

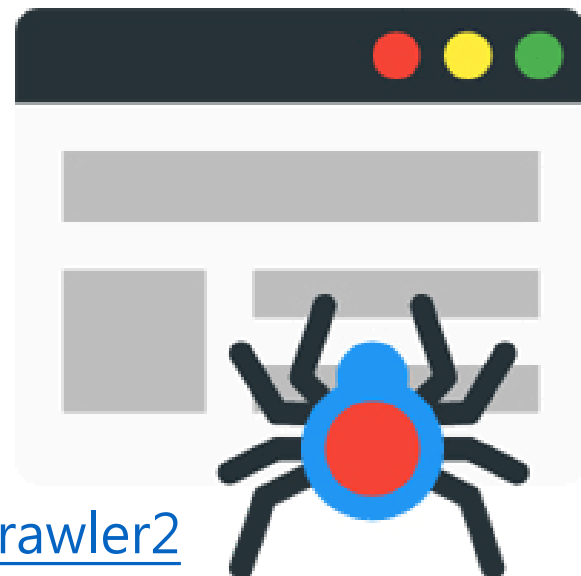
# Python爬蟲實作(四)

## 虛擬貨幣抓取 及區塊鏈介紹

主講人：陳東笙

程式碼：

<https://github.com/dong945/Python-Crawler2>



# 免責聲明

以下分享內容  
純為社團交流活動  
無從事任何商業行為

## 注意事項：

簡報內容截錄自網路及參考書籍  
並未取得作者授權，故僅供會中討論  
請勿散佈，以免侵犯作者權利

# 爬蟲應有的道德

- ◆不告而取謂之『偷』
- ◆尊重智慧財產，不作商業用途
- ◆做好偽裝，保護自己
- ◆避免過度抓取，影響網站運作

重要事情要說三遍

**Bitcoin  $\neq$  Blockchain**

**Bitcoin  $\neq$  Blockchain**

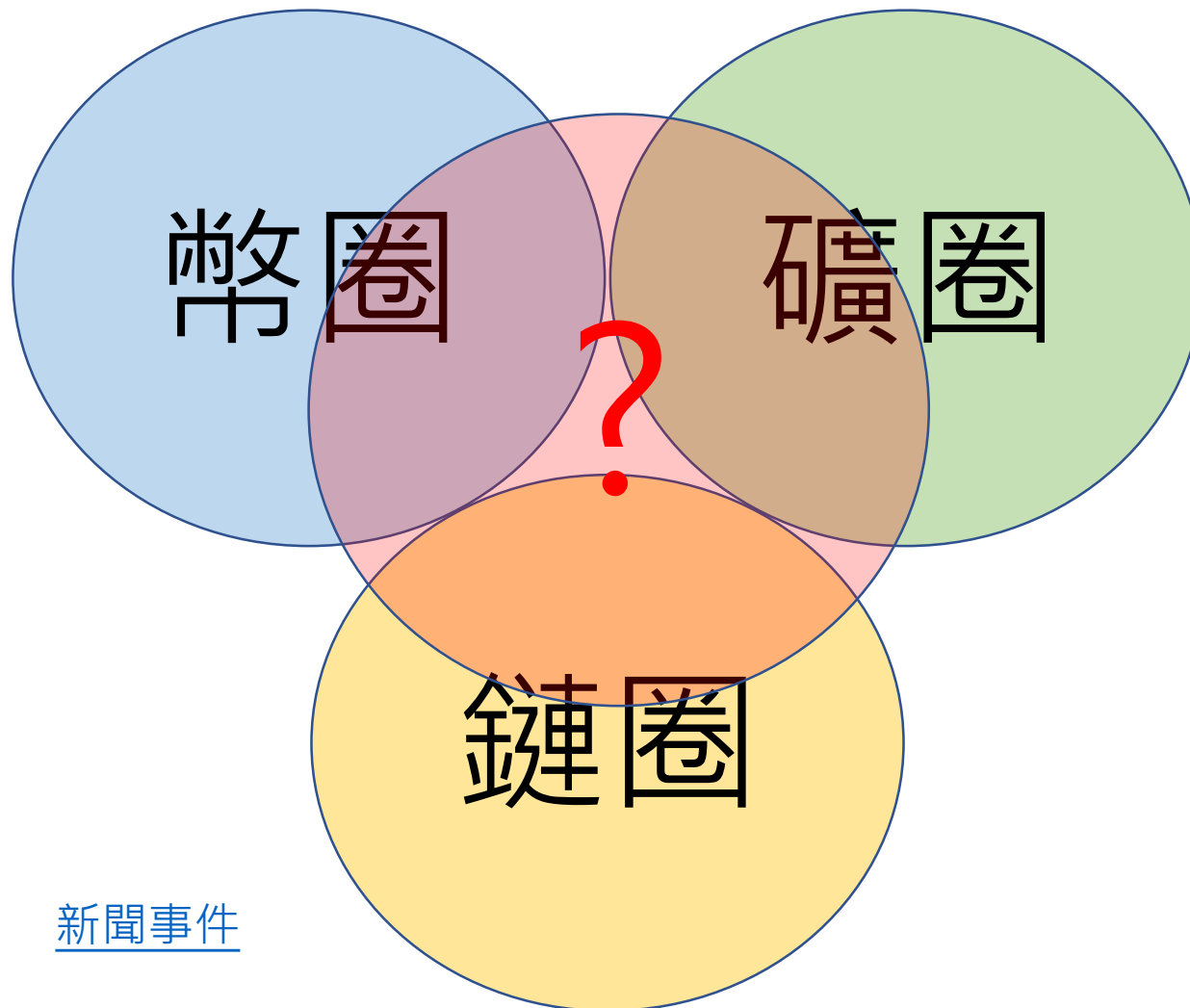
**Bitcoin  $\neq$  Blockchain**

**比特幣  $\neq$  區塊鏈**

**比特幣  $\neq$  區塊鏈**

**比特幣  $\neq$  區塊鏈**

# 你是那一圈？

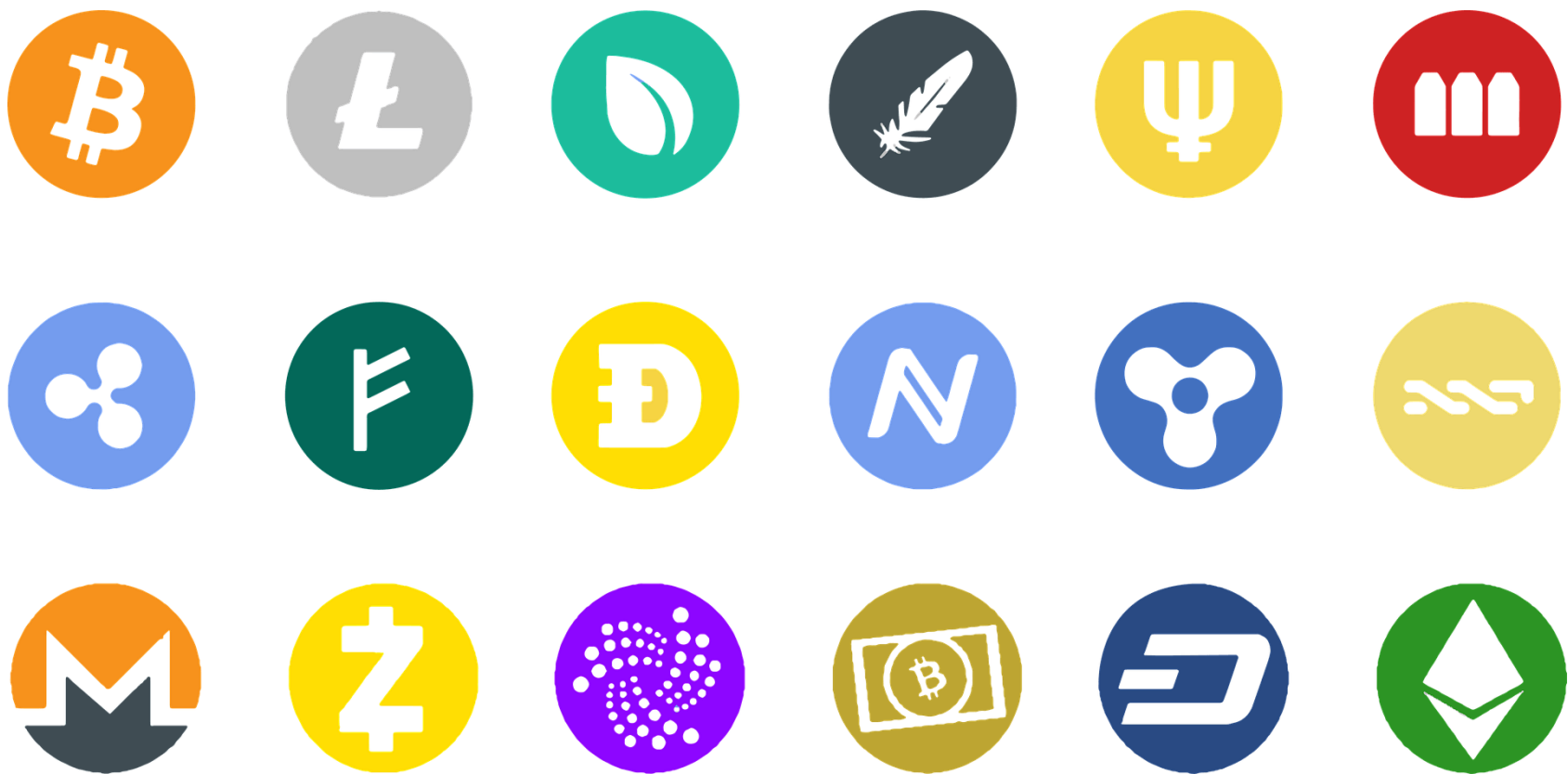


新聞事件

# 比特幣生態圈



# 數位貨幣、加密貨幣、虛擬貨幣 傻傻分不清



# DEMO

## 抓取總市值 前100名的虛擬貨幣



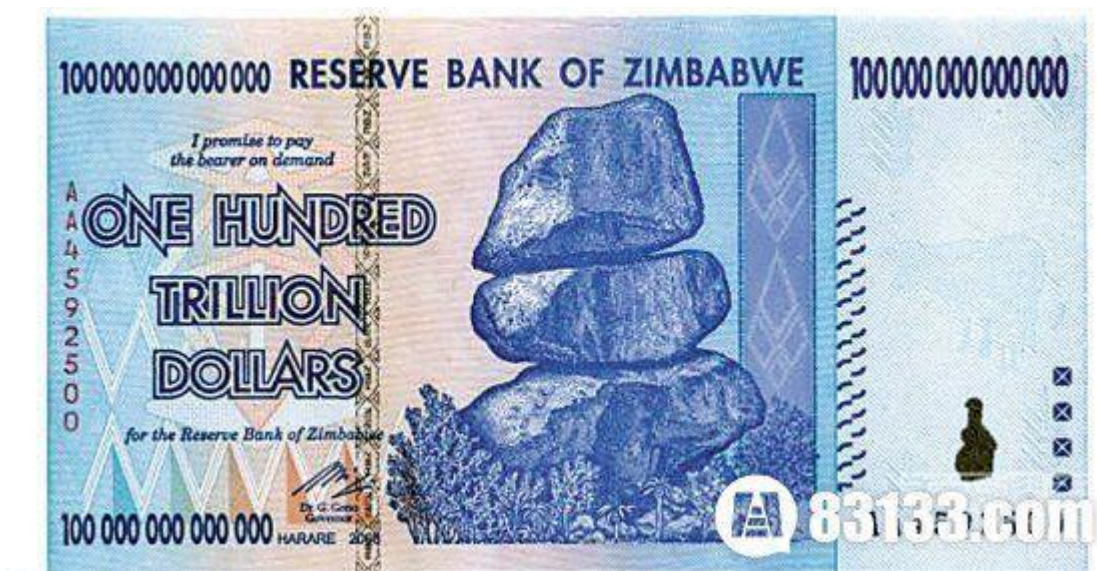
# 法幣的定義

<https://zh.wikipedia.org/wiki/法定貨幣>

**法定貨幣**（英語：Fiat Money），簡稱**法幣**，是政府發行的紙幣。依靠政府的法令使其成為合法通貨的貨幣。

發行法定貨幣的國家或銀行，會將其法定貨幣與一種或數種外幣掛鉤，並以政府外匯儲備維持其匯價在一定的水平。



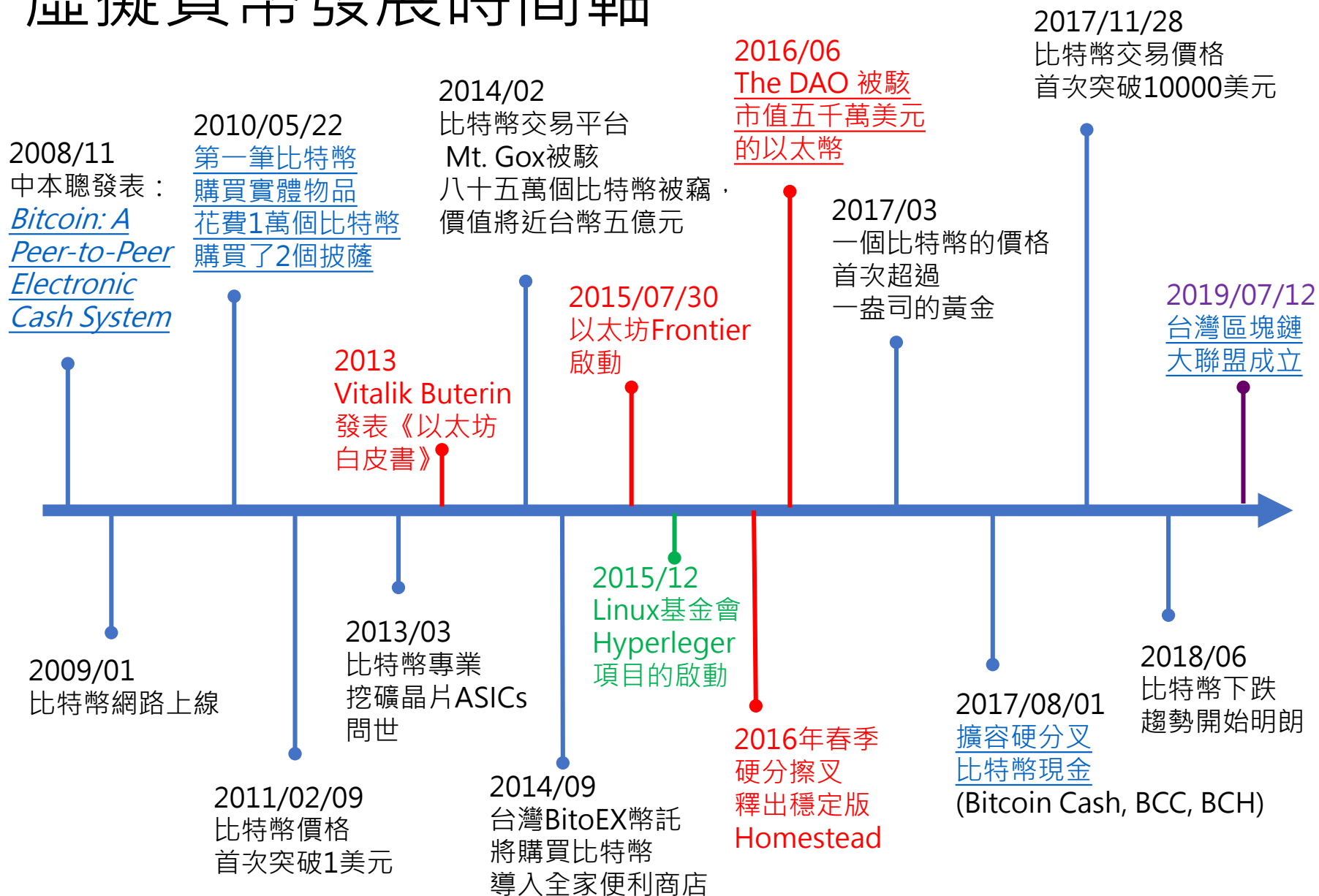


印有14個0的辛巴威幣

一億辛巴威元可以買3顆雞蛋



# 虛擬貨幣發展時間軸





# 比特幣(BTC) 以太幣(ETH) 瑞波幣(XRP) 萊特幣(LTC)



# 區塊鏈的特性

- 去中心化
- 加密
- 不可竄改
- 可追蹤

<https://www.youtube.com/watch?v=bBC-nXj3Ng4>

# 區塊的構成

<https://www.blockchain.com/>

每一個區塊包含有：

## 區塊的容量大小(Block Size)

## 區塊頭(Block Header)

## 交易數量(Transaction Counter)

## 交易資訊(Transaction)



圖片來源：《[區塊鏈運作原理大剖析：從一筆交易看區塊鏈運作流程](#)》

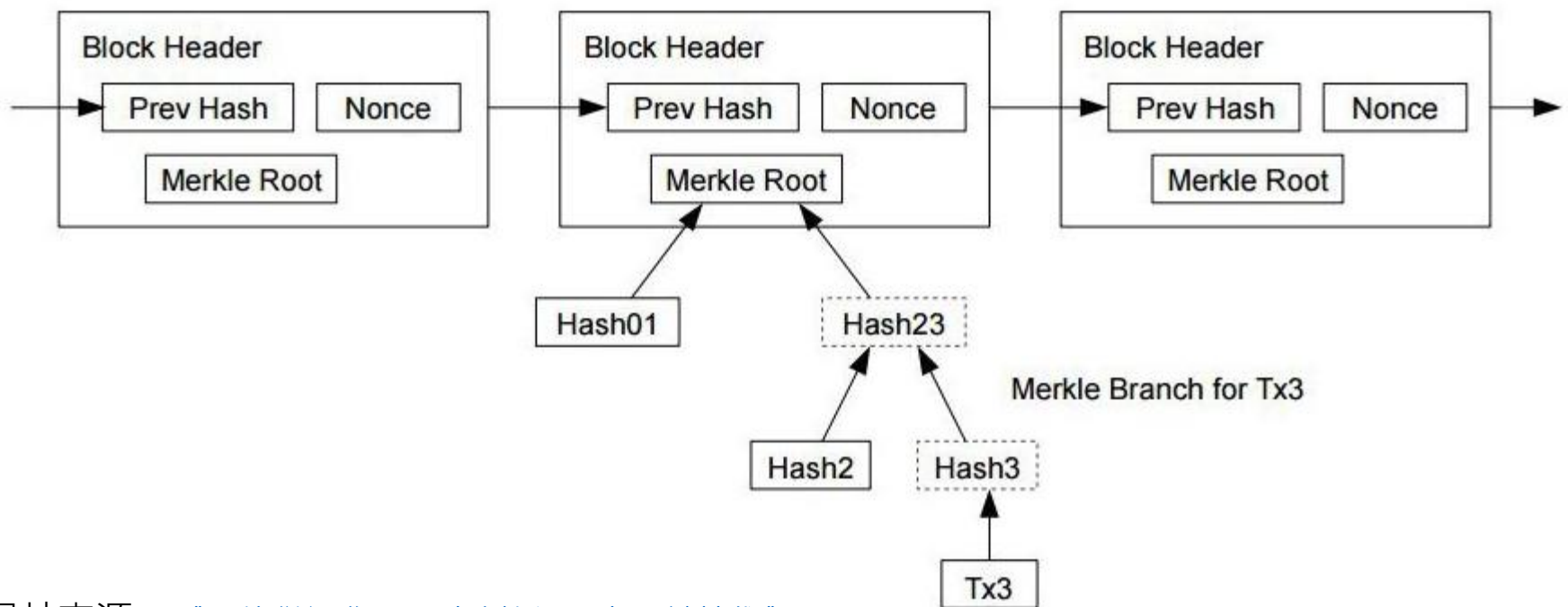
區塊頭固定80Bytes，包含有：

第一組32Bytes的Hash值(Previous Block Header Hash)

第二組為中繼資料，由Difficulty Target、

Timestamp及Nonce值所組成

第三組為彙整多筆交易紀錄的資料結構Merkle Tree Root



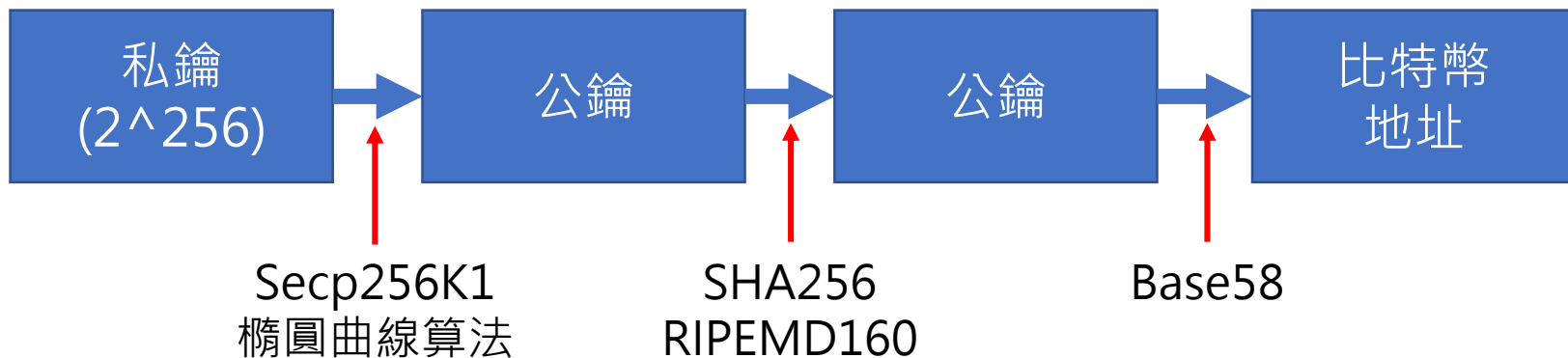
圖片來源：[《區塊鏈運作原理大剖析：5大關鍵技術》](#)

# DEMO

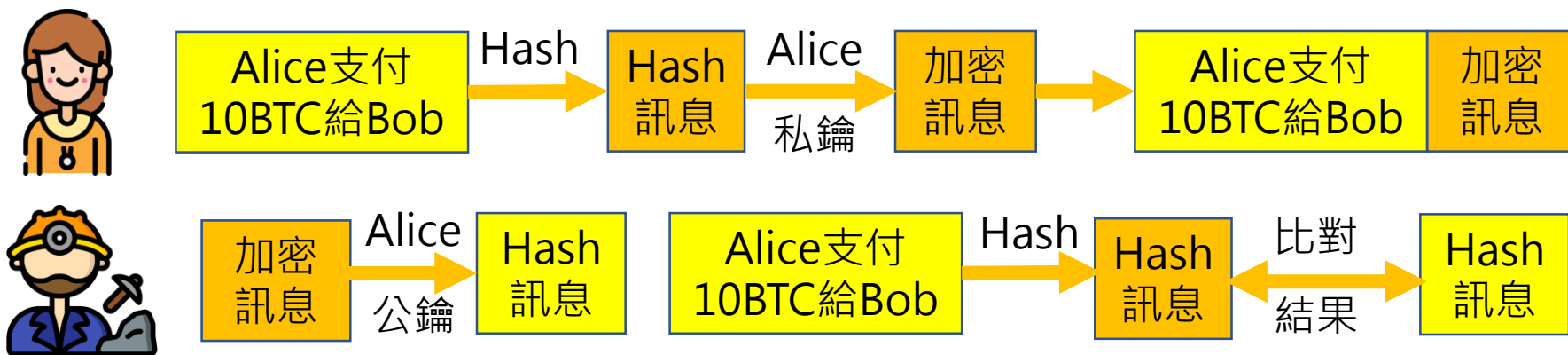
## 查看區塊0及區塊結構 抓取交易資訊



# 比特幣非對稱加密機制



## 橢圓曲線簽名與驗證簽名



# DEMO

比特幣公、私鑰產生  
加密簽章驗證

# 比特幣區塊鏈的特性

- ★採用工作量證明機制(Proof of Work, POW)
- ★每產生2016個區塊會調整一次難度，  
以每10分鐘產生一區塊估算，  
大約是每兩周會調整一次Difficulty
- ★每筆交易採橢圓曲線數位簽章演算法加密
- ★ Hashcash演算法及多種Hash函數確保資料不被竄改
- ★經由Merkle Tree將大量訊息縮短成一個Hash值
- ★用時間戳伺服器 ( Timestamp Server ) 確保區塊序列

※時間戳是指格林威治時間1970年01月01日 00時00分00秒起至現在的總秒數

# 難度係數調整公式

每10分鐘出塊一次，

每2016個區塊調整難度係數一次

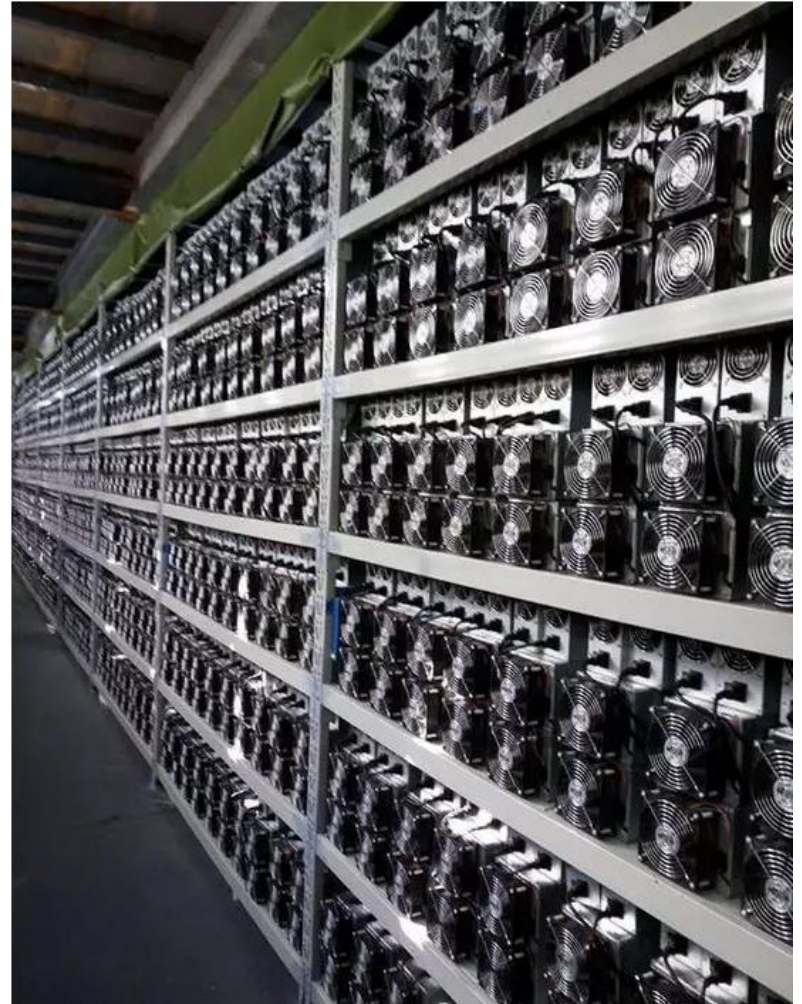
$$D_{new} = D_{old} * \left( \frac{\text{Actual Time of Last 2016 Blocks}}{2016 * 10 \text{ minutes}} \right)$$

比特幣的交易速度 = 7 tps(每秒7筆)

$$1024000(1M)/250B(\text{一笔交易基本大小})/600s(10minutes)=6.6 \text{ tps} \approx 7 \text{ tps}$$

# 工作量證明機制 ( Proof-of-Work , PoW )

來解一道數學題  
最先求出答案者  
獲取記帳權及獎勵



# 比特幣為通貨緊縮



比特幣具有總量有限，  
前4年總額將產生10500000BTC，  
每隔4年產出數額減半，  
在第4年至第8年會產生5250000BTC，  
第8至12年則只有2625000BTC，如此類推。  
到最後，

總共產生的比特幣數量為接近**21000000BTC**。

2009/01/03，創世區塊被挖出，獎勵礦工50BTC

2012/11/28，獎勵由50BTC降為25BTC

2016/07/10，獎勵由25BTC降為12.5BTC

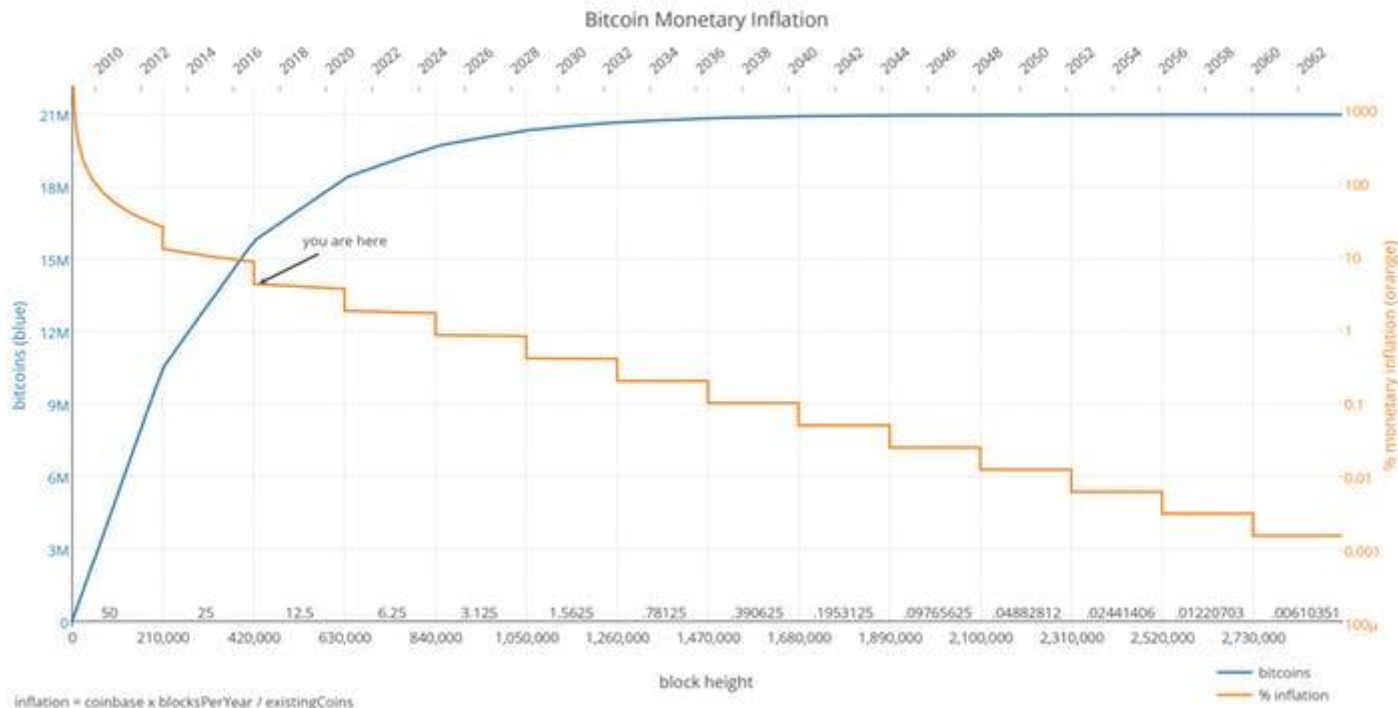
預計2020年，獎勵由12.5BTC降為7.5BTC

# 比特幣如何產生

2009/01/03，中本聰挖出第一個比特幣區塊，  
創建了首批 50 枚比特幣。

每隔 210000 個區塊，獎勵就會減少一半。

在 2016 年 7 月，獎勵已經減至 12.5 個比特幣。  
最後一枚比特幣將在 2140 年 5 月份被挖出來。



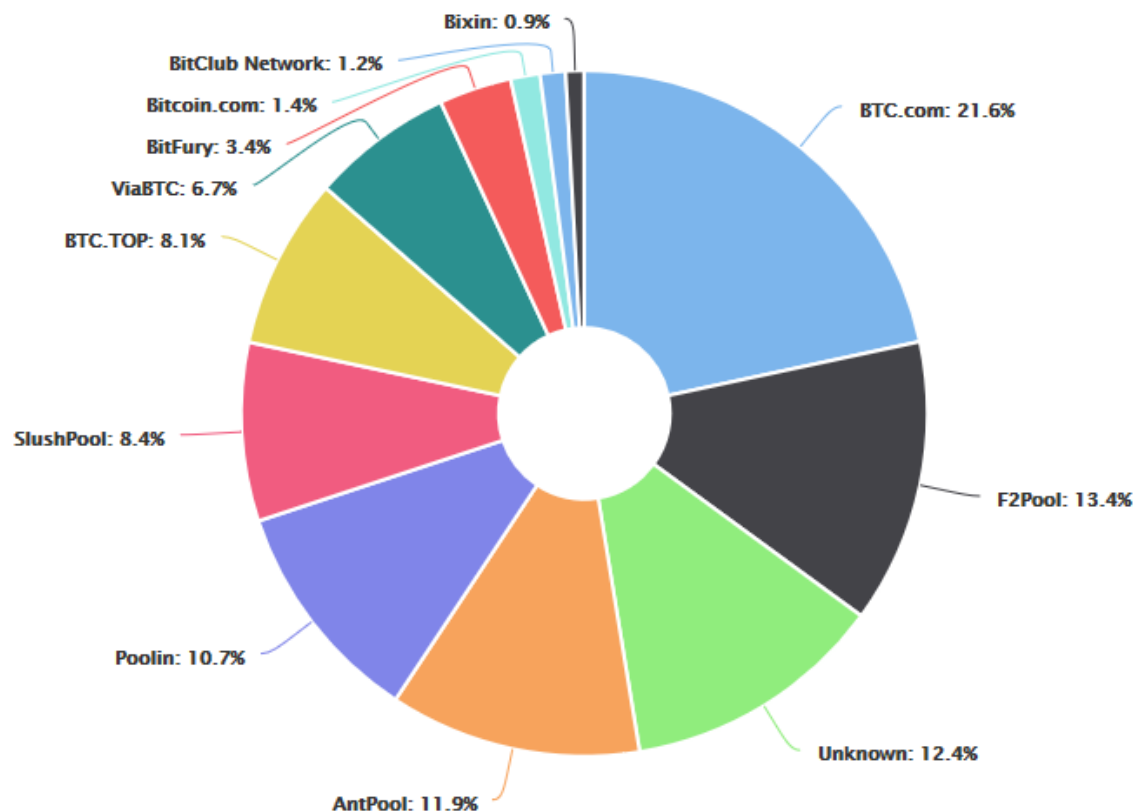
# DEMO

查看區塊高度  
抓取各種虛擬貨幣



# 比特幣礦池分佈

<https://www.blockchain.com/zh-tw/pools>



目前全球算力較大的礦池有比特礦池（BTC Pool）、魚池（F2Pool）、蟻池（AntPool）、幣印（Poolin）、Slushpool、ViaBTC等，其中僅前五大礦池的算力就超過全網算力的65%。除了slushpool外，其餘礦池都來自中國。

# 拜占庭將軍問題(Byzantine Generals Problem)

古代東羅馬帝國的帝都，

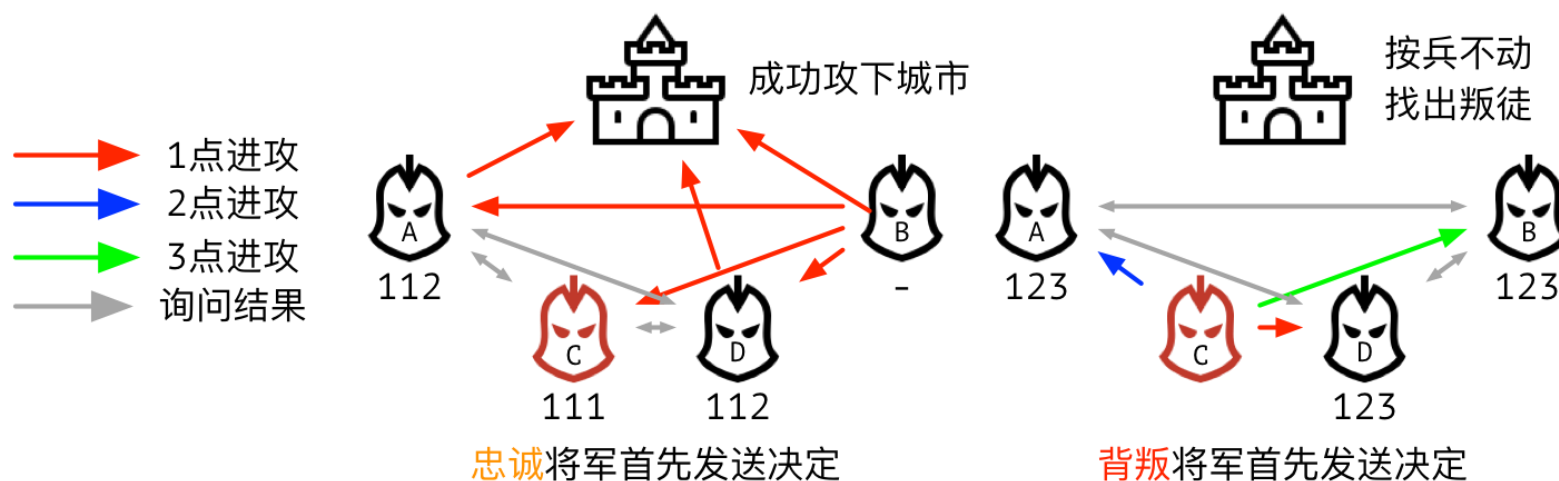
一組拜占庭將軍分別各率領一支軍隊共同圍困一座城市。

各支軍隊的行動策略限定為進攻或撤離兩種。

因為部分軍隊進攻部分軍隊撤離可能會造成災難性後果，

因此各位將軍必須通過投票來達成一致策略，

即所有軍隊一起進攻或所有軍隊一起撤離。



# 達摩克斯特之劍

## 51%算力攻擊

“51%算力攻擊”是指在控制了比特幣全網的51%算力之後，用這些算力來重新計算已經確認過的區塊，使得區塊鏈變得可以被篡改。



# Facebook Libra



<https://nextandnexus.com/libra/>

<https://www.cw.com.tw/article/article.action?id=5095751>

## 參考資料：

iThome『區塊鏈』專題：

<https://www.ithome.com.tw/article/105368>

CoinGecko(幣虎)：

<https://www.coingecko.com/zh-tw>

Blockchain.info：

<https://www.blockchain.com/>

iThome 鐵人幫幫忙：

<https://ithelp.ithome.com.tw/articles/10192847>

施威銘研究室。《Python技術者們實踐!》。  
旗標出版