2022 年【全國科學探究競賽-這樣教我就懂】

大專/社會組 科學文章表單

文章題目： 帶你輕鬆認識通往元宇宙的鑰匙—加密貨幣的典型代表—白話入門比特幣原理、加密貨幣與元宇宙密不可分的關係

文章內容：（限 500 字~1,500 字）

元宇宙(Metaverse)的鑰匙—加密貨幣:

隨著科技越來越發達，現在絕大數人類已經跟不上科技發展的速度，「數位化」帶來兩大不可取締的優點—效率和自由度。如果要數位貨幣能滿足此兩大優點，必不可少的條件就是完備的系統,目前世界上能滿足這技術特點的就是使用了區塊鏈技術與 SHA-256 加密技術(一個完善的加密方法)的加密貨幣。另外，未來二十年沉浸式虛擬世界(元宇宙)能夠把效率和自由度實現到最大化，可是實現系統完整的元宇宙有著不可缺的兩大元素，一，是標識虛擬資產的東西—NFT，二，是虛擬世界的交易工具—加密貨幣。目前，世界上有 18,465 加密貨幣，若未來在虛擬世界真的要進行最穩定的貨幣交易，首選必定是比特幣。有鑑於其影響力，在此科學文章裡帶大家認識加密貨幣的典型代表—比特幣。

- 甚麼是比特幣? — 比特幣的誕生:

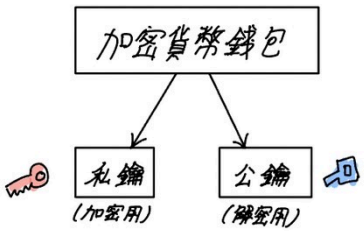
在 2008 年 10 月 31 日，「metzdowd.com」上，有一位論文著作人以假名 Satoshi Nakamoto 透過電郵郵寄方式發表了一篇論文，標題名為「Bitcoin: A Peer-to-Peer Electronic Cash System」(《比特幣：一種對等式的電子現金系統》)，論文中詳細地描述了如何建立一套去中心化的電子交易體系。2009 年 1 月 3 日，Satoshi Nakamoto 開發出首個實現了比特幣演算法的客戶端程式，並進行了首次「挖礦」，獲得了第一批的 50 個比特幣，在此，比特幣金融體系的正式誕生。比特幣是一種數位加密貨幣，於 2009 年問世。毋須銀行或中央機構作為託管資產的機構，故不會透過金融中介進行交易，所有交易記錄也不會保存在任何金融中介裡，即去中心化。而是把每一筆交易記錄和加密貨幣資產記錄在區塊鏈裡，並在點對點網路上進行交易。

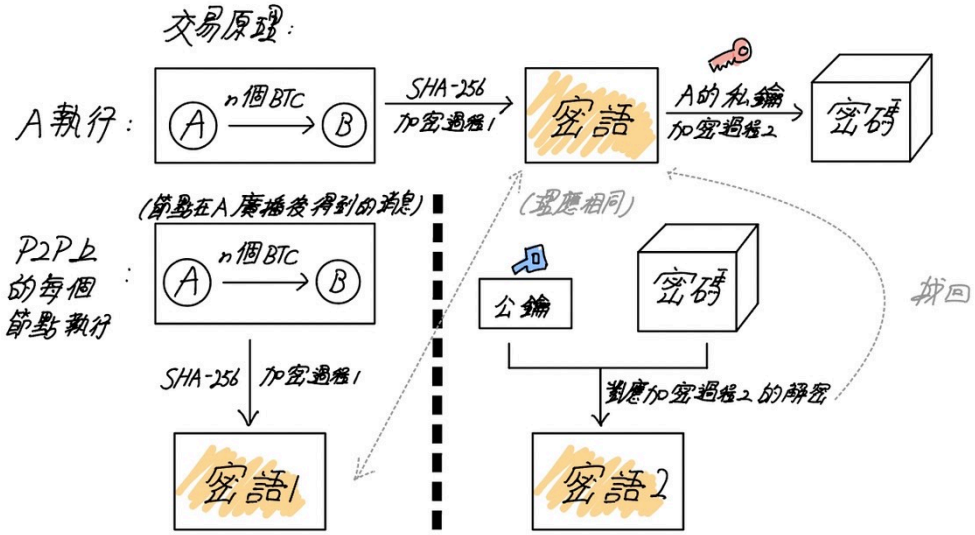
- 比特幣的產生原理—「挖礦」機制:

比特幣的產生原理就是「挖礦」，即創造新的區塊。這個獎勵機制，簡單來說，是一個完成 SHA-256 演算法解題後再經點對點網路上的多個節點驗證，驗證成功後領取獎勵的一系列過程(事實上，這套機制的步驟其實更多，但以簡馭繁，這邊只歸納並摘要了核心的三個步驟)，就可以得到一定數量的比特幣當作獎勵，這些新產生出來的比特幣是經由區塊鏈上每個區塊「發行」，在比特幣系統中，每個區塊都會允許「發行」一定數量的新比特幣。在不同的加密貨幣中，可「挖礦」的量有所不同。此外，並非所有加密貨幣都存在著獎勵機制。

- 比特幣的交易原理:

欲購買比特幣，首先要先建立一個加密貨幣錢包。可以使用電腦、手機等行動裝置下載，每一個加密貨幣錢包都儲存著一把用來加密的「私鑰」和一把解密的「公鑰」。這對「私鑰」與「公鑰」是透過非對稱加密法計算出來，「公鑰」是透過「私鑰」計算並產生出來，但「私鑰」則沒法透過「公鑰」反推算出來，確保了使用「私鑰」進行加密這項動作是安全的。交易比特幣時，系統以會將支付訊息以完善的 SHA-256 演算法加密成「密語」，確保不會有人篡改當中的支付訊息，以防別人篡改金額或收、付款方身份等，再使用付款方 A 的「私鑰」加密「密語」成為一個「密碼」，再對點對點網路進行廣播，告知點對點網路的所有節點「付款方 A 支付 n 個比特幣給收款方 B」、「付款方 A 的『公鑰』」和「密碼」這三件事。接著，點對點網路上的所有節點會對「付款方 A 支付 n 個比特幣給收款方 B」進行 SHA-256 演算，得出一個「密語 1」來。同時，利用「付款方 A 的『公鑰』」對「密碼」進行解密，得出一個「密語 2」來。利用相同的東西，弄出的東西應該是一樣，對吧?所以，當「密語 1」=「密語 2」，說明「付款方 A 支付 n 個比特幣給收款方 B」的內容不是偽造的。





密語1 = 密語2 → ✓

密語1 = 密語2 → ✗

參考資料

1. Satoshi Nakamoto. Bitcoin: A Peer-to-Peer Electronic Cash System. satoshin@gmx.com. https://bitcoin.org/bitcoin.pdf
2. SHA256 演算法原理詳解。程式前沿。 https://codertw.com/%E7%A8%8B%E5%BC%8F%E8%AA%9E%E8%A8%80/602774/
3. 什麼是區塊鏈技術？。IBM Blockchain-台灣。 https://www.ibm.com/tw-zh/topics/what-is-blockchain
4. 挖礦(數位貨幣)。維基百科。 https://zh.wikipedia.org/wiki/%E6%8C%96%E7%A4%A6_(%E6%95%B8%E4%BD%8D%E8%B2%A8%E5%B9%A3)

註：

1. 沒按照本競賽官網提供「表單」格式投稿，不予錄取。
2. 建議格式如下
   - 中文字型：微軟正黑體；英文、阿拉伯數字字型：Times New Roman
   - 字體：12pt 為原則，若有需要，圖、表及附錄內的文字、數字得略小於 12pt，不得低於 10pt
   - 字體行距，以固定行高 20 點為原則