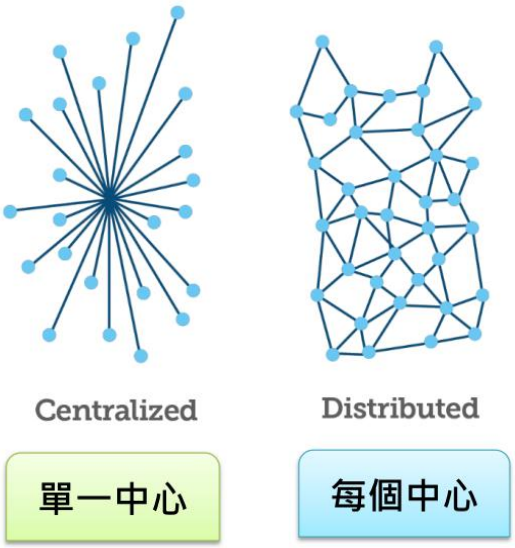
區塊鏈與比特幣 (Block Chain and Bitcoin)

2008 年全球發生了金融危機，美國大型銀行接連倒閉，讓老百姓不禁擔心起銀行會不會停擺，存在銀行的錢可能會領不出來，金融轉帳也將無法進行。同年 11 月，中本聰(目前還不知他到底是誰?)發表了比特幣的白皮書[1]，以點對點(peer-to-peer)的技術，實現了去中心化的電子現金線上支付，不必透過金融機構或第三方機構認證就可以直接支付。而區塊鏈就是源起於中本聰的比特幣，它是比特幣的底層技術。

去中心化是區塊鏈重要的特點，區塊鏈基本上就是一個分散式的記帳系統。目前消費者的金融支出，不管是信用卡或銀行提款轉帳，都是由銀行來進行記帳，銀行做為單一的中心負責保管著所有的帳本，一旦銀行的帳本遺失或遭到駭客竄改，消費者將會蒙受損失。那怎麼樣可以做到去中心化呢？就是讓所有區塊鏈應用的參與者都進行記帳，讓完整的帳本保存在所有的節點上。舉例來說，當你要將錢轉帳給小明時，你就要向所有人大聲宣布，“我轉帳一萬元給小明”，透過網路的廣播，所有的人都會收到這一訊息並記錄下來。因此在區塊鏈系統中的每一筆交易都會傳送給每個人，讓每個人都可以進行記賬，並將一段時間內的交易記錄打包為一個區塊，但因為每個人收到訊息的時間不一致，因此區塊內記錄的交易資料也有可能會不一樣。在這裏區塊可以想像成是帳本的一個頁面，將各頁串在一起就形成了一個區塊鏈，也就是整個帳本。



圖一、區塊鏈的去中心化 [2]

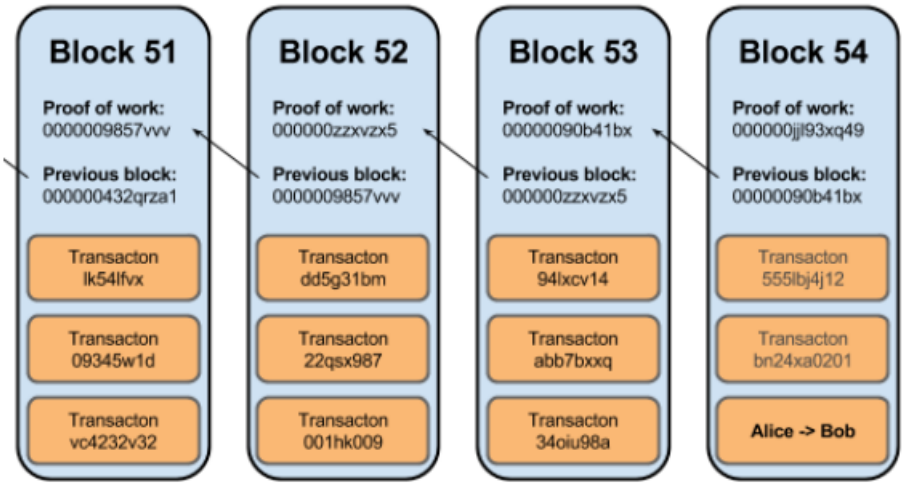
那誰有權力將記帳的區塊加到帳本中呢？比特幣區塊的容量大小為 1MB，平均每 10 分鐘就可以產生一個區塊，負責記帳產生區塊的人被戲稱為礦工，產生區塊的動作則被稱為挖礦。每位礦工都需要通過解 SHA256 的難題，去競爭這 10 分鐘區塊的記帳權，而 SHA256 的難題具有難以算出，卻容易驗證的特點。礦工完成的區塊會被送到網路中，系統會判斷和驗證這段時間內記帳最快最好的人，把他產生的區塊寫入帳本中，並給予比特幣作為他記帳的獎勵。

SHA(Secured Hash Algorithm) 是安全雜湊算法的縮寫，256 則是因為算法計算的輸出為 256 位元固定長度的資料，稱為雜湊值(Hash)。安全雜湊算法的特性是不論輸入資料的多寡，都能得到固定長度的雜湊值，只要一點點內容的變動，就可以產生出完全不同的雜湊值。如表一：“apple”和 “Apple”僅相差一個字母，但二個計算出來的雜湊值就完全不一樣[3]。若想從雜湊值，反推如何修改原始檔案的數據是非常困難的，因此可以確保資料無法被竄改的安全性。

輸入文字	雜湊值(以 16 進位表示，每個字母代表 4 位元，共 64 個字母)
apple	3a7bd3e2360a3d29eea436fcfb7e44c735d117c42d1c1835420b6b9942dd4f1b
Apple	f223faa96f22916294922b171a2696d868fd1f9129302eb41a45b2a2ea2ebbfd

表一、SHA256 輸出值

每一個區塊裏都包含了前一個區塊的雜湊值，交易記錄，時間戳記及一個可變動的數字 nonce，它的範圍從 0 到 2^32。調整 nonce 的值可以讓 SHA256 產生不同的雜湊值，而挖礦就是透過不斷地調整 nonce 值，讓所產生的雜湊值前面 n 個位元值均為 0，如圖二中 Proof of Work 的值。由於無法由雜湊值反推出 nonce 值，所以只能靠不斷地計算和嘗試來求出解。第一個解出這個難題的人取得記帳權，他會將區塊傳送到網路上讓其它的礦工進行驗證。n 的值越大計算難度越高，透過調整 n 值就可以控制挖礦的難度和產生區塊的平均時間。



圖二、區塊的內容示意圖[2]

區塊鏈的第一個應用是比特幣，也是目前最成功的應用，未來區塊鏈可以應用在很多領域上，例如：公益團體的記帳，捐款流向可以被追蹤且難以被竄改；也可以透過區塊鏈整合分散在各醫療院所的醫療資料，再透過加密技術授權資料開放的對象[4]。

參考資料:

1. "Bitcoin: A Peer-to-Peer Electronic Cash System," Satoshi Nakamoto, https://bitcoin.org/bitcoin.pdf
2. "Blockchain as a Service," 陳立群, https://s.itho.me/egov/2017/B-1135.pdf
3. SHA-256 Generator, https://www.freeformatter.com/sha256-generator.html#ad-output
4. "區塊鏈全面入侵，翻轉你生活的 7 大應用," 張道宜、蘇思云, https://www.cheers.com.tw/article/article.action?id=5091866