A very basic Guide: Blockchain Technology

The open chain initiative

written 9 september 2024

1 Blockchain?

A blockchain is a decentralized and distributed ledger technology that securely records transactions across multiple computers. Its primary purpose is to provide transparency, security, and immutability, making it particularly well-suited for financial transactions, supply chain management, and more. Unlike traditional ledgers, blockchains do not rely on a central authority, as they use consensus mechanisms to validate and verify transactions.

Transparency is a cornerstone of blockchain technology. All participants in the network can view the history of transactions, ensuring trust and accountability. This openness eliminates the need for intermediaries, reducing costs and increasing efficiency.

2 Key Components of a Blockchain

2.1 Hash Functions

A hash is a cryptographic function that transforms input data into a fixed-size string of characters, regardless of the input's size. Each block in the blockchain contains a unique hash that acts as its digital fingerprint.

Ethereum, for instance, employs the **Keccak-256** hashing algorithm. This ensures that even the slightest change in the input data results in a vastly different hash, preserving the integrity and immutability of the blockchain.

2.2 Block Structure

A blockchain is composed of individual blocks, each of which contains:

- **Previous Hash:** Links the block to the previous one, forming a chain.
- **Hash:** A unique identifier for the current block.
- **Nonce:** A variable number used by miners to solve cryptographic puzzles.
- **Block Number:** The sequential position of the block in the chain.
- **Data:** Contains transaction details or other relevant information.

2.3 Nonce and Cryptographic Puzzles

The nonce is a number miners adjust to solve cryptographic puzzles required to validate blocks. This process involves brute-forcing different nonce values until the block's hash meets a specific condition (e.g., starting with a predefined number of zeros). Solving this puzzle ensures that the block is valid and can be added to the chain.

3 Cryptocurrency Units and Fees

3.1 Gwei

In Ethereum, Gwei is a unit of computational cost. More complex transactions, such as deploying smart contracts, consume more computational resources and thus require more Gwei. This system ensures that resources are allocated efficiently.

3.2 Base Fee

The base fee is a minimum transaction cost set by the network. It is dynamically adjusted based on network demand. If blocks are more than 50

4 Consensus Mechanisms

4.1 Proof of Work (PoW)

PoW was the original consensus mechanism used by blockchains like Bitcoin and early Ethereum. It involves miners competing to solve computationally intensive puzzles to validate transactions and create new blocks. This method ensures security and decentralization but has significant downsides:

- **Energy Consumption:** PoW requires substantial computational power, leading to high energy costs.
- **Scalability Issues:** As the network grows, PoW becomes slower and more resource-intensive.

4.2 Proof of Stake (PoS)

Ethereum transitioned to PoS to address the limitations of PoW. In PoS, validators are chosen to create new blocks based on the amount of cryptocurrency they stake (lock up as collateral). This system offers several advantages:

- **Energy Efficiency:** PoS reduces energy consumption dramatically compared to PoW.
- **Scalability:** It enables faster transaction processing and better handles network congestion.
- **Enhanced Security:** Validators risk losing their stake if they act maliciously, discouraging dishonest behavior.

4.3 Why the Transition from PoW to PoS?

The move to PoS was motivated by the need for:

- **Sustainability:** To reduce the environmental impact of blockchain networks.

- **Scalability:** To handle increased adoption and transaction volumes.
- **Efficiency:** To lower transaction fees and improve user experience.

5 Security and Immutability

One of the most critical features of blockchain technology is its security:

- **Cryptographic Signatures:** Transactions are secured through private keys and verified by public keys.
- **Immutability:** Once a block is added to the chain, altering its data would require changing all subsequent blocks, which is computationally infeasible in a decentralized network.