

Blockchain Jargon Buster



These are some of the key concepts and terms to understand when talking about blockchain technologies.

Blockchain

Digital currencies that use cryptography to secure and verify transactions.

Cryptocurrency

Cryptocurrencies are digital currencies that use cryptography to secure and verify transactions.

Cryptography

Various mathematical techniques for encrypting and decrypting data, to keep it private when transmitted or stored electronically. Cryptography is also a skill used to communicate in or decipher secret writings or ciphers.

Decentralised

Not managed by any one central authority.

Digital Wallet

Instead of storing your money as a real-world wallet does, a digital wallet for cryptocurrencies saves your public and private keys (which you need to send and receive money). This gives you quick access to your funds and there are a wide range of options and support for different devices.

Iterative Content

During consensus, each node evaluates proposals from a specific set of peers, called chosen validators. Chosen validators represent a subset of the network which, when taken collectively, is "trusted" not to collude in an attempt to defraud the node evaluating the proposals. This definition of "trust" does not require that each individual chosen validator is trusted. Rather, validators are chosen based on the expectation they will not collude in a coordinated effort to falsify data relayed to the network.

Mining

Mining is the process by which recent cryptocurrency transactions are checked and new blocks are added to the blockchain.

Peer-to-peer Networks

In a peer-to-peer (P2P) network, the "peers" are computer systems which are connected to each other via the Internet. Files can be shared directly between systems on the network without needing a central server. In other words, each computer on a P2P network becomes a file server as well as a client.

Private Keys

Private keys act as personal digital signatures.

Proof of work

Proof of work is a protocol that has the main goal of deterring cyber-attacks such as a distributed denial-of-service attack (DDoS).

Ransomware

Malicious software designed to block access to a computer system until a sum of money is paid.

Single Point of Failure

A single point of failure (SPOF) is a critical system component that if failed, stops the whole system from working.

The most common cryptocurrencies



Bitcoin

The first ever cryptocurrency.



Bitcoin Cash

A variation of Bitcoin.



IOTA

Has removed dedicated miners from the process by asking the sender to handle the proof of work (PoW) using technology called Tangle.



Ethereum

A programmable currency that lets developers build different distributed apps and technologies that wouldn't work with Bitcoin.



NEO

Uses smart contracts which makes it more suited to all kinds of financial contracts and third-party distributed apps to be developed on top of it. Similar to Ethereum, but developed in China provides access to the biggest market in the world.



Litecoin

A variation of Bitcoin, which can generate blocks four times faster and have four times the maximum number of coins.



NEM

Unlike most other cryptocurrencies that work using proof of work algorithm, it uses "Proof of Importance" meaning you need some currency in order to acquire new coins - trying to encourage users to spend their currency rather than hold on to it.



Ripple

Unlike most cryptocurrencies, it doesn't use a blockchain for validating its transactions. Instead, a different process is used (iterative consensus) which makes it faster than Bitcoin but less safe, as it could be hacked.



Dash

A two-tier network. The first tier are miners that secure the network and record transactions, while the second one consists of 'master nodes' which relay transactions. Tier 1 is much faster than Bitcoin, whilst Tier 2 is completely anonymous.

What can you do with cryptocurrency?

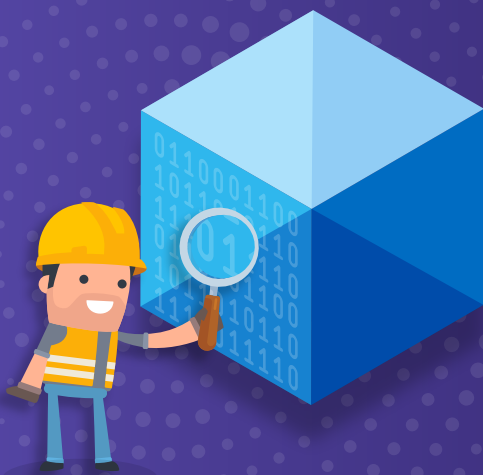
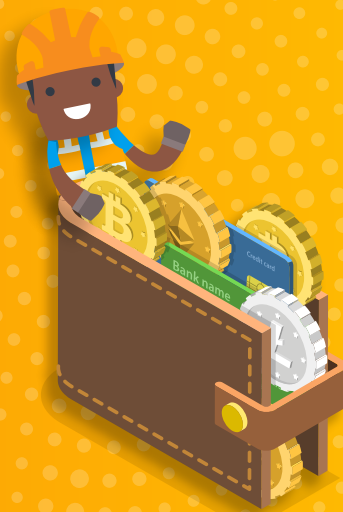


Buy Goods

More and more companies are accepting cryptocurrency as a way of paying for things – both online and offline.

Invest

People have been buying cryptocurrency in the hope of selling it off at a higher price – much like the way shares work. It is important to understand that cryptocurrencies are high-risk investments. The value rises and drops like no other investable item – and so need close attention, or you can quickly lose a lot of money.



Mine

Mining is critical in making any cryptocurrency network work, and to have the sufficient computer power to solve the ever-complicated cryptographic puzzles needs constant attention. As the difficulty of the puzzles constantly increases, so does the number of computers trying to solve it, making it harder for your computer to be credited with solving the algorithm and so acquire the associated transaction fee.