Road map:

Bitcoin Protocol
(blockchain networks)

0. Introduction
   - technology and design = <u>decentralized digital currency</u>
   - something about economics, but not crypto stock market.
   - history - 1997 hashcash by Chaum } centralized
     - 1998 B-money by Dai }
     - 2008 Bitcoin by group of people - decentralized

1. Network model - Byzantine environment
2. from centralized DC to decentralized DC.
3. Blockchain network
4. Blockchain (data structure)
5. Proof of Work
6. Incentives and economics

1 Byzantine Generals Problem → Byzantine Enviroment

In distributed system nodes deviate from their expected behavior.

- honest nodes

- faulty: power problem, bug in software, ...

- malicious nodes toward gain

- malicious nodes toward disturbing

- fail to deliver, duplicate, delay, out of order

Practical Byzantine Fault Tolerance Consensus Algorithm

$$t < \left\lfloor \frac{n-1}{3} \right\rfloor$$

n - total nodes

t - byzantine nodes

only for permissioned systems

②

Centralized: 1. „Alice sends a coin to Bob" - all attacks

↓ PKI, DSA

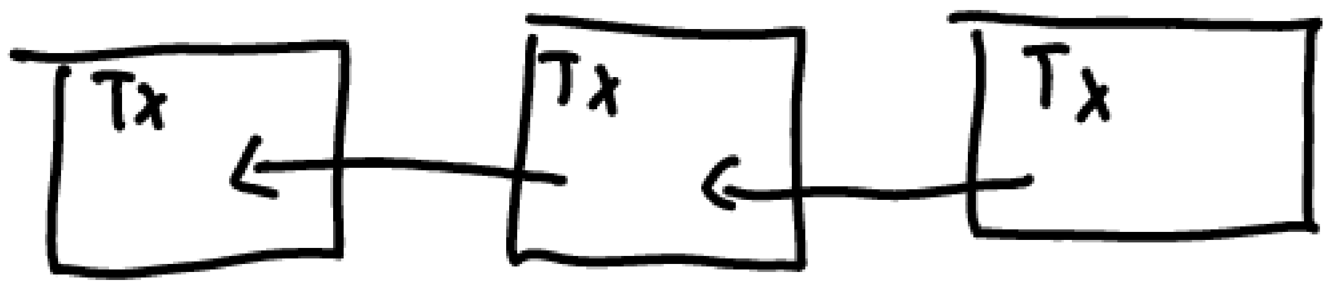
2. („PK_A sends a coin to PK_B", σ_A) - replay

we need id on coins

↓ id coins

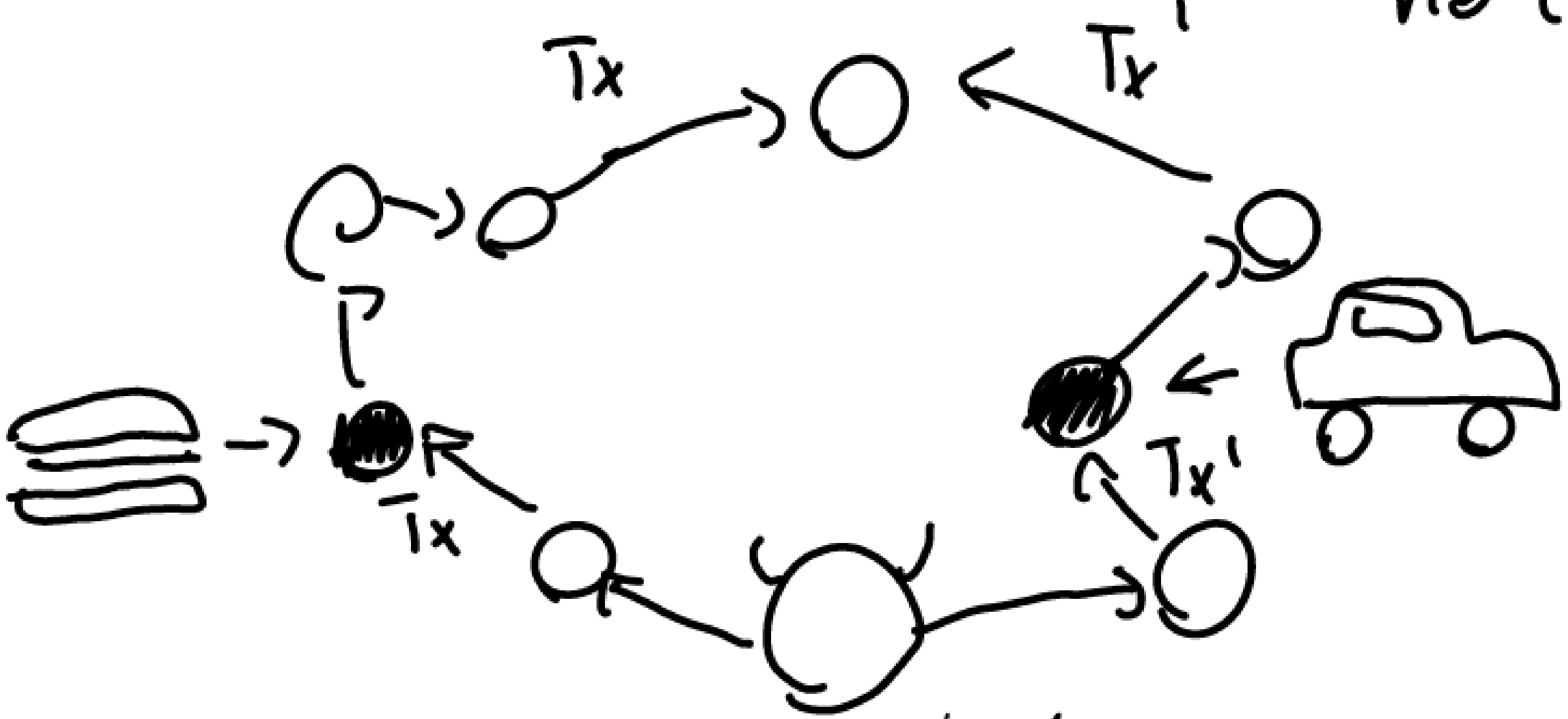
3. („PK_A sends ID_{coin} to PK_B", σ_A)

- -

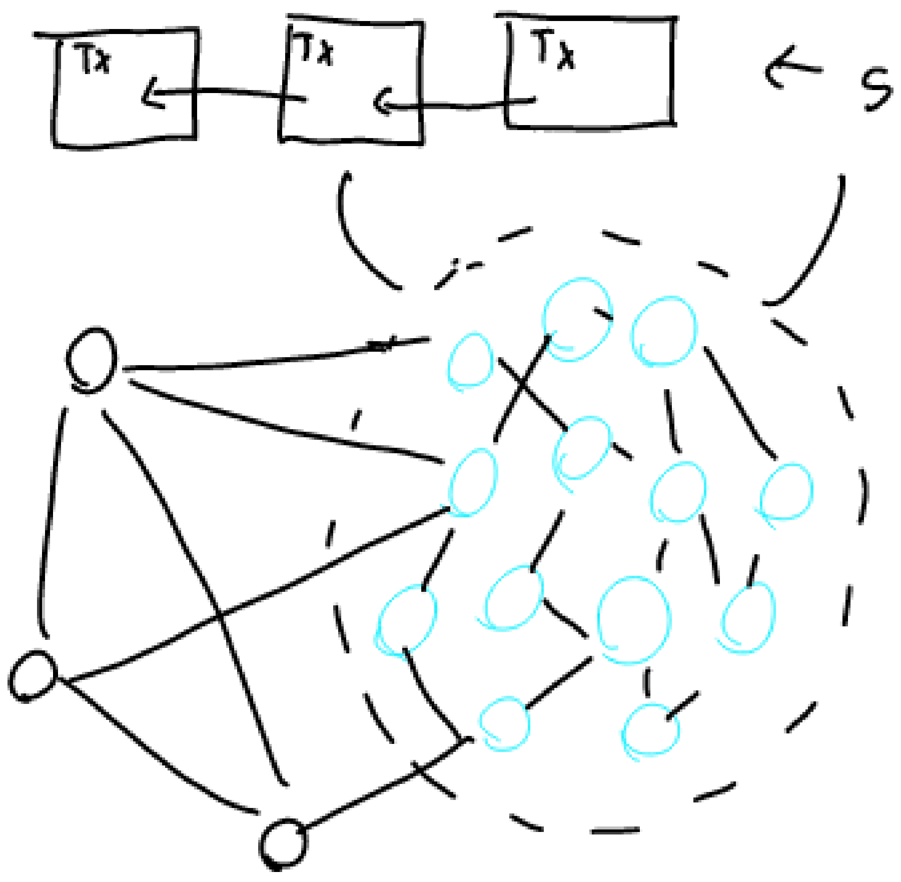
Decentralized: 4. 

- double spending

no central authority



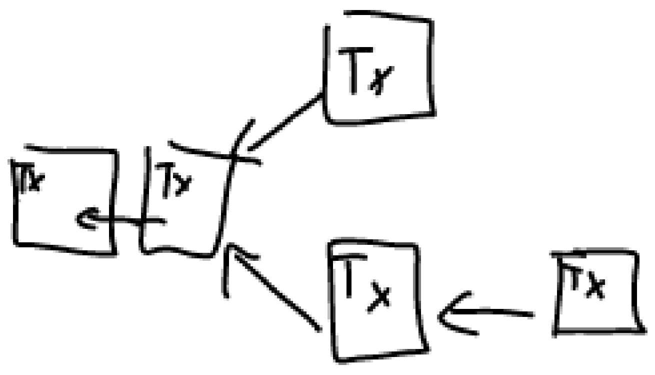
↓ random leader election

5. 

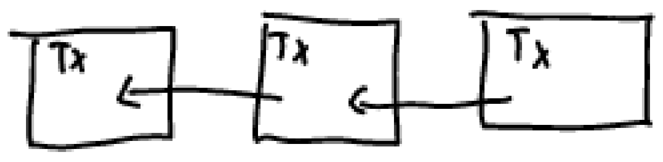
← sybil attack

many entities attack

↓ consensus mechanism (PoW)

6. 

↓ longest rule

7. 

↓ incentive

8. Bitcoin

③

Blockchain network architecture;

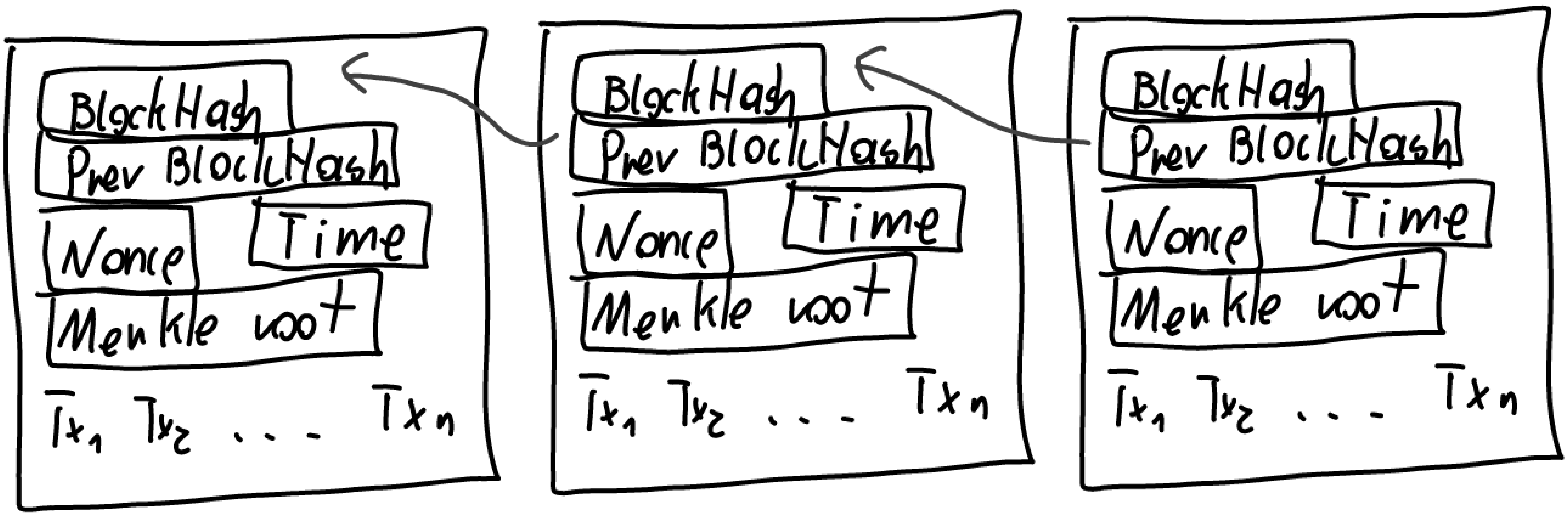
- Application layer - Cryptocurrencies, distributed Apps (Ethereum)
- Global State Machine layer - Services provided by distributed nodes (VMs)
- Consensus Mechanis Layer - Byzantine Fault tolerant Protocols
- Data and Network Organization Layer - Storage for Ledger Replica (Blockchain) and P2P Network protocols.

④ Blockchain data-structure

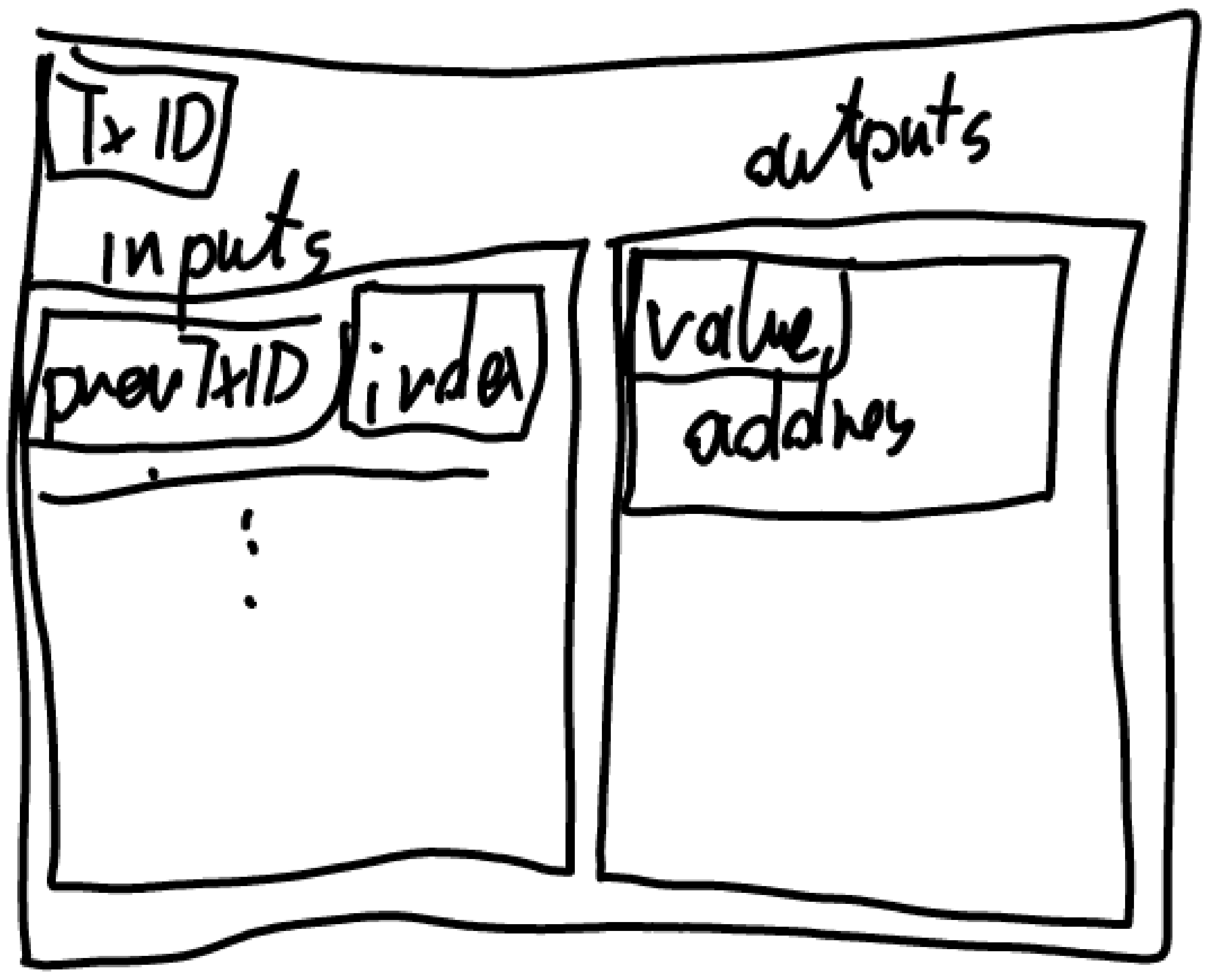
- linked-list
- order persistant

+ timestamping

Block:



Transaction:



- Unspent Transaction Output
- Spent Transaction Output
- change by making transaction to self

⑤ PoW having resource is proof of existing.

consensus mechanism as weighted leader election

$$\Pr[L = i] = \frac{w_i}{\sum_{j \in N} w_j}$$

$x = \text{str(block)}$ artificialy increasing cost

z = difficulty level

$D(n) = 2^{l-n}$, where l - is hash length

then hash inverse problem is finding such n that

$$\mathcal{H}(n \| x) \leq D(z)$$

z number of zeroes at hash

$T(\text{solution\_search}) = N$

$T(\text{validation}) = 1$

achieves $f \leq \left\lfloor \frac{n-1}{2} \right\rfloor$

⑥ Incentive

- block reward
- transaction fees.