Blockchain Structure

Blockchain is a Distributed Ledger Technology. It is a distributed and decentralized database and it is secured ever as compared to other technologies.

What is Blockchain Architecture?

Blockchain is a technology where multiple parties involved in communication can perform different transactions without third-party intervention. Verification and validation of these transactions are carried out by special kinds of nodes.

Benefits of Blockchain:

- It is safer than any other technology.
- To avoid possible legal issues, a trusted third party has to supervise the transactions and validate the transactions.
- There's no one central point of attack.
- Data cannot be changed or manipulated, it's immutable.

1. Block Structure

A blockchain is composed of a series of blocks, each containing key elements that ensure its function within the blockchain network.

a. Block Header

The block header contains metadata about the block and is crucial for linking blocks together:

1. **Version**: Indicates the version of the blockchain protocol used. This helps ensure compatibility with various software versions.
2. **Previous Block Hash**: The hash of the previous block's header. This links the current block to the previous one, creating a chain. This field ensures the immutability of the blockchain by making any tampering detectable.
3. **Merkle Root**: A hash of all transactions included in the block. This is derived from the Merkle Tree, a binary tree structure where each leaf node is a hash of a transaction, and each non-leaf node is a hash of its child nodes. The Merkle Root summarizes all transactions in the block and facilitates efficient and secure verification.
4. **Timestamp**: The time when the block was created. This helps in ordering blocks chronologically and is used to prevent double-spending.

5. **Difficulty Target**: A value that defines the difficulty of the proof-of-work puzzle. It adjusts periodically to maintain a consistent block creation rate (e.g., every 10 minutes in Bitcoin).
6. **Nonce**: A random value used during the mining process. Miners adjust the nonce to find a hash that meets the difficulty target, validating the block through proof-of-work.

b. Block Body

The block body contains the actual transaction data and additional information:

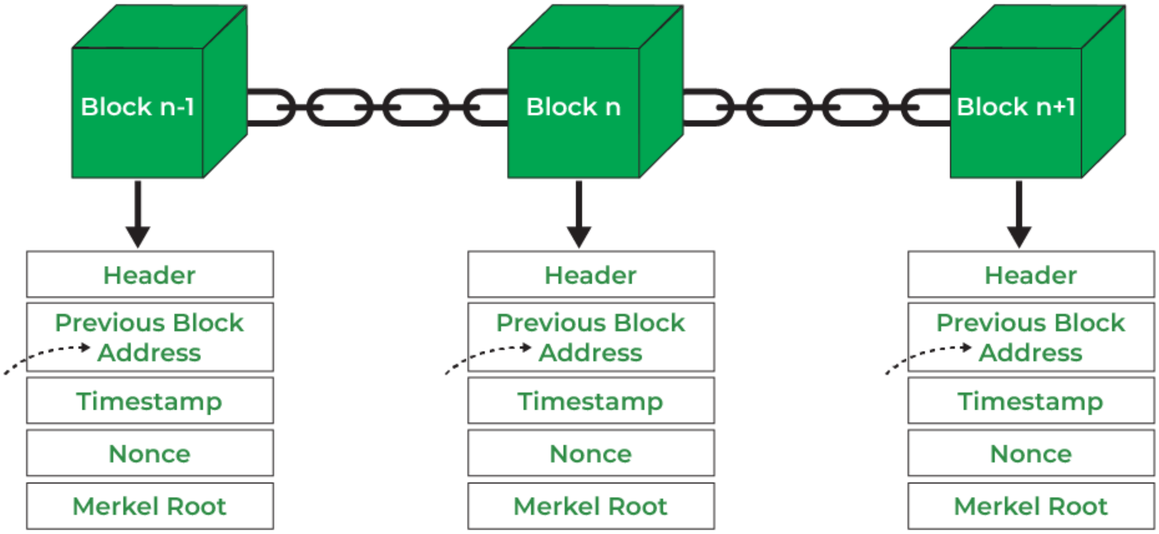
1. **Transaction List**: A list of transactions included in the block. Each transaction typically includes details such as inputs (source addresses), outputs (destination addresses), and the amount of cryptocurrency transferred.
2. **Transaction Count**: The number of transactions in the block, providing a summary of the block's content.

2. Blockchain Structure

Blocks are linked together to form a blockchain. The key elements of this structure are:

- **Chain of Blocks**: Each block contains a reference to the previous block's hash in its header. This linkage forms a continuous chain from the genesis block (the first block) to the current block.
- **Hash Function**: Each block header is hashed using a cryptographic hash function (e.g., SHA-256 in Bitcoin). This hash includes the current block's data, previous block's hash, and nonce. The resulting hash is used to link blocks and validate data integrity.
- **Immutability**: Due to the cryptographic linking of blocks, altering any data in a block would require changing all subsequent blocks. This property ensures that once data is recorded on the blockchain, it cannot be easily altered.

3. Diagram of Blockchain Structure



1. **Header:** It is used to identify the particular block in the entire blockchain. It handles all blocks in the blockchain. A block header is hashed periodically by miners by changing the nonce value as part of normal mining activity, also Three sets of block metadata are contained in the block header.
2. **Previous Block Address/ Hash:** It is used to connect the i+1th block to the ith block using the hash. In short, it is a reference to the hash of the previous (parent) block in the chain.
3. **Timestamp:** It is a system verify the data into the block and assigns a time or date of creation for digital documents. The timestamp is a string of characters that uniquely identifies the document or event and indicates when it was created.
4. **Nonce:** A nonce number which uses only once. It is a central part of the proof of work in the block. It is compared to the live target if it is smaller or equal to the current target. People who mine, test, and eliminate many Nonce per second until they find that Valuable Nonce is valid.
5. **Merkel Root:** It is a type of data structure frame of different blocks of data. A Merkle Tree stores all the transactions in a block by producing a digital fingerprint of the entire transaction. It allows the users to verify whether a transaction can be included in a block or not.

Key Concepts

- **Hashing**: Ensures each block's integrity and creates a unique identifier for each block. Hash functions make it computationally difficult to alter any block without detection.
- **Merkle Tree**: Optimizes the efficiency and security of transaction verification within a block.
- **Proof of Work**: A consensus mechanism requiring miners to solve complex problems to add a block to the blockchain, ensuring network security and validating transactions.
- **Immutability**: Changes to a block would require recalculating hashes for all subsequent blocks, making the blockchain tamper-evident.

5. Consensus and Security

- **Consensus Mechanisms**: Such as Proof of Work (PoW) in Bitcoin or Proof of Stake (PoS) in other blockchains, ensure agreement among network participants on the blockchain's state.
- **Security**: Cryptographic methods and consensus algorithms protect the blockchain against fraud, tampering, and attacks.

Understanding the structure of a blockchain is fundamental to grasping how cryptocurrencies and decentralized applications function, providing transparency, security, and resilience in distributed networks.

Key Characteristics of Blockchain Architecture

- **Decentralization:** In centralized transaction systems, each transaction needs to be validated in the central trusted agency (e.g., the central bank), naturally resulting in cost and the performance jam at the central servers. In contrast to the centralized mode, a third party is not needed in the blockchain. Consensus algorithms in blockchain are used to maintain data stability in a decentralized network.
- **Persistency:** Transactions can be validated quickly and invalid transactions would not be admitted by persons or miners who mining the crypto. It is not possible to delete or roll back transactions once they are included in the blockchain network. Invalid transactions do not carry forward further.
- **Anonymity:** Each user can interact with the blockchain with a generated address, which does not disclose the real identity

of the miner. Note that blockchain cannot guarantee perfect privacy preservation due to the permanent thing.

- **Auditability:** Blockchain stores data of users based on the Unspent Transaction Output (UTXO) model.
  Every transaction has to refer to some previous unspent transactions. Once the current transaction is recorded into the
  blockchain, the position of those referred unspent transactions switches from unspent to spent. Due to this process, the transactions can be easily tracked and not harmed between transactions.
- **Transparency:** The transparency of blockchain is like cryptocurrency, in bitcoin for tracking every transaction is done by the address. And for security, it hides the person's identity between and after the transaction. All the transactions are made by the owner of the block associated with the address, this process is transparent and there is no loss for anyone who is involved in this transaction.
- **Cryptography:** The blockchain concept is fully based on security and for that, all the blocks on the blockchain network want to be secure. And for security, it implements cryptography and secures the data using the cipher text and ciphers.