Algorithm - level

2/25

3/4

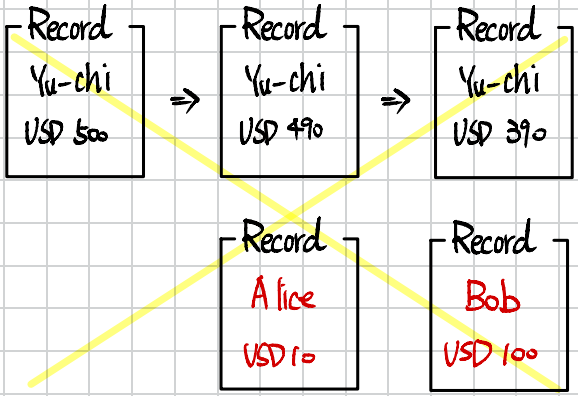
- Node

- Node's goal : "Award" Incentive model 激勵機型

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

  Different service, different award.

Data Structure - level (Ledger)



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

Ledger

Yu-Chi (~~500~~) → Alice (10)

other Info → Yu-Chi (490)

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

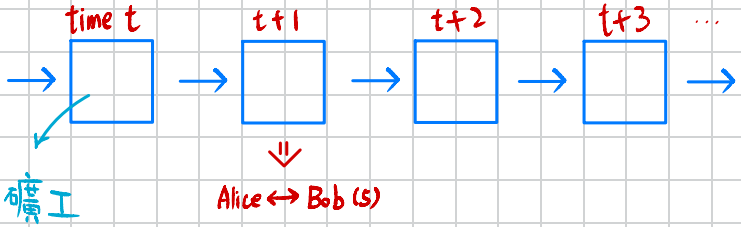
Date: Feb 25, 2025

time T.

time 0 ~ time T-1

time T-6

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

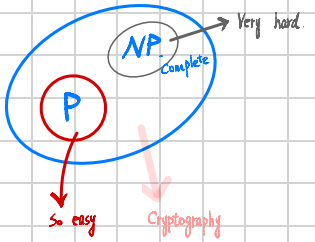


Each round

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

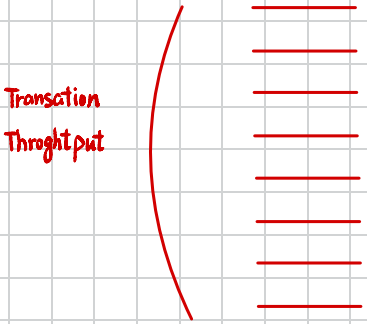
有時間序列的關係

Puzzle

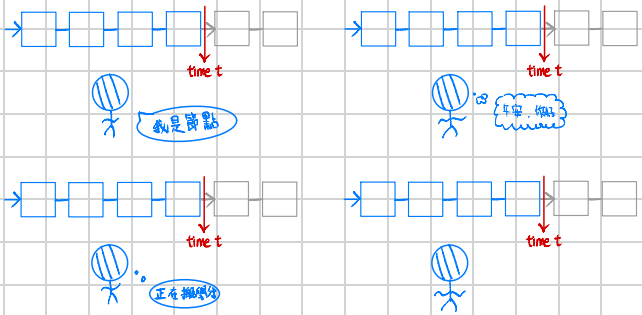


Early stage design of many blockchains: use puzzle to decide the winner.

Crypto: Cryptography ***
Cryptocurrency ********



Decentrailized Ledger 去中心化



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

Hash Functions (Collision - resistant functions)

Compression

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

hash value, hash code, fingerprints

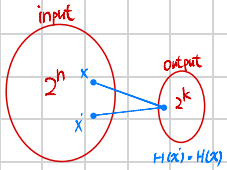
(one-way functions)

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

難題 Puzzle

Hash function is a "compression" function.

discuss collisim.

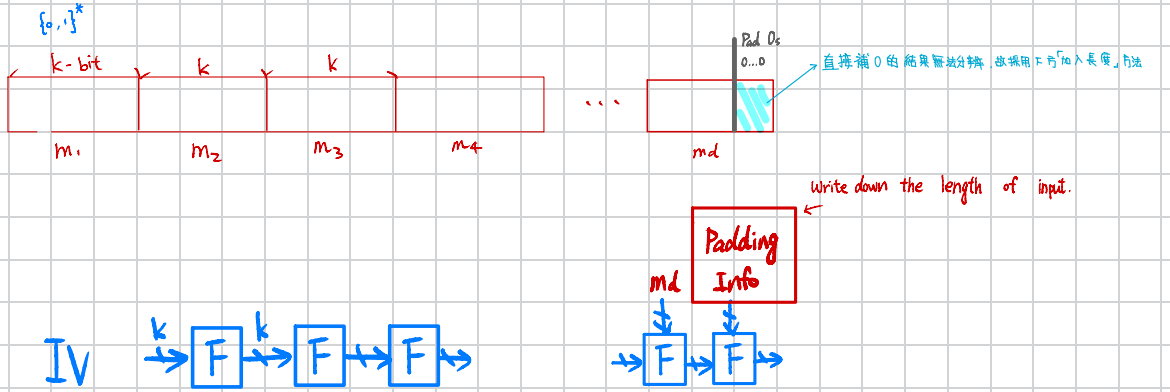


$n>k$

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

arbitrary length input (in poly many)

k bit output



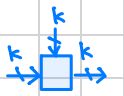
If no recording padding information (k=4)

(a) 00000 1 ⇒ m_1, m_2 → 00000 1 00 ❌

(b) 00000 1 00 ⇒ m_1, m_2 → 00000 1 00 ✅

with padding info

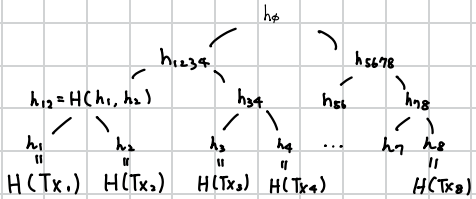
Padding info

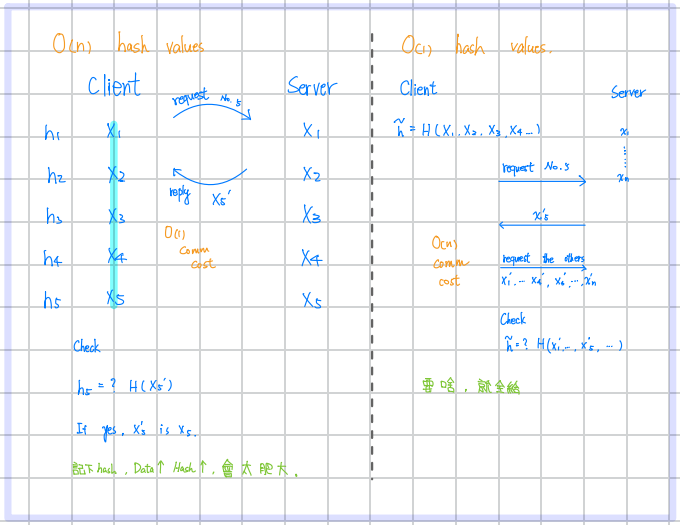


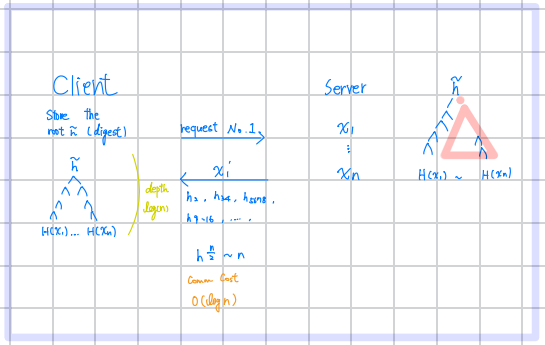
$\binom{k}{0\ldots0}$ to $\binom{k}{1\ldots1}$: 0 to 2^k-1 不用擔心，不會爆炸

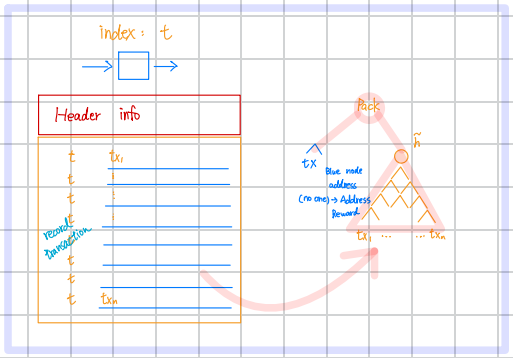
"Merkle-Damgard Transformation"

Merkle Tree









Puzzle [BitCoin Wining Condition]

If all txs are verified and ① find a nonce.

such that

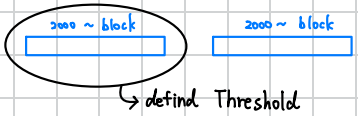
H (Prev_block_hash_value , Pack , Nonce) < Threshold

(Prev_block_hash_value: deterministic; Pack: deterministic)

For a slot (2000 ~ blocks)

Threshold is adapted via (previous 2000 ~ blocks info)

2000 個 block 調整一次



Digital Signature

1. tx generation by (address) who hold coins.

2. verification of tx really from

m : msg
σ : signature

Syntax of Digital Signature.

- Gen(a) → sk, vk ← verification key
  sec parameter
  ↓ signing key
- Sig(sk, m) → σ
- Vrfy(vk, m, σ) → accept / reject

sk
↓
vk ⟷ address

Signature
- Authentication : Verify m from S.
- Integrity : m is not modified.
- Non-repudiation : cannot withdraw the sig.