區塊鏈與比特幣

區塊鏈（BLOCK CHAIN）

區塊鏈的特徵

- 去中心化
- 開放性
- 獨立性
- 安全性
- 匿名性

去中心化

- 不依賴額外的第三方管理機構或硬體設施，沒有中心管制，除了自成一體的區塊鏈本身，通過分散式核算和存儲，各個節點實現了信息自我驗證、傳遞和管理。

開放性

- 基礎是開源的，除了交易各方的私有信息被加密外，區塊鏈的數據對所有人開放，任何人都可以通過公開的介面查詢區塊鏈數據和開發相關應用，因此整個系統信息高度透明。

獨立性

- 不依賴其他第三方，所有節點能夠在系統內自動安全地驗證、交換數據，不需要任何人為的干預。

安全性

- 只要不能掌控全部數據節點的51%，就無法肆意操控修改網路數據，這使區塊鏈本身變得相對安全，避免了主觀人為的數據變更。

匿名性

- 除非有法律規範要求，單從技術上來講，各區塊節點的身份信息不需要公開或驗證，信息傳遞可以匿名進行。

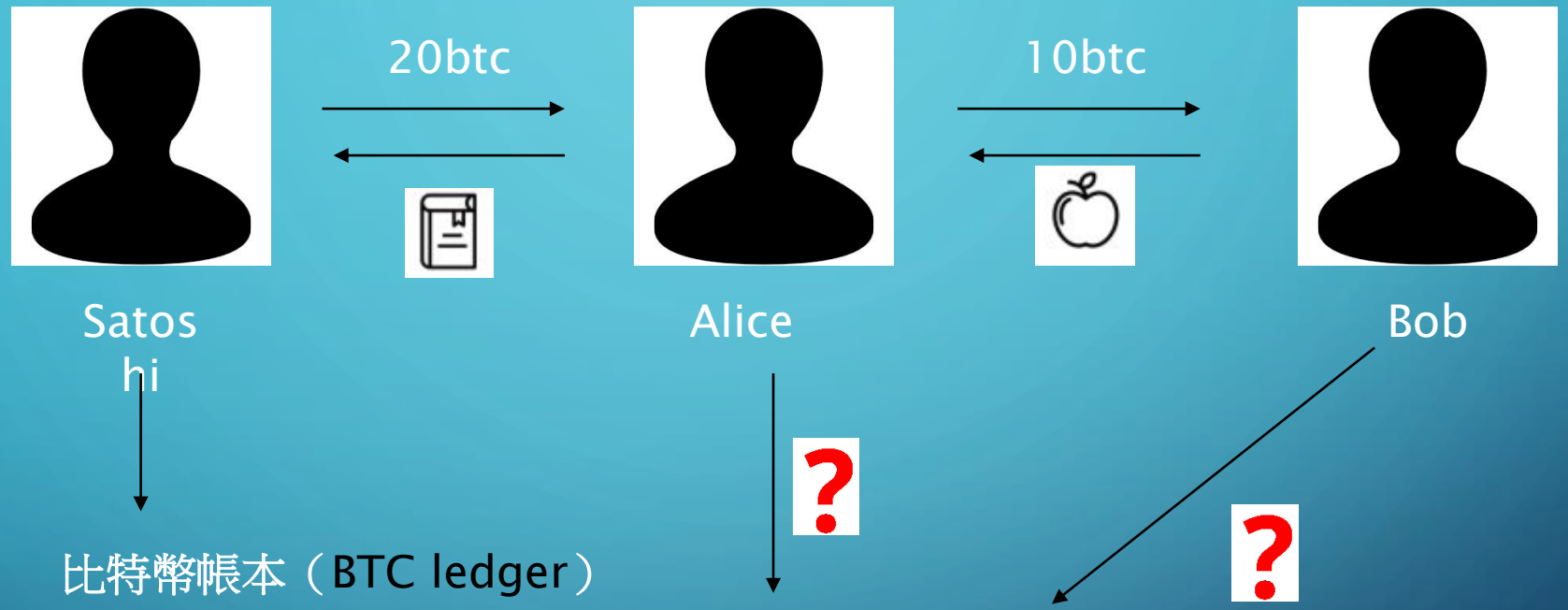
比特幣(BITCOIN)

起源

發明人：中本聰（Satoshi）

在 2008 年發表了一篇名為《比特幣：一種對等式電子現金系統》（Bitcoin: A Peer-to-Peer Electronic Cash System）的論文，提出了稱為「比特幣」的電子貨幣及其演算法

運作方式



收款人	交易金額	交易項目
Alice	20btc	書本
Bob	10btc	蘋果

運作方式

Satos

Alice

Bob

Node S

Node A

Node B

收款人	交易金額	交易項目
Alice	20btc	書本
Bob	10btc	蘋果

收款人	交易金額	交易項目
Alice	20btc	書本
Bob	10btc	蘋果

收款人	交易金額	交易項目
Alice	20btc	書本
Bob	10btc	蘋果

網際網路
Internet

特性

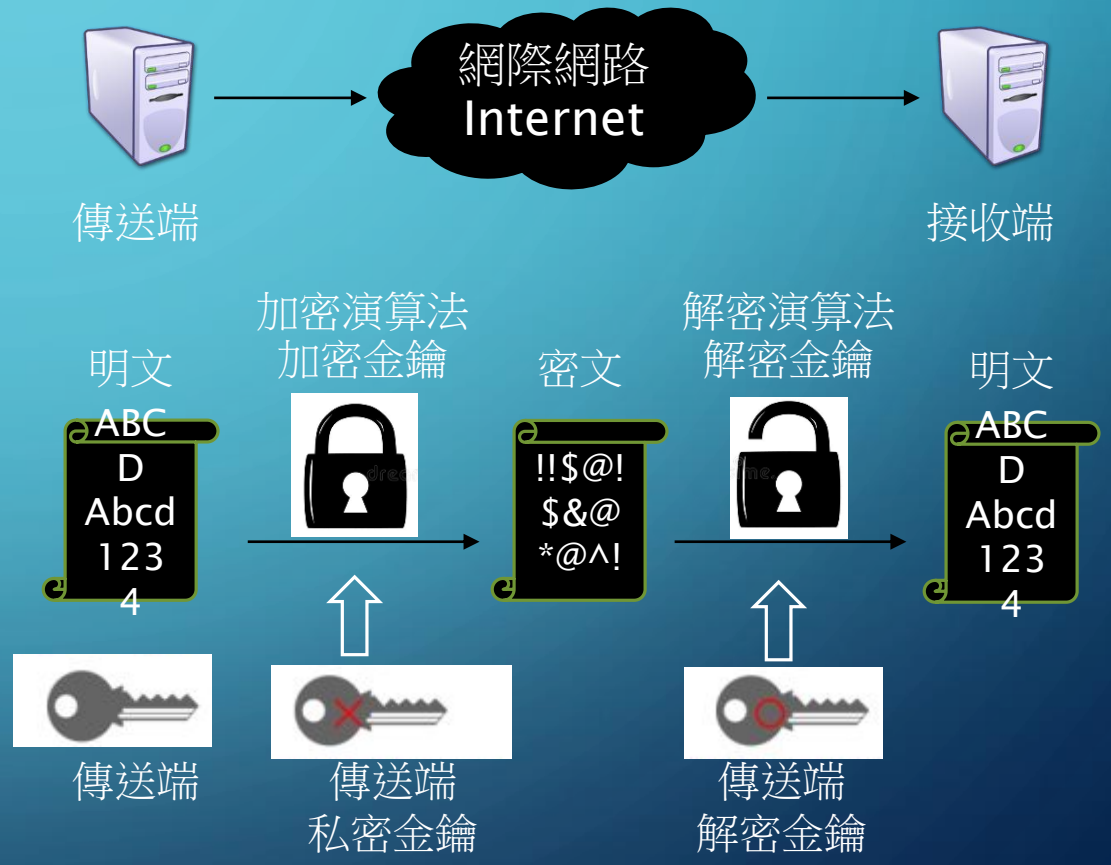
- **交易識別確認**：使用數位簽章驗證機制，確認這筆交易的真實性，使用者不可否認，而且是屬於「可驗證的匿名制」。

- **資料無法篡改**：使用「區塊」與「鏈結」確保交易資料無法篡改。其中「區塊」主要是利用「條件雜湊」（Conditional hash）確保傳送資料不被駭客篡改，由於篡改區塊內的交易資料已經很困難，區塊與區塊之間又被鏈結起來，等於篡改一個區塊要把所有的區塊都一起篡改，因此在合理的時間內根本不可能。

- **節點資料同步**：使用「工作量證明」（POW：Proof of Work）達成收斂同步，。

交易識別確認

- 每一位使用者必須自行產生自己所擁有的金鑰對（Key pair），包括一把「私密金鑰」（Private key）與一把「公開金鑰」（Public key），加密與解密使用不同的金鑰，使用者必須祕密地保存自己的私密金鑰，並且在網路上發表公開金鑰。公開金鑰可以用來加密，也可以用來驗證，驗證的流程如圖所示，傳送端使用自己的「私密金鑰」對文件（明文）進行加密（簽署文件）產生密文再傳送到網路中，接收端使用傳送端的公開金鑰解密（確認簽署者）得到明文，如果可以解密代表確認文件真的是傳送端的某人傳送出來的，數位簽章就是使用這種方式來驗證文件的真偽。



雜湊演算法（HASH ALGORITHM）

- 雜湊演算法是將任何長度的資料轉換成「雜湊值」。某一段資料對應到某一個雜湊值，不同資料具有不同雜湊值，就好像不同人具有不同指紋一樣，所以稱為「數位指紋」（Digital fingerprint），我們可以利用雜湊值來確認資料有沒有被篡改。

參考文獻

- http://wiki.mbalib.com/zh-tw/%E5%8C%BA%E5%9D%97%E9%93%BE
- http://newjust.masterlink.com.tw/HotProduct/HTML/Basic.xdjhtm?A=PA321-1.HTML
- https://finance.technews.tw/2017/05/11/block-chain-principle-and-application-bitcoin-pt1/
- https://finance.technews.tw/2017/05/17/block-chain-principle-and-application-bitcoin-part-2/