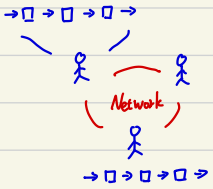
2008 後，出現了 blockchain 這個字詞，中本聰提出

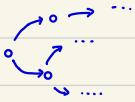
區塊鏈比較像是資料結構



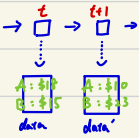
網路 → 為了傳遞訊息

- 網路 (Network) — Distributed-version blockchain

  Peer-to-Peer (P2P)：資源共享，人人都是 client 也是 server



- 資料結構 (Data Structure) (Ledger)



(能量守恆)

not good

- 一次性記了全部資料 不是件好事

A ↦ B (8)：改成記錄變化 (改變) better

- 演算法 (Algorithm)

  Node (in blockchain network)

  - 目的，e.g. earning money in BTC (Award)
  - 服務，為交易做服務，做銀行櫃員

Everyone provides services, but only one has the award !!

究竟誰能獲得獎勵

Proof-of-work，能力強

Proof-of-stack，資產強

Node-to-node：consensus（同識）

（DS, Algo, Network）

為什麼會能夠信任各個節點且各個節點自發不會亂搞？

因為他是為了這條鏈做事，使它有價值

將交易事件包裝成問題（很難），然後發包出去解題，最後得出一獲獎者

Hash Function

long input → short output

File → 🔒 → Hash value

Avalanche effect（雪崩效應）

使結果前後無關

Hash（Prev hash value, Root, Nonce）= $Prev\ hash_{(t)} <$ threshold

解答

算完後廣發解答

Time t-1

Hash（$prev\_hash_{(t-1)}$, $pack_{(t-1)}$, $nnce_{(t-1)}$）= $prev\_hash_{(t-1)}$ < threshold

用交易資料（block body）

Proof - of - work

one winner → other waste energy

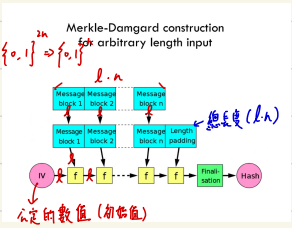
比算力

Proof - of - stack

會用力才決定誰來做運算，nobody waste

像是資產抵壓，多的人當

Hash Function 需要可以吃下任意長度字符，所以用方法壓縮



☆ 為什麼要做 length padding 這個動作？