

Technical Architecture of Bitcoin



Bitcoin, introduced by Satoshi Nakamoto in 2008, revolutionized the concept of decentralized digital currency. It is like digital money that people can use to buy things online. But instead of using banks or other companies to handle the transactions, Bitcoin works in a different way. This report explains how Bitcoin works and what makes it special.

Blockchain: At the center of Bitcoin is something called the blockchain. A big digital ledger, like a giant book that records every transaction made with Bitcoin. Each transaction is grouped together into blocks, which are connected in a chain. This chain keeps growing as more transactions happen.

Decentralization and Consensus: Unlike traditional money systems, Bitcoin doesn't depend on a central authority to control it. Instead, decisions are made by agreement among the majority of nodes in the network. This means that no single person or company has control over Bitcoin.

Proof-of-Work: To add a new block to the chain, people need to do something called mining. Mining is like solving puzzles on a computer. Miners compete to solve these puzzles, and the first one to solve it gets to add a new block to the blockchain. This process makes sure that transactions are secure and can't be changed later.

Peer-to-Peer Network: Bitcoin works on a network of computers called nodes. These nodes talk to each other and share information about transactions and blocks. When someone makes a transaction, it gets sent to all the nodes in the network. Miners then pick up these transactions and include them in the next block they mine.

Transaction Verification: Every Bitcoin transaction is verified using digital signatures. These signatures prove that the person sending the Bitcoin is the rightful owner. It's like signing your name on a check to show that it's really you.

Incentive Structure: People who help maintain the Bitcoin network by mining new blocks are rewarded with newly created bitcoins. This encourages more people to participate in mining and helps keep the network secure.

Conclusion: Bitcoin's technical setup is pretty clever. It uses a combination of computer puzzles, digital signatures, and a network of computers to create a system where people can send money to each other without needing a bank. This makes Bitcoin unique and has led to its popularity as a digital currency.