Blockchain

- Network

- Algorithm (Cryptography)

- Data Structure (Format)

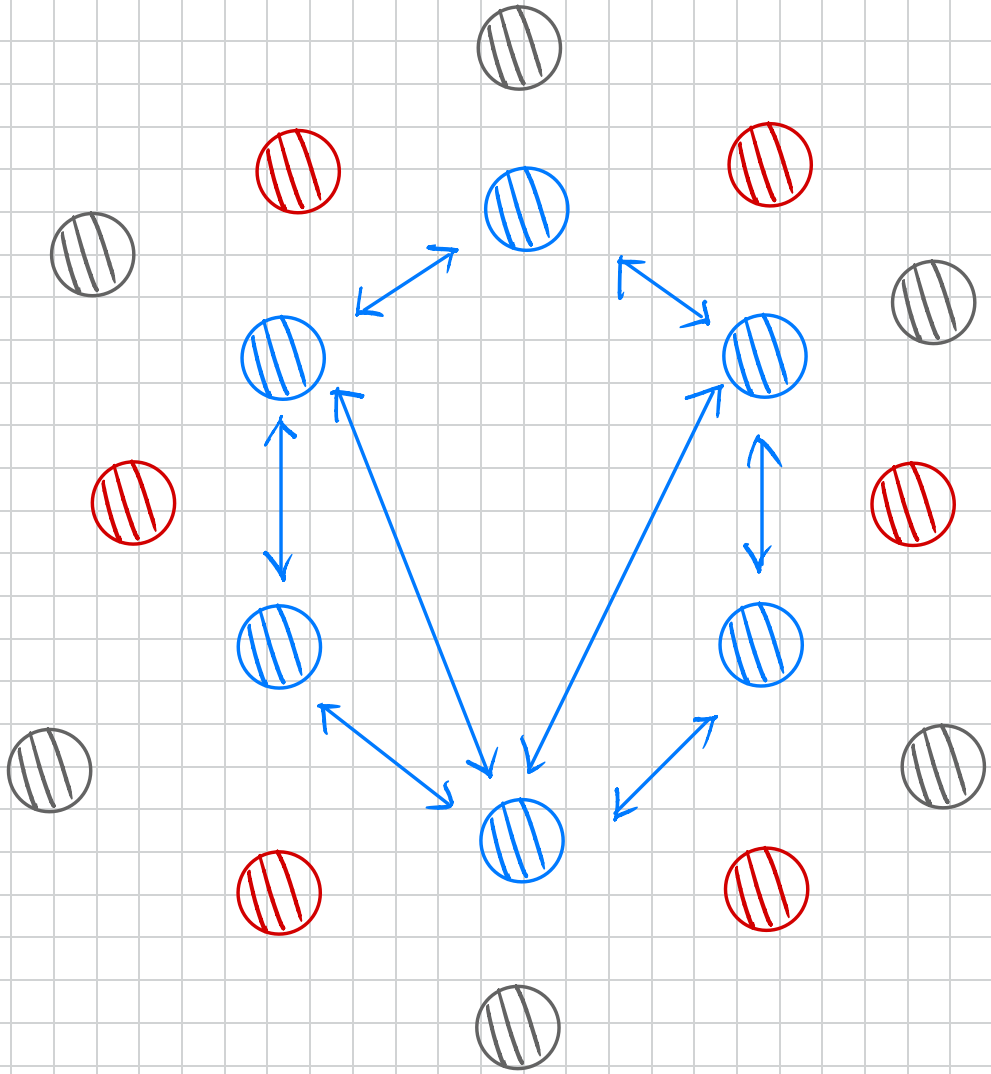
Network - level

Blue node : 積極型節點 (Peer - to - Peer)

Goal :

Red node : User

Grey node : 極少出現



Algorithm - level

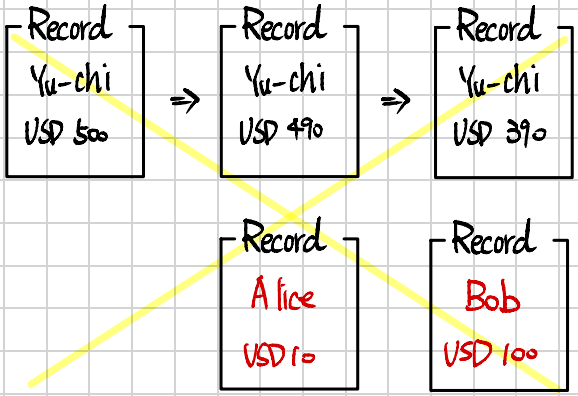
- Node

- Node's goal : Award

- Node's service : (provides services, but one has the award "each reward").

  Different service, different award.

Data Structure - level (Ledger)



Yu-Chi → Alice (10)
Yu-Chi → Bob (100)

Ledger

Yu-Chi (500) → Alice (10)
→ Yu-Chi (490)

Bitcoin
(2025) 616 GB,
(2017) 250 GB,
(2009) 0 GB

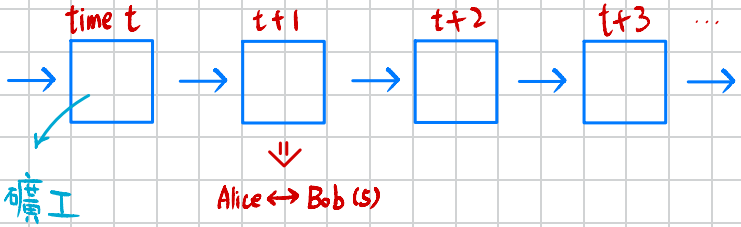
Date: Feb 25, 2025

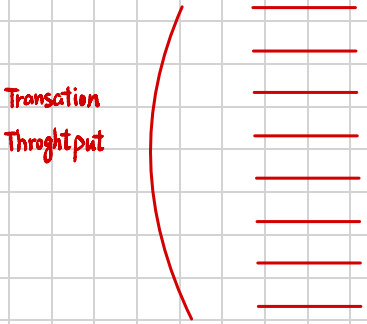
time T.

time 0 ~ time T-1

time T-6

Search Yu-Chi records. → NTUT → Yu-Chi (500)

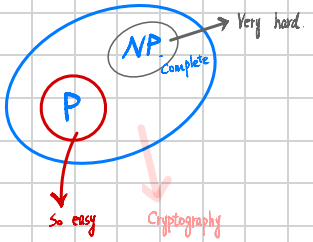




Each round

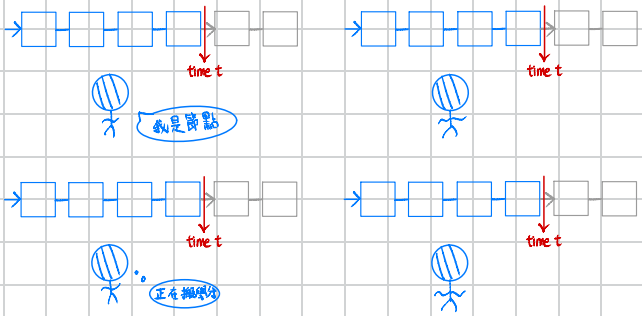
1. A new block is generated.
2. A miner (blue node) wins the award.

Puzzle



Early stage design of many blockchains use puzzle to decide the winner.

Decentrailized Ledger 去中心化



- Blocks before t are identical in every node.
- Blocks after t may not.

Hash Functions (Collision - resistant functions)

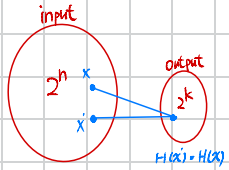
Give H, it's hard to find $H(x)=H(x')$ where $x \neq x'$

(one-way functions)

Give $H(x)$, it's hard to find x.

Hash function is a "compression" function.

↓ discuss collisim.

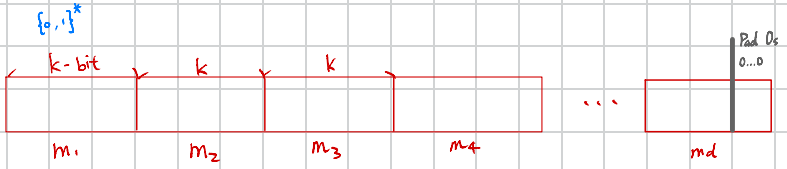


$n>k$

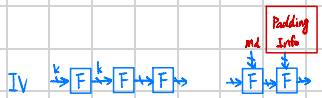
$H: \{0,1\}^* \to \{0,1\}^k$: Usually, $H: \{0,1\}^* \to \{0,1\}^k$ is used to build H in practice.

arbitrary length input

k bit output



Write down the length of input.



k=4

If no recording (a) 00000 1 ⇒ m_1, m_2 00000 1 00 with padding info

padding information (b) 00000 1 00 ⇒ m_1, m_2 00000 1 00

"Merkle-Damgard Transformation"