敦品勵學 創新卓越

揚子學校財團法人雲林縣
揚子高級中等學校
Yang-Tze High School

獎　狀

高一忠班

林坤逸、林浚楷、楊博丞、蔡承峰、
賴銘傑 同學

作品名稱：加密貨幣中的數學

參加 111 學年度 揚中之”數”

發現生活中的數學競賽 榮獲**優選**

表現優異　殊堪嘉許

特頒此狀　以資鼓勵

校長 鍾月娥

中　華　民　國　一一二　年　一　月　四

１１１年揚中之“數”作品

作品名稱：加密貨幣中的數學

組員：林坤逸、林浚楷、楊博丞、
蔡承峰、賴銘傑（按座號排序）

壹、前言

一、摘要

隨著化名為中本聰（Satoshi Nakamoto）的不具名人士於 2008 年在網路上發表了比特幣的白皮書（Satoshi Nakamoto, 2008）以後，加密貨幣已在無論科技界或金融界掀起一股巨浪。而近日全球第二大的加密貨幣交易所破產之後，不禁令世人對於加密貨幣產生質疑。究竟加密貨幣是一場高度包裝的騙局，抑或是數學原理之下安全性無庸置疑的產物呢?為了瞭解以下幾點問題，我們將針對加密貨幣的數學原理進行研究。

二、研究目的

(一)、 認識加密貨幣

(二)、 了解加密貨幣的數學原理

三、研究流程

圖一、 研究流程簡圖

四、應用單元

(一)、 高二：機率（應用：互斥事件的概念、運算複雜度與時間的關係）

(二)、 高一：指數與對數（應用：控制區塊形成）

(三)、 國中：等比數列（應用：礦工的獎勵）

壹、文獻探討

一、加密貨幣（cryptocurrency）

加密貨幣，最早由中本聰（化名）提出，是「**一種允許直接從一方送到另一方，無須經手金融機構，為線上支付的點對點類型電子貨幣**」（自譯）（Satoshi Nakamoto, 2008）的虛擬貨幣。根據 Jan Lansky 博士的定義：「**加密貨幣是符合下列六個條件的系統**」（Jan Lansky, 2018）加密貨幣可以達到去中心化、利用密碼學產生新幣並紀錄交易等效果（Jan Lansky, 2018）。

二、雜湊函數（Hash function）

雜湊函數，具有唯一性和不可逆性，亦即不可能找到任兩個字串能得出相同的雜湊值，且無法從雜湊值推論出輸入字串。SHA-256 即是加密貨幣常使用的雜湊函數。一個好的雜湊函數會竭力避免碰撞（雜湊值缺乏唯一性），並使字串有微小的改變時，雜湊值卻有巨大的改變。

三、SHA-256 的數學原理

SHA-256 是由美國國家標準暨技術研究院（National Institute of Standards and Technology）研發的雜湊演算法標準，其實踐方法如下（Chen Yan Long, 2021）：

(一)、 填充（Padding）

取得來源訊息後，我們先將原有訊息補上一個 1 ，接著再把數字串連續補 0 ，值到字串長度為 512 倍數減去 64 位元。而 64 個位元則是要記錄原始資料長度。

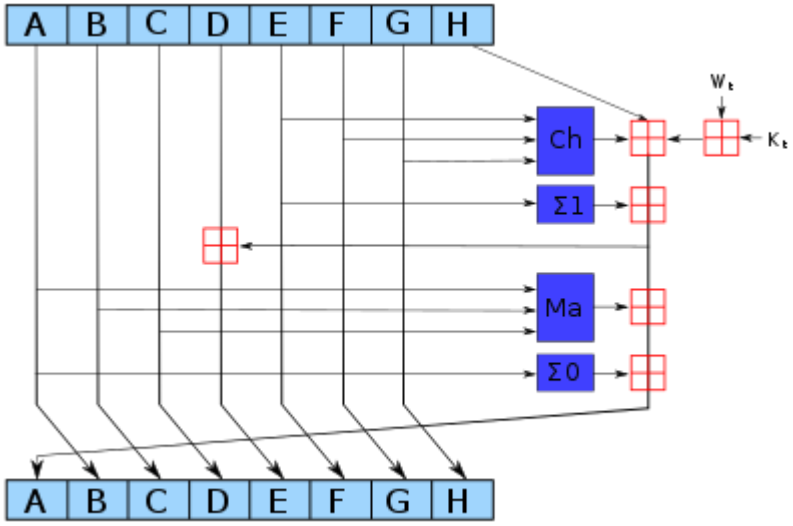
(二)、 擴散

接著，把每 512 位元稱作一區塊，把區塊化作 32 位元一組，經由一連串的位元運算與數學上的取互斥聯集（即是把兩兩區塊已一定的方式做左移或右移位元運算，再做 XOR 運算）

(三)、 壓縮

方法與擴散類似，差異在於取聯集後會將輸出值指派給向量指標，不斷遞迴運算以增加複雜性。方法如下圖

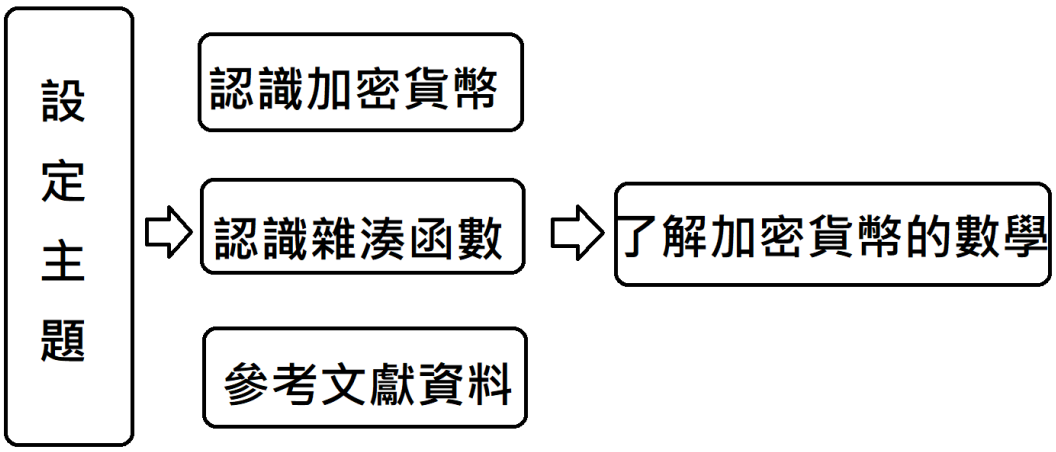
圖二、 SHA-256 的壓縮



貳、研究方法

我們透過了解加密貨幣如何應用數學原理，使虛擬的電子數字有了價值可言，並更加了解這個產業的潛在風險。

圖三、 研究流程圖



參、研究分析與結果

一、加密貨幣的運作（3Blue1Brown, 2017）

(一)、 帳本與區塊

中心化的帳本在記帳時，是採用具有公信力的單位統一紀錄的帳本查詢匯款資料，當數筆交易完成時，交易資訊會經由第三方按照順序一筆一筆記在公共帳本上。然而，前述有提到，比特幣是點對點的型態進行交易的，亦即，每個人手裡各有一本自己的帳本，在加密貨幣中，我們稱之為區塊。每當一筆交易完成時，我們便會把交易紀錄以一定的格式記錄在區塊中，並廣播出去。

(二)、 區塊與區塊鏈

當我們廣播我們的區塊時，我們同時也會收到來自其他地方廣播的區塊交易資訊。當一個區塊所記錄的交易資訊達到一定的量時，所謂「礦工」(負責運算並打包區塊鏈的人）會先在自己所在的區塊中添加一筆資料，表示自己因打包而獲得的比特幣作為獎勵（如果打包的區塊被加到區塊鏈，自己便能擁有該獎勵)，再打包整個區塊的資料，並發布給所有使用者。當我們各個區塊的資訊串連在一起，就成了所謂的區塊鏈。因此，我們的帳本中也可以即時得到更新。

二、如何有效運用數學防止區塊鏈不法竄改

(一)、 雜湊函數與最長鏈原則

我們的雜湊值在區塊鏈扮演重要角色。當每個區塊鏈要打包時，我們規定區塊最後面要加上幾個隨機數字，使整個區塊資料的雜湊值的開頭為 n 個 0 ，而各種加密貨幣主要差異即是在 n 數的設定。首先，我們規定每個區塊的開頭必須加上上一區塊雜湊值的末幾碼。假設我們規定要記錄末 5 碼到下一區塊，而有不法人士想要竄改 5 個以前區塊鏈的資料，他就必須要搶先所有使用者修改後五個區塊鏈的雜湊值。此外，由於雜湊函數的不可逆性，計算雜湊值只能依賴電腦反覆進行雜湊運算，因此僅僅 5 碼的雜湊值及需要進行 10 的 5 次方再 5 次方，也就是：

10^5 x 10^5 x 10^5 x 10^5 x 10^5 = 10000000000000000000000000 次運算！

令加密貨幣更加安全的是，加密貨幣遵從「最長鏈原則」，也就是不同區塊鏈上的交易紀錄有所衝突時，以最長的區塊鏈為準。因此如果有人想要偽造區塊，則那個人的運算能力必須高出全世界，才能使自己的假區塊鏈被拿來使用！

(二)、 加密貨幣如何控制區塊生成的速度（李永樂, 2019）

除了限制區塊長度以外，加密貨幣長透過控制打包區塊的門檻（上一段的 n 值）來限制區塊的生產。假設一台礦機（運算雜湊函數並打包區塊的電腦或機器）每秒可以進行三兆次運算，且我們將運算雜湊值視為產生一段由 0 和 1 組成的字串，若設全世界有一萬台礦機，且加密貨幣創立者希望每六百秒生成新的區塊，球 n 值應設為 62，因為：

3 x 109 x 10000 x 600 = 2n

n = log(18) x 15 ÷log(2) ≒ 62

(三)、 比特幣與等比數列（IG 集團控股有限公司, 未知）

前文提到，礦工辛苦耗費 CPU 或 GPU 資源運算能獲得比特幣作為獎勵，最初每打包一次區塊便能獲得 50 枚比特幣，但為了避免比特幣氾濫，每生成二十一萬次區塊(大約需要四年)，獎勵金就會減半，直到小於比特幣的最小單位（1 聰＝0.00000001 個比特幣）為止。由於每次區塊生成約需十分鐘，因此我們能推算 X 年後比特幣會開採完畢：

50 個 x 0.5^X =(86400 秒 x 365 天) x (600 秒 x 210000 次)

X ≒ 33

由於比特幣在 2009 年開啟了第一個區塊，因此在 2009 + 33 x 4 = 2141 年時，比特幣會被開採完，共有 21000000 枚比特幣：

210000(50 + 25 + 12.5 + … + 50 x 0.533) ≒ 21000000

肆、研究結論與建議

基於以上論述，我們**發現**加密貨幣不只是遊戲中簡單的虛擬貨幣，而是運用大量數學建構而成的複雜系統。由於加密貨幣的開採具有限性，這種貨幣不會像遊戲虛擬寶物的價格不停翻倍，但無法確保他不能夠被炒作。由於加密貨幣應用了以上數學原理，加密貨幣不容易遭到非法人士破壞，但由於使用者通常都是匿名交易，此類交易平台長被拿來做為洗錢或黑市交易用（蕭白雪等，2022）。不過，從比特幣的例子，我們了解到，數學與生活其實是息息相關的，只要仔細觀察，就能在日常生活中玩出數學來。

伍、參考文獻

Satoshi Nakamoto (2008), Bitcoin: A Peer-to-Peer Electronic Cash System. 取自 https://bitcoin.org/bitcoin.pdf

Jan Lansky（2018）, Possible State Approaches to Cryptocurrencies. 取自 https://pdfs.semanticscholar.org/c14a/cbbb00b5baee7f10b24d224d429ee6b39e0e.pdf

Chen Yan Long （2021）DAY 18- 雜湊函數 SHA-256。取自 https://ithelp.ithome.com.tw/articles/10271904

NIST（2004）Secure Hash Standard, FIPS PUBS. 取自 https://www.nist.gov/publications/secure-hash-standard

3Blue1Brown（2017）你有疑惑過比特幣（與其他加密貨幣）的運作原理嗎。取自 https://youtu.be/bBC-nXj3Ng4

李永樂（2019）比特幣和區塊鏈到底是啥？礦機挖礦咋回事？李永樂老師講比特幣(1)。取自 https://youtu.be/g_fSistU3MQ

IG 集團控股有限公司（無日期）比特幣減半。取自 https://www.ig.com/cn/bitcoin-btc/bitcoin-halving

蕭白雪、李奕昕、張宏業（2022/03/06）熱議題／虛擬貨幣洗錢 列非常高風險。聯合報。取自 https://udn.com/news/story/7315/6143535