Block Chain Technology (Architecture)

Dr. Siddhartha Roy

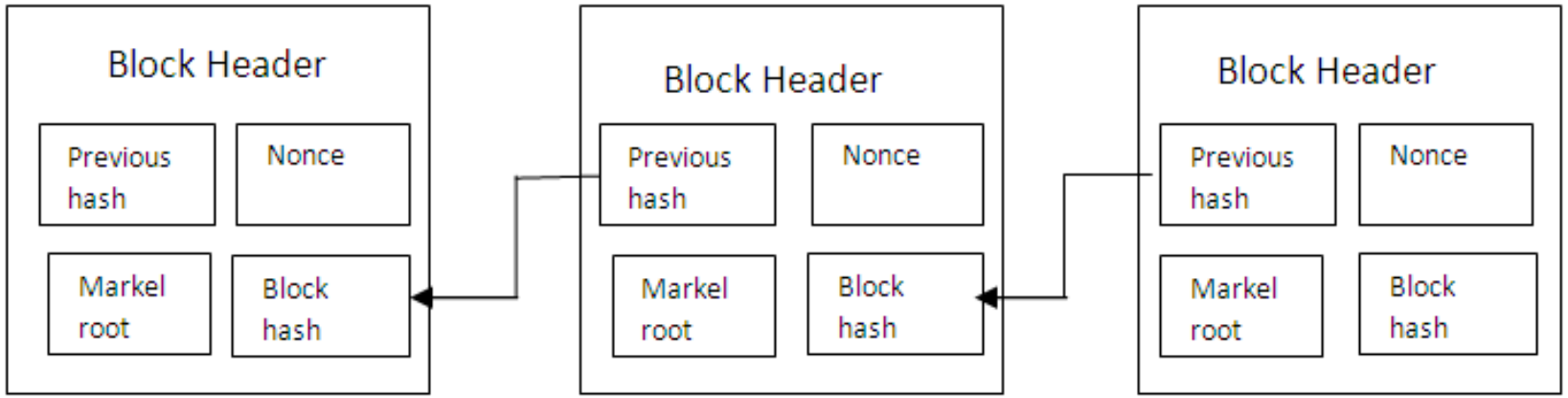
Block Chain Architecture

- Basic assumption
- Multiple organizations or individuals spanned over who may not **trust** each other
- An append-only shared ledger of digitally signed and encrypted transactions replicated across a network of peer nodes
- Digitally signed and encrypted transactions “verified” by each peers

Structure of a Block

- A block is a **container data structure** that contains a series of transactions
- **In Bitcoin:** A block may contain more than 500 transactions on average, the average size of a block is around 1 MB (an upper bound proposed by Satoshi Nakamotoin 2010)
- May grow up to 8 MB or sometime higher
- Larger blocks can help in processing large number of transactions in one go.
- But longer time for verification and propagation
- Two components:
- **Block Header**
- **List of Transactions**

Block chain

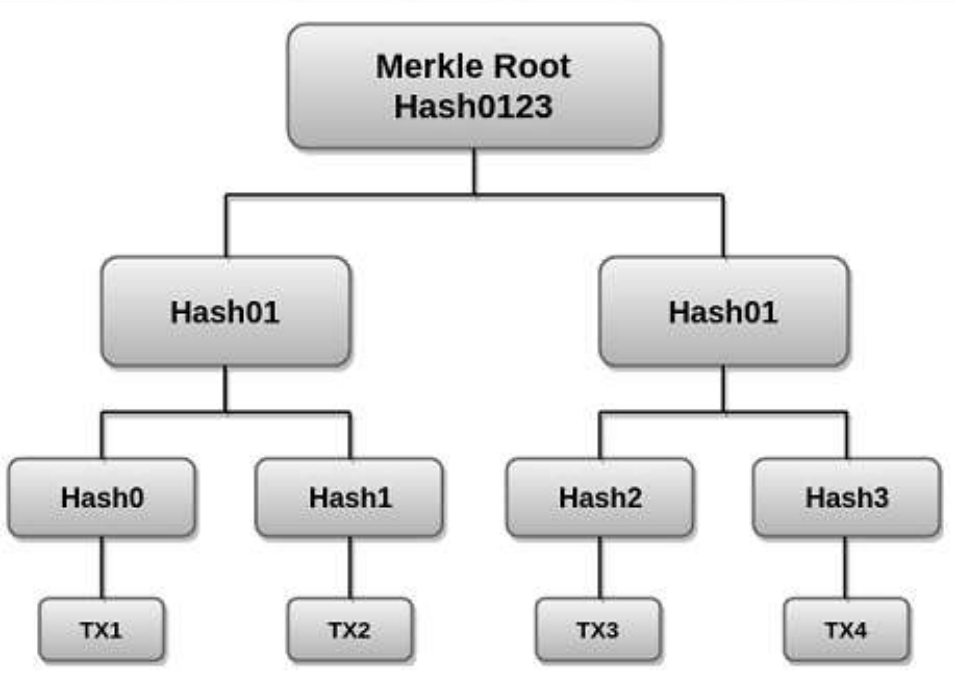

Block Header
Previous hash
Nonce
Markel root
Block hash
Block Header
Previous hash
Nonce
Markel root
Block hash
Block Header
Previous hash
Nonce
Markel root
Block hash

- Block hash
- Previous block hash: Every block inherits from the previous block –we use previous block's hash to create the new block's hash –make the blockchain **tamper proof**
- Merkletree root
- Nonce

Markle tree

- Merkle tree is a **data structure** composed of hashes of different blocks of data, and which serves as a summary of all the transactions in a block. It also helps to verify the consistency and content of the data. Both Bitcoin and Ethereum use Merkle Trees structure. Merkle Tree is also known as **Hash Tree**.

Construction of Markle Tree



Source: https://www.javatpoint.com/blockchain-merkle-tree

Nonce

- Nonce is the central part of this Proof of Work. Nonce, short for “number used once”, is a random number that can only be used one time. Nonces are generated for a specific use, most often to modify the result of a function in a cryptographic communication.
- Typically, a nonce is a number that varies with time, in order to ensure that some values cannot be reused. It can be a timestamp or a special marker intended to prevent unauthorized reproductions of a file.

Some typical Application of Block chain Technology

Investment Management

Digital IDs (Passports, Personal IDs, Marriage Certificates)

Digitizing the land and property records

Supply Chain Management

References

- Cryptography and Network Security – Principles and Practice by William Stallings, Pearson (2017)
- Blockchain Basics: A Non-Technical Introduction in 25 Steps by Daniel Drescher, Apress (2017)
- Blockchain: Blueprint for a New Economy Paperback(2015) by Melanie Swa
- https://btc.com/btc/blocks
- https://www.businessinsider.com/blockchain-technology-applications-use-cases

- Thank you