區塊鏈是什麼？可以吃嗎？

戴葦婷 文 2018/04/22

比特幣早在2009年就在網路上流通，隨著時間的推演，比特幣的底層技術區塊鏈越來越成熟，直至2016年時，區塊鏈終於普遍被認為是一項有前景的技術，其不需要中間人監管的特性，讓技術人員紛紛開始投入研究。究竟令人著迷的的區塊鏈為何物？

拜占庭問題催生區塊鏈概念

談到為何有區塊鏈的誕生，就要搞清楚何謂拜占庭問題。在國土極為遼闊的東羅馬帝國時代，戰爭頻仍，將軍們常帶領士兵各自前往分配的要塞駐守，而每個要塞距離都十分地遠，各個將軍之間很難互相傳遞訊息，若是在已知有內賊的情況下，形勢更加雪上加霜。如何在這樣的狀況下彼此取得共識、傳遞正確訊息以及決定是否出兵，就是著名的「拜占庭問題(The Byzantine Generals Problem)」。

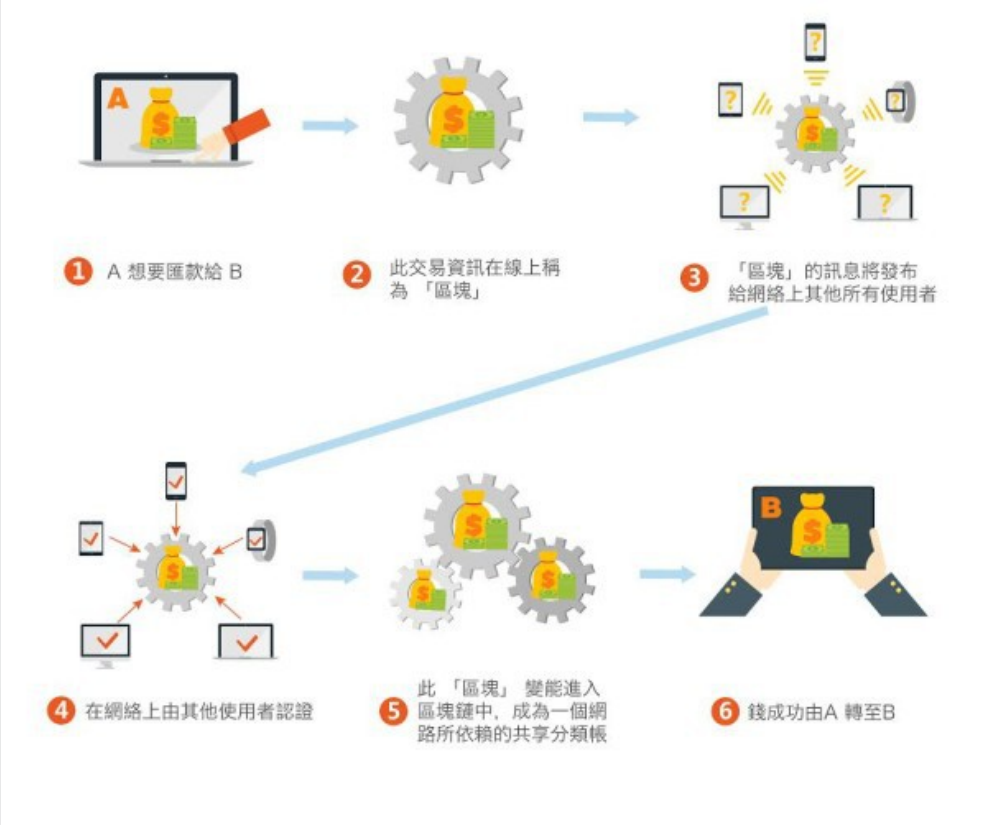
區塊鏈相關概念是1982年美國計算機科學家萊斯利．蘭波特試圖在運算領域解決拜占庭問題時衍生而出。蘭波特建立具容錯性的分散式獨立系統，也是當今被視為區塊鏈的雛形。該系統不需要依靠全部節點仍可順利運作，並讓彼此陌生的節點達成共識，使資訊內容傳遞一致。

相關的研究一直在進行著，而在2008年世界金融危機，雷曼兄弟倒閉後兩週，一位自稱中本聰的人發表了〈比特幣:一種點對點的電子現金系統〉論文，該文中的比特幣即建立在區塊鏈上。隔年，中本聰率先實作出比特幣系統，區塊鏈於焉出世。

區塊鏈為何方神聖

區塊鏈是比特幣的底層技術，那它到底如何運作？其實可以把區塊鏈想像成是帳本系統。把區塊鏈以字拆開，「區塊」是帳本的內頁，用來記錄交易，並標有頁碼（蓋時間戳），這不僅能夠防止重複支付問題，也能確保區塊的前後相連。那麼時間戳由誰來蓋？由一群參與記帳的「礦工」來執行這個任務。中本聰讓他們去競爭記帳權，規則是在正確記帳的同時也要解SHA256演算法難題，誰最先解出題目，誰就能得到記帳權並獲得獎勵（二十五個比特幣）。

「鏈」則是指在每個礦工的電腦中都保存著相同的帳本，裡頭的每一筆資料皆要互相達成共識，才能確保帳本內容是同步的。換句話說，礦工都擁有同一份帳本，而每一筆交易都必須由全部記帳者核對正確才能被記錄於帳本中，這樣的機制使中本聰完美地創造出「去中心化」的信用系統，以群體共識取代中央信任，不需要中間人的存在。



以匯款圖解區塊鏈運作原理。（圖片來源 / beBit）

區塊鏈不可忽略的特性是安全性十足。在網路世界，資安是令人擔憂的問題，而區塊鍊藉由必須讓礦工集體達成共識才能記錄於帳本的特性，使得駭客若想變更交易紀錄，必須讓51%的礦工達成共識，這比單單駭入銀行系統還難上許多，這個特性使得區塊鏈安全性較高。

區塊鏈可以細分為私有鍊（private blockchain）、公共鍊（public blockchain）及聯盟鍊（consortium blockchain）。它們之間的關係可以想像成是學校課程。公共鍊是通識課，供任何人選修，每筆交易都是匿名公開，是區塊鏈最原始的樣貌，知名的比特幣區塊鏈即屬此類。這樣的特性無法滿足企業對交易資訊隱私的要求，於是出現具有排他性的私有鍊以及聯盟鍊。私有鍊有限制性，可以比擬做限本系選修的課，而聯盟鍊則居於公共鏈及私有鏈中間，可以比擬做某學程開的課，不限任何系只要是該學程的學生都能選修。

事物總有一體兩面，講完優點，就該講缺點了。區塊鏈雖能確保資料在傳遞過程中不被竄改，但並沒辦法驗證作為源頭的資料是否正確，是導致現今區塊鏈無法

普遍應用在各行業的主因，舉例來說，某物流公司運用區塊鏈技術來紀錄貨物從發出到接受過程中的所有資訊，然而若運送人員作假標示成已出貨，因區塊鏈無法驗證源頭資料，使客戶無從知曉鏈上資訊的真實性。另外，區塊鏈運作效率仍有待提升，當在鏈上的礦工越來越多時，就會加長取得共識的時間，處理速度也會越來越緩慢。雖然已陸續研究出應對方法，但可惜的是目前仍沒辦法完美地解決問題。

ICO與代幣經濟

區塊鏈的應用十分多元，近期火熱的ICO（Initial Coin Offering，中譯：首次代幣眾籌）即是基於區塊鏈概念衍生而出。ICO可以比擬做區塊鏈世界的IPO（Initial Public Offerings，中譯：首次公開募股），ICO通常結合專案發行數位貨幣，概念相當於IPO的公司股票，差別是ICO的貨幣募資後能夠兌換服務，而這樣的特性衍生出代幣經濟。舉個例子，假設現在要買雞排，那就要拿60元跟店家換一塊雞排，而在代幣經濟下，就像是去電子遊樂場換限量的代幣一樣，拿錢去換「雞排幣」，然後再用「雞排幣」去買雞排，發行「雞排幣」的動作就是ICO。值得討論的是，直接拿法幣買跟用代幣「雞排幣」買有什麼差別？其實，發行「雞排幣」的行為對不論是消費者還是生產者某種程度上都是更有利的。對生產者而言，能夠降低生產風險，在投入大部分成本之前，就能基於募資的程度先勘查市場；對消費而言，能夠因為「雞排幣」的稀有性而讓幣值水漲船高，使得「雞排幣」有類似股票的特性。

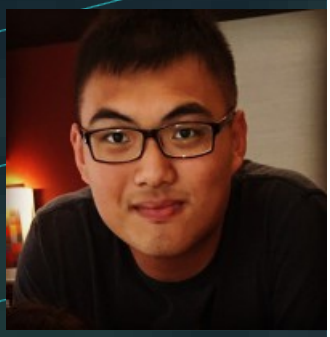
在投資ICO專案以前，通常有白皮書（相當於說明書）可以看，這可以讓人判斷是否要投資，換句話說，我們可以推得白皮書是需要受管制的。若不在適當管制之下，白皮書內容就能夠隨意增添，天花亂墜的內容將可能造成投資者吃虧。現今ICO的多數國家包括台灣都沒有明確的法令規範，這使得內容品質優劣不一，有些專案甚至不提供白皮書，在這樣的情況下，漸漸有端看發起人的名氣決定是否投資的情勢，讓投機者有機可趁。中國、韓國則採嚴禁態度，視ICO為非法行為；近期諸如德國、日本逐漸正視其問題，強化ICO的法規，防止民眾因為盲從而造成財物損失。

ICO專案Bitconnect在今年1月17日突然宣布關閉，加密貨幣BCC暴跌97%，是一場經典的ICO騙局。（圖片來源 / Bitconnect）

是未來還是泡沫

區塊鏈的出現達成了資產交易的去中心化，免除了是否要信任中間者的疑慮，加上應用的多元性，為人們的生活帶來相當大的方便。然而，有心者仍可利用區塊鏈特性造成他人利益的損害，例如前面提過的ICO專案，即是看準投資人對代幣經濟的信心，而賺取利潤；另外，人稱「股壇長毛」的大衛韋伯曾說過建立在區塊鏈上的比特幣是世上首個分散式的龐式騙局，在加密貨幣市場上擁有大批資源的大戶掌控相當大比例的貨幣，運用技巧讓幣值大起大落，高賣低買，謀取利益。區塊鏈是一門具高競爭力、高前景的技術，但就如同雙面刃一樣，必須小心發展。儘管風險不低，仍是一場你我不能錯過的數位革命。

記者 戴葦婷



編輯 鄭頎