比特幣簡介

中壢高商 王建岳

比特幣（Bitcoin）是一種電子虛擬貨幣，不過不像網路遊戲中的虛擬貨幣，而是一種生產與儲存在 P2P 網路系統中的虛擬貨幣，發行單位不像網路遊戲中的發行公司或實體貨幣有法律地位的中央銀行，比特幣的發行與儲存是一種分散式系統，在網路上的眾多節點擁有、交易與生產比特幣的權利。

比特幣的起源：

哈耶克（Friedrich von Hayek1899~1992）提出既然自由市場最具競爭力，那貨幣的發行為何不能開放競爭呢？弗德理曼（Hilton Friedman1912~2006）提出可以用數學及資訊技術達成自由發行貨幣的理想，不再被各國央行所管制，或者是說貨幣的發行不再被各國央行上下其手。2008.11.1 一個自稱是中本聰[註一]的人，發表一篇論文：「比特幣：一種點對點的現金支付系統」，說明了電子貨幣的新構想，透過哈爾芬尼的建議，2009.1.3 中本聰發表了第一個比特幣(bitcoin)的客戶端程式。哈爾芬尼也是比特幣的第一個礦工。

一個貨幣系統的建立必須建立在許多工作與條件上，發行、儲存、交易、安全、偽造、確認等都是問題，比特幣在一個 P2P 的分散式網路上那問題的就要透過一連串加密、解密、雜湊的演算法中解決。

比特幣的產生：

首先是發行，每一個比特幣的發行是被命名為採礦，像是傳統金幣一樣。但是這個採礦的過程是經由電腦一堆數學運算，幣值的價值是建構在運算的工作上，電腦運算的難度會自動調節增加，最初的四年發行 10,500,000 個比特幣，這個數字每四年減半，最終的數額會停留在 21000000 個比特幣。

它的運算過程是，網路節點會蒐集尚未確認的交易紀錄打包為一個數據塊，加上以前所產生比特幣的數據塊結合為一個新的數據塊，節點隨機產生的一個調整數，與這個數據塊去進行雜湊運算（Hash Function），去達成一個設定好的目標值，若是達成了則可以在比特幣網路上公佈，經 6 個節點確認後，比特幣產生了。

目前一般家庭電腦的運算能力估計一年可獲得 0.018 個比特幣，一部 30 萬元的電腦一天大約可以挖得 3.5 個比特幣，而且難度會愈來愈高。

比特幣一開始就被設定在不想像現實世界中實體貨幣一樣，各國央行可以大量發行貨幣以達成其經濟目的，造成貨幣的通貨膨脹，所以比特幣的最大量訂在 2140 年 21,000,000 個上。

比特幣的交易：

比特幣的交易使用了公開密鑰系統。當錢幣從 A 付給 B 時，A 將 B 的公鑰加密比特幣，然後這個比特幣又被 A 用私鑰來加密以確認來自於 A。當 B 利用 B 的私鑰解密，B 就擁有這個

比特幣並且可以使用，而 A 就不可能再次使用了，因為所有的交易記錄以被全體網路電腦收錄維護。在每筆交易前，錢幣的有效性都必須經過檢驗確認。

比特幣的安全性：

比特幣的安全性是建構在目前電腦的計算能力在某個能力以下，需要運算一定的時間才能解決，所有交易紀錄不能被篡改，如果篡改，則篡改電腦的運算能力必須比其餘比特幣系統中更強才行。

比特幣的儲存：

任何人都可以下載比特幣（bitcoin.org）的錢包安裝在電腦裡，系統會建立一個比特幣的地址，只要告訴他人這個地址，那別人或你自己就可進行比特幣的交換。

比特幣的現況：

在剛開始，比特幣幾乎一文不值，1 美元平均能夠買到 1309.03 個比特幣，比特幣價格在 2014 年 1 月時在 Mt. Gox 交易所收盤報價 814.7 美元，並可以透過 Mt. Gox 交易所換成現金。除此之外還有幾家規模較大的交易所，能夠進行比特幣兌換和交易。目前有很多商家接受比特幣，例如豪生連鎖酒店（Howard Johnson）和 BitElectronics 消費電子產品商店。2013 年 10 月，全世界首臺比特幣 ATM 在加拿大溫哥華出現，機器外觀與傳統 ATM 類似，它可以接受紙幣，並加快了在網上可能要幾天時間的用戶身份驗證過程。

比特幣的問題：

比特幣因為固定發行量所以不會造成通貨膨脹，但是有可能會通貨緊縮。由於大量買家的炒作，目前比特幣的幣值起伏極大。

比特幣在不同國家的法律定位不清，2013 年 6 月底德國財政部認定比特幣為“記賬單位”，這意味著比特幣在德國已被視為合法貨幣，並且可以用來交稅和從事貿易活動。韓國金融當局 2013 年 12 月宣佈比特幣缺乏穩定性，因此並不擁有“固有價值”。中國央行於 2013 年 12 月，在通知中稱比特幣不是貨幣，只是一種虛擬商品，金融機構不得進行比特幣相關的業務。

比特幣的支付具有匿名性，因此對於不想讓自己買什麼東西曝光的人來說是一個很用的工具，因此曾報導有不法分子利用比特幣來購買毒品和武器等非法商品。

比特幣未來：

2013.9.6 美聯儲主席伯南克在寫給參議院國土安全和政府事務委員會的信件中提到比特幣，「比特幣和其它虛擬貨幣，如同任何線上支付體系一樣，或許具有長期的承諾，也能夠某一天促進更快速、更安全和更高效的支付體系，然而，在執法和監管相關事宜上也伴隨風險，美聯儲沒有權力直接監管虛擬貨幣，但還是會監控該領域的發展。」比特幣透過電腦網路及電腦運算技術達成一種新時代貨幣的觀念，擁有完全匿名、交易無需成本、不屬於任何國家、

不受地域限制等使用新概念，不管比特幣是否最後成為合法且大量運用的貨幣，這樣的技術與概念的實現可能在未來的世界會全然進入我們的生活中，可能不是比特幣，但比特幣在貨幣歷史中必然也是一個重要的里程碑。

註一：

中本聰在網路上是一個神秘的人，連性別都是無法確認，不過資訊專家泰德尼爾森（Ted Nelson）曾在 Youtube 上爆料，中本聰是京都大學的數學教授望月新一，望月新一 16 歲就進入普林斯頓大學，22 歲讀完博士，32 歲就進入京都大學。尼爾林的證據是，一是望月新一夠聰明，他常獨立工作，沒有與他人合作，常發表論文，讓其他人討論，另外，他研究的領域就是比特幣的數學演算法。