國立政治大學金融學系研究所

碩士學位論文

區塊鏈應用：台灣股票結算交割系統

Blockchain Application: Taiwan Stock Clearing and Settlement System

指導教授：廖四郎 博士

研究生：王肇遷 撰

中華民國 106 年 6 月

謝辭

碩士論文完成之際是兩年碩士學習的終點，也是作為學生的一個里程碑，達成個里程碑靠自己一個人是無法達成的，是靠著許多人有形無形的幫助，對我完成論文有極大的幫助。

最先要感謝我的指導教授 廖四郎老師，每次與老師討論結束後總會讓我對論文內容產生方向感，並且因此充滿動力，有繼續堅持下去的能量。感謝口試委員老師，林建秀老師與陳芬英老師提出的寶貴建議。感謝我的朋友們的陪伴與互相扶持，每每在我有困惑時願意與我討論的朋友們，讓我釐清疑惑並且找到解決的辦法。最後也是最重要感謝我的父母，感謝他們對於我的照顧及包容，讓我可以無後顧之憂的完成學業。

謹以本論文獻給我最親愛的父母、最尊敬的老師以及每位幫助過我的朋友。

王肇遷　謹致於

國立政治大學金融系

中華民國 106 年 6 月

摘要

區塊鏈技術藉著比特幣而發揚光大，經過將近十年的考驗，區塊鏈被視為足以改變全球經濟模式的火紅科技，各種應用的想法如雨後春筍般出現，本文趁勢提出台灣股票結算交割的區塊鏈應用。本文從最原始的區塊鏈系統——比特幣介紹起，深入討論區塊鏈運作的機制，包括共識的形成與交易的驗證方式。比特幣的區塊鏈系統中的某些設定對於股票結算交割來說是缺陷，本文提出改良的方式，包括許可制的區塊鏈、引入特殊功能節點及採用實名制等，試圖讓區塊鏈技術能夠完美的應用於結算交割系統。最後分析應用區塊鏈之後所能夠達到的經濟與社會效益。

關鍵字：比特幣、區塊鏈、台灣股票結算交割系統

Abstract

After nearly ten-year challenge, blockchain was known because of Bitcoin, and regarded as the most famous technology that could change the way how the whole world works. Lots of application ideas appear at this moment, this paper tries to follow the trend and discuss about the Taiwan stock clearing and settlement system. Begin with the original blockchain system, Bitcoin, reveal how actually blockchain works including the formation of consensus and the way of transactions verification. There are some defects when implementing the application by using Bitcoin system directly. This thesis proposes the way to improve the blockchain system which includes permission blockchain system, special functional nodes and implementation of real name blockchain system, and try to make modified blockchian system applicable to clearing and settlement system. Last but not least, this thesis analyzes the benefit of economy and society when the application is employed.

Keywords: Bitcoin, Blockcahin, Taiwan Stock Clearing and Settlement System

目次

表次

圖次

第一章 緒論

第一節 研究背景與動機

2008 年，區塊鏈幾乎橫空出世，中本聰一篇不到十頁的論文 ”Bitcoin: A Peer-to-Peer Electronic Cash System” 奠定了區塊鏈技術的雛形。等待了十年之久，區塊鏈終於躍上了世界的舞台，成為最火紅、討論度最高的新科技之一，人們對於區塊鏈的想像來到了巔峰，生活中幾乎所有的事物都能跟區塊鏈搭上關係，舉凡醫療、產銷履歷甚至是政府都將成為區塊鏈的應用範疇，區塊鏈似乎無所不能，沒有什麼應用是它做不到的，但區塊鏈真有如此神通廣大嗎？深入了解區塊鏈之後會發現，區塊鏈確實存在龐大的潛能，但中本聰十年之前提出的區塊鏈系統存在著一些缺陷，並無法適用於每個應用，必須根據不同的應用修正區塊鏈系統中的設定，才能將區塊鏈的潛能完全發揮。

區塊鏈的應用主要分為兩種：一是分散式帳本，作為一個無法任意篡改的資料庫；另一是成為如同比特幣的價值交換網絡。成為另一種資料儲存的形式固然有很廣的應用，但是將價值交換網絡拓展到其他領域能夠產生更大的效益，所以本文以價值交換網絡的角度看待區塊鏈，並將價值交換的網絡應用到台灣的股票結算交割。股票的結算交割將股票所有權轉移，為一個價值交換的過程。區塊鏈是一個價值交換的網絡，透過區塊鏈進行結算交割將會有助於加快結算交割的速度，以及降低人事與系統的成本，為台灣的資本市場創造更有效率的運作方式。

第二節 研究架構

區塊鏈運用到的概念環環相扣，密碼學中的非對稱公開金鑰加密讓資產的所有權可以被確認；哈希函數讓區塊鏈中的所有交易資訊無法被竄改；工作量證明是讓所有的節點達成共識的演算法。以上三點是區塊鏈能夠成為價值交換網絡的要素，本研究的編排期望能讓讀者以有條理及有邏輯的方式了解其中的細節。章節安排如下：

第一章為緒論，說明研究的背景及動機本；第二章會先簡單介紹比特幣，因比特幣為區塊鏈最成功的應用，其地位無法忽視；第三章會對十年前中本聰提出的區塊鏈系統完整的說明，包括其詳細的運作方式；第四章搜集目前正在嘗試以區塊鏈應用股票結算交割的案例，幫助讀者了解區塊鏈在結算交割領域中的進程；第五章為本研究提出的區塊鏈架構、設定與實際的運作方式，也探討經濟效益的分析；第六章為結論。

第二章　區塊鏈簡介—最成功的應用：比特幣

第一節　從比特幣說起

在正式進入區塊鏈之前，我想先從比特幣說起，因為比特幣是區塊鏈到目前其為止最成功的應用。如果將區塊鏈視為一種技術，區塊鏈更是集近代科學的大成，將許多不同領域的技術巧妙地結合起來，完美的解決網路世界中傳遞價值時所產生的問題。

2008 年美國的金融海嘯重創全球經濟，民眾對於金融機構的不信任感達到高峰，美國政府對於各大投資銀行的紓困更是無法被諒解，影響甚至擴散到每個產業、每家公司以及每個家庭。金融機構是整個金融體系的中心，為市場增加流動性、媒合每筆交易的買賣雙方，是維護金融市場健全運作的關鍵。但當金融機構愈來愈龐大、交易的金融商品愈來愈多，與其往來的投資人卻對其一無所知，也認為毋須知道，認為金融機構會替我們管好一切，並且沒有人相信任合一家金融機構會倒閉。事實證明，金融機構並不是不會倒閉，只是大的不能倒罷了（Too big to fail）。

2008年，比特幣的創始人中本聰以電子郵件的方式，在一個密碼學的網站發表了一篇論文” Bitcoin: A Peer-to-Peer Electronic Cash System ”，完整地描述了目前比特幣的架構，以及實際運作的細節。2009年，比特幣正式上線，由中本聰本人開啟了比特幣的第一個區塊「創世區塊」，並在區塊中留下了一段文字，當天泰唔士報的頭條新聞「The Times 03/Jan/2009 Chancellor on brink of second bailout for banks」。隨後，當初收到中本聰信件的玩家們也一一加入，展開這龐大的電子加密貨幣實驗計畫。

2009年1月，中本聰寫下第一個區塊「創世區塊」，並發行第一筆比特幣，共50個。

2009年10月，靠著當時挖礦所消耗的電腦資源，估算出 $1=1309 BTC。

2010年5月，第一筆用比特幣購買商品的交易發生，10000 BTC買一個價值$25的披薩，一美元相當於400個比特幣。

2010年11月，一個比特幣相當於0.5美元，比特幣的市值超過一百萬美元。

2013年3月，比特幣市值超過10億美元。

2013年12月，中國人民銀行表示比特幣不具有實質貨幣的意義，與法幣沒有相同法律地位。中國是最多比特幣交易的國家，超過80%的交易發生在中國。

2014年2月，全球最大的比特幣交易所之一MT.GOX遭到駭客入侵，損失約85萬個比特幣，合當時市值約4.7億美元。

將近十年的時間過去了，比特幣依然存在，且使用的社群愈來愈龐大，人們開始慢慢認同這個電子貨幣，開始利用比特幣交易商品，建立起比特幣的貨幣價值。在這十年之間，比特幣價格反應著三個不同面向的因素：

（一）挖礦所投入的資源：比特幣的產生方式非常特別，礦工（玩家）必須利用電腦運算解決困難的數學問題，最快解出問題的礦工可以獲得比特幣作為報酬，由於獲得比特幣的機會與電腦運算的速度成正比，因此利用更快更好的設備會凸顯自身的挖礦優勢。隨著礦工之間的競爭愈來愈激烈，投入的電腦資源（電力、硬體設施、冷卻系統）也愈多，比特幣的價格必需至少與這些投入相等，對礦工而言才有獲利空間。

（二）市場供需：隨著使用的社群愈來愈大，比特幣卻不會因此增加產量，仍然依照著當初規劃的方式發行（每個區塊產生50個比特幣，約每四年半減半一次，總計發行2100萬個比特幣），所以需求大於供給的情況下，比特幣的價格大幅的上升。

（三）投機行為：當比特幣產生了貨幣價值，人們會對其價值產生預期，成為投機行為的構成要件。在2013年比特幣價格曾經瘋狂的上漲，原因在於中國玩家的投機炒作，價格來到當時的新高1151美元兌換1個比特幣，但隨著中國政府的打壓以及隔年（2014）年初最大的比特幣交易所發生駭客入侵，導致85萬個比特幣遭到竊取，相當於市價4.7億美元的損失，接連的兩個重大事件重創比特幣的價格。經過將近一年的下滑，比特幣看似回歸合理的價格，由下面兩圖可以看出，比特幣的價格與挖礦難度一同上升，代表比特幣反應出其的生產價值。

圖 一 比特幣市場價格[1]

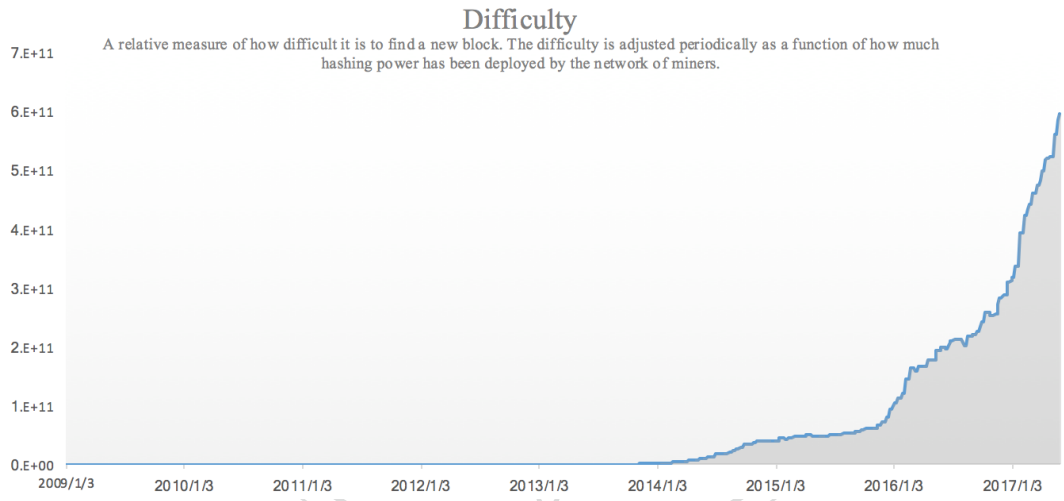


圖 二 運算困難度[2]

比特幣成功的運行了將近十年的時間，除了2014年初MT.GOX交易所遭竊之外，幾乎沒有發生比特幣轉帳交易過程中的錯誤，這對於一個去中心化的電子貨幣系統來說，是史無前例的巨大成功，成功背後隱含著劃時代的意義，不僅僅是在技術上克服了先前難以克服的問題，對於整體社會經濟未來的走向，提供一種選擇空間。去中心化代表著重塑社會經濟的可能性，過去金融市場集中在金融機

[1]資料來源：blockchain.info（網站）

[2]資料來源：blockchain.info（網站）

構，轉帳支付、跨國交易必須仰賴銀行作為金流與信任的中心，區塊鏈技術將有可能取代掉這些銀行的功能，改變金融體系的運作方式。區塊鏈是一種破壞式的創新技術，它改變了原有的制度，並以另一種面貌出現在世人面前。

第二節 共識與信任的建立——拜占庭將軍問題與雙花問題

區塊鏈究竟是何方神聖，可以對發展已久的制度產生巨大衝擊。有兩個存在已久的問題阻礙著電子加密貨幣的發展，比特幣的發明者中本聰在2008年發表的論文" Bitcoin: A Peer-to-Peer Electronic Cash System"中，輕描淡寫且優雅的同時化解了這兩個問題，造就比特幣目前無法取代的地位。

一、拜占庭將軍問題

這是1982年一位美國的計算機科學家所提出的問題，以古老的場景描述著點對點網絡中的共識問題。拜占庭位於現在的土耳其伊斯坦堡，為東羅馬帝國的首都。東羅馬帝國的國土幅員遼闊，為了防守敵軍的入侵，每個拜占庭將軍都必須負責很大的一塊區域，所以將軍們彼此間的距離都相當的遠，將軍與將軍之間只能靠著信差傳遞。在戰爭的時候，只有在所有將軍都同意的情況下，攻打敵方陣營才有勝算，但是軍隊之中可能會有叛徒和敵方間諜左右將軍們的決策，在將軍們達成共識的過程中，如何不被叛徒和間諜影響而達成一致攻擊的共識，就是所謂的「拜占庭將軍問題」。點對點的網絡就像是古老的拜占庭將軍一樣，彼此之間沒有統一發布命令的中心，比特幣卻能透過某些機制達到共識，完美的解決拜占庭將軍問題。

二、雙重花費問題（Double Spend）

在虛擬的網路中，點對點網路的電子貨幣會遇到雙重花費的問題，由於沒有一個中心的結算機構，任何人都可以將同一筆錢重複支付給不同的人，並且沒有方法可以確認哪些交易是合法的。在這樣的情況下，信任不存在於這個網絡之中，貨幣就無法建立價值。區塊鏈特殊的方式記帳，以及上述拜占庭將軍的共識形成，雖然不能完全禁止雙重花費的行為，但能夠保護收款者不會收到重複花費的比特幣。

解決了上述的兩個問題就代表著建立了信任和共識，中本聰的比特幣實驗中，成功讓區塊鏈變成一台信任機器，讓每個節點對於帳本產生共識，而在比特幣爆

紅之後，區塊鏈最為其底層運作的技術，成為多方矚目的重點。

比特幣的成功告訴我們，數位化的資產也能夠產生價值，只要保證數位資產的所有權與唯一性。所有權指的是當我們將資產放上區塊鏈之後，沒有人能夠更改，並且我是唯一有權能夠對此資產進行轉移的人；唯一性指的是這個數位資產沒有辦法被隨意地複製並轉移，也就是沒有雙重花費的可能。保證了這兩件事情，則此價值交換的網絡是完整的。因此，這樣的性質開啟了我們對於資產數位化的想像，以房地產為例，將房地產數位化放上區塊鏈之後，每間房屋會對應到不同的所有權人，當房地產買賣交易產生的時候，房地產的移轉就如同比特幣轉帳一般，直接將所有權轉移給買家。當然，上述的例子簡化了太多的細節，不過理念是一樣的，如果說網際網路是資訊交換的網絡，那區塊鏈就是一個「價值交換的網絡」。

第三節 區塊鏈的特性

這邊歸納出比特幣區塊鏈最重要的幾個特性：

（一）去中心化：區塊鏈是一個點對點的網絡系統，沒有存在任何權威的中心或第三方來維護整體運行，完全靠內部自身的機制來完成信任與共識的建立。

（二）不可篡改性：區塊鏈上的任何資料都無法被竄改，由於其為一條鏈的緣故，所有的資料都依照時間的順序排列，只要竄改了其中一部分的內容就會牽動到其他的區塊，必須要連同所有區塊都一併修改，才能符合所有節點之間的共識。這在實際運作上是不可行的，重新運算每個區塊困難的數學難題過於耗時耗力，因此任何在區塊鏈上的內容都不可能被竄改。

（三）唯一性：以比特幣來說，任何一筆的比特幣都是唯一的，只有那些比特幣的擁有者有辦法使用，並且只會發生一次的所有權轉移，不會發生同一筆比特幣同時支付給兩個不同的人的情況。

（四）公開透明：比特幣的區塊鏈是完全公開的，任何一個參與的節點都會擁有一個完整的帳本，紀錄從創世區塊開始的所有交易紀錄，即使不是節點，任何想要看到區塊鏈上的交易紀錄也是可行的。這樣的特性也是在建立信任，一個每個人都能看到的帳本，當然

能夠取信於別人。但公開透明的特性卻不利於商業上的應用，企業為了維護自身利益，不可能將所有資訊全都放上區塊鏈共享給每個人，造成不必要的損失。因此在應用上，企業仍然傾向於不公開區塊鏈上的內容。

第三章　區塊鏈技術原理

區塊鏈由幾個不同的部分組合而成，宏觀來看，區塊鏈是由一個點對點的網絡構成，每個節點都保有一本形成共識後的帳本，記錄著發生在區塊鏈網絡中的每筆交易；微觀來看，區塊鏈顧名思義就是由一個一個區塊串起來變成一條鏈，依照著區塊生成的時間依序排列下去，每個區塊內記錄著若干筆交易，每筆交易使用數位簽章的方式驗證，確保每筆交易的合法性。

在對比特幣以及區塊鏈有初步認識後，區塊鏈有非常良好的性質，能夠應用的層面也非常的廣，接下來本文將會深入探討比特幣區塊鏈為何能夠擁有這麼多的好性質，運用了哪些技術以及實際上的運作細節。本文將會從最微觀的角度切入，一窺區塊鏈技術的微妙之處。

第一節 哈希函數

哈希函數，又稱雜湊函數。當資料（通常為字串）通過哈希函數之後，哈希函數會壓縮資料的大小，成為一串由英文及數字組成的字串，因此將產生的字串視為資料的摘要（或是指紋），稱為哈希值。

哈希函數有幾個有用的性質：

（1） 易於檢驗：相同的資料輸入哈希函數會得到相同的哈希值。

（2） 單向不可逆函數：無法利用哈希值反推原始的資料內容。

（3） 碰撞性：由於任何資料都可以放入哈希函數，並產生相對應的哈希值（無限大的值域與有限的對應域），因此哈希函數是個多對一的函數。當兩筆不同的資料輸入哈希函數得到相同的哈希值時，就稱為碰撞（collision）。好的哈希函數產生碰撞的機率極低，目前比特幣區塊鏈使用的哈希函數 SHA-256，還沒有被破解，仍然找不到不同的資料卻得到相同哈希值的情況。

（4） 雪崩效應：輸入的資料產生細微的變化時，相對應產生的哈希值會劇烈的變化(超過一半的位元改變)。因此，想要利用資料與哈希值之間的關聯性反推原始資料的難度大幅提高，有效降低資料與其哈希值間的關聯性。例子如下：

Hash(0)= 5feceb66ffc86f38d952786c6d696c79c2dbc239dd4e91b46729d73a27fb57e9

Hash(00)= f1534392279bddbf9d43dde8701cb5be14b82f76ec6607bf8d6ad557f60f304e

Hash(apple)=3A7BD3E2360A3D29EEA436FCFB7E44C735D117C42D1C1835420B6B9942DD4F1B

Hash(apples)= F5903F51E341A783E69FFC2D9B335048716F5F040A782A2764CD4E728B0F74D9

在比特幣的區塊鏈系統中，使用的哈希函數式是 SHA-256，SHA-256 會將資料對應到 $[0,2^{256}]$ 的區間中，產生出一組 256 位元的哈希值。由於上述哈希函數的好性質，區塊鏈廣泛地使用哈希函數，包括交易、區塊、工作量證明與數位簽章，是將整個區塊鏈串連起來的關鍵核心。

第二節 交易

一、交易的紀錄方式

區塊鏈技術除了能夠讓數位貨幣的轉帳順利運營，它還有一個備受關注的功能——「記帳」。區塊鏈是一個分散式的帳本，每個參與的節點都會自己保留並更新這個帳本，除了帳本本身無法被竄改之外，區塊鏈特殊的記帳方式讓每筆交易都可以被追蹤。使用比特幣的玩家都會擁有一個錢包（類似銀行帳戶），存放著所有的比特幣（從別人那邊轉帳而來，或是自己挖礦獲得），不同於一般帳戶管理的方式將所有款項加總，比特幣的錢包會將每筆收到的比特幣分開來存放，這些收到的比特在還沒有被花費之前稱為「未使用的交易輸出」（Unspent Transaction Output, UTXO）。舉例來說，如果乙付給甲 10 比特幣，丙也也付給甲 20 比特幣，甲的錢包不會總計 30 比特幣，而是紀錄一筆 10 比特幣的款項和一筆 20 比特幣的款項，分別來自付款者乙以及丙，且是未使用的交易輸出，這樣紀錄比特幣的方式是為了讓區塊鏈上的記帳更清楚、更容易驗證與追蹤。比特幣的交易紀錄中包含輸入（Input）與輸出（Output），每筆未被使用的交易輸出（UTXO）會是下一筆交易的輸入（Input）。

每一筆交易可能包含若干個輸入（Input）和輸出（Output），上述的例子中，如下圖三，甲分別從乙和丙拿到 10 比特幣和 20 比特幣，若甲欲支付 25 比特幣給丁，就必須把 20 比特幣和 10 比特幣合在一起支付，所以交易的輸入（Input）就有兩筆合計 30 比特幣，把 25 比特幣給丁，再把剩下的 4.9 比特幣還給自己，產生兩筆交易輸出(Output)。而輸入和輸出的差額 0.1 比特幣則會成為節點的交

易手續費（Implied transaction fee）。

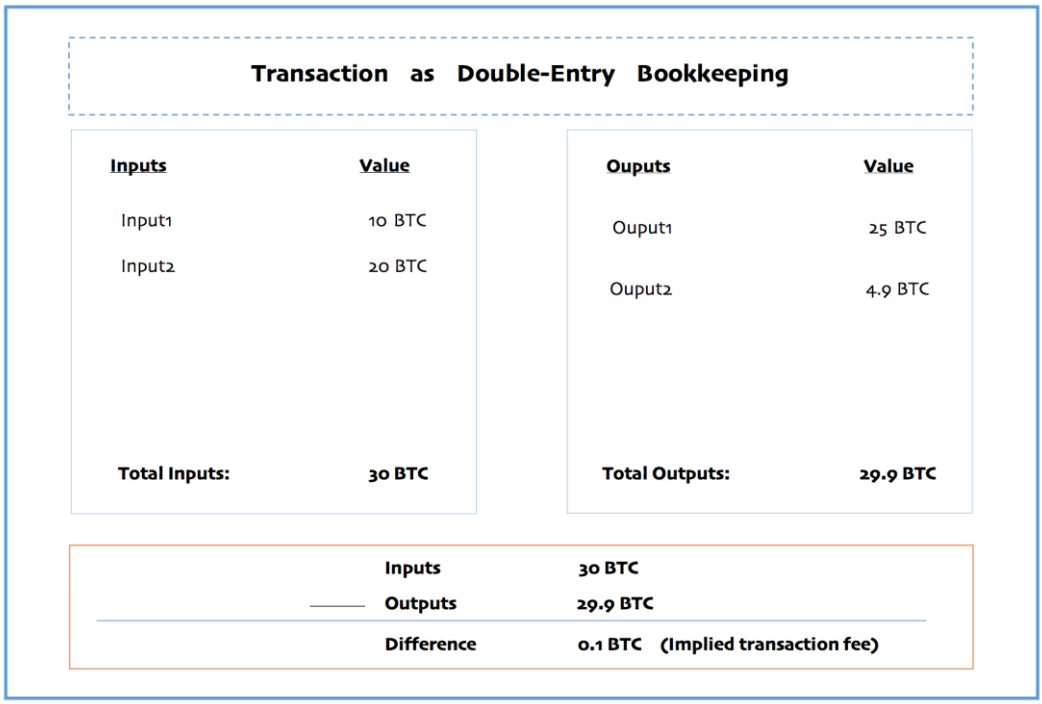


圖 三 比特幣記帳方式

另一個例子如下圖四，第一筆交易中（第一層）Alice 從 Joe 那邊獲得 0.1 比特幣（Output）；第二筆交易中，Alice 要付給 Bob 0.015 比特幣，Alice 在第一筆交易中得到的 0.1 比特幣成為第二筆交易的輸入（Input），同時也被標記為「已花費的交易輸出」（Spent Transaction Output）。而交易的輸出為兩筆，第一筆給 Bob 0.015 比特幣，第二筆將剩下的比特幣 0.0845 還給自己（這兩筆在還沒有花費之前會被視為未被使用的交易輸出），輸入和輸出的差額 0.0005 比特幣會被默認為支付給節點的交易手續費。

圖 四 比特幣的交易紀錄方式

同樣的，當 Bob 要支付給 Gopesh 時，使用到第二筆交易中從 Alice 那邊得到的 0.015，此時這筆比特幣從未被花費的（unspent）變為已花費（spent），並成為第三筆交易的輸入（Input）。

上述為比特幣區塊鏈紀錄交易的方式，使用這樣的方式是有原因的，可以讓交易的驗證更容易，以下會詳細說明比特幣驗證交易的過程。

二、交易的驗證

比特幣交易的紀錄方式讓驗證的過程非常有效率，保留每筆不同來源的比特幣就是為了方便驗證。以上圖第二筆交易為例，Alice 要使用他在第一筆交易獲得的 0.1 比特幣時，這 0.1 比特幣成為第二筆交易的輸入（Input），並且包含第一筆交易的哈希值 (7957a35fe64f80d234d76d83a2a8f1a0d81de548f0a65a8a999f6f18)，節點不用回溯整個區塊鏈一筆一筆的找，只要沿著哈希值找到第一筆交易，就可以確認這筆比特幣是否被花費過。除了確認比特幣是否被花費過之外，更重要的是確認比特幣的所有權，節點需要確認在第一筆交易中，Joe 真的把比特幣的所有權轉移給 Alice，且 Alice 有能夠使用這筆比特幣的權利。確認所有權轉移的過程需要使用到數位簽章的概念，利用密碼學中的非對稱加密技術，達成交易的驗證。

非對稱加密技術提供每個使用者一對公鑰及私鑰，公鑰是公開的，任何人都

有權限獲得其他人的公鑰；相對的，私鑰只有本人會知道，其他人沒有權限得知自己以外的私鑰。當一份文件需要加密的時候，有兩種加密的選擇，一是使用公鑰加密，另一是使用私鑰加密，兩者加密後所傳達的資訊並不同，使用的情況也有所不同。

假設現在有 A、B 兩個人，他們之間有文件的往來並且希望透過加密技術保護文件的隱私，當 A 要將文件發送給 B，A 有以下兩種加密的方式，加密方式產生的效果並不同：

1. 使用自己的私鑰加密：

當 A 使用自己的私鑰加密文件，只要任何擁有 A 的公鑰的人皆可以得知內容，但由於私鑰只有 A 自己才知道，因此這份由私鑰加密的文件所傳達的訊息為：這份文件一定是由 A 加密的。

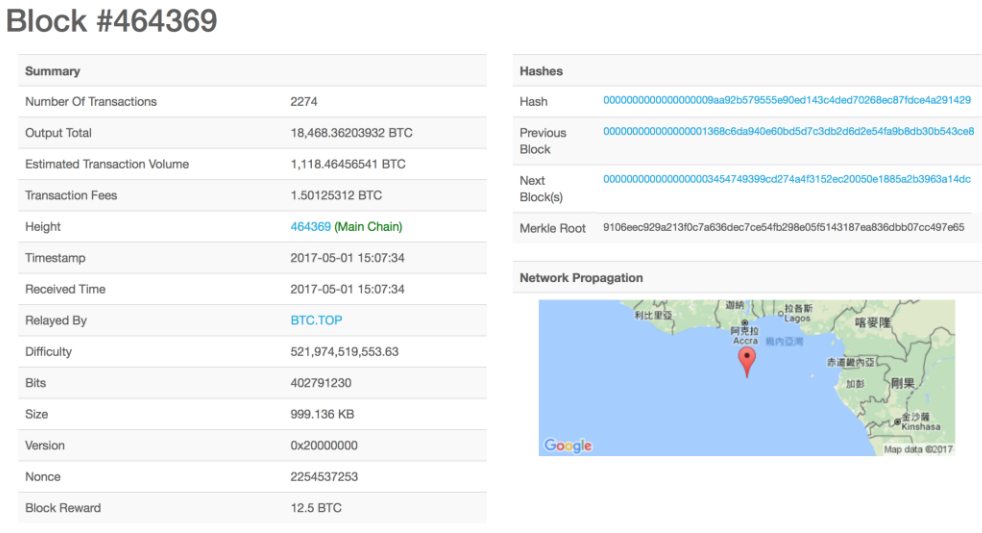
2. 使用 B 的公鑰加密：

當 A 使用 B 的公鑰加密文件，則這份文件只有 B 能夠透過自己的私鑰解密，並得知其中的內容。

數位簽章運用上述兩種加密的方式達成交易的認證，延續上圖的例子，當 Joe 支付 Alice 比特幣時，Joe 會利用 Alice 的公鑰以及上一筆交易的哈希值做成戳記；當 Alice 在支付給 Bob 時，Alice 需要使用自己的私鑰做成數位簽章，節點或 Bob 就可以比對戳記（Alice 的公鑰）和數位簽章（Alice 的私鑰），確定 Alice 是比特幣的擁有者，達成交易驗證。

第三節 區塊

上一節描述的是一筆交易產生及驗證的過程，而一個區塊之中紀錄著若干筆交易，每筆交易都是以上述的方式儲存在區塊鏈上。一個區塊除了記載交易紀錄外，還包括關於這個區塊的所有資訊。如下圖所示，將會解釋幾個重要的區塊資訊：



Block #464369

Summary	
Number Of Transactions	2274
Output Total	18,468.36203932 BTC
Estimated Transaction Volume	1,118.46456541 BTC
Transaction Fees	1.50125312 BTC
Height	464369 (Main Chain)
Timestamp	2017-05-01 15:07:34
Received Time	2017-05-01 15:07:34
Relayed By	BTC.TOP
Difficulty	521,974,519,553.63
Bits	402791230
Size	999.136 KB
Version	0x20000000
Nonce	2254537253
Block Reward	12.5 BTC

Hashes	
Hash	00000000000000000009aa92b579555e90ed143c4ded70268ec87fdce4a291429
Previous Block	00000000000000000001368c6da940e60bd5d7c3db2d6d2e54fa9b8db30b543ce8
Next Block(s)	000000000000000000003454749399cd274a4f3152ec20050e1885a2b3963a14dc
Merkle Root	9106eec929a213f0c7a636dec7ce54fb298e05f5143187ea836dbb07cc497e65

Network Propagation

圖 五 比特幣的區塊[3]

（1） Height：代表這個區塊在主鏈上的位置，其為第 464369 個區塊。

（2） Difficulty：代表計算工作量證明的難度。

（3） Size：比特幣區塊鏈系統中，每個區塊的大小約為 1MB，實際上可能或大或小，由節點搜集的交易數量而定。

（4） Nonce：在區塊未形成之前（計算出工作量證明前），這是個待定的數字，節點反覆的猜測這個數字使得區塊的哈希值小於某個事先約定的目標，猜中這個數字的節點完成工作量證明，可以將區塊放上區塊鏈，並獲得報酬。（工作量證明詳見第四節）

（5） Block Reward：圖中的區塊報酬為 12.5 個比特幣。Block Reward 記錄著節點能夠獲得多少的比特幣報酬。比特幣的系統中，計算工作量證明是唯一產生比特幣的方式，一開始的發行量是每個區塊產生 50 個比特幣，大約每四年半會減半一次，發行的總數不會超過 2100 萬個。

（6） Merkle root：如下圖所示，假設一個區塊有 A 到 P 共 16 筆交易，將每筆交易放入哈希函數產生相對應的 16 個哈希值 #A 到 #P，再將哈希值兩兩再放入哈希函數，產生八個哈希值 #AB、#CD、#EF…、#OP，再兩兩以重複相同的方式計算哈希值，最終會產生一個 Merkle root。

[3] 資料來源：blockchain.info（網站）

Merkle root 可以方便節點驗證交易，簡化驗證交易所需的資料，提高效率。以交易 #K 為例，節點想要驗證這筆交易的話，只需要保留哈希值 #L、#IJ、#MNOP、#ABCDEFGH，再比對 Merkle root 即可。（如圖六）

除了提高驗證效率外，Merkle tree 的架構還可以減少需要儲存的資料量，如果這個區塊只剩 K 交易產生的輸出(Output)還未被花費掉，則除了上述驗證需要用到的哈希值外，其他交易的哈希值都可以從硬碟中清除。如圖七所需儲存的資料量少於圖六。

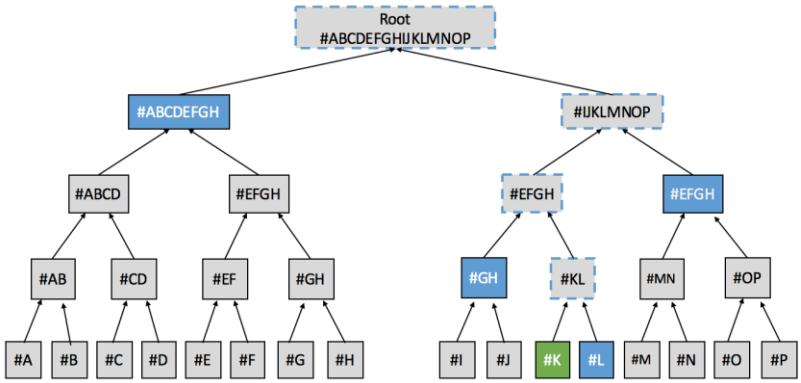


圖 六 Merkle tree 示意圖

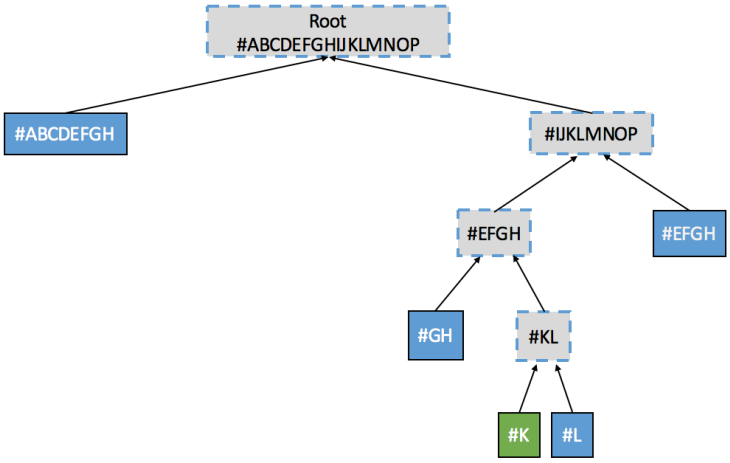


圖 七 Merkle tree 的簡化圖

第四節 工作量證明與誘因

一、工作量證明（挖礦）

第二章的第二節中曾經提過拜占庭將軍問題，點對點的網絡中共識該如合形成的問題，答案是利用工作量證明達成共識。在點對點的網絡之中，如果每個節點都可以聲稱自己的區塊是合法的，則這個網絡中沒有共識，無法產生一個所有節點都認同的區塊。中本聰的區塊鏈達成共識的方法是，每個節點在宣稱自己的區塊是合法的之前，必須經過一連串的電腦運算，最先完成計算的節點得到「工作量證明」，則其他的節點就會認同這個區塊是合法的，共識就形成了。工作量證明除了可以讓節點間達成共識之外，由於必須付出電腦資源作為代價，居心不良的節點也會為之卻步。如果說人類展現誠意的方式是良好的態度，則電腦展現誠意的方式就是不停的運算。有個關於電腦展現誠意的有趣例子：

電子郵件剛建立的時候，信箱中常常會有許多來路不明的郵件，包含廣告與意義不明的內容，被稱為垃圾信件。由於散播垃圾郵件通常都是以數量極大的方式發送，因此只要一般信件在發送之前，讓電腦運算一個簡單運算，並附上運算證明，就可以與漫無目的發送的垃圾信件區隔出來。當然，發送垃圾信件依然可以做出一樣的運算證明，只是必須消耗的電腦原算資源會過於龐大，而不願意做出這樣的運算證明，以目前垃圾信件的過濾來看，成效是非常顯著的。

所以，工作量證明到底在計算什麼？

目標：找出 Nonce

在第二節介紹區塊的時候曾經提過其中有個待定的值 Nonce，工作量證明就是在計算 Nonce。每個區塊都會有一個哈希值，哈希值的計算如下：

$$H(Nonce \parallel previous\ hash \parallel tx_1 \parallel tx_2 \parallel \cdots \parallel tx_n) < target$$

放入哈希函數的資料包括此區塊中的所有交易的內容（tx，交易的內容如同第一節所討論）、前一個區塊的哈希值（previous hash）與 Nonce，此區塊的哈希值必須小於某個設定的門檻（target）（例如：哈希值的前 10 個位數為零）。由於交易的內容與前一個區塊的哈希值都是固定的，只有不斷的改變 Nonce 並找出滿足上述條件的哈希值，才算完成工作量證明。而當一個節點 A 向網絡廣播自己完成工作量證明之後，其他節點認同這個區塊的合法性（透過重新運算哈

希函數得知，哈希函數易於檢驗的性質使得驗證很容易），承認節點 A 所做的工作量證明，會將節點 A 所廣播的區塊當作前一個，並接在這個區塊之後計算，也就是計算上式的時候將節點 A 所廣播的區塊哈希值當作 previous hash 代入。

因此區塊鏈中的每個內容透過哈希值與工作量證明的機制環環相扣，如果有惡意的節點想要竄改區塊鏈中的內容，則必須重新計算所有的工作量證明，使得每個區塊的哈希值符合小於某個門檻，當區塊鏈的長度愈大的時候，要成功竄改資料的可能性會愈小，與其竄改交易紀錄將比特幣轉入自己的錢包，並重新計算所有的工作量證明，不如直接計算工作量證明並獲得應有的報酬，任何人權衡後都不會有誘因去竄改資料，所以區塊鏈才能產生無法任意篡改的特性。

二、誘因

節點為什麼要花費自己的電腦運算資源來計算工作量證明呢？在完成工作量證明之後，節點還需要驗證區塊之中的所有交易，確認交易無誤之後，才能將這個區塊是為合法的，所以節點在區塊鏈中是負責維護運行的角色。每次完成工作量證明的節點都會得到一筆報酬，是節點願意犧牲電腦運算資源，並維護區塊鏈運行的誘因。提供誘因是目前比特幣能夠成功運行的關鍵，除了節點間相互競爭能夠確保系統的穩定之外，也有效遏止惡意節點篡改區塊鏈內而從中竊取比特幣的企圖，與其消耗資源竄改內容全部重新計算工作量證明，還不如當個老實的節點，正當的獲取維護區塊鏈的報酬。

第五節 點對點網絡

在區塊鏈網絡中，節點與節點之間是相連的，一般使用比特幣的用戶也會與其中幾個節點互動，當一有交易發生的時候，與用戶互動的幾個節點會最先聽到這筆交易，再由這幾個節點向外廣播，只要有其他相連接的節點都會聽到這筆交易，節點會將這筆交易放入即將計算工作量證明的區塊中。同一時間，很多筆交易一一的發生，快速在整個點對點網絡中廣播傳遞，節點會搜集還未被放上區塊鏈的所有交易形成一個交易暫存池[4]（Mempool），並將其中一些交易放入區塊之中，接著開始進行工作量證明，當區塊被放上區塊鏈之後，所有的節點都會驗證區塊之中的交易，確保每筆交易沒有問題。步驟如下：

1. 新的交易被廣播到所有節點。
2. 每個節點各自收集交易到區塊中。
3. 每個節點開始運算工作量證明（Proof of work）。
4. 當有節點率先解出工作量證明，此節點會將這個區塊廣播被每個節點。
5. 如果區塊中的每個交易都是合法的且沒有被花費過，則所有的節點都會接受這個區塊。
6. 網絡中的其他節點接受這個區塊的話，會利用這個區塊的哈希值去計算下一個區塊的工作量證明，創造新的區塊。

當兩個節點（A、B）同時計算出工作量證明並廣播給所有節點時（如下圖八），區塊鏈會產生分岔，有一部分的節點會先聽到節點 A 的區塊，另一部分會先聽到節點 B 的區塊，這樣的情況下，他們會在第一個聽到的區塊後面運算，且保留第二個聽到的區塊，並留意下一個區塊是生成在哪個區塊之後，保持著在最長的那條主鏈之後計算工作量證明。而分岔的區塊內的交易，一部分可能已經被包含在主鏈上被放上區塊鏈了，另一部分則會回到交易暫存池中，等待成為另一個區塊內的交易。

[4]交易暫存池：英文為 Mempool，mem 有記憶的意思，所以翻譯為暫存。所有未被放上區塊鏈的交易都會在交易暫存池中。

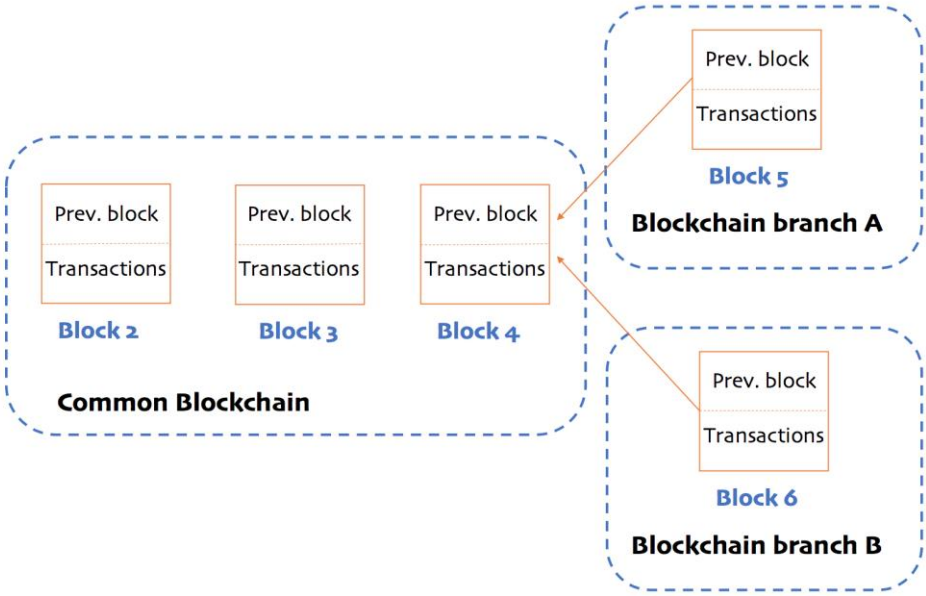


圖 八 區塊鏈分岔示意圖

上一章所提到的雙重花費問題在這裡獲得解決。區塊鏈上的每個參與者都只認同最長的那條鏈，這就是區塊鏈的「共識」。以下有兩種雙重花費的情境：

1. 不同時間點重複使用同一筆比特幣

這是相對單純的情況，如果有人想要重複使用比特幣的話，節點在驗證交易時馬上就能知道這些比特幣已經被花費掉，是已花費的交易輸出（spent transaction output）。

2. 相同時間使用同一筆比特幣

如果幾乎在相同時間花費同一筆比特幣，而且又剛好被不同的節點在相同的時間點放上區塊鏈，如上一段所描述的情況，區塊鏈會產生分岔，但最終只有其中一筆比特幣交易會被保留在最長的主鏈上，另一筆交易會回到交易暫存池中，等待成為下一個區塊內的交易。如此一來，當雙重花費的另一筆交易再度被放上區塊鏈時，就與第一個情境相同，節點能立即發現這筆比特幣已經被花費過了。

因此，使用比特幣交易的時候，為了避免雙重花費的情況，在接收比特幣的時候最好等待六個確認（confirmations），也就是在自己的交易被放上區塊鏈之

後，後面還有接續的六個區塊產生，這樣幾乎可以保證交易永遠被保留在區塊鏈上，不會再回到交易暫存池中。

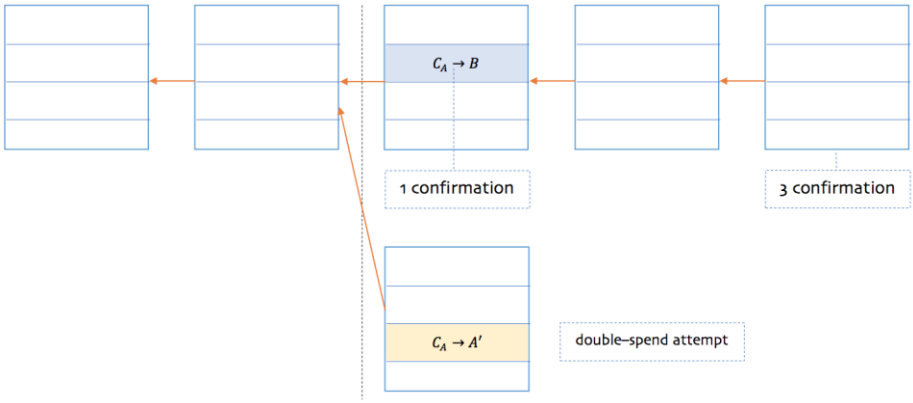


圖 九 區塊鏈分岔及確認(confirmations)示意圖

點對點網絡與交易驗證的方式，做到了完全去中心的目的，在這個價值交換的網絡當中，利用節點之間的共識與數位簽章的驗證機制，取代傳統授權中心機構的功能，交易雙方不需要信任的第三方便可達到轉帳目的，只要信任這個區塊鏈系統，信任這個機制能夠很安全的幫助他們達到價值交換的目的即可，因此區塊鏈又被經濟學人雜誌稱為「信任機器(The Trust Machine)」。

過去，網路之中的虛擬化商品所面臨的問題是，數位化的任何東西都很容易被複製，以虛擬貨幣為例，在比特幣出現之前，虛擬貨幣之所以無法順利運行的主因就是容易被複製，沒有一套有效的機制能夠遏止複製虛擬貨幣，任何人都有辦法做到這件事，在這樣的情況下，導致虛擬貨幣無法產生其應有的價值，而以區塊鏈為基礎的價值交換系統能夠保持數位化物品的唯一性，確保每個數位化的物品在網路之中都是獨一無二的，如此一來價值就會存在，參與這個價值交換系統的人們也會產生信任。

第六節 總結與目前現況

一、 總結

區塊鏈主要由三種技術結合而成，分別是非對稱加密技術、哈希函數以及共識演算法，並且以點對點網絡的方式運作。

非對稱加密技術應用於數位簽章，利用公鑰形成戳記、私鑰形成簽章，用以

比特幣交易時的所有權轉移確認；哈希函數將所有區塊串連在一起，並用於工作量證明的計算，使得區塊鏈上的任何資料都無法被竄改；工作量證明的共識演算法讓點對點的網絡中形成共識，使得每個節點間產生出一致的帳本。

這三種技術及應用缺一不可，它們共同達成了區塊鏈的去中心化、唯一性以及不可篡改性，是比特幣及區塊鏈能夠如此成功的關鍵。深入了解比特幣區塊鏈是如何運作之後，本文將針對其目前運行的狀態提出看法。

二、 目前現況

隨著比特幣的價格愈來愈高，愈來愈多人參與挖礦（計算工作量證明），使得整體區塊鏈中的運算力大幅增加（節點所投入的電腦資源），在比特幣的區塊鏈系統中，約每十分鐘可以挖到一個區塊，利用時間的間隔減少區塊鏈分岔的情況。在運算力大幅增加的情況下，系統會將門檻值變小（下式中的 target），以提高運算的難度（Difficulty），保持每十分鐘一次的區塊間隔時間。

$$H(Nonce \parallel previous\ hash \parallel tx_1 \parallel tx_2 \parallel \cdots \parallel tx_n) < target$$

下圖中的 Hash rate（每秒可以計算的湊值數目）代表整個比特幣區塊鏈系統中所有電腦的運算資源，隨著 Hash rate 的上升，Difficulty 也以幾乎一樣的斜率上升。

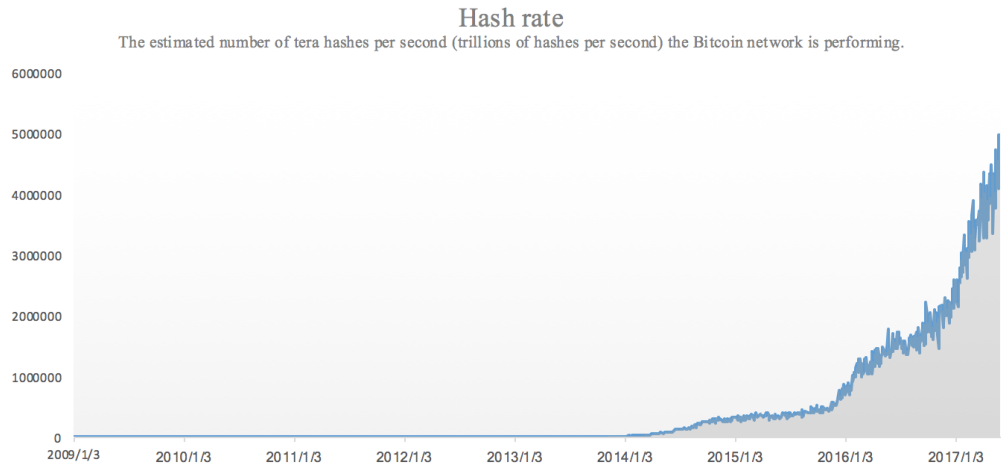


圖 十 比特幣系統中哈希函數的運算量[5]

[5] 資料來源：blockchain.info（網站）

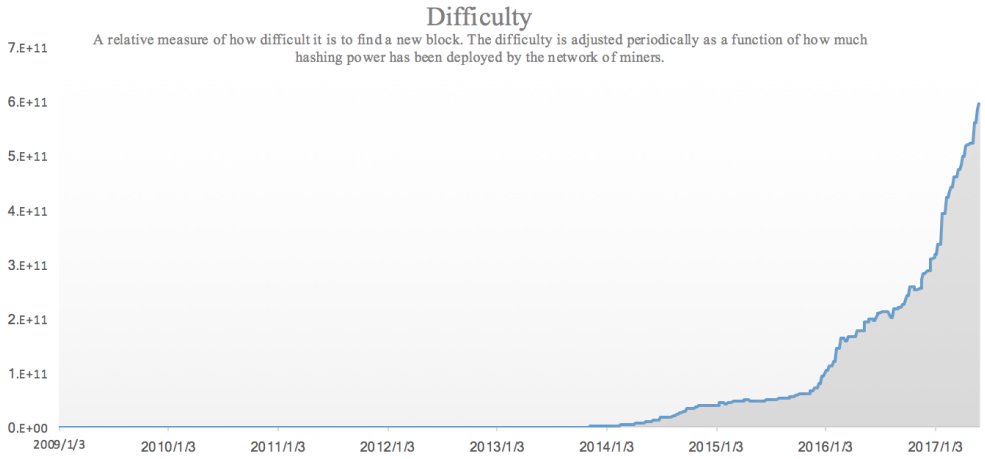


圖 十一 運算困難度[6]

由於目前挖礦的困難度大幅的攀升，挖礦也從使用個人電腦發展成一整個機房由專門的電腦挖礦，這使得挖礦的進入門檻變得高不可攀，一般人幾乎沒有能力建置一個機房來挖礦，為了對抗專門挖礦的機構，既然一台電腦的算力不夠，十台電腦、一百台電腦呢？所謂的挖礦池（mining pool）就應運而生，挖礦池結合每個想要參與挖礦的個人，同時提供電腦的算力計算同一個區塊，只要分配每台電腦不同的計算區域，就可以大幅提升挖到礦的機率，最後的報酬則會以公平的方式分配給每個提供算力的個人。

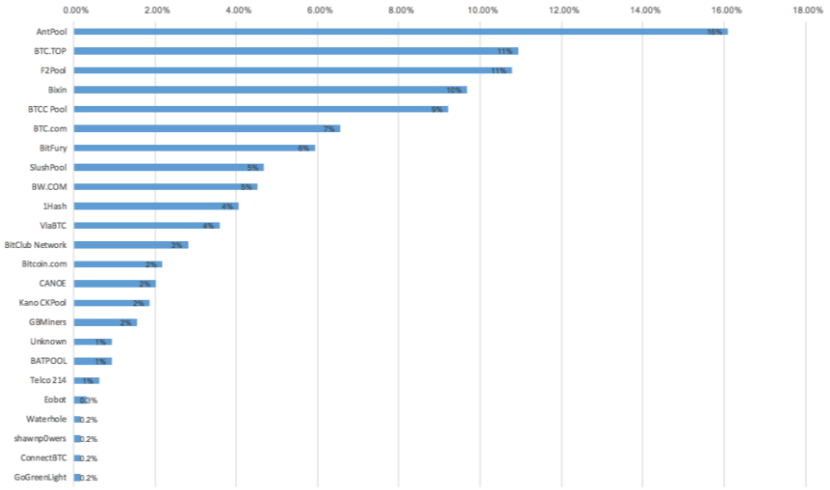


圖 十二 比特幣系統運算量的分佈長條圖[7]

[6]資料來源：blockchain.info（網站）
[7]資料來源：blockchain.info（網站）

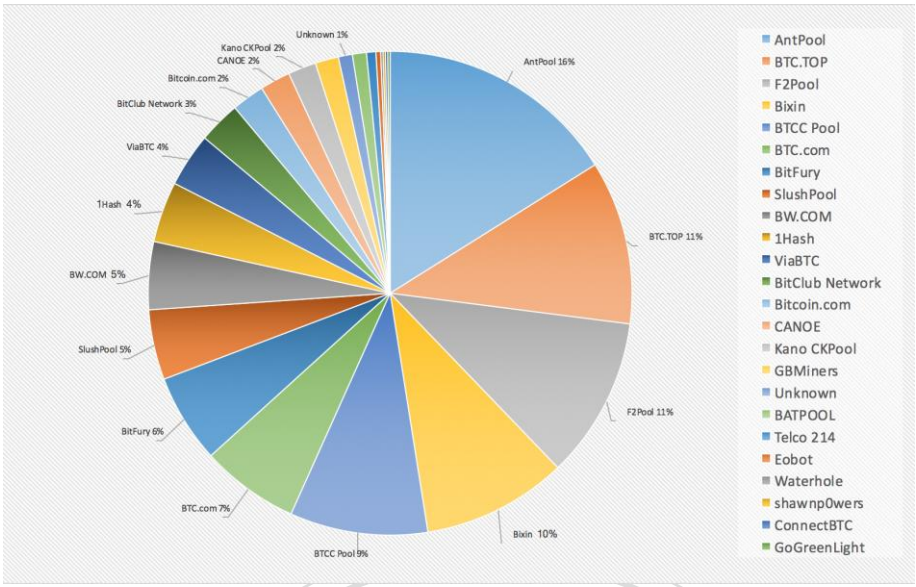


圖 十三 比特幣系統運算量的分佈圓餅圖[8]

挖礦行為的競爭下，除了每天需要的付出的電腦算力與電力過大之外，由於大型的挖礦機構與挖礦池掌握大部分的算力（computing power），這些機構對於區塊鏈的記帳有一定程度的影響力，減弱了區塊鏈去中心化的程度。原本希望相互競爭之下能夠排除不良的礦工的機制，反而使比特幣的使用者可能需要信任些大型挖礦機構，導致信任再度集中。

當然，目前還不能斷言信任再度集中在某些礦工上是好是壞，就實際運作上來看，這些投入龐大資源的大型挖礦機構當然會想好好維護，因為破壞了整個區塊鏈系統只會使得比特幣的價值不再，是這些機構最不願看到的，所以即使信任集中，區塊鏈的運作仍會繼續下去。但就理想的去中心化角度來看，這樣的發展當然是不好的，如前所提，區塊鏈是一個信任機器（The Trust Machine），信任應該來自於區塊鏈的機制，而非某些特定的對象。但從比特幣運行這麼多年的經驗中，或許對於機制作出調整，就能夠完善區塊鏈的去中心化功能。

[8]資料來源：blockchain.info（網站）

第四章 案例介紹

了解區塊鏈的運作原理之後，會發現可以應用的層面非常的廣，其中大致上分為兩類的應用，一類是著重在區塊鏈分散式帳本的記帳功能，單純用作紀錄資料的工具；另一類是擴大區塊鏈所形成的價值網絡的範疇，如果比特幣的價值可以在網絡上傳遞，其他無形化的資產也能夠做到。由於本文最後所做的應用屬於後者，因此以下三個案例也都與價值網絡有關，是國外嘗試將區塊鏈帶入證券交易結算的例子。

第一節 Overstock 股票交易平台 tϕ

Overstock 是美國網的證券零售商，自 2015 年開始參與區塊鏈的嘗試，與區塊鏈技術的公司合作，致力於用區塊鏈實現股權的交易與結算功能。2015 年 4 月，Overstock 發表了其以區塊鏈技術為基礎的交易平台 tϕ，以彩色幣的方式來記錄數位資產，將硬幣標記以不同顏色的數位貨幣代表不同的股票或債券。2015 年 6 月，tϕ 發行了一種數位公司債券，價值兩千五百萬美金，這些債券將會在 tϕ的平台上交易與結算。

2015 年 8 月，在納斯達克的活動上正式發佈區塊鏈交易平台 tϕ，並宣稱可以實現股票證券交易的即時結算功能，同時也包含發行股票證券的功能。同時，tϕ也已經開始進行私募債權發行的嘗試，依據美國監管機構的規定，私募債權並不需要監管機構的許可，但公募證券的發行則需要美國證券交易委員會（SEC）的批准。公募證券發行 tϕ也向美國證券交易委員會提出申請，並得到申請的許可，這是美國監管部們首次公開批准以區塊鏈技術為基礎的業務。未來，Overstock 計畫將發行價值達 5 億美元的股票或其他證券的發行。

第二節 Linq 私募股權平台

Linq 為納斯達克交易所基於區塊鏈所建立的交易平台，目標為私募股權市場，期望建立全新的股票發行、轉讓以及出售方式。新創公司在公開上市之前，資金的需求以及為了維持內部管理的獨立性，往往會經由私募股權的方式籌資，以獲得足夠的融資需求。傳統的私募股權過程相當的繁瑣，除了需要大量手工作業與紙本的記載，更容易造成紀錄上的錯誤，衍生出許多股東或合夥人間的糾紛，其中也可能需要律師的協助，釐清權利義務關係。因此對於新創公司而言，私募股權的融資成本其實非常的高，許多企業都在尋求一個能夠順利解決私募股權成本過高的解決方式，而納斯達克交易所的 Linq 平台提供了一個全新的選擇。

納斯達克交易所與區塊鏈的新創公司 Chain 合作，基於區塊鏈的技術，為投資人提供一個不可篡改、永久保存的紀錄，且兼具透明度與可審計性，服務的範圍將會涵蓋新創企業的股票發行、交易及登記管理等功能，快速的結算交割過程將會有效降低交易對手與第三方操作的風險，讓股票所有權的轉移更有效率。由於納斯達克交易所本身就提供非常豐富的股權服務，因此 Linq 作為納斯達克旗下的私募股權交易平台，更是被賦予極高的期望。

2015 年 12 月，Linq 正式上線，而作為 Linq 的孕育者之一的新創公司 Chain，理所當然地成為第一個由 Linq 完成並記錄私募股權交易的公司。其後使用 Linq 平台的新創公司還有 ChangeTip、PeerNova、SYNACK、Tango、Vera。

第三節 澳洲證券交易所

2016 年 1 月，澳洲交易所（ASX）認購了區塊鏈開發商 Digital Asset Holdings（DAH）約百分之五的股權，支付 1,490 萬澳幣。在與 DAH 的合作中，雙方的目標為以區塊鏈技術取代現有的清算支付系統 CHESS（清算所電子附屬登記系統），現有的系統 CHESS 即使運行的非常，但 CHESS 已經到達其系統的極限，無法再提供更高效能的服務。隨著區塊鏈的技術愈來愈成熟完整，澳洲證券交易所也願意投入研究，期望提供投資人更快速的交易結算服務。

澳洲交易所表示需 6 至 12 個月的時間來開發原型解決方案，與監管機構與市場參與方合作，試圖找到使用區塊鏈系統的途徑，並預期在 18 個月之後得到最終的結論。澳洲交易所的顧問表示，採用區塊鏈系統之後將可為終端客戶節省 40 至 50 億澳元的花費，主要來自於後台管理費用與合規成本，以及區塊鏈實時

結算可望降低交易對手風險，也可以減少投資所需的成本。

直至今年（2017）二月，澳洲交易所仍然對使用區塊鏈作為結算交易的基礎保有信心，在已經投入近兩千萬澳幣之後，澳洲交易所的執行長 Dominic Stevens 表示，在年底投資的總金額會上升到五千萬澳幣。

第五章 區塊鏈應用：股票交割結算

中本聰的比特幣區塊鏈成功的展示了網際網路的價值交換，比特幣在區塊鏈上交易並創造價值，開啟了許多應用的想像空間。第四章的例子可以看到，已經有許多企業在嘗試使用區塊鏈進行股票的結算與交割，不僅僅因為現有的結算交割機制存在難以解決的痛點，在區塊鏈技術逐漸成熟的背景下，掌握了區塊鏈技術的核心之後，人們了解到區塊鏈技術非常適合應用在結算交割，因為股票的結算交割就是一種價值的交換與轉移。本章的安排如下：

第一節會先探討目前台灣的結算交割制度，與其痛點的分析；第二節則會提出具體的區塊鏈架構，與實際運行的方式；第三節則會分析實際執行可能遇到的問題與解決方案；最後第四節將會分析使用區塊鏈能夠達成的經濟效益，與其對社會的影響。本文此章節所提出的區塊鏈系統會與第三章所解釋的不盡相同，但原理與核心的概念是一致的。

第一節　台灣現行股票結算交割制度

一、　現行股票結算交割制度

台灣目前的結算交割制度由三個不同的單位共同運作，分別是台灣證券交易所、集中保險結算所與央行的同資系統。依據我國證券交易法、台灣證券交易所營業細則，台灣證券交易所進行股票以及款項的結算，集保中心負責證券的交割，款項的交割則由央行的同資系統負責。台灣證券交易所為同日結算制，且以多邊餘額的方式進行，計算每個券商的應付應收券款的餘額，直接由餘額交割。

從交易日(T)結束交易之後，證交所需與券商與證金公司交互交易的資訊，經過多次資訊的交換之後，多方才能夠確認交割清單並於當日晚上九點結帳。交易日的次一日（T+1），證交所需於上午八點前完成交割清單，券商則須備妥信用交易資料與轉融通資料，完成結算工作，並在交易日後的第二日（T+2）執行交割任務。

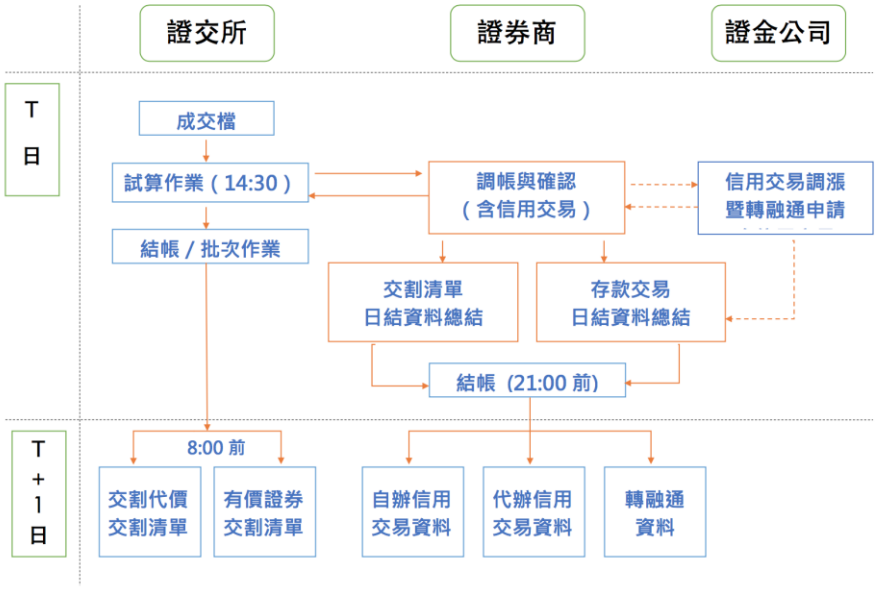


圖 十四 證交所 T 日到 T+1 日的結算流程

在交易日後的第二日完成（T+2），投資人需要在上午 10 點之前備足券款，券商才能夠履行對集保中心與央行的交割業務。投資人經由券商下單，券商將委託單送至證交所集中搓合，在一日的交易結束後，證交所會對每日的交易結算，結算的方式為買賣互抵，為淨額交割。舉例來說，A 券商只有兩個客戶，甲客戶買進 100 張台積電股票，乙客戶賣出 90 張台積電股票，由於券商內部可以自行轉移其中的 90 張台積電股票，所以證交所結算時只需要計算餘額的部分：A 券商買進 10 張台積電股票，並且支付 10 張台積電的價格。

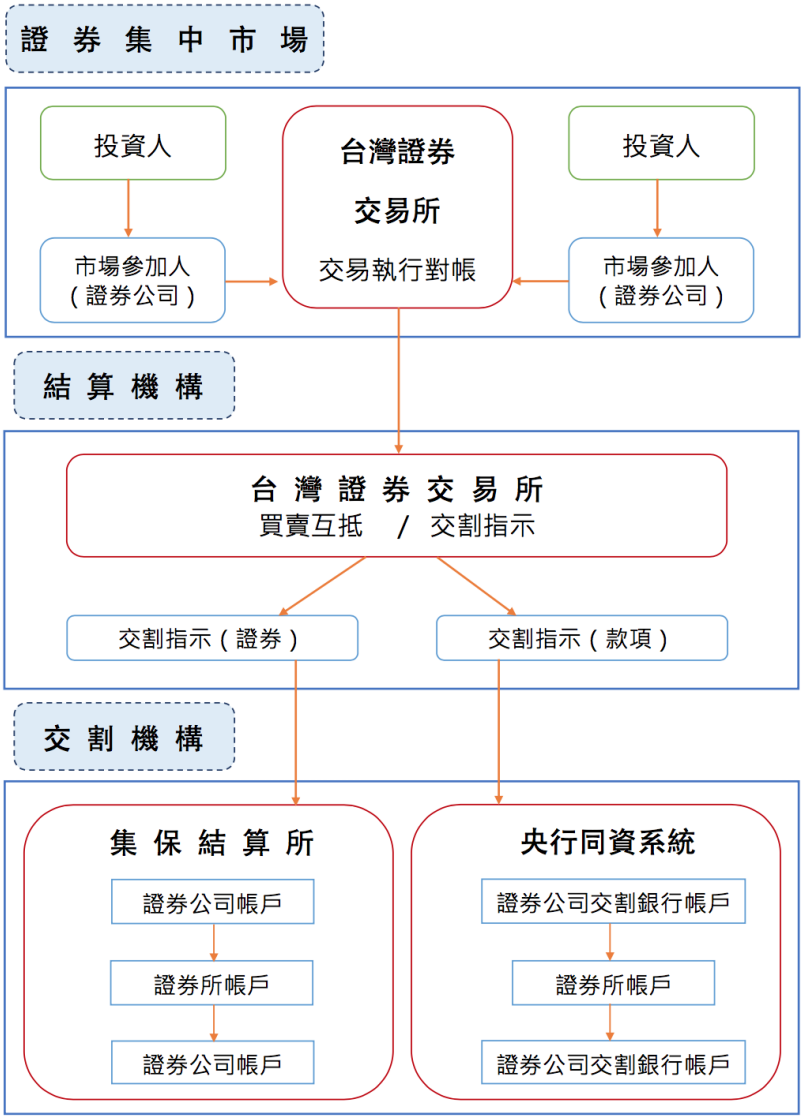


圖 十五 股票結算交割示意圖

詳細的作業流程如下圖：

（1） 台灣證交所完成結算工作，並通知買方券商撥款、賣方券商撥券。

（2） 買方券商將應付股款存入其合作的清算銀行 A；賣方券商通知集保中心將證券撥入台灣證交所的集保證券戶中。

（3） 清算銀行 A 透過央行同資系統撥付款項。

（4） A 銀行將款項由其準備金甲戶[9]撥入台灣證交所在央行的專戶中，並通知證交所 A 銀行已撥款。

（5） 台灣證交所通知集保中心將證券撥入買方券商帳戶，同時通知央行將股款撥入賣方券商的清算銀行 B 的準備金甲戶中。

（6） 買方券商由集保中心完成入券；賣方券商的股款也經由銀行 B 入帳。

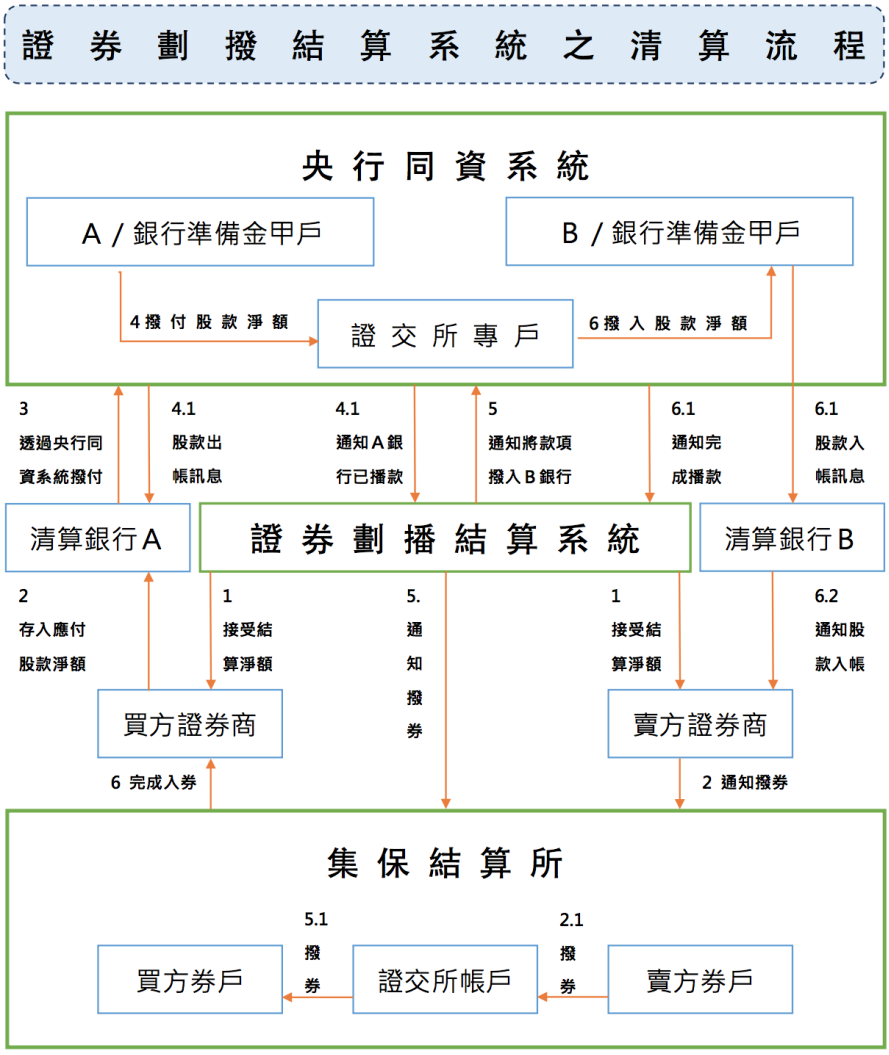


圖 十六 股票交割流程（含金流）

[9]準備金甲戶：準備金甲戶又稱為往來戶，是指憑開戶金融機構 簽發的支票或利用中央銀行同業資金調撥清算系統，可以隨時提存的存款，準備金甲戶的存款不計利息。

二、 現行制度的痛點分析

了解現有的結算交割制度後不難發現，其中所隱含的作業程序極其複雜，需要透過多方的資訊交換才能達到結算交割的目的，雖然目前整體運行並沒有太大的問題，但仍然有待改善的空間。

1. 交易存在多個版本：由於整體的結算涉及到台灣證交所、多個券商以及證金公司，彼此之間都存在著不同的系統，當系統間出現交易細節的不一致時，仍然需要人工干預的方式才能獲的解決。
2. 結算過程耗時較長：結算交割的流程需在交易日後兩日（T+2）才完全達成，造成資本與金流的佔用。
3. 券商交易對手風險：由於款券交割於 T+2 日才發生，投資人若無法在時限內備足款券，則券商需要承擔投資人違約交割的損失。使用區塊鏈讓交易及交割同時發生，能降低投資人違約發生的機率。

第二節　應用股票結算交割的區塊鏈架構

了解現有的結算交割制度與其運作時產生的痛點之後，本文將提出應用於台灣股票結算交割的區塊鏈架構，利用區塊鏈技術為基礎，發展出更具效率與準確性的結算交割系統，將有助於節省資本市場運作的成本。高盛 2016 年的一份區塊鏈研究報告中指出，區塊鏈估計可以為美國股票交易節省每年約 90 億美元的費用，雖然台灣的市場規模無法與美國相提並論，但區塊鏈應用在結算交割的領域中無疑存在極大的潛能。區塊鏈屬於硬實力的專業技術，若能將其應用在各種領域中，將會是台灣軟實力的展現。

一、 比特幣區塊鏈的缺陷

第二章及第三章介紹的比特幣區塊鏈是最原始的區塊鏈系統，當初的設計理念是為了創造一個點對點的價值交換網絡系統，並且不用任合權威的中心管理網絡中的任合交易，所有的交易驗證皆依靠網絡中的節點完成。這樣的開放式系統任何人都可以成為節點，為了避免惡意的節點攻擊同時獎勵好的節點，利用工作量證明及誘因的機制，達到價值交換的目的。但比特幣的區塊鏈系統仍然有些缺陷，很難原封不動的直接應用，其缺陷有以下四點：

（一）交易的不確定性：當區塊鏈產生分岔的時候，就是交易不確定性產生的時候，其中一條分岔中區塊不會被節點認同，並消失在區塊鏈中，

雖然其中的交易仍然會重新被節點放上區塊鏈，但仍會造成交易發生時的不確定性。中本聰很清楚這項缺點，所以拉長區塊之間產生的時間，以降低區塊鏈產生分岔的可能性，並建議等待交易的確認（confirmations）達六個，才能確保交易紀錄永遠保留在區塊鏈上。比特幣區塊鏈平均十分鐘產生一個區塊，等待六個區塊鏈意味著需要等待約六十分鐘，過長的等待時間在商業上的應用是無法忍受的。

（二）交易量不夠大：受限於每十分鐘產生一個區塊的設計，區塊鏈能夠認證的交易量約每秒七個，無法負荷規模稍較大的應用。縮短區塊產生的時間會導致交易的不確定性更高，在不改變區塊生成時間的前提下，增加區塊的容量也能夠提高交易量，只要每個區塊內可以存放的交易數量增加，交易量也會上升。比特幣區塊鏈系統考量到傳輸時的頻寬問題，所以設計每個區塊大小約 1MB，讓每個人都能夠參與。未來如果頻寬提升，或許能夠透過加大區塊來達到提高交易量的目的。

（三）工作量證明：工作量證明機制讓點對點的網路產生共識，認同完成工作量證明的節點所發佈的區塊。這樣產生共識的方式過於費時費力，消耗過多的運算資源，對於一個公開的區塊鏈或許只有這樣的共識方式，但對私有鏈或是可許制的區塊鏈而言，會有更有效率的共識方式。

（四）匿名性：比特幣區塊鏈中，利用密碼學的方式讓每個交易的使用者能夠保持匿名性，也造成很多非法目的（洗錢、非法交易）都使用比特幣的缺陷。在金融領域中監管尤其重要，直接使用比特幣區塊鏈會造成無法監管的情況。

區塊鏈的技術經過演化之後，已經有方法能夠解決上述的缺陷，雖然可能會犧牲掉某些比特幣區塊鏈的優良性質，但實際應用上能夠確實運行之後，再想辦法彌補犧牲掉的好性質，也是一種對於區塊鏈技術的實驗精神。以下將會提出本應用使用的區塊鏈模式，包括可許制的區塊鏈、監管方式、隱私政策、共識演算法以及金流處理的方式。

二、 區塊鏈模式

由於上述原生型（比特幣）區塊鏈的缺陷，以及各種應用有其規範與限制，

所以無法直接使用原生型的區塊鏈模式，雖然其中的原理是不變的，但須調整其某些運作的方式，才能達到真正的配適不同的應用。本文以下將就「股票結算交割」的應用，提出適合此應用的區塊鏈模式。

3.1 許可制的區塊鏈

不同於比特幣區塊鏈完全公開的特性，任何人都能成為節點維護區塊鏈的運作，許可制的區塊鏈僅開放給特定的節點進入區塊鏈中，由於成為節點需要經過申請，所以稱為許可制的區塊鏈。許可制區塊鏈失去了去中心化的特性，不同於比特幣區塊鏈的使用者不幣信任人，許可制區塊鏈的使用者必須信任幾個被許可參與的節點，相信這些節點會驗證交易，維護帳本且不會任意篡改。

股票結算交割的應用中，許可制區塊鏈是必須的：減少參與的節點數量可以使用不同的共識演算法，加快共識形成的速度以提高交易量以及消弭交易的不確定性；只允許少數節點進入區塊鏈中可以保持帳本的隱私，讓投資人的資產配置受到一定程度的保護；在少數的被許可的節點中包含監管單位，其有權限存取任合交易資訊，以達到監理的目的。

3.2 特殊功能節點

在許可制的區塊鏈中，每個節點都有其功能，稱之為「特殊功能節點」。以下將介紹不同功能的節點：

（1） 證交所：由於所有的撮合成交資料都在證交所，所以證交所作為一個特殊節點的功能為發佈成交資訊，包括買賣雙方、成交的股票及金額，這些資訊會成為股權轉移的依據，經由負責驗證交易的節點完成。除此之外，證交所也需要負責股票的發行，成為區塊鏈之中唯一的發行機構。

（2） 券商：券商依據投資人的委託下單，並且為投資人與集保中心的窗口，從事經紀業務並收取手續費，其現有的功能非常適合成為區塊鏈中驗證交易的角色，尤其收取手續費能夠轉變為券商驗證交易的誘因，取代比特幣區塊鏈中完成工作量證明獲得的比特幣。券商成為區塊鏈中少數幾個負責驗證交易的節點。

（3） 集保中心：集保中心的角色轉變最為巨大，從負責交割業務

變為監督券商驗證交易的角色。雖然券商為了其企業形象與信譽，不太可能任意變造交易紀錄以圖自身利益，但為了維護投資人的權益，仍然需要第三方的監督機構，集保中心成為再次確認交易的角色。

（4） 中央銀行同資系統:此結算交割的區塊鏈系統只有股票所有權的轉移，並不包含金流，金流的處理仍須連結回原有的金流系統「央行同資系統」，其聆聽證交所發布的每筆交易，並將金流的資訊送往央行同資系統，完成金流的轉移。

結算交割的過程就由這幾個主要的節點完成,投資人成為一般的使用者，並不負責任合事情，如同比特幣區塊鏈中的使用者，可以知道自己的股票餘額，也可以透過券商進行移轉。

個節點功能整理如下表：

節點	功能
證交所	發布交易資訊、發行股票
券商	進行交易的驗證
集保中心	監督券商的驗證行為，並再次確認交易
央行同資系統	聆聽證交所發布的交易資訊，並連結回原有的金流系統

表格 一 特殊功能節點的功能表

3.3 實名制

不同於比特幣區塊鏈的使用者是匿名的,應用於股票結算交割的區塊鏈系統必須實名制，如同銀行開戶一樣，每個投資人成為一般使用者時需要經過身份的認證。實名制除了有利於監管的目的外，還有連結個人銀行帳戶的作用，由於金流的往返仍需仰賴原有的金流系統，實名制可以確認投資人的身份，從資訊流到金流的效率會增加。

3.4 隱私政策

區塊鏈中所記載的交易紀錄將不會完整公開,負責運行與監督的節點能夠存取完整的資訊,但一般投資人或法人能夠存取的資料會受到限制，一般投資人只能看到自身所擁有的股票資訊，法人則可以看到其股東相關的資訊，以及其股東組成的比例。

3.5 共識方法

不同於比特幣的系統，由於許可制的區塊鏈已經排除惡意的節點，使用工作量證明的共識方法只會讓好的節點相互競爭且消耗不必要的資源，實務上並不效率。目前大部分以「拜占庭容錯共識演算法」以及「Paxos 共識演算法」取代工作量證明，以加快共識形成的速度。

3.6 金流處理

目前金流的處理方式有三種：

1. 連結回原有的金流系統。
2. 以代幣的方式直接在區塊鏈中進行交易。
3. 直接使用虛擬貨幣在區塊鏈中交易。

如同在特殊節點功能中提到，本研究認為連結回原有的金流體系是較可行的方式。由於目前虛擬貨幣的發展未成熟，各國對於使用區塊鏈的虛擬貨幣仍抱有很大的疑慮，所以第三的處理方式較為不可行。第二的處理方式則須連結到銀行，將法定貨幣存入銀行後，再轉換為區塊鏈上的虛擬貨幣，此方法涉及到銀行端的合作，與連結回原有的金流系統相比之下，同樣也需要仰賴銀行，在保有原本架構的前提下，第一個選項是最為適合的。

第三節 實際運行之探討

上節最後一部分說明了區塊鏈應用上的模型設定。以下將說明當交易發生時各個節點該如何運作，來完成股票所有權的轉移。最後會討論實際運作時可能發生的問題，以及可能的解決辦法。

一、 彩色貨幣——將硬幣標記為股票

由比特幣的系統當中，可以知道比特幣在區塊鏈中能夠做到所有權的轉移，成功的在網絡中將一個有價值的虛擬商品轉移。從第二節的討論中，我們可以知道比特幣區塊鏈在應用上的缺陷，也針對這些缺陷提出了修改的方式，企圖讓區塊鏈能夠應用到股票結算交割的領域。第四章的案例介紹當中，Overstock 的股票交易平台 tφ使用一種名為「彩色貨幣」的方式來進行股權的轉移，本研究的股權轉移也會使用到「彩色貨幣」。

將硬幣標記為不同的股票，就是「彩色貨幣」的使用方式。

本文的應用中以自行架構區塊鏈系統的方式，而不會使用現有的區塊鏈系統（比特幣、以太坊等），建立獨立的價值交換網絡。這個區塊鏈系統中仍然會有其虛擬貨幣（假設取名為 K coin），目前只是作為股票交換的媒介，每個硬幣會被標記成為不同的股票。進行股權轉移的時候，券商會去確認每個硬幣所對應的股票以及所有權的轉移是否正確，來完成整個交易的驗證。目前金流的處理方式設定為連結回原有的金流系統，但未來很可能直接使用系統中的 K coin 來處理金流，需視社會對於虛擬貨幣的接受程度而定。

二、 實際運作的方式

現行的結算交割制度為兩段式的，台灣證交所將集中撮合的結果依券商各別進行款券餘額的結算，而券商內部再各自對其客戶結算。區塊鏈的技術還不足進行股票的交易，集中搓合仍然需仰賴證交所，所以以目前證交所的作業方式來引入區塊鏈技術，能夠減少系統代換之間的摩擦，行政與人員的調整也能夠做到最小的影響。

以例子說明會較為具體：

投資人甲委託 A 券商賣出一張台積電股票。

投資人乙委託 B 券商買進一張台積電股票。

證交所撮合成交。

成交金額為 205,500 新台幣（5/24 下午 1:23 的成交價）。

股票所有權的轉移步驟如下：

1. 撮合成交，證交所向節點發布成交資訊，成交資訊包含雙方成交的券商、成交的股票張數以及成交的金額總數。
2. 證交所一共會發布三個交易資訊：
   （1） 投資人甲將一張台積電股票轉移給券商 A，券商 A 應付 205,500 新台幣給投資人甲。
   （2） 券商 A 將一張台積電股票轉移給券商 B，券商 B 應付 205,500 新台幣給券商 A。
   （3） 券商 B 將一張台積電股票轉移給投資人乙，投資人乙應付 205,500 新台幣給券商 B。
3. 券商搜集證交所發布的交易資訊。

4. 券商間達成共識，由其中一券商驗證交易資訊並放上區塊鏈。
5. 交易資訊受到驗證後，表示股票所有權的轉移已經完成，央行透過區塊鏈上的交易資訊進行金流的交換。
6. 集保中心隨時再次驗證交易資訊的正確性，保障個券商與投資人的權益。

上述的步驟與比特幣認證交易的流程大同小異(比特幣交易認證流程詳見第三章第五節），比特幣經過將近十年的考驗，足以證明這套流程是可靠的。所以本文沿用比特幣的交易認證流程，並讓特殊的節點負責不同的工作，期望達到與比特幣一樣堅不可破的交易驗證方式。

三、 實際運行可能遇到的問題

討論至目前為止，此應用的結算交割功能都屬於最基本的股票買賣，但股票市場的結算交割還必須包含融資、融券或是借券，這之中涉及到保證金或擔保的抵押品，對於目前的區塊鏈技術而言，本文認為還不足以應付較複雜的交易，雖然智慧合約可能是解決的方案，但目前智慧合約的技術還不成熟，仍然處於發展的階段，因此處理較複雜的交易還需等待技術的完整性。本文將不會深入探討智慧合約的應用，但以下會介紹基本的概念與原理，以及如何解決複雜交易的交割。

智慧合約（Smart Contract）衍生於比特幣區塊鏈，但其概念與使用方式截然不同。區塊鏈是一個價值交換的網絡;智慧合約則是基於區塊鏈系統的應用程式，又稱為去中心化應用程式（Decentralized Application）。實際上，智慧合約既不智慧也不是合約，而是一個透過區塊鏈運行的應用程式，由區塊鏈上的節點執行程式。目前最大的智慧合約平台是以太坊，以太坊將比特幣區塊鏈的功能擴充，成為一個能夠線上執行應用程式的平台。其底層的運作原理與比特幣大同小異，但擁有更大的交易量，約每 15 秒會產生一個區塊。以下將會以最簡單「慈善募款」的例子說明智慧合約：

智慧合約當中可以部署很多的行為，行為以程式碼呈現的話就是函式，一個函式代表著一個行為。以太坊中每個智慧合約是一個帳戶，部署慈善募款的智慧合約，就會產生一個相對應的帳戶，用於處理金流或是資訊的進出，慈善募款的智慧合約中有以下三種行為：

1. 接受捐款人的捐款，並記錄每個捐款人的地扯（address）。
2. 若達捐款金額，則關閉捐款帳戶（智慧合約本身），不在接受捐款。
3. 若未達捐款金額，則將款項全數退還給捐款人。

透過這三個行為（函式）就可以在以太坊上達成慈善募款所需的基本功能。因此融資融券相關的保證金及抵押品或許有機會使用智慧合約解決，只要在智慧合約中載明詳細的規則及其相對應的行為，就可以在系統中完成這部分的交割。

第四節　經濟效益之分析與社會影響

一、 系統整合

如同在第一節的痛點分析中提到，目前結算交割體系中多方存在著不同的系統，券商、證交所和集保中心都有各自負責維護及運行的系統，並且維持系統間的運作順暢。使用區塊鏈能夠解決痛點並整合多方的結算交割系統，讓所有的結算交割作業都在區塊鏈上完成，並共同維護一個結算交割系統，好處有以下三點：

(1) 減少總體的系統運作成本
(2) 減少結算交割過程的錯帳
(3) 減少處理錯帳時的作業困難。

然而，由於引入區塊鏈涉及多方的系統整合以及利益分配，因此能否實際運行區塊鏈仍然取決於券商、證交所以及集保中心的協調及合作方式。

二、 加快結算交割流程

現行的結算交割是交易日的兩天之後（T+2）才完成，因此投資人只要在兩天內備齊券款就可以做交易，但引入區塊鏈系統之後，幾乎在交易的當下就完成交割，因此投資人在交易的同時就必須備足券款，才能完成交割，這樣的改變足以影響投資人的行為。對於賣方而言，能夠及時地獲得交割款項有利於資金運用的效率；但對買方而言，資金需要即時的到位，有可能會延長其進入市場交易的時間點，造成市場流動性的下降。對於結算交割時間縮短的改變，實際執行上不一定要直接到位，實現交易即結算交割的最終目標，反而應該一步一步地縮短交割時間，讓投資人有足夠的時間適應這樣的改變，以達到減少改變制度所造成的摩擦。另外，對於券商而言，交易即結算交割能夠有效降低投資人違約交割的風險，券商可以減少自身的風險負擔程度。

三、 減少股票市場運作的成本

高盛（2016）的一份區塊鏈報告中指出，資本市場使用區塊鏈將可節省每年二十億美元的成本，其中包含減少結算交割的人事費用以及簡化結算交割系統所減少的支出。以台灣現有的結算交割制度來看，由於券商是投資人與集保中心的唯一窗口，所以券商向投資人收取手續費當中，一部分會支付給證交所及集保中心作為結算交割以及維護帳戶的費用。

台灣集保中心每年的營業收入約為 36 億新台幣，其中清算交割服務佔營業收入的 18%、帳戶劃撥處理服務佔 21%、轉帳處理服務佔 13%、帳戶維護服務佔 10%，合計為佔總營收的 62%，約為 22 億新台幣。營業費用的部分包含用人費用以及業務費用，合計約 20 億新台幣。假設區塊鏈能夠完全取代台灣集保中心股票結算交割的功能，則可預期每年節省約 40 億新台幣的運作成本。區塊鏈初期的建置成本會較高，但長期的運作維護費用會遠小於現有的結算交割系統，因此長期來看，使用區塊鏈作為結算交割的系統能夠大幅的縮減股票市場運作的成本。節省的運作成本會直接反應在交易手續費上，當交易手續費有效的降低，會提高投資人進行股票交易的誘因，進而提高逐年萎縮的股票市場成交量。成交量的提升不僅對資本市場有益，對於券商而言，結算交割費用減少的同時提升經紀業務的收入。

整理本節所提到應用區塊鏈的優點如下表：

	優點
系統整合	減少總體的系統運作成本 減少結算交割過程的錯帳 減少處理錯帳時的作業困難
加快結算交割流程	提高資金運用的效率 降低投資人違約交割的風險
減少股票市場運作的成本	提高整體股票市場的成交量 券商可提升經紀業務的收入

表格 二 區塊鏈應用股票結算交割的優點整理

第六章 結論

透過了解區塊鏈的技術原理，以及三個案例的說明，本文以股票結算交割作為區塊鏈的應用，提出區塊鏈的模式以及實際執行的方式。在比特幣的區塊鏈系統中，有幾個好的性質，包括不可篡改性、唯一性、公開透明以及去中心化，但這些性質其實過於理想，在實際的應用上無法一一保留，特別是在金融領域中，公開透明及去中心化幾乎無法達成，因此本文所提出的區塊鏈模式調整了區塊鏈的最初設定，在保障投資人的隱私同時，兼顧交易認證時的準確度。透過許可制的區塊鏈只允許特定的節點參與，每個節點各司其職共同維護區塊鏈的運作，並以更有效率方法達成節點間的共識，除了減少消耗電腦運算資源，也增加每天能夠確認的交易數量；透過實名制以達到監管目的；提出金流的處理方式以及目前保護投資人的隱私政策。

然而，將區塊鏈應用在結算交割會讓交割的時間點前移，對於整個股票市場的運作造成一定的衝擊，這之中的改變或好或壞其實難以預測，本文嘗試分析其結果並提出解決的辦法。

最後，區塊鏈技術仍然處於發展階段，除了區塊鏈本身之外，與之息息相關的是智慧合約。區塊鏈是基礎的技術而智慧合約則適用於更複雜的應用，兩者的發展街備受期待，期望有朝一日能夠突破應用上的門檻。

參考文獻

一、中文部分

1. 徐明星、劉勇、段新星、郭大治，區塊鏈革命。台灣：遠足文化事業股份有限公司。
2. 林雅苓（2017），我國證券及期貨市場應用區塊鏈技術之探討。國立台灣大學，社會科學院經濟學系在職專班，台灣。
3. 中央銀行編著，中華民國支付及清算系統，檢自：https://www.cbc.gov.tw/public/Attachment/972016463871.pdf
4. 台灣證券交易所網站，檢自：http://www.twse.com.tw/zh/
5. 杜宏毅，Blockchain 的前世今生與未來，檢自：www.cosa.org.tw/public_files/OSSForum/OSSF15/105lecture6.pptx
6. 香港金融管理局，2016 分布式帳本技術白皮書，檢自：www.useit.com.cn/thread-15071-1-1.html
7. 高盛，區塊鏈研究報告，檢自：http://www.chainconnected.com/static/upfile/video/file/20161107/c0d25c105add9c1093afb46ac49e35e3.pdf
8. 張錚文，一種用於區塊鏈的拜占庭容錯算法，檢自：https://www.antshares.org/Files/66c6773b.pdf
9. 黃志典，台灣的法定準備金制度，檢自：www.ib.ntu.edu.tw/jdhwang/files2/台灣的法定準備金制度.pdf
10. 廖世偉，顛覆性科技－區塊鏈，檢自：www.tfsr.org.tw/Uploads/files/201603%20顛覆性科技區塊鏈_廖世偉副教授.pdf
11. 臺灣證券集中保管股份有限公司，我國證券暨期貨市場結算交割制度現況分析，檢自：http://smart.tdcc.com.tw/pdf/others/a67.pdf
12. 臺灣證券集中保管股份有限公司，集保參加人制度，檢自：smart.tdcc.com.tw/pdf/others/a61.pdf

13. 證基會，集中市場交割結算制度，檢自：
http://libsvr.sfi.org.tw/download/knowledge/證期重點專區/證券交易市場簡介/結算交割.pdf

二、英文部分

1. Narayanan, Arvind, Joseph Bonneau, Edward Felten, Andrew Miller, Steven Goldfeder, (2016). Bitcoin and cryptocurrency technologies, Princeton University.

2. Swan, Melanie, (2015). Blockchain: Blueprint for a New Economy, O'Reilly Media
3. Nakamoto, Satoshi, (2008). Bitcoin: A Peer-to-Peer Electronic Cash System.
4. Castro, Miguel, Barbara Liskov, (1999). Practical Byzantine Fault Tolerance, Proceedings of the Third Symposium on Operating Systems Design and Implementation, pages 173-168.
5. Japan Exchange Group, Applicability of Distributed Ledger Technology to Capital Market Infrastructure, from: http://www.jpx.co.jp/english/corporate/research-study/working-paper/b5b4pj000000i468-att/E_JPX_working_paper_No15.pdf