Bitcoin Vocabulary

Source: https://bitcoin.org/en/vocabulary

Address

A Bitcoin address issimilar to a physical address or an email. It is the only information you need to provide for someone to pay you with Bitcoin. An important difference, however, is that each address should only be used for a single transaction.

Bit

Bit is a common unit used to designate a sub-unit of a bitcoin - 1,000,000 bits is equal to 1 bitcoin (BTC). This unit is usually more convenient for pricing tips, goods and services.

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."; it is also often abbreviated BTC or XBT.

Block Chain

The block chain is apublic record of Bitcoin transactionsin chronological order. The block chain is shared between all Bitcoin users. It is used to verify the permanence of Bitcoin transactions and to preventdouble spending.

Block

A block is arecord 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 theblock chainthroughmining.

BTC

BTC is a common unit used to designate one bitcoin.

Confirmation

Confirmation means that a transaction has beenprocessed by the network and is highly unlikely to be reversed. Transactions receive a confirmation when they are included in ablockand for each subsequent block. Even a single confirmation can be considered secure for low value transactions, although for larger amounts like $1000 USD, it makes sense to wait for 6 confirmations or more. Each confirmationexponentiallydecreases the risk of a reversed transaction.

Cryptography

Cryptography is the branch of mathematics that lets us createmathematical 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 theblock 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 tospend their bitcoins to two different recipients at the same time, this is double spending. Bitcoinminingand theblock chainare there to create a consensus on the network about which of the two transactions will confirm and be considered valid.

Hash Rate

The hash rate is themeasuring unit of the processing power of the Bitcoin network. The Bitcoin network must make intensive mathematical operations for security purposes. When the network reached a hash rate of 10 Th/s, it meant it could make 10 trillion calculations per second.

Mining

Bitcoin mining is the process ofmaking computer hardware do mathematical calculations for the Bitcoin network to confirm transactionsand 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 tosystems that work like an organized collectiveby 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 asecret piece of data that proves your right to spend bitcoins from a specific walletthrough a cryptographicsignature. Your private key(s) 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 wallet.

Signature

Acryptographicsignature isa mathematical mechanism that allows someone to prove ownership. In the case of Bitcoin, aBitcoin walletand itsprivate key(s)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 bitcoins being spent. However, there is no way for the world to guess your private key to steal your hard-earned bitcoins.

Wallet

A Bitcoin wallet is looselythe equivalent of a physical wallet on the Bitcoin network. The wallet actually contains yourprivate key(s)which allow you to spend the bitcoins allocated to it in theblock chain. Each Bitcoin wallet can show you the total balance of all bitcoins it controls 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.