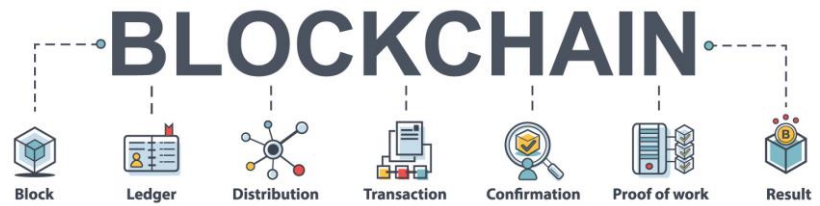
2021/2022(2)
IF184605 Framework-Based Programming

Lecture #12c

Blockchain: Data Management

Misbakhul Munir IRFAN SUBAKTI
司馬伊凡
Мисбакхул Мунир Ирфан Субакти

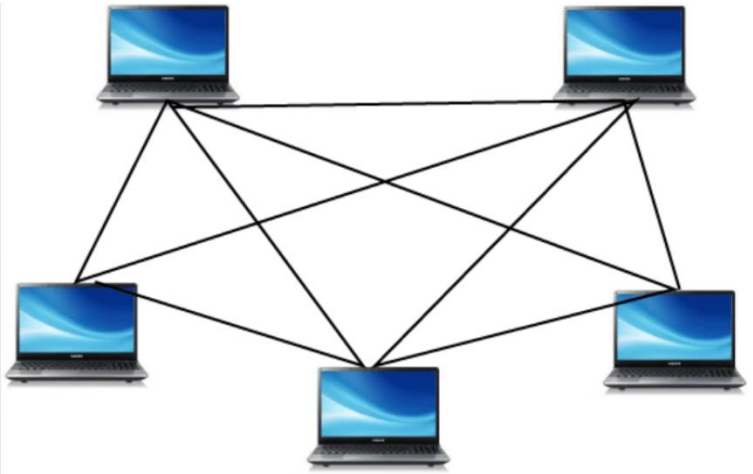


Blockchain: Basic & advanced concepts

- Link: https://www.javatpoint.com/blockchain-tutorial

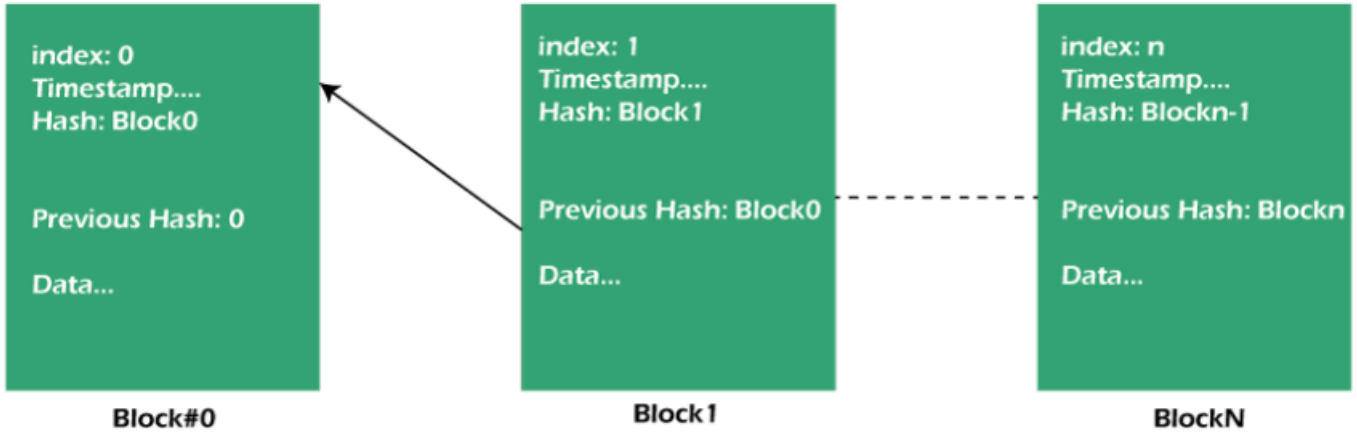
Blockchain: Distributed structure

- As we are aware, Blockchains are distributed structures that follow peer-to-peer networks and inherit the advantages of a peer-to-peer network such as speed, avoidance of single-point failures, etc.
- The below diagram gives an overview of the Peer-to-Peer networks.
- Each node is linked to each other and shares resources, meaning there is no dependence on central machines similar to the traditional client-server design.



Data management on chain

- We'll try to comprehend how data is stored on blockchains and the contents of every block on the blockchain. Each transaction is grouped into units, and each unit is called a **block**. We can refer to the following image:



Data management on chain (continued)

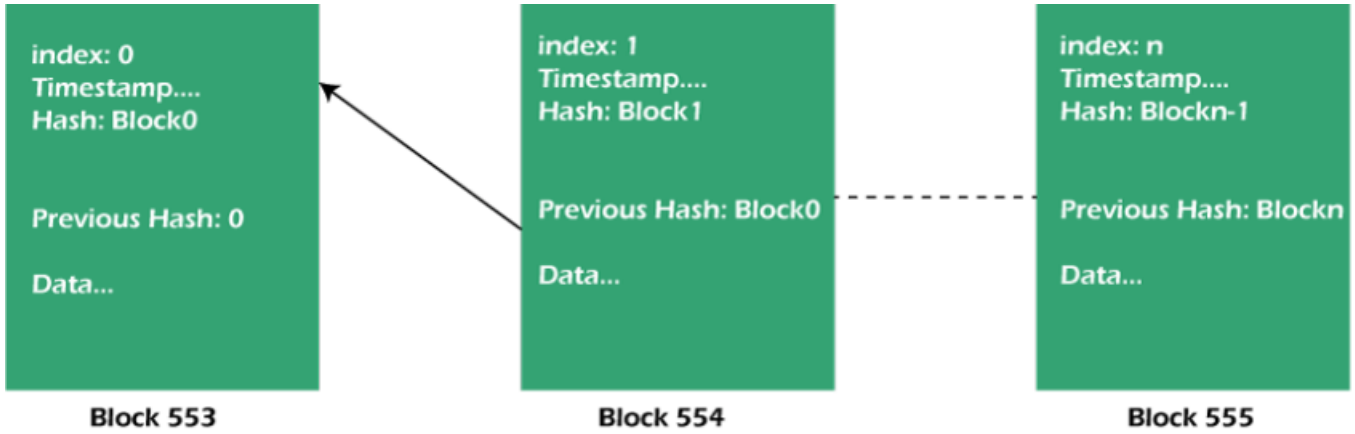
- In the above picture, some blocks have actual transaction information on them. Apart from transaction data, there are other common characteristics of every block that are like this:
  1. **Index:** The term ‘index’ is nothing more than a number that is a sequential block number.
  2. **Timestamp:** Date on the day that blocks the data was added.
  3. **Hash:** It is a unique hash value used to identify the information. It is created using mathematical formulas. Each block contains different hash values that directly communicate via data changed (i.e., if data changes, then it will be reflected in the hash value as well).
  4. **Previous hash:** It has values for the hash of previous blocks in order to gain references backward.

Blockchain: Immutability

- We all know that databases. Traditional databases are designed for **CRUD** (Create, Read/Retrieve, Update, and Delete) operations. However, blockchain is only able to append and retrieve, meaning that the data once added can't be removed or changed.
- In the blockchain, any node that has access to the ledgers can verify and check whether the ledger has been altered or if any transaction in any block has changed. This is typically performed by calculating the hash value of the block's data and then comparing it to the hash value of previous blocks in the next block.

Blockchain: Immutability (continued)

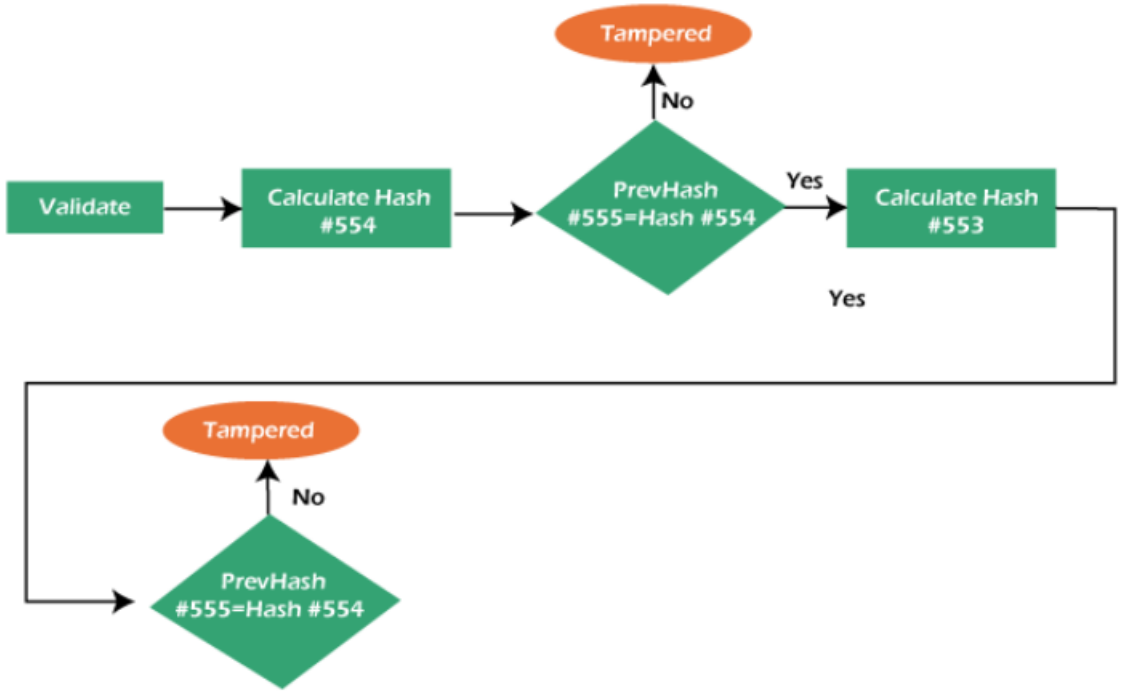
- E.g., here is the Blockchain, which shows the latest block, Block#555.



- The peer or node here can determine the hash value of block#554 as well as determine whether the hash value for block#555 is the same as the value for block#554. If it's not, the block is declared compromised. The image below illustrates the verification process.

Blockchain: Immutability (continued)

- If the data is altered and invalid validation fails, rejection of a block will occur by all nodes.
- Blockchain uses the consensus (general agreement) method to validate the transactions.



Blockchain: Consensus

- It's a method whereby peers agree to the current state of the ledger. It makes sure that all peers share the same copy of the ledger. Fraudulent transactions are kept off the ledger. It also ensures that it records transactions in chronological order.
- Here is a brief description of the consensus protocols that are common to all.

Proof of Work (PoW)

- **Proof of Work** (PoW) as the name implies, it's the confirmation of the work done and the proof that it is accurate. This is the method of consensus to ensure that the chain's authenticity is valid.
- The major drawback of PoW is that it demands more electrical power and high-end computing hardware, which can be expensive.

Proof of Stake (PoS)

- The **Proof of Stake** (PoS) is a different method of confirming and verifying the block or transaction. PoS chooses the validator according to the stake that the validator holds and their age of stake. In PoS, the validated player earns the entire or a portion from the fee for transactions.
- PoS eliminates the biggest issues with PoW and is believed to have an advantage since there's no need for expensive hardware. It is also energy efficient because it doesn't draw as much power as PoW.

Tendermint

- The **Tendermint** is an open-source project designed to tackle scaling, speed as well as environmental issues of Bitcoin's Proof-of-Work consensus algorithm. It utilises the BFT (Byzantine fault-tolerant consensus) algorithm.
- The Bitcoin, as well as Ethereum blockchain networks, use Proof of Work (PoW).