June 19.
3. Swan, Melanie (2014), "Decentralized Money: Bitcoin 1.0, 2.0, and 3.0," *Institute For Ethics and Emerging Technologies,* Nov. 10.
4. US Securities and Exchange Commission (2017), "SEC Issues Investigative Report Concluding DAO Tokens, a Digital Asset, Were Securities," *SEC Press Release*, July 25.
5. World Economic Forum (2016), "The Future of Financial Infrastructure – An Ambitious Look at How Blockchain Can Reshape Financial Services," *World Economic Forum,* Aug.
6. World Economic Forum (2018), "Trade Tech – A New Age for Trade and Supply Chain Finance," *World Economic Forum,* Sep.
7. 杜宏毅、宋倬榮（民 107 年）。《區塊鏈之書》
8. 杜宏毅(民 106 年)。《如何建置一個實用的區塊鏈平台》。財金資訊季刊，90，44-45。取自 https://www.fisc.com.tw/Upload/b0499306-1905-4531-888a-2bc4c1ddb391/TC/9006.pdf
9. 龔鳴（民 106 年）。《寫給未來社會的帳本》
10. Frank Lin（2017）。公共鏈 vs. 聯盟鏈 — 談區塊鏈的價值〔電子版〕。哈佛商業評論。取自 http://dweb.cjcu.edu.tw/ShepherdFiles/C0180/File/20180124115022861.pdf
11. 取自 https://www.inside.com.tw/article/13992-mining-miner-hash-ledger