Unit-V
Bitcoins

Introduction

Bitcoin is the world's first and most well-known cryptocurrency. It was created in 2009 by an anonymous person or group of people using the pseudonym Satoshi Nakamoto. Bitcoin revolutionized the world of finance and introduced the concept of a decentralized, digital, and censorship-resistant form of currency. Here's an introduction to Bitcoin:

Digital Currency: Bitcoin is a purely digital currency, meaning it exists only in digital form. It's not backed by any physical asset like gold or a government's guarantee.

Decentralization: Bitcoin operates on a decentralized network of computers, known as nodes, which are spread across the globe. This network collectively maintains the blockchain, a public ledger that records all Bitcoin transactions.

Blockchain Technology: The blockchain is the technology that underpins Bitcoin. It's a secure and transparent ledger that records every transaction ever made with Bitcoin. It ensures the integrity of the currency and prevents double-spending.

Limited Supply: Bitcoin has a fixed supply. There will only ever be 21 million Bitcoins in existence, making it a deflationary asset. This scarcity is often cited as a reason for its value.

Mining: New Bitcoins are created through a process called mining. Miners use computational power to solve complex mathematical puzzles, validate transactions, and secure the network. In return, they're rewarded with newly created Bitcoins and transaction fees.

Security: Bitcoin transactions are secured through cryptographic techniques. The network is highly secure and resistant to fraud and hacking.

Pseudonymity: While Bitcoin transactions are recorded on the blockchain and are public, users are represented by pseudonymous addresses, not personal information. This provides a level of privacy, but it's not entirely anonymous.

Use Cases: Bitcoin has evolved to serve various use cases. It can be used as a digital currency for online purchases, a store of value, a hedge against inflation, and a means of transferring wealth across borders.

Volatility: The price of Bitcoin can be highly volatile. It's subject to market demand, supply, and external factors, which can lead to both significant gains and losses for investors.

Legal and Regulatory Landscape: The legal status of Bitcoin varies from country to country. Some nations have embraced it, while others have imposed restrictions or bans.

Wallets: Users store their Bitcoins in digital wallets. These wallets can be software-based, hardware-based, or even paper wallets, and they're used to send, receive, and manage Bitcoin holdings.

Investment and Trading: Many people view Bitcoin as a speculative asset and invest in it. It's also actively traded on various cryptocurrency exchanges. In recent years, some institutional investors and large corporations have started to invest in Bitcoin.

Bitcoin's creation marked the beginning of a revolutionary era in finance and technology. It has inspired the development of thousands of other cryptocurrencies, known as "altcoins." Bitcoin remains the most recognized and widely adopted cryptocurrency, and it continues to be a subject of significant interest and debate in the world of finance, technology, and economics.

Working of Bitcoin:

The working of Bitcoin involves a complex interplay of technology, economics, and cryptography. To understand it, let's break down the key components and processes:

Blockchain Technology:

Bitcoin is built on a decentralized ledger called the blockchain. The blockchain is a chain of blocks, each containing a batch of Bitcoin transactions. Miners, who are participants in the Bitcoin network, group new transactions into a block and compete to solve a cryptographic puzzle. The first miner to solve the puzzle gets to add the block to the blockchain.

Transactions:

Users initiate Bitcoin transactions by sending digital coins from one Bitcoin address to another. These transactions are signed cryptographically to ensure their security and integrity. Transactions are broadcast to the network, and they are collected into a pool (mempool) awaiting confirmation.

Consensus Mechanism:

The network uses a consensus mechanism, known as Proof of Work (PoW), to validate and add transactions to the blockchain. Miners compete to solve a computationally intensive puzzle, and the first miner to solve it broadcasts their solution to the network.

Validation and Block Creation:

Once a miner's solution is verified by the network, they are authorized to create a new block. This block contains a set of recent transactions, a reference to the previous block, and a special transaction called the "coinbase transaction" that rewards the miner with newly created Bitcoins and transaction fees.

Adding Blocks to the Blockchain:

The new block is added to the existing blockchain, creating a permanent record of transactions. This process occurs approximately every 10 minutes, creating a consistent time interval for block creation.

Security:

The blockchain is secured through cryptographic hashing, which makes it extremely difficult to alter past transactions. Once a block is added to the chain, it's practically impossible to change. Bitcoin's security is enhanced by the network's decentralized nature, as it would require an extraordinary amount of computational power to compromise the network.

Mining Reward and Halving:

Miners are rewarded with newly created Bitcoins and transaction fees for their work in creating new blocks. The reward decreases over time through a process called "halving." Approximately every four years, the block reward is halved, reducing the rate at which new Bitcoins are created.

Node Validation:

All nodes in the network validate and store a copy of the blockchain. This ensures the integrity and consistency of the ledger.

Public Ledger:

The blockchain is a public ledger, meaning anyone can view all transactions and the entire transaction history. However, user identities are pseudonymous, not tied to real-world identities.

Wallets:

Users manage their Bitcoins through digital wallets. Wallets store the cryptographic keys needed to access and spend the Bitcoins associated with a particular Bitcoin address.

Peer-to-Peer Network:

Bitcoin operates on a peer-to-peer network, meaning there is no central authority. Nodes in the network communicate directly with one another to transmit transactions and blocks.

Decentralization:

Decentralization is a key feature of Bitcoin, as it removes the need for intermediaries and central authorities, making it a censorship-resistant and borderless digital currency.This process of mining, validating, and adding blocks to the blockchain is what ensures the integrity and security of the Bitcoin network. It's this process that allows users to send and receive Bitcoins, and it's what has made Bitcoin the first and most well-known cryptocurrency in the world.

Merkle Trees:

Merkle trees, named after their inventor Ralph Merkle, are a fundamental data structure used in computer science and cryptography. They are particularly well-known for their use in blockchain technology, including cryptocurrencies like Bitcoin. Merkle trees offer several advantages, including data integrity verification and efficient data retrieval.

Here's how a Merkle tree works:

Building the Tree: A Merkle tree is a binary tree where each leaf node represents a specific piece of data, such as a transaction in a blockchain. The tree is constructed by recursively hashing pairs of nodes until a single root hash remains.

Hashing: Each leaf node contains the hash of the data it represents. To create parent nodes, you concatenate the hashes of their two child nodes and then hash the result. This process continues until you reach the root node, which is also known as the Merkle root.

Verification: To verify the integrity of the data in the Merkle tree, you can compare a piece of data's hash to the Merkle root. If they match, it means the data is unchanged and hasn't been tampered with. This process is highly efficient since you only need to compare a few hashes to verify a specific piece of data.

Efficient Data Retrieval: Merkle trees enable efficient data retrieval. For example, in a blockchain, you can prove that a specific transaction is included in a block without needing to download the entire block. Instead, you request the necessary branch of the Merkle tree, starting from the transaction in question and working your way up to the Merkle root.

Merkle trees have many applications beyond blockchains, such as in file systems, peer-to-peer networks, and distributed databases. They provide a way to ensure data integrity and verify the existence of specific data elements in a large dataset without having to check the entire dataset, making them a valuable tool in various areas of computer science and cryptography.

Bitcoin Block Structure:

A Bitcoin block is a fundamental component of the Bitcoin blockchain, and it serves as a container for a set of transactions. The structure of a Bitcoin block is as follows:

Block Header: The block header is a fixed 80 bytes in size and contains several fields, including:

Version: A 4-byte field that indicates the software version used to create the block.

Previous Block Hash: A 32-byte field that references the hash of the previous block in the blockchain. This establishes the chain of blocks, hence the term "blockchain."

Merkle Root: A 32-byte hash that represents the root of the Merkle tree of all transactions in the block. This Merkle root is used to efficiently verify the existence of specific transactions within the block.

Timestamp: A 4-byte field that denotes the approximate time when the block was mined.

Bits: A 4-byte field representing the current network difficulty target for mining the block.

Nonce: A 4-byte field used in the mining process. Miners repeatedly change the nonce in an attempt to find a valid block hash that satisfies the network's difficulty requirements.

Transaction Counter: A 1- to 9-byte field that indicates how many transactions are included in the block. This field can represent a variable-length integer.

List of Transactions: The actual Bitcoin transactions are stored in the block following the header. The number of transactions corresponds to the value in the

transaction counter. Each transaction contains information about the sender, receiver, amount, and more.
The block header is crucial for ensuring the integrity of the block, and the proof-of-work process (mining) involves finding a valid nonce that, when combined with the other header fields, results in a block hash that meets the network's current difficulty target. Miners compete to find this nonce, and the first one to succeed can broadcast the new block to the network. The structure of a Bitcoin block is designed to provide security, transparency, and immutability in the blockchain. Once a block is added to the blockchain, it becomes extremely difficult to alter any of its contents, making Bitcoin a secure and decentralized digital currency system.

Bitcoin Address:

A Bitcoin address is a fundamental component of the Bitcoin cryptocurrency system and serves as a way to send and receive Bitcoins. It is essentially a cryptographic representation of a user's public key, allowing them to receive Bitcoin payments securely. Here's an overview of how a Bitcoin address is structured:

Public Key: Every Bitcoin address is associated with a public key, which is a cryptographic key used for encrypting and verifying data. In the context of Bitcoin, this public key is derived from the user's private key through a process known as Elliptic Curve Cryptography (ECC).

Hashing: The public key is put through a one-way cryptographic hash function, specifically the SHA-256 (Secure Hash Algorithm 256-bit). This produces a 256-bit hash.

RIPEMD-160 Hash: The SHA-256 hash is then processed through another hash function known as RIPEMD-160 (RACE Integrity Primitives Evaluation Message Digest 160). This step further reduces the length of the hash to 160 bits.

Prefixes: A prefix or version byte is added to the RIPEMD-160 hash. This prefix identifies the network or type of address (e.g., mainnet or testnet) and is typically 1 byte long.

Checksum: To enhance security and detect errors, a 4-byte checksum is generated from the prefix and RIPEMD-160 hash.
Base58 Encoding: The result is encoded in Base58, which is a binary-to-text encoding scheme that excludes characters that are easily mistaken for one another (such as '0' and 'O', '1' and 'l', etc.). This encoding results in a Bitcoin address that is a string of letters and numbers.

The final Bitcoin address is the string that you can share with others to receive Bitcoin payments. It looks something like this: "1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa."

Important points about Bitcoin addresses:

A Bitcoin address is case-sensitive.

It's important to keep your Bitcoin address private, as it is associated with your public key, which is derived from your private key. Sharing your Bitcoin address allows others to send you Bitcoins, but it doesn't reveal your private key.

To send Bitcoins, you would need to sign a transaction with your private key, proving ownership of the associated Bitcoin address.

There are different address formats for Bitcoin, including Segregated Witness (SegWit) addresses and Pay-to-Script-Hash (P2SH) addresses, which have variations in the structure but serve the same basic purpose.

Be cautious when transacting with Bitcoin, as errors can result in the loss of funds. Always double-check the accuracy of the Bitcoin address you're sending funds to.

Remember that Bitcoin addresses are for receiving funds, and the private key associated with them is used to send funds. Keeping your private key secure is of utmost importance to protect your Bitcoin holdings.

Bitcoin Transactions:

Bitcoin transactions are at the heart of the Bitcoin network. They are the means by which Bitcoins are transferred from one party to another and recorded on the blockchain. Here's an overview of how Bitcoin transactions work:

Inputs and Outputs:

Input: In a Bitcoin transaction, the sender (the person or entity transferring Bitcoin) references unspent transaction outputs (UTXOs) from previous transactions. These UTXOs are essentially the "coins" being spent. To spend them, the sender creates inputs in the new transaction, providing references to the previous UTXOs.

Output: The transaction also contains one or more outputs. Each output specifies the recipient's Bitcoin address and the amount being transferred. Unspent amounts in the transaction's inputs are sent back as "change" to the sender, effectively creating a new UTXO.

Digital Signature:

To create a transaction, the sender must sign it using their private key. This digital signature provides cryptographic proof that the sender is the legitimate owner of the UTXOs being spent.

Transaction Fee:

To incentivize miners to include the transaction in a block, a transaction fee is typically included. The sender can choose the fee amount, and higher fees usually result in faster confirmation times.

Transaction Validation:

Once a transaction is created, it is broadcast to the Bitcoin network. Nodes on the network verify the transaction's validity, ensuring that the digital signature is correct, the inputs are unspent, and the transaction doesn't create more Bitcoin than it spends.

Mempool:

Valid transactions are temporarily stored in the mempool (short for "memory pool") while they await confirmation in a block. Miners select transactions from the mempool to include in their candidate blocks.

Confirmation:

When a miner successfully mines a new block, the transactions in that block are considered confirmed. The first confirmation means the transaction is included in one block, and additional confirmations occur as more blocks are added to the blockchain. Typically, as the number of confirmations increases, the transaction is considered more secure and irreversible.

Blockchain Recording:

Once confirmed, the transaction and its details (inputs, outputs, digital signatures) are recorded on the Bitcoin blockchain. This creates a transparent and immutable ledger of all transactions on the network.

Double Spending Prevention:

The decentralized nature of the Bitcoin network and the proof-of-work consensus mechanism make it extremely difficult to perform double spending, ensuring the integrity of transactions.

Bitcoin transactions play a critical role in enabling the transfer and management of value on the network. They are secure, transparent, and irreversible once confirmed, making them a key element of the Bitcoin system.

Bitcoin Network:

The Bitcoin network is a decentralized, peer-to-peer network that underlies the Bitcoin cryptocurrency. It was created by an anonymous person or group of people using the pseudonym Satoshi Nakamoto and was launched in 2009. The Bitcoin network serves as a global, digital, and trustless system for the transfer and storage of value (Bitcoins) without the need for intermediaries like banks. Here are some key aspects of the Bitcoin network:

Decentralization: The Bitcoin network is decentralized, meaning it operates without a central authority, such as a government or financial institution. It relies on a distributed ledger called the blockchain, which is maintained by a network of nodes (computers) run by participants (miners) all around the world.

Blockchain: The blockchain is a public, immutable ledger that records all Bitcoin transactions in chronological order. New transactions are grouped together into blocks, and these blocks are linked together to form the blockchain. This technology ensures transparency and security in the network.

Miners: Miners are participants in the network who validate and confirm transactions. They compete to solve complex mathematical puzzles through a process known as proof-of-work. The first miner to solve the puzzle can add a new block to the blockchain and is rewarded with new Bitcoins and transaction fees. This process secures the network and ensures the validity of transactions.

Bitcoin Addresses: Bitcoin users have addresses, which are derived from their public keys and are used to send and receive Bitcoins. The private key associated with an address is used to authorize transactions.

Cryptography: Cryptography is central to the Bitcoin network. It secures transactions, protects user identities, and ensures the integrity of the blockchain. Public and private key pairs, digital signatures, and cryptographic hashing are all essential components.

Consensus Mechanism: The Bitcoin network relies on a consensus mechanism called proof-of-work. Miners compete to solve a cryptographic puzzle, and the first one to solve it adds a new block to the blockchain. This process makes it computationally expensive and time-consuming to alter the blockchain, making it secure against attacks.

Scarcity and Halving: Bitcoin has a capped supply of 21 million coins. Approximately every four years, a "halving" event reduces the block reward miners receive for adding new blocks to the blockchain. This halving process ensures that the total supply of Bitcoins will never exceed 21 million, making it a deflationary digital currency.

Security: The Bitcoin network is highly secure due to its decentralized nature and cryptographic safeguards. Altering past transactions or attempting to double-spend is extremely difficult and computationally expensive.

Global Access: Anyone with an internet connection can participate in the Bitcoin network. There are no geographic restrictions, making it accessible to a global audience.

Pseudonymity: While Bitcoin transactions are public and recorded on the blockchain, they are not directly tied to personal identities. Users are represented by their Bitcoin addresses, providing a degree of privacy.

The Bitcoin network has fundamentally changed the way we think about money and finance. It offers a digital alternative to traditional currency and banking systems, promoting transparency, security, and financial sovereignty for its users.

Bitcoin Wallets:

Bitcoin wallets are digital tools that allow you to manage your Bitcoin holdings, send and receive Bitcoins, and monitor your transactions. They come in various forms, each with its own features, security levels, and use cases. Here are the main types of Bitcoin wallets:

Software Wallets:

Desktop Wallets: These are applications that you install on your computer, offering a higher level of security than online wallets. Examples include Electrum, Bitcoin Core, and Exodus.

Mobile Wallets: Mobile wallets are apps designed for smartphones and tablets, providing convenience and portability. Popular mobile wallets include Coinbase, MyEtherWallet, and Trust Wallet.

Web Wallets:

**Web wallets are accessible through a web browser and offer convenience but may be less secure because your private keys are stored online. Examples include blockchain.info, and GreenAddress.

Hardware Wallets:

Hardware wallets are physical devices that store your private keys offline, providing the highest level of security. Examples include Ledger Nano S, Ledger Nano X, and Trezor.

Paper Wallets:

A paper wallet is a physical document that contains a public address for receiving Bitcoin and a private key for spending or transferring Bitcoin. It is highly secure but should be stored in a safe place to prevent physical damage or loss.

Brain Wallets:

A brain wallet is a wallet where the private key is generated and remembered in your mind. It's a risky option because if someone discovers your passphrase, they can access your Bitcoin.

Multisignature Wallets:

Multisignature wallets require multiple private keys to authorize a Bitcoin transaction, adding an extra layer of security. For example, a 2-of-3 multisig wallet would require two out of three private keys to initiate a transaction.

Custodial Wallets:

Custodial wallets are provided by third-party services (e.g., exchanges like Coinbase). In these wallets, the service holds your private keys, making it convenient but less secure, as you don't have full control over your funds.

Lightning Network Wallets:

The Lightning Network is a second-layer solution for Bitcoin that enables faster and cheaper transactions. Lightning wallets are designed for this network and provide instant payments. Examples include Zap and Eclair.

Bitcoin Payments:

Bitcoin payments are transactions involving the exchange of Bitcoin, the popular cryptocurrency, as a means of transferring value between parties. Bitcoin payments

have become increasingly popular for a wide range of use cases, including online purchases, remittances, investments, and more. Here's how Bitcoin payments work:

Sender Initiates Payment:

To make a Bitcoin payment, the sender (payer) initiates the transaction. The sender must have a Bitcoin wallet, which contains their private key. The private key is used to sign and authorize the transaction.

Recipient's Bitcoin Address:

The sender needs the recipient's Bitcoin address to send funds. The recipient provides their Bitcoin address, which is a cryptographic representation of their public key. It serves as an identifier for receiving payments.

Transaction Details:

The sender specifies the amount of Bitcoin to send and includes transaction details, such as any optional transaction fee (miners' reward), and a brief message or note if desired.

Digital Signature:

The sender's wallet signs the transaction with their private key, creating a digital signature. This signature is used to verify that the sender is the legitimate owner of the Bitcoins being spent.

Broadcasting the Transaction:

The sender's wallet broadcasts the signed transaction to the Bitcoin network. This is done by relaying the transaction to a Bitcoin node, which then propagates it to other nodes.

Transaction Confirmation:

The transaction is included in a block by a miner who successfully solves a cryptographic puzzle (proof-of-work). Once a transaction is included in a block, it is considered "confirmed." The first confirmation means the transaction is in one block, and more confirmations occur as additional blocks are added to the blockchain.

Recipient Acknowledges Payment:

When the recipient sees the incoming transaction on the blockchain, they acknowledge receipt of the payment. This can be an automated process for online merchants or a manual confirmation for peer-to-peer transactions.

Blockchain Record:

The details of the transaction, including sender, recipient, and amount, are recorded on the Bitcoin blockchain, ensuring transparency and immutability.

It's important to note that Bitcoin payments offer several advantages, such as security, low transaction fees (compared to traditional financial systems), and fast settlement times. However, Bitcoin transactions are irreversible once confirmed, so it's essential to double-check recipient addresses to avoid errors.

Bitcoin payments are versatile and can be used for everyday purchases, international remittances, investment, and more. Bitcoin's decentralized and borderless nature makes it a compelling option for individuals and businesses looking for alternatives to traditional payment methods.

Bitcoin Clients:

Bitcoin clients, also known as Bitcoin wallet software, are applications that allow users to interact with the Bitcoin network. These clients provide the functionality to send and receive Bitcoins, manage addresses, and monitor transactions. There are several Bitcoin client options available, each with its features and capabilities. Here are some of the most well-known Bitcoin clients:

Bitcoin Core: Bitcoin Core is the reference client developed by the Bitcoin community and is considered the original Bitcoin wallet. It is a full-node wallet, meaning it downloads and maintains a complete copy of the Bitcoin blockchain. Bitcoin Core is highly secure but requires substantial storage space and computational resources.

Electrum: Electrum is a lightweight Bitcoin wallet known for its speed and simplicity. It doesn't require users to download the entire blockchain but instead connects to remote servers. Electrum is available as both a desktop client and mobile app.

Armory: Armory is a feature-rich Bitcoin wallet designed for advanced users. It offers advanced security features, including the ability to create cold storage and multi-signature wallets. Armory is a desktop wallet.

Exodus: Exodus is a user-friendly desktop and mobile wallet known for its attractive interface and support for various cryptocurrencies, not just Bitcoin. It provides a built-in exchange feature for users to swap one cryptocurrency for another.

Mycelium: Mycelium is a mobile Bitcoin wallet that is popular for its user-friendliness and robust security features. It is designed for Android devices and offers advanced features like hardware wallet integration.

Trezor Suite: While Trezor is primarily known for its hardware wallets, they also offer the Trezor Suite software wallet. This software wallet can be used with or without a Trezor hardware device, providing an additional layer of security.

Ledger Live: Similar to Trezor, Ledger is a hardware wallet manufacturer that offers Ledger Live, a software wallet to manage cryptocurrencies. It supports various cryptocurrencies, including Bitcoin.

GreenAddress: Green Address is a web-based and mobile wallet that offers both ease of use and security features. It uses a multi-signature system to enhance the security of user funds.

Bitcoin Wallet by Coinbase: Coinbase offers a user-friendly online wallet for those who are new to Bitcoin. It also provides a cryptocurrency exchange platform.

However, please note that this is a custodial wallet, meaning Coinbase has control over your private keys.

Breadwallet (now BRD): BRD is a mobile wallet available on both iOS and Android. It is designed for simplicity and ease of use and is a non-custodial wallet, meaning you have control over your private keys.

Bitcoin Supply:

Bitcoin has a capped and limited supply, which distinguishes it from traditional fiat currencies that can be printed or issued by central banks without a fixed limit. The total supply of Bitcoin is limited to 21 million coins, making it a deflationary digital currency. Here's how the Bitcoin supply works:

Block Rewards: New Bitcoins are created and introduced into circulation as block rewards for miners who successfully add a new block to the blockchain. These block rewards serve as incentives for miners to secure and maintain the network.

Halving Events: Approximately every four years, the number of new Bitcoins created as block rewards undergoes a process known as "halving." During a halving event, the number of new Bitcoins issued to miners is reduced by 50%. The first halving occurred in 2012, reducing the block reward from 50 BTC to 25 BTC. Subsequent halving events have further reduced the reward.

First Halving (2012): Block reward reduced from 50 BTC to 25 BTC.

Second Halving (2016): Block reward reduced from 25 BTC to 12.5 BTC.

Third Halving (2020): Block reward reduced from 12.5 BTC to 6.25 BTC.

Fourth Halving (Expected around 2024): Block reward expected to reduce from 6.25 BTC to 3.125 BTC.

Maximum Supply: The Bitcoin protocol sets a maximum supply limit of 21 million Bitcoins. This cap is expected to be reached around the year 2140 when there will be no more block rewards issued to miners. From that point on, miners will rely solely on transaction fees for their incentives.

Transaction Fees: In addition to block rewards, miners receive transaction fees paid by users to include their transactions in a block. As block rewards decrease due to halving events, it is expected that transaction fees will become a more significant part of a miner's income.

The limited and capped supply of Bitcoin is designed to create scarcity, similar to precious metals like gold, and help maintain the value of the currency over time. This deflationary aspect, combined with the security and transparency of the blockchain, is one of the key features that make Bitcoin an appealing digital asset and store of value for many investors and users.