Search Docs

Other Documentation Guides

What is blockchain?

Blockchain extends beyond finance and cryptocurrencies. It serves as the underlying technology for creating decentralized applications and forms the foundation of the next generation of the internet. It enables users to send and receive digital assets securely and transparently without the need for a central authority. It achieves this by having a copy of all transactions, or ledger, duplicated and distributed across a network of computers (nodes).

Blockchain is also referred to as **Distributed Ledger Technology** (DLT) and it provides a decentralized and accessible data structure for performing several types of transactions, from financial payments to information exchange, IoT and many others. A blockchain is a transaction record database that is distributed, validated, and maintained around the world by a network of computers. A blockchain operates on a peer-to-peer (P2P) network of computers (nodes), each maintaining a copy of the ledger. This decentralized nature eliminates the need for an intermediary, such as a bank, and instead relies on a large community to oversee and validate the records. No individual person has control over these records, ensuring a high level of security, transparency, and trust.

The name blockchain comes from:

- **Block** refers to data and state being stored in sequential units called "blocks" that are cryptographically secured.

- **Chain** signifies that each block cryptographically references its predecessor, effectively linking the blocks together in chronological order. This chaining ensures that the data in a block cannot be altered without modifying all subsequent blocks.

Key characteristics of blockchain technology include:

- **Decentralization**: The ledger is distributed across a network of nodes, which collectively validate and maintain the records. This decentralization enhances the system's resilience and reduces single points of failure.
- **Transparency**: Transactions recorded on a blockchain are visible to all participants in the network, providing a high level of transparency. Each participant has access to the entire ledger, which helps in maintaining trust and accountability.
- **Immutability**: Once a block is added to the blockchain, it is extremely difficult to alter or delete. This immutability is achieved through cryptographic hashing and consensus mechanisms, ensuring the integrity and permanence of the data.
- **Security**: Blockchain employs advanced cryptographic techniques to secure transactions and data. Each block contains a cryptographic hash of the previous block, a timestamp, and transaction data, making it computationally impractical for anyone to alter past records without detection.

WATCH: What is a Blockchain? (Animated + Examples)

What is the Blockchain trilemma?

The blockchain trilemma is a concept introduced by Ethereum co-founder Vitalik Buterin. It addresses the challenge of balancing three crucial aspects of a blockchain: **decentralization**, **security**, and **scalability**. The trilemma posits that achieving all three at an optimal level simultaneously is exceedingly difficult.

- **Decentralization**: the extent to which a blockchain is distributed across a network of nodes, ensuring no single entity has control over the entire system. High decentralization enhances resistance to censorship and failures.

- **Security**: a blockchain's ability to defend against attacks and vulnerabilities. A secure blockchain ensures that transactions are tamper-proof and the network is robust against various threats.

- **Scalability**: the blockchain's capacity to handle a growing number of transactions and data without performance degradation. High scalability is essential for mass adoption and efficient operation.

The trilemma suggests that improving two of these aspects typically results in compromises in the third. For example, **enhancing decentralization and security** might **reduce scalability**. Blockchain projects continually strive to find innovative solutions to address this trilemma and create more balanced systems.

What is a Consensus Algorithm?

A consensus algorithm is a mechanism that enables users or machines to coordinate in a distributed environment. It ensures that all participants in the system can agree on a single source of truth, even if some participants fail. This means the system must be fault-tolerant. In a centralized setup, a single entity controls the system and can make changes at will, without the need for a complex governance system to achieve consensus among multiple administrators.

Users' balances are recorded in a database known as the blockchain. It is crucial that everyone (or more accurately, every node) maintains an identical copy of this database. Otherwise, conflicting information would arise, undermining the entire purpose of the decentralized network. Public-key cryptography ensures that users cannot spend each other's tokens, but a single source of truth is still necessary for network participants to determine whether funds have already been spent.

Satoshi Nakamoto, the creator of Bitcoin, proposed a Proof of Work (PoW) system to coordinate participants. We will discuss how PoW works shortly, but first, let's identify some common traits of the many existing consensus algorithms.

Firstly, users who want to add blocks (referred to as validators) must provide a stake. The stake is a form of value that validators must put forward, which discourages dishonest behavior. If they cheat, they will lose their stake. Examples of stakes include computing power, cryptocurrency, or even reputation. Why would validators risk their resources? Because there is a reward available, usually consisting of the protocol's native cryptocurrency. This reward is made up of fees paid by other users, newly generated cryptocurrency units, or both.

Lastly, transparency is essential. We need to be able to detect when someone is cheating. Ideally, it should be costly for validators to produce blocks but inexpensive for anyone to validate them. This ensures that validators are kept in check by regular users.

Types of Consensus Algorithms

Proof of Work (PoW) is the earliest blockchain consensus algorithm, first utilized by Bitcoin. In PoW,validators (known as miners) compete to add new blocks containing processed transactions to the blockchain. The first miner to solve a complex mathematical puzzle shares the new block with the rest of the network and receives a reward of newly minted BTC. The solved puzzle creates a cryptographic link (hash) between the current block and the previous one, embodying the "proof" in Proof of Work. A hash is a seemingly random sequence of letters and numbers created by processing data through a hash function. The same input will always generate the same hash as an output, but even a small change in the input will result in a completely different hash.

In PoW, the protocol defines conditions for block validity, such as requiring a block hash to start with a specific pattern like "00". Miners must brute-force different inputs to meet this condition, adjusting their data until the correct hash is found. Meeting these conditions requires substantial computational power and specialized hardware (ASICs). The cost of these machines and the electricity to run them represent the miner's stake. The network can easily verify a miner's work by running the data through the hash function once. If the hash is valid, the block is accepted, and the miner receives a reward. If not, the effort and resources spent are wasted.

The network's security relies on the immense computational power required to alter the blockchain. An attacker would need to control 51% of the network's total computing power, necessitating significant investment in hardware and energy, likely exceeding any potential gain.

WATCH: What is Proof of Work (PoW) | Explained For Beginners

Proof of Stake (PoS) Proof of Stake (PoS) is used by blockchains such as Ethereum, Polygon, Optimism, Cosmos, Solana, Cardano, Polkadot, Algorand, etc. In PoS, validators are responsible for creating blocks and they do not consume large amounts of energy. Instead, they must hold and lock up cryptocurrency as a **stake**. Validators lock their funds in a wallet (or delegate them into an Stake Pool), making them ineligible for movement while staking. The more funds locked up (staked), the higher is the likelihood to get selected for producing the next block and get the rewards.

The protocol selects a validator randomly to produce the block and receive the rewards which are the transaction fees proportionate to their stake. Dishonest actions, such as proposing invalid transactions, result in losing part or all of the staked funds. This incentivizes honesty similarly to PoW.

This validator's consensus client requests a bundle of transactions, termed an 'execution payload' from their execution client. This payload, combined with consensus data, forms a new block that is propagated to other nodes in the PoS network. Validators are rewarded with tokens for successful block production.

A PoS system ensures security through economic incentives and penalties. Attackers would need to risk and potentially lose a substantial amount of tokens to take control of the network. Rewards motivate validators to act honestly, while penalties deter malicious behavior, maintaining the integrity of the blockchain.

WATCH: What is Proof of Stake (PoS) | Explained For Beginners

Smart Contracts

In addition to recording transactions, some blockchains support programmable contracts known as smart contracts. These self-executing contracts with predefined rules and conditions automate processes and can facilitate complex agreements without the need for intermediaries. They are computer programs stored on the blockchain that follow "if this then that" logic, and are guaranteed to execute according to the rules defined by its code, which cannot be changed once created.

How Smart contracts work?

Step 1 - Coding: In EVM ecosystem, smart contracts are written in Solidity, but this varies based on the programming language specific to each blockchain. It is very important that the code has the proper logic to do precisely what the different parties want to do.

Step 2 - Distributed Ledger: Once the code is written, it is encrypted and sent out to the nodes of the distributed network.

Step 3 - Execution: Each node comes to an individual agreement on the results of the code. The network records the execution of the contract and monitors for compliance with the terms of the smart contract.

WATCH: Smart contracts - Simply Explained

Wallets

Just like your physical wallet, it contains everything you need to prove your identity and handle your digital assets. Your wallet allows you to sign in to applications, read your balance, send transactions and verify your identity. Wallets store the cryptographic keys (both public and private) that allow users to send and receive cryptocurrency. The actual coins are stored on the blockchain, but the wallet provides access to them.

Public Key: An address that others can use to send cryptocurrency to your wallet. Think of it like an email address.

Private Key: A secure code that allows you to access and manage your cryptocurrency. It should be kept secret, similar to a password. It is used for signing your transactions.

A wallet dynamically creates private keys for you and stores them. The app signs the transaction with your private key without explicitly revealing it, which signals to the whole network that you have the ability to transfer the funds to the address from which you are sending.

Types of wallets

Hot wallets: Connected to the internet, these are convenient for frequent transactions. Examples include mobile wallets, web wallets, and desktop wallets.

Cold wallets: Not connected to the internet, these are more secure and used for long-term storage. Examples include hardware wallets and paper wallets.

WATCH: What is a Cryptocurrency Wallet? (3 Types + Key Examples)

Tokens

Tokens are digital assets created and managed on the blockchain. They represent various types of value or assets and are typically used for different purposes within blockchain ecosystems. Types of tokens:

Fungible Tokens (ERC-20, BEP-20) These are those types of cryptographic tokens that are basically identical or uniform and can be interchanged with other fungible tokens of the same type without any issues. Examples: **Cryptocurrency tokens**: These are tokens that serve as a medium of exchange, store of value, or unit of account within a blockchain network. Examples include Bitcoin (BTC) and Ether (ETH). **Utility tokens**: These tokens provide access to a specific product or service within a blockchain-based platform. They are not designed as investments. **Security tokens**: These represent ownership in a real-world asset, such as shares in a company or real estate. They are subject to federal securities regulations. **Governance tokens**: These tokens give holders the right to participate in the governance of a blockchain project. Holders can vote on decisions such as protocol upgrades or fund allocations. **Non-Fungible Tokens (ERC-721)** These tokens represent unique digital assets, such as digital art, collectibles, or real estate within virtual worlds. Each NFT has distinct attributes and values. They are unique in the sense that they cannot be split or exactly changed for other non-fungible tokens of the same type.

WATCH: What is a Token? (Explained Simply)

Exchanges

DEX (Decentralized Exchange)

- **Decentralization**: DEXs operate without a central authority. They facilitate peer-to-peer trading directly between users.
- **Security**: Users retain control of their private keys and funds, reducing the risk of hacks and theft associated with centralized exchanges.
- **Anonymity**: Typically, DEXs require less personal information for transactions, preserving user privacy.
- **Liquidity**: Liquidity on DEXs can be lower than on centralized exchanges, which might result in higher slippage for large orders.
- **Examples**: Minswap, Uniswap and SushiSwap.

CEX (Centralized Exchange)

- **Centralization**: CEXs are managed by a central authority or organization that facilitates trading and holds user funds.
- **Ease of Use**: They generally offer a more user-friendly interface and customer support, making them accessible to beginners.
- **Liquidity**: CEXs usually have higher liquidity, which means trades can be executed more quickly and with less slippage.
- **Security Risks**: Users need to trust the exchange to secure their funds and personal data. Centralized exchanges are more susceptible to hacks.
- **Examples**: Binance, Coinbase and Kraken.

WATCH: CEX vs DEX: Which Crypto Exchange Is Better?

Now that you understand the basics of Blockchain, learn more about Apex Fusion Basics.

Privacy policy Terms of service