

淺談區塊鏈

驊達科技 程正孚 整理

大家均是從事電腦通信科技業，身處在科技是日新月異的浪頭上，對於一些科技新知更須有些許的認識與了解，今天就為大家簡易介紹較新鮮的《區塊鏈》與它的應用層面。

甚麼區塊鏈

區塊鏈（英語：blockchain或block chain）是藉由密碼學串接並保護內容的串連文字記錄（又稱區塊）。

每一個區塊包含了前一個區塊的加密雜湊、相應時間戳記以及交易資料（通常用默克爾樹（Merkle tree）演算法計算的雜湊值表示），這樣的設計使得區塊內容具有難以篡改的特性。用區塊鏈技術所串接的分散式帳本能讓兩方有效紀錄交易，且可永久查驗此交易。

目前區塊鏈技術最大的應用是數位貨幣，例如比特幣的發明。因為支付的本質是「將帳戶A中減少的金額增加到帳戶B中」。如果人們有一本公共帳簿，記錄了所有的帳戶至今為止的所有交易，那麼對於任何一個帳戶，人們都可以計算出它當前擁有的金額數

量。而區塊鏈恰恰是用於實現這個目的的公共帳簿，其儲存了全部交易記錄。在比特幣體系中，比特幣位址相當於帳戶，比特幣數量相當於金額。

區塊鏈源起二說

拜占庭問題

關於區塊鏈的起源有兩個故事可以討論：首先是今日土耳其的伊斯坦布爾，是當年東羅馬帝國的首都拜占庭，當時東羅馬帝國強盛、國土遼闊，在國防的配置上，每一個軍隊的駐點都相隔遙遠，將軍與將軍之間只能夠依靠信差來傳遞重要消息，因此在對外作戰的時候，拜占庭軍內部所有的將軍和大官員需要達成一致的共識，才能夠決定是否出兵，但若軍隊中存有叛徒或是間諜更可能影響將軍的判斷，結果往往不能夠得到大多數人的意見，在已知有成員謀反的情況如何連結相隔遙遠的軍營來取得一致協議，就成了有名的「拜占庭問題（The Byzantine Generals Problem）」。



拜占庭將軍問題在網路世界的解讀是在容許入侵體系的一種模型化，後來發現區塊和區塊鏈可以解決這個問題，1982年美國計算機科學家Leslie Lamport把軍中各地軍隊彼此取得共識、決定是否出兵的過程，延伸至運算領域，設法建立具容錯性的分散式系統，即使部分節點失效仍可確保系統正常運行，可讓多個基於零信任基礎的節點達成共識，並確保資訊傳遞的一致性，而2008年出現的比特幣區塊鏈便應用了此觀念。

比特幣夯翻全球

第二個也就是大家所熟知的區塊鏈起源就是「比特幣」，為了比特幣而產生了區塊鏈，比特幣就是區塊鏈的第一個應用。區塊鏈就是比特幣的底層技術，或是可以說，比特幣帶動了區塊鏈觀念的興起，去中心化的公開性讓所有人都能夠自由購入與售出，交易的匿名性和金流資料的安全性更是比特幣所依靠的基礎。

比特幣是由一個名叫中本聰（Satoshi Nakamoto）的人所發明，但其實現實中並沒有人知道中本聰究竟是誰，連其性別、職業或是年齡都不甚清楚，關於比特幣的討論交流全部在網上進行。比特幣的命名是「Bitcoin」，取自電腦運算的最小位元，是一套點對點（P2P）形式的「虛擬貨幣」，不需要依靠特定的貨幣機構發行，對持有者而言，比特幣除了幣值相對穩定，而且在全球都能夠使用，加上它去中心化的安全性，讓它在全世界一炮而紅。

這樣的虛擬貨幣交易成本低、穩定安全，有些國家（例如俄羅斯）甚至考慮要開發國定的虛擬貨幣，但在現有的金融制度底下，

大多數國家的法律還無法定義比特幣，這樣的虛擬貨幣並不受到任何政府、任何銀行控制，因此它目前也還未被合法化。

比特幣將所有的交易歷史都記錄在區塊鏈之中，區塊鏈會持續延長並相互連結，且新的區塊一旦加入到區塊鏈中就不會再被移走。比特幣的交易數據需要連續得到六個區塊的驗證後成立。

區塊鏈其實是公眾的電子記帳資料庫

首先，對區塊鏈需要的第一個理解是，它是一種「將資料寫錄的技術」，區塊鏈起源於比特幣，因此區塊鏈就是作為比特幣的底層技術，是一個「去中心化的分散式資料庫」，透過集體維護讓區塊鏈裡面的資料更可靠，或是可以把它理解成是一個全民皆可參與的電子記帳本，一筆一筆的交易資料都可以被記錄。

區塊鏈技術可以說是互聯網時代以來，最具顛覆性的創新技術，依靠複雜的密碼學來加密資料，再透過巧妙的數學分散式演算法，讓互聯網最讓人擔憂的安全信任問題，可以在不需要第三方介入的前提下讓使用者達成共識，以非常低的成本解決了網路上信任與資料價值的難題。

去中心化和不可竄改性

區塊鏈有幾個最重要的特色，首先就是它的核心宗旨——去中心化，為了強調區塊鏈的共享性，讓使用者可以不依靠額外的管理機構和硬體設施、讓它不需要中心機制，因此每一個區塊鏈上的資料都分別儲存在不同的雲端上，核算和儲存都是分散式的，每個

節點都需要自我驗證、傳遞和管理，這個去中心化是區塊鏈最突出也是最核心的本質特色。

在去中心化的前提之上，每個運算節點的運作方式就會透過「工作量證明機制（Proof of Work，POW）」來進行，也就是誰先花費最少的時間，透過各自的運算資源來算出答案並得到認可它就成立，如此一來就可以實現多方共同維護，讓交易可以被驗證。

與去中心化類似的概念是區塊鏈的「開放性」和「獨立性」，區塊鏈技術的基礎是開源的，除了其中交易的訊息會另外被加密之外，其中所有的運算數據都是對所有人開放，任何人都可以透過公開的介面去查詢區塊鏈中的數據，系統信息非常透明。而獨立性指的是整個區塊鏈的系統不需要依靠第三方，因此便不會受到任何外力的干預。

同時也就衍生出了區塊鏈的相對「安全性」和「匿名性」，因為區塊鏈的數據是分散式的演算，因此也沒有人可以隨意修改網路上的數據，去除了人為操控的可能，也就讓區塊鏈本身相對安全，因為區塊鏈上的訊息不需要公開驗證，彼此之間的訊息傳遞都可以匿名進行。

區塊鏈的另一大特色是其「不可竄改性」，區塊鏈中的每一筆資料一旦寫入就不可以再改動，只要資料被驗證完就永久的寫入該區塊中，其中的技術是透過Hashcash演算法，透過一對一的函數來確保資料不會輕易被竄改，這種函數很容易可以被驗證但卻非常難以破解，無法輕易回推出原本的數值，資料也就不能被竄改，每個區塊得出的值也會被放進下一個區塊中，讓區塊鏈之間的資料也都被正確的保障。





區塊鏈將成長為超級帳本

目前區塊鏈的演進大約可以分為三個主要階段，第一階段也就是以比特幣作為代表，這個體系將區塊鏈建立起來，而第二階段是以以太坊為主，以太坊（Ethereum）也是一個開源的公共區段鏈平台，其中以太幣（Ether）也是透過專用加密技術的去中心化的虛擬貨幣，到目前為止以太幣已經是市值第二高的加密貨幣，僅次於比特幣。

區塊鏈的第三階段目標就是超級帳本，以Linux基金會所創辦的「超級帳本計畫（Hyperledger Project）」為例，這是第一款專門為大型企業所設計的區塊鏈模組，主要是希望讓企業可以更輕鬆的導入區塊鏈技術，也代表著區塊鏈的發展日趨成熟。

「Hyperledger Fabric」有許多專門為商業導向所設計的用途，包含貨運追蹤、智慧合約等功能，期待可以落實區塊鏈的應用，因為區塊鏈有共享式帳本的特性，在這個區塊鏈中所有的成員不論是上下游或是協同關係，都能夠透過區塊鏈來快速的共享大量的資源，同時也能兼顧安全性，因此這樣成熟的區塊鏈技術可以應用的層面應該值得各界期待。

區塊鏈應用

目前區塊鏈應用的情況以金融業最多，同時也不少政府部門表示對區塊鏈的運作感興趣，另外像是醫療界也能夠妥善運用區塊鏈技術，醫院中病人的數據、病歷等等都需要隱私，同時區塊鏈的不可竄改性也讓病患資料可以被保障，甚至未來能夠結合人工智慧，將病歷更進一步的導向智能諮詢、智能抓藥

等功能，行動機器人醫生的需求就是大量的、可靠的安全資料，這樣的需求可以透過區塊鏈技術來滿足，在醫療費用越來越高的此刻，遠端醫療的低成本市場、結合人工智慧區塊鏈的醫療保健服務值得我們期待。

麻省理工學院（MIT）採用了區塊鏈技術，讓百餘名畢業生透過智慧型手機領取他們的數位文憑，成為全球首批頒發虛擬證書的大學之一。當學生下載Blockcerts Wallet之後，它會產生一組金鑰（私鑰加上公鑰），並將公鑰傳送給MIT，把它寫入數位紀錄中，再於該區塊鏈加上認證碼。區塊鏈上並沒有記錄文憑資訊，有的只是MIT建立該紀錄的時戳，最後MIT再寄出含有公鑰的數位文憑，藉由學生手機上的私鑰來進行本人驗證。

FinTech - 金融 科技

FinTech（Financial technology）將我們所認知的傳統金融服務，轉型並透過科技的手段進行，讓企業可以提供更有效率的服務，也讓使用者可以更便利即時的操作。換一個角度切入也可以想成是，科技業漸漸佈局到以往傳統的金融業，試圖帶來一波新的衝擊性改變。

不論從哪一個角度來解讀，可以知道的是Fintech將會是未來科技和金融業界都無法忽視的趨勢。在這個數位崛起的時代，Fintech也不僅僅只是科技與金融，甚至市場與政府，都是這個趨勢下需要應運出新服務的角色。而區塊鏈Blockchain技術的應用，也是站在金融的基礎之上進而興起。

資料來自 維基百科、Cloud Mile

