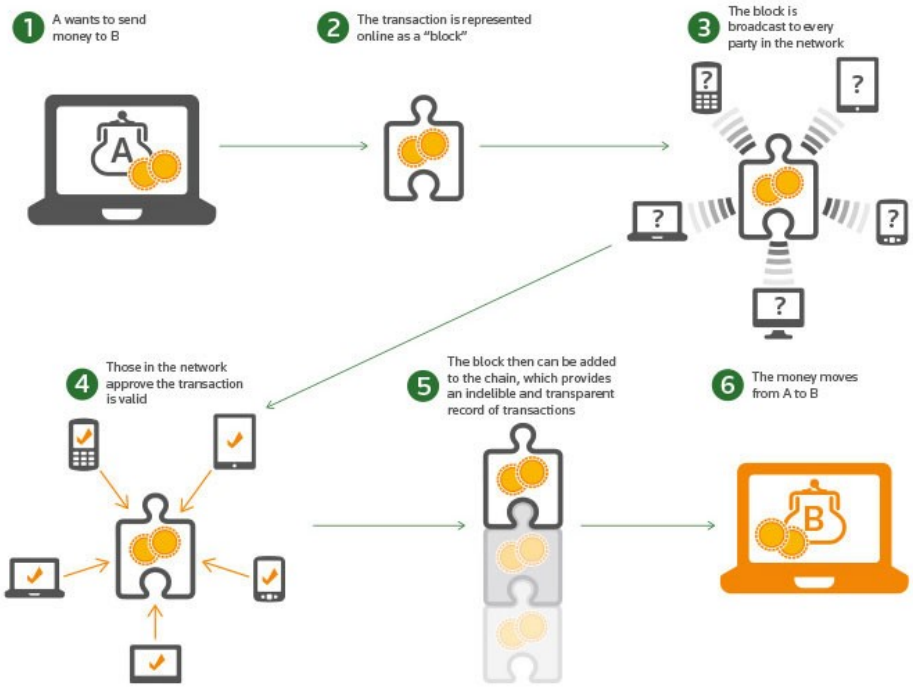
技師園地

# 淺談區塊鏈 (Blockchain) ◆馮靖博技師

最近幾年伴隨者金融科技(Fintech)這個火紅的產業，區段鏈（英語：blockchain 或 block chain）這個字眼也變成熱門，筆者對於這個新領域也好奇了起來，這次來跟大家分享一下。根據維基百科[i]，區段鏈（英語：blockchain 或 block chain）是用分散式資料庫識別、傳播和記載資訊的智慧化對等網路，起源自比特幣(Bit Coin)。區段鏈是一串使用密碼學方法相關聯產生的資料塊，每一個資料塊中包含了若干次比特幣網路交易的資訊，用於驗證其資訊的有效性（防偽）和生成下一個區段。該概念於 2008 年在中本聰的白皮書中提出，在隨後一年當比特幣網路開始，中本聰在實現了第一個區段，即「創世區段」。區段鏈在網路上是公開的，可以在每一個離線比特幣錢包資料中查詢。比特幣錢包的功能依賴於與區段鏈的確認，一次有效檢驗稱為一次確認。通常一次交易要獲得數個確認才能進行。輕量級比特幣錢包使用線上確認，即不會下載區段鏈資料到裝置儲存中。

我們可以用以下的圖來說明一下區塊鏈應用實施的概念，如果 A 要把錢轉給 B，則過程可以如下所示；

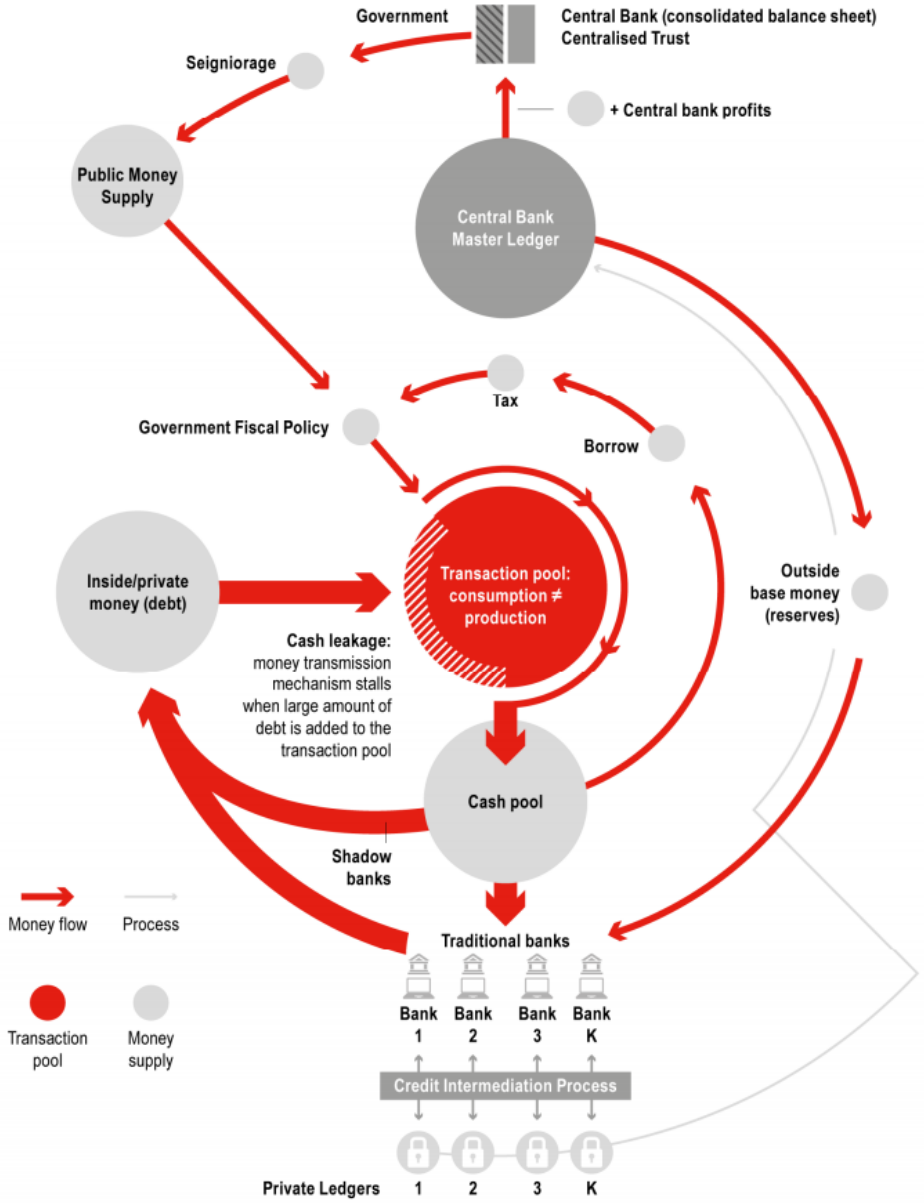


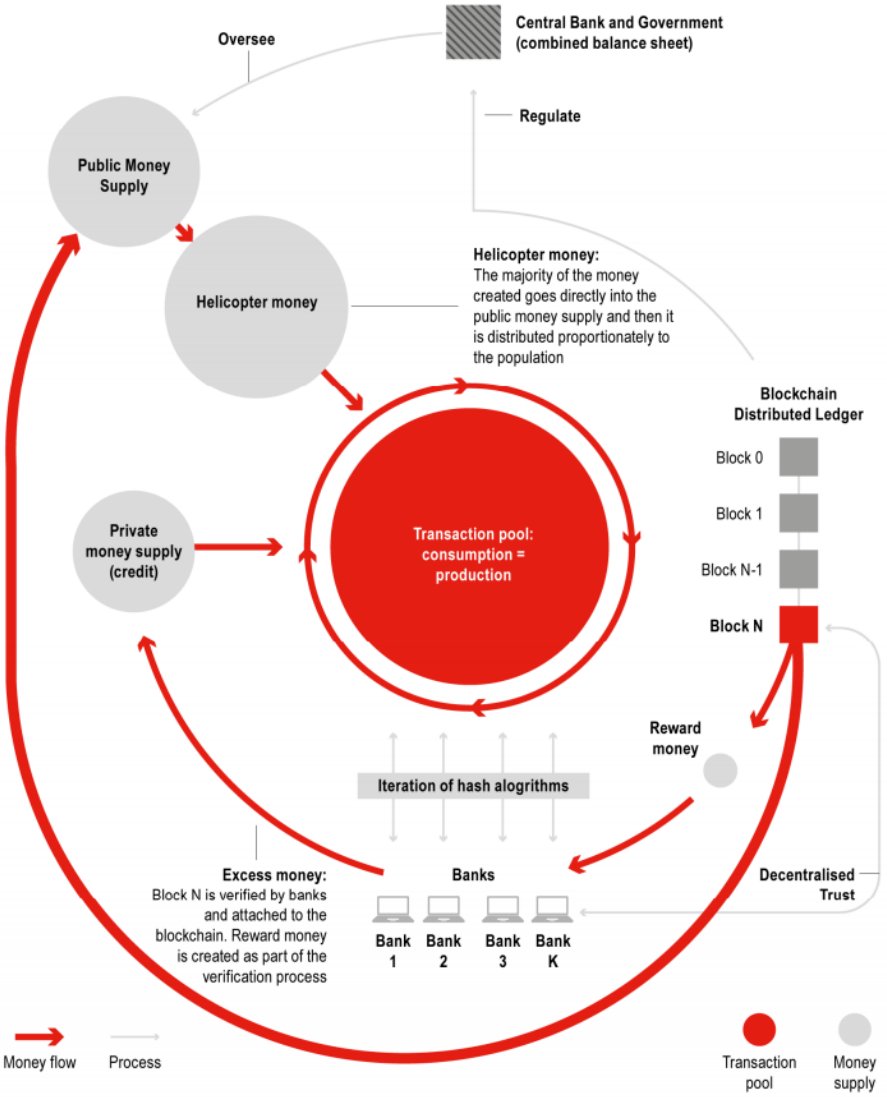

Source: https://www.thejmgroup.com/blog/blockchain-technology-by-alex-powell/

由上面的運行釋例我們可以看到很多人提到區塊鏈的特徵是「去中心化」、「不容竄改」，這對於我們理解區塊鏈技術是一個很好的理解，以往的金融交易往往都

有所謂的中介者如銀行等中心的腳色，交易雙方往往都必須透過特定的第三者，如此一來交易成本必然會被墊高(中介者的利基所在)，當使用區塊鏈技術之後中心的重要性就不在，也就是傳統金融機構的掌控性不在，交易成本預期也能夠降低，交易雙方可以達到雙贏。至於第二個特徵「不容竄改」是因為傳統中心的話要竄改只要改中心的資料即可，然而區塊鏈技術每個帳本存在每個節點，所以改一個點是沒有任何意義的，由此可以看出區塊鏈技術的安全性亦比傳統模式高。

我們再以下兩圖理解一下傳統金融體系貨幣利率形成以及改採區塊練的方式






Source:
http://www.businessinsider.com/hsbc-says-the-blockchain-could-be-used-for-radical-central-bank-helicopter-money-policies-2015-11

由上兩圖可以看到去中心化以及使用了區塊(Block)，接下來我們開始聊聊區塊鏈技術產物**比特幣（英語：Bitcoin）**，2009 年以來，比特幣等虛擬通貨紛紛出現，他是一種全球通用的加密網際網路貨幣。與採用中央伺服器開發的第一代網際網路不同，比特幣採用對等網路開發的區塊鏈，開啟第二代網際網路的廣泛應用。比特幣是經由一種稱為「挖礦」的過程產生(電腦計算)，參與者透過處理交易驗證和記錄來獲取作為手續費的比特幣，或取得新產出的比特幣。使用者利用個人電腦、行動裝置或網路上的電子錢包軟體來交易比特幣。比特幣可經由挖礦取得，也可用來交換貨物、服務，以及其他貨幣。

## 什麼是挖礦？

比特幣礦工通過解決具有一定工作量的工作量證明機制問題，來管理比特幣網路：

確認交易並且防止雙重支付。中本聰在他的論文中闡述說，「在沒有中央權威存在的條件下，既鼓勵礦工支援比特幣網路，又讓比特幣的貨幣流通體系也有了最初的貨幣注入源頭。」中本聰把通過消耗 CPU 的電力和時間來產生比特幣，比喻成金礦消耗資源將黃金注入經濟。比特幣的挖礦與節點軟體主要是透過對等網路、數位簽章、互動式證明系統來進行發起零知識證明與驗證交易。每一個網路節點向網路進行廣播交易，這些廣播出來的交易在經過礦工(在網路線上的電腦)的驗證後，礦工用自己的工作證明結果來表達確認，確認後的交易會被打包到資料塊中，資料塊會串起來形成連續的資料塊鏈。中本聰本人設計了第一版的比特幣挖礦程式，這一程式隨後被開發為廣泛使用的第一代挖礦軟體 Bitcoin,這一代軟體從 2009 年到 2010 年中旬都比較流行。每一個比特幣的節點都會收集所有尚未確認的交易，並將其歸集到一個資料塊中，礦工節點會附加一個隨機調整數，並計算前一個資料塊的 SHA-256 雜湊運算值。挖礦節點不斷重複進行嘗試，直到它找到的隨機調整數使得產生的雜湊值低於某個特定的目標。由於雜湊運算是不可逆的，尋找到符合要求的隨機調整數非常困難，需要一個可以預計總次數的不斷試錯過程。這時，工作量證明機制就發揮作用了。當一個節點找到了符合要求的解，那麼它就可以向全網廣播自己的結果。其他節點就可以接收這個新解出來的資料塊，並檢驗其是否符合規則。如果其他節點通過計算雜湊值發現確實滿足要求（比特幣要求的運算目標），那麼該資料塊有效，其他的節點就會接受該資料塊。

比特幣對等網路將所有的交易歷史都儲存在區塊鏈中，比特幣交易就是在區塊鏈帳單上「記帳」，通常它由比特幣用戶端協助完成。付款方需要對交易進行數位簽章，證明其認可該交易。比特幣會被記錄在收款方的位址上，交易無需收款方參與，收款方可以不線上，甚至不存在。交易的資金來源稱為「輸入」，資金去向稱為「輸出」。如有輸入，輸入必須大於等於輸出，輸入大於輸出的部分即為交易手續費。礦工產出交易沒有輸入，只有輸出，除礦工產出交易外，一個輸入必然是另一筆交易的一個輸出。一個輸出沒有成為另一筆交易的輸入時，它是「未花費的」，也就是「帳戶餘額」。收錄此交易的區段被廣播後，此交易就有了「1 個確認」。礦工們平均每 10 分鐘產生一個區段，每一個新區段的誕生會使此交易的確認數加 1。當確認數達到 6 時，通常這筆交易被認為比較安全、難以逆轉。[ii]

## 那麼比特幣到底是不是貨幣呢？

我國央行表示，就法律觀點而言，法償貨幣是指專屬發行權的政府機關（例如中央銀行）發行的鈔券與硬幣，並在國家法律架構下，賦予債務清償效率的貨幣。虛擬通貨並非由官方發行，不具法償效力，因此就法律觀點而言並非貨幣。

雖然就法律觀點比特幣並非貨幣，但是他還是有其市場價值，現在世界上已經有許多的交易所在交易，下圖是比特幣的價格走勢圖


Source: https://www.maicoin.com/zh-TW/charts

我們可以看到一個比特幣價格在 2012 年的時候大約在百元台幣上下，而在 2013 年以及最近都來到台幣超過 3 萬元的價位，可以看出來這已經形成了一個波動率滿高的次級市場。

**區塊鏈技術也被認為可運用在洗錢防制上。**

區塊鏈簡而言之是一個分布式的帳簿，點對點連結，可以儲存虛擬貨幣網路上交易，區塊鏈可以確認擁有者真實身分、透明性、審計性、提高銀行工作效率，運用在銀行系統上，等於是一個不可能更改的數據庫，能記錄銀行帳戶以及客戶交易訊息，因為不能被修除或是修改，可以協助金融業遵守反洗錢規定，監管部門也能隨時查證。[iii]

由以上的討論我們可以知道區塊鏈基本上就是一個分散式的帳本，具有去中心化以及不可竄改的特性，目前除了金融科技領域的應用之外，這樣的特點在我們土木工程領域上面是否也有可能利用的領域呢??這充滿了想像空間.....

參考資料

[i] https://zh.wikipedia.org/wiki/%E5%8C%BA%E5%9D%97%E9%93%BE
[ii] https://zh.wikipedia.org/wiki/%E6%AF%94%E7%89%B9%E5%B8%81
[iii] 2017-02-13 經濟日報 https://udn.com/news/story/7243/2280640