Blockchain Fundamentals

Main elements

- Cryptography
- Distributed networks
- Game theory

Cryptography

- The study of the principles and techniques by which information can be transformed from its original form to an unreadable one.
- Information can be known only to its recipient (holder of the “secret key”).
- Difficult to read by an unauthorised person.
- Only the recipient of the message can read the information easily.
- It is a branch of mathematics, part of cryptology.

Cipher-text

$$Ci = E(Pi) = Pi + 3$$

Plaintext : A - Z

Ciphertext : Start at d and end at c

Cryptography in blockchain

- Hash function
- Public key and private key
- Merkle tree

Hash function

It is algorithm that maps variable - length Dara to fixed - length data.

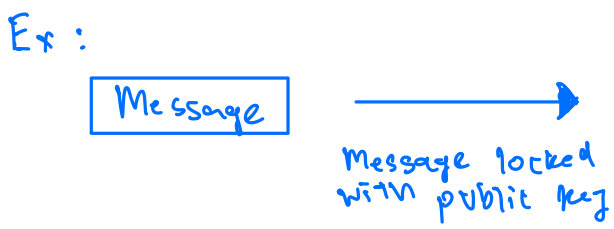
- Each hash is deterministic = same text or document will generate the same hash every time.
- Fast
- One way: from the hash it is not possible to return to the original.
- Small change in the input generates a completely different hash (it seems random).
- Collision resistant: two documents do not generate the same hash (depending on hash algorithm).

Public key and private key

- **Cryptography key** there are two types of cryptography keys

  A. Symmetric (single - key encryption)

  B. Asymmetric (pair - key encryption) This one is use in Blockchain.



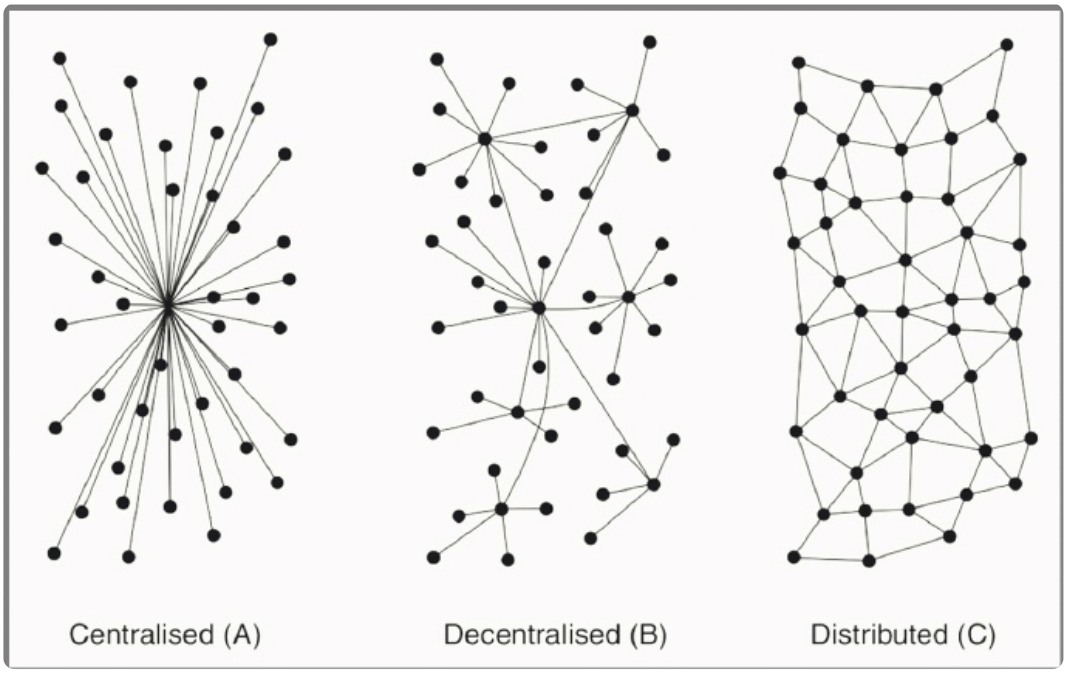
- Only private key holder can read
- Message could be from anyone
- Role can be switched

- **Public key and private key in Blockchain**
  - *Cryptography*
    - Anyone can encrypt a message using the recipient's public key.
    - Only the private key owner can decrypt messages encrypted with the corresponding public key.
  - *Authentication*
    - Only the private key owner run sign / authorise transactions (digital signature).
    - The public key confirms the sender's identity, verifying that the private key holder sent the message

- **Merkle tree** :

“ it is used to summarise all the transactions in a block, producing an overall digital finger prime of the entire set of transactions, providing a very efficient process to verify whether a transaction is included in a block” - according to Andreas M. Antonopoulos, in “ the Bitcoin protocol”yy

Distributed Networks



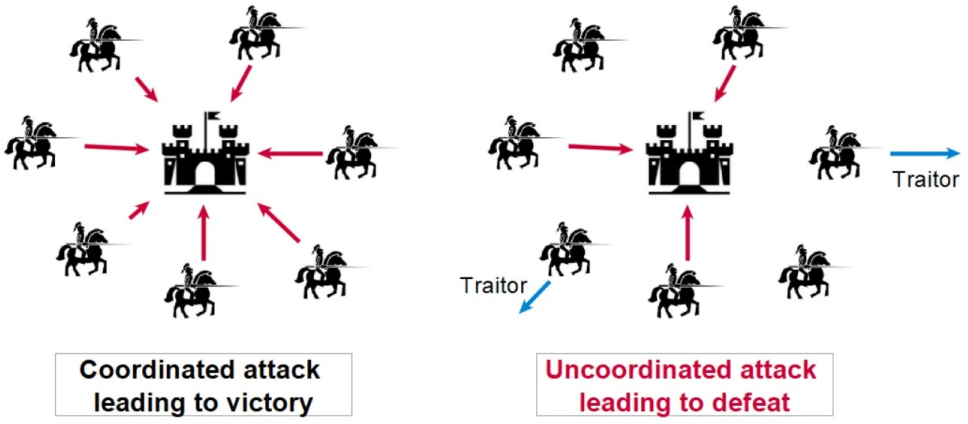
Game Theory

- Study of decision making between individuals.
- Outcome of each depends on the decisions of the others.
- Game-like interdependence.
- "Probabilities" in decision making

Game theory in blockchain

Interaction between participants in the blockchain ecosystem and their incentives to behave honestly.

- **Byzantine General Problem**



  - Armies must attack together to win
  - Messages can be intercepted or generals can be dishonest.
  - How do decentralised parties agree on consensus without a trusted centralised party?

- **Consensus**

  - Mechanism to ensure that all preppies agree that a certain state of the system is correct
  - The truth
  - Consensus mechanisms are based or game theory

  A. **Proof of work (PoW)**

    a. Concept by Cynthia Dwork and Moni Naor in 1992 in the paper “Pricing via Processing, or, Combatting Junk Mail, Advances in Cryptology”

    b. Name by Markus Jakobsson in 1999 in the paper “Proof of Work and Bread Pudding Protocols”

    c. Asymmetry:

      1. Requires a significant amour of computational effort to solve a puzzle or perform a certain task.
      2. Verging that the work has been done is relatively simple and quick.

d. It ensure that participants in the network agree on the state of the ledger (i.e., the order and validity of transaction) through a process that involves solving complex cryptographic puzzles.rerreuii

e. “Miners” do mathematical calculations on their computers to verify that the transactions are valid.

f. Mining comes from trial and error of finding a nonce (random number) that satisfies the degree of difficulty of the network.

g. Difficulty ensure that the process of adding new blocks to the blockchain requires a significant amour of computational work. This makes it economically infeasible for malicious actors to manipulate the blockchain.

B. **Proof of Stake (PoS)**

a. Know as proof of participation

b. To participate in the validation, the amount of coins that the validator has is used, instead of the computational power.

c. The validator must place his deposited coins in a kind of safe to "prove" his participation, without moving the coins.

d. The more coins you have the greater the chance of validating transactions and earning from them.

e. In terms of energy, it is more economical than PoW.

f. It should bring more security and decentralisation, but it makes lager coin holders more likely to set more coins.

C. **Proof of Authority (PoA)**

a. Used in permissioned blockchain

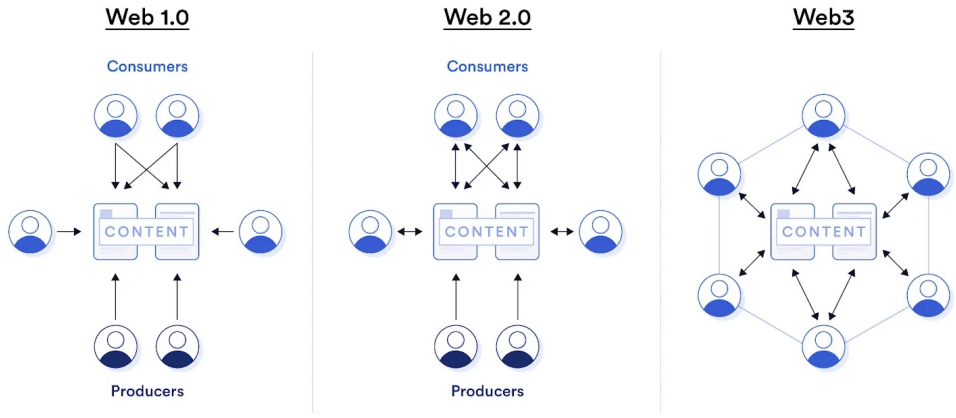
b. Group of “authorities”

c. Specific nodes are defined and authorised to create new blocks in a chain.

d. It needs approval from most of the nodes for the block to be created.

e. Used in private Ethereum networks and others.

Web3



Wallet in web3

- Key manager used to manage your cryptocurrencies or tokens.
- Authorise transactions and interact with web pages or decentralised applications.
- Subscribe to messages demonstrating that you own a wallet address.