台北外匯市場發展基金會委託計畫

金融科技(Fintech)之應用與影響—以區塊鏈為例

研究人員：邱唯婷

日期： 中華民國一零捌年伍月

摘要

區塊鏈技術的發明，讓使用者得以實施去中心化(decentralize)的交易，不必再依賴無形的信賴基礎或第三方權威機構，即是金融創新的一種形式。而透過分散式記錄的帳簿，使得每台電腦都可保留並共同維護完整交易紀錄的資料庫，在區塊鏈網絡上發生的交易因此無法被竄改或停止，藉此達到公開透明的效果。此外，區塊鏈技術的應用很大部分倚靠密碼學原理，透過密碼學，利用時間戳以明確交易發生的順序、數位簽章進行防偽的身分驗證，雜湊函數來串接資料以形成不可逆的資料鏈（區塊鏈）。最後，透過每台電腦持續耗費電力資源以驗證交易的挖礦機制，使區塊鏈網路得以自動解決交易的衝突。

雖然區塊鏈的系統是公開的，但其核驗、發送等資料交流過程卻採用了先進的加密技術，這種技術不僅確保了資料的來源正確，也確保了資料在中間過程不被人攔截、更改。如果此技術的應用更為廣泛，那麼未來或可在多種不同的領域降低傳統網路安全風險，透過區塊鏈系統不需依靠第三方中間人的特性，降低駭客襲擊風險，也減少了潛在的人事支出成本，更可提升最終服務的品質。

目　　錄

圖　目　錄

壹、 金融創新之應用

金融創新的含義，目前國內外尚無統一的解釋。有關金融創新的定義，大多是根據美籍奧地利著名經濟學家熊彼特的《經濟發展理論》(Theory of Economic Development, Joseph Alois Schumpeter,1912)的觀點衍生而來。其對創新所下的定義是：新的生產函數的建立，亦為企業家對企業要素進行新的組合，包含技術創新（產品創新與工藝創新）與組織管理上的創新，因為兩者均可導致生產函數或供應函數的變化。具體地講，創新包括五種情形：(1)新產品的出現、(2)新工藝的應用、(3)新資源的開發、(4)新市場的開拓、(5)新的生產組織與管理方式的確立，也稱為組織創新。

金融業務創新包括金融產品、金融交易方式和服務方式、金融市場、金融經營管理機制和監控機制等的創新。金融技術創新要在金融業務創新的基礎上，大力發展以信息技術為基礎的先進的金融設施，完善電子金融體系建設，實現質的提升。

區塊鏈技術的發明，即是金融創新的一種形式，讓使用者得以實施去中心化(decentralize)的交易，不必再依賴無形的信賴基礎或第三方權威機構。以下就區塊鏈技術的原理中最知名的殺手級應用—比特幣為例，進行介紹。

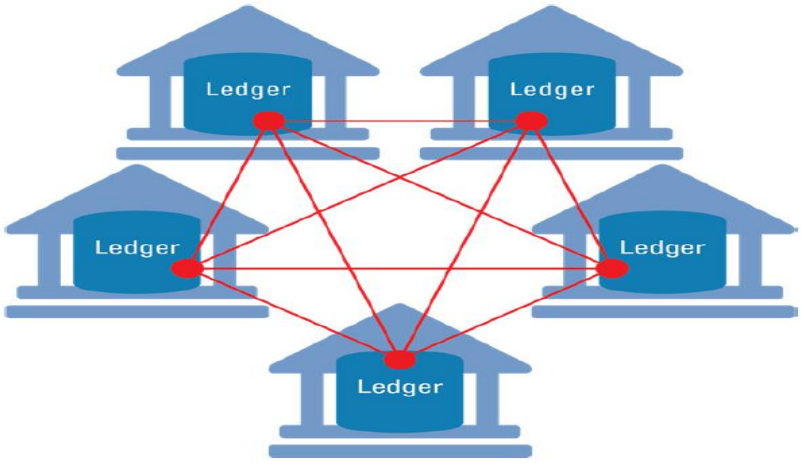
貳、區塊鏈技術

區塊鏈的特色，在於分散式帳簿(distributed ledger technology, DLT)、共同維護公開帳簿(public ledger)、具備時間戳(timestamps)、防止交易竄改(tamper resistant)、自動解決交易衝突(conflict resolution)等。在目前所有區塊鏈技術的應用中，比特幣是最為人所知的一項應用。

在比特幣網路中的帳簿(ledger)，它是記錄著所有的交易紀錄軌跡的電子檔案。而

這帳簿並非存放在一個中央機構，而是將無數份副本散佈存放在區塊鏈網絡上的每一台電腦，也就是節點(node)中。使用分散式帳簿的優點在於每一個節點均保留所有交易紀錄的軌跡，在使用中央機構系統的情況，個人只能得知自身的交易紀錄和帳戶餘額，而在區塊鏈網絡裡，每個節點均儲存所有發生的交易紀錄，惟節點儲存的交易紀錄僅能顯示交易流動的軌跡，對於帳戶的個人隱私資訊則是利用哈希函數(hash function)生成的私鑰（數位簽章）及公鑰（錢包位置）進行機密信息的保護[1]。

圖 1 分散式帳本



資料來源：Goldman Sachs Global Investment Research(2016)

比特幣用戶首先要取得一個或多個電子錢包(wallet)作為交易的工具。電子錢包中包含多個帳戶，每個帳戶可包含多個私鑰。每個錢包被密碼學加密法所保護，必須使用一對獨特且相對的公鑰和私鑰才能解鎖並進行交易，使得虛擬貨幣的交易不同於傳統的方式，有更高的防偽性。比特幣位址由公開發布的公鑰得出，使得比特幣用戶能利用公鑰產生的一組比特幣位址進行轉帳交易；而私鑰則由私人保管。使用私鑰加密

[1]每個電子錢包必須利用密碼學，使用一對獨特且相對的公鑰和私鑰才能解鎖並進行交易（使用公鑰替內容加密，並使用私鑰替密文解密），如此使得虛擬貨幣的交易不同於傳統的方式，有更高的防偽性。

後，會產生一個電子簽章，藉此確認交易訊息的發送來源和真偽。

電子簽章內容是由交易訊息和私鑰所組成的一串文字，所以特定的電子簽章不能用在其他的交易訊息上。如果第三方更改交易訊息中任何一個字元，電子簽章將因為雪崩效應(avalanche effect)[2]造成輸出值大幅度的改變，所以駭客很難更改已加密的交易訊息或是得知交易金額，達到防止交易被竄改的效果(tamper resistant)。

圖 2 哈希函數的雪崩效應

Plain text	Cipher text	Avalanche effect
11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11	79 f8 cc 24 01 82 dd 7f 2d 89 f7 e7 78 b7 ee 30	.4375(56)
11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 10	9d 4c 1d b4 6a 93 27 b5 20 64 37 d1 3d 9d 2a	
11 22 33 66 55 44 55 44 77 88 99 66 44 45 36 12	4a a9 16 11 e2 8a 9f 67 35 30 1f 80 16 c5 b7 cd	.5153(66)
11 22 33 66 55 44 55 44 77 88 99 66 44 45 36 11	D7 00 43 2d 51 78 f7 65 50 03 03 75 b1 e4 2d a0	
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	C6 a1 3b 37 87 8f 5b 82 6f 4f 81 62 a1 c8 79	.4453(57)
10 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	0d 19 33 06 27 42 fe 01 9c fe 06 e1 a8 1a a0 01	

虛擬貨幣去中心化的核心概念，使得每個節點中都保有一份交易軌跡的帳簿，並藉由持續更新自己節點內留存的交易資訊，以共同維護此公開交易紀錄。而在區塊鏈系統中，並非透過紀錄每個帳戶目前所擁有的「餘額」，只有紀錄網絡上每筆「交易紀錄」，所以欲得知某帳戶內尚可花用的虛擬貨幣時，必須分析及驗證所有曾經跟特定錢

[2]在密碼學中，雪崩效應(avalanche effect)指加密演算法的一種理想屬性，當輸入發生微小的改變（如二進位位元順序反轉）時，將導致輸出的不可區分性的改變（輸出中每個二進位位元有50%的機率發生反轉）。雪崩效應使得利用輸出數據反推原始輸入數據的難度大增，而比特幣使用的 SHA-1哈希函數即擁有良好的雪崩效應特性。

包地址產生交易的紀錄。

比特幣網絡將多筆交易訊息包成一組資料塊，稱為區塊，每個區塊包含的若干個比特幣交易訊息，和一個連到前個區塊的連結。而比特幣網路同時在每個區塊內加入時間戳記(timestamp)，藉此排出交易發生的先後順序，一個區塊跟著另一個區塊，跟隨著時間軸形成一條資料區塊的長鏈，此就為區塊鏈。

在時間序列上，同個區塊內的交易訊息被認為是同時發生，還未被打包進區塊的交易訊息會被視為未確認狀態。每個節點(full node)都可以自己選擇若干個交易訊息，打包成內容不同的區塊（交易訊息包），發送到網絡上，並建議其他節點自己打包的這個區塊為鏈上的最新候選區塊。因為任何節點都可以打包並發送候選區塊，區塊鏈系統使用加密哈希函數(cryptographic hash function)，運用工作量證明機制(proof of work, POW)來決定鏈上的最新區塊。

每一個區塊所包含的資訊，包括區塊容量大小(block size)、區塊頭(block header)、該區塊所打包的交易數量(transaction counter)，以及在此區塊中每一筆交易的交易明細(transactions)的哈希值。其中區塊頭包含許多重要資訊，如追蹤區塊鏈協議升級的版本號(version)、前一區塊的區塊頭之哈希值(previous block header hash)、工作量證明相關及彙整交易紀錄的中繼資料。

接著，區塊鏈系統利用工作量證明機制來決定哪個候選區塊能成為鏈上的最新區塊。系統的加密哈希函數設計了一道複雜的數學題，各節點打包的候選區塊只要找到正確答案，就可以成爲鏈上的最新區塊。正確的答案是以一個數字的形式呈現，各節點用試誤法(trial and error)反覆嘗試，找出符合題目要求的正確解答。隨著比特幣網路中加入的節點越多，集體算力的增強將使得找出正確解答的速度越來越快，故系統為了控制區塊產生的速度維持在大約每 10 分鐘一個，將定期調整產生新區塊，也就是哈希函數數學題的難度。

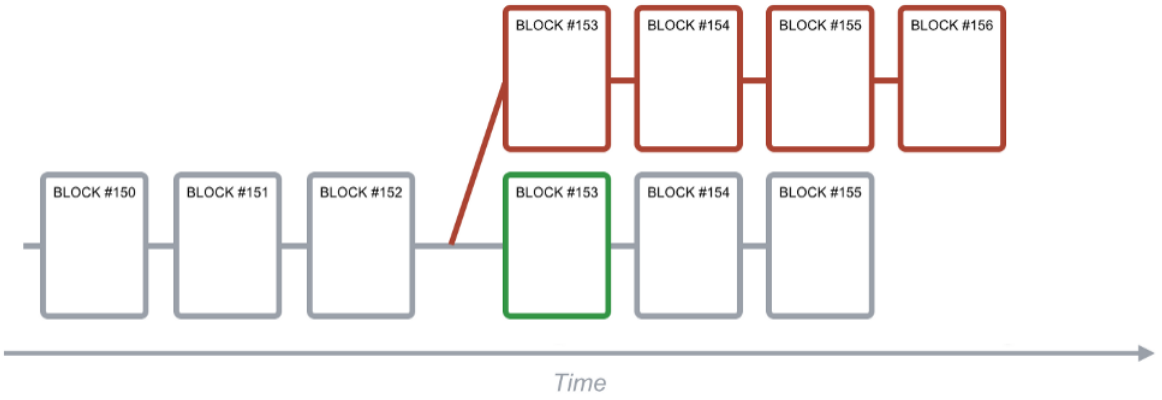
以上試誤的過程，就稱為工作量證明。工作量證明是一種對應服務與資源濫用、或是阻斷服務攻擊的經濟對策。一般是要求使用者（節點）進行一些耗時的複雜運算以得出解答。利用密碼學，此解答之取得雖然需花費很長的時間，但卻可被第三方快速地驗算，以此耗用的時間、裝置與能源做為擔保成本，以確保服務與資源是被真正的需求所使用，即是工作量證明的原理。

而此技術成為了加密貨幣的主流共識機制之一，利用哈希函數的特性，輸入函數 h(　)任意值 n，將對應到一個h(n)結果，此結果 n 也就是函數的解，哈希值。而 n 只要微小的變動，就會引起哈希值的雪崩效應，所以幾乎無法從h(n')反推回 n。因此，藉由指定 h(n)的哈希值符合特定的難度條件，讓使用者進行大量的窮舉運算，就可以達成工作量證明。此耗費大量時間、裝置或能源，以得到特定獎勵的過程，被中本聰在比特幣的論文中比喻成金礦消耗資源將黃金注入經濟，也就是形象化的「挖礦」(mining)一詞的由來。

按照最長鏈原則，所有節點都將接受現行網路中最長的鏈，並在繼續開挖新的備選區塊，而形成區塊鏈資料鏈狀結構紀錄的要件，為節點在開挖最新備選區塊石，將前一認證區塊的區塊頭進行哈希函數處理，得到的哈希值會被成為下一個的候選區塊的一部分，前一區塊的區塊頭之哈希值，是形成區塊鏈鏈狀結構最關鍵的連結，利用在每個區塊中包含上一個區塊的區塊資訊，使每一個區塊與前一個區塊資料產生無形的連結，並能確保區塊時間序列及歷史紀錄的正確性。這麼做可讓這些被驗證完的交易區塊依序串接形成鏈狀結構，一旦節點哈希值不正確，便會立刻被其他節點驗證出來，並拋棄此鏈採納其他的最長鏈。而透過哈希函數將原始資訊轉換固定長度的字符串，每個節點都將線下保有一份經過哈希加密的交易紀錄，此特性亦使區塊鏈具有防輕易竄改(tamper-proof)的特性。

區塊鏈機制在近期發展時面臨的挑戰，就包含女巫攻擊(Sybil Attack)[3]等問題。在點對點傳輸(P2P)網絡中，因為節點可隨時加入、退出等原因，區塊鏈機制為了維持網絡穩定，會將同一份數據備份到多個分散的節點上，如此一來便造成數據冗餘的現象。在惡意攻擊區塊鏈機制的情況下，網絡中的惡意使用者可以同時具有多重身份（持有大量節點），原來需要備份到多個節點的數據被欺騙地備份到了同一個惡意節點（該惡意節點偽裝成多重身份），這樣一來惡意的使用者就有可能掌握網絡的控制權。

圖 3 交易衝突



資料來源：Michele D'Aliessi(2016)

反女巫攻擊的方法有很多種，比如採用工作量證明機制，即讓每一個節點運用算力證明其影響力，這樣的方式將極大地增加攻擊成本，也是目前比特幣系統採用的方式。另一種方式則為權益證明(proof of stake, POS)，是影響力居次的以太坊(Ethereum)未來在棄用 PoW 共識之後將採取的證明模式。

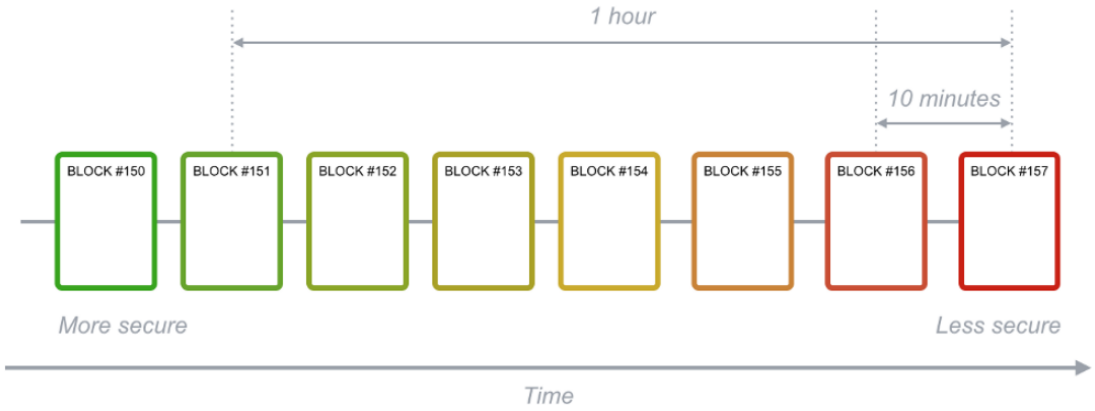
比幣系統防止女巫攻擊的方式，就是利用密碼學的哈希函數的工作量證明機制。

[3]女巫攻擊(Sybil Attack)，是一種在線網路安全系統威脅，是指個人試圖通過創建多個帳戶身份，多個節點或電腦坐標從而控制網絡。攻擊樣態包含直接通信、間接通信、偽造身份、盜用身份、同時攻擊或非同時攻擊等方式。

該惡意節點的解題速度必須高於網絡上所有的節點，才可能把包含取消交易的候選區塊放到鏈的尾端，等同於該惡意用戶必須與整個網絡上節點們競速，因為比特幣網路上有大量的節點，在確切的時間點假造多個區塊來進行攻擊是相當困難的。

比特幣網路的節點在即時發送交易後，平均需要 10 分鐘才可確認完成，並包含在區塊的尾端，而其中「確認」代表的意涵，即為「網路上有至少一個節點認可交易中未被花費的交易支出(UTXO)的合法性」。一旦交易被打包入區塊鏈中，它會被它後面的區塊所掩埋，後接區塊的工作量證明將呈指數增長，加強此共識並降低交易內容更動（如取消交易）的風險。

圖 4 區塊交易安全



資料來源：Michele D'Aliessi(2016)

一般而言，經過 6 個區塊確認後的交易結果已具備可信性並無法被逆轉。惡意節點必須控制強大的算力來追趕前一筆交易的確認速度，當落後 6 個區塊來追趕之前的交易時，將需耗費非常大的計算量。從經濟的角度考慮，擁有如此強大算力的節點並無誘因去追趕經 6 次確認的區塊，因在此過程中浪費的資源用來正經挖礦將可獲得更高的收益。

參、資本市場工具之應用

資本市場又稱長期資金市場，是金融市場的重要組成部分。資本市場的資金供應者為各金融機構，如商業銀行、儲蓄銀行、人壽保險公司、投資公司、信託公司等，需求者主要為國際金融機構、各國政府機構、工商企業、房地產經營商以及向耐用消費零售商買進分期付款合同的銷售金融公司等。而在全球化的趨勢下，投資活動亦趨於全球化，跨國交易日漸頻繁而重要。不同於單一市場或國內市場交易的結算交割運作模式，跨國結算交割涉及眾多的主體，其運作方式更是複雜多樣，必須透過新的風險管理機制以降低可能的風險。

應用區塊鏈系統，通過簡化交易後結算和清算流程，提高此市場的效率與安全性。通過減少對買方客戶、經紀商、自營商、信託託管銀行及存管信託公司(the depository trust & clearing corporation, DTCC)重複確認交易的行為，可以有效降低人工確認和對帳造成的成本與作業風險。此外，通過區塊鏈去中心化的特性，金融機構得不必再依第三方權威機構確認，可降低員工人數和後台辦公成本。美國機構研究指出，導入區塊鏈系統，將可節省約 20 億美元的外顯成本與機會成本。

多年來，金融市場內的清算和結算流程已有一定程度的簡化。但在交易和結算交易之前，交易雙方往往還需要在客戶、經紀商、存管信託公司和保管銀行之間，進行繁瑣的人工對帳和來回確認交易的細節。目前，在整個清算和結算過程中，資本市場金融工具交易時能有許多得改進之處：

1. 涉及不同版本的交易系統時：當跨國交易涉及多方參與者時，參與者各方可能使用不同系統或不同版本的交易確認模式。故在交易參與者各方對交易確認細節不一致時，必須使用人工介入確認，增加了成本與隱含的作業風險。

2. 結算過程耗時長：雖然股票交易成立所需時間甚短，但依照目前的系統，交易後續的結算及交割過程卻相當耗時（於美國股票市場的情況，2017 時為兩個工作日），結算過程耗時過長將造成資金空轉與流動性的問題。

3. 交割帳戶訊息或交易指示更動：在交易後，若發生帳戶訊息或交易指示更動等情況（如開立新戶或關閉舊戶、使用帳號變更、所有人變更等），導致需要增加確認流程和人工介入的情形，特別是使用常設交割指示(sanding sttlement instructions; SSIs)的狀況。

4. 作業風險：作業風險可能包括人為錯誤、行為不當、系統問題或不可預見的外部環境等因素所引起的風險，此風險可以通過區塊鏈技術進行交易前檢查來排除。

應用區塊鏈系統，可以控制資本市場交易行為中的清算和結算的成本，特別在減少或消除交易錯誤、簡化後台機制，縮短交割時間部分。

依照目前的交易實況，估計所有交易量中約有 10%以上的交易，將需要第三方機構與多方市場參與者之間的聯繫與溝通。經由人工介入的方式，雖然可使交易細節在不致重大問題的情況下解決，但是人工介入所產生的成本以及後續衍生的交易安全的問題，也是懸而未決的隱患。使用區塊鏈系統，將有關身分驗證與交易相關的訊息都記錄在每個區塊中，如此以來，各節點在讀取系統中所有串連的區塊時，可同時驗證並確認各筆交易的真實性，用此方式排除第三方機構或其他人工介入的問題。透過在節點參與系統時強制各節點執行定制協議的方式，亦可以消除常見的交易後錯誤(post-trade errors)，如錯誤的交割指示或錯誤的帳戶／交易明細。

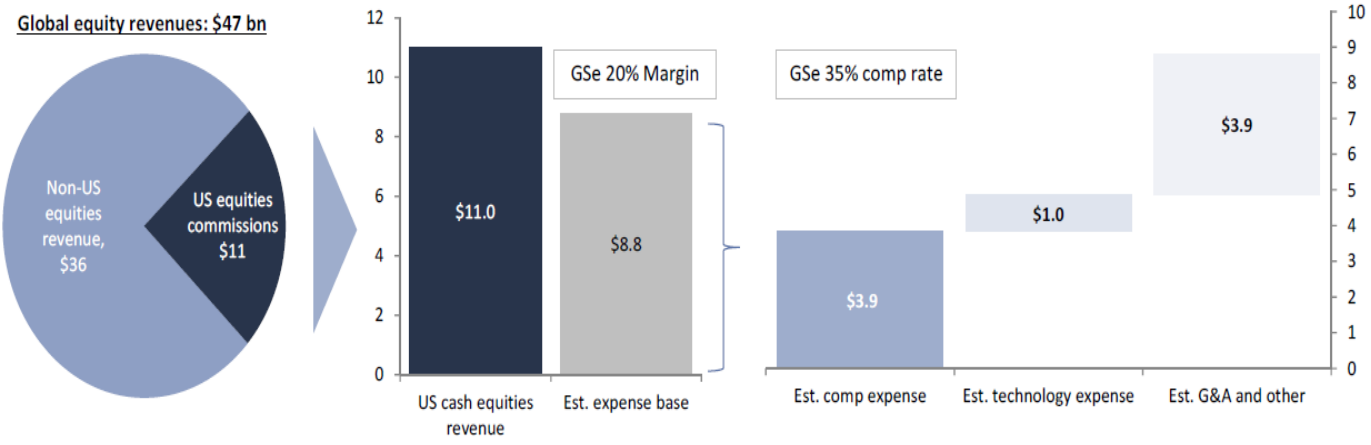
區塊鏈系統可利用其智能合約自動執行的特性，將這些在交易生命週期內必須反覆確認／認證的部分寫入智能合約，所有的採用此方式的市場參與者節點（包含存管信託公司、託管人、經紀商及客戶）在參與系統前，都將自動執行這些交易前的檢核

與驗證，以避免交易後的反覆確認的作業風險。

至於簡化後台機制與縮短交割的部分，通過區塊鏈系統，可以減少需求的人工數量、降低中台與後台機能在交易生命週期中的重要性，從而減少交易錯誤的發生及降低人工確認所衍生的問題，並降低整體交易的風險。

由全國 21 家央行市場業務資深官員組成市場委員會，所制定的全球外匯守則中，亦有針對交易的確認程序，做出參考的指導方針，「…市場參與者應在執行、修改或取消外匯交易後…使用自動化的交易確認比對系統，並在市場實務中區隔交易確認（後台）與交易執行（前台）的責任歸屬。市場參與者應盡可能地以安全的方式傳送交易確認，並鼓勵建立電子化自動交易確認機制，使用市場認可的標準化確認格式，進行各項外匯產品的交易確認。」應用區塊鏈系統，符合自動化比對交易、區隔各部分責任歸屬、安全的傳送的方式、與標準化的確認格式，皆是符合此指導方式下的一種解決對策。

圖 5 於資本市場使用區塊鏈之成本效益



資料來源：Goldman Sachs Global Investment Research(2016)

肆、洗錢防制(AML)計畫之應用

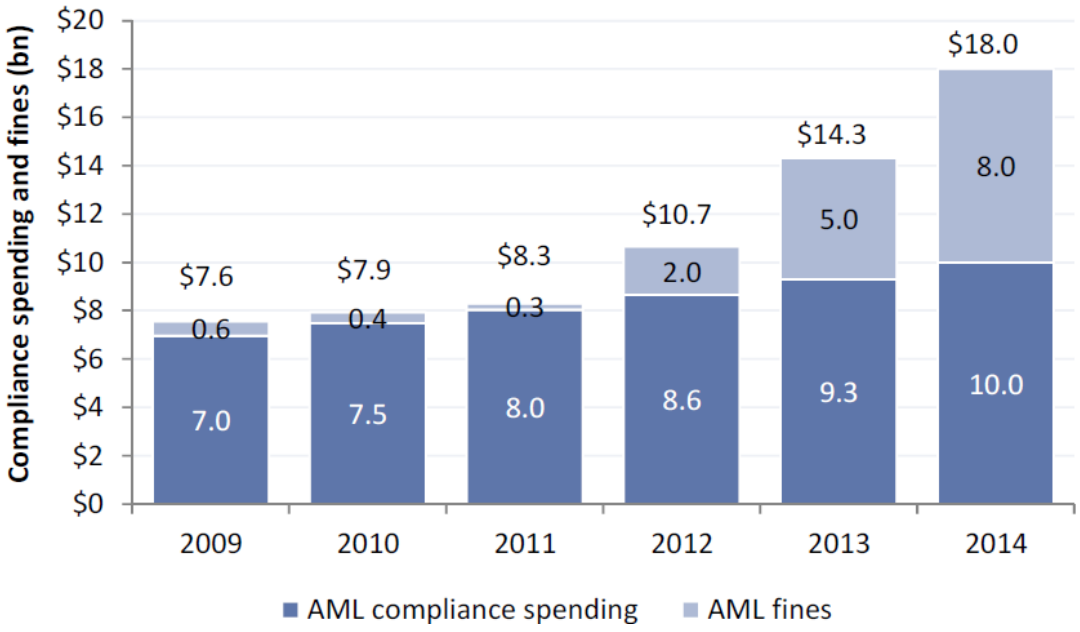
當前金融科技風潮席捲全球，全球金融機構大舉投入資金進入金融科技相關應用，期以防範金融犯罪(financial crime)的風險。金融犯罪所涉及之領域廣泛且複雜，包含舞弊及不當行為、網際網路犯罪，或金融產品或服務之作業流程等議題。而我國於 2018 年接受亞太防制洗錢組織(asia pacific group on money laundering, APG)第三輪相互評鑑，對台灣數家金融機構進行洗錢防制相關審查作業，包含防制洗錢、打擊資助恐怖主義、依其業務多樣性或重要性之客戶審查等。

將販毒或金融欺詐等非法活動所得之非法收益，藉由洗錢方式，使其看似來自合法的來源或活動，是目前國際金融體系中的不可忽視的嚴重問題。反洗錢的法規遵循支出，每年總計約可至 100 億美元。據世界銀行估計，洗錢交易的金額，每年約在 2.0 萬億至 3.5 萬億美元之間，約為全球 GDP 的 3~5%。

為了解決這個問題，全球經濟體的監管機構，皆為司法管轄區內的銀行內部反洗錢合規計劃制定了深遠的指導方針；儘管如此，第三方數據顯示，目前只有不到 1% 的洗錢活動被發現，亦使銀行因此遭受了嚴重的監管處罰。包括監管處罰在內，銀行承擔的洗錢防制法遵成本總額，約為每年 180 億美元，其中 2014 年的資料顯示，僅洗錢防制罰款總額就為 80 億美元。

利用區塊鏈相關的技術與系統，有機會可利用分散式帳本來共享金融交易信息，藉此簡化金融機構洗錢防制之監控程序，不僅可有效的同時施行監控與節省法遵成本，亦可利用於認識你的客戶(Know Your Customer, KYC)或客戶審查時實行。

圖 6 反洗錢防制合規費用與罰款逐年增加



資料來源：Goldman Sachs Global Investment Research (2016)

目前業界針對洗錢防制規劃所延伸的問題，多半屬於在實施洗錢防制時的高度勞動密集所引發的成本。為了遵守不斷發展的反洗錢法規，金融機構花費大量資源開發及維護自身的反洗錢合規計畫。建置相應的檢核系統，雖然可使銀行自動化了某些程序，但絕大多數的反洗錢預算都專門投入於手動審查可疑的支付交易，或審核新客戶合規與否的人員成本。目前銀行現有的系統所面臨的結構性問題如下，：

1. 金融機構間之間缺乏信息共享(mutualization)機制，致必須重複施行客戶審查工作。當開發了新客戶及建立新的客戶關係時，根據「了解你的客戶」規定，銀行必須進行徹底的客戶盡職調查(customer due diligence, CDD)流程，而在整套 CDD 流程中，KYC 的檢查通常是重複的。在大多數司法管轄區，即便某一帳戶已經被另一家銀行審查，其他銀行在與此客戶建立新關係時，亦必須獨立審查該帳戶，造成人工與時間上重複審查的資源浪費。
2. 因缺乏帳戶彙編機制，導致交易監控中明顯的誤報率。銀行依靠交易監控軟

件來檢測可疑的交易行為，而金融機構的合規人員，會再對所有支付交易的2~5%進行人工審查，以確認是否確實發生了洗錢事件。在這種情況下，在人工審查下的誤報率可達 99.9%。

由於這些因素，金融機構僱用大量人員來執行其反洗錢合規計劃。在客戶審查、交易監控和招聘人員等流程，估計相關造成的人員成本可達 AML 總預算的近 80%，而這些成本中的大部分，是由於金融交易對手之間可靠信息無法順暢地相互流動所造成，而導致必須要合規人員的人工介入來完善流程的進行。

而利用區塊鏈技術，將可改善目前反洗錢合規計畫的結構性問題，並簡化金融機構洗錢防制執行上的複雜程度。使用創新的分散式帳簿管理技術，可使資料儲存於分散的資料庫中，並藉此解決上述的幾點問題，增強訂定策略和執行程序的結合，並大幅地降低金融機構 AML 法遵成本。

此外，針對每個使用帳戶的相關詳細信息進行安全編碼，藉以提高交易監督機制的透明度和效率，通過彙整每一個參與支付交易帳戶的部分訊息，在不喪失帳戶信息完整性（如發送和接收方資訊、法律實體信息等）與保護機密資訊的安全性前提下，區塊鏈系統可以提高支付交易的透明度並降低誤報率，並可減少帳戶調節(reconciliation)流程、警示交易等活動所需的勞動力開銷。

而利用分散式帳本方式記錄過去已發生的所有交易，可以有效簡化帳戶使用、保管的記錄與事後審計的程序。金融機構可以利用以區塊鏈基礎的系統，取得每個客戶進行所有交易的歷史記錄、共享文件或其他法規允許之行為。區塊鏈系統中保持記錄最長鏈的特性，節點將自動追蹤與更新與特定客戶關聯的所有交易，使得該記錄可用於提供銀行依 AML 要求採取行動的規定，並能盡速符合其他監管要求。

可確保安全性的分散式帳本方式，亦有助於各個單位間重複的客戶審核工作。現行的作法下，每個金融機構都需要對開設的新帳戶進行KYC審查，藉此驗證個人帳戶、

公司帳戶或子實體帳戶間金流的來源和關聯性。與客戶建立長期關係的金融機構可以通過區塊鏈以促進資訊的安全，從而幫助客戶與其他機構的聯繫認證。雖然區塊鏈系統並不會完全消除其他金融機構的 KYC 負擔，但它可以減少重複性的人工步驟，並有效地降低客戶審查的成本。

通過簡化這些流程，區塊鏈可以幫助重新建置更有效洗錢防制實施流程。藉由保存資料更完整的詳細數據，以及提升儲存資料的可訪問性，大大降低依賴人工來進行 KYC 檢查和查核可疑的洗錢活動的情況，從而通過減少員工數來節省大量成本。除此之外，藉由區塊鏈技術提高交易對手風險的查核性，確定其交易不被用於促成洗錢、資恐或其他犯罪活動，藉此減少金融機構的罰款金額。

伍、小結

金融創新是在於新的生產函數的建立，亦為企業家對企業要素進行新的組合，導致生產函數或供應函數的變化，包含技術創新（產品創新與工藝創新）)與組織管理上的創新兩種。金融創新的動因，主要於順應供給與需求的變化、以及規避現有的法規架構管理。

經濟環境的變化，刺激了投資者對更高報酬率產品的需求，創造了一些能夠降低利率風險的新的金融工具，如 70 年代的可變利率抵押貸款(adjustable rate mortgages)、金融期貨交易(futures)和金融工具的期權交易(option trading)。而後電腦和通訊技術的改善，是導致金融市場內的供給條件發生變化，電腦技術被運用於大幅度地降低金融交易成本、及完全競爭市場下不可或缺資訊的公開透明化，更多新金融產品和新金融工具也因此產生，如改善金融市場運作機能的資產證券化(asset securitization)過程。而由於金融業較其他行業受到更為嚴格的管理，政府管理法規就成為這個行業創新的另外一股推動力量。當管理法規的某種約束可以合理地或被預設地予以規避，並可以帶來更高的收益，創新就會發生。

過度依靠創新科技之隱憂

2018 年 9 月，日本北海道發生震度 6.7 的強烈地震，除導致機場關閉、交通路線部分封閉之外，震災所致的停電亦使很多工廠和零售店等無法開工和營業，札幌證券交易所也停止了全部股票的買賣。除了對企業的對生產和物流造成打擊外，平日消費習慣以電子支付方式為主的北海道居民，亦面臨了即便帳戶有錢卻無法進行消費的窘境。而早在同年的 2 月，瑞典中央銀行的行長就對此提出警告。瑞典身為目前全球國

家裡全面推動貨幣電子化的先驅國家，其央行行長 Stefan Ingves 針對過度依靠金融科技之下的隱患，表示無現金社會在面對戰爭或天災時毫無抗性，在極端的狀況下，可能導致龐大的社會金融體系瞬間崩塌。

科技創新面臨的挑戰

在金融科技創新的應用中，區塊鏈系統目前遭遇的最大障礙，在於其共識算法、保密算法與智能合約方面等三項底層技術。現階段若欲發展其他更多的殺手級應用，系統架構者必須確保系統運作的順暢性與安全性：在一般性的金融交易中，系統必須能承受每秒處理幾千幾萬筆的交易量，同時並保證每筆交易成立的安全可靠性，雖然以上都只是金融交易最重要基本的要求，惟目前現行的區塊鏈系統仍還沒有辦法突破。

以台灣推行區塊鏈系統的現行狀況為例，目前推行區塊鏈技術兩大障礙，即為技術標準建立方面及相關法律制定方面的不足，區塊鏈的底層結構、標準體系、監管環境若不明確，實際上將很難明確的應用。技術與監管是相互促進、相輔相成的兩個力量，若技術本身沒有突破性的進展，將能難找到實際可應用的場景與業務、盈利模式。而監管機構針對新興科技創新領域的監管，也必須在考慮入新業務型態將衍伸的潛在風險下，同時具備靈活的特性。

此外，在處理新技術系統和現有業務系統兩者之間的替代關係，也是必須考慮的課題之一。金融創新科技的其中一個特性，就是在創新階段時通常需投入較大的成本，並可能需要一定的時間之後才能回收。以區塊鏈系統為例，架設區塊鏈系統、節點、分散式帳本的架設，甚至是存儲的資源大量膨脹甚至浪費的問題，都是龐大的前期投入成本。

監管機構的反思

區塊鏈面臨的另外一個難題與挑戰，在於監管機構的立場。技術與監管是相互促進、相輔相成的兩個力量，金融科技創新業務的快速發展也帶來了一系列的監管問題，監管機構在該領域，由於沒有先例，很容易陷入「手中鳥，捏緊了怕牠死掉，鬆手又怕牠飛走」的窘境。

各國監管機構對於金融科技創新的監管態度不一，如針對虛擬貨幣的監管上，亞洲鄰近國家中南韓基於業者壓力，最終開放了比特幣小額跨境匯款業務；日本金融廳則依 2017 新版的支付服務法將虛擬貨幣業者納入監管，並免徵消費稅；新加坡金管局則表明監管首次代幣眾籌(ICO)的立場。而美國則為首個發給虛擬貨幣衍生性商品交易之結算執照的國家，相較於歐盟則草擬規範將虛擬貨幣交易所納入洗錢防制。

而目前數位時代的典型問題，任何現有的框架都無法適切的套用這項破壞性的新技術。主管機關針對於創新方面的資訊或尚未理解，亦欠缺可以做到有效監管的資源。紐約州金融署代理署長 Benjamin M. Lawsky 就曾說過，「了解的越多，就對這項技術越感興趣，如果能把監管的事情做對…避免過度束縛的監管，就有機會幫助這項有用的技術，為我們的體制帶來改進。」

是故，各國央行、監管機構、立法部門和金融機構等相關市場參與者，需展開持續深入的研究與合作，並根據應用領域的實際情況，建立適當、有效的法律框架。主管機關若能避免缺乏因應快速變遷世界訣竅的問題，尋求網路中其他利益關係人，及全球各主管機關的意見交流，再扶持業界技術創新發展的情況下，共同研議重要的領導課題、合作推薦議程，才是解決此難題的最佳做法。

陸、參考文獻

1. Nakamoto Satoshi(2009), “Bitcoin: A Peer-to-Peer Electronic Cash System.”
2. Michele D'Aliessi(2016), “How Does the Blockchain Work?”
3. Markus Jakobsson(1995-2014); Juels, Ari. “Proofs of Work and Bread Pudding Protocols. Communications and Multimedia Security (Kluwer Academic Publishers). 1999: 258–272.”
4. Rob Jesudason, Block.one President(2018), “How Blockchain Offers an Answer to Banks’ KYC and AML Issues.”
5. Goldman Sachs Group, Inc(2016), “Blockchain: Profiles in innovation, putting theory into practice.”
6. Don Tapscott, Alex Tapscott(2017), “Blockchain Revolution:How the Technology Behind Bitcoin is Changing Money, Business, and the World”
7. 2018 上海區塊鏈互聯網金融應用研討會會議議題(2018)
8. 上海財經大學學報：金融創新與道德風險控制，郝雲(2009)