區塊鏈之相關技術發展與應用

陳永祚

中華民國 111 年 5 月

作者任職於中央銀行資訊處，本文內容純屬個人意見，與服務單位無關，如有錯誤亦概由作者負責。

摘　　要

隨著資訊科技的發展，以及網際網路的普及，近年來興起了許多網路上的虛擬貨幣，如：比特幣、以太幣等，此類型的虛擬貨幣採用了一種去中心化的技術，由網路上的節點共同維護一個一致的帳本，彼此同步、相互驗證以確保其安全性，這種去中心化的技術稱為區塊鏈(Blockchain)技術。

區塊鏈技術雖然為近期之新興科技，但建構起該技術的卻是行之有年且經過市場驗證過的成熟技術，例如：P2P 網路、公私鑰加密演算法、雜湊演算法以及數位簽章等，本文對於區塊鏈所使用的各個技術進行介紹與探討。

比特幣是使用區塊鏈技術的最早應用，了解其運作原理可以更容易理解區塊鏈技術的內涵，本文深入探討比特幣區塊鏈技術，以及其安全性，並闡述使用區塊鏈技術之優缺點，可供未來相關應用參考；區塊鏈技術本身也隨著時間演進，發展出了不同的類型與變形，以符合各種實際應用場景的需要。

區塊鏈技術除了目前常見的虛擬貨幣應用外，配合其智能合約的設計，還有許多其他種類的應用發展，例如：資產所有權、身分認證等，本文亦闡述其相關未來可能應用以及近年國內外的應用案例。

目　　次

圖　目　次

表　目　次

壹、近期技術發展

邁向數位時代，網路上的各樣需求不斷出現，如：隱私保護、交易安全、資料備份、高可用性[1]之網路服務等，驅使資訊技術快速地成熟發展，許多技術已經廣泛地被使用在現行市場上的應用產品中，例如：在網路上資料共享的 P2P 技術、建立安全連線的網路憑證公私鑰加密技術、保護機密文件的對稱式加密技術、應用於網路交易的數位簽章技術，以及廣泛應用於加密技術中的雜湊演算法等，區塊鏈技術便是以這些成熟技術建構而成。

一、P2P 網路(Peer-to-Peer Network)

P2P 網路，又稱對等網路、對等技術、或點對點技術，是無中心伺服器、依靠使用者群（peers）交換資訊的網際網路體系，它的作用在於共享所有節點的運算與儲存資源，以降低資料遺失的風險並提升服務效率。與有中心伺服器的中央網路系統[2]不同，P2P 網路的每個使用者端既是一個節點，也有伺服器的功能，任何一個節點無法直接找到其他節點，必須依靠其用戶群進行資訊交流(圖 1)。

圖 1、P2P 網路與中央網路系統

P2P 網路　　**中央網路系統**

資料來源：本文整理

P2P 節點能遍布整個網際網路，在高網路隱私需求和檔案分享領域中，得到了廣泛的應用。這種網路設計模型不同於用戶端-伺服器(Client-Server)模型，在用戶端-伺服器模型中，通訊通常來

[1] 高可用性（high availability，），指系統無中斷地執行其功能的能力

[2] 一種網路架構，它把客戶端（Client）與伺服器（Server）區分開來。每一個客戶端都向中心伺服器發出請求。

往於一個中央伺服器。

二、RSA 公開金鑰加密演算法(非對稱式加密)

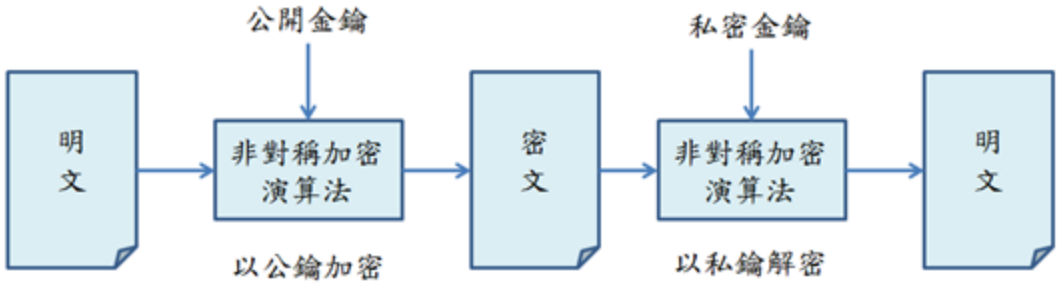
在非對稱式加密系統中，每個人都可以產生一對金鑰[3](Key)，稱為公開金鑰(Public Key)和私密金鑰(Private Key)，私密金鑰必須被擁有者好好保管。所有參與者都可以取得每個人的公開金鑰，而私密金鑰為個人所擁有，不在網路上傳輸。一個訊息用同一個人的公鑰加密，就必須用私鑰解開，反之，用私鑰加密就必須用公鑰解開(圖 2)。

RSA 加密演算法是一種非對稱加密演算法。在公開金鑰加密和電子商業中，RSA 被廣泛使用。RSA 是 1977 年由羅納德·李維斯特（Ron Rivest）、阿迪·薩莫爾（Adi Shamir）和倫納德·阿德曼（Leonard Adleman）一起提出的，當時他們三人都在麻省理工學院工作，RSA 就是他們三人姓氏開頭字母拼在一起組成的。

對極大整數做因數分解的難度，決定了 RSA 演算法的可靠性。換言之，對一極大整數做因數分解愈困難，RSA 演算法愈可靠。假如有人找到一種快速因數分解的演算法的話，那麼用 RSA 加密的訊息可靠性，就肯定會極度下降，但找到這樣的演算法的可能性是非常小的，今天只有短的 RSA 金鑰才可能被強力方式破解。目前世界上還沒有任何可靠的攻擊 RSA 演算法的方式，只要其金鑰的長度足夠長，用 RSA 加密的訊息理論上是無法被破解的。

[3] 密碼學中加密或解密用的秘密信息。

圖 2、非對稱式加密演算法之加密與解密

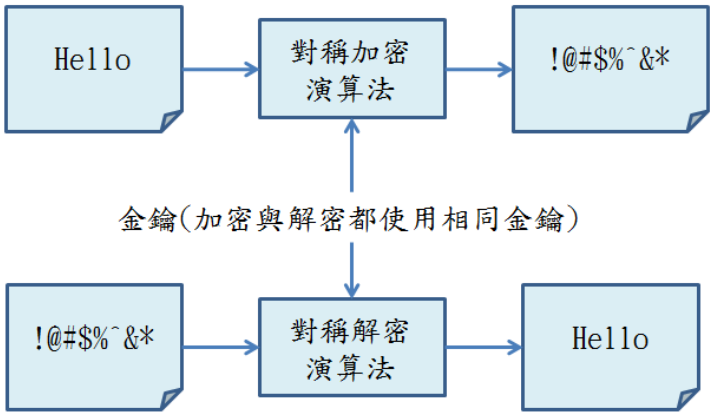


資料來源：本文整理

三、對稱式加密

相對於非對稱式加密演算法，對稱式加密演算法在加密和解密時使用相同的密鑰(圖 3)。常見的對稱加密算法有 DES、3DES、AES[4]、Blowfish、IDEA、RC5、RC6。

圖 3、對稱式加密演算法之加密與解密



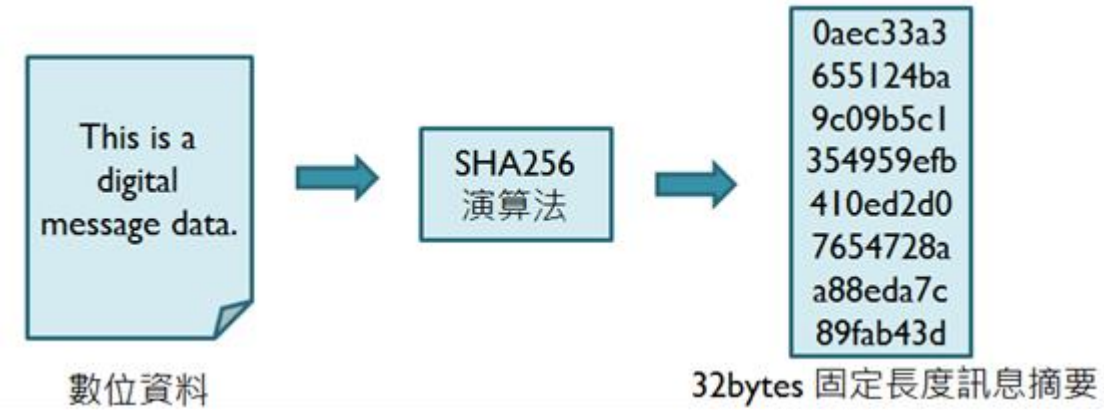
資料來源：本文整理

[4] 進階加密標準（Advanced Encryption Standard，AES），是美國聯邦政府採用的一種區塊加密標準。這個標準用來替代原先的 DES，已經被多方分析且廣為全世界所使用，現在進階加密標準已成為對稱金鑰加密中最流行的演算法之一。

四、SHA 雜湊(Hash)演算法

SHA 安全雜湊演算法（Secure Hash Algorithm）是一種能計算出一個數位訊息所對應到之雜湊值(Hash Value，是一個長度固定的字串，又稱訊息摘要)的演算法，SHA256 是輸出字串為 256bits(即 32bytes)的雜湊演算法(圖 4)。若輸入的訊息不同，它們對應到不同字串的機率很高。這演算法之所以稱作「安全」是基於以下兩點：

圖 4、雜湊演算法示意



資料來源：本文整理

1. 由訊息摘要反推原輸入訊息，從計算理論上來說是很困難的。
2. 想要找到兩組不同的訊息對應到相同的訊息摘要，從計算理論上來說也是很困難的。任何對輸入訊息的變動，都有很高的機率導致其產生的訊息摘要迥異。

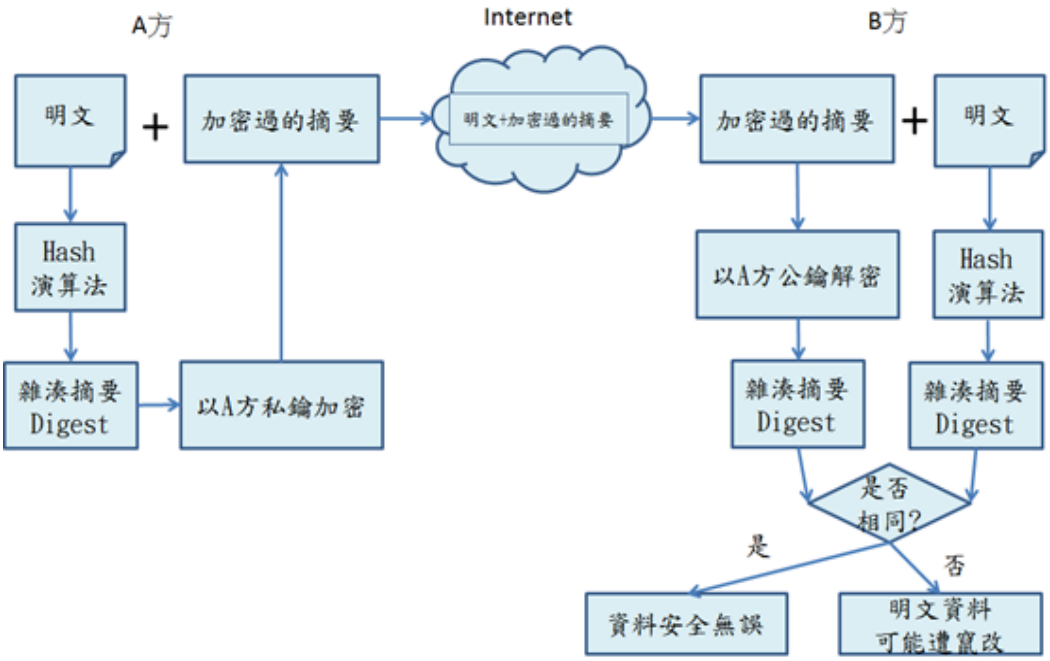
五、數位簽章

數位簽章是針對資料內容，先用不可逆的雜湊演算法，例如 SHA1 或 MD5，產出雜湊摘要（Digest）。接著，再運用簽章私鑰（Private Key）對雜湊摘要內容進行非對稱式的加密演算，例如使用 RSA 演算法，產生數位簽章的簽體內容(圖 5)。最後，將簽章資料內容、簽章者憑證、簽體內容封裝成標準資料格式。

雜湊摘要又被稱為數位指紋，因為雜湊演算法本身具有輸入資料不同，演算出來的雜湊摘要（Digest）就會有不同的特性。因此，運用雜湊摘要可以確保簽章資料的完整性，即沒有在傳輸過程中途被攔截竄改過。

數位簽章的驗證過程，就是使用簽章者的公鑰（Public Key），對簽體解密還原得到簽章資料的雜湊摘要（Digest）。另外，再對簽章資料進行與簽章相同的摘要演算法運算，得到雜湊摘要（Digest）。兩個雜湊摘要值進行比對，如果一致，代表用來簽章的簽章私鑰（Private Key）和簽章者的公鑰（Public Key）是成對的，而且簽章資料的內容也確保沒有被竄改，這樣可以達到簽章者的身分確認。

圖 5、數位簽章與驗證流程



資料來源：本文整理

貳、區塊鏈技術

區塊鏈(Blockchain)是建構比特幣(Bitcoin[5])、以太幣(Ethereum[6])等虛擬貨幣背後的主要技術。此類虛擬貨幣是一種網路上的數位貨幣，有別於諸如 PayPal、支付寶等集中式的線上金流系統，其與眾不同之處是基於 P2P 網路的去中心化設計與搭配了密碼學的運用。依據其設計，不論政府或任何人都很難惡意干擾其運作，同時也擁有匿名的特性，使得個人的隱私得以受到保護，本章將以區塊鏈技術最早被應用的比特幣區塊鏈為例，深入探究區塊鏈技術的內部運作細節。

一、比特幣(Bitcoin)運作原理

比特幣利用密碼學來組成發展貨幣的條件(例如：可以組成不同的面額、耐久與可輕易用於交易、容易識別真偽並確認價值)。它不受任何中央單位管理，性質較類似黃金。其產出的量有受到限制，但供應量充足(上限 21,000,000 單位)。它利用密碼學來確保製造比特幣非常困難，要偽造更是困難，但驗證卻非常簡單。

最初的比特幣是從礦工(Miner)獎勵而來。在比特幣的設計中，最重要的結構叫做區塊(Block)。區塊裡面收錄交易紀錄等重要資料，類似於帳本。要產生一個區塊需要大量的運算資源，所以得提供一些獎勵給礦工來鼓勵他們生產區塊。因此系統的設計上對於產生區塊的人，最初可獲得 50 比特幣作為獎勵(獎勵金額會隨著時間變動而遞減)。這些初始的獎勵金就是比特幣最原始的來源。可以想像是金礦坑裡礦工很辛苦地挖礦，最終挖到了黃金。這個過程也因此被稱為挖礦（Mining）。

比特幣並不是由某個單位集中管理，它的轉帳運用了公開金鑰加密演

[5] Satoshi Nakamoto (2009)
[6] Vitalik Buterin (2014)

算法來進行數位簽章，如此可以達到交易的不可否認性與完整性(即不被惡意更改)。實際帳戶名稱在系統裡其實是一把公開金鑰(又稱公鑰)，而私鑰則有如印章。私鑰可以用來簽署轉帳訊息給其它的帳戶，而公鑰除了當帳戶名稱，也可以讓大家驗證轉帳訊息是否屬實。例如：當礦工有了最原始的比特幣之後，他們就能用來花費。花費的方式，就是以個人的私鑰進行數位簽章，簽下「A(公鑰)將 X 元轉帳給 B(公鑰)」之交易訊息。這樣的交易訊息會經由 P2P 網路廣播出去，到最終，網路上的每個節點都會收到，礦工也會收到，並且將交易資料放入區塊中。

在收到交易紀錄後，礦工會先檢查這筆交易是否合法、有沒有重覆花費、來源的帳號是否有足夠的資金、數位簽章是否正確等。有問題的交易會被直接忽略。接著礦工在產生下一個區塊時，便會將所有收到的合法交易紀錄都寫進去。而在這個區塊被產生之後，它會透過 P2P 網路廣播到網路上，大家最終都會收到同樣的結果並且可以驗證。有了最新的區塊，搭配以前收到的所有區塊裡的礦工獎勵和轉帳紀錄，就能推斷出誰到底擁有多少錢。

如此，所有的交易紀錄共同由廣大的使用者與礦工群利用 P2P 技術維護與驗證，這些區塊前後串接在一起便形成了區塊鏈(Blockchain)，即為所有交易紀錄的帳本，也是支撐比特幣運作背後的終端技術，分散式帳本技術(Distributed Ledger Technology，DLT)。

二、區塊鏈(Blockchain)

比特幣區塊鏈是由各個區塊串接而成(圖 6)，區塊大致包含下列資訊:

A. 隨機值(Random nonce)

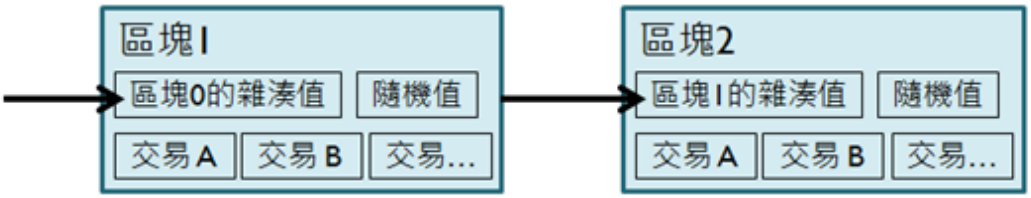
B. 難度值(Difficulty)

C. 上一個區塊的雜湊值(Hash Value)

D. 礦工獎勵，如：簽署 50BTC(比特幣簡稱)給礦工 Tom

E. 合法的交易資料

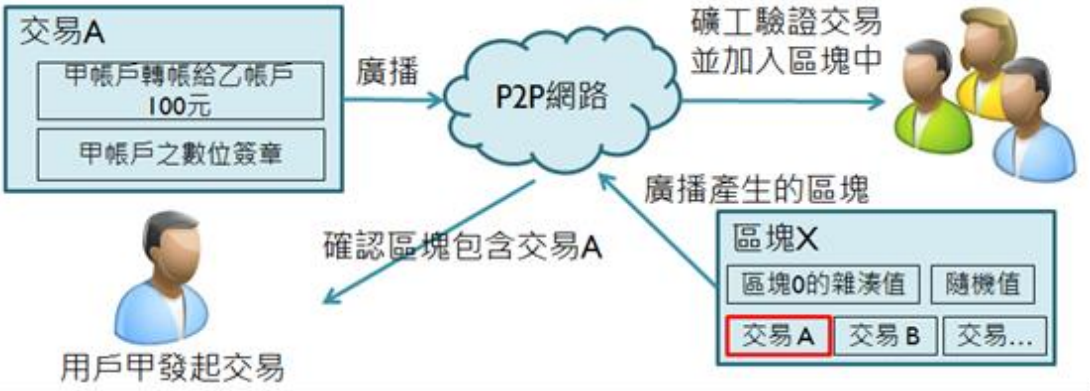
圖 6、區塊鏈示意圖



資料來源：本文整理

每個區塊都有記錄上一個區塊的雜湊值，形成一個可以往前稽核的區塊鏈。其中的合法交易資料是透過公鑰加密演算法進行數位簽章，每個戶頭都是一把公鑰，透過每個人的私鑰進行數位簽章，就可以把款項簽給收款人的戶頭，接著把簽章的資料廣播到 P2P 網路，最終被某個礦工驗證為合法交易後，收錄在區塊裡，再將區塊廣播至 P2P 網路，如此整個 P2P 網路就認可了這筆交易(圖 7、8)。

圖 7、比特幣區塊鏈交易流程



資料來源：本文整理

實際的區塊都是透過 P2P 網路來進行交換，所以資訊是完全公開的，每位礦工都會保存一個區塊鏈，可以對新的區塊進行驗證，每隔約 10 分鐘就會有新的區塊被產生。交易被收錄於區塊中得到初步的確認，區塊會再連結到前一個區塊，以得到更多確認。所有的交易歷史都儲存在「區塊鏈」中，是對所有交易歷史的紀錄。

一個合法的區塊，要在 P2P 網路上被所有的節點認可，必需符合一個條件，就是整個區塊產生出來的雜湊值，要小於難度值:

SHA256(Block data + Random nonce) < 難度值

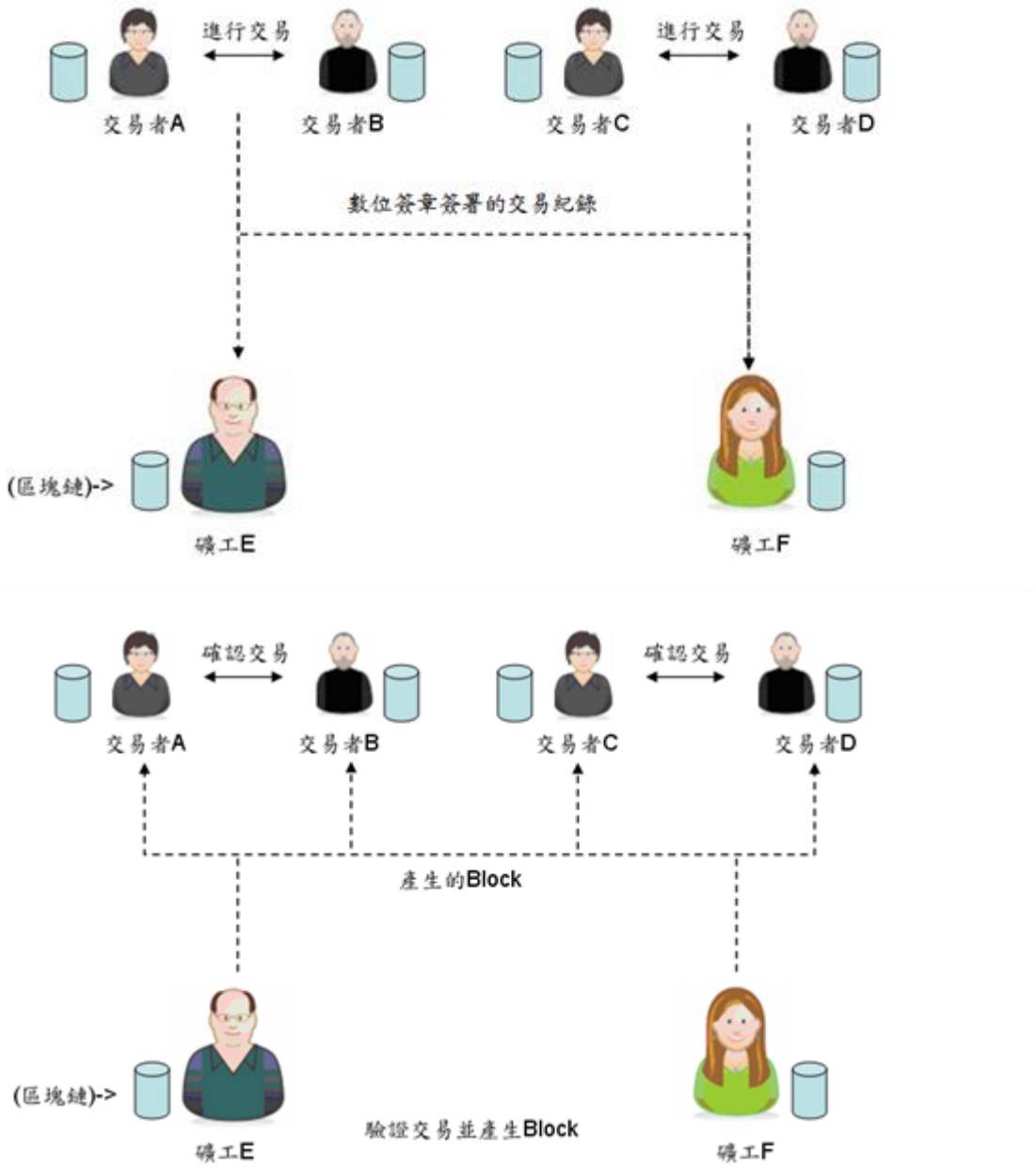
SHA256 算出來的長度是 256bits，也就是 32Bytes，這是一個很長的數字範圍，難度值則是一個較小的數字。SHA 雜湊函數算出來的數值一般都視為亂數且無法預測的數值，因此，產生合法的一個區塊唯一的方法，就是大量代入不一樣的隨機值(Random nonce)，進行大量運算直到產生一個區塊的 SHA256 雜湊值小於難度值，這樣的一個區塊才會被 P2P 網路上的所有節點認可[7]，當首先產生這樣一個區塊就叫做挖到礦了，礦工除了產生區塊的獎勵外，還會得到每筆交易的手續費。

配合當初就設計好的速度(約每 10 分鐘產出一個被認可的區塊)，每週系統會自動依照上週區塊平均產出速率去調整難度值，因此當越多礦工挖，會自動調整出一個更難挖的、更小的難度值來，如此可以確保比特幣的產出速度與量能夠穩定。而礦工獎勵金 50BTC，也會隨著時間變動，它設計每產生 210,000 區塊，獎勵金便會減半，越到後面挖礦的 BTC 獎勵金會越少，例如:最初是 50BTC 到 2020 年已經過了 3 次減半，變成了 6.25BTC，這樣來控制發行總量，到最後會變成沒有獎勵，但透過收取交易手續費用，

[7] 此種作法稱為工作量證明(Proof-of-Work，POW)，要求使用者進行一些耗時適當的複雜運算，並且答案能被服務方快速驗算，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。

還是會有礦工願意提供運算資源進行挖礦而生成區塊。

圖 8、區塊鏈上的交易示意



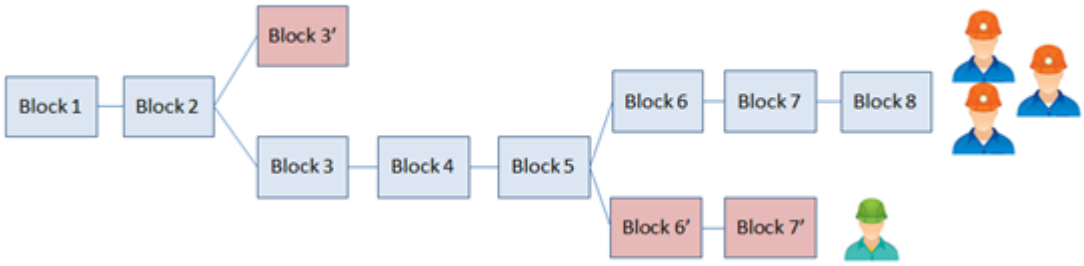
資料來源：本文整理

三、區塊鏈的收斂與安全性

區塊鏈為去中心化的設計，需要”共識”來確保網路上所有節點的區塊鏈

是一致的，區塊鏈用戶的共識是，鏈中難度總和最難的區塊鏈為共同認定的鏈條(通常也是最長的鏈條)。下圖來示意一個區塊鏈的全貌(圖 9)：

圖 9、區塊鏈全貌示意



資料來源：本文整理

由於區塊的產生是由礦工生成並於 P2P 網路上廣播，而網路上的廣播速度不一，如果有兩個礦工同時產生了一個區塊便會產生僵局，如圖中的 Block3 與 Block3'，鏈條產生了分支，由於這兩個區塊都是合法且正確的，所以會被區塊鏈保留下來，而透過網路的傳輸，礦工最終也會發現這個分歧，這時礦工可以選擇繼續於 Block3 之後生成區塊，或是在 Block3'之後生成區塊。然而，區塊鏈的共識是最難的鏈條才會被視為認定的區塊鏈，所以最終礦工會選擇較難的鏈條進行挖礦以達成共識，如此區塊鏈即完成收斂。

那麼如果一個駭客想要修改某一筆交易，他就必須與整個 P2P 網路上的礦工進行競爭，搶先於其他的區塊產生前，生成較長的鏈條來影響正確的鏈條，如 Block6 與 Block6'，然而由於駭客的競爭力遠小於整個 P2P 網路，最終正確的鏈條仍會獲勝。根據中本聰所著比特幣白皮書[8]中的計算證明，即使駭客擁有整個 P2P 網路上 10%的運算能力，在產生 6 個區塊後，他的獲勝機率為 0.1%。所以，依目前比特幣設計，一個交易只要有 6 個確

[8] Satoshi Nakamoto (2009)

認(即包含交易的區塊後方串接了 5 個區塊)，就被認為是一個足夠安全的交易。

近年來仍然有許多比特幣的交易網站遭受到駭客攻擊，損失慘重，甚至導致破產的局面，其最終的原因並不是區塊鏈的設計被破壞，而是網站的安全管理出現漏洞導致許多帳戶的私鑰被竊取，因此私鑰的安全保存將成為另一個課題。

四、區塊鏈的分類

目前已知的一些區塊鏈技術應用大致有以下三類：

(1)公開區塊鏈(public blockchain)

具有比特幣的一切特點，公開區塊鏈上的資料，所有人都可以使用，所有人都可以發出交易等待被寫入區塊鏈。共識過程的參與者（對應比特幣中的礦工）通過密碼學技術以及內建的激勵方式，維護資料庫的安全。公開區塊鏈是完全的去中心化，但需要有足夠的成本來維持系統運行，並依賴於內建的激勵。公開區塊鏈上試圖保存的資料越有價值，越要審視其安全性以及安全性帶來的交易成本與系統擴展性問題。目前公開區塊鏈中只有比特幣、以太坊等區塊鏈平台算是足夠安全的，應用實例：比特幣、以太幣。

(2)聯盟區塊鏈(federated blockchain)

參與區塊鏈的節點是事先選擇好的，節點間很可能是有很好的網路連接。這樣的區塊鏈上可以採用非工作量證明的其他共識演算法[9]，比如有 100 家金融機構之間建立了某個區塊鏈，規定必須 67 個以上的機構同意才算達成共識。這樣的區塊鏈上的資料可以是公開的，也可以是這些節點參與者內部的。聯盟區塊鏈是部分意義上的去中心化，可以做到很好的節點間的

[9] 如：POS、PBFT、Raft 等共識演算法

連接，只需要極少的成本就能維持運行，提供迅速的交易處理，低廉的交易費用，有很好的擴展性，資料可以有一定的隱私。開發者在共識下有能力更改協議，但是這也意味著在共識下，大家可以一起篡改資料。聯盟區塊鏈也意味著這個區塊鏈的應用範圍不會太廣，缺少比特幣的網路傳播效應。應用實例：Quorum、Corda、Ripple 平台。

(3)私有區塊鏈(private blockchain)

這樣的一個系統可以對比的是傳統意義上的共用資料庫。參與者全部是私有的，參與的節點只有使用者自己，資料的使用有嚴格的許可權管理。應用實例：Hyperledger Fabric 平台。

五、區塊鏈技術的優缺點

區塊鏈的特性是匿名性與去中心化的設計，由 P2P 網路上的用戶來進行交易驗證與交易紀錄的儲存，其優缺點歸納如下：

優點：

(1) 歷史交易資料透明，可追蹤且難以更改

在區塊鏈中可以找到所有交易資訊，任何人可以對它進行核實並隨時使用。同時它是加密安全的，透過雜湊值，區塊彼此串接，要更改交易資訊極其困難。

(2) 交易成本低

每筆交易只收取很少量的手續費。由於區塊鏈的運作資源來自整個 P2P 網路，用戶幾乎不需要花費設備成本來處理交易。

(3) 支付方便自由

任何時候在世界的任何地方，即時支付和接受任何數量的金額是可能的，不受銀行放假的影響，也不受國界的限制，也沒有任何強制的限制。

(4) 隱私與掌控權

用戶對他們的交易有完全的掌控權，商家不會像中心化的支付方式一樣被強迫支付不想要的收費。同時支付不需要個人信息和交易綁定，可以有利保護用戶的隱私資訊。

缺點：

(1) 帳戶匿名，發生爭議難以究責

帳戶匿名可以確保個人隱私，但同時也讓它易成為黑市洗錢的管道，一旦資產失竊或交易發生爭議，會發生無法追討與究責的問題。

(2) 交易的不確定性

區塊鏈是由 P2P 網路的共識而形成，在鏈條收斂的過程中，會導致某些交易的確認狀況改變，雖然可以經由多個確認來改善，但仍有不確定性的因子存在，若攻擊者掌握 P2P 網路上大部分的運算資源，則有可能癱瘓或操控整體系統。

(3) 私鑰的保存安全問題

竊盜者只要有辦法取得私鑰，就等於有能力偷走虛擬貨幣，目前仍然沒有百分之百安全的防竊機制。最常見的網路虛擬貨幣失竊案，主要出現於提供比特幣線上儲存機制的機構，而且亦有可能為內賊動的手腳，並不一定是外界的網路駭客。內賊所需要做的只有複製所有虛擬貨幣金鑰，接下來所有虛擬貨幣帳戶即任人宰割，一旦得手，被竊的虛擬貨幣就完全任竊賊運用，失主想找都找不回來。

六、區塊鏈的變形

由於比特幣的成功應用案例，許多各類型的去中心化虛擬貨幣以及區塊鏈的應用也如雨後春筍般陸續推出，在原始比特幣區塊鏈運用上做了不同的設計與改良，大致可以歸納出以下 6 類：

(1) 共識演算法的變形

區塊鏈的區塊生產認證是根據礦工的工作量證明(proof-of-work)，礦工透過花費大量的運算時間與資源來獲取產生區塊的認可，這樣會導致資源的浪費，而攻擊者若能獲取大量的運算資源即可操控區塊鏈。改良的變形，如 Nextcoin、Blackcoin、Blackcoin，係採用權利證明機制(proof-of-stake)，礦工獲取產生區塊的認可是根據其擁有的數位貨幣的總量以及持有時間來判定，如此可避免運算資源的浪費，亦可解決擁有大量運算資源即能操控區塊鏈的風險。

(2) 雜湊演算法的變形

SHA256 是目前區塊鏈使用的雜湊演算法，由於其算法特性易於平行處理，導致有許多客製化的硬體設備的推出，如比特幣挖礦機，這樣便會導致擁有一般設備的礦工無法與擁有特殊硬體設備的礦工競爭，產生高進入門檻以及運算資源掌握於特定礦工手中的問題。改良的變形，如 Litecoin、Dogecoin、Auroracoin，係採用 Scrypt 演算法，此演算法不易平行運算，很難以特殊硬體來進行加速運算，可以改善礦工競爭能力的平衡。

(3) 發行總量的變形

不同於比特幣有發行總量的限制，Peercoin 能以每年 1%的通膨率增加發行總量，而 Dogecoin 則無發行總量上限。

(4) 功能的變形

區塊鏈的應用不僅在虛擬貨幣，Nextcoin 更擴展至將數位資產記錄於區塊鏈上，可以進行各種去中心化的資產交易，如：股票、債券、黃金等，即俗稱的彩色幣(colored coin)。

(5) 去中心化的變形

區塊鏈的分散式帳本概念可以減少交易成本與提升交易效率，亦能取代備援的機制，然而完全的去中心化卻會給交易者帶來無擔保的風險。改良的變形，如高盛 SETLcoin 與 Ripple 平台，係採用多中心化的方式，由金

融機構擔任礦工的角色來驗證交易與產生區塊，如此既可以有中心化的金融機構來做交易的擔保，又可以擁有分散式帳本的優勢。

(6) 匿名制的變形

區塊鏈使用公鑰來作為交易帳戶名稱，可以有效保護交易者的個資與隱私，然而卻容易成為黑市洗錢的管道。改良的變形，如 CBDC(Central Bank Digital Currency，央行數位貨幣) ，係由金融機構替使用者建立一組公鑰與私鑰，使得帳戶與擁有者的資訊在金融機構有紀錄，如此可以防治區塊鏈淪為黑市洗錢的管道。

參、區塊鏈應用

區塊鏈技術除了在虛擬貨幣領域的應用外，還有許多可以發展的應用領域(如表 1)，「區塊鏈-新經濟藍圖」(Blockchain-BLUEPRINT FOR A NEW ECONOMY)一書[10]作者 Melanie Swan 將區塊鏈技術分成了三個不同的應用層面：區塊鏈 1.0(貨幣)、區塊鏈 2.0(契約)、區塊鏈 3.0(應用)。

表 1、區塊鏈技術的未來應用

類別	實例
金融交易	股票、群眾募資、債券、基金、養老金、退休金
一般	擔保交易
公共紀錄	土地和財產所有權、汽車登記、商業許可證、結婚證書、死亡證明
身分證明	駕駛證、身分證、護照、選民登記
私人檔案	借據、貸款、合約、賭注、簽名、遺囑、信託
證明	保險證明、所有權證明、公證證明
實體資產	房屋、飯店房間、汽車租賃、汽車使用權
無形資產	專利、商標、版權

資料來源：區塊鏈-新經濟藍圖

區塊鏈 1.0—貨幣，這是最初也是最典型的範例，即虛擬貨幣的機制和目前的市場應用。透過演算法和加密技術，區塊鏈的應用將虛擬貨幣推升成為網路上的貨幣，一種數位支付系統，同時它還可能成為“金錢的網絡”。貨幣和支付構成了第一個也是最顯著的應用。

[10] Swan, Melanie (2015)

區塊鏈 2.0－契約，契約即指區塊鏈技術未來應用方式，應用到現實世界中和商業契約相關領域。區塊鏈 2.0 開始脫離貨幣領域的創新，轉換到涉及契約功能的其他商業領域。

區塊鏈 3.0－超越貨幣、經濟和市場的應用，區塊鏈 3.0 是認證的應用。隨著全球交流和互動越來越頻繁，會有大量認證的需求出現，網路上的智慧財產權在過去一直是很難解決的問題，儘管各國政府和企業花費了大量時間和金錢投入到該領域中，但始終沒有取得良好的效果。區塊鏈認證方式提供了一個全新的思路，能夠把版權證明通過去中心化的方式來使用，可以做到跨越國家的客觀證明。

近期國內外產業與機構亦將區塊鏈應用於不同的領域，例如：財金公司的金融區塊鏈函證服務、各國的 CBDC 試驗計畫以及 NFT 等，以下針對各個實際應用案例說明。

一、財金公司金融區塊鏈函證服務

函證是會計師事務所在查核企業財務報表時，向金融機構發詢證函，以獲取查核證據(例如企業在銀行的存款餘額)的作業。以往需由查核人員先將紙本詢證函遞交受查企業用印後，再寄給企業往來之金融機構的總行或分行，由於金融機構多以人工方式填覆後再回寄給查核人員，過程不僅耗時費力，內容亦有人工填具疏漏錯誤之可能，且若未以掛號交寄，恐衍生企業印鑑及財務資料外洩、詢證函遺失及遭竄改、變造等作業風險。

金融區塊鏈函證服務是由財金公司協助推出，透過區塊鏈技術將函證作業數位化，使資料得以更加安全、機密、快速地傳遞，函證查詢時間可由平均半個月縮短到一天。除了節省作業時間及成本外，以往受查企業動輒須用印數十件、甚至上百件的企業授權書，只要以工商憑證、證期共用憑證等電子簽章進行一次線上授權即可輕鬆完成，大幅提升人員工作效能。

金融區塊鏈函證服務詢證函之收送皆由金融機構及會計師事務所之憑證加密簽章，未被授權的第三方無法讀取內容，查核人員並可使用專屬 QR Code[11] App 掃碼，驗證詢證函內容是否有被竄改，使函證作業更為安全可靠；結合區塊鏈技術及數位簽章，將函證作業數位化及自動化，為全球之首創，透過網路平台發送與回覆函證作業，大幅節省資料交換之人力、物力與時間，並解決紙本函證遺失及補發之情形，可提升企業財務報表透明度、保護投資人權益、及降低人為錯誤與舞弊問題，也是台灣金融科技的一大進展。

二、各國 CBDC 試驗計畫

隨著網路上虛擬貨幣的興起，世界各國也開始意識到本國的主權貨幣遭受威脅，紛紛嘗試計畫發行屬於本國主權的數位化貨幣，稱為央行數位貨幣(Central Bank Digital Currency，CBDC)，同時也嘗試以區塊鏈技術來進行試驗。

新加坡金管局(MAS)從 2016 年起至 2020 年歷經 5 年完成了 5 個階段的 Wholesale CBDC 試驗[12]，其中即採用了許多不同的區塊鏈技術平台來進行測試，如：Ethereum、Quorum、Hyperledger Fabric 以及 Corda 等平台，亦嘗試使用智能合約來達成交易隱私與安全需求；初期試驗場景包含了基本 CBDC 的發行、流通與回籠功能，也嘗試將流動性節省機制(Liquidity Saving Mechanism，LSM)設計於其中，後續又試驗了款券同步(Delivery vs. Payment，DVP)、跨境支付(Cross-border Payment)以及與新創科技業者合作進行許多創新商業應用，例如：私募證券買賣、債券發行、跨境換匯、貿易金融服務等。

---

[11] QR code（Quick Response Code，快速回應碼）是二維條碼的一種，在世界各國廣泛運用於手機讀碼操作。比普通一維條碼具有快速讀取和更大的儲存資料容量，。

[12] MAS (2017a)、MAS (2017b)、MAS (2018)、MAS (2019)、MAS (2020)

近期瑞典[13]以及歐洲央行[14]也積極探索 Retail CBDC，採用 Corda 平台進行各樣場景的試驗，甚至已有國家以區塊鏈技術正式發行 Retail CBDC，如：巴哈馬[15]的沙錢(Sand Dollar)亦結合區塊鏈平台技術研發。

三、NFT (Non-Fungible Token)

近期在網路上虛擬貨幣圈中最熱門的話題莫過於 NFT(Non-Fungible Token，非同質化代幣)，不同於一般同質化的虛擬貨幣可以累加，例如：5 個比特幣、10 個以太幣，NFT 是非同質化的代幣，亦即每一個代幣它的特徵和所代表的意義與價值皆是不同的，例如：藝術創作、歌曲、球員卡等。

數位化的創作，其檔案資料本身是可以無限複製的，例如：圖片、聲音、影片等，所以並不能藉著擁有其資料檔案來聲明其所有權，透過區塊鏈技術可以將這些作品以數位的形式記錄在區塊鏈帳本上，成為 NFT，可以像貨幣一般進行移轉與買賣，藉以實現數位世界中的所有權轉移。

[13] Riksbank (2017)、Riksbank (2018)、Riksbank (2021)
[14] ECB (2020)
[15] Central Bank of the Bahamas (2019)

肆、結語

區塊鏈技術運用了現今已成熟的資訊技術，建構出網路上的虛擬貨幣，透過 P2P 的去中心化網路技術，將交易資訊儲存在每個端點，運用共享各端點的運算資源來進行交易的處理與驗證，配合公私鑰加密演算法進行數位簽章以確保每筆交易的不可否認性與完整性，並運用雜湊演算法來確保每個區塊的一致性，同時每個帳戶以公鑰來識別以保障交易人的隱私。再配合礦工獎勵與交易費用等規則鼓勵使用者參與，使得虛擬貨幣自行成為了一個線上的金流生態圈。

區塊鏈 1.0(貨幣)、2.0(契約)、3.0(認證)等不同層面的應用，也隨著科技的進步與相關產業及機構的參與逐步地實現，不只在虛擬貨幣的領域，許多的應用場域如金融函證、CBDC 以及 NFT，為區塊鏈技術的未來應用塑造了更多的想像空間。

參考文獻

1. Central Bank of the Bahamas (2019) , “Project Sand Dollar: A Bahamas Payments System Modernisation Initiative,” Dec. 24.
2. ECB (2020) , “Report on a digital euro,” Oct. 2.
3. MAS (2017a) , “Project Ubin: SGD on Distributed Ledger,” Mar. 9.
4. MAS (2017b), “Project Ubin Phase 2 Report: Re-imagining RTGS,” Nov. 14.
5. MAS (2018) , “Delivery versus Payment on DLT,” Nov. 11.
6. MAS (2019) , “Jasper-Ubin Design Paper: Enabling Cross-Border High Value Transfer using DLT,” May. 2.
7. MAS (2020) , “Project Ubin Phase 5: Enabling Broad Ecosystem Opportunities,” Jul. 13.
8. Riksbank (2017) , “E-krona report 1,” Sep.
9. Riksbank (2018) , “E-krona report 2,” Oct.
10. Riksbank (2021) , “E-krona pilot Phase 1,” Apr.
11. Satoshi Nakamoto (2009), “Bitcoin: A Peer-to-Peer Electronic Cash System,” May. 24.
12. Swan, Melanie (2015), “Blockchain: Blueprint for a New Economy,” Feb. 24.
13. Vitalik Buterin (2014), “Ethereum Whitepaper,” Jan. 11.