Week 1 - Bitcoin Whitepaper Overview [Offline Video]

💡 *Title*: Bitcoin: A Peer-to-Peer Electronic Cash System

Author: Satoshi Nakamoto

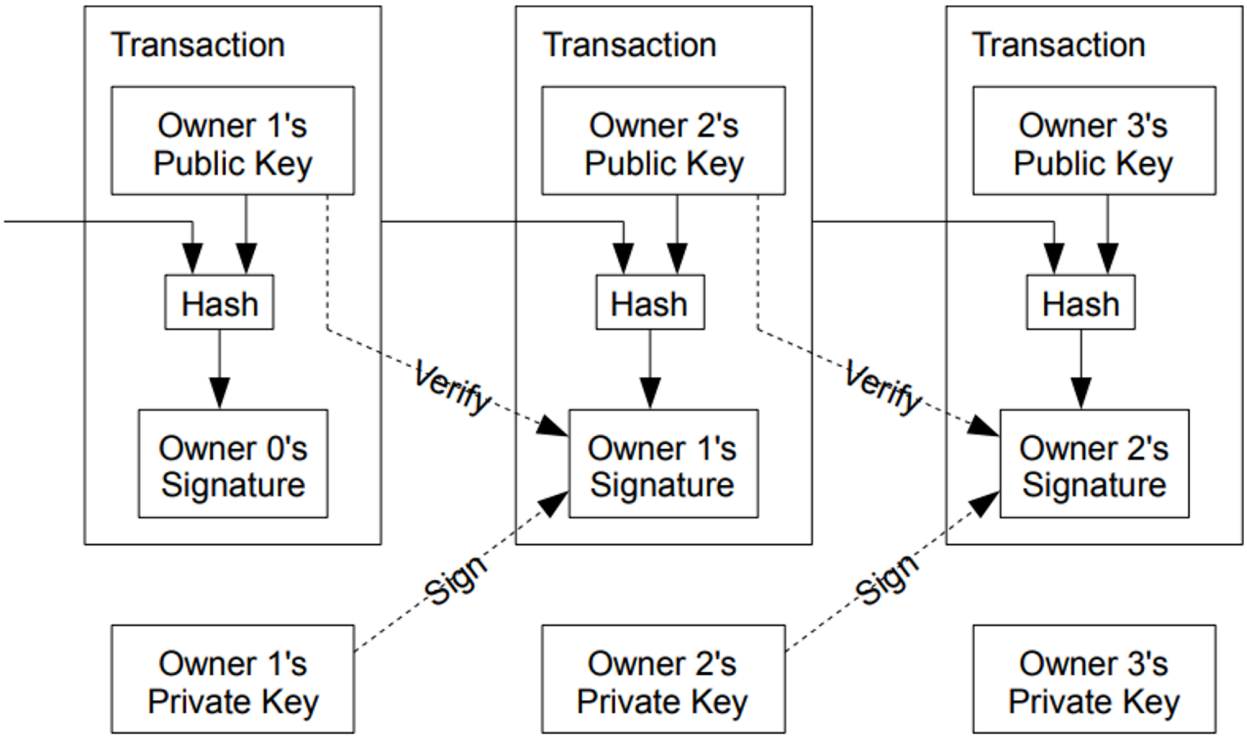
Published: October 31, 2008

Paper: Bitcoin: A Peer-to-Peer Electronic Cash System

Introduction

- **Problem Statement**: The goal is to create a purely peer-to-peer version of electronic cash, enabling online payments to be sent directly from one party to another without needing a financial institution or trusted third party.
- **Purpose**: Introduces a decentralized digital currency system, eliminating the need for intermediaries like banks.
- **Problem Crux**: Double spending in digital currencies, where a single digital token could be spent more than once.

Defining Electronic Coins in Bitcoin



Concept of an Electronic Coin

- **Definition**: An electronic coin in Bitcoin is defined as a chain of digital signatures. This chain represents the ownership history of the coin, tracking each time it changes hands.

How Ownership is Transferred

- **Transaction Structure**:
  - Each time a coin is transferred, the current owner signs a digital hash of the previous transaction.
  - The hash includes:
    1. **The Previous Transaction**: Proof of how the current owner acquired the coin.
    2. **The Public Key of the Next Owner**: Designates the new owner of the coin.
- **Digital Signatures**:
  - The current owner uses their private key to create a digital signature, adding it to the end of the coin's chain and effectively transferring ownership.
  - **Hash of the Transaction**: A unique string generated from the transaction data, ensuring even a small change produces a completely different hash.
  - **Public Key of the Next Owner**: Serves as the address to which the coin is sent; only the holder of the corresponding private key can access and spend the coin.

Verification of Ownership

- **Verification Process**:
  - The payee can verify the transaction's authenticity by checking the chain of digital signatures.
  - This involves:
    1. **Verifying the Signatures**: Ensuring each signature in the chain is legitimate by checking against the corresponding public key.
    2. **Verifying the Chain of Ownership**: Tracing back the chain of transactions to confirm that the coin's ownership has been validly transferred.

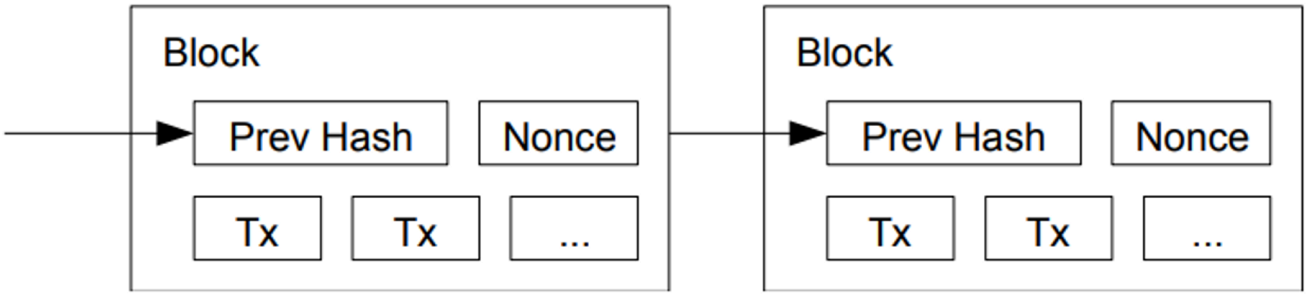
Chain of Ownership

- **Purpose**: The chain of digital signatures serves as a record of ownership, proving that the current owner has legitimately acquired the coin.
- **Security**: Ensures that the ownership of the coin is secure and can be verified without relying on a central authority.

Digital Signatures

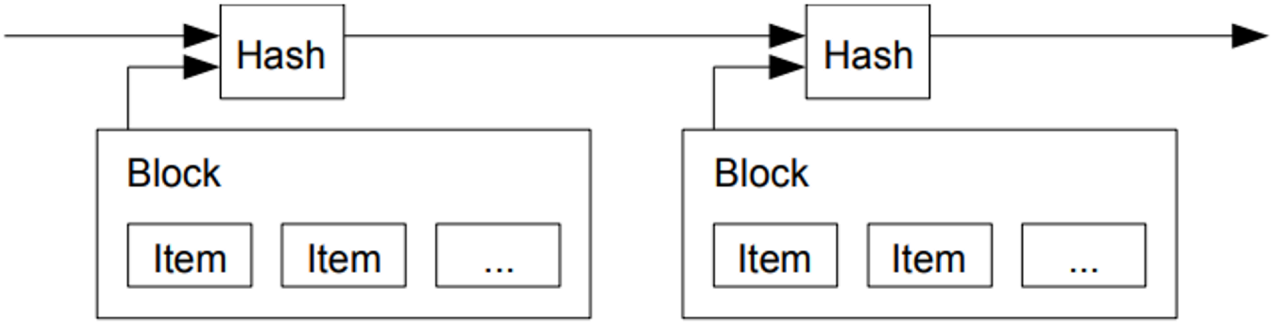
- **Partial Solution**: Digital signatures ensure the authenticity and integrity of a transaction. While crucial for securing transactions, they do not fully solve the double-spending problem.
- **Double-Spending Problem**: Refers to the risk of a single digital token being spent more than once, an issue arising from the ease of copying digital information.
- Transactions are secured with digital signatures.
- Each Bitcoin user has a pair of cryptographic keys: a public key and a private key.
- The private key signs transactions, ensuring only the owner can spend their Bitcoins.

Peer-to-Peer Network and Proof-of-Work (PoW)



- **Proposed Solution**: Solving the double-spending problem using a peer-to-peer (P2P) network. The network's key innovation is the proof-of-work mechanism.

- **Network Operation**: Nodes in the network validate and relay transactions.
- **Timestamps and Hashing**:
  - Each transaction is timestamped and hashed into a chain (the blockchain).
  - The chain is secured through proof-of-work, where nodes (miners) expend computational power to solve cryptographic puzzles.



- **Immutable Record**:
  - The blockchain forms an ongoing, immutable record of transactions.
  - Once a block is added to the chain, it cannot be altered without redoing the proof-of-work for that block and all subsequent blocks.
- **Mining Process**: Nodes (miners) solve complex mathematical problems to validate transactions and add them to the blockchain.
- **Rewards**: The first miner to solve the problem gets to add a new block and is rewarded with newly minted Bitcoins.

What is Proof-of-Work?

- **Concept**: Proof-of-work is a cryptographic mechanism where participants (miners) must perform computational work to solve a problem. In Bitcoin, this problem involves finding a value that, when hashed using a cryptographic hash function like SHA-256, produces a hash with a certain number of leading zero bits.
- **Origin**: The PoW system used in Bitcoin is similar to the one proposed by Adam Back in Hashcash, originally designed to combat email spam by requiring senders to perform a small amount of computational work.

How Proof-of-Work Works

- **Hash Function**: Bitcoin uses the SHA-256 hash function, which takes an input and produces a fixed-size output (the hash). The goal is to find an input (a block of transactions) that produces a hash beginning with a specific number of zero bits.

- **Difficulty**: The number of leading zero bits required in the hash determines the difficulty of the proof-of-work. The more zero bits required, the harder it is to find such a hash. The difficulty is set to maintain a consistent average time to find a solution across the network.

Longest Chain Rule

- **Chain Validity**:
  - The longest chain in the blockchain is considered valid because it represents the most computational work (CPU power) invested.
  - This chain serves as proof of the sequence of events (transactions) and indicates that it was generated by the majority of the network's computing power.
- **Security Assumption**:
  - The network's security relies on the assumption that a majority of CPU power is controlled by honest nodes.
  - As long as this is true, the honest nodes will always generate the longest chain, outpacing any attackers.
- Once a transaction is confirmed and added to the blockchain, it cannot be altered.

Network Structure and Operation

- **Minimal Structure**:
  - The network is designed to operate with minimal structure.
  - Nodes do not need to follow strict protocols or maintain constant connectivity.
- **Broadcasting and Rejoining**:
  - Transactions and blocks are broadcasted to the network on a best-effort basis.
  - Nodes can leave and rejoin the network at will. When they rejoin, they accept the longest proof-of-work chain as the authoritative record of transactions.
- **Resilience and Flexibility**: This decentralized approach ensures the network's resilience and flexibility, allowing it to continue operating even if some nodes go offline or the network is under attack.
- **Incentives and Mining**:
  - Miners are incentivized to secure the network through block rewards and transaction fees.
  - As more miners join, the difficulty of the mathematical problems increases, maintaining a steady block generation rate.

- **Limited Supply**:
  - Bitcoin has a fixed supply of 21 million coins, designed to create scarcity and mimic precious metals like gold.
  - The block reward halves approximately every four years in an event known as "halving."
- **Decentralized Ledger (Blockchain)**:
  - Transactions are grouped into blocks and linked together to form a blockchain.
  - The blockchain is a public ledger, visible to all participants in the network.
  - Each block contains a list of validated transactions and a reference (hash) to the previous block, ensuring immutability.
- **Security and Attacks**:
  - The network is secure as long as honest nodes control more CPU power than any attacking group.
  - Discusses the "51% attack" scenario, where a malicious actor with more than 50% of the network's hashing power could potentially alter the blockchain.

Applications and Implications

- **Decentralization**: Bitcoin’s model removes the need for centralized financial institutions.
- **Trust**: Users do not need to trust a third party; trust is placed in cryptography and the network itself.
- **Global Currency**: Bitcoin can be used globally without restrictions, offering an alternative to traditional currencies.
- **Future of Finance**: Paved the way for the development of other cryptocurrencies and the broader decentralized finance (DeFi) ecosystem.

> 💡 Additional - The Bitcoin Whitepaper | Fully Explained (With Animations!) (youtube.com)