網路安全技術與比特幣

賴昭正
前清大化學系教授、系主任、所長；合創科學月刊

去年（2017 年）的世界一大新聞是：比特幣（bitcoin）從年初的不到美金 1000 元，在 12 月初暴跳到幾乎美金 20,000 元，最後以 16,500 元左右收盤！這一沒有任何政府做後盾的貨幣，如雲霄飛車的升降，實在很難令人相信人類的經濟活動是理性的（註一）。雖曾看過些比特幣文章，但除了一些名詞外，可以說什麼都沒學到；難道它真有什麼特別的技術讓它值這麼多錢嗎？此一新聞突然讓筆者再次對比特幣感到興趣。作為一位喜好科普的科學家（註二），當然心裡癢癢的，也想寫一篇比較深入點的技術性比特幣文章。底下便是筆者猛 K 後的心得報導，希望在這裡與讀者分享。

密碼學

資訊在網路上的傳送，最重要的當然是需要能保密。所以我們在這裡先談一談網路上的保密是如何達成的。保密當然並不是網路出現後才有的——早在公元前 2000 年就有保密的記載；二次世界大戰之聯軍所以能夠打敗德國，事實上可能還得歸功於解碼的成功：使得聯軍對德軍的一切行動瞭若指掌。

保密是透過一定的規則將原來的資料改成無法理解的文字組合，在密碼學裡我們稱此一過程為「加（密）碼」（encryption）。例如

I Love Science 透過「加碼函數」變成 J3Mpwd5Tdjdodf

要想得回原來的信息，我們當然需要知加碼規則才能「解（密）碼」（decryption）。全世界有上億人口使用網路，因此每個團體都使用自己的密碼規則是不實際的。通用的「密碼函數」只有數種，因此除了加密外，還需加鎖。如此則雖然你知道我所使用的加密規則，但沒有我特別製造的鑰匙，你還是無法打開我加密後之資料的。

如果用來開鎖的鑰匙與加鎖的鑰匙相同，我們稱之為「對稱加密」（symmetric encryption），其鑰匙稱為「（對稱）鑰匙」；如果不一樣，則稱之為「不對稱加密」（asymmetric encryption）：自己保有的鑰匙稱為「私鑰」（private key），發給大家的鑰匙則稱為「公鑰」（public key）。「私鑰」與「公鑰」是成對的：用「私鑰」鎖住的東西只能用其相對之「公鑰」來開。反之亦然：用「公鑰」鎖住的東西只能用其相對之「私鑰」來開。

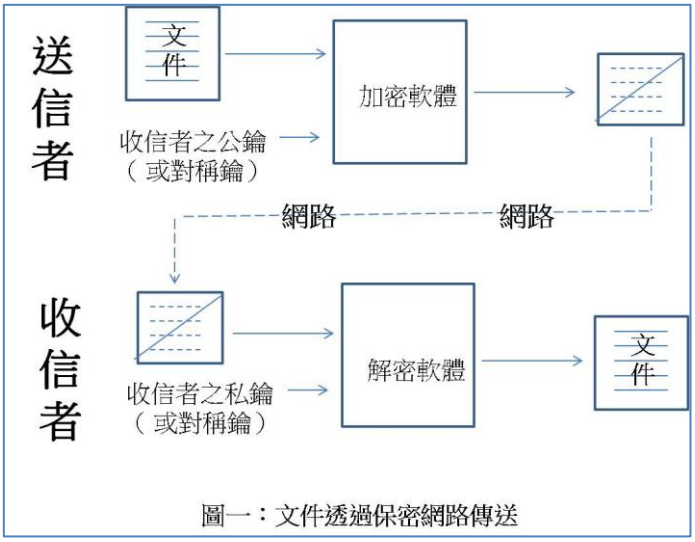
從上面的闡釋看來, 加密及加鎖好像是先後使用的兩碼事；但事實上它們大部分都是同時使用上的：

（資料 + 鑰匙）→（加密碼軟體）→（diwlae;ajp2$）

（diwlae;ajp2$ +鑰匙）→（解密碼軟體）→（資料）

網路保密傳送

我們現在就用一個實際的例子來說明它們的使用方法：你在台灣銀行有戶頭，想到台灣銀行網頁轉一些錢到另外一個銀行的戶頭。當你上台灣銀行網頁時，你第一個注意到的應是網頁前的「https: 」 ：與一般網頁前之「 http: 」多的 s 是告訴你這是安全網站，一切的資訊來往均需加密碼及加鎖保護。



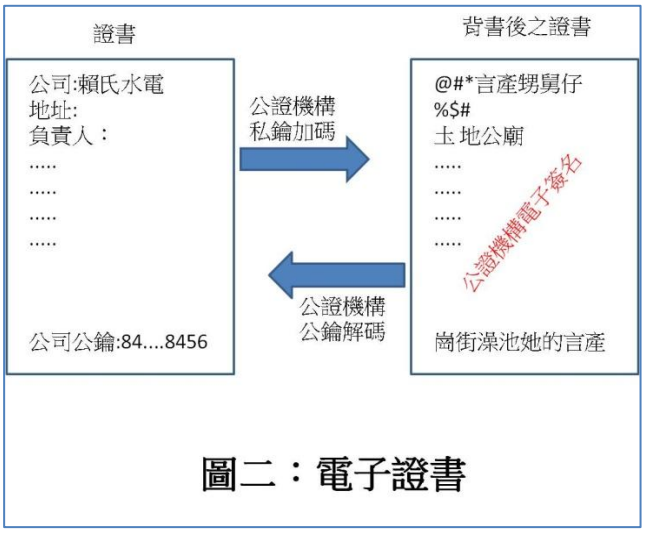
圖一：文件透過保密網路傳送

在經過一番「握手」談如何交換資訊後，台灣銀行網頁就將它的「公鑰」寄給你，要你用同意後之加碼規則及它的公鑰、將你的電腦軟體製造之「對稱鑰匙」及其它資料加密及加鎖寄給它：此後你們的資訊來往就全使用這把「對稱鑰匙」來加密及加鎖（見圖一）。讀者可以自己分析一下：在上述的資訊交換中，萬一有人偷偷攔劫了，因為缺少正確的鑰匙，他還是沒法得到任何保密過的資訊！

「對稱鑰匙」在交易完後就丟掉，但該「公鑰」是永遠屬於台灣銀行的。這就產生了兩個問題：（1）我怎麼知道它確是屬於台灣銀行的，而沒有被調包過？（2）我怎麼知道「台灣銀行」確是真正的台灣銀行？這就涉及到網路公證機關（certificate authority, 簡稱 CA）：它們負責頒發證書（certificate）及（公、私）鑰匙。網路上的鑰匙只是一連串的數字而已；越長的數字當然越難破解：一般的「對稱鑰匙」大概只有 128 位元（bit），「不對稱加密」的「鑰匙」長度則常高達 2048 位元！

電子證書

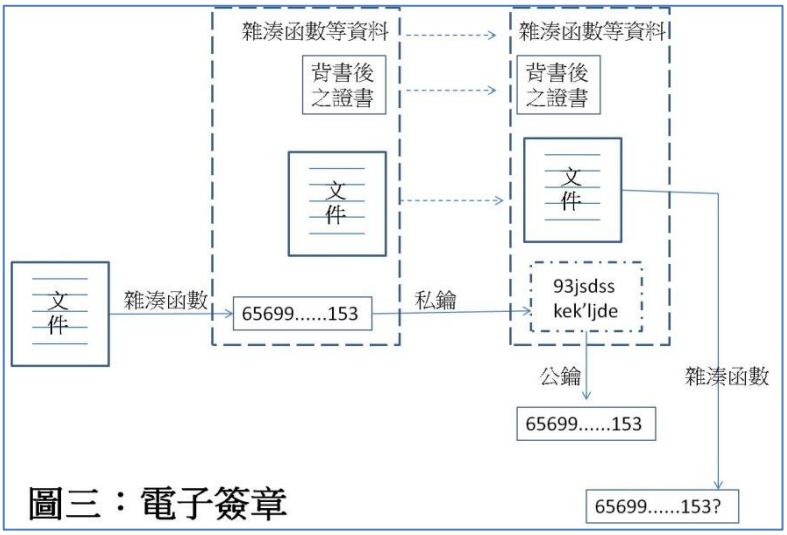
當你跟台灣銀行正式交易前，台灣銀行將傳給你一張某個網路公證機關「簽名」過的證書，來證明（1）它確是台灣銀行；（2）它給你的「公鑰」也是該網路公證機關發給台灣銀行的。公證機關如何「簽名」呢？就是用它獨特的「私鑰」加碼（見圖二），而你也只能用它的獨特「公鑰」來解碼！因為該網路公證機關的「公鑰」，並不是台灣銀行給的，因此後者實在是很難作弊。這些網路公證機關的資料及「公鑰」事實上



圖二：電子證書

均早就存在於你的網路瀏覽器內！因此如果你的電腦或網路瀏覽器被綁架了，其後果將是不堪想像的！

電子簽名



圖三：電子簽章

因為只有你有獨特的「私鑰」，用它來加碼，就像在文件上用你獨特的筆跡簽名一樣，稱為電子簽章（digital signature）。如是的電子簽章一般是具有法律效力的！因此除了上述之用於頒發網路之證書外，它也適用於民間之合約等的簽定。合約須保存，因此在實際的操作上可能與上網有點不同（見圖三）：需要簽名之正式合約或文件一般先經過雜湊函數改成固定長度之「雜湊」（hash）數。雜湊之長短決定安全的程度。理想的雜湊函數（hash function）必須具有：（1）不同的輸入——即使只差一個符號或空間——一定產生不同的雜湊（值）；及（2）不可能由雜湊值反推出原來之輸入資料。

將合約或文件改成「雜湊」後，簽名者就用自己獨有的「私鑰」加碼，然後將該加碼、合約、背書後之證書、及其他資料透過網路傳給對方。在此筆者得聲明一下：因不是專攻電子簽章，故細節上可能跟實際操作有點出入（例如傳了那些資料）。但筆者認為這些細節是不重要的，因此也不擬深究。就像 x 總統一樣，雖然只有年薪百萬（台幣）的固定收入，但當了 4 年總統後，卻是家財億貫（美金）；因此結論除了是「貪污」外，筆者實在想不出其他答案。至於如何貪污等細節，則因人而異，除了寫 x 總統的傳記外，在討論整個國家的政治環境時，實在沒有深究之必要！

收到合約者可以（1）用「背書後之證書」確定簽名者之身份；（2）用簽名者之公鑰解碼，得到合約之雜湊值；（3）將收到的合約透過同一雜湊函數取得另一雜湊值。如果兩個雜湊值完全符合，則因雜湊值的獨特性，可以毫無懷疑地相信合約的真實性——從未被有意或無意地偷偷修改過！

比特幣交易

比特幣至少有五點非常不同於一般貨幣之處：（1）它沒有任何國家、團體、或實物當後盾，而是建基於彼此間之互相信任及遊戲規則（protocol），如有爭議則以多數（51%以上）來決定；（2）它沒有任何一個特定的機構和團體在管理任何人的賬戶和買賣；（2）它沒有任何實體貨幣，因此只能在網路上交易；（4）它的所有交易記錄都是不

記名而且公開的；（5）它不能像政府一樣隨便發行鈔票（比特幣），而是需要靠「礦工」開採出來。因為全在網路上交易，上面所談到的一些網路保安問題，在這裡全部用上了！

要想使用比特幣，首先需要有個稱為「地址」（address）的帳號，及其獨特的「公、私鑰」。這個賬號雖然可以自己設，但較簡單的方法當然是破費到比特幣網站開個「錢包」（wallet）戶頭：它們可以提供一條龍的服務，如幫助你設定好幾個地址做買賣，以減少被盯上的可能性。當你（地址 a）要付錢給老賴（地址 p）時，你就將所有資料（你的比特幣來源、付給誰等）以該地址獨特的私鑰加碼，廣播到所有的比特幣網點去。這些網點都可以用你的公鑰解碼，與他們手上之公開賬本比較，看看你是否真的有那些錢。當他們確定一切都沒有錯誤後，這筆交易就進入等待開發之「礦池」內。

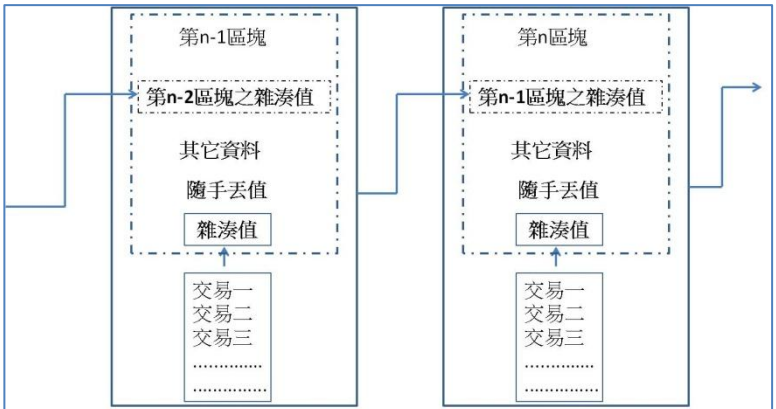
比特幣開礦

當礦池內有足夠之交易筆數後，礦工們便開始其開採的工作了：（1）收集某些交易，透過雜湊函數將它們改成雜湊（比特幣使用稱為 SHA-256 的雜湊函數，其輸出之雜湊長度為 256 位元）；（2）將此一雜湊加上一稱為「隨手丟」（nonce）之自選數字（256 位元數字），再次透過雜湊函數得到第二個雜湊值；（3）如果這第二個雜湊值小於當時之「目標值」時，就算挖礦成功，可得到一筆「新印製」之比特幣獎金；（4）如果這第二個雜湊值大於當時之「目標值」，則得改變「隨手丟」之值，繼續嘗試！

筆者當初以為挖礦是一個大數學問題，將來的數學家一定大有出路；但現在了解後才發現它根本是一個硬碰硬的瞎猜方法！它要的不是人的腦力，而是電腦的快速運算能力！隨著洛陽紙貴的大爆漲，想當礦工的的人當然越來越多（下載一個礦工軟體就可以）！但這種瞎猜卻絕不是一台電腦就可以達成的，而是需要成百上千台聯合起來工作的！其所耗的電力當然非常可觀：據荷蘭比特幣分析師迪非雷斯（A. de Vries）估計，即使使用效率最高的計算機，全世界用來開礦的電力可能已高達美國全國用電量的 0.7%（註三）！更糟的是 58%的大開礦機均設在大量使用燃煤來發電的中國邊疆區域（註四）！

比特幣區塊鏈

一旦開礦成功，礦工馬上將其結果廣播到所有的網點，經大家（51%以上）確認後，那些交易及其雜湊值、「隨手丟」值、上一區塊之雜湊值、以及其它資料等，就可各自下載到每個礦工之最新的區塊內，行成如圖四之「區塊鏈」（blockchain）。下一個用來決定開礦成功與否的「目標值」也依特定的數學模式跟著產生出現：目標值越大，越



圖四：區塊鏈

容易成功開礦；原則上他們希望每 10 分鐘能成功地開一個礦，每兩週調整一次「難度」指數（difficulty, 難度指數不是「目標值」本身，而是用來決定目標值大小的指數）。「區塊鏈」就是公開的賬本，它記載了所有曾經發生過的交易。因為「區塊鏈」廣泛地使用雜湊，任何修改均將牽一髮而動全身，馬上會被發現，因此「區塊鏈」將永遠只有一個大家公認的版本！

因為所有的交易都清清楚楚地記錄在區塊鏈裡，因此你的銀行（地址 a）裡有多少錢，大家都是清清楚楚的；因為沒有人在意你到底是誰（黑社會趨之若狂），所以不需要電子證書。可是你一旦丟掉該地址之私鑰，那你就可以跟那裡的比特幣說拜拜了：那些比特幣將永遠只是可望不可即（永遠沒有辦法拿出來交易）！

比特幣結論

上述的闡釋只是非常理想化地說明了比特幣的運作原理，實際的操作因網路的資訊傳送不是瞬間，而是有一定的速率，因此複雜多了！例如你的交易額不大，因此被礦工從礦池中挑出來的機會將較小（因獎金常是用交易額之百分比來決定的），怎麼辦呢？又如兩個礦工幾乎同時挖到了礦怎麼辦？我剛寄出的交易還沒被確認，我又寄出了另一筆交易怎麼辦？..... 這些實際運作上的細節，比特幣的白皮書裡當然都有規定——但願本文之基礎能幫助有興趣的讀者繼續自行做進一步的深入探討。儘管如此，因為比特幣之「美」（價值）實在連「情人眼裡出西施」都配不上，筆者認為它完全是一種賭博投機，所以根本不值得深究！有人說它是世界經濟崩潰的避風港，但就在筆者完稿的今天（2018 年 2 月 4 日），美國道瓊指數下降了有史以來的最多點數（-1175 點，-4.60%），比特幣竟然也不後人，當天也下降了 15%至不到美金 7,000 元！！！

事實上如果開礦的「工資」太低或者電價太貴，而使得礦工們開始罷工或轉行，那麼將沒有足夠的人力去做驗證的工作，比特幣可能就必須關門大吉了。還有，如果開礦們因要降低成本而合作起來分享資源（事實上已經開始了），當他們人數過半時，原則上要聯合起來偷偷修改區塊鏈（需要大量的電力）就不再是天方夜譚了！.....比特幣的基礎是建立在人們彼此間的互信，你相信人性本善嗎？

********** 註 **********

註一：「經濟是科學嗎」：科學月刊 2014 年 5 月號。

註二：「我愛科學」：本書是收集筆者自 1970 年元月起在科學月刊及少數其它雜誌所發表之文章編輯而成；由華騰文化有限公司2017年12月出版。

註三：比較保守的估計認為只有 0.1%而已。

註四：筆者在科學月刊2013年7月號發表「電動汽車值得發展嗎」一文後，行政院環境保護署空氣保護及噪音管制處處長謝燕儒即投稿台灣立報謂：將污染轉到鄉下，.... 發電廠容易集中管制，可嚴格控制污染要求。話是不錯，可是實際上呢？嚴格控制要花錢，住在鄉下的人數少，教育水準一般也較低，聲音也因此較弱，政府會自動地關切嗎？誰會為他們說話呢？為什麼（高科技）開礦公司「喜歡」設在人煙稀少、

大量使用煤碳發電之中國邊疆區域呢？又例如經濟日報去年11月18日報導：「彰化縣環保局長江培根指出，台化自2008年1月以來，長期違反環評法第17條規定，燃燒品質不符合標準的生煤，直接所得利益龐大，環保局多次要求台化針對M22製程歷年發電、售電、獲利等提供詳細資料，但台化始終沒有正面回應。」不在鄉下的廠都這麼難「管」，更甭談鄉下廠了。筆者之其它回應，見科學月刊2014年3月號或「我愛科學」。（補註）2021年3月2日美國CNBC報導謂：僅內蒙古就佔全球所有比特幣開採量的8％左右，超過全美國的7.2％。內蒙古地區計劃禁止新的加密貨幣採礦項目，並關閉現有活動，以減少能源消耗運營。