Topic: What Bitcoin Is and How it Works

Target Site: Cypherpunkholdings.com

Word Count: 1092/1,000

What Bitcoin Is and How it Works

Bitcoin is the first and most widely recognized digital currency that was created in January 2009 anonymously by a group of technologists using the alias Satoshi Nakamoto. It allows the peer-to-peer exchange of value through the use of the decentralized protocol, cryptography and a public transaction ledger called a “blockchain”.

Bitcoin exists independently of any government, state or financial institution. It can be transferred globally without the need for a centralized intermediary. Bitcoin is legal to use, with varying restrictions across different regions, in all major economies. The coin is now a globally traded financial asset with a daily volume measured in tens of billions of dollars.

What is Bitcoin used for?

Bitcoin is used for transactional purposes outside the traditional financial system. The currency is used for international payments which are faster and more secure. Bitcoin provides lower transactional fees than through legal settlements methods.

With the increasing acceptance of cryptocurrencies, Bitcoin became more widely used and less competitive as a medium of exchange.

Bitcoin Features

1. **Decentralized:** Bitcoin network is not controlled by anybody. The network is made up of individual participants that are willing to agree to the rules of a protocol. Bitcoin is the most decentralized cryptocurrency. This feature is a major attribute that strengthens its position as an untouched collateral for the global economy.
2. **Transparent:** Additions of new transactions on the blockchain ledger and the state of the Bitcoin network

3. **Distributed:** All transactions carried out using Bitcoin are stored on a public ledger known as the blockchain. The network is designed to rely on people voluntarily storing copies of the ledger and running the Bitcoin protocol software. These nodes allow for the correct propagation of transactions across the blockchain network by following the protocol defined by the software client. With over 80,000 nodes globally, it is next to impossible for the network to suffer a loss of information or downtime.
4. **Peer-to-peer:** There is no need for any third party to act as an intermediary when used for payment. The payment goes directly from one person to the other.
5. **Public:** All transactions carried out on the Bitcoin network are recorded and publicly available for anyone on the network to see. This removes the possibility of fraudulent transactions. It also allows individuals to be tied to a specific Bitcoin address.
6. **Pseudo-anonymous:** Identity information is not tied to transactions carried out on the Bitcoin network. They are tied to specific addresses that take the form of random alphanumeric numbers.

How Bitcoin Works

Contrary to the images of shiny coins with a modified Thai baht symbol, Bitcoin actually is a software. It is a digital phenomenon with a set of protocols and processes. Bitcoin is abbreviated as BTC and it is referred to as an entity on its own.

Blockchain

Bitcoin is a network that is designed to work on a protocol known as the blockchain. Satoshi Nakamoto first described Bitcoin and the blockchain in a white paper in 2008. A blockchain consists of a single chain of discrete blocks of information that are arranged chronologically. Blockchain is sometimes referred to as a distributed ledger and it consists of transactional information. The Bitcoin blockchain is made public and anyone can download its entirety

Post-Trust

Contrary to the traditional currency that is transacted through a third party, usually a bank, the Bitcoin network is decentralized. No authority is required to preside over the network or keep the ledger. Everyone can keep an eye on the transactions carried out on the Bitcoin network. Bitcoin

is resistant to tampering. You don't need to trust anyone in particular for the system to function correctly.

Mining

This is a process that involves maintaining the public ledger. A network of miners secures the transactions carried out by Bitcoin users by recording the transactions on the blockchain. The Bitcoin software is designed to make the mining process artificially time-consuming. This makes fraudulent activities impossible. When mining, Bitcoin software adjusts the difficulty miners face to limit the network to a new 1-megabyte block of transaction every 10 minutes. This ensures the network has time to check the new blocks and the ledger ahead of it. By this, the volume of transactions carried out is digestible. Miners are rewarded for their work.

Halving

Miners are compensated with Bitcoin for verifying blocks of transactions. The reward given is cut into half for every 210,000 blocks mined or about every four years. This process is known as *halving.* The system is designed to reduce the rate at which new Bitcoin is released into circulation. This process ensures that the reward for Bitcoin mining is continued for a longer period, till about 2140.

The reward for each block mined became 6.25 after the third halving that took place on May 11, 2020. When all Bitcoin is mined from the code and halving is completed, miners will be encouraged by fees charged from network users.

Hashes

The hash technology allows the Bitcoin network to check the validity of a block. Network of miners, who are scattered across the globe, obtain a batch for a transaction data. They are required to run the data through a cryptographic algorithm that generates a "hash". Hash is a string of numbers and letters that check the information validity but does not reveal the information itself. To prevent fraudulent activities and ensure the network could not be spammed, the Bitcoin protocol requires proof of work during hashing.

Hashing, mining, and other details of the Bitcoin network might be irrelevant to most individuals involved in the Bitcoin network. Outside the mining community, Bitcoin owners usually purchase the cryptocurrency from exchange platforms. These are online platforms that enhance the buying, selling and trading of Bitcoin and other cryptocurrencies. Some of the common exchanges that facilitate the buying, selling and trading of Bitcoin are Coinbase and Binance.

For Bitcoin owners and traders to ensure the security of their digital currency, keys and wallets are utilized. A public key is a cryptographic code that allows you to receive cryptocurrencies into your account. A private key is a more sophisticated key that grants you access to your cryptocurrency. Public key functions more like a username, while a private key functions like a password.

Wallets are used to send and receive digital currencies. A bitcoin wallet is a digital wallet that stores the cryptographic information needed to access your Bitcoin address and make transactions. Digital wallets can either be cold wallets or hot wallets. Hot wallets are connected to the internet and cold wallets are not.