虛擬貨幣值得信賴嗎？由「分散式共識」談起

◆ 社團法人台灣 E 化資安分析管理協會、元智大學資訊學院 — 陳昱圻

近年越來越多人願意相信並使用比特幣，不過這種看不到、摸不到，更沒有如同真鈔般防偽特徵的虛擬貨幣，是否值得信賴？

比特幣與區塊鏈的基本概念

伴隨比特幣的名詞便是區塊鏈，區塊鏈的概念是由中本聰（Satoshi Nakamoto 筆名）於發表比特幣時所提及的。在區塊鏈運作上最重要的一點，**就是一群人對同一件事物有同步的共識**。就比特幣來說，所有交易與金錢持有都是虛擬資料，要使用就必須有非常多的認證才能證明其值得信賴，而這份證明資料就是由區塊鏈支撐。由各資料區塊按照時序串成鏈，形成完整的證明。這些單位在區塊鏈網路上被稱之為節點。這項技術的特色如下：首先其所有運算結果都是公開透明的，也因此並沒

有第三方管理，取而代之的是所有節點的共同監督；另外上面的資料皆不可被修改，以保證區塊鏈的安全性；最後是匿名性，所有使用者皆可使用，而且不需要用個人資料來公開驗證，因此所有交易皆可匿名執行。

比特幣從挖礦中誕生

比特幣運行也倚賴工作證明（Proof of Work, PoW），概念上的區塊鏈如圖 1 表示。PoW 就是一種「分散式共識」，該共識由節點完成，且確保所有交易以及區塊鏈上所有內容皆不容竄改，而這些維運工作就是節點的工作。

在 PoW 上，節點們互相競爭，除維護工作外也要負責解難題，第一個解出難題者則可以獲得獎勵。在比特幣的環境，解出節點答案的動作稱為挖礦，挖礦者稱為礦工。要解決的問題如同圖 1，找出隨機數並滿足區塊成立的條件。從這裡我們可以得知比特幣的幣從挖礦誕生，而所有交易就由這些節點來確保正確性。確認這點並非難事，因為這裡的帳本都是公開的，所有節點身上都有這份帳本而且同步並持續更新。

有趣的是，我們能輕易地追尋我們所持有的比特幣可能是何時誕生的，因為交易地點是虛擬的（在區塊鏈網路上）。

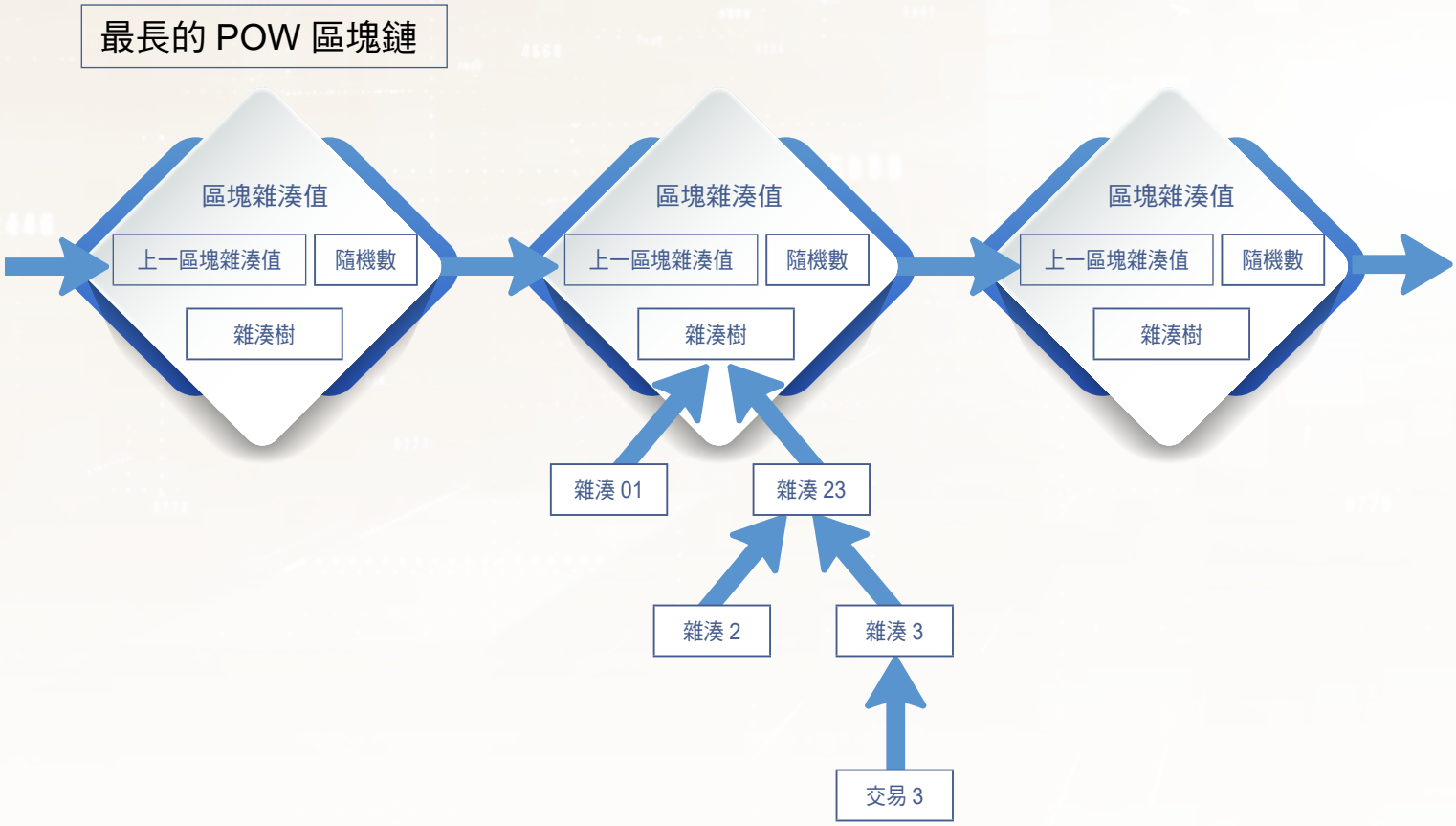
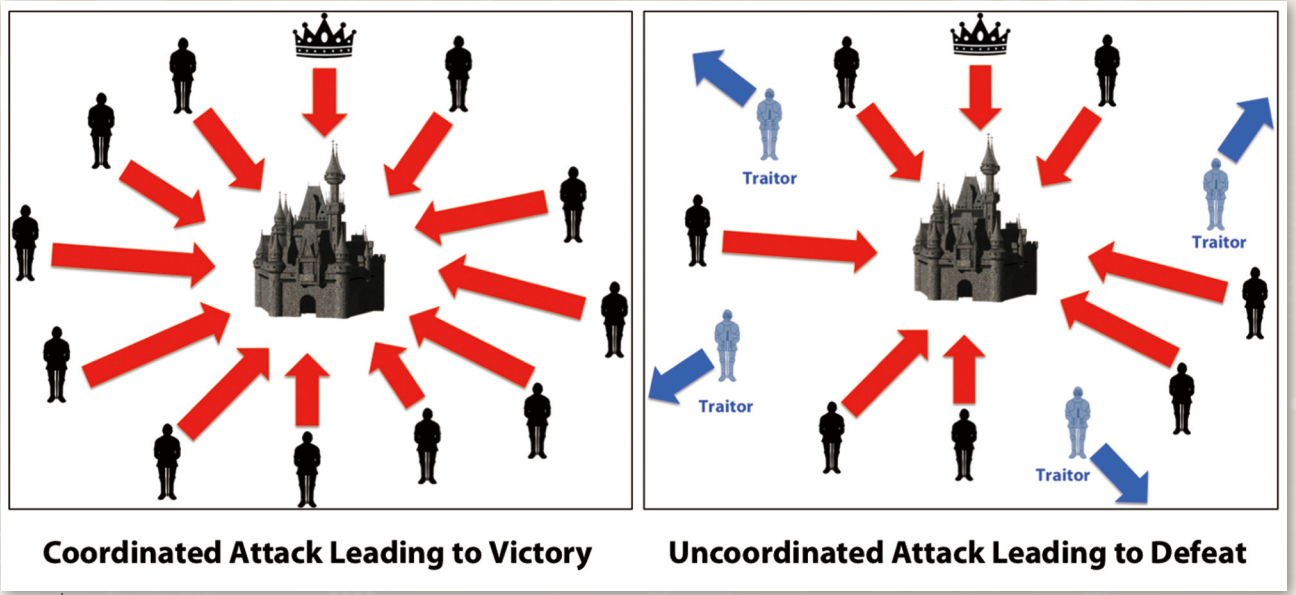


圖 1　中本聰提出的區塊鏈概念之區塊標頭內容，包含前一個區塊的雜湊值、隨機數、交易壓縮後的雜湊樹等資訊



只能靠信使傳遞訊息的將軍們，如何避免叛徒影響共識，就是拜占庭問題。（Photo Credit: Paul DeCoste, https://medium.com/@paul_12056/byzantine-generals-problem-ff4bdc340e56）

重要的是確保挖礦歷程正確且能讓所有人認可，就要靠「分散式共識」。以下我們將透過簡單的例子介紹「分散式共識」概念。

分散式共識

又到了社團要選出下任新社長的時候，社員們打算開會來決定人選，但因為疫情關係，究竟要舉辦實體會議還是線上會議，社長決定先發訊息徵詢大家意見。然而有人圖謀不軌，藉由傳送錯誤訊息，讓有些人以為要實體，另些人以為要線上舉辦，進而使會議人數未過半而開不成，而要如何讓所有人對開會方式有共識，就是著名的拜占庭問題（Byzantine Problem）。[1] 然而，這作法有不小的漏洞。我們假設有壞心眼的就是社長，他將兩個選項分別傳給其他半數的人，這將導致有一半的人收到剛好過半要召開實體會議的決定，另一半則收到剛好過半要舉行線上會議的通知，最後就是選舉過程無法進行，而原社長就可以繼續連任下屆社長。

解決方式是對訊息附上各自的簽名來防止訊息竄改，也就是數位簽章，並多投幾輪票，這樣就能確認是誰在亂傳訊息了，這個方案被稱為 Dolev-Strong 協定。關於這個，我們再用以下例子比喻。

[1] 拜占庭是古代東羅馬帝國的首都，由於地域寬廣，守衛邊境的將軍們需透過信使來傳遞消息，以達成是否一起進攻或撤退的決定。在過程中，若某將軍故意拒絕合作（惡意節點），就是叛徒。將軍們需根據接收到的所有消息來決定最終作法，如何避免叛徒影響共識，就是拜占庭將軍們所需解決的問題。詳見：https://www.inside.com.tw/article/14439-blockchain-bitcoin-byzantine-node

「元宇宙」發展也需要「分散式共識」。

老師帶群小孩去玩找泥巴人遊戲，遊戲開始前老師會在部分小孩額頭上塗抹泥巴（不能讓孩子們知道自己是否被塗上泥巴）。老師會先告知本次被塗上泥巴的人數，然後要大家圍成一個圈（每個人只能看見別人額頭上有沒有泥巴，也不能進行任何溝通行為）。遊戲開始後，頭上有泥巴的小孩需退出圈外，持續到所有泥巴小孩都退出而結束。小孩們都非常聰明，若老師說此次只有 1 個泥巴小孩，當小孩發現其他人都沒有泥巴時，就會推論出自己是唯一的泥巴小孩，主動退出，然後遊戲結束。若遊戲原先設定有 2 個泥巴小孩，當某位小孩發現另一個泥巴小孩沒有站出來時，他就會推論自己也是泥巴小孩而主動退出，依此類推，就可以讓原先看不到自己的全數小孩們找到正確答案。因此，**「分散式共識」就是一種能讓在不同位置的所有人產生共識的方法**，即使在惡意者數量不夠的情況下，還得以維持大部分人的共識；而比特幣的信用度就是靠這項技術維持的。

「元宇宙」VS.「分散式共識」

不僅虛擬貨幣[2]，早在 1970 年代，就已經有「分散式共識」的需求，Dolev-Strong 協定更早在區塊鏈技術還未出現的

[2] 通常只在虛擬環境中使用，有時候也可以購買實體商品和服務。

1983 年時就提出，當初設計目的是為了使控制系統的所有電腦資料同步並取得共識。另外共識機制也可用在日常生活中的大小事，例如虛擬錢包和即時的天氣預報，只要和同步或共識有關的就能使用「分散式共識」。可想而知，「元宇宙」的發展無疑也需要這項技術作為基底，「分散式共識」可以說是當今網路時代十分重要的一項技術。

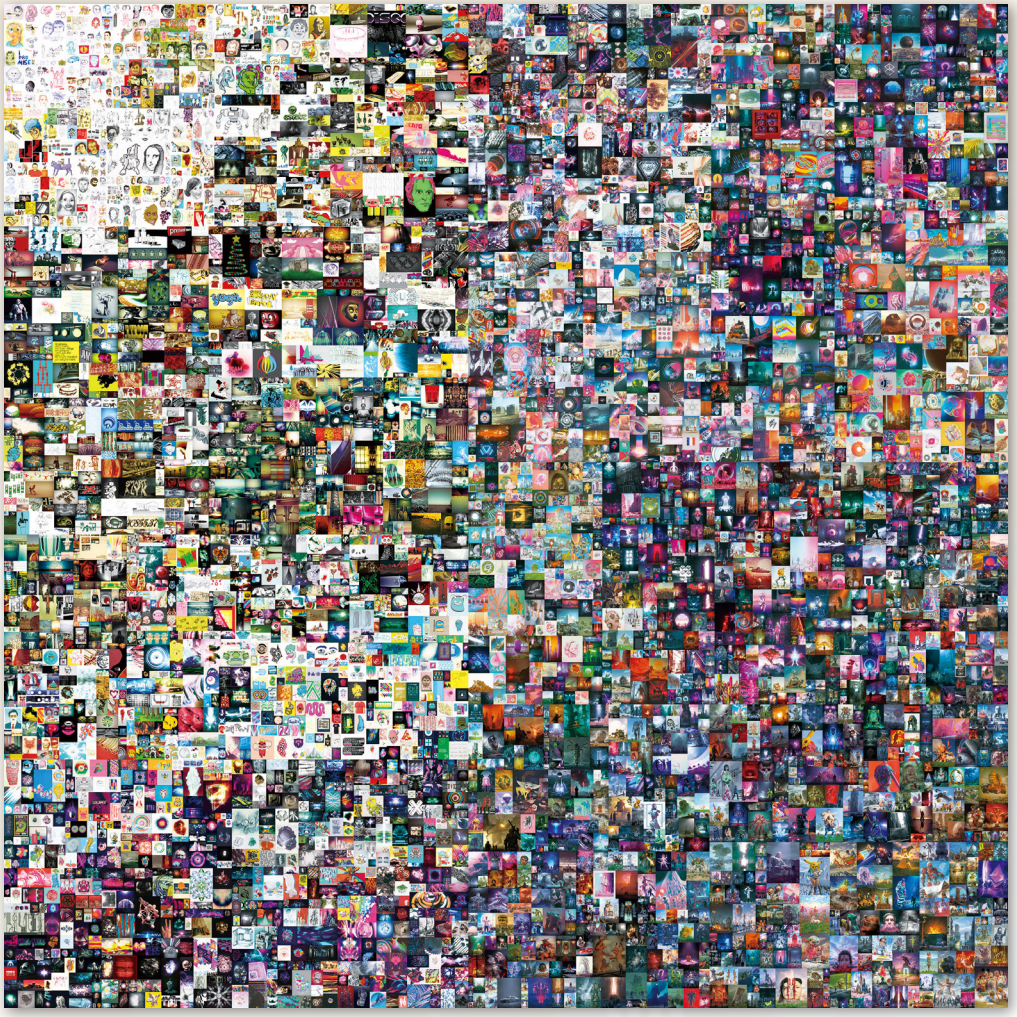
虛擬貨幣力抗貨幣波動

接著我們回到另個根本問題，既然現實生活中有貨幣，那為何還要選擇比特幣這類的貨幣存錢或交易呢？其實貨幣都有升值和貶值的時候，有些國家的貨幣並不穩定，當國家的法定貨幣波動比率比虛擬貨幣大時，該國民眾將錢換成這類虛擬貨幣反而是相對穩定。阿根廷可說是最具代表性的例子，作為通膨率榜上有名的國家，其 2021 年統計的通膨率甚至高達 40% 以上，對當地人民而言，比起政府法定貨幣，阿根廷民眾更寧可使用比特幣。

最火紅的 NFT 型態藝術品

2021 年 3 月，英國佳士得拍賣（Christie's）以 6,900 萬美元售出《Everydays: The First 5000 Days》的數位藝術品後，「非同質化代幣」（Non-Fungible

阿根廷的通膨率在 2021 年高達 40% 以上，對當地人民來說，比起政府法定貨幣更寧可使用比特幣。（Source: OECD, https://data.oecd.org/price/inflation-cpi.htm）



上圖為價值 6,900 萬美元的數位藝術品《Everydays: The First 5000 Days》，下圖為莫內親手繪製的《睡蓮池》作品，在 2021 年 5 月的蘇富比拍賣會也才以 7,035 萬美元賣出，顯示 NFT 數位藝術品價值已直逼藝術家畫作真跡。（Source: Christie's, created by Beeple, https://onlineonly.christies.com/s/beeple-first-5000-days/beeple-b-1981-1/112924; Sotheby's, created by Claude Monet, https://www.sothebys.com/en/buy/auction/2021/impressionist-modern-art-evening-sale/le-bassin-aux-nympheas-2）

Token, NFT）就躍升為虛擬貨幣的要角。該作品是彙集 Instagram 圖片的數位拼貼作品而成，而莫內親手繪製的《睡蓮池》作品，在 2021 年 5 月的蘇富比拍賣會也才以 7,035 萬美元賣出，NFT 藝術品價值直逼莫內作品。近期最火紅的 NFT 藝術品，也是目前銷售最高的 NFT 型態藝術品，是 2021 年 12 月在 NFT 平臺 Nifty Gateway 上累積銷售 9,180 萬美元天價的《Merge》作品。

我們可透過以下例子來理解其概念。小明製作的電子周刊上有自己親手電繪的精美插圖，也在同一時間被瘋傳到網路上，心理忿忿不平的小明，覺得自己繪圖這件事情應該是有所報酬的，然卻因為公開在網路上而成為免費的物品，甚至也無法認證這張圖片的作者究竟是不是小明，於是小明開始研究 NFT 以維護自己的權利。

為何 NFT 型態藝術品是無可取代？由於每張圖畫都經由特殊編碼記錄著，當他人複製該圖畫並引用時，是無法修改隱藏其後的原始編碼，因此每張圖畫都只有一個真正的持有者。舉例來說，所有人都可以在網路上查詢並複製達文西的《蒙娜麗莎的微笑》，但永遠只有一處可以持有該畫作的真跡，而它如今坐落在法國的羅浮宮內。達文西真跡畫作上擁有無法被複製的細節，猶如當時顏料成分、長年的風化裂痕等等，就像是 NFT 的特殊編碼，是獨一無二且無法仿製的，這即是 NFT 藝術品的殊勝之處。

NFT 還有一個特點是每筆交易利潤的 10%，會回饋給原創作者，因此相較於在傳統市場拍賣實體畫作，NFT 交易對於創作者會產生較大的誘惑。因此當小明將自己畫作上傳至網路平臺，隨著小明名氣越來越高，越來越多人願意購買小明的畫作，買家再度成為賣家，小明與買家皆大歡喜。

在「分散」中有「共識」，才能獲取全球民眾信賴

人為世界，分分合合，科技演進在人的世界裡當然也有著合合分分的各式發展需求。網路興起已創造出新交易模式，而若我們能在「分散」中尋找「共識」，即在不同國籍種族的人群中，都能對同件事物達到共識時，各種虛擬貨幣之網路交易就值得被長久信賴，也才能創造出更高之貨幣價值。

社團法人台灣 E 化資安分析管理協會（ESAM）