Distributed System : BitCoin & BlockChain

Houmin Wei

Electronics Engineering & Computer Science
Peking University

北京大學
PEKING UNIVERSITY

December 13, 2017

Talks about crypto.

Cryptography

- Cryptography is the science of secret, or hidden writing
- **Privacy/confidentiality**
  - Ensuring that no one can read the message except the intended receiver
- **Authentication**
  - The process of proving one's identity
- **Integrity**
  - Ensuring that a message has not been surreptitiously altered
- **Non-repudiation**
  - A mechanism to prove that the sender really sent this message
- **Key exchange**
  - The method by which crypto keys are shared between sender and receiver

Encryption: Cipher

- Cipher is a method to encrypting messages
- Encryption algorithm are standardized and published
- The key
    - Key is a string of numbers of characters
    - Symmetric(same key is used for encryption/decryption)
    - Asymmetric(different key for encryption/decryption)

SKC, Secret Key Cryptography

- Block Cipher
- Stream Cipher
- DES, AES, IDEA

PKC, Public Key Cryptography

- RSA
- Diffie-Hellman
- ECC

Hash

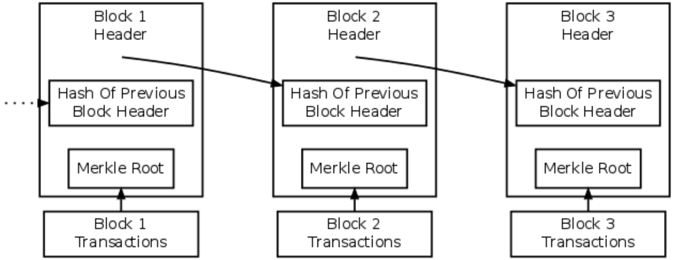
- MD5
- SHA-1
- SHA-2

SSL/TLS

PGP

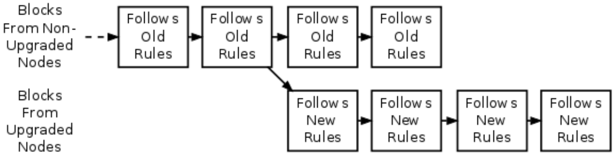
- The block chain provides Bitcoin's public ledger, an ordered and timestamped record of transctions.
- This system is used to protect against double spending and modification of previous transactions records.
- Each full node in the Bitcoin network independently stores a block chain containing only blocks validated by that node.

Block Chian Overview



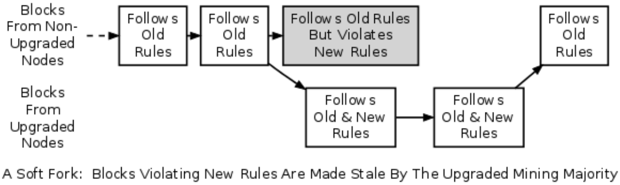
Simplified Bitcoin Block Chain

Hard Fork



A Hard Fork: Non-Upgraded Nodes Reject The New Rules, Diverging The Chain

Soft Fork


Blocks From Non-Upgraded Nodes
Blocks From Upgraded Nodes
Follows Old Rules
Follows Old Rules
Follows Old Rules But Violates New Rules
Follows Old & New Rules
Follows Old & New Rules
Follows Old Rules
A Soft Fork: Blocks Violating New Rules Are Made Stale By The Upgraded Mining Majority