密碼學
Cryptography

密碼學是信息安全技術的核心

傳統密碼學

密碼學發展的簡史

- 近代加密技術 應用於美國獨立戰爭、美國內戰和兩次世界大戰
- German Enigma 密碼機
- 1949年，Shannon發表《保密系統的通信理論》
- 1976年，迪菲(Diffie)和赫爾曼(Hellman)建立公鑰密碼系統的新概念
- 1977年美國頒佈數據加密標準(DES)

密碼學(Cryptography)

- 偽裝信息，令局外人不能理解其真實含義，而局內人卻能夠理解偽裝信息的含義。
- 希臘單詞 Kryptos （隱藏）和 Graphin （寫）
- 代表用來隱祕的傳遞信息

密碼學(Cryptography)

- 在密碼學領域，密碼並非一個獨立的概念，對應的定義稱為「密碼體制（Cryptosystem）」，包括5個要素：
- **明文(Plaintext)**：源信息
- **密文(Ciphertext)**：經過偽裝後的信息
- **加密(Encrypt)**：把明文轉換為密文的過程
- **解密(Decrypt)**：把密文轉換為明文的過程
- **密鑰(Key)**：由數字、字母或特殊符號組成的字符串，可以控制加密和解密的過程。

以英文為例，明文和密文的編碼集合都是A-Z（通常不分大小寫），或者加上標點符號。

加密和解密就是加/解密的方法，密鑰就是在加密和解密過程中分別與明文和密文進行運算的元素。

密碼學(Cryptography)

- 在密碼學發展的歷史中，主要分為兩個階段，

✓古典密碼學

以「置換法」（**Transposition ciphers**）及「替換法」（**Substitution ciphers**）爲基礎

✓現代密碼學

建立在數學、電腦與通信科學的基礎

密碼學(Cryptography)

「置換法」（**Transposition ciphers**）

改變明文中單元的位置，而單元本身沒有轉變

例子:**籬笆密碼法 (Railfence cipher)**

「替換法」（**Substitution ciphers**）

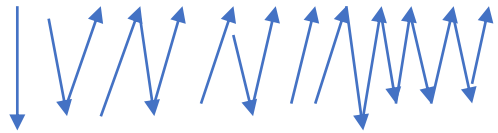
「**單表加密**」（ Monoalphabetic cipher ） 以一個字母為一單元進行加密例子:「凱撒密碼」

「**多表加密**」（ Polyalphabetic cipher ）以數個字母為一單元進行加密 例子:「維吉尼亞密碼」

密碼學(Cryptography) - 「置換法」

籬笆密碼法 (Railfence cipher)

d y u n w h t s l c c a n

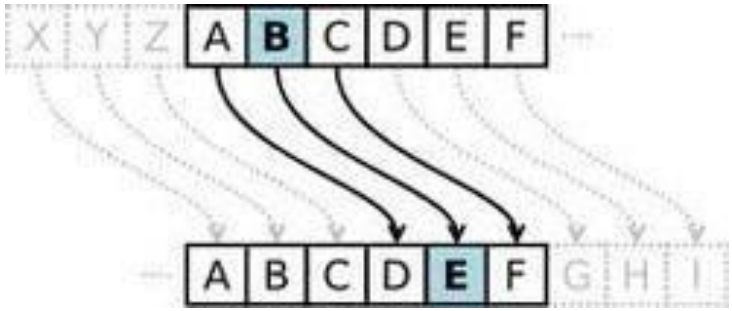


o o k o w a i b o k h i

Do you know what is blockchain

密碼學(Cryptography)-「替換法」

- 「凱撒密碼」
- 英文字字母用其後的第三個字母替換，如果數到Z則從頭開始。
- 例如WEWONTHEWAR加密後就是ZHZRQWKIZDU，收到消息的一方解密的時候再向前推三個英文字字母就解密，推到結果有意義的就是明文。



凱撒密碼 (Caesar Cipher)

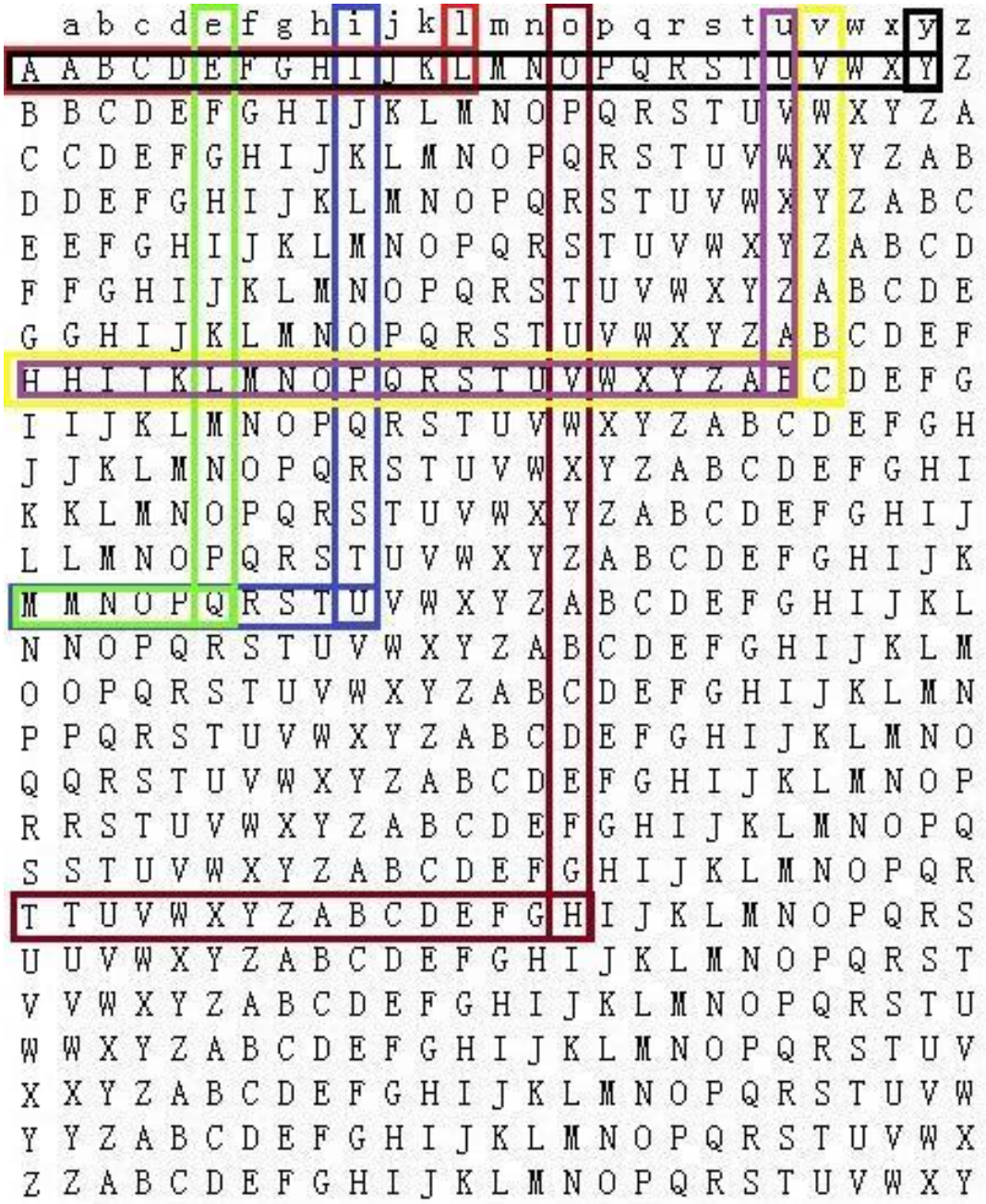
- 從A到W的每個字母在加密時用字母表中位於後三位的字母代替，字母XYZ分別被替換成ABC。即將字母向右移動三位。
- 在三個移位的情況下，信息CAT（「明文」）就變成FDW（「密文」）；密文GRJ對應的明文則是DOG。
- 加密和解密過程都是以字母移位為參照。算法中依賴的參數則被稱為——密鑰。

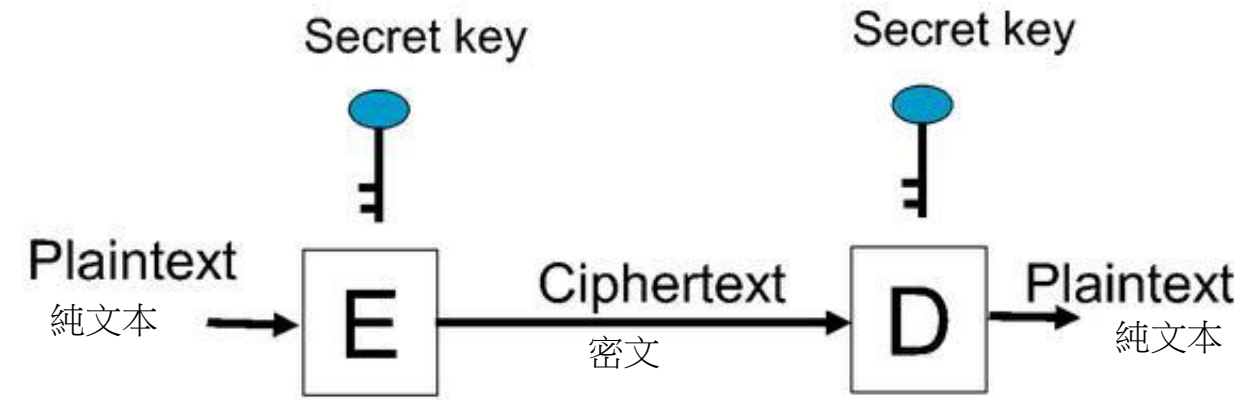
BLOCKCHAIN = EORNFKDLQ

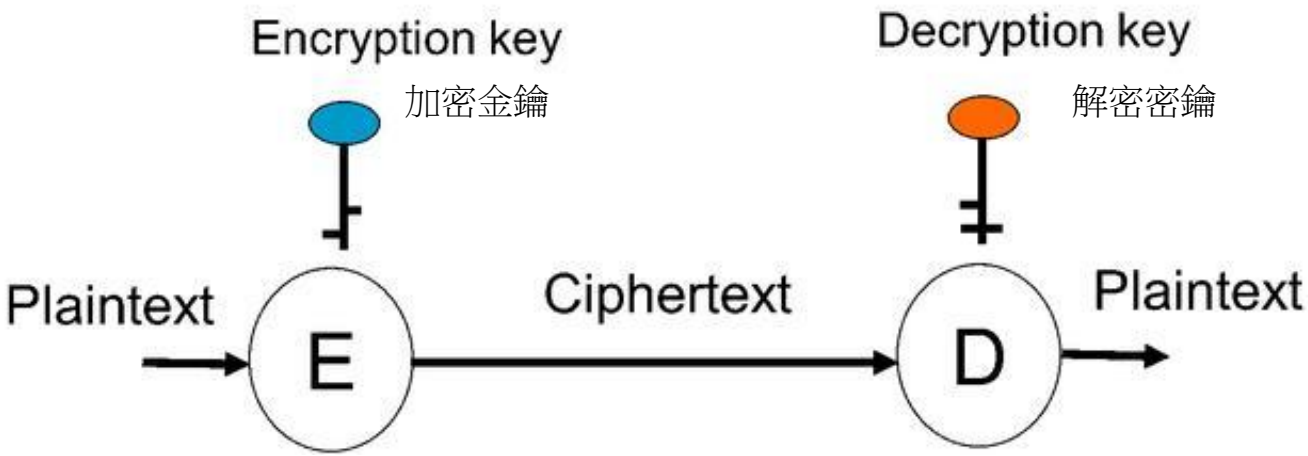
HADP = EXAM

維吉尼亞密碼 (Vigenère cipher)

- 維吉尼亞密碼或維熱納爾密碼：首先選擇一個無重複字母的密鑰詞（比如 MATH ），重複密鑰詞直至它成為一個和明文信息一樣長的字母序列，再利用下頁的圖(方陣)加密信息。
- 加密第一個字母 I，此時它下方對應的密鑰詞是 M，於是，加密 I 時由 M 對應的那行中讀出 i 列下的字母即 U，類似的，得出所有密文：
- 信息ILOVEYOU密鑰MATHMATH密文ULHCQYHB




Secret key
Secret key
Plaintext
純文本
E
Ciphertext
密文
D
Plaintext
純文本


Encryption key
加密金鑰
Decryption key
解密密鑰
Plaintext
E
Ciphertext
D
Plaintext

非對稱加密

公鑰密碼學

- 區塊鏈使用密碼學技術 -公鑰密碼學 (Public Key Cryptography) – 即公開的資訊
- 而私鑰 即自己個人保管的資訊
- 公/私鑰同時可以進行加密同解密，當公鑰加密成為鎖，私鑰就是他的解，反之亦然，形成兩種不同的資訊保安用途
- 1)公鑰加密，私鑰解密：保護被傳送的訊息本身，證明只有私鑰擁有者可以閱讀。
- 2)私鑰加密，公鑰解密：保護公鑰持有者，證明發佈人(私鑰擁有者) 的正當性

雜湊函數 (Hash Function)

- 接收各種檔案形式（包括數字、文字、圖像、影片等）、檔案大小，並經雜數方程式運算，壓縮後，輸出一串固定大小的數字
- 想像是一台轉換器，轉換是「單向」(one-way function)，輸入可以經由轉換得到輸出，但輸出卻不可得到輸入，具有不可逆的特性
- https://blockbar.io/blockchain/hash%E6%98%AF%E4%BB%80%E9%BA%BC-what-is-hash/

- 常使用的單向雜湊函數包括MD5、SHA-1、SHA-256、SHA-384及SHA-512等，MD5的Hash值長度為128位元，雖然廣為使用，但因長度不夠較容易破解，SHA-1的Hash值長度有160位元，雖比MD5好但仍然不夠安全，因此美國國家安全局（NSA）又提出多種更複雜的SHA-2演算法，包括224、256、384、512位元長度的Hash值算法。

Merkle Tree 將大量訊息縮短成一個 Hash 值

- 在比特幣區塊鏈中，每筆交易產生後，都已經被Hash成一段代碼才廣播給各節點，不過這樣做還不夠，因為在各節點的區塊中，可能包含數百筆到數千筆的交易，因此，為節省儲存空間並減少資源耗費，比特幣區塊鏈的設計原理採用Merkle Tree機制，讓這些數百到數千筆的交易Hash值，經由兩兩一組形成一個新Hash值的方式，不斷重複進行，直到最後產生一組最終的Hash值，也就是Merkle Tree Root，這個最終的Hash值便會被記錄到Block Header中，只有32 Bytes的大小。Merkle Tree機制可大幅減少資料傳輸量與運算資源消耗，驗證時，只需驗證這個Merkle Tree的Root值即可。

Hash Function – Merkle Tree

https://passwordsgenerator.net/sha256-hash-generator/

SHA256 Hash Generator

This online tool allows you to generate the SHA256 hash of any string. SHA256 is designed by NSA, it's more reliable than SHA1.

Enter your text below:

hi

Generate | Clear All | MD5 | SHA1 | SHA512 | Password Generator

☐ Treat each line as a separate string

SHA256 Hash of your string:

```
8F434346648F6B96DF89DDA901C5176B10A6D83961DD3C1AC88B59B2DC327AA4
```

雜湊函數 (Hash Function)

- 雜湊函數是以**十六進位**為基礎
- 例子 MD5 (128-bit) 、 SHA-256 (256-bit) 、 SHA-512 (512-bit) 。bit代表檔案壓縮後產出數字的大小，bit越大代表可能產生的數字越多種
- https://xorbin.com/tools/sha256-hash-calculator

- DOG - 6237ac702a421096cf4f46e46ef3fe65101fe6e11292a320b9eb80850a0939c9 [SHA-256]
- DOGS – 70930360b81e5f4ef2e06d2bf64978b44d4b87fb85d78788e001cdf8812d13d1 [SHA-256]

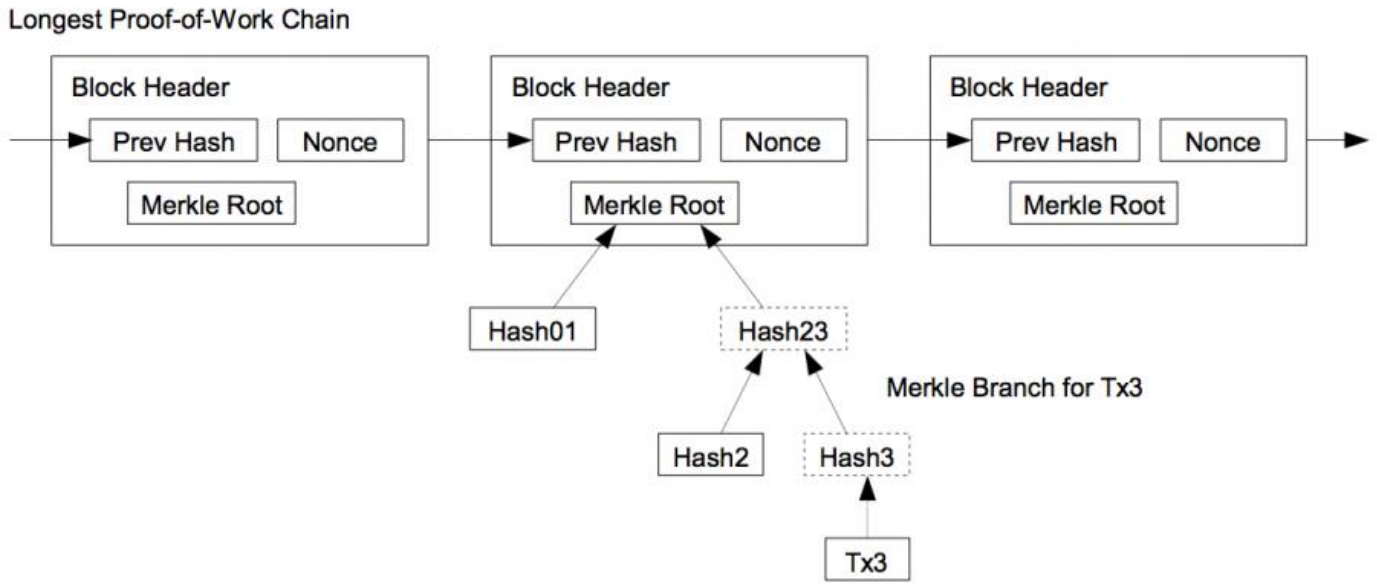
Hashcash 演算法

Hashcash是一種工作量證明(Proof of work)演算法

The header contains:
- *ver*: Hashcash format version, 1 (which supersedes version 0).
- *bits*: Number of "partial pre-image" (zero) bits in the hashed code.
- *date*: The time that the message was sent, in the format YYMMDD[hhmm[ss]].
- *resource*: Resource data string being transmitted, e.g., an IP address or email address.
- *ext*: Extension (optional; ignored in version 1).
- *rand*: String of random characters, encoded in base-64 format. 一串隨機字符
- *counter*: Binary counter, encoded in base-64 format. 二進制計數器，以 base-64 格式編碼

Hashcash最早在1997年由Adam Back提出，並於2002 正式發表一篇描述雜湊現金系統的論文。比特幣區塊鏈採用Hashcash來建立一套幾乎無法被竄改的電子現金系統，每個區塊的Block Header都會被Hash成一串很難被回推的代碼後，放進下一個區塊中，來確保區塊的正確性。

區塊鏈



比特幣區塊鏈的關鍵核心技術，包括採用Hashcash演算法來進行工作量證明，讓區塊鏈中的各節點有機會參與驗證，達到公正性，且交易過程採用橢圓曲線數位簽章演算法來確保交易安全，並在每筆交易與每個區塊中使用多次Hash函數以及Merkle Tree，不只是為了節省儲存空間，更重要的是藉由將前一個區塊的Hash值加入新區塊中，讓每個區塊環環相扣，也因此做到所謂的可追蹤且不可竄改的特性，同時也使用時間戳來確保區塊序列

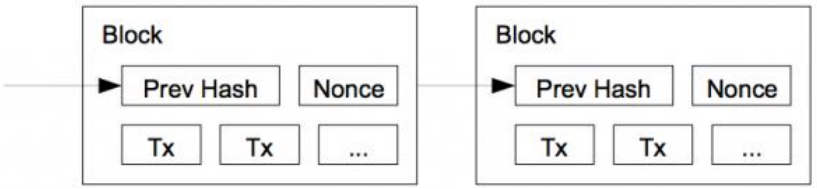
共識機制 (共識演算法)

- 如同參與區塊鏈記帳的遊戲規則 {礦工的挖礦規則}
- 目的就是要讓公有區塊鏈網路中的參與者(節點)，在彼此不相互信任且無中央權威機構存在(去中心化)的網路中，也能達成共識
- 在去中心化的體制下，區塊鏈帳本的維護需仰賴網路上各個礦工，由於帳本存在於網路上各個節點之中，因此，必須讓節點之間的帳本達成共識，才能保證**帳本的一致性**與**交易的最終性**。

共識機制

PROOF OF WORK 工作量證明

- 每個運算節點的運作方式就會透過「工作量證明(Proof of Work, PoW)」來進行
- 誰先用最少時間透過**工作量證明**運算技術計算出答案並獲認可便成立（找到區塊頭元數據的哈希值(Hash)），這可實現多方共同維護，交易可被驗證。{挖礦}



- Bitcoin 就是使用PoW

Proof of work

PROOF OF WORK 工作量證明 -算力挖礦

- 比特幣採用 PoW 共識機制保障區塊鏈帳本的一致性與交易的最終性
- 容易實現，節點可自由進入，去中心化程度高
- 破壞系統需要投入極大的成本，安全性極高
- 為了保證去中心化程度，區塊的確認時間難以縮短。
- 透過礦工的計算能力以及硬體成本確保礦工立意良善，挖礦過程中能源消耗多，機制非常不環保
- **驗證效率差、浪費能源**
- Bitcoin 用了PoW

工作量算力

PROOF OF STAKE 權益證明

- Proof-of-Stake與股票市場類似
- 想像你要決定一間上市公司未來的發展方向，必須要先持有該公司的股票，成為stakeholder後才能在股東大會上發言。佔有的股分權益越多越有機會在投票時影響結果
- 用加密貨幣抵押量(token)取代礦工算力的比拚，節點不需要買礦機，他們須買加密貨幣，並將其抵押在智能合約中
- 鍛造者仍然保有該加密貨幣的所有權，只是不能隨意動用

權益證明

PROOF OF STAKE 權益證明

- PoS 機制下的節點稱為鍛造者 (Forger / Validators)
- 鍛造者不需像礦工一樣花費大量的電力競爭，能源消耗的問題被解決
- 若鍛造者希望在這個區塊鏈加密貨幣因此有機會增值，就經濟考量， PoS 對節點也比較有利
- 由於 PoS 的挖礦成本比 PoW 低很多，PoS 不一定需要產出新的加密貨幣作為區塊獎勵，只需以該區塊的交易費作為獎勵，即足以維持系統安全
- 以太坊正在逐漸由PoW改以PoS方式運行

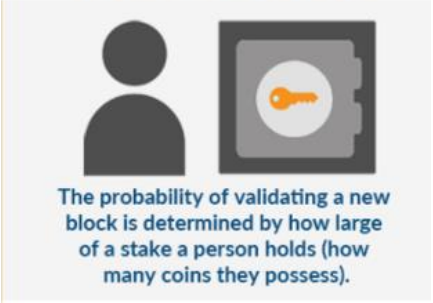
挖出一個區塊的概率取決於礦工完成了多少計算工作.

獎勵第一個解決每個區塊密碼難題的礦工

網絡礦工使用計算能力相互競爭. 挖礦社區往往會變得更加集中化.

圖片來源 *3iQResearch Group*

PROOF OF STAKE

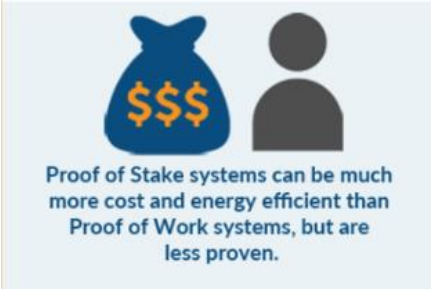


The probability of validating a new block is determined by how large of a stake a person holds (how many coins they possess).

驗證新區塊的概率取決於一個人持有的股份有多少 (他們擁有多少硬幣)

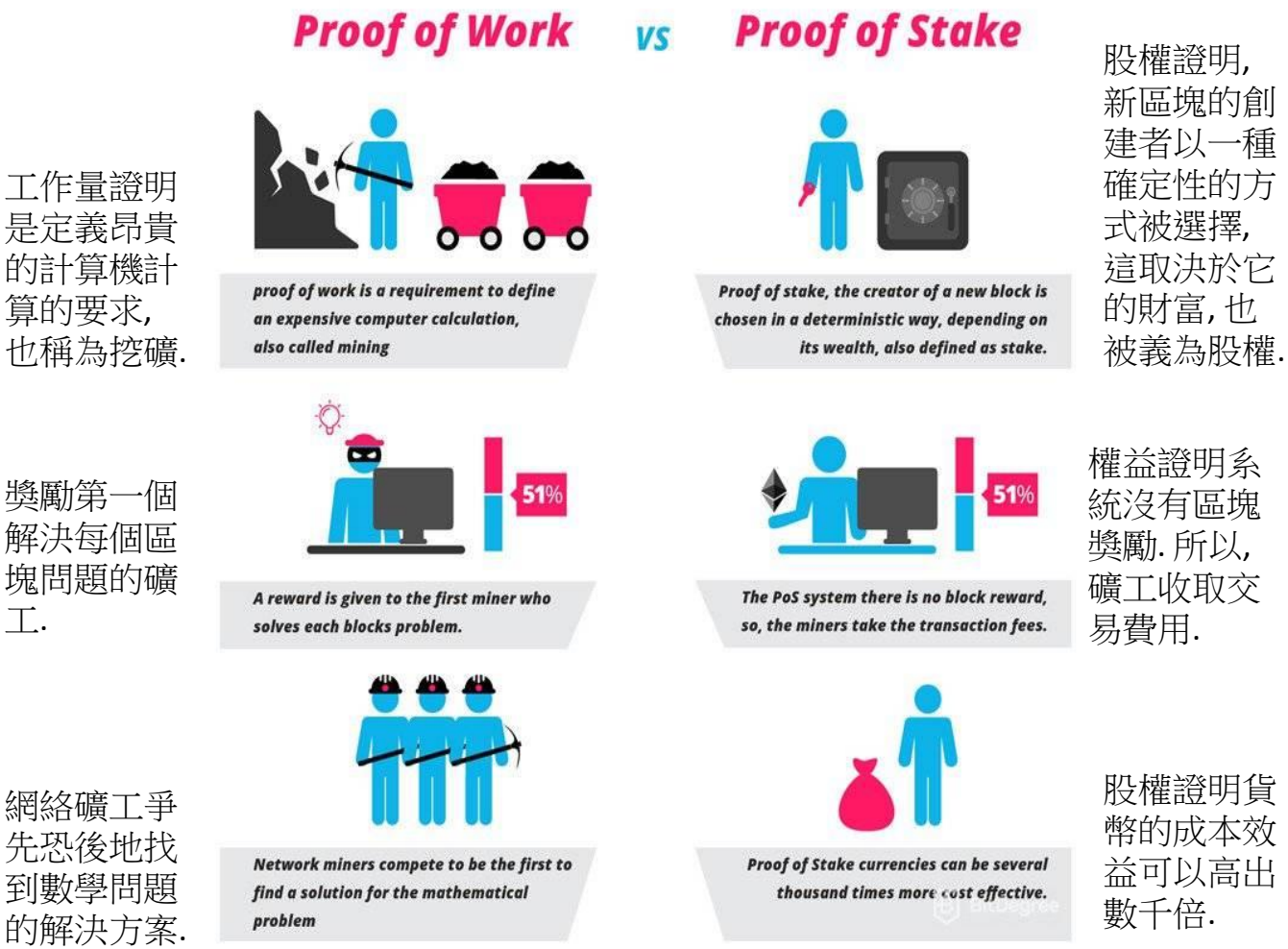
The validators do not receive a block reward, instead they collect network fees as their reward.

驗證者不會獲得區塊獎勵, 而是收取網絡費作為獎勵.



Proof of Stake systems can be much more cost and energy efficient than Proof of Work systems, but are less proven.

股權證明系統可以比工作量證明系統更具成本和能源效率, 但證明較少.



工作量證明是定義昂貴的計算機計算的要求，也稱為挖礦.

獎勵第一個解決每個區塊問題的礦工.

網絡礦工爭先恐後地找到數學問題的解決方案.

股權證明，新區塊的創建者以一種確定性的方式被選擇，這取決於它的財富，也被義為股權.

權益證明系統沒有區塊獎勵. 所以，礦工收取交易費用.

股權證明貨幣的成本效益可以高出數千倍.