Bitcoin

Satoshi Nakamoto introduced the bitcoin in the year 2008. Bitcoin is a cryptocurrency (virtual currency), or a **digital currency** that uses rules of cryptography for regulation and generation of units of currency. A Bitcoin fell under the scope of cryptocurrency and became the first and most valuable among them. It is commonly called **decentralized digital currency**.

A bitcoin is a type of digital assets which can be bought, sold, and transfer between the two parties securely over the internet. Bitcoin can be used to store values much like fine gold, silver, and some other type of investments. We can also use bitcoin to buy products and services as well as make payments and exchange values electronically.

A bitcoin is different from other traditional currencies such as **Dollar**, **Pound**, and **Euro**, which can also be used to buy things and exchange values electronically. There are no physical coins for bitcoins or paper bills. When you send bitcoin to someone or used bitcoin to buy anything, you don?t need to use a bank, a credit card, or any other third-party. Instead, you can simply send bitcoin directly to another party over the internet with securely and almost instantly.

How Bitcoin Works?

When you send an email to another person, you just type an email address and can communicate directly to that person. It is the same thing when you send an instant message. This type of communication between two parties is commonly known as Peer-to-Peer communication.

Whenever you want to transfer money to someone over the internet, you need to use a service of third-party such as banks, a credit card, a PayPal, or some other type of money transfer services. The reason for using third-party is to ensure that you are transferring that money. In other words, you need to be able to verify that both parties have done what they need to do in real exchange.

For example, Suppose you click on a photo that you want to send it to another person, so you can simply attach that photo to an email, type the receiver email address and send it. The other person will receive the photo, and you think it would end, but it is not. Now, we have two copies of photo, one is a simple email, and another is an original file which is still on my computer. Here, we send the copy of the file of the photo, not the original file. This issue is commonly known as the double-spend problem.

The double-spend problem provides a challenge to determine whether a transaction is real or not. How you can send a bitcoin to someone over the internet without needing a bank or some other institution to certify the transfer took place. The answer arises in a global network of thousands of computers called a Bitcoin Network and a special type of decentralized laser technology called **blockchain**.

In Bitcoin, all the information related to the transaction is captured securely by using maths, protected cryptographically, and the data is stored and verified across the entire network of computers. In other words, instead of having a centralized database of the third-party such as banks to certify the transaction took place. Bitcoin uses blockchain technology across a decentralized network of computers to securely verify, confirm and record each transaction. Since data is stored in a decentralized manner across a wide network, there is no single point of failure. This makes blockchain more secure and less prone to fraud, tampering or general system failure than keeping them in a single centralized location.

Bitcoin Mining

Bitcoin mining is the process of adding transaction records to Bitcoin's public ledger of past transactions. This ledger of past transactions is called the blockchain as it is a chain of blocks. Bitcoin mining is used to secure and verify transactions to the rest of the network.

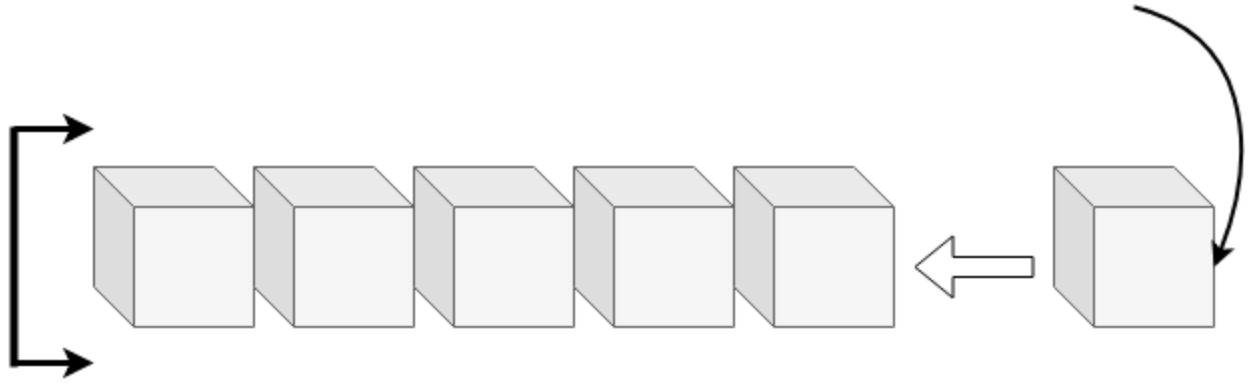
Role of Bitcoin Miners

Within the bitcoin networks, there are a group of people known as Miners. In miners, there was a process and confirm transactions. Anybody can apply for a minor, and you could run the client yourself. However, these minors use very powerful computers that are specifically designed to mine bitcoin transaction. They do this by actually solving math problems and resolving cryptographic issues because every transaction needs to be cryptographically encoded and secured. These mathematical problems ensure that nobody is tampering with that data.

Additionally, for this task, the minors are paid in bitcoins, which is the key component in bitcoin. In Bitcoin, you cannot create money as like you create regular fiat currencies such as Dollar, Euro, and Yuan. The bitcoin is created by rewarding these minors for their work in solving the mathematical and cryptographical problems.

How is the Bitcoin Blockchain built?

The role of a minor is to build the blockchain of records that forms the bitcoin ledger. These ledgers are called blocks, and each block contains all the different transactions that have taken place. A new block is added in every 10 minutes as a new Bitcoin Transaction takes place. So, as the minors process these different transactions, they build the block, and when a block is confirmed, it gets added to the blockchain. The bitcoin blockchain provides a permanent record of all bitcoin transactions to the beginning.



Blockchain Key Areas

In the blockchain technology, bitcoin is the best-known implementation of the blockchain. There is a lot of development and the direction is based on the premise of what blockchain does to enable Bitcoin to happen. We can learn and expand how it can spread into so many different areas.

The blockchain technology fixes three things that the Internet was not designed to do. These three things are:

1. Value
2. Trust
3. Reliability

Value

With blockchain, you can actually create value on a digital asset. The value can be controlled by that person who owns it. It enables a unique asset to be transferred over the internet without a middle centralized agent.

Trust

Blockchain enables to securely assign ownership of a specific digital asset and be able to track who actually controls that asset at a time. In other words, blockchain creates a permanent, secure, unalterable record of who owns what. It uses advanced hash cryptography to preserve the integrity of the information.

Reliability

Blockchain distributes their workload among thousands of different computers worldwide. It provides reliability because if you have everything localized in one location, it becomes a single point of failure. But, its decentralized network structure ensures that there is no single point of failure which could bring the entire system down.