國立臺灣大學社會科學院經濟學系在職專班

碩士論文

Mid-Career Master Program

Department of Economics

College of Social Sciences

National Taiwan University

Master Thesis

我國證券及期貨市場應用區塊鏈技術之探討

A Study on the Application of Blockchain Technology in Taiwan's Securities and Futures Markets

林雅苓

Lin, Ya-Ling

指導教授：李顯峰 博士

Advisor: Lee, Hsien-Feng, Ph.D.

中華民國 106 年 1 月

January, 2017

doi:10.6342/NTU201700214

國立臺灣大學碩士學位論文
口試委員會審定書

我國證券及期貨市場應用區塊鏈技術之探討

A Study on the Application of Blockchain Technology in Taiwan's Securities and Futures Markets

本論文係林雅苓君（學號 P03323002）在國立臺灣大學經濟學系在職專班完成之碩士學位論文，於民國 106 年 1 月 18 日承下列考試委員審查通過及口試及格，特此證明

口試委員：李顯峰（指導教授）

陳正倉

林惠玲

doi:10.6342/NTU201700214

誌　謝

看著手中的臺大碩士學生證，終於，我要把它換成校友證了。

一路上，要感謝的人好多，首先要感謝我親愛的老公源楷，在我需要苦讀時，支持著我念書的決心，獨自照顧我們的一對兒女，讓我能兼顧工作與學業。還有我可愛的一對寶貝棋涯與曉潔，雖然對於我要去圖書館念書感到不捨，但仍然支持我，並在我疲憊時，給予我最深、最貼心的擁抱，給我力量。還要感謝我的婆婆秋香，支持我並參與我的畢業典禮，與我一同分享這份榮耀，還有我前年往生的公公沐仁，在生時亦給予我最溫暖的鼓勵。另外還有我最親愛的爸爸、媽媽、姊姊們，總是對我噓寒問暖、給我支援，謝謝你們，家庭是我最深的依靠。

此外，要非常感謝這次接受我訪談邀約的臺灣證券交易所黃乃寬副總經理，以及臺灣大學資工系廖世偉教授，兩位高階專業人士，願意在百忙之中撥冗、接受一名渴求知識的學生訪談請託，在訪談的過程中，給予我最熱切的解說，讓我對區塊鏈技術有了更深的瞭解，對於商業運作本質－信任的認知，也更加根深蒂固，給予我最重要也最深刻的知識，並使我的論文除了理論架構外，亦能透過實務面進行完整的探討。

本次論文能夠順利完成，最要感謝我的指導教授李顯峰博士，指引我論文寫作的方向，對於我的論文提供寶貴的意見，大至內容與架構、小至寫作格式，都給予耐心與細心地指導，使我獲益良多。老師對於區塊鏈技術有深入的瞭解，亦舉辦並主持區塊鏈主題之座談會，邀請區塊鏈技術與金融業專家進行與談，使我在撰寫如此新穎的研究題目時，給予我最明亮的指引，能夠請李老師擔任我的指導教授，是我就讀台大經濟系碩士的最大幸運。

這次口試非常榮幸能夠邀請到陳正倉教授與林惠玲教授擔任我的口試委員，並給予我親切的指導，以及溫暖的鼓勵，透過與教授們問答的過程中，使我論述

doi:10.6342/NTU201700214

區塊鏈技術的邏輯架構更加精進。

身為一名母親，要同時兼顧家庭、工作與學業，蠟燭三頭燒的情況下，非常需要好同學，非常幸運地，我遇到了利真與君怡同學，讓我在求學的過程中，考試與報告皆能順利、愉快地通過，只能說三個臭皮匠、勝過一個諸葛亮呀。還有全班同學，讓我在求學的過程中，享受著求知的過程、充滿樂趣。

經過這麼多年，還能夠回到校園，完成我的臺大夢，並深入研究一個我渴求瞭解的主題—區塊鏈技術，要感謝的人真的太多了，謝謝公司長官、同事在工作上的支持與鼓勵，家庭給我的依靠，以及學校教授與同學的指導與協助，謝謝大家。

doi:10.6342/NTU201700214

摘　要

近年來，金融科技蔚為顯學，其中的區塊鏈技術更被喻為第四次工業革命創新科技的中心。區塊鏈技術是一種分散式帳冊技術，不同於現今的網際網路是資訊的傳遞，區塊鏈技術可以做到價值的傳遞，擔任過去金融中介機構信任的角色，故又稱為信任機器。

本研究先以較為人所熟知的比特幣，進行區塊鏈技術的簡介。但由於比特幣的區塊鏈技術並不完全適用於高度監管的證券及期貨業，故我們建議可以採用不同的技術方法，例如採用私有鏈、運用智能合約、納入監管單位為節點、運用於洗錢防制等作業，並可提升法遵科技之應用效率，使得區塊鏈技術與證券及期貨業的作業能相輔相成，達到簡化交易後之結算交割流程。區塊鏈技術可降低作業成本，再加上可全年無休及跨國特性，預期可推升我國證券及期貨之交易量，達到活絡我國資金流通之效果，進而繁榮實體經濟。此外，本研究亦探討新科技將能促使我國工作數量增加，並達到產業升級、提高我國競爭力之效果，惟該工作轉型過程將是一場嚴格的考驗。

我們亦檢討了區塊鏈技術尚面臨著法規面、速度面，以及實證面之挑戰，並提出政府、業界與學界如何透過合作，使產官學達到三贏綜效之建議。本研究亦訪談業界專家，以瞭解實務面的觀點，以及區塊鏈技術刻正面臨以太坊的 DAO 硬分岔事件等現實挑戰。本研究針對證券及期貨業應用區塊鏈技術的理論面與實務面，進行完整的探討與建議。

關鍵字：區塊鏈、分散式帳冊技術、證券及期貨、結算及交割、法遵科技、金融科技、交易量。

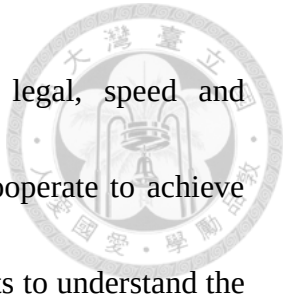
doi:10.6342/NTU201700214

Abstract

Recently FinTech becomes a school, in which blockchain technology has hailed as the center of the fourth industrial revolution. Today's Internet is for the transmission of information, while blockchain technology is a distributed ledger technology, and can transmit values, like the trusty role of financial intermediaries in the past. Thus, it is also known as a Trust Machine.

In this paper, we introduce the blockchain technology with bitcoin. However, blockchain technology of bitcoin cannot be fully applicable to the highly regulated securities and futures industry, it is suggested to adopt different technical methods such as the use of the private blockchain, the use of smart contracts, the incorporation of the supervisory unit as a node, enforcement in anti-money laundering. It can improve the efficiency of RegTech, making the complement between the securities and futures markets operations, and simplifying the post-trade clearing and settlement process. It can reduce the operating costs, coupling with the 24/7 and transnational characteristics. And it is expected to increase the trading volume of Taiwan's securities and futures in Taiwan, and then enhance the real economy. In addition, the study will explore the new technology that could be able to increase employment and enhance Taiwan's competitiveness. But the transformation process will be a rigorous process.

doi:10.6342/NTU201700214



Blockchain technology is facing the challenges from the legal, speed and operational aspects. The government, industry and academia can cooperate to achieve win-win synergies goal. This study also interviewed industrial experts to understand the practical aspects, as well as the challenge from Ethereum DAO hard-fork.

Keywords：Blockchain, Distributed Ledger Technologies (DLT), Securities and futures, Clearing and settlement, RegTech, FinTech, Trading volume

doi:10.6342/NTU201700214

目　錄

doi:10.6342/NTU201700214

doi:10.6342/NTU201700214

圖　目　錄

doi:10.6342/NTU201700214

表 目 錄

doi:10.6342/NTU201700214

第一章　緒論

1.1 研究動機與背景

金融業為國家各產業發展之根基，根基不穩，各產業難以茁壯，而透過金融業的資金流通，使得各產業得以健全發展。反之，金融業若發生弊案，將使國內經濟動盪不安，而現今國際金融流通發達，更將引爆全球金融危機。

以 2008 年的雷曼事件為例，雷曼兄弟控股公司 (Lehman Brothers Holdings Inc.) 係於 1850 年創辦的國際金融機構及投資銀行，更被美國《財富雜誌》選為財富 500 強公司之一，為當時美國第四大投資銀行。2008 年中，受到次級房貸風暴連鎖效應波及，在財務方面受到重大打擊而虧損，致使股價甚至下跌到低於一美元，陸續裁員六千人以上，並尋求國際間的金主進駐。2008 年 9 月 15 日，在美國財政部、美國銀行及英國巴克萊銀行相繼放棄收購談判後，雷曼兄弟公司宣布申請破產保護，負債達 6,130 億美元，其發行的連動債 (信用違約交換，Credit Default Swap，即 CDS) 價值暴跌，進而引發全球金融風暴。過去美國金融機構曾稱為信任企業 (Trust Company) ，但經過多次的金融風暴後，人們對於銀行等金融體系已產生信任感的動搖。

就在金融風暴的同 (2008) 年，中本聰 (Satoshi Nakamoto) 發表了一篇「比特幣：一種點對點的電子現金系統」 (Bitcoin:A Peer-to-Peer Electronic Cash System) 的論文，即論述透過區塊鏈技術產生的一種電子貨幣。隔 (2009) 年，比特幣的創世區塊 (Genesis block，即區塊鏈的第一個區塊) 誕生。

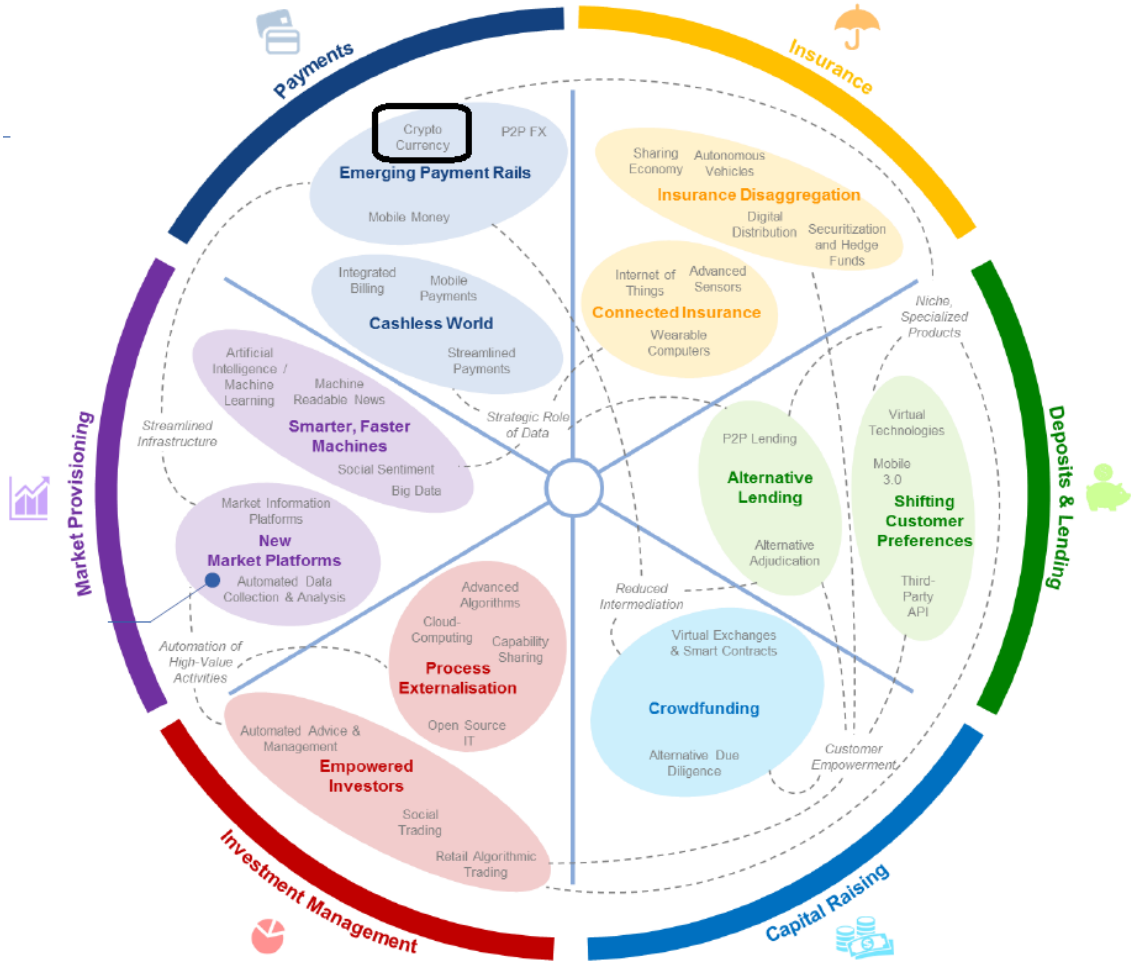
比特幣是一種透過去中心化的分散式帳冊技術，加上雜湊算法使其交易紀錄不可竄改的加密電子貨幣。《經濟學人雜誌》(The Economist) 於 2015 年 10 月 31 日的雜誌封面，將該技術喻為「信任機器」，而其副標題為「比特幣背後的技術將改變經濟的運作」，該期雜誌並以「確保萬物的巨大鎖鏈」專題報導區塊鏈技術。

doi:10.6342/NTU201700214

除了期待金融業再度成為信任企業，我們亦渴求金融業能提升服務品質、更加人性化，帶給人們更便利而美好的生活。透過科技發展，金融業才能不斷升級，而金融 (Finance) 和科技 (Technology) 兩者的結合，創造出「金融科技」(FinTech) 新名詞。依據美國賓州大學華頓商學院 (Wharton School) 成立的華頓金融科技俱樂部 (Wharton FinTech Club) 對金融科技所下的定義，其係指一群企業運用科技手段使得金融服務變得更有效率，因而形成的一種經濟產業。

2015 年 6 月的世界經濟論壇 (World Economic Forum, WEF) ，即對「金融服務的未來」提出報告。該報告以「破壞性金融服務創新」 (詳見圖 1) 刻畫出金融科技可能帶來的明日金融環境樣態。圖 1 中的圓，在 11 點鐘方向「支付」(Payments) 中的「新興支付」 (Emerging Payment Rails) ，其項下的「加密電子貨幣」(crypto-currency，詳見圖 1 黑框處) ，即係以加密電子貨幣比特幣為代表之區塊鏈技術。

doi:10.6342/NTU201700214



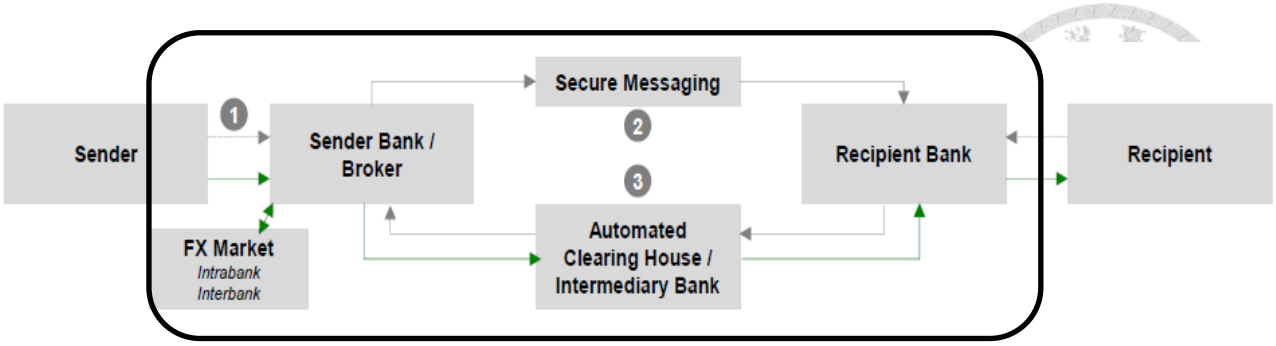
資料來源：WEF (2015.6)

圖 1　破壞性金融服務創新[1]

依據 WEF 報告 (2015.6) 指出，現行支付流程 (詳見圖 2) 需要透過許多中介機構 (詳見圖 2 黑框處) 的移轉，才能完成一筆簡單的交易，但透過分散式支付網路 (詳見圖 3) ，則能利用密碼協議以近乎安全、低成本、接近瞬時的方式，迅速完成價值的傳遞。這種分散式支付協議的實現正是比特幣網路，而其背後的基礎正是本研究所熱切探討的區塊鏈技術，而區塊鏈技術的應用，絕不僅於支付或貨幣。

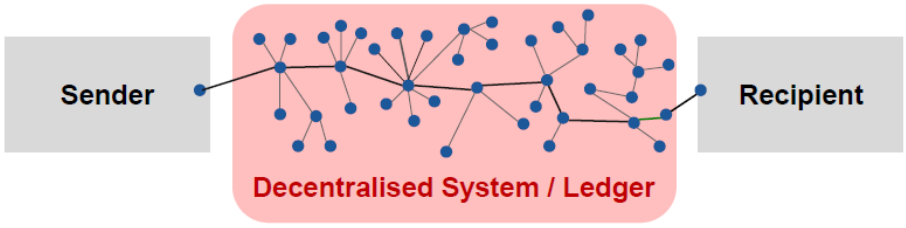
[1] 從11點鐘方向開始順時針端看，分別為支付 (Payments) 、保險 (Insurance) 、存貸 (Deposit & Lending) 、籌資 (Capital Raising) 、投資管理 (Investment Management) 和市場資訊供給 (Market Provisioning) 。

doi:10.6342/NTU201700214



資料來源：WEF (2015.6)

圖 2　現行支付流程圖



資料來源：WEF (2015.6)

圖 3　分散式支付網路圖

依據 WEF 報告 (2015.9) 指出，其預期 2027 年全球 10%的 GDP 將儲存在區塊鏈技術內。2016 年 1 月 20 日，在瑞士達沃斯 (Davos) 舉辦的 WEF 年會，創辦人兼執行主席施瓦布 (Klaus Schwab) 指出，在人類眼前面臨的諸多挑戰中，其認為最艱鉅的，就是如何了解和應對第四次工業革命[2]，包括物聯網、3D 列印、人工智慧、無人駕駛車輛、機器人等令人驚嘆的創新，施瓦布更將區塊鏈喻為第四次工業革命的中心 (詳見表 1)。

[2] 第一次工業革命係蒸汽動力、棉紡織和鐵路的問世，帶來機械生產。第二次工業革命是組裝生產線和電力普及，帶來大量生產。第三次工業革命就是電腦革命，帶來電腦與網際網路。

doi:10.6342/NTU201700214

表 1　工業革命演進歷史

工業革命	重點	項目
第 1 次工業革命	機械生產	蒸汽動力、棉紡織和鐵路
第 2 次工業革命	大量生產	組裝生產線和電力普及
第 3 次工業革命	電腦革命	電腦與網際網路
第 4 次工業革命	創新科技	區塊鏈技術、物聯網、3D 列印、人工智慧、無人駕駛車輛、機器人

資料來源：吳怡靜 (2016)，經本研究整理。

除了國際重視區塊鏈技術的重要性，我國金融監督管理委員會亦為推動科技創新金融服務，並促進金融科技產業發展，於 2016 年 5 月完成「金融科技發展策略白皮書」(下稱白皮書) ，希望推動資通訊業與金融業跨業合作，達成充分運用資通訊科技，打造智慧金融機構，創新數位便民服務，強化虛擬風險控管的發展藍圖。前揭白皮書中，即將區塊鏈列為 11 項應優先發展或強化項目之一[3]。

區塊鏈技術的發展，除了可以帶給人們更便利的金融服務，亦希望能利用這項新工具，改變金融業近年來引人詬病的弊端。

美國商品期貨交易委員會 (CFTC) 委員 J. Christopher Giancarlo 在 DTCC 的 2016 區塊鏈座談會中表示，如果 2008 年有準確的分散式帳冊技術紀錄，可用於掌握雷曼的所有交易，那麼監理機構即可辨識其交易活動的異常，更快地對其信譽惡化作出反應。或即使不足以預防雷曼事件，亦能在其申請破產時的數分鐘內，掌握其曝險值，進而加快結算其未平倉部位及帳戶，而非耗時數年。

對照我國金融弊案的發生，例如 2016 年 7 月的第一銀行 ATM 駭客盜領案，

[3] 該11項應優先發展或強化項目，分別為電子支付、銀行業、證券業、保險業、虛擬整合金融服務、法規調適、風險管理、人才培育、創新創業、區塊鏈、身分認證等。

doi:10.6342/NTU201700214

以及 8 月份的兆豐銀行紐約分行因疑似洗錢申報作業未依規定辦理，違反洗錢防制法，遭美國紐約金融服務署 (DFS) 裁罰 1.8 億美元 (約新臺幣 57 億元) 案，亦可望透過區塊鏈技術改善相關問題。

1.2 研究目的與架構

因此，本研究的目的係希冀透過瞭解區塊鏈技術的背後原理，進而延伸至如何改進我國金融市場的效率與安全性，並針對國內證券及期貨市場如何引用相關技術，達到節省結算交割費用、提高款券撥轉時效、降低洗錢防制成本等，探討我國證券及期貨市場應用區塊鏈技術之相關效益。

本研究的章節安排如下，第一章為緒論，敘述本研究的研究動機與背景，以及研究目的；第二章為區塊鏈技術最成熟的應用—比特幣，由於比特幣的崛起，使得世人注意到其背後的區塊鏈技術；第三章為比特幣背後的區塊鏈技術，進行區塊鏈技術的基本介紹；第四章為區塊鏈技術於國內外的應用案例，列舉國內外較知名或具規模之應用單位；第五章為區塊鏈技術在我國證券及期貨業之應用探討，先簡介我國證券及期貨市場的交易結算制度，再論述應用區塊鏈技術之預期效益，並提出相關建議與有待加強之處；第六章為區塊鏈技術對我國經濟之影響與建議，條列區塊鏈技術對我國經濟之可能影響並提出建議方案；第七章為結論與檢討。

doi:10.6342/NTU201700214

第二章 區塊鏈技術最成熟的應用－比特幣

要說明區塊鏈技術，最佳的範例就是比特幣 (bitcoin) 。比特幣是一種全球通用的加密電子貨幣 (crypto-currency) ，由 bit 和 coin 兩字所組成的新名詞，bit 是位元，即資訊的最小單位，coin 是錢幣，意喻其為一種貨幣，實際上比特幣創始時並沒有發行實體硬幣或紙鈔。

2.1 交易方式的演進

比特幣是一種加密電子貨幣，以交易為初始目的。而經濟活動即係自交易開始，從一開始透過面對面進行以物易物，提升了交易雙方效益，隨著交易內容豐富化、複雜化，人類陸續發明了商品貨幣、金屬貨幣、紙鈔、電子貨幣等，現行已進展到無實體化的加密電子貨幣—比特幣 (詳見表 2)。

表 2　交易的演進過程

階段	交易方式	內容
第一階段	以物易物	只能面對面、且一物換一物，便利性低，且選擇性少
第二階段	商品貨幣	選擇性變多，但商品貨幣本身不易攜帶，例如貝殼及金銀貴金屬等
第三階段	紙鈔	較商品貨幣攜帶方便，但易損壞
第四階段	電子貨幣	信用卡
第五階段	加密電子貨幣	無實體化的比特幣

資料來源：本研究整理

隨著貨幣發明後，由於貨幣具有四大功能，分別為交易的媒介、記帳的單位、儲存的價值，以及延期支付的標準，使得交易的選擇更多了，但也由於人們是自私的且有限理性的，使得人與人之間無法完全信任對方，因此需要一個具有公信

doi:10.6342/NTU201700214

力的第三方中介者撮合交易，使雙方履行買賣約定行為，而第三方中介者的服務費用即是交易時所需支付的額外成本，例如銀行的手續費，以確保雙方交易的安全性與成功，也使得金融體系越加複雜。

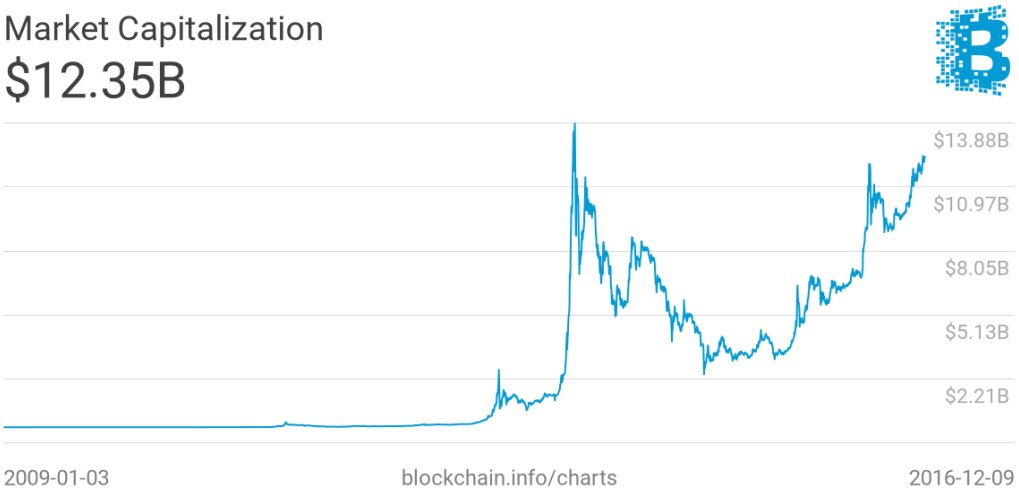
金融機構之所以能夠擔任交易行為的中介角色，即是其具有令人信任的功能。由於全球化的關係，交易雙方不再侷限於熟識的親友，陌生人之間如何在瞬間建立彼此的信任關係，就是透過雙方信任的金融機構才能立刻進行金錢與商品的交付移轉，也因此透過第三者中介機構必須付出高昂的手續費用成本，又隨著金融體系越來越複雜的運作，金錢的傳遞需要耗費許多時間。

2.2 比特幣的爆紅

比特幣並非任一特定機構所發行之貨幣，而是經由區塊鏈技術，透過挖礦的過程產生的一種全球通用的加密電子貨幣，比特幣使用者可以透過電腦、手機等方式，利用電子錢包來交易比特幣、或其他商品及服務等。與各國央行發行之法定貨幣不同，比特幣係採點對點技術、去中心化的網際網路體系的區塊鏈技術所開發，不屬於任何特定機構發行之貨幣。正由於比特幣並非各國政府所發行的法定貨幣，故目前尚有許多國家政府並未承認其合法性。

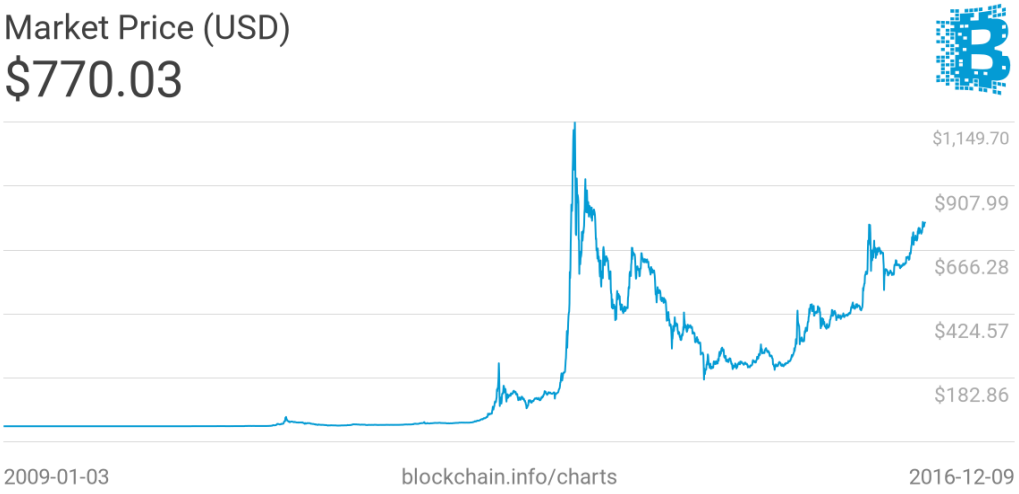
截至 2016 年 12 月 9 日，比特幣總市值已經高達 123.5 億美元 (詳見圖 4) ，當日一枚比特幣市值為 770 美元 (詳見圖 5，約當新臺幣 23,100 元，以匯率 30 元臺幣兌換 1 美元計算，以下亦同) 。一枚比特幣之最高價曾於 2013 年 12 月 5 日達到美金 1089.09 元 (詳見圖 6，約當新臺幣 32,672 元) 。比特幣並非由任何政府單位或認證機構所核發之貨幣，理論上其本身是沒有價值的，但因眾人對其具有信心，使其有了價格，且其竟能在短短數年間，價格高漲，更引發了世人對於比特幣好奇心。但從比特幣市價圖 (詳見圖 5) 可以看出，比特幣價格波動極大，這也是比特幣未來必須解決的問題之一。

doi:10.6342/NTU201700214



資料來源：blockchain.info，2016.12.9 查詢

圖 4　比特幣總市值



資料來源：blockchain.info，2016.12.9 查詢

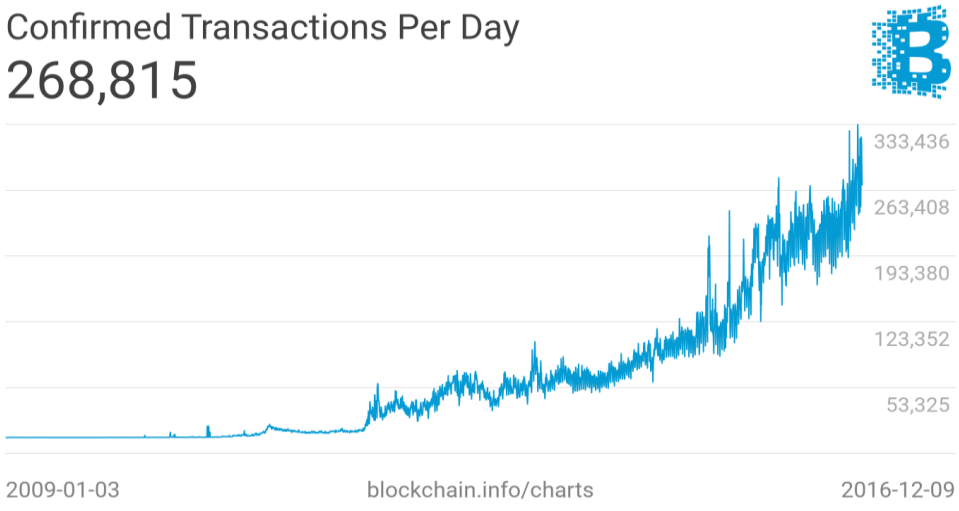
圖 5　比特幣市場價格

doi:10.6342/NTU201700214

資料來源：maicoin.com，2016.8.15 查詢

圖 6　比特幣市場價格最高處

隨著比特幣多年來的運作尚稱順暢，越來越多人利用比特幣進行交易活動，例如美國購物網站 Amazon.com 及國際旅遊網站 Expedia.com 等，使比特幣交易量也日益增加。從圖 7 可以看出比特幣自 2009 年來的使用率快速增長，單日交易量已高達 30 萬餘筆。



資料來源：blockchain.info，2016.12.9 查詢

圖 7　比特幣交易量

除了比特幣之外，亦有其他機構利用區塊鏈技術，發展出更多加密電子貨幣，表 3 是目前總市值前十名的加密電子貨幣。以總市值來說，比特幣仍佔據加密電

doi:10.6342/NTU201700214

子貨幣榜首，其次為以太坊，第三名為瑞波幣。而在加密電子貨幣的市場價格中，比特幣亦為最高者。

表 3　加密電子貨幣總市值排行榜

#	Name	Market Cap	Price	Available Supply	Volume (24h)
1	Bitcoin	$12,320,891,300	$768.32	16,036,062 BTC	$56,013,700
2	Ethereum	$710,215,561	$8.18	86,803,999 ETH	$8,642,010
3	Ripple	$244,424,636	$0.006791	35,994,609,608 XRP *	$1,438,720
4	Litecoin	$178,631,399	$3.66	48,826,804 LTC	$1,682,530
5	Monero	$106,017,770	$7.84	13,521,347 XMR	$1,276,440
6	Ethereum Classic	$78,570,934	$0.905930	86,729,586 ETC	$1,100,990
7	Dash	$62,521,315	$9.00	6,946,465 DASH	$883,304
8	Steem	$48,482,575	$0.214408	226,122,977 STEEM	$93,042
9	Augur	$34,118,040	$3.10	11,000,000 REP *	$328,206
10	NEM	$30,532,770	$0.003393	8,999,999,999 XEM *	$31,247

資料來源：coinmarketcap.com，2016.12.9 查詢

比特幣這幾年來的爆紅，引發眾人對其背後的區塊鏈技術好奇，由於比特幣美好地展現了區塊鏈技術的信用機制、加密技術，以及價值移轉的應用，使得全球高端金融機構爭相追求研究。另一方面，由於比特幣的去中心化特性，威脅了法定貨幣發行單位的地位，挑戰了各國央行的底線，故目前在貨幣發行的發展上，比特幣等加密電子貨幣尚有疑義。比特幣與法定貨幣之差異比較表，詳見表 4。

doi:10.6342/NTU201700214

表 4　比特幣與法定貨幣的比較

項目	比特幣	法定貨幣
發行來源 (信任對象)	區塊鏈技術設計，由礦工運算產生	政府發行、中央銀行印製
貨幣價值	兩者之價值來自擁有者相信貨幣擁有購買力，但貨幣本身並無內在價值，但兩者相信的對象 (見上欄位：發行來源) 不同	
儲存方式	比特幣錢包，匿名制	銀行帳戶，實名制
使用方式	透過網際網路使用	現場使用
真偽辨識	以密碼學驗證	以防偽特徵辨識
耐久度	純數位資料，可永久保存	實體紙幣或硬幣，有使用年限，舊幣會收回並重新發行
面額	可以表示至小數點後八位	依發行所定單位，即紙鈔及硬幣面額
第三方擔保	無	由政府發行債券或儲藏黃金
總量控制	系統已預先設計限量發行	由政府與中央銀行等中央體系決定，可無限發行

資料來源：黃詠淳 (2014)，經本研究整理並新增項目

區塊鏈技術使得比特幣等加密電子貨幣順利發展，比特幣的順利運作亦使區塊鏈技術受到世人矚目，兩者相輔相成，而現今區塊鏈技術的其他應用正如火如荼地發展中。

doi:10.6342/NTU201700214

第三章 比特幣背後的理論基礎－區塊鏈技術

網際網路在 1983 年 TCP/IP 協議的標準制定後蓬勃發展，實現了全球高速度、低成本的資訊互聯網，其高效率地複製與傳播資訊，發展成為資訊爆炸的時代，滿足了全球對資訊的渴求，稱為網際網路 1.0 時代。但網際網路 1.0 是資訊複本的傳遞，但應用在金融資產的交易運作上，資產複本的傳遞是沒有意義的，故資產移轉仍然必須透過可信任的金融機構擔任中介者。

2009 年比特幣出現了，由於其解決了重複支付問題，使得線上移轉資產成為可能，其背後的區塊鏈技術正是網際網路的升級版，即網際網路 2.0，亦稱為比特幣 2.0，這使得網際網路能從「資訊互聯網」，進階成為「價值互聯網」，舉凡數位貨幣、數位金融資產之移轉都能實現。

3.1 區塊鏈技術的前身

區塊鏈技術並非一夕誕生，而是累積了過去數十年來跨領域的技術整合，克服各項技術不足之處，才產生的新科技。1996 年 Adam Back 提出雜湊現金 (Hashcash) ，其為一種工作量證明演算法 (Proof of Work, POW) ，此演算法最早被應用於阻擋垃圾信件，而後被改造為比特幣區塊鏈的安全關鍵技術之一，即挖礦行為；1982 年 David Chaum 推出注重隱私的密碼學網路支付系統 eCash，由於其具有不可追蹤的特性，成為比特幣區塊鏈技術在隱私安全上的雛型，但不同的是，其並非去中心化的系統；1985 年，Neal Koblitz 和 Victor Miller 提出橢圓曲線密碼學，建立了公開金鑰加密的演算法，發展歷史詳見表 5。

doi:10.6342/NTU201700214

表 5　區塊鏈技術的前身

西元年	區塊鏈技術的前身	特性
1996 年	Adam Back 提出雜湊現金 (Hashcash)	一種工作量證明演算法，此演算法最早被應用於阻擋垃圾信件，而後被改造為比特幣區塊鏈的安全關鍵技術—挖礦行為
1982 年	David Chaum 推出密碼學網路支付系統 eCash	具有不可追蹤的特性，成為比特幣區塊鏈技術在隱私安全上的雛型，但其並非去中心化的系統
1985 年	Neal Koblitz 和 Victor Miller 提出橢圓曲線密碼學	建立了公開金鑰加密的演算法

資料來源：辜騰玉 (2016)，經本研究整理

在前人提出多項技術後，中本聰於 2008 年發表一篇論文，改良並結合前揭多項技術後，提出比特幣想法，而後於 2009 年比特幣的創世區塊誕生。隨著使用比特幣的人數與交易量的增加，比特幣機制也越加成熟，雖然這幾年比特幣的合法地位一直爭議不斷，價格也大幅波動，但也由於這些不同的意見，讓大家漸漸注意到比特幣背後區塊鏈技術的重大意義與價值，除了前揭許多加密電子貨幣的陸續開發之外，也將區塊鏈技術推展到加密電子貨幣之外的領域。

依據區塊鏈科學研究所 (Institute for Blockchain Studies) 創始人梅蘭妮·斯萬 (Melanie Swan) 所撰寫之《 Blockchain: Blueprint for a New Economy》 (中文暫譯為區塊鏈：新經濟藍圖) ，提出區塊鏈發展可分為三階段，區塊鏈 1.0 係貨幣 (currency) ，即利用區塊鏈技術為基礎，開發出來的比特幣等電子貨幣，其係具備加密特性之數位貨幣或支付系統；區塊鏈 2.0 為智能合約 (contracts) ，即能自動執行合約條款的電腦程式，主要應用領域為金融資產交易活動，例如證券及期貨

doi:10.6342/NTU201700214

之交易等；區塊鏈 3.0 為超越貨幣、經濟及市場的公正應用 (Justice Applications Beyond Currency, Economics, and Markets) ，其係更複雜的智能合約應用，主要運用在社會活動上，例如政府稅收、醫療、慈善事業等 (詳見表 6)。

表 6　區塊鏈技術的發展三階段

階段	特色	應用範圍	發展階段
區塊鏈 1.0	具備加密特性之數位貨幣或支付系統	虛擬貨幣，例如比特幣	最成熟
區塊鏈 2.0	智能合約	金融資產交易活動，例如跨國匯款、證券及期貨之交易等	尚在研究中
區塊鏈 3.0	可編程經濟	社會活動，例如政府稅收、醫療、慈善事業等	尚在研究中

資料來源：Swan Melanie (2015)，經本研究整理

由於比特幣自 2009 年即已出世，故現行區塊鏈 1.0 於數位貨幣之應用為最成熟，但由於其與法定貨幣之地位有競爭關係，造成爭議問題。而區塊鏈 2.0 則為探討金融交易活動，例如跨國匯款、證券及期貨之交易行為，故現行以金融業對於區塊鏈技術最為熱切，希冀能夠過這項新技術，使複雜的金融體系能夠發展趨向簡單而便利的環境。區塊鏈 3.0 則是探討社會中的經濟活動，舉凡政府的稅收、社會福利、電子投票制度、醫療的機密資料儲存、慈善機構收受捐贈後的支出行為監管，甚至是大眾關切的食品安全問題，都能透過區塊利技術進行相關運用。

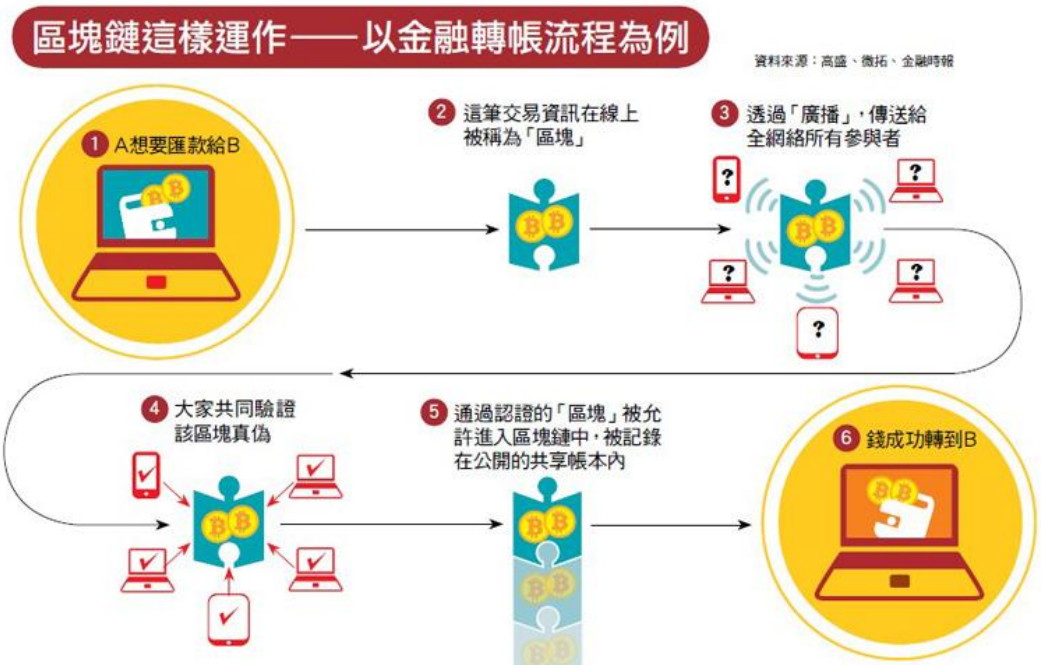
本文主要探討區塊鏈 2.0 的應用，希望能透過現行所知的技術以及國際應用範例，探討臺灣證券及期貨市場如何應用區塊鏈技術，希冀在這一波區塊鏈新技術推出的洪流中，使臺灣的證券及期貨交易市場能掌握新技術崛起的契機。

doi:10.6342/NTU201700214

3.2 比特幣的區塊鏈技術的基本特性

區塊鏈 (blockchain) 的名稱簡單來說，是以資訊技術將資訊封包於一個區塊 (block) 中，並以時間戳封存，依序衍生下一個區塊，並將各區塊如同鏈鎖 (chain) 般，依時間順序緊接著排列並一直延展下去的技術 (詳見圖 9)。

比特幣的區塊鏈技術是一種去中心化的分散式帳冊技術，一個區塊鏈體系由許多節點構成，每個節點通常就是一台電腦，當交易完成後會記錄在一個區塊內，並由記帳能力最快的節點進行區塊完成的廣播，其他節點確認新區塊內容正確後即會放入自己的帳冊中，串聯新的區塊到之前的最後一個區塊，繼續進行完成的區塊鏈，且各節點的帳冊皆完全一致，故又稱為分散式帳冊技術，亦可稱分散式資料庫。區塊鏈技術的運作流程，詳見圖 8。



資料來源：廖君雅 (2016)

圖 8　區塊鏈技術的運作流程圖

doi:10.6342/NTU201700214

以下介紹比特幣的區塊鏈技術的特性與優點：

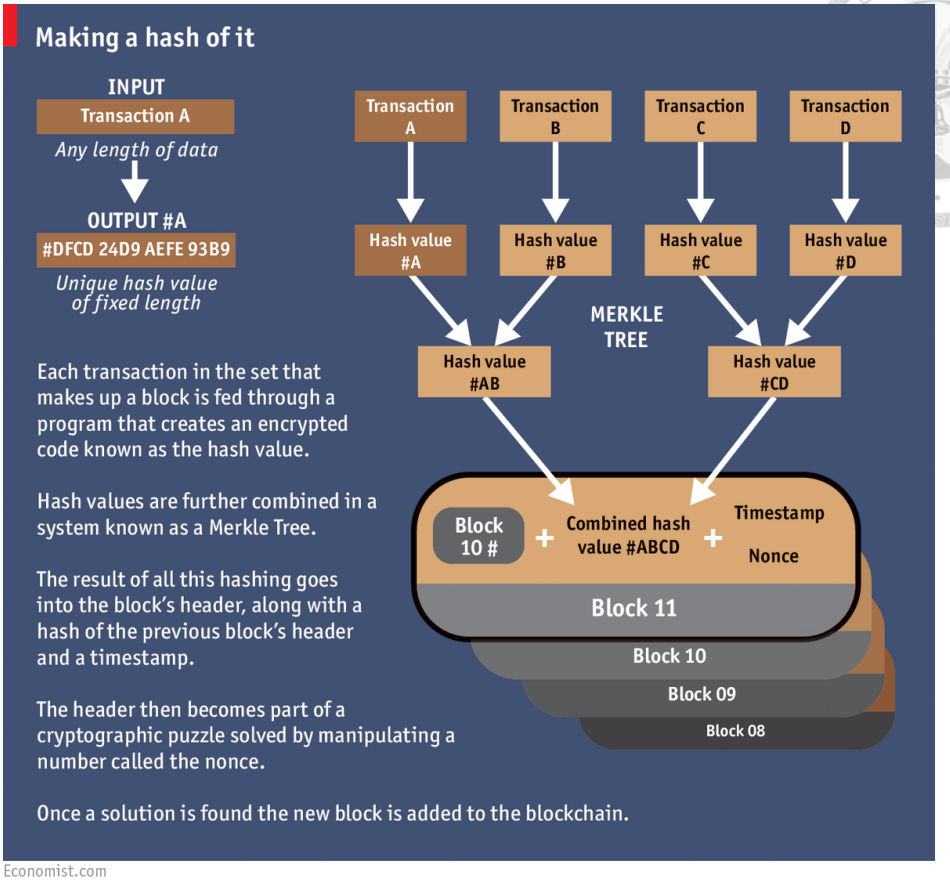
1.動態的點對點網路 (peer to peer，即 P2P)：區塊鏈的各節點可以透過該網路與其他節點直接進行交易，而不需經由中介機構，故其可為去中心化的。此外，區塊鏈網路的節點可自由進出，即新節點可以不斷加入，原有節點亦可隨時退出，任何節點的增減或損壞皆不影響整個系統的運作，並隨著節點增加而增強其網路的穩健性。

2.分散式帳冊技術 (Distributed Ledger Technology，即 DLT) ：區塊鏈上的各節點在交易完成後，都會接收到此交易訊息，並記錄在自己的帳冊上，即各節點皆保存所有交易的歷史紀錄，且其帳冊內容完全相同，此即共識機制。這些交易資訊皆是公開透明、且經過加密、不可竄改的，使得交易紀錄完整保留，並具可靠性。如果有人想竄改紀錄，必須更動所有節點的帳冊紀錄，這使得竄改紀錄無法實現。此外，由於區塊鏈的資料係透過分散式帳冊如此多餘的資訊儲存方式，故只要全世界還有最後一台裝有比特幣程式的電腦存在，這條區塊鏈就能完整地被讀取與繼續運用，即其在保存上具有高度的安全性。

3.雜湊算法 (hashing)：區塊鏈技術透過雜湊算法，即一種單向密碼體制的散列函數，該算法在接收一段明文後，將以一種不可逆的方式將它轉成一段輸出散列，即無法以輸出散列推斷出原文的資訊。此外，由於原文與輸出散列是單向一對一的特性，故原文只要有一點差異，即會導致輸出散列有明顯的變化，故雜湊算法亦可以用來驗證訊息是否被竄改。

區塊鏈技術並以 Merkle Tree 簡化驗證程序。以圖 9 為例，交易 A 得雜湊值 #A，交易 B 得雜湊值 #B，合併後變雜湊值 #AB，且再與交易 C、D 合併後，變成聯合雜湊值 #ABCD，其他結點可用原來的交易資料進行雜湊算法，驗證最後的聯合雜湊值確實為 #ABCD，但聯合雜湊值 #ABCD 無法回推至原來的各個交易 A、B、C、D，故雜湊算法使紀錄易於驗證、不可竄改。

doi:10.6342/NTU201700214



資料來源：The Economist (2015)

圖 9　區塊鏈的雜湊算法

4.時間戳 (timestamp) ：區塊鏈利用時間戳為區塊進行封存，由於時間戳是直接寫在區塊上，且已經生成的區塊無法修改，一旦區塊被修改，則生成的雜湊值無法匹配，竄改行為會立刻被分散式帳冊的系統偵測到。

以圖 9 為例，前一個區塊頭的雜湊值 (Block 10 #)、聯合雜湊值 #ABCD、時間戳，再加上隨機元素 Nonce[4]，共同組成區塊 (Block 11) 的區塊頭。即每一個時間戳會將前一個時間戳納入其隨機雜湊值中，故每一個後生的時間戳都對前一個時間戳進行了安全性的強化效果，這個過程不斷重複、向前推進，最後形成一個完整的區塊鏈。時間戳與雜湊算法共同增強了區塊鏈的安全性。

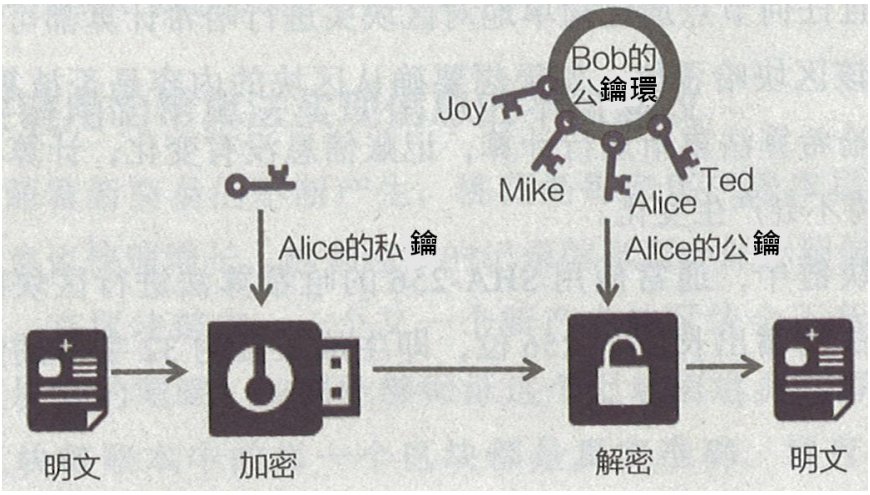
[4] 在安全工程中，Nonce 是一個在加密通訊只能使用一次的數字。在認證協定中，它往往是一個隨機或偽隨機數，以避免重送攻擊。

doi:10.6342/NTU201700214

5. 密碼學機制 (Cryptography) ：區塊鏈技術利用公鑰與私鑰，即非對稱加密 (asymmetric cryptography) ，一種密碼學演算法類型，完成身分驗證與授權機制，故其能擔任信任機制本身。

非對稱式密鑰中，公開的密鑰稱為公鑰，不公開的密鑰稱為私鑰，且其滿足兩個條件。以愛麗絲 (Alice) 希望把一條訊息傳送給鮑伯 (Bob) [5]為例，說明如下：

(1) 利用 Alice 的私鑰對訊息加密，訊息接收者 Bob 可以利用對應的 Alice 的公鑰對訊息解密，得以驗證該訊息是完整而正確的，且此訊息確實來自於擁有私鑰的 Alice，此即數位簽章，而公鑰的形式就是數位憑證，即達到身份驗證，詳見圖 10。



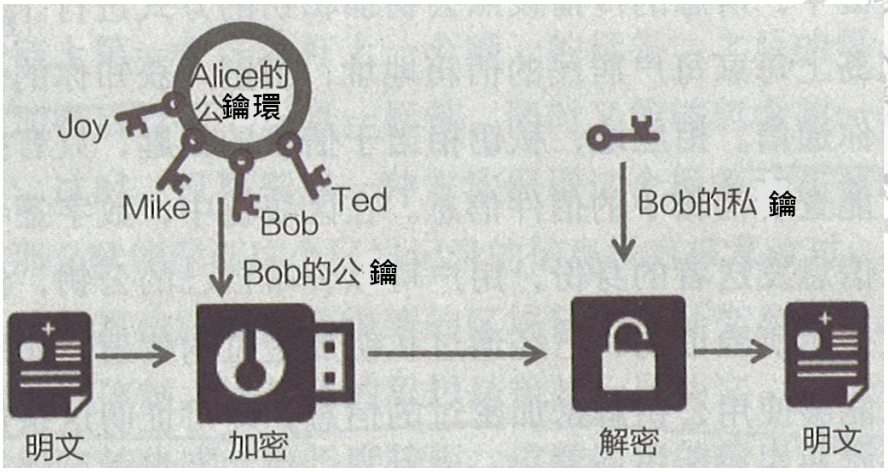
資料來源：唐文劍，呂雯等 (2016)，經本研究整理

圖 10　密碼學機制-身份驗證

另外，Alice 對訊息用 Bob 的公鑰加密後，只有利用對應的 Bob 的私鑰才能解密，故保證訊息或價值傳遞的安全性，Bob 解密後，即完成訊息或價值的移轉與接收作業，詳見圖 11。

[5] 愛麗絲與鮑伯：愛麗絲 (Alice) 與鮑伯 (Bob) 是廣泛地代入密碼學和物理學領域的通用角色。通例上，愛麗絲希望把一條訊息傳送給鮑伯。(資料來源：維基百科)

doi:10.6342/NTU201700214



資料來源：唐文劍，呂雯等 (2016)，經本研究整理

圖 11　密碼學機制-保證訊息傳遞的安全性

(2) 無法依據公鑰去測算出對應的私鑰。

區塊鏈技術利用密碼學機制，使節點之間不需要相互信任，即不需提供自己的身分資料，即可進行交易，故其可為匿名制。

6.獎勵機制：比特幣為了鼓勵記帳者進行誠實記帳活動，給予記帳者手續費，即記帳者可以獲得新產生的比特幣作為獎勵。記帳者將新的交易紀錄資料記載於區塊鏈上的行為，稱為挖礦 (mining)；負責將資料寫入區塊鏈的記帳者就稱為礦工 (miner)；而不進行挖礦、僅進行交易的區塊鏈參與者稱為使用者。

7.最長鏈是唯一的合法鏈：為了解決分散式網路的衝突問題，比特幣規定最長的區塊鏈是唯一的合法鏈，因其亦擁有最大工作量證明[6]，這個規定可以阻止兩個礦工同時找到解答，避免兩個分岔的鏈各自持續延續下去，甚至能阻止惡意竄改交易紀錄的行為。

如果有惡意組織要竄改紀錄，必須比其他節點更快地延長那條被竄改的區塊鏈，使那條被竄改的區塊鏈成為最長的鏈，而惡意組織必須具有整個區塊鏈算力的一半以上，才有機會竄改成功，也就是所謂的「51%攻擊」，而攻擊要成功具

[6] 礦工取得該區塊記帳權的必要條件。

doi:10.6342/NTU201700214

有相當的難度，但基本上不可能做到。

比特幣的區塊鏈技術的特性，彙整詳見表 7。

表 7　比特幣的區塊鏈技術的特性與優點

排序	特性	優點
1	動態的點對點網路	去中心化、節點可自由進出，並隨著節點增加而增強其網路的穩健性
2	分散式帳冊技術	交易資訊公開透明、不可竄改，且在保存上具有高度的安全性
3	雜湊算法	易於驗證、不可竄改
4	時間戳	每一個後生的時間戳都對前一個時間戳進行了安全性的強化效果
5	密碼學機制	身分隱密性高、可為匿名制
6	獎勵機制	鼓勵記帳者進行誠實記帳活動的手續費
7	最長鏈是唯一的合法鏈	避免分岔，並能阻止惡意竄改交易紀錄的行為

資料來源：唐文劍，呂雯等 (2016)，經本研究整理並新增項目

3.3 區塊鏈解決過往無法解決的問題

區塊鏈是一種網路底層的共識協議，各節點的行為必須依照區塊鏈上的規則執行，否則無法運作。區塊鏈的時間戳、分散式帳冊以及工作量證明等特性，共同解決了過去無法解決的拜占庭將軍問題[7]，以及重複支付問題[8]。

[7] 由美國計算機科學家 Leslie Lamport 提出的點對點通訊中的基本問題，即共識問題。古代的拜占庭羅馬帝國由於國土遼闊，為了防禦目的，因此每個軍隊都分隔很遠，將軍與將軍之間只能靠信差傳消息。在戰爭時，拜占庭軍隊內所有將軍和副官必需達成一致的共識，決定是否有贏的機會才去攻打敵人的陣營。如何在已知有成員謀反的情況下，讓其餘忠誠的將軍在不受叛徒的影響下，達成一致的協議，拜占庭問題就此形成。信息在計算機間互相交換後，以多數的結果作為解決辦法，無法找到一個絕對的答案，但可以用來驗證一個機制的有效程度。

doi:10.6342/NTU201700214

1.拜占庭將軍問題 (Byzantine Generals Problem)：過去的點對點通訊作業，只能以多數結果作為解決辦法，但無法找到一個絕對的答案。而區塊鏈技術透過雜湊算法的工作量證明機制，降低訊息傳遞速度，並加入隨機元素 Nonce[9]，使一個時間內只有一個節點可以進行廣播，其他節點收到訊息並驗證成功後，會將新的區塊加入自己的帳冊中，即各節點之帳冊內容完全相同，此即共識機制。區塊鏈技術使網路上的節點都有相同的帳冊內容，即只有一個絕對答案，解決了拜占庭將軍問題。

2.重複支付問題 (double spending)：由於數字貨幣可無限複製，過去必須透過可信賴的第三方機構管理，以確保每一筆數字貨幣只能被使用一次。但透過區塊鏈的時間戳與共識機制等特性，可以確保每一筆貨幣只能被使用一次，因為該筆貨幣在前一個區塊得到確認並以時間戳封印後即無法變更，如果想進行第二次使用，將無法得到全網認證，而導致交易失敗，故避免了重複支付問題。

本節介紹的區塊鏈技術是在比特幣的應用上，事實上，現今各國對於區塊鏈技術的研究發展，並不全然依照比特幣的架構去做，例如比特幣是一種去中心化的分散式帳冊技術，即公有鏈技術，但全球金融業目前研發的方向則多為私有鏈(含聯盟鏈)。

[8] 重複支付是指一筆數字貨幣被交付給兩個收款人，造成款項重複使用。

[9] 在安全工程中，Nonce 是一個在加密通訊只能使用一次的數字。在認證協定中，它往往是一個隨機或偽隨機數，以避免重送攻擊。

doi:10.6342/NTU201700214

第四章 區塊鏈技術於國內外金融業之應用案例

由於比特幣的區塊鏈技術具去中心化之特性，對於中介者的地位產生極大的威脅，包含銀行等金融中介機構、甚至是政府機構，所以這些單位在比特幣展露頭角之初，對於此新技術自然地採取了排斥的態度。但面對新技術越來越強勁的能力表現，與其等待其更茁壯、變成更強大的敵人，不如深入去瞭解它，使它成為中介者降低成本、提高效率的新武器，故現行全球金融業與政府機構，皆積極參與區塊鏈技術的研究，企圖成為這項新技術、新武器的主人，取得技術上的領先地位。以下分別介紹國外及國內，金融業應用區塊鏈技術的代表機構與組織。

4.1 國外案例

國外應用區塊鏈技術於證券及期貨市場，可以私人股份交易平台 Linq、股權交易平台 t0，以及 R3 CEV 聯盟為例 (詳見表 8)。

1.私人股份交易平台 Linq

美國那斯達克證券交易所與區塊鏈公司 Chain 合作，利用區塊鏈技術改造私有股權交易，在 2015 年推出私人股份交易平台 Linq。過去未上市股票交易是透過大量人工與紙本實體作業，故容易產生人為錯誤，且難以進行審計作業。透過 Linq 使未上市股票能夠數字化所有權，同時能縮短結算時間， Chain 表示原來結算時間可由 3 天縮短為 10 分鐘，大幅提高結算效率，並降低結算風險 99%，亦降低資金成本與系統性風險。交易雙方亦可在線上完成發行與申購股票的作業，大幅減少行政風險與成本。

2.股權交易平台 t0

美國線上購物業者 Overstock 以區塊鏈技術開發了 t0 股權交易平台，證券無須透過 Nasdaq 等交易平台，即可在區塊鏈上完成交易。傳統證券交易市場的結

doi:10.6342/NTU201700214

算機制為 T+1 日，當天買入要隔天才能賣出，款項與證券的交付至少需要一天才能完成，而區塊鏈使得交易結算可以同時完成，故 t0 被評論為「交易即結算」。2015 年 7 月，Overstock 向 FNY 資本子公司銷售第一個區塊鏈上的加密債券；同年 10 月，有 5 個客戶透過該平台借出股票；同年 12 月，美國證券交易委員會 (SEC) 批准 Overstock 透過區塊鏈發行該公司股票[10]。

3. R3 CEV 聯盟

R3 CEV 是一家總部位於紐約的區塊鏈公司，由其發起的 R3 區塊鏈聯盟，迄今已超過 50 家領先的金融機構參與，其中包括富國銀行、美國銀行、紐約梅隆銀行、花旗銀行、德國商業銀行、德意志銀行、滙豐銀行、三菱 UFJ 金融集團、摩根士丹利、澳大利亞國民銀行、加拿大皇家銀行、法國興業銀行等，該組織之主要目標係建立銀行業區塊鏈技術開發的行業標準[11]。

表 8　國外案例表

單位或組織	成員	技術特色
私人股份交易平台 Linq	美國那斯達克證券交易所與區塊鏈公司 Chain 合作	改良私有股權交易
t0 股權交易平台	Overstock	交易即結算
R3 CEV 聯盟	富國銀行、美國銀行等 50 餘家巨頭銀行	致力於為銀行提供探索區塊鏈技術的渠道以及建立區塊鏈概念性產品

資料來源：本研究整理

[10] 公司網址 https://www.t0.com/，2016.12.9 查詢。
[11] 公司網址 http://www.r3cev.com/，2016.12.9 查詢。

doi:10.6342/NTU201700214

4.2 國內案例

在國內應用區塊鏈技術並推動相關合作應用者，可以 Gcoin 與 MaiCoin 為例(詳見表 9)。

1.Gcoin 平台

Gcoin 平台是臺灣第一套自行開發的區塊鏈協議，由臺灣大學資工系廖世偉教授與臺大新創團隊合作，自主研發 Gcoin 區塊鏈技術，並無償授權 Gcoin 技術予國立臺灣大學金融科技暨區塊鏈中心，力圖使上層各種區塊鏈創新應用遍地開花。該平台有 6 大特色，分別為交易去中介化、交易發生後 15 秒即完成結算、認許制聯盟架構、最小化信任成本、分散式共識，以及安全加密機制[12]。

2.MaiCoin

MaiCoin 是一家經營比特幣和臺幣交易平台的金融科技公司，近年致力於區塊鏈的商業化應用，朝向企業端提供商業解決方案為主，並受到富邦金控青睞點名合作帳聯網[13]。

表 9　國內案例表

組織	成員	技術特色	營運狀況
Gcoin	臺灣大學資工系廖世偉教授與臺大新創團隊合作	交易發生後 15 秒即完成結算、認許制聯盟架構	無償授權 Gcoin 技術予國立臺灣大學金融科技暨區塊鏈中心
MaiCoin	金融科技公司	向企業端提供商業解決方案為主	與富邦金控等金融機構合作

資料來源：本研究整理

[12] 臺大金融科技區塊鏈 https://fintech.csie.ntu.edu.tw/，2016.12.9 查詢。
[13] 公司網址 https://www.maicoin.com/zh-TW，2016.12.9 查詢。

doi:10.6342/NTU201700214

第五章　我國證券及期貨業應用區塊鏈技術之探討

區塊鏈技術之應用範圍眾多且廣泛，舉凡數位貨幣、國際匯款、政府公共服務、慈善、農業認證、工業生產，以及 P2P 借貸平台業務等，皆有重大影響力，其中，證券及期貨市場為活絡經濟的重要市場，故若能透過區塊鏈技術使我國證券及期貨市場更加發達、追上國際腳步，將能使我國經濟更穩健、亦更繁榮。

證券及期貨業務中，最廣為討論應領先應用部分即為結算交割作業，故針對該項業務討論如下。

5.1 我國證券及期貨市場之交易結算制度簡介

本章介紹臺灣證券交易所及臺灣期貨交易所之交易結算制度，先瞭解現行作業方式，俾利後續討論應用區塊鏈技術之益處。

1.證券市場

臺灣證券交易所開業以來，集中交易市場之買賣即採公開競價方式，現行集中交易市場每營業日交易時間：星期一至星期五 9:00 至 13:30。集中市場除權證外，其餘有價證券均採集合競價決定成交價格。權證則於盤中採逐筆交易，開收盤則仍維持集合競價。臺灣證券交易所自 2014 年 12 月 29 日將盤中集合競價撮合循環秒數縮短至 5 秒。

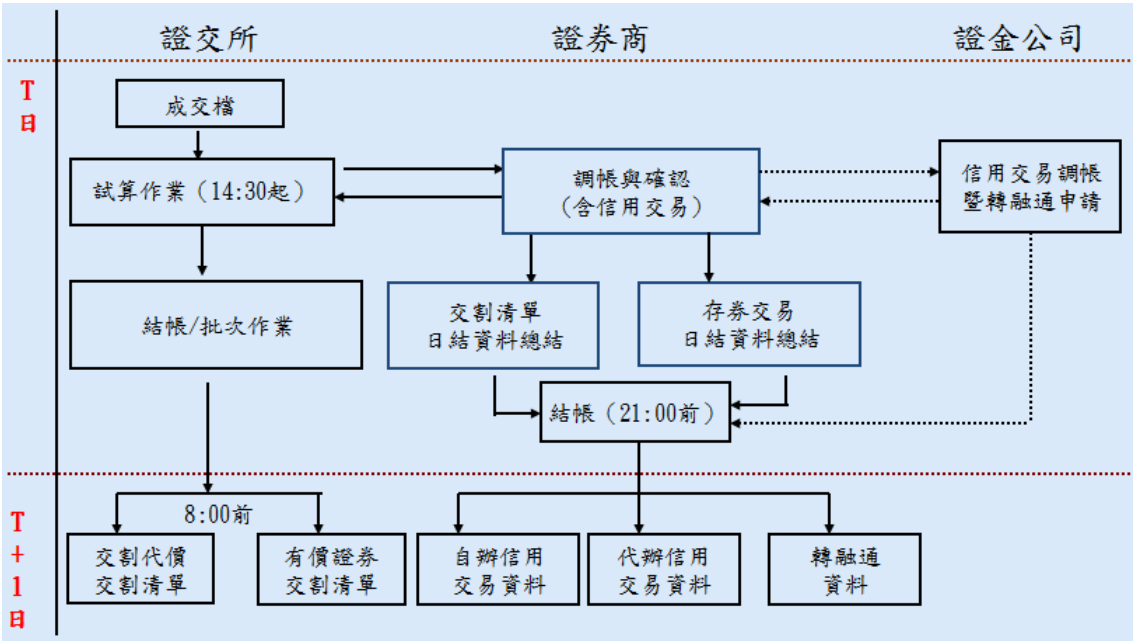
完成交易後將進行款券交割，為了解決證券及期貨的重複支付問題，現有的金融體系皆必須透過結算，以完成款項與有價證券的交割，在當次結算作業尚未完成前，不能進行下一次的交易活動。

依據我國證券交易法、臺灣證券交易所營業細則，及供給使用有價證券集中交易市場契約規定，臺灣證券交易所擔任證券集中交易市場之結算所角色。證券商不分經紀商及自營商，需分別對臺灣證券交易所履行結算交割義務。臺灣證券

doi:10.6342/NTU201700214

交易所採同日結算制，經由多邊餘額交割方式，計算證券商對臺灣證券交易所之應收應付款券數額，證券商按該數額與臺灣證券交易所完成款券收付。交割時點為成交日後次二營業日 (T+2 日) 辦理交割。臺灣證券交易所的交割制度採每日淨額交割制度 (Daily Netting Settlement；DNS) ，證券商須於交割期限前對臺灣證券交易所完成交割，未完成交割之部位不予延後。臺灣證券交易所負責交割款券收付作業之完成，證券收付作業委由集保結算所辦理，交割款項則經由「中央銀行同業資金調撥清算作業系統」辦理收付，完整流程詳見圖 14。

圖 12 係證券交易於 T 日及 T+1 日之作業流程，證交所及證券商於 T 日完成結帳作業，證交所並於 T+1 日完成款券之交割清單。

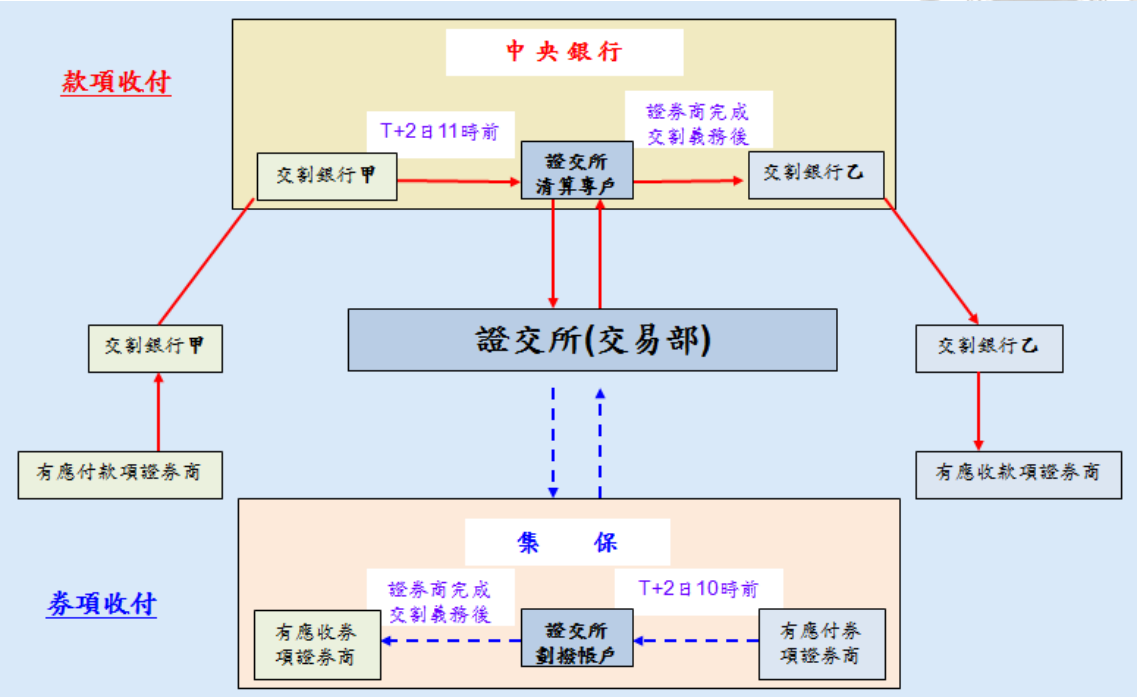


資料來源：證交所網站「105 交割實務宣導說明會 (1) 」講義

圖 12　證交所結算作業—T 日及 T+1 日

doi:10.6342/NTU201700214

圖 13 係證券交易於 T+2 日之作業流程，由證交所、證券商、集保，以及銀行體系，共同完成款券收付之交割作業。

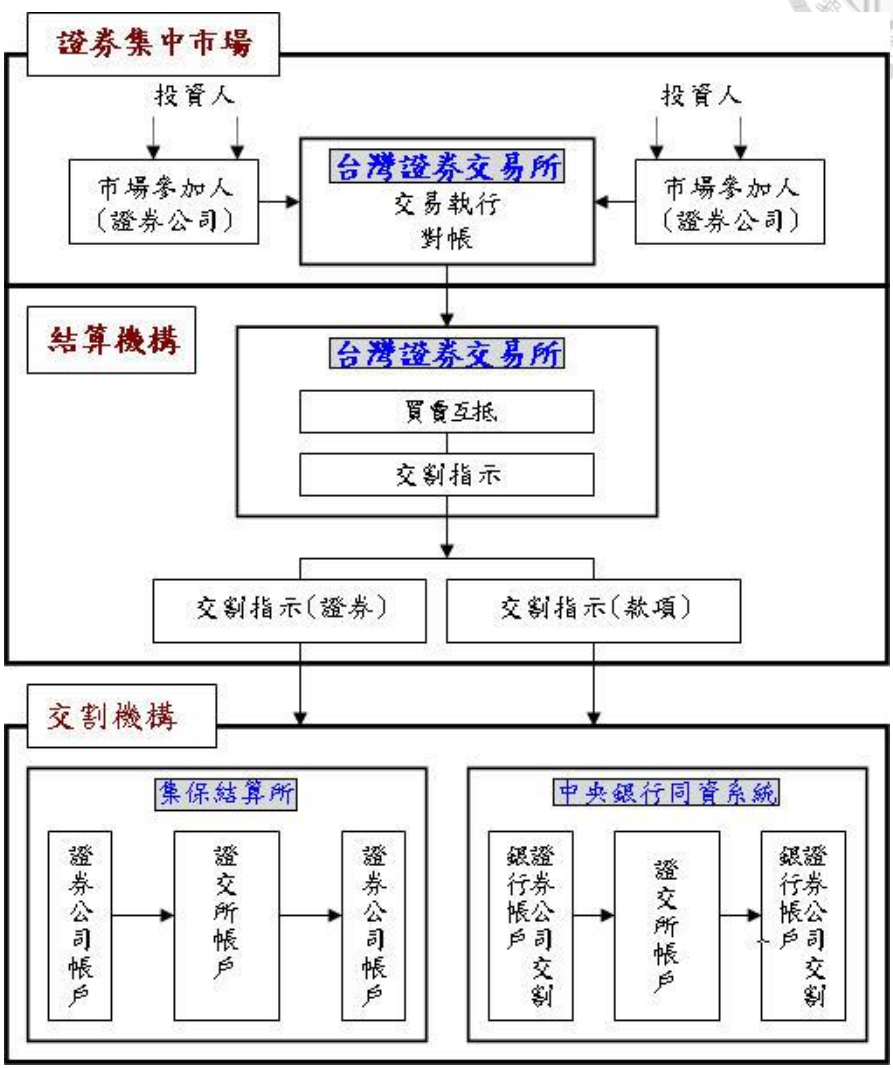


資料來源：證交所網站「105 交割實務宣導說明會 (1) 」講義

圖 13　證交所交割作業—T+2 日

doi:10.6342/NTU201700214

由圖 14 可看到結合圖 12 及圖 13，即證券交易自 T 日、T+1 日至 T+2 日之完整之交易、結算、交割作業流程。



資料來源：證交所網站/結算作業/款券交割作業

圖 14　證券交易、結算、交割之完整流程

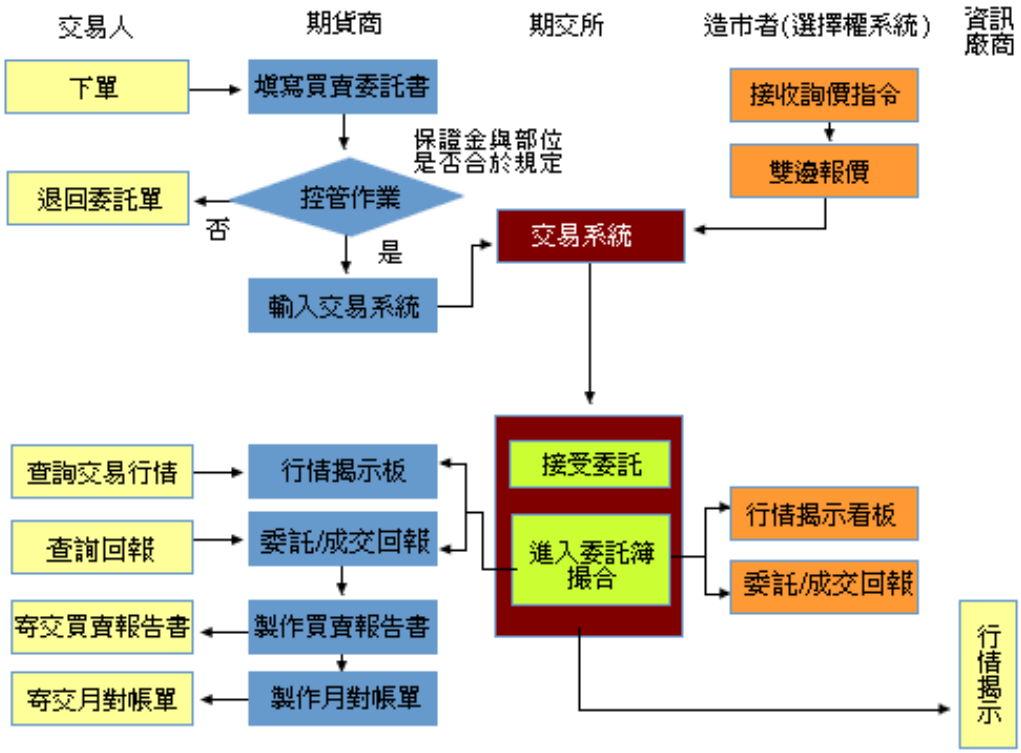
2.期貨市場

我國國內期貨市場之交易日與證券市場相同，但交易時間係自上午 8：45 至下午 1：45，交易時間較現貨證券集中市場提早 15 分鐘，並晚 15 分鐘收盤，以發揮價格發現及避險功能。隨著網路遍布與智慧型手機普及化，電子交易比例日益提升。目前所有期貨商品交易時段之撮合方式，全數係採逐筆撮合。

doi:10.6342/NTU201700214

我國期貨交易之第一步驟為繳存期貨交易保證金，交易人必須於期貨商指定之金融機構開立存款帳戶，並與期貨商約定入金帳戶，透過該帳戶將保證金轉入期貨商客戶保證金專戶後，始得從事期貨交易，即我國期貨交易係採保證金預繳制，及事先約定入金帳戶之規範。

我國期貨交易所商品之交易流程中，共有五個主體，分別交易人、期貨商、期交所、造市者，以及資訊廠商。交易流程係自交易人下單，期貨商接受其委託買賣，再經由期交所進行買賣撮合，並提供委託及成交回報，以及期貨商製作交易之買賣報告書及每月對帳單資料，詳見圖 15。



資料來源：期交所網站

圖 15　我國期貨交易流程圖

依據期交所之結算作業流程規定，期交所與期貨商將進行保證金存提作業、盤中損益試算追繳作業、交易收盤作業、補繳盤後不足保證金作業、每日最終結算保證金權益數額等核帳作業，以及結算作業等。

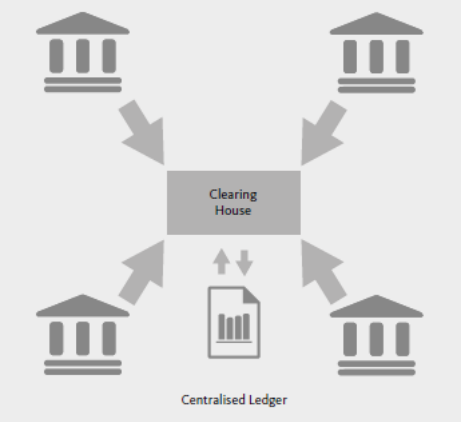
doi:10.6342/NTU201700214

5.2 我國證券及期貨業應用區塊鏈技術後之預期效益

應用區塊鏈技術，可望縮短結算時程，甚至達到交易即結算之境界，並使系統具相對穩定等特性，介紹如下：

1.交易即結算

即股票與款項可即時完成移轉，使現行證券 T+2 日的交割時程可在數分鐘，甚至數秒鐘內完成。由於過去所有的交易系集中透過結算所等可信賴的中介機構進行結算作業，故中介機構必須負責大量的買賣雙方訊息，無法於交易後即時完成後續的結算交割作業，如圖 16。



資料來源：Santander InnoVentures, Oliver Wyman and Anthemis Group (2015)

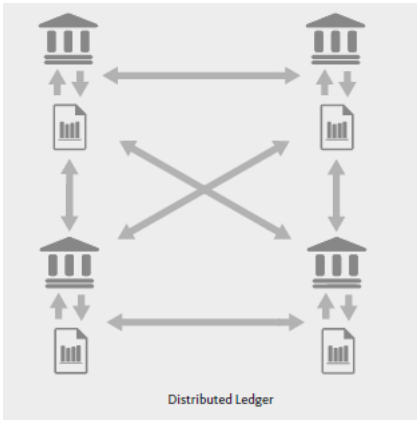
圖 16　集中式帳冊結算方式

若採區塊鏈技術，預計可達下列 3 項優點：

(1)簡化交易後結算交割流程

由於區塊鏈技術可進行點對點交易，加上其基於數學原理，可以確認所有權並完成價值的移轉，當每個人都看到的數據資料都相同時，將產生更有效率的交易結算流程，並且能快速地在市場中流通更新，如圖 17。

doi:10.6342/NTU201700214



資料來源：Santander InnoVentures, Oliver Wyman and Anthemis Group (2015)

圖 17　分散式帳冊結算方式

對證券交易而言，當兩個客戶在區塊鏈上交易時，可透過公私鑰的非對稱式密鑰方式，進行雙方的款券相互移轉作業，而無須透過中介機構、支出額外的對帳程本，達到交易即結算，詳見圖 18。

依據高盛報告 (2016) ，區塊鏈技術主要係透過簡化交易後結算交割流程，減少結算時間和對帳成本，提高現金股票市場的效率，且有助於降低交易過程中業者所需的資本條件、運營成本和託管費，全球每年約可節省 110~120 億美元的成本。

(2)降低交易違約風險

交易即結算除可降低結算對帳成本，亦可降低我國現行證券市場 T+2 日才完成款券交割造成之 T+2 日才發現的違約交割風險。

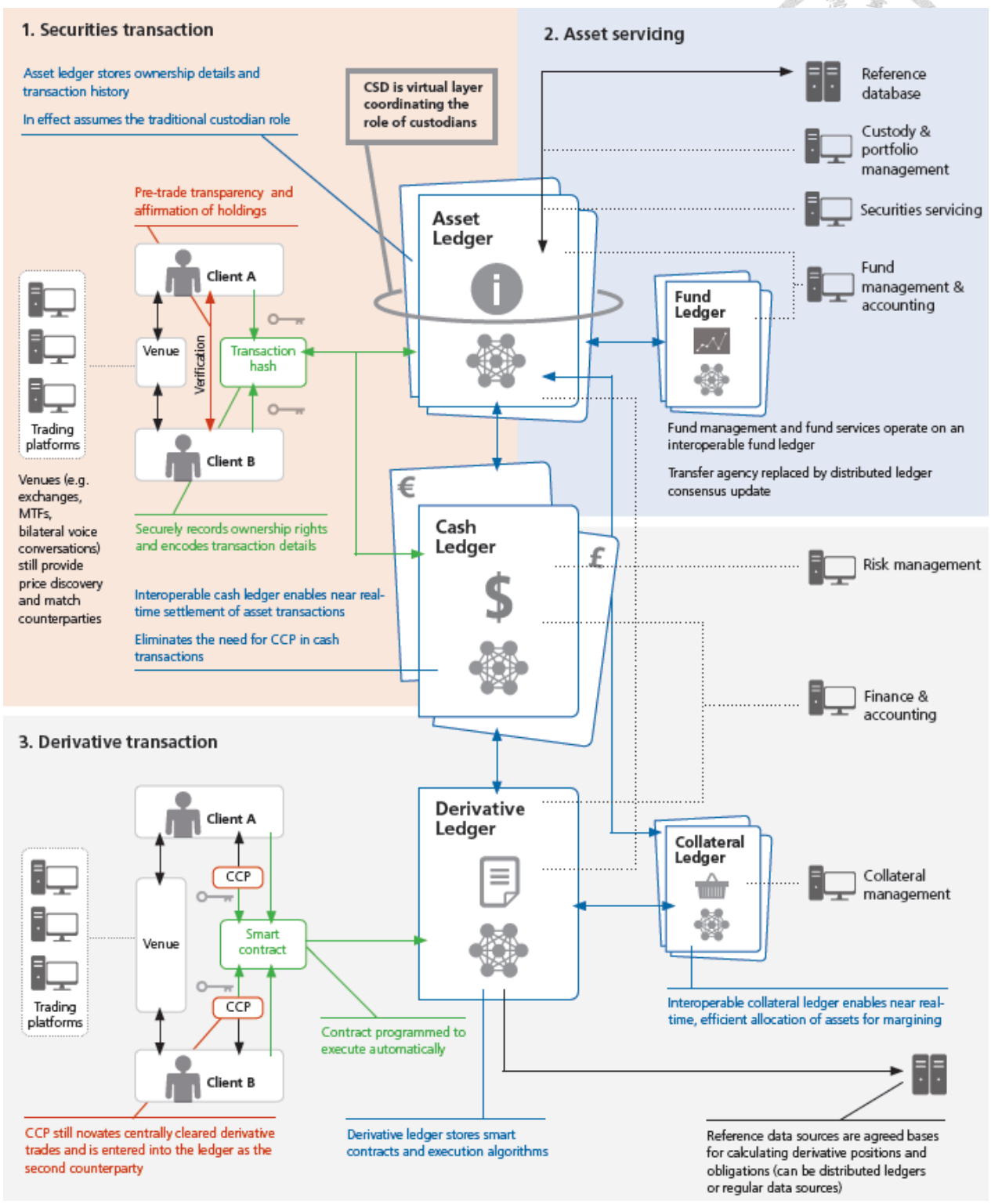
(3)或可調整期貨交易之預繳保證金制度等規範

有鑑於期貨商品的高波動、高風險性，我國期貨交易現行係採預繳保證金制度，並須事先約定入金帳戶，以保證交易雙方之安全，未來利用區塊鏈技術可達到交易即結算，或可調整期貨交易之預繳保證金制度等規範。

doi:10.6342/NTU201700214

依據 Euroclear & Oliver Wyman 報告 (2016) 指出，區塊鏈技術對期貨等衍生商品來說，區塊鏈技術將帶來最大的改變，透過智能合約，可以扣住兩個交易對手的義務 (例如保證金) 。智能合約可以依據約定之條件，自動再計算風險值，以重新計算所需的追加保證金。可互相操作的衍生性商品和抵押分類帳，將允許合約借調在資產分類帳中的額外抵押單位，以因應這些需求。到期時，智能合約會計算最終淨負債，並在現金分類帳中自動生成付款指示，以結束交易，詳見圖 18，故未來我國若採區塊鏈技術應用，或可調整期貨交易之預繳保證金制度，或約定入金帳戶等相關規範。

doi:10.6342/NTU201700214



資料來源：Euroclear & Oliver Wyman (2016)

圖 18　資本市場應用區塊鏈技術之理想觀點

doi:10.6342/NTU201700214

2.交易無休

截至目前為止，全球尚無商品可在交易所進行交易 24 小時不間斷，即使是外匯集中市場，在周末都需要休市。而比特幣之區塊鏈自 2009 年運作以來，迄今超過 8 年交易運作未曾中斷，故若交易所可透過區塊鏈技術提供交易活動的運作，不再需要為了維護或更新系統而暫停營業，將可達到 24 小時、365 天的營業不間斷，將可避免發生全球市場震盪時，因非證券及期貨市場交易時間而無法下單所造成之風險，達到保障交易人套利與避險的權益。

3.提升證券及期貨之交易量

透過運用區塊鏈技術，可降低證券及期貨之交易成本，其交易安全性及跨國便利性，更將吸引國際交易人之參與，加上前項所提之交易無休，可進而推升我國證券及期貨之交易量，達到活絡我國資金流通之效果，進而繁榮實體經濟。此外，證券及期貨交易量之提升，亦可促進我國稅收增加，進而達到政府與企業雙贏之效果。

4.系統具有相對穩定的特性

金融業最大的風險即是遭到駭客攻擊或伺服器當機，由於區塊鏈技術係採用分散式帳冊技術，而非傳統由中心統一控制管理，故即使駭客攻擊任一節點，亦無法影響其他節點的帳冊內容，使交易即使在被攻擊的情況下，依舊能準確地傳遞價值，故可節省中央的備援系統設置成本，使得風險大幅降低，有效預防攻擊與故障事件。以倫敦金屬交易所 (LME) 為例，其於 2016 年 7 月 22 日發生近 4 小時電子交易系統當機事件為例，期間交易人僅能仰賴電話進行交易。

5.減少錯帳

依據高盛報告 (2016) 指出，高達 10%的股票交易受到不同的錯誤影響，導致需要人工介入，因而延長了交易的結算時間，但透過區塊鏈技術應用於股票結算

doi:10.6342/NTU201700214

交割作業，估計可以節省 100~120 億美元處理錯帳之成本。

6.節省寄送交易紀錄之成本

區塊鏈技術可詳實記錄每一個流程，故交易人透過網際網路就可看到自己完整的開戶與交易資料，證券及期貨業者不再需要寄送買賣報告書與對帳單等交易後彙整資料給予投資人和交易人，交易人亦無需到交易所或證券及期貨商查詢自己的開戶或交易資料，既可節省交易人往返的時間成本、交易所與業者人員服務的時間成本，亦可節省紙張的列印、存放等成本，達到節能減碳之效。

7.提高業者資金運用效率，並可節省中介機構之相關作業成本

現行結算會員繳存至期交所結算保證金專戶內之款項，由期交所逐日計算，每半年付息一次。利用區塊鏈技術可達交易即結算，期貨商無須先將保證金預繳於保證金帳戶中，故無資金暫留之問題，可提高期貨商資金之運用效率，亦可節省期貨交易所等中介機構進行付息等相關作業成本。

將上述證券及期貨業應用區塊鏈技術之預期效益整理列於表 10 中。

doi:10.6342/NTU201700214

表 10　我國證券及期貨業應用區塊鏈技術之預期效益

序號	特色	優點
1	交易即結算	(1)簡化交易後結算交割流程 (2)降低交易違約風險 (3)或可調整期貨交易之預繳保證金制度等規範
2	交易無休	避免發生全球市場震盪時，因非證券及期貨市場交易時間而無法下單所造成之風險，達到保障交易人套利與避險的權益
3	提升證券及期貨之交易量	透過成本降低，交易安全性及跨國便利性提高，加上前項所提之交易無休，可推升我國證券及期貨之交易量，進而繁榮實體經濟、稅收增加，達到政府與企業雙贏之效
4	系統具有相對穩定的特性	降低駭客攻擊或伺服器當機之風險，並可節省中央的備援系統設置成本
5	減少錯帳	可節省處理錯帳之成本
6	節省寄送交易紀錄之成本	可節省交易人為查詢資料造成業者寄送資料、交易人往返的時間成本、交易所與業者人員服務的時間成本，亦可節省紙張的列印、存放等成本，達到節能減碳之效
7	提高業者資金運用效率，並節省中介機構之相關作業成本	無資金暫留之問題，且可節省中介機構進行付息等相關作業成本

資料來源：本研究整理

doi:10.6342/NTU201700214

5.3 對我國證券及期貨市場如何應用區塊鏈技術之建議

比特幣的區塊鏈技術實現最強大的匿名共識機制，卻不完成適合在高度監管的證券及期貨市場上應用，我們建議採取部分的技術，或調整使用的方式，期使我國證券及期貨市場之效益最大化，並條列如下：

1.採私有鏈

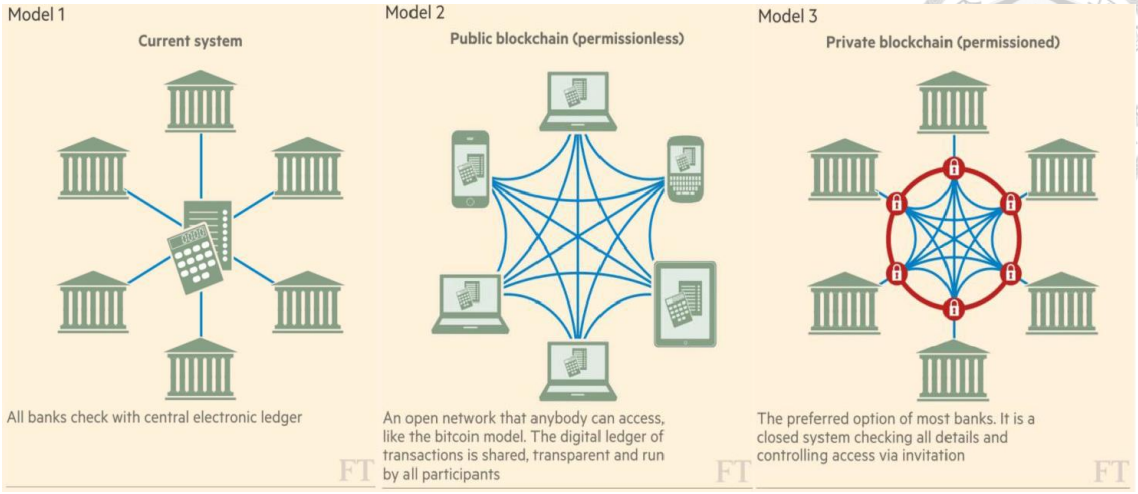
現行金融業作業方式為集中式管理 (詳見圖 19 之模式 1)，若改採區塊鏈的分散式帳冊技術，若以比特幣區塊鏈為例，由於比特幣區塊鏈之去中心化與共識機制效率兩者之間的效率難以兩全，去中心化程度越高、共識機制的效率越低，將導致交易所需確認時間越長、交易量越低。

有關區塊鏈的分散式帳冊技術，依各節點的進出自由度，可分為公有鏈及私有鏈 。

(1) 公有鏈 (Public blockchain) ：即非認許制 (permissionless)，該系統係採開放式的存取架構，沒有集中化的主管單位，任何人或單位都可以加入該網路，不需要通過任何審核程式，故亦可匿名參加，例如比特幣。公有鏈的優點是節點進出自由，資料公開透明，詳見圖 19 之模式 2。

(2) 私有鏈 (Private blockchain) ：即認許制 (permission)，該系統係由管理單位或原有成員辦理新成員之加入或退出審核作業，成員係由管理單位事先選定成員，或後續參與的成員必須通過管理單位或原有成員之審核，通常用於政府、私人企業、相同產業或彼此有合作關係的產業中。私有鏈的優點是節點間信任度高，故完成共識的速度快、成本低，且因不對外公開，故資料隱密性高，詳見圖 19 之模式 3。

doi:10.6342/NTU201700214



資料來源：Wild Jane, Arnold Martin and Stafford Philip (2015)

圖 19　模式 1:集中式管理；模式 2:公有鏈；模式 3:私有鏈

由於金融業係屬特許事業，故我國證券及期貨商之設立，須經主管機關之許可及發給證照，方得營業，故應由管理單位限制節點進出，即可參採私有鏈制度 (詳見表 11)。

表 11　公有鏈及私有鏈之比較表

制度	特色	優點	應用
公有鏈	成員可自由進出	節點進出自由，資料公開透明	比特幣
私有鏈	由管理單位或原有成員辦理新成員之加入或退出審核作業	完成共識的速度快、成本低，且資料隱密性高	政府、私人企業、相同產業或彼此有合作關係的產業

資料來源：Wild Jane, Arnold Martin and Stafford Philip (2015)，經本研究整理並新增項目

另應由管理單位賦予區塊鏈之節點不同權限，將各節點之交易、記帳、查詢、修改等權限納入管理，可區分為交易會員、結算會員等不同資格與權限之管理方式，以確保資料安全性與隱密性，只有被授權的節點可查閱所屬管轄範圍各帳戶基本資料及交易相關資訊。

doi:10.6342/NTU201700214

2.採用其他共識機制

比特幣的區塊鏈技術係採去中心化的工作量證明機制，但依據前項討論業建議金融業採行私有鏈，由於節點已是選定之成員，成員們具有共同利益目標，故無需再採工作量證明，可利用其他方式，使交易速度提升，解決因挖礦活動造成巨大的資源耗損與浪費的高耗能問題。

目前常見的共識機制有 3 種，分別為工作量證明、權益證明、股份授權證明。這幾種共識機制各有優缺點，分別說明如下：

(1) 工作量證明機制 (Proof of work；PoW) ：一種競爭式的共識，即所有節點必須花費時間和運算資源，去算出一個數值的結果，而完成運算的過程必須要有一個有效的工作量證明[14]，以取得區塊的記帳權，亦即挖礦；此外，其他節點可利用公式，輕易地驗證這個數值是否有效，係比特幣現行的共識機制。優點是完全的去中心化，每個節點是平等、可自由進出的；缺點是進行電腦計算挖礦時，必須耗費大量的電力，造成能源浪費，達成共識的週期也較長。

(2) 權益證明機制 (Proof of Stake；PoS) ：係工作量證明的升級版，降低挖礦浪費資源的問題。主要係依據各節點擁有加密電子貨幣的所有權 (即權益) 的比例，來決定其挖礦的難度，故其優點為縮短達成共識的時間，即減少浪費資源，缺點則是與工作量證明一樣，仍然要挖礦，且可能會造成富者越富的財富集中現象。

(3) 股份授權證明機制 (Delegate Proof of Stake；DPoS) ：係權益證明機制的改良版。與董事會投票機制類似，讓每個擁有加密電子貨幣的節點進行投票，選出一定數量的節點代表，由這些節點來輪流代理全體進行記帳。故其優點是不需要透過挖礦的競爭，可以大幅縮小交易確認的時間，甚至達到秒級的共識驗證，

[14] 以生活實例來說明，一個英語聽說讀寫很好的臺灣人，依照常理，應該是花費許多時間和精力去研讀英語，才能達到英語流利的程度，此即簡單的工作量證明。

doi:10.6342/NTU201700214

缺點則是股份授權證明機制還是需要依賴加密電子貨幣，不完全適用於一般的商業應用。

比特幣的區塊鏈技術係採工作量證明機制，造成挖礦資源浪費的爭議，若採用其他證明機制除可解決挖礦浪費問題，亦可提高交易完成速度 (詳見表 12)。

表 12　區塊鏈技術的共識機制

名稱	特色	優點	缺點
工作量證明機制 (PoW)	競爭式的共識	完全的去中心化，每個節點是平等、可自由進出的	造成大量的挖礦資源浪費，達成共識的週期也較長
權益證明機制 (PoS)	依據各節點擁有加密電子貨幣的所有權 (即權益) 的比例，來決定其挖礦的難度	縮短達成共識的時間	仍然要挖礦，且可能造成財富集中現象
股份授權證明機制 (DPoS)	投票選出節點代表來代理全體進行記帳	大幅縮小交易確認的時間，甚至達到秒級的共識驗證	仍依賴加密電子貨幣，不完全適用於一般的商業應用

資料來源：唐文劍，呂雯等 (2016)，經本研究整理

3.運用智能合約 (Smart Contracts)

比特幣為區塊鏈技術 1.0 之應用，而區塊鏈 2.0 應用即為智能合約之發展。所謂的智能合約係指事先在電腦中設定條件，在環境觸發到設定條件時，即可由電腦程式自動執行，而不需人工介入執行，保證了交易執行的自動性與完整性。

簡單說明智能合約，可以自動販賣機為例，區塊鏈技術就如同自動販賣機，買家投入指定金額的貨幣，並選擇商品，販賣機將提供買家選定之商品，過程沒

doi:10.6342/NTU201700214

有人工介入，即自動完成交易。自動販賣機有鑰匙或密碼的設置，可避免偷竊事件，並可辨別真鈔或偽鈔，以保障自動販賣機運作上的安全性。

在集中制的體系下，由於管理者有權力隨時修改或刪除該合約，故過去智能合約之效益不大，但區塊鏈的智能合約是事先寫入程式中且自動執行約定的條款，任何人或機構都不能修改、刪除該合約，也無法阻止該合約自動執行。

智能合約能使價值交易的時間與金錢成本大幅降低、效率亦大幅提高，避免違約風險與操作風險。此外，現行金融交易仍需要大量的人工作業，因此亦伴隨著大量的作業風險，智能合約可簡化交易流程，減少了完成整筆交易所耗費的時間，並且降低交易成本。將智能合約與傳統合約的差異比較彙整列於表 13 中。

表 13　智能合約與傳統合約的差異

項目	智能合約	傳統合約
運作方式	依原先設定，觸發條件時自動運作	人工運作
執行時間	事前設定	事後執行
適用環境	客觀且明確的環境條件下	主觀且模糊的環境條件下
成本	邊際成本低	邊際成本高

資料來源：本研究整理

由於智能合約的邊際成本低，在大量交易的環境下，將使區塊鏈技術的效益最大化。依據唐文劍，呂雯等 (2016) 所述，與區塊鏈技術最相配的交易屬性即為「標準化程度高、連續性強、自動化需求大，以及品質證明要求多」等特性，例如跨境支付、匯款、證券及期貨集中交易市場等應用 (參見表 14) ，將能使區塊鏈技術之效益最大化、成本最低化。

doi:10.6342/NTU201700214

表 14　適合透過區塊鏈技術之特性

特性	內容	適合應用範圍
標準化程度高	每項商品的規格相同	貨幣 (跨境支付、匯款)、證券及期貨交易市場等
連續性強	交易頻率高	
自動化需求大	人工處理之需求低	
品質證明要求多	每個商品的品質皆相同	

資料來源：唐文劍，呂雯等 (2016) ，經本研究整理

4.將監管單位設為節點

此外，由於證券及期貨交易係屬專業知識，仍然需要瞭解證券及期貨交易規則的專業機構或專業人員確保交易、結算、監視、資訊等各項作業的運作正常，甚至在交易雙方發生爭端時，進行行政調查，以作為法院審判的依據。故建議將主管機關及交易所等監管單位設為節點，以利相關作業運作正常，且擔任糾紛處理的中立單位。

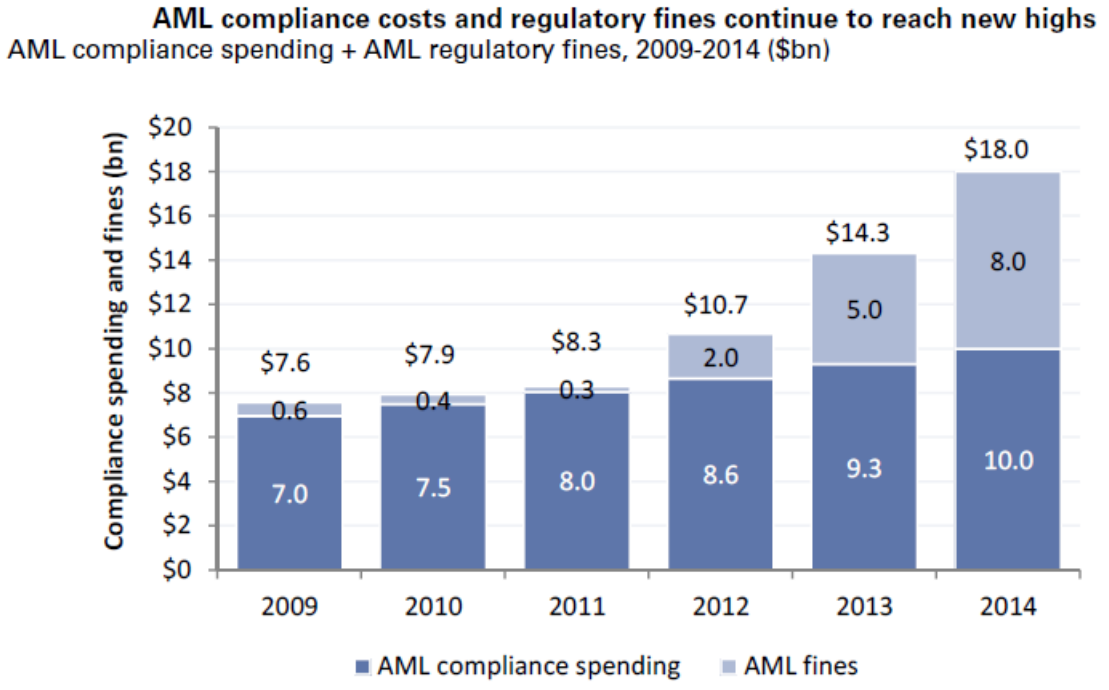
5.運用於洗錢防制與 KYC 作業之執行

洗錢 (money laundering) 即資金洗淨，係指將透過犯罪或其他非法手段所獲得的金錢、偽鈔，經過合法金融作業流程等方法，將其洗淨為看似合法的資金，以便合法使用其非法取得的錢財。洗錢常與經濟犯罪、毒品交易、恐怖活動及黑道等重大犯罪有所關連，也常以跨國方式進行。為遏止洗錢非法行為，全球監理機構皆極力推廣洗錢防制 (anti-money laundering, AML) 規範，我國監理機構亦制定「洗錢防制法」，以防制洗錢，打擊犯罪，健全防制洗錢體系，穩定金融秩序，促進金流之透明，並強化國際合作。

依據高盛報告 (2016) 指出相關數據顯示，偵測到的洗錢行為不到全體洗錢的 1%，因此銀行受到嚴重的監管懲罰，正如我國兆豐銀行紐約分行，即在 2016 年因

doi:10.6342/NTU201700214

違反洗錢防制法的疑似洗錢申報作業規範，而遭美國主管機關裁罰 1.8 億美元 (約新臺幣 57 億元) 為例。從圖 20 可以看到，銀行業為洗錢防制規範付出之成本自 2009 年節節高升，至 2014 年時已高達 180 億美元，其中為遵循洗錢防制規範花費達 100 億美元、罰款總額則高達 80 億美元。



資料來源：The Goldman Sachs Group (2016)

圖 20　銀行業為洗錢防制規範付出之成本

高盛報告 (2016) 更指出，若能透過區塊鏈技術，將可降低洗錢防制之作業成本，從 100 億美元，降低為 75 億美元，約降低 25%；而罰款則可望能從 80 億美元，降低為 55 億美元，約降低 31%，即可大幅降低成本之金額與幅度。

我們可以利用區塊鏈技術的分散式帳冊技術，以及智能合約等功能，將疑似洗錢的行為、模式寫入程式中，透過電腦系統輔助交易流程等作業監控，達到預警標準時提出警示等，可以降低大量的人工判讀成本，並降低人工判讀錯誤的機率，協助法遵人員追蹤不斷變化的法律規範，甚至避免遭受鉅額罰款，進而達到

doi:10.6342/NTU201700214

降低成本的效果。

洗錢防制 (AML) 與「認識你的客戶」 (KYC) 之架構，皆是要求金融業對客戶進行身分驗證，現行兩者之作業皆須透過大量人工作業，且不同銀行或不同部門之間，皆為了相同客戶、甚至相同資訊，進行重複的審查作業。透過區塊鏈技術的分散式資料庫技術，可以促使金融業之間快速完成身分確認作業，並進行分享與使用資訊，減少不必要的重複作業成本，簡化洗錢防制與 KYC 之作業流程。

6.提升法遵科技應用之效率

因應金融科技的急速發展，新型態的「法遵科技」 (RegTech) 誕生，其係結合監理 (Regulation) 與科技 (Technology) 兩字所組成的另一個新專有名詞，係指利用資訊科技，廣泛蒐集各國金融監理制度與法規要求，提供分析與管理的工具，自動協助金融機構遵守法規要求，以降低作業風險，廣義的法遵科技亦包含前項洗錢防制與 KYC 之應用。

區塊鏈技術有利法規的遵循，將法律規則與邏輯寫入區塊鏈智能合約的程式中，智能合約將自動檢測所有交易與各節點的適法性，使得與規則不相符之交易或節點無法執行，進而使整個系統都在符合規則的環境下運作，使交易風險更低，確保買賣雙方的交易安全性。

區塊鏈技術應用於法遵科技的優點可分為下列三個部分：

(1) 節省執行成本：經濟發展的關鍵因素，係透過制定法律，使人們有共同規則得以依循，若能透過區塊鏈技術，將共同規則寫入程式中，只有合規的行為可以執行，將可節省自簽約、修約、到履約之成本，且在條件觸發時由系統自動執行，減少人工執行成本，對於大量、高頻率、規格相同的交易，其效益尤其明顯。

(2) 節省舉證成本：由於區塊鏈具有不可竄改、永久保存紀錄之特性，能使交易

doi:10.6342/NTU201700214

雙方有效率地解決舉證問題，亦為監理單位與司法單位節省判定真偽與責任歸屬之成本。在跨國交易時，其效益尤其明顯，過去由於兩國間法規制度不同，資訊取得不易，透過區塊鏈技術係屬全球性的流通，可有效降低時間與金錢成本。

(3) 發揮專業機構與專業人士能力之最大效益：區塊鏈技術不能完全取代律師和會計師等專業人士或專業機構之功能，其現行功能係審核個別契約，而未來則須透過這些法律與會計之專業人士，設計區塊鏈智能合約的條款，使條款內容更完備且執行更順利，以發揮契約之最大效益，即交易雙方都得到簽約時的預期結果。

7.先以鉅額交易等較不具時間急迫性之作業試行

區塊鏈技術在理論上可達交易即結算之境界，但現行證券及期貨業之交易技術已相當成熟，係數量大、高頻率之作業環境，且現行運作亦屬流暢。以目前的區塊鏈技術尚無法應付如此高量、高頻之交易活動，建議可先從股票發行作業，尤其是鉅額交易、場外交易等雙方相互議價的交易，進行初步的試驗，雙方議價交易係最適合區塊鏈技術的 P2P 特性，且不具時間急迫性，可累積技術應用之經驗，並隨著技術的日益成熟，將可逐步應用到證券及期貨集中市場。

8.業界共組聯盟鏈以達資訊共享

區塊鏈技術可使業者之間建立資訊互通之橋梁，過去必須透過正式管道才能互通資訊，未來業者可共組聯盟鏈 (私有鏈的一種)，於建置區塊鏈系統平台後，可透過密鑰傳遞私訊或公共訊息，例如客戶黑名單等，使業界資訊暢通，節省建置資料庫等資訊重複建置成本。

透過前揭 8 項建議規劃，將可達到提升交易相關流程之效率，並降低成本費用的效益，相關建議與效益彙整如表 15。

doi:10.6342/NTU201700214

表 15　對我國證券及期貨市場如何應用區塊鏈技術之建議

序號	建議	效益
1	採私有鏈	完成共識的速度快、成本低，且資料隱密性高
2	採用其他共識機制	解決比特幣的挖礦浪費問題，亦可提高交易完成速度
3	運用智能合約	邊際成本低，在大量交易的環境下，將使區塊鏈技術的效益最大化
4	將監管單位設為節點	證券及期貨交易係屬專業知識，需要專業機構或人員確保各項作業的運作正常，並擔任糾紛處理的中立單位
5	運用於洗錢防制與 KYC 作業之執行	預期洗錢防制之作業成本可降低 25%；罰款可降低 31%
6	有效應用法遵科技	節省執行及舉證成本，並可發揮專業機構與專業人士能力之最大效益
7	先以鉅額交易等作業試行	雙方議價交易係最適合區塊鏈的 P2P 技術特性，且不具時間急迫性，可累積技術應用之經驗，並隨著技術的日益成熟，將可逐步應用到證券及期貨集中市場
8	業界共組聯盟鏈以達資訊共享	可透過密鑰傳遞私訊或公共訊息，節省不必要的資訊重複建置成本

資料來源：本研究整理

5.4 區塊鏈技術尚有待加強之處

區塊鏈技術發展迄今，應用於證券及期貨市場上仍存在許多挑戰需要克服，主要可分為下列 3 點可進行強化：

1.法規面—法規修改尚未趕上技術進步的速度

由於法規係規範眾人行為的準則，牽一髮而動全身，修正法規時必須考量所有面向的影響，避免引發其他負面作用，故修正法規之時程較長，而區塊鏈技術

doi:10.6342/NTU201700214

等金融科技進步的速度日新月異，若法規修正速度過慢或修改錯誤，反而可能限制了新技術的發展，或導致業者違反法規的風險。

2.速度面—尚未達到可高頻交易之速度

以比特幣區塊鏈為例，每筆交易約為 250 byte，由於區塊大小限制於 1 MB，即每個區塊可容納交易為 4,000 筆，目前比特幣交易的確認時間約為 10 分鐘，即每秒最高可處理 7 筆交易。

雖然相較國際匯款動輒 2、3 天，甚至一個禮拜的時程，區塊鏈技術已大幅縮短交易完成所需時間，但對於需要即時性之交易活動，例如刷卡消費，或高頻交易需求，例如證券及期貨集中市場來說，交易確認時間太長，導致尚無法實地應用。現行證券交易系統於尖峰委託處理筆數每秒可達 30,000 筆，期貨交易系統尖峰處理容量更高達每秒 48,000 筆，與比特幣區塊鏈技術最高每秒僅能處理 7 筆交易，速度相距甚遠。

3.實證面—區塊鏈技術尚未受到完整的實證考驗

由於區塊鏈技術尚處於萌芽階段，尚未大量應用於實際生活中，當大量應用後，將帶來許多討論。例如 2016 年 6 月發生的 The DAO 以太幣竊案[15]，後來 The DAO 決議以硬分支方式處理，此係區塊鏈技術問世後，首次發生大規模逆轉區塊鏈的事件，而眾人皆有不同意見。

我們透過訪談臺灣證券交易所黃乃寬副總經理，以及創立 Gcoin 的臺灣大學資訊工程學系廖世偉教授，兩位專家意見皆認為商業的本質應為保證雙方交易的完成，不能因某個惡意交易行為，而一併犧牲、抹去其他交易行為，這將傷害商業的本質—信任，亦傷害了區塊鏈的信任機器美譽。

[15] 2016 年 6 月 17 日，一個利用以太坊技術打造智能合約平台的去中心化網路組織 The DAO 遭到駭客入侵，盜走了約 370 萬個以太幣。而後持有 The DAO 以太幣 Token 的投資人，投票決議採取硬分岔作法，從遭竊前一刻的區塊，重新分出另一條獨立的分支區塊鏈，讓 The DAO 的區塊鏈回復到被盜前的狀態，讓遭竊的以太幣的該段區塊鏈失效作廢。

doi:10.6342/NTU201700214

未來我們將面臨更多應用，而應用亦將帶來更多問題與討論，這些正面與負面的意見，都將使區塊鏈技術更加成熟，區塊鏈技術未來的走向也將更加明確。

doi:10.6342/NTU201700214

第六章 區塊鏈技術對我國經濟之影響與建議

透過區塊鏈技術，除了對證券及期貨業有提升效率與降低成本的效果之外，對我國經濟亦有相當影響，另本研究亦針對區塊鏈技術之應用提出建議。

6.1 區塊鏈技術對我國經濟之影響

區塊鏈技術對於我國經濟之影響力，可分正面、負面，以及綜合效果進行討論。

1.正面效果

(1) 對我國經濟發展的優化

證券及期貨市場乃是經濟發展的資金池，透過資金流動，企業得以募集資金、進行避險，透過區塊鏈技術，企業得以更低廉的成本進行企業投資、融資、避險之資金，帶動實質經濟活動之效益。

(2) 培育金融人才

由於區塊鏈技術已獲得政府與業者之重視，透過政策宣導與產學合作，使學生與在職者獲得區塊鏈技術之相關技能，進而使我國金融人才之質與量皆提升。

(3) 我國就業走向人才高品質、高科技、高產值

區塊鏈技術屬高科技產業，應用到金融業，促使金融業人才更加高端、高品質，透過低成本、高產值，提升我國就業人才品質，並提高產品的附加價值。

(4) 有利於普惠金融之發展

法國經濟學家 Thomas Piketty (2014) 提出貧富不均將成為嚴重的社會問題，必須進行改革，否則真正的民主秩序會受到威脅。透過區塊鏈技術的低成本，將

doi:10.6342/NTU201700214

使貧富不均的情形有所改善，例如非洲肯亞的銀行設施稀少，但智慧型手機幾乎無處不在，透過業者推出的移動支付系統 M-PESA 可購買比特幣，幫助在國外工作的肯亞人無需支付高額國際銀行轉帳費寄錢回家，或沒有銀行帳戶的窮人們，亦能透過手機進行便利的轉帳活動，且手續費比透過銀行轉帳更低廉，能使過去接觸不到金融服務的貧窮階級亦能有利用新科技發展經濟的機會。

區塊鏈技術能降低金融活動成本，並使得金融服務的效率提升，將有利於普惠金融之目標，降低貧富不均的問題。

2.負面效果

(1) 加大高低能力者的所得差距

由於區塊鏈技術係屬高級知識型的專業技術，低能力者不具備學習與適應新科技的技巧，將加大使用者能力的差距，而低能力者可能必須進行工作轉型、甚至有失業的危機，顯見專業技術的轉換困難。

(2) 法令修改尚未趕上科技進步的速度

當區塊鏈技術欲應用於某些行業或作業時，可能面臨無法規可適用，可能導致創新產業遊走在法律邊緣，甚至發生違法的風險。

3.綜合效果

正如 BCG 研究報告 (2016) 指出，預估德國於 2025 年全面採用工業 4.0，將導致淨增加 35 萬個工作，實際情形為機器人與電腦取代人力、減少 61 萬個工作，而資訊科技與資料科學的應用導致 96 萬個工作的增加，即達到產業升級、提高我國競爭力之效果。故新技術不必然導致工作減少，甚至會使工作機會增加，但必然的是必須面對工作型態轉變，區塊鏈技術的智能合約可使因交易對方不履約之爭議案件減少，但不代表律師工作的消失，而是律師工作內容進階為設計區塊鏈

doi:10.6342/NTU201700214

的智能合約程式，這樣的協議程式必須由律師這樣的專業人士設計才能將交易爭議最小化。惟區塊鏈技術導致的工作轉型，過程將是一場嚴格的考驗。

表 12　區塊鏈技術對我國經濟之影響

效果	影響層面
正面效果	(1) 對我國經濟發展的優化 (2) 培育金融人才 (3) 我國就業走向人才高品質、高科技、高產值 (4) 有利於普惠金融之發展
負面效果	(1) 加大高低能力者的所得差距 (2) 法令修改尚未趕上科技進步的速度
綜合效果	BCG 預估德國於 2025 年全面採用工業 4.0，將導致淨增加 35 萬個工作。即工作機會增加，但必須面對工作型態轉變的考驗

資料來源：本研究整理

6.2 建議我國因應對策

因應區塊鏈技術的快速發展，我國監理單位、業界與學界，應共同學習、迎接新挑戰。

1.儘速調整法規

由於金融業法規繁複，金融業者必須隨時注意主管機關所頒布的法令，甚至是關心未來法規的走向，以避免投入大量成本進行研究發展後，卻面對法令規章的禁止，不僅耗費研發成本，甚至可能導致違反法規的風險。故建議主管機關在面對新科技時，可以先提出法規修改的大方向，給予業者、市場去進行討論後，再主導一個各界希冀發展的方向，以降低我國金融業者的研發成本，亦使我國整體市場能共同朝同一個方向發展前進。

doi:10.6342/NTU201700214

2.規劃因應監理沙盒 (Regulatory Sandbox) 未來的挑戰

由於科技的日新月異，新科技的使用範圍可能已經超過現行法規規範之範圍，為避免因法規限制，而導致國內運用新科技的產業發展受限，甚至違法，英國、新加坡與香港政府已先後推出「監理沙盒」方案。監理沙盒係指在一個模擬環境中，讓業者測試新的產品、服務，以及新的商業模式，而不必受限於現行規範，但必須與監理單位進行良好的溝通與陳報，共同解決測試過程中發現的問題。

我國刻正因應推出監理沙盒，進行研議修正相關金融法規，2016 年 12 月 19 日，我國立法院已初審通過「監理沙盒」（金融科技創新）八法，包含銀行法、證券交易法、期貨交易法、電子支付機構管理條例等 8 個法部分條文修正草案，預估 2017 年下半年可正式上路。金融監督管理委員會亦於 2017 年 1 月 12 日公布「金融科技創新實驗條例」草案，此可為我國金融科技發展之里程碑，草案中條列申請進入金融科技創新實驗之流程，並廣邀業者提供意見，以利我國金融科技發展符合市場所需。

特別要注意的是，未來這些在沙盒中的實驗都將進入現實環境中，如何兼顧原有金融機構與新創業者皆能符合相同的金融業法規，又能提供消費者高品質、低費用的金融服務，是未來完成實驗後的另一個挑戰，建議監理單位與業界可共同研議規劃。

3.建立研究聯盟

一個新技術的養成的過程艱辛，由於眾人尚不知如何應用新技術，故集合眾人力量，將有利於新技術的開發，甚至在群體中能建立規範，獲取主導地位，可制定共同標準，形成領導者的優勢利益，使眾人以其為架構執行。故國際間已組成多個聯盟進行區塊鏈技術研究中，例如前述的 R3 聯盟，政府與業界若能合作組成團體，共同研究區塊鏈技術，分享彼此觀點，縮短切入跨領域的時間與成本，

doi:10.6342/NTU201700214

從彼此的想法中獲取新創意，應可使臺灣市場更加便利交易，進而吸引更多國內外交易人進入市場。

4.由內部先試行區塊鏈技術

政府與業界皆可透過私有鏈做法，先內部試行相關區塊鏈技術，將部分作業應用區塊鏈技術試行，再進行調整與研究。

5.積極舉辦黑客松活動

黑客松 (Hackthon) 係結合程式設計 (hack) 和馬拉松 (marathon) 兩個字的新名詞，即程式設計馬拉松大會，透過高手們在短時間內進行腦力激盪，進行開發程式的競賽活動。2016 年 8 月，臺大黑客松 (HackNTU) 即以區塊鏈為重點，並以食安為主題，進行黑客松競賽。建議未來可舉辦以證券及期貨業應用為主題之黑客松，使證券及期貨業應用區塊鏈技術更加成熟。

6.業者加強與科技公司合作，或直接轉投資金融科技公司

區塊鏈為資訊新技術，而主管機關已開放銀行及金融控股公司申請轉投資資訊服務業及金融科技業，例如利用區塊鏈技術從事輔助金融機構業務發展之資料蒐集、處理、分析或供應等，得不受銀行法及金融控股公司法有關投資非金融相關事業之額度限制。故建議金融機構可加強與科技公司合作，甚至直接轉投資金融科技公司，使其凝聚創造最大績效。

7.產學合作

人才的培養之路耗時數年，若能由業界與學界共同合作，由業界高階主管至學校演說，使學校與學生們瞭解現行業界的人才需求方向，進而提供所需的教學，將可提高學生們習得應用技術之品質，並可達畢業即就業之效。

doi:10.6342/NTU201700214

第七章 結論與建議

7.1 結論

金融機構以信任為基礎，具有「信任機器」美譽的區塊鏈技術，自然吸引著金融機構研究的好奇心。本研究透過較為人所熟知的區塊鏈應用—比特幣，來介紹區塊鏈技術的基本特性，而比特幣自 2009 年推出後的 8 年期間，區塊鏈技術亦已開始應用於跨國匯款與證券發行等實際作業中。

比特幣的區塊鏈技術有許多優點可以應用於金融業中，例如資料易於驗證且不可竄改、保存具高度安全性、身分隱密性高，且能阻止惡意竄改交易紀錄的行為等，更重要的是，區塊鏈技術解決了過去技術無法解決的拜占庭將軍問題與重複支付問題，這是網路技術上的一大突破。

我們將區塊鏈技術應用於證券及期貨市場時，可以預期將得到交易即結算、交易無休、提升證券及期貨之交易量、系統具相對穩定性、減少錯帳、節省寄送交易紀錄之成本，以及節省中介機構的相關作業成本等效益，其中交易即結算作業，能達到簡化交易後結算交割流程、降低交易違約風險，以及或可調整期貨交易之預繳保證金制度等規範，此 3 大效益最為顯著。

但事實上，比特幣的技術原理，並不完全適用於金融業，例如比特幣的去中心化、匿名制等，皆是高度監管的證券及期貨業中所不適合運用的。但透過發展的過程中的技術演變，建議可以採用不同的技術方法，例如採私有鏈、採用其他共識機制、運用智能合約、將監管單位機構為節點，甚至運用於洗錢防制與 KYC 作業之執行、提升法遵科技應用之效率，並可先以鉅額交易等較不具時間急迫性之作業試行，而業界若組成聯盟鏈更可達到資訊共享之效，使得區塊鏈技術與證券及期貨業的作業能相輔相成，達到提升交易相關流程之效率，並降低成本費用的效果。其中，運用於國際重視的法遵科技時，更可達到節省執行成本、節省舉

doi:10.6342/NTU201700214

證成本，以及發揮專業機構與專業人士能力之最大效益等 3 大功效。

區塊鏈技術有相當大的應用潛力，但目前仍有法規面、速度面、實證面等三大議題尚待解決，分別為完成交易的速度慢、法規修改未及，以及尚未受到完整的實證考驗，以太坊的硬分岔事件只是一個起點，待未來技術的改進，且經過更多應用與討論後，這些正負面的意見，都將使區塊鏈技術更加成熟，區塊鏈技術未來的走向也將更加明確。

7.2 區塊鏈技術對我國經濟之影響與建議

區塊鏈技術具有使我國經濟發展與金融人才優化，並促使普惠金融的實現等正面效益，但亦難免產生加大高低能力者的所得差距與法規修改未及科技進步速度等缺點，而綜合來說，工作數量將可能是淨增加，但是卻必須面臨工作型態轉變的嚴格考驗。

為了與全球區塊鏈技術的進步同速，建議政府機構儘速修正法規，並規劃因應監理沙盒未來的挑戰，使相關業者能實地推出新商品及新服務，了解理論與現實的不同，儘速進行修正。另建議政府與業者皆可建立研究聯盟，並於內部先試行區塊鏈技術，並可透過舉辦證券及期貨市場相關應用之黑客松活動，集眾人之力、集思廣益，來推動區塊鏈技術，業者亦可加強與科技公司合作，或直接轉投資金融科技公司，學校亦可透過產學合作，直接瞭解業界所需要的技能，培養業界所需專業人才，以提高我國產業發展效率，並降低相關時間與金錢成本。

7.3 建議未來研究方向

區塊鏈技術隨著越來越多人力的投入研發，刻正急速發展中，本研究撰寫之時，區塊鏈技術尚處於探索期，當開始進入初步運用、成長期時，將有出現更多問題，也出現更多解決問題的答案，後續研究可再針對各節點權力如何配置，或

doi:10.6342/NTU201700214

共識機制的改良，以及智能合約的應用等新技術的演進，進行下一步討論，將使區塊鏈技術築夢踏實、更加成熟。

doi:10.6342/NTU201700214

參考文獻

Accenture, Blockchain-enabled distributed ledgers: Are investment banks ready?

Accenture, Blockchain-enabled distributed ledgers: Are investment banks ready? 2016.2。

BCG (2015) , Man and Machine in Industry 4.0: How Will Technology Transform the Industrial Workforce Through 2025?, 2017.1.4。

blockchain.info 網站，2016.12.9。

CFTC, Special Address of CFTC Commissioner J. Christopher Giancarlo Before the Depository Trust & Clearing Corporation 2016 Blockchain Symposium，2016.3.29。

coinmarketcap.com 網站，2016.12.9。

De Sousa, Agnieszka, Metals Trading Goes Old School During LME's Electronic Shutdown , Bloomberg, 2016.7.22。

Euroclear & Oliver Wyman, Blockchain-In-Capital-Markets, 2016.2。

Gil-Pulgar, Julio, Bitcoin: Welcome to the Fourth Industrial Revolution, Bitcoin.com, 2016.10.7。

maicoin.com 網站，2016.8.15。

Moody's Investors Service, Credit Strategy -- Blockchain Technology: Robust, Cost-effective Applications Key to Unlocking Blockchain's Potential Credit Benefits , 2016.7.21。

Piketty, Thomas，二十一世紀資本論，衛城出版，譯者：詹文碩、陳以禮，2014.11.14。

Santander InnoVentures, Oliver Wyman and Anthemis Group , The Fintech 2.0 Paper, 2015.6。

Satoshi Nakamoto, Bitcoin:A Peer-to-Peer Electronic Cash System, 2008。

doi:10.6342/NTU201700214

Swan, Melanie, Blockchain: Blueprint for a New Economy, Oreilly & Associates Inc, 2015.2.8。

The Economist, The great chain of being sure about things, 2015.10.31。

The Goldman Sachs Group, Inc. Blockchain: Putting Theory into Practice, 2016.5.24。

Wadhwa, Tina, Welcome to the 'self-driving car of finance', Business Insider, 2016.8.21。

WEF, Deep Shift Technology Tipping Points and Societal Impact Survey Report , 2015.9。

WEF, The Future of Financial Services, 2015.6。

Wharton FinTech blog, What is FinTech? 2014.9.4。

Wild, Jane, Arnold Martin and Stafford Philip, Technology: Banks seek the key to blockchain, Financial Times, 2015.11.2。

台灣金融研訓院資料，監理科技創新趨勢新思維及對我國金融業之影響，2016.12.15。

朱漢崙，金融區塊鏈平台成軍，工商時報，2016.10.17。

吳怡靜，下一件大事：第四次工業革命，天下雜誌 590 期，2016.1.19。

沈庭安，DAO 遭駭事件打破區塊鏈不可逆神話，iThome 電腦報周刊，2016.7.30。

金融監督管理委員會，金融科技發展策略白皮書，2016.5。

唐文劍，呂雯等，區塊鏈將如何重新定義世界，機械工業出版社，2016.6.1。

許庭瑜，第 5 代高速交易系統 今上線，工商時報，2016.12.19。

陳一姍，兆豐繳 57 億給銀行業上的課，天下雜誌 605 期，2016.8.31。

彭禎伶，金融創新准許試辦 財委會初審通過修正案，工商時報，2016.12.19。

期交所網站，網址 http://www.taifex.com.tw/。

辜騰玉，區塊鏈技術演進史，iThome 電腦報周刊，2016.4.23。

黃彥棻，駭客入侵一銀 ATM 流程追追追，iThome 電腦報周刊，2016.7.25。

doi:10.6342/NTU201700214

黃詠淳，加拿大皇家銀行舉辦之「中央銀行及官方機構研討會」出國報告，中央銀行，2014.8.1。

楊雅筑，46 小時動腦不間斷 台大黑客松圓滿落幕，中時電子報，2016.8.21。

廖君雅，一次搞懂什麼是區塊鏈 第四次工業革命最大的驅動力，財訊雙週刊第 507 期，2016.7.20。

睿富者，世界經濟論壇研究報告出爐！6 張表，掌握 FinTech 創新關鍵，數位時代雜誌，2015.12.21。

維基百科，金融科技，比特幣，區塊鏈，位元，洗錢，雷曼兄弟迷你債券事件，公開金鑰加密，拜占庭將軍問題，Nonce，湯瑪斯•皮凱提，TCP/IP 協定族，駭客松。

蔡淑芬，FinTech 成全球金融業里程碑，工商時報，2017.1.10。

魏喬怡，新聞辭典－監理沙盒，工商時報， 2016.7.22。

證交所網站，網址 http://www.twse.com.tw/。

doi:10.6342/NTU201700214

附錄一

日期：2016 年 12 月 30 日

時間：下午 4 時 30 分

受訪人：臺灣證券交易所 黃乃寬副總經理

訪談紀錄

一、發展現況

問題 1：經過這些年的發展，比特幣與區塊鏈逐漸走入金融、食安等大眾應用，您如何看待目前正在發展的區塊鏈技術?

答：無論是證券或期貨，以集中市場是一個求高速的交易模式，不太容易在現在的交易環節就可以應用區塊鏈，也許是交易完成後，不求時間的作業，例如交割是可以的。

銀行的業務有許多是 over-the-counter (場外交易) 的，例如 Swap[16]，正是所謂的 P2P，最適合區塊鏈應用，交易雙方不需要相互認識，但證券及期貨交易本來就有交易所為中心，不透過交易所很難，不論什麼都是有成本的，無論是交易結算都很有效率了，要比交易所或集保有效率很難，都是有成本的，集中式已經壓低成本。

鉅額期貨交易是可能的，舉例來說，IRS 就是一種 over-the-counter 的衍生性金融商品，有一部小說改編的電影「大賣空」(The Big Short)，作者 Michael Lewis 在撰寫這篇小說時，考證較多、誤導較少，可參考。小說中即提到 Swap 有高達三十幾頁的合約內容，必須由律師等專業人士審定，故過去需要 3000 萬美金才能承作，若能以區塊鏈技術將契約條款程式化，可以降低大量律師、

[16] 一種衍生性金融商品，係交易雙方約定在未來某一期限相互交換各自持有的資產或現金流的交易形式。較為常見的是外匯或利率之到期交易，多以避險或投機為目的。(資料來源：維基百科，掉期交易)

doi:10.6342/NTU201700214

CFA 去看合約、契約的成本，原來需要兩個禮拜的作業時間可以縮短為兩天，用到的人力很少，成本降低，門檻就降低，R3 已經利用區塊鏈做到目前 (場外交易) 市場最大的 IRS。

問題 2：目前區塊鏈技術尚在發展初期，且存在很多問題，例如國內外之區塊鏈技術皆缺乏統一標準、新型監管方式尚無明確定論(例如監理沙盒)等。對於這些現實生活中存在的挑戰，您有什麼看法?

答：目前區塊鏈技術還沒有進入監理沙盒的資格，例如前揭的 IRS 不需要進入監理沙盒，Swap 合約是自律的。因應 2008 年雷曼兄弟案後成立的 Dodd-Frank Act[17]規定，亦只是從不需申報到申報，而不需事前申請，從此後只要做 over-the-counter derivatives (衍生性金融商品) 都要向監理機構 (以臺灣來說就是櫃買中心) 進行申報。

監理沙盒最重要的概念是，因為應用的新的商業模式，此模式尚無法規依循，如同做實驗中的新藥，有些不治之症的病人，經醫病雙方合意進入實驗，如同正式法律不允許，但你從前醫不好的病，或醫病很貴，可以醫好或降低成本，引申到夠新的服務或更低的成本服務，能成為普惠金融。

如同 IRS 的合約可以降低成本，如同 Robo-advisor (機器人理財)，數位經濟的特色即每多一份服務或商品的邊際成本趨近於零，故其營運需要規模化、大量的服務人數，因收費雖低，但規模大，故總量大，故其連結性必須很高。

二、防弊、資安問題

問題：對於以太坊的 The DAO 遭盜幣衍生之硬分岔事件，開發者 Vitalik Buterin

[17] 全稱《多德-弗蘭克華爾街改革和消費者保護法》(Dodd-Frank Wall Street Reform and Consumer Protection Act)，被認為是 20 世紀 30 年代以來美國改革力度最大、影響最深遠的金融監管改革。該法案旨在通過改善金融體系問責制和透明度，以促進美國金融穩定、解決大而不倒問題、保護納稅人利益、保護消費者利益。(資料來源：MBA 智庫百科，多德-弗蘭克法案)

doi:10.6342/NTU201700214

逆轉區塊鏈，有何看法?

答：以太坊的硬分岔事件如同兒戲，證券及期貨市場亦有此概念，即「倒帶」(unwind)。

以 1995 年的「327 國債期貨事件[18]」為例，上海證券交易所宣布所有國債期貨交易無效，宛如以太坊事件，因有人操縱市場。Unwind trade 的代價是交易所董總下台，國債期貨 20 年不再交易、直到去年，代價很大。但在臺灣我們仍然保證交割，證交所是交易所，亦是結算所，是買方的賣方、賣方的買方，即 novation。在民國 81、83 年厚生、華國股票違約案，同一批人將市場不要的股票炒高，買賣方、證券商都是串通好的，T+2 日買方不付錢，負責交割的證券商進而宣布倒閉，當時我們有兩個選擇，unwind 或認賠，第一次賠 8 億元、第二次賠 20 億元，unwind 是一種選擇，但不會選擇它。87 年的順大裕，如果要賠是 80 億元，但在過程中即已發現這一個不值錢的股票被炒高，那次就有抓到 (企圖犯罪者)。

以太坊的硬分岔，在真正的商業中等同兒戲，作為一個中介平台，正辦應是自賠，認了自己做的不是。以太坊開發者是一個技術人員，企圖做商業，但離商業還太遠。交易所的責任即是保證交割，無論是自己拿出錢來，或是找到應該負責的人負責，而非 unwind。

硬分岔在網路遊戲時可以做，但做商業生意是不能這樣作業的。身為第三中介者，還是必須由我們做到。不重要的事可以做，重要的事、跟資產有關的，不能這樣做。

三、應用端

問題 1：請問證交所對區塊鏈技術的主要發展業務與規劃為何?初步成果為何?

[18] 1995 年 2 月 23 日晚 23 點，上交所經過緊急會議後宣布：1995 年 2 月 23 日 16 時 22 分 13 秒之後的所有交易是異常的無效的。(資料來源：維基百科，327 國債期貨事件)

doi:10.6342/NTU201700214

答：如同剛才所講到的，最適合的就是場外交易，所以可能是櫃買最先適用，債券是議價的，最適合 P2P，又沒有時間急迫性的交易。集保的目前效率雖然很難被挑戰，但其最有壓迫感。以國外案例來說，也是 post trade 為區塊鏈最佳應用。

問題 2：對於臺灣金融市場，或針對證券及期貨市場，未來應用區塊鏈技術發展有何建議或看法?

答：可以分為下列 3 點：

1.不要拘泥於比特幣如何應用，比特幣用了許多很老的技術來做信任機制，分別為:

(1)分散式資料庫；

(2)共識決解決拜占庭問題；

(3)smart contact，如同銀行的第三方支付，買賣雙方合意，DVP[19]；

(4)密碼學技術

①hash

②金鑰:可加密卻不需要第三方認證的憑證，現行我國證券及期貨已經正在使用，唯一不同的是，區塊鏈技術連發憑證的單位都不需要，使用者可以自己找到公鑰及私鑰，公開的就是我的 ID，私鑰就是 key，但比特幣可以不斷找新的 key，即可不斷使用新的，故初始時被用來洗錢、販毒等不法行為，但金融業要求實名制。

但我們是可以從前面這四項中挑選其中的幾樣來使用，例如比特幣達到

[19] 貨銀對付制度（Delivery Versus Payment，簡稱 DVP，即一手交錢、一手交貨）又稱券款對付，是指證券登記結算機構與結算參與人在交收過程中，當且僅當資金交付時給付證券、證券交付時給付資金，交收完成後不可撤銷。（資料來源：MBA 智庫百科，貨銀對付制度）

doi:10.6342/NTU201700214

共識需要 10 分鐘，對於交易來說速度太慢了。

2.做區塊鏈是為了趕流行，還是為了用而用？這不一定是最好的解決辦法，只是很多解法的其中一個。區塊鏈技術還處在行銷名詞這個階段。

3.區塊鏈不是不要錢的，也是要錢的，誰付錢？如果把建造及維持成本考慮進去，成本不一定是原來想的這麼低。

doi:10.6342/NTU201700214

附錄二

日期：2017 年 1 月 12 日

時間：下午 8 時 20 分

受訪人：臺大金融科技暨區塊鏈中心召集人、臺灣大學資訊工程學系 廖世偉教授

訪談紀錄

一、交易機制

問題：Gcoin 如何做到每 15 秒結算一次？與比特幣設計有何不同？風險差異為何？

答：我們假設聯營的 (風險) 機率會降低，我們用的是馬可夫鏈[20]去 model (設計模型、架構)，比特幣是 51% attack (攻擊)，Gcoin 可以達到 99.99% attack，設計一個安全性比較高的 model，且 Gcoin 風險低又是認許制 (permission)，而比特幣是非認許制 (permissionless)，兩者的 security model (安全架構) 不同。

二、發展現況

問題：目前區塊鏈技術尚在發展初期，且存在很多問題，例如國內外之區塊鏈技術皆缺乏統一標準、新型監管方式尚無明確定論(例如監理沙盒)等。對於這些現實生活中存在的挑戰，您有什麼看法？

答：現在監理沙盒要過金融八法，(臺灣) 現在已改名為金融科技創新法，今年下半年才可能完全通過，要看應用為何。例如玉山銀行與臺大校園點數系統合作，因為沒有牽涉到新臺幣，這不是數位新臺幣，只是點數，所以可以由臺大 100 家商家有一半來使用這個系統。但 F 銀行是做行員之間的小額支付，可能就會碰到數位新臺幣的問題，可能就會需要等金融八法通過才能落地。

[20] 比特幣的區塊鏈技術採「均勻工作量證明機制」(Uniform Proof of Work)，Gcoin 則採用動態非線性工作量證明機制 (Non-Uniform and Non-Linear Proof of Work)，並透過馬可夫鏈 (Markov Chain) 的模擬，調整每個聯盟成員獲選為驗證者的困難度，避免趨向獨佔驗證的可能性，解決了 51% 攻擊 (51% Attack) 的問題。(資料來源：資料來源：Gcoin white paper Chinese, Hank edited this page on Sep 20 2016, 2 revisions)

doi:10.6342/NTU201700214

這是我們臺大可以超前的地方，我們不需要進入監理沙盒。

三、防弊、資安問題

問題：對於以太坊的 The DAO 遭盜幣衍生之硬分岔事件，開發者 Vitalik Buterin 逆轉區塊鏈，有何看法?

答：以太坊不只是去(2016)年 7 月 20 日發生的硬分岔，過去紀錄已達 3 次硬分岔了，這讓我們認為比特幣可能會比較成功，以太坊這樣做讓人擔心。就像銀行如果被盜，這家銀行說我被盜的新臺幣我都不認，我硬分岔來重新發行新臺幣，銀行不太可能這樣做，應該是該賠的賠，以及趕快去抓駭客。但以太坊的開發者採硬分岔，不認賠這個錢。

但是如果把以太坊想成一個 experimental platform (實驗平台) 的話，不像比特幣是玩真的，那又還好，但它還是會影響到比特幣、區塊鏈的聲譽，也會影響到大家對區塊鏈的信心。

四、應用端

問題 1：請問臺大金融科技暨區塊鏈中心對區塊鏈技術的主要發展業務與規劃為何? 初步成果為何?

答：我們就做兩件事，一件事是 build infrastructure (建立基礎建設)，第二件事就是 develop talents (培養人才)，就是去訓練最優秀的 google 等級的人才。目前不專注於營利，就像 1992 年做互聯網的基礎建設是賺不到錢的，希望為臺灣、為這個世界奉獻，我們在思考怎麼改變世界。

問題 2：對於臺灣金融市場，或針對證券及期貨市場，未來應用區塊鏈技術發展有何建議或看法?

答：應該是可以幫助交割的部分，因為區塊鏈沒有 database (資料庫) 的速度那麼

doi:10.6342/NTU201700214

快。有些交割的時間越長，或牽涉到手動的部份，如果靠區塊鏈可以讓作業都在智能合約上，加上它有共同帳本的好處，可以讓交易所更 streamline (作業簡化、有效率)，這是解決的一個痛點。

另一個痛點是 Private equity (私募股權)，其實在矽谷也是比較黑箱的，可能只給親朋好友，可不可以讓它都在區塊鏈上，讓它可以比較公平、公正、公開，讓募資容易一些。

交易之後還有清算、結算、還有 custodian (保管機構)，就像我買的黃金不會到我手上，會到 custodian 的地方。如果是交易的部份，現在還不太適合用區塊鏈，因為區塊鏈是一個安全、信任的機制，希望它不能竄改、又要永久保存，這些都是有成本的，所以它再快都比不過 database 快。

故在證券及期貨市場，如果是談論交易的部分，它再快都比不過 database 快，但從交易到交割，中間有很繁複的一些過程，而它能幫助的是交割的這部分。如果有人說他的交易可以比較 relax (不急迫的)，每秒 7 個 tps[21]他都可以接受，就比較想對方向了。在這個領域，如果有人說「天下武功，唯快不破」，他應該是錯的方向，他有點 miss 掉 (未領會) 區塊鏈的本質，交割和保管的部分比較適用。

智能合約也是需要先圈存，如何能確保十個人執行交易結果會相同，就必須先繳保證金、圈存，否則十個人的執行結果可能會不同。如果後執行的人看局勢不對、可能會賠錢，就把錢抽走，將造成執行先後順序不同的人，得到的結果不同，所以智能合約要先圈存、再開始執行，才能確保每個交易的執行結果相同。

21 Tps (transaction per second)，即每秒交易筆數。

doi:10.6342/NTU201700214