The Bitcoin Mechanics (Simple)

How Bitcoin Works (Blockchain, Mining, Transactions)

Blockchain: A blockchain is like a digital ledger or record book. Every time someone sends or receives Bitcoin, that transaction is recorded in a new "block". Each block is added to a chain of previous blocks, forming the blockchain. This ledger is stored on thousands of computers around the world, so it can't be changed or deleted. It ensures that every Bitcoin transaction is transparent and can be verified by anyone.

Nodes: Nodes are computers that run the Bitcoin software. They help keep the system running smoothly by checking transactions, keeping copies of the blockchain, and helping share updates with other users. By running a node, you become part of the system that keeps Bitcoin decentralised and trustworthy.

Transactions: When you send Bitcoin, your wallet creates a message that proves you own the coins and want to send them to someone else. This message is shared with the network and verified by nodes. If everything checks out, miners will include it in a block so that it becomes part of the permanent blockchain record.

Mining: Mining is the process of confirming transactions and adding them to the blockchain. It involves solving difficult puzzles using powerful computers. Miners compete to solve these puzzles, and the first one to succeed adds the next block to the chain and earns a reward. This process helps keep Bitcoin secure and also introduces new bitcoins into circulation.

Bitcoin Nodes

What is a Bitcoin Node:

Running a node is totally optional, but it gives you more control and trust in your Bitcoin use. So, what is a node? A node is simply a computer running Bitcoin software that connects to the network and helps enforce the rules. It stores a full copy of the Bitcoin blockchain and checks every transaction and block to make sure they are valid. This helps keep the network honest. By running a node, you don't have to trust any third parties, your own node will confirm that a payment is real and follows the rules. This gives you more privacy and peace of mind when using Bitcoin. Nodes also share information with other nodes, helping to spread updates and keep the whole system decentralised. The more nodes there are, the harder it is for anyone to cheat, lie, or shut down Bitcoin. Running a node won't earn you money, but it gives you independence and helps support the Bitcoin network.

Why Run a Bitcoin Node:

As mentioned, running a node lets you verify your own transactions without needing to trust anyone else. When you receive Bitcoin, the nodes checks that the payment is valid and confirmed on the blockchain. Each node acts like a checkpoint that ensures all transactions follow the same rules. This strengthens the network and makes it more resistant to censorship or attack. The more nodes that exist, the harder it is for any single person or group to interfere with Bitcoin. To run a node, you need a computer with a good amount of storage (at least 500 GB), a stable internet connection, and the Bitcoin Core software (which is free). While you don't earn money by running a node, you gain greater privacy, security, and a deeper understanding of how Bitcoin works.

Mining Bitcoin:

What is Mining:

Mining is the process of validating Bitcoin transactions and adding them to the blockchain. It plays a crucial role in keeping the network secure and up to date. Miners use specialised machines called ASICs (Application-Specific Integrated Circuits) that are built solely for the purpose of solving Bitcoin's complex mathematical puzzles. These machines are powerful but also very expensive and consume a lot of electricity, which is why mining is often done in places with access to cheap energy. For most everyday users, mining isn't necessary. It's usually better to learn how mining works and understand its importance rather than trying to do it yourself.

Mining Is Completely Optional: You do not need to mine Bitcoin in order to use it. Most people simply buy Bitcoin from an exchange or receive it as payment. Mining is typically done by people who want to support the network or try to earn new bitcoins as a reward. The process of mining helps confirm new transactions and keeps the blockchain running smoothly.

Mining Can Be Expensive: ASIC miners are not only costly to buy, but they also require a lot of electricity to run. In most places, the cost of electricity makes it hard to mine profitably unless you have access to very low-cost power. On top of that, the mining environment is very competitive. Since many people around the world are mining at the same time, it's difficult for one individual miner to find a new block and earn the reward alone. Because of this, most miners join mining pools. A mining pool is a group of miners who work together to solve blocks. When the pool successfully mines a block, the rewards are shared among all the participants based on how much work each one contributed. This allows smaller miners to receive more regular payouts, even if they could never find a block on their own.

Buying and Selling Bitcoin:

To get Bitcoin, most people use cryptocurrency exchanges or mobile apps. These are online platforms that allow you to buy Bitcoin using your local currency, such as pounds, dollars, euros, or any other type of fiat money. These services are easy to use and are the most common starting point for beginners.

How to Buy:

The basic process of buying Bitcoin on an exchange is simple. First, you sign up for an account on a trusted exchange. This involves choosing a strong password and securing your account. Most exchanges will then ask you to verify your identity. This usually means uploading a photo ID (like a passport or driver's licence) and sometimes a proof of address (such as a utility bill). This step is called KYC, “Know Your Customer”, and is required by law in many countries to prevent fraud and money laundering.

Once your account is verified, you can deposit money into it. Most exchanges accept bank transfers, debit cards, or sometimes even credit cards (although credit card purchases often come with extra fees or restrictions). After depositing funds, you can use them to buy Bitcoin at the current market price. Many platforms make this process as easy as clicking a “Buy” button and entering how much you want to purchase.

After buying Bitcoin, it is best practice to move it from the exchange into your own personal wallet. Keeping your Bitcoin in a wallet that you control gives you more security and ownership. If your Bitcoin stays on the exchange, you are relying on that company to keep it safe, which carries some risk. Transferring your Bitcoin to a wallet means you hold the private keys and have full control.

How to Sell:

Selling Bitcoin works much like buying, but in reverse. If you want to sell, you transfer your Bitcoin from your personal wallet back to the exchange. Once the Bitcoin is on the platform, you can sell it at the market price and receive fiat currency in return. You can then withdraw that money to your bank account. Most exchanges allow fast withdrawals via bank transfer or other payment methods. Be sure to check what fees apply before making a sale.

Some apps and exchanges also let you convert Bitcoin directly to other cryptocurrencies or even spend it using crypto debit cards, which automatically sell your Bitcoin at the time of purchase. While convenient, these features may come with higher fees or fewer privacy protections, so it’s good to compare your options.

Whether you're buying or selling, always use secure platforms, protect your login details, and stay aware of local laws or tax responsibilities in your area. With a bit of care, buying and selling Bitcoin is very straightforward and safe.

Wallets and Storage Options

A Bitcoin wallet is like a digital keychain. It doesn't actually hold coins like a physical wallet, instead, it stores the keys that give you access to your Bitcoin on the blockchain. Think of it as your personal control panel for sending, receiving, and managing your Bitcoin. Each wallet has a pair of keys: a public key, which is like your account number that you can share with others, and a private key, which is secret and used to approve or "sign" transactions, similar to a pin number. If someone gets access to your private key, they can spend your Bitcoin, so keeping it safe is essential.

Hot Wallets:

Hot wallets are wallets that are connected to the internet. These include mobile apps, desktop apps, and web wallets. Hot wallets are easy to use and convenient for everyday spending or small transactions. Since they're online, you can quickly access your Bitcoin anytime. However, being connected to the internet also makes them more vulnerable to hacking, phishing, and malware. For this reason, hot wallets are best used like a "current account", good for small amounts that you plan to use soon.

Cold Wallets:

Cold wallets, on the other hand, are offline wallets. These include hardware wallets (such as Ledger or Trezor devices) and paper wallets (where your keys are written or printed out and stored physically). Because they are not connected to the internet, cold wallets offer much higher security. They're considered the safest way to store Bitcoin for the long term, especially for larger amounts. Think of a cold wallet like a safe or vault, perfect for savings that you want to protect from online risks.

Custodial Wallets:

Custodial wallets are wallets where someone else (usually a company or exchange) holds the private keys on your behalf. This makes them easy to use, especially for beginners, since the provider manages the technical side of storage. However, it also means you're trusting that company to keep your Bitcoin safe and give it back when you want it. If something goes wrong (like a hack or the company shutting down), you could lose access to your funds. In this case, you don't truly "own" your Bitcoin, you're relying on a third party.

Non-Custodial Wallets:

Non-custodial wallets are wallets where you hold the private keys yourself. This gives you full control over your Bitcoin and means no one else can freeze, block, or take your funds. It's the most secure option if you manage it carefully, but it also means you're fully responsible for protecting your keys and backups. If you lose your private key or seed phrase and don't have a backup, your Bitcoin will be lost forever, there is no way to recover it.

What's Best:

Best practice is to use a non-custodial wallet, especially for savings or long-term holding. Always write down your wallet's backup phrase (usually 12 or 24 words shown when you first set it up) and store it safely offline: never share it or store it in cloud services or screenshots. That phrase is the only way to recover your Bitcoin if your wallet is lost or damaged. Treat it like the keys to your digital vault. By understanding the differences between wallet types and using a combination of convenience (hot wallets) and security (cold storage), you can protect your Bitcoin and use it confidently.

Making Transactions

Sending Bitcoin is easy, but you need to pay attention to the details to make sure everything goes smoothly. Once you understand the steps, it becomes a quick and safe process.

To send Bitcoin, you first need the receiver's Bitcoin address. This is a long string of letters and numbers that works like a bank account number. Many wallets also let you scan a QR code to make this easier and avoid typing mistakes. After that, you enter the amount of Bitcoin you want to send. Some wallets let you type the amount in your local currency and convert it for you. Next, you choose a transaction fee. This fee goes to Bitcoin miners who confirm your transaction. Most wallets will suggest a fee based on how busy the network is. If you want your payment to go through quickly, use a higher fee. If you're not in a rush, a lower fee can save you money. Once everything looks right: the address, the amount, and the fee, you simply confirm and send the transaction. After it's sent, your wallet will show the status.

Bitcoin transactions are confirmed when they are added to a new block in the blockchain. Each time a block is added, your transaction gets one "confirmation". For small payments, one confirmation is usually enough. For bigger payments, it's common to wait for up to six confirmations to be extra safe. Confirmations help make sure the payment is final and can't be reversed.

Safety and Self-Custody

Bitcoin gives you full control over your money, which is one of its biggest strengths. But with that control comes the responsibility to keep your Bitcoin safe. There's no bank to call if something goes wrong, so it's important to understand how to protect yourself.

Seed Phrase:

The most important thing to protect is your private key or seed phrase (usually 12 or 24 words shown when you set up a wallet). This is like the master key to your Bitcoin. If anyone else gets access to it, they can steal your funds, and there's no way to get them back. You should never share your seed phrase with anyone. Store it safely offline: write it down on paper or metal and keep it in a secure place. Never save it in cloud storage, take photos of it, or enter it on websites.

Scams:

You also need to watch out for scams. Some scammers promise to double your Bitcoin or claim they need your seed phrase to help you. These are always fake. No one needs your seed phrase except you. Also, always check the address you're sending Bitcoin to; scammers sometimes trick people into sending funds to the wrong place by swapping in fake addresses.

Security:

To stay secure, use a hardware wallet if you have a large amount of Bitcoin. These devices store your keys offline and are much harder to hack. If you use exchanges or apps, turn on two-factor authentication (2FA) for extra protection, this means you'll need a code from your phone in addition to your password. Lastly, it's smart to keep quiet about how much Bitcoin you own. Telling people can make you a target for scams or theft, so it's best to stay private about your holdings. By following these simple rules, you can enjoy the benefits of Bitcoin while staying safe and in control.

Common Mistakes to Avoid

Seed Phrase: Never share it with anyone, ever.

Sending to the wrong address: Always check the full address carefully.

Not backing up your wallet: If you lose your device without a backup, your Bitcoin is gone.

Leaving Bitcoin on exchanges: Exchanges can be hacked or go offline.

Using weak passwords or no 2FA: Make it hard for hackers to access your accounts.

Falling for scams: Always question offers that seem too good to be true.

Forgetting about taxes: Many countries require you to pay tax on Bitcoin gains.