雲報專欄：區塊鏈技術之我見
-- 財團法人資訊工業策進會盛敏成處長/技術專家委員會委員

當人們提到Fintech時，事實上是指在比特幣(Bitcoin)背後的區塊鏈(Block chain)技術。對此，已經有許多專家預言區塊鏈技術將會帶來比互聯網(Internet)技術更大的影響。其主要目的並不是要取代貨幣或成為電子貨幣；事實上，它是設計來去除所有可信賴的第三方(Trustable 3rd Party)。區塊鏈是一個 P2P 方法來建立的分散式的共享帳本系統，使用此系統架構之概念為，讓所有參加者共享帳本的複本，並建立一套在交易有效的條件下，使用者同意變更帳本資訊的程序（即讓所有使用者達到共識）。由於任何人可以透過公開帳本檢查任何已進行之交易，故此種方法不需要中央機構集中式管理總帳，最終能夠去除一切中間人，包含：政府、銀行、公證單位、簽證會計師與貨幣。此系統能夠以可程式化與開放的形式，為幾乎所有的交易行為提供一個完整而忠實的記錄，能夠更有效、透明的紀錄交易訊息，並有充分的彈性支援創新的交易需求。

Fintech 是這二年來，台灣社會與金融界最熱門的技術名詞了。而當人們提到 Fintech 時，事實上是指在比特幣(Bitcoin)背後的區塊鏈(Block chain)技術。

對於區塊鏈技術，已經有許多專家預言區塊鏈技術將會帶來比互聯網(Internet)技術更大的影響。如同互聯網是許多技術堆疊而成的，區塊鏈也是由一些成熟的技術整合而成，是既存技術的新整合應用。這些技術有：① Distributed System, ② P2P network, ③ Hash Functions, ④ Public-Private key cryptography, ⑤ Cryptographic signature, ⑥ Elliptic curve cryptography。 由於這些技術模組是以耦合的方式整合，且都有可調整改善的空間，這使得區塊鏈成為一個開放且有無限可能的技術堆疊。

區塊鏈的主要目的並不是要取代貨幣或成為電子貨幣。事實上，它是設計來去除所有可信賴的第三方(Trustable 3rd Party)，當然也包含貨幣。區塊鏈是一個 P2P 方法來建立的分散式的共享帳本系統，其中以匿名的方式記錄了所有交易者在系統上的交易訊息，如 Alice 付 Robert, $B 1.25。在此系統中，所有的交易記錄都是加了時間戳記的，且一旦記錄就無法被更改；並且此平台提供了通知交易者的機制：一個交易發生，相關使用者就會得到通知。通過上述技術的整合，這個平台已經在 7 年間(2009 迄今)證明技術上可行，並足以承擔可能的駭客攻擊，能夠擔任記錄所有可能的交易行為的可信任平台。所以「經濟學人」就曾專文認

定區塊鏈是：Trust Machine。它可以為其平台上所發生的交易行為提供一個“Shared single source of truth”.

人們交易從以物易物開始，進而建立可信任的第三方；如石頭、貝殼、貨幣等來促進交易的便捷性。

以現金進行交易為例：

- 以貨幣為被信任的第三方
- 交易者自負的風險控管
- 匿名的，不需要辨識的
- 分散式

時至今日，以導入信用卡或電子支付來看，則

- 需要可信任的第三方來維護帳冊與清算
- 流程變複雜
- 風險由 3rd Party 控管
- 每一個步驟都產生成本與費用

為解決複雜流程的需求，資訊技術早就導入相關的系統流程中。並主要以兩個方向影響支付系統：① 從紙本式簿記方式轉為電子化紀錄，提昇交易處理速度，並降低作業風險；② 促成低成本之創新支付技術的發展，如行動支付。然而新技術的運用，並未改變支付系統階層式的基本架構，現代支付系統主要架構

是透過集中式的中央總帳管理，並透過存款，由擔任結清算的中央機構完成帳務簿記與清算。為了防範其中舞弊的風險，就產生更多的成本：巨大的基礎設施、複雜的法規與僵化之系統。而此進展仍與最原始之 P2P 現金交易行為之便捷性有著極大之距離。這也是悠遊卡等電子支付，一直未能導入夜市交易之主要原因之一。

使用區塊鏈建立的分散式共享帳本系統架構之概念為，讓所有參加者共享帳本的複本，並建立一套在交易有效的條件下，使用者同意變更帳本資訊的程序(即讓所有使用者達到共識)。由於任何人可以透過公開帳本檢查任何已進行之交易，故此種方法不需要中央機構集中式管理總帳。最終能夠去除一切中間人，包含：政府、銀行、公證單位、簽證會計師與貨幣。

或許去中間化的結果不一定發生；但區塊鏈技術發展出來的分散式總帳的潛在衝擊或許較支付系統本身更加廣泛。目前大多數的金融資產，例如放款、債券、股票及衍生性商品，現在只以電子形式存在，意謂金融體系本身已經是一組數位紀錄。這些紀錄目前存放於一個集中式的層級式架構下（亦即個人帳戶的紀錄集中儲存於其往來銀行，而銀行則在中央銀行集中開立準備金帳戶），但金融體系現行的基礎設施未來有可能逐漸被各種分散式帳本系統所取代。

此外由於各項技術，如 IOT，的快速進展，讓非人物件的自主交易，變得必然。例如自駕車輛，將可能於行駛途中，將優先路權以交易的方式與其他車輛進

行交易。或者無人機拍攝的資訊，也將可以以訊息交付的方式，向訂閱者進行安全而可信任交易。而此類的交易需求，都是金融體系在現行的支付系統架構下，難以因應的。而區塊鏈技術就提供了滿足這些需求的可能，因為在分散式帳本中，其上登載的數值是可細分的（可分成 100M 份）、可程式的。它能夠代表：比特幣、歐元、股份、能源（KW）、石油或者是投票的可否。

總之，以區塊鏈技術建立的分散式的共享帳本系統，能夠以可程式化與開放的形式，為幾乎所有的交易行為提供一個完整而忠實的記錄。較諸現有的交易帳務系統，區塊鏈技術誠然提供了一個更直觀的實現（Realization）。所以專家們都認定區塊鏈技術能夠更有效、透明的紀錄交易訊息，並有充分的彈性支援創新的交易需求。