Some Bitcoin words you might hear

Bitcoin provides a new approach to payments and, as such, there are some new words that might become a part of your vocabulary. Don't worry, even the humble television created new words!

Choose your wallet
You need to know
Support Bitcoin

Table of contents

Address

A Bitcoin address is **like a physical address or an email**. It is the only information you need to provide for someone to pay you with Bitcoin.

Bitcoin

Bitcoin - with capitalization, is used when describing the concept of Bitcoin, or the entire network itself. e.g. "I was learning about the Bitcoin protocol today." bitcoin - without capitalization, is used to describe bitcoins as a unit of account. e.g. "I sent ten bitcoins today."

Block Chain

The block chain is a **public record of all Bitcoin transactions**, in chronological order. The block chain is shared between all Bitcoin users. It is used to verify the balance of Bitcoin addresses and to prevent double spending.

Block

A block is a **record in the block chain that contains and confirms many waiting transactions**. Roughly every 10 minutes, on average, a new block including transactions is appended to the block chain through mining.

BTC

BTC is the common unit of Bitcoin currency. It can be used in a similar way to USD for US dollar instead of ฿ or $.

Confirmation

Confirmation means that a transaction has been **verified by the network and is highly unlikely to be reversed**. One confirmation is pretty secure. Although for larger amounts (e.g. 1000 $USD and above), one can wait for a transaction to have more confirmations - six is a frequently chosen number. Each new confirmation decreases the risk of a reversal exponentially.

Cryptography

Cryptography is the branch of mathematics that lets us create **mathematical proofs that provide high levels of security**. Online commerce and banking already uses cryptography. In the case of Bitcoin, cryptography is used to make it impossible for anybody to spend funds from another user's wallet or to corrupt the block chain. It can also be used to encrypt a wallet, so that it cannot be used without a password.

Double Spend

If a malicious user tries to **spend their bitcoins to two different recipients at the same time**, this is double spending. Bitcoin mining and the block chain are there to create a consensus on the network about which of the two transactions will win.

Hash Rate

The hash rate is the **measuring unit of the processing power of the Bitcoin network**. The Bitcoin network must make intensive mathematical operations for security purposes. When the network reaches a hash rate of 10 TH/s, it means it can make 10 trillion calculations per second.

Mining

Bitcoin mining is the process of **making computer hardware do mathematical calculations for the Bitcoin network to confirm transactions** and increase security. As a reward for their services, Bitcoin miners can collect transaction fees for the transactions they confirm, along with newly created bitcoins. Mining is a specialized and competitive market where the rewards are divided up according to how much

calculation is done. Not all Bitcoin users do Bitcoin mining, and it is not an easy way to make money.

P2P

Peer-to-peer refers to **systems that work like an organized collective** by allowing each individual to interact directly with the others. In the case of Bitcoin, the network is built in such a way that each user is broadcasting the transactions of other users. And, crucially, no bank is required as a third party.

Private Key

A private key is a **secret piece of data that proves your right to spend bitcoins from a specific Bitcoin address** through a cryptographic signature. Each Bitcoin address has its own unique private key. Your private keys are stored in your computer if you use a software wallet; they are stored on some remote servers if you use a web wallet. Private keys must never be revealed as they allow you to spend bitcoins for their respective Bitcoin addresses.

Signature

A cryptographic signature is **a mathematical mechanism that allows someone to prove ownership**. In the case of Bitcoin, a Bitcoin address and its private key are linked by some mathematical magic. When your Bitcoin software signs a transaction with the appropriate private key, the whole network can see that the signature matches the Bitcoin address. However, there is no way for the world to guess your private key to steal your hard-earned bitcoins.

Wallet

A Bitcoin wallet is loosely **the equivalent of a physical wallet on the Bitcoin network**. The wallet actually contains your private keys which allow you to spend the bitcoins allocated to your Bitcoin addresses in the block chain. Each Bitcoin wallet can show you the total balance of all Bitcoin addresses it contains and lets you pay a specific amount to a specific person, just like a real wallet. This is different to credit cards where you are charged by the merchant.