Crypto Glossary

A glossary of crypto words, crypto terms, and crypto definitions.

Search for a term...

Categories:

All | General | Slang and Memes | CoinMarketCap Specific

#

51% Attack:
If more than half the computer power or mining hash rate on a network is run by a single person or a single group of people, then a 51% attack is in operation. This means that this entity has full control of the network and can negatively affect a cryptocurrency by taking over mining operations, stopping or changing transactions, and double-spending (reusing) coins.

A

Address:
A place where cryptocurrency can be sent to and from, in the form of a string of letters and numbers. A cryptocurrency address can be shared publicly in the form of text or QR code to those who want to send you cryptocurrency.

Airdrop:
A marketing campaign that distributes a specific cryptocurrency or token to an audience. It is usually initiated by the creator of a cryptocurrency in order to encourage use and build popularity of the coin or token. Most airdrop campaigns run with mechanics such as receiving coins or tokens in exchange for simple tasks like sharing news, referring friends or downloading an app.

Algorithm:
A process or set of rules to be followed in problem-solving or calculation operations, usually by a computer, although humans tend to follow steps algorithmically as well (let’s say doing math or following a recipe).

Anarcho-capitalism:
A political philosophy and school of thought that believes in removing centralized states in favor of self-ownership, private property and free markets. Many of the early adopters of Bitcoin were proponents of anarcho-capitalism, believing it would give power and control back to the masses.

Anti-Money Laundering (AML):

A set of international laws enacted to curtail criminal organizations or individuals laundering money through cryptocurrencies into real-world cash.

Arbitrage:
A practice of taking advantage of differences in price of the same commodity in two or more markets or exchanges. For example, cryptocurrency prices on Korean exchanges can be different from those on US exchanges. An arbitrage trader would be in both markets in order to buy in one and sell in another for profit.

ASIC:
Short for “Application Specific Integrated Circuit”; it is a mining equipment that is used specifically to mine a certain cryptocurrency. Often compared to GPUs, ASICs are specially created and bought for mining purposes and offer significant efficiency improvements and power savings due to its narrow use case.

Ask Price:
In any financial market, buyers and sellers place their orders to determine the highest price they are willing to buy and the lowest price they are willing to sell. The buyers place “bids" and sellers place "asks," or offers to sell. If a "bid" is higher than an "ask," a trade occurs, as the buyer is willing to pay more than what the seller wants. At any given point in time, the lowest ask order that is unmatched becomes the "Ask Price" of the market.

Atomic Swap:
A way of letting people directly exchange one type of cryptocurrency for another on a different blockchain or off-chain without a centralized intermediary such as an exchange.

Attestation Ledger:
An attestation ledger is an account book designed to provide evidence of individual transactions. It is generally used to “attest” that a financial transaction took place, or to prove authenticity of transactions or products.

B

Bear:
A person who is pessimistic about market prices and expects them to decline. This person is also known to be "bearish" about the market or price. *see Bull.

Bear Trap:
A technique played by a group of traders, aimed at manipulating the price of a cryptocurrency. The bear trap is set by selling a large amount of the same cryptocurrency at the same time, fooling the market into thinking there is an upcoming price decline. In response, other traders sell their assets, further driving the price down. Those who set the trap then release it, buying back their assets at a lower price. The price then rebounds, allowing them to make a profit.

Bitcoin ATM (BTM):
A machine from which you can withdraw bitcoin.

Bitcoin Improvement Proposal (BIP):
A technical design document providing information to the Bitcoin community, describing new proposed features, processes or environments affecting the Bitcoin protocol. Suggested changes to the protocol are submitted as a BIP. The BIP author is responsible for soliciting feedback and consensus for his or her suggested improvements within the community, and documenting dissenting opinions.

BitLicense:
A business license issued to cryptocurrency companies in New York, created and provided by the New York State Department of Financial Services (NYSDFS).

Bits:
A sub-unit of one bitcoin. There are 1,000,000 bits in one bitcoin.

Block:
A container or collection of transactions occurring every time period on a blockchain.

Block Explorer:
An online tool to view all transactions that has taken place on the blockchain, network hash rate and transaction growth, among other useful information.

Block Height:
The number of blocks preceding the block in question on the blockchain, or can be thought of as total blocks in the chain before this point.

Block Reward:
An incentive for a miner who successfully calculates a valid hash in a block during mining. By contributing to the security and liveness of the chain, the miner is rewarded with this incentive, ensuring that miners continue to act in the best interest of the blockchain by legitimately taking part in the process (instead of hacking it).

Bollinger Band:
A tool developed by Bollinger to help in the recognition of systemic pattern recognition in prices; it is a band that is plotted two standard deviations away from the simple moving average, or exponential moving average in some cases.

Brute Force Attack (BFA):
A method of trial-and-error in which automated software generates and tries a large number of possible combinations in order to crack a code or key.

Bubble:
A bubble describes a situation where market participants drive prices up above their value, which is usually followed by a steep, rapid drop in prices as the market corrects.

Bug Bounty:
A reward offered for finding vulnerabilities and issues in computer code. It is often offered by cryptocurrency companies like protocols, exchanges and wallets to identify potential security breaches or bugs before they are exploited by unfriendly parties.

Bull:
A person that is optimistic and confident that market prices will increase. This person is also known to be "bullish" about the market or price. *see Bear.

Bull Trap:
A false market signal where the declining trend of an asset appears to be on the upturn, but does not actually materialize, leading bulls to lose money after going long.

Buy Wall:
A situation where a large limit order has been placed to buy when a cryptocurrency reaches a certain value. This can sometimes be used by traders to create a certain impression in the market, preventing a cryptocurrency from falling below that value, as demand will likely outstrip supply when the order is executed.

Byzantine Generals' Problem:
A situation where communication that requires consensus on a single strategy from all members within a group or party cannot be trusted or verified. An example of this agreement problem is where a group of generals, encircled around a city, must decide whether to attack or retreat. Every general must agree to attack or retreat, or everyone will be worse off. Some generals may be treacherous, voting falsely, and messengers may deliver false votes. Under these circumstances, a consensus must be reached. In cryptocurrency, when network participants post false or inaccurate information to others about transactions taking place, it could lead to network failure. *see Byzantine Fault Tolerance (BFT).

Byzantine Fault Tolerance (BFT):
A property of fault-tolerant distributed computing systems, reaching consensus through a mechanism, where components may fail and there may be imperfect information. For example, Bitcoin is Byzantine Fault Tolerant, utilizing the proof-of-work system to reach consensus on the blockchain. Its applications are beyond blockchain, including messaging and networking systems, among others.

C

Candlesticks:
A candlestick chart is a graphing technique used to show changes in price over time. Each candle provides 4 points of information: opening price, closing price, high, and low. Also known as "candles" for short.

Cash:
Cash is physical form of a currency, such as banknotes or coins.

Centralized:
An organization structure in which a small number of nodes is in control of an entire network.

Central Ledger:
A ledger maintained by a centralized agency (such as a bank) that records all financial transactions.

Central Processing Unit (CPU):
Central Processing Unit, also known as a processor or CPU, is defined as the “brains” of the computer, coordinating different components running on a computer. CPU clock speed is measured in gigahertz or GHz for short.

Change:
Bitcoin transactions are made up of inputs and outputs in a system called Unspent Transaction Output. When you send bitcoins, you can only send them in a whole output, and the rest are sent back as change.

Chargeback:
A demand made by a credit-card provider for a retailer to make good on the loss on a fraudulent or disputed transaction, reversing said payment or money transfer after it was authorized.

Chain Split:
Another term used to describe Fork.

Cipher:
The name given to the algorithm that encrypts and decrypts information.

Client:
Software that can access and process blockchain transactions on a local computer. A common application of this is a cryptocurrency software wallet.

Close:
Refers to the closing price; similar to the same term used in financial stocks.

Cloud Mining:
Mining with remote processing power rented from companies operating outfits in countries like Iceland, where the electricity is abundant and cost-efficient, and the ambient temperature is cold year-round. Another term for this is mining contract.

Coinbase:
First designed in the Bitcoin system, a coinbase is a compulsorily-included transaction on a block, the output of which directs where to send the mining reward. In the Bitcoin system, the coinbase has a 100 byte size input, where messages can be attached or used as an extra nonce.

Cold Storage:
Offline storage of cryptocurrencies, typically involving hardware non-custodial wallets, USBs, offline computers or paper wallets. *see Hot Storage.

Cold Wallet:
A cryptocurrency wallet that is in cold storage, i.e. not connected to the internet.

Confirmations:
A transaction is only confirmed when it is included in a block on the blockchain, at which point it has one confirmation. Each additional block is another confirmation. Different exchanges require a different number of confirmations to consider a cryptocurrency transaction final.

Consensus:
Consensus is achieved when all participants of the network agree on the order and content of blocks and transactions contained in those blocks.

Consortium Blockchain:
A privately owned and operated blockchain in which a consortium shares information not readily available to the public, while relying on the immutable and transparent properties of the blockchain.

Correction:
A correction is a (usually negative) reverse movement of at least 10% in a cryptocurrency or general market, to adjust for over- or under-valuations.

Co-Signer:
A person or entity that has partial control and access over a cryptocurrency wallet.

Cryptoasset:

Cryptoassets leverage cryptography, consensus algorithms, distributed ledgers, peer-to-peer technology and/or smart contracts to function as a store of value, medium of exchange, unit of account or decentralized application.

Cryptocurrency:
A cryptocurrency is a digital medium of exchange using strong cryptography to secure financial transactions, control the creation of additional units, and verify the transfer of assets.

Cryptography:
A field of study and practice to secure information, preventing third parties from reading information to which they are not privy.

Cryptographic Hash Function:
Cryptographic hashes produce a fixed-size and unique hash value from variable-size transaction input. The SHA-256 algorithm is an example of a cryptographic hash function.

Custodial:
Usually referring to the storage of keys in relation to wallets or exchanges, a custodial set-up is one in which private keys are being held by the service provider while they provide a login account. *see Non-custodial.

D

Dark Web:
A portion of internet content existing on darknets, not indexed by search engines, that can only be accessed with specific software, configurations or authorizations.

Decentralized Applications (DApps):
A type of application that runs on a decentralized network, avoiding a single point of failure.

Decentralized Autonomous Initial Coin Offerings (DAICO):
A method for decentralized funding of projects, combining ideas from Decentralized Autonomous Organizations (DAOs) and initial coin offerings (ICOs), proposed by Vitalik Buterin, creator of Ethereum. It introduces a form of governance in the ICO process, allowing backers to vote for the return of their funds if certain conditions are met.

Decentralized Autonomous Organizations (DAO):
An organization that is run through rules encoded in smart contracts.

Decryption:
The process of transforming data that has been rendered unreadable through encryption back to its unencrypted form.

DeFi:
DeFi (decentralized finance) is the creation of an ecosystem of financial tools built on blockchain. Also known as open finance, DeFi apps take traditional financial services and rebuild them as open and permissionless.

Deflation:
Reduction of the general level of prices in an economy. May also refer to deflationary monetary policy, such as Bitcoin, where there is a fixed supply of coins.

Delegated Proof-of-Stake (dPOS):
A consensus mechanism where users can vote for delegates producing blocks on the blockchain, with votes proportional to their stake. It aims to increase efficiency and environmental friendliness of blockchain consensus protocols.

Depth Chart:
A graph that plots the requests to buy (bids) and the requests to sell (asks) on a chart, based on limit orders. The chart shows the point at which the market is most likely to accept a transaction.

Deterministic Wallet:
A type of wallet that derives keys from a starting point called a seed. As long as you have this seed, you are able to backup and restore any wallet. *see Hierarchical Deterministic Wallet (HD Wallet).

Difficulty:

A relative measure of how difficult it is to discover a new block. In Bitcoin, the difficulty is adjusted periodically as a function of how much hashing power has been deployed by the network of miners.

Digital Commodity:
An intangible asset that is transferred electronically, and has a certain value.

Digital Currency:
Digital currency, also known as digital money or electronic money or electronic currency, is a type of currency available only in digital form, allowing for instantaneous transactions and borderless transfer-of-ownership.

Digital Identity:
Digital representations and storage of personal information such as name, address, social security number and more; on the blockchain, digital identity can be decentralized and used for identity verification in a secure manner.

Digital Signature:
A digital code generated by key encryption that is attached to an electronically transmitted document to verify its contents and the sender's identity.

Directed Acyclic Graph (DAG):
A directed acyclic graph or DAG is a structure that is built out in one single direction and in such a way that it never repeats.

Dildo:
In the non-sexual connotation (get your mind out of the gutter!), a dildo is a long green or red bar found on a graph showing the changes in price of a cryptocurrency, in relation to the green and red candles found on price charts.

Distributed Consensus:
Collective agreement by various computers in a network enabling it to work in a decentralized manner without a central authority.

Distributed Denial of Service (DDoS) Attack:
A cyber-attack in which the perpetrator seeks to make a machine or network resource unavailable, disrupting services of a host connected to the internet, by overloading the system with requests so that legitimate requests cannot be served.

Distributed Ledger:
Distributed ledgers are ledgers in which data is stored across a network of decentralized nodes. A distributed ledger does not necessarily involve a cryptocurrency and may be permissioned and private.

Distributed Ledger Technology (DLT):
The technology underlying distributed ledgers. This term is most often discussed in the context of enterprise use cases around adoption of distributed ledger technology.

Distributed Network:
A type of network where processing power and data are spread over the nodes without a centralized data center or authority.

Double Spending:
A situation where a sum of money is (illegitimately) spent more than once.

Dump:
To sell off all your coins.

Dumping:
The action of collective market sell-offs, creating downward price movement.

Dust Transactions:
Minuscule transactions that flood and slow the network, usually deliberately created by people looking to disrupt it.

Dusting Attack:
When a scammer sends tiny amounts of a cryptocurrency to random users' wallets, and then analyzes and tracks the subsequent transactions in order to identify the specific users behind each address.

E

Enterprise Ethereum Alliance (EEA):
A group of Ethereum developers, startups and large corporations working together to commercialize and use Ethereum for business applications.

Emission:
Emission, also known as Emission Curve, Emission Rate and Emission Schedule, is the speed at which new coins are created and released.

ERC-20:
A token standard for Ethereum, used for smart contracts implementing tokens. It is a common list of rules defining interactions between tokens, including transfer between addresses and data access.

ERC-721:
A token standard for non-fungible Ethereum tokens. An Ethereum Improvement Proposal introduced in 2017, it enables smart contracts to operate as tradeable tokens similar to ERC-20 tokens.

Escrow:
An escrow is a contractual arrangement in which a third party receives and disburses money or documents for the primary transacting parties, with the disbursement dependent on conditions agreed to by the transacting parties. This is possible to be automated using smart contracts on the blockchain.

Ether:
The form of payment used in the operation of the distribution application platform, Ethereum, in order to incentivize machines into executing the requested operations.

Ethereum Improvement Proposal (EIP):
Ethereum Improvement Proposals (EIPs) describe standards for the Ethereum platform, including core protocol specifications, client APIs, and contract standards.

Ethereum Virtual Machine (EVM):
A Turing-complete virtual machine that enables execution of code exactly as intended; it is the runtime environment for every smart contract. Every Ethereum node runs on the EVM to maintain consensus across the blockchain.

Exchange:
Cryptocurrency exchanges (sometimes called digital currency exchanges) are businesses that allow customers to trade cryptocurrencies for fiat money or other cryptocurrencies.

Exchange Traded Fund (ETF):
A security that tracks a basket of assets such as stocks, bonds, and cryptocurrencies but can be traded like a single stock.

F

Faucet:
A cryptocurrency reward system usually on a website or app, that rewards users for completing certain tasks. It is mostly a technique used when first launching an altcoin to interest people in the coin.

Fiat:
Fiat currency is “legal tender” backed by a central government, such as the Federal Reserve, and with its own banking system, such as fractional reserve banking. It can take the form of physical cash, or it can be represented electronically, such as with bank credit.

Fiat-Pegged Cryptocurrency:
Also known as “pegged cryptocurrency,” it is a coin, token or asset issued on a blockchain that is linked to a government- or bank-issued currency. Each pegged cryptocurrency is guaranteed to have a specific cash value in reserves at all times.

Flipping:
An investment strategy (mostly popularized by real estate investing) where you buy something with the goal of reselling for a profit later, usually in a short period of time. In the context of ICOs, flipping refers to the strategy of investing in tokens before they are listed on exchanges, then quickly reselling them for a profit when they start trading on exchanges in the secondary market.

Fork (Blockchain):
Forks, or chain splits, create an alternate version of the blockchain, leaving two blockchains to run simultaneously. An example is Ethereum and Ethereum Classic, which was forked after the DAO hack.

Fork (Software):
A software fork, also known as a project fork, is when developers take the technology (source code) from one existing software project and modify it to create a new project. An example is Litecoin, which was a software fork of Bitcoin.

Full Node:
Nodes that download a blockchain's entire history in order to observe and enforce its rules.

Fundamental Analysis (FA):
A method in which you research the underlying value of an asset by looking at the technology, team, growth prospects and other indicators. Some people perform fundamental analysis as part of an investment strategy called "value investing."

G

Gains:
Gains refer to an increase in value or profit.

Gas:
A term used on the Ethereum platform that refers to a unit of measuring the computational effort of conducting transactions or smart contracts, or launch DApps in the Ethereum network. It is the "fuel" of the Ethereum network. *see Gas Limit and Gas Price.

Gas Limit:
A term used on the Ethereum platform that refers to the maximum amount of gas the user is willing to spend on a transaction.

Gas Price:
A term used on the Ethereum platform that refers to the price you are willing to pay for a transaction. Setting a higher gas price will incentivize miners to prioritize that transaction over others.

Genesis Block:
The first block of data that is processed and validated to form a new blockchain, often referred to as block 0 or block 1.

Gold-Backed Cryptocurrency:
A coin or token issued that represents a value of gold; for example, one physical gram of gold equals one coin. The gram of gold is stored in a safe and can be traded with other coin holders.

Graphical Processing Unit (GPU):
More commonly known as a graphics card, it is a computer chip that creates 3D images on computers, but has turned out to be efficient for mining cryptocurrencies.

Group Mining:
Another term used to describe a Mining Pool.

Gwei:
The denomination used in defining the cost of gas in transactions involving Ether.

H

Hacking:
Hacking is the process of using a computer to manipulate another computer or computer system in an unauthorized fashion.

Halving:
An event in which the total rewarded bitcoin per confirmed block halves, happening every 210,000 blocks mined.

Hard Cap:
The maximum amount that an ICO will raise. If a hard cap is reached, no more funds will be collected. *see Soft Cap.

Hard Fork (Blockchain):

A type of protocol change that validates all previously invalid transactions, and invalidates all previously valid transactions. This type of fork requires all nodes and users to upgrade to the latest version of the forked protocol software. In a hard fork, a single cryptocurrency permanently splits into two, resulting in one blockchain that follows the old protocol and the other that follows the newest protocol. Some examples are Bitcoin and Bitcoin Cash, or Ethereum and Ethereum Classic. *see Soft Fork.

Hash:
The act of performing a hash function on input data of arbitrary size, with an output of fixed length that looks random and from which no data can be recovered without a cipher. An important property of a hash is that the output of hashing a particular document will always be the same when using the same algorithm.

Hash Function:
Any function used to map data of arbitrary size to data of a fixed size. *see Cryptographic Hash Function.

Hash Power / Hash Rate:
A unit of measurement for the amount of computing power being consumed by the network to continuously operate. The Hash Rate of a computer may be measured in kH/s, MH/s, GH/s, TH/s, PH/s or EH/s depending on the hashes per second being produced.

Hierarchical Deterministic Wallet (HD Wallet):
A wallet that uses Hierarchical Deterministic (HD) protocol to support the generation of crypto-wallets from a single master seed using 12 mnemonic phrases. *see Deterministic Wallet.

Hidden Cap:
Hidden cap is an unknown limit to the amount of money a team elects to receive from investors in its initial coin offering (ICO). The purpose of a hidden cap is to even the playing field by letting smaller investors put in money, without the large investors forming an accurate understanding of the total cap and adjusting their investment as a result.

Hosted Wallet:
A wallet managed by a third-party service.

Hot Storage:
The online storage of private keys allowing for quicker access to cryptocurrencies. *see Cold Storage.

Hot Wallet:
A cryptocurrency wallet that is connected to the internet for hot storage of cryptoassets, as opposed to an offline, cold wallet with cold storage. *See Cold Wallet.

Hybrid PoW/PoS:
A hybrid PoW/PoS allows for both proof-of-stake and proof-of-work as consensus distribution algorithms on the network. This approach aims to bring together the security of PoW consensus and the governance and energy efficiency of PoS.

Hyperledger (Hyperledger Foundation):
Hyperledger is an umbrella project of open source blockchains and blockchain-related tools started by the Linux Foundation in 2015 to support the collaborative development of blockchain-based distributed ledgers.

I

Immutable:
A property that defines the inability to be changed, especially over time.

Inflation:
A general increase in prices and fall in the purchasing value of money.

Initial Coin Offering (ICO):
A type of crowdfunding, or crowdsale, using cryptocurrencies as a means of raising capital for early-stage companies. It has come under fire due to the occurrence of scams and market manipulators.

Initial Exchange Offering:
An initial exchange offering (IEO) refers to a fundraising event where a cryptocurrency exchange raises money on its own platform, as opposed to an ICO, where a team conducts the fundraising. *See Initial Coin Offering.

Initial Token Offering (ITO):
Similar to ICOs, but the focus is on the offering of tokens with proven (or unproven) intrinsic utility in the form of software or usage in an ecosystem.

Initial Bounty Offering (IBO):
An initial bounty offering or IBO is the limited-time process by which a new cryptocurrency is made public and distributed to people who invest time and skill into earn rewards in the new cryptocurrency, such as doing translation or marketing. Unlike an initial coin offering where you can buy coins, an IBO requires more mental commitment from the receiver.

Instamine:
A period in time, shortly after launch, when a large portion of total mineable coins or tokens are mined in a compressed time frame, and may be unevenly and quickly distributed to investors.

Intermediary / Middleman:
An intermediary, or middleman, is a person or entity that acts as the go-between different parties to bring about agreements or carry out directives.

K

KYC:
Acronym for “Know Your Customer,” this process refers to a project’s or financial institution’s obligations to verify the identity of a customer in line with global anti-money laundering laws.

L

Ledger:
A record of financial transactions that cannot be changed, only appended with new transactions.

Leverage:
A loan offered by a broker on an exchange during margin trading to increase the availability of funds in trades.

Lightning Network:
The Lightning Network is a "second layer" payment protocol that operates on top of a blockchain. Theoretically, it will enable fast, scalable transactions between and across participating nodes, and has been touted as a solution to the Bitcoin scalability problem.

Limit Order / Limit Buy / Limit Sell:
Orders placed by traders to buy or sell a cryptocurrency when a certain price is reached. This is in contrast with market orders at which a cryptocurrency is sold at the current best available price.

Liquidity:
How easily a cryptocurrency can be bought and sold without impacting the overall market price.

Long:
A situation where you buy a cryptocurrency with the expectation of selling it at a higher price for profit later.

M

Mainnet:
An independent blockchain running its own network with its own technology and protocol. It is a live blockchain where its own cryptocurrencies or tokens are in use, as compared to a testnet or projects running on top of other popular networks such as Ethereum.

Market Order / Market Buy / Market Sell:
A purchase or sale of a cryptocurrency on an exchange at the current best available price. Market orders are filled as buyers and sellers are willing to trade. This is in contrast with limit orders at which a cryptocurrency is sold only at a specified price.

Margin Call:
When an investor's account value falls below the margin maintenance amount. The broker will then demand that the investor deposit additional money or securities to meet the minimum required maintenance amount to continue trading.

Masternodes:
Masternodes are a server maintained by its owner, somewhat like full nodes, but with additional functionalities such as anonymizing transactions, clearing transactions, and participating in governance and voting. It was initially popularized by Dash to reward owners of these servers for maintaining a service for the blockchain.

Merkle Tree:
A tree structure in cryptography, in which every leaf node is labelled with the hash of a data block and every non-leaf node is labelled with the cryptographic hash of the labels of its child nodes. Hash trees allow efficient and secure verification of the contents of blockchains, as each change propagates upwards so verification can be done by simply looking at the top hash.

MicroBitcoin (uBTC):
One millionth of a bitcoin or 0.000001 of a bitcoin. Often confused as a fork of Bitcoin.

Microtransaction:
A business model where very small payments can be made in exchange for common digital goods and services, such as pages of an ebook or items in a game.

Miners:
Contributors to a blockchain taking part in the process of mining. They can be professional miners or organizations with large-scale operations, or hobbyists who set up mining rigs at home or in the office.

Mining:
A process where blocks are added to a blockchain, verifying transactions. It is also the process through which new bitcoin or some altcoins are created.

Mining Contract:
Another term for cloud mining, where users can rent or invest in mining capacity online.

Mining Pool:
A setup where multiple miners combine their computing power to gain economies of scale and competitiveness in finding the next block on a blockchain. Rewards are split according to different agreements, depending on the mining pool. Another term for this is Group Mining.

Mining Reward:
The reward resulting from contributing computing resources to process transactions. Mining rewards are usually a mix of newly-minted coins and transaction fees.

Mining Rig:
A computer being used for mining. A mining rig could be a dedicated piece of hardware for mining, or a computer with spare capacity that can be used for other tasks, only mining part time.

Mixing Service:
Also known as a tumbler, it is a service to improve the privacy and anonymity of cryptocurrency transactions by mixing potentially identifiable or "tainted" cryptocurrencies with other unrelated transactions, making it harder to track what the cryptocurrency was used for and who it belongs to.

Mnemonics:
Mnemonics are memory aids with a system such as letters or associations that help in recall. *see Mnemonic Phrase.

Mnemonic Phrase:
A mnemonic phrase (also known as mnemonic seed, or seed phrase) is a list of words used in sequence to access or restore your cryptocurrency assets. It should be kept secret from everyone else. It is a standard in most HD wallets.

Money Transmitter/Money Transfer License:
In the legal code of the United States, a money transmitter or money transfer service is a business entity that provides money transfer services or payment instruments, whether it is real currency, cryptocurrency or any other value. Money transmitters in the US are part of a larger group of entities called money service businesses or MSBs.

Moving Average Convergence Divergence (MACD):

A technical analysis method, it is a trend-following momentum indicator that shows the relationship between two price moving averages. The calculation is done by subtracting the 26-day exponential moving average (EMA) from the 12-day EMA.

Mt. Gox:
Mtgox or Mt. Gox was one of the first websites where users could take part in fiat-to-bitcoin exchange (and vice versa). In 2014, Mt. Gox was shut down after about 850,000 bitcoin was declared lost or stolen. Mt. Gox was created in 2006 by Jed McCaleb who named it after Magic: The Gathering Online Exchange where users could use the cards like stocks. Jed later sold Mt. Gox to Mark Karpelès in 2011.

Multi-Signature (Multi-sig):
Multi-signature addresses provide an added layer of security by requiring more than one key to authorize a transaction.

N

Network:
A network refers to all nodes in the operation of a blockchain at any given moment in time.

Node:
A copy of the ledger operated by a participant of the blockchain network.

Non-custodial:
Usually referring to the storage of keys, in relation to wallets or exchanges, a non-custodial setup is one in which private keys are held by the user directly. *see Custodial.

Nonce:
When a transaction is hashed by a miner, an arbitrary number meant to be used only once is generated, called a nonce.

O

Off-Ledger Currency:
A currency that is created (minted) outside of the specified blockchain ledger but is accepted or used.

Offline Storage:
The act of storing cryptocurrencies in devices or systems not connected to the internet. *see Online Storage.

On-Ledger Currency:
A currency that is both minted on the blockchain ledger and also used on the blockchain ledger, such as bitcoin.

Online Storage:
The act of storing cryptocurrencies in devices or systems connected to the internet. Online storage offers more convenience but also increased risk of theft. *see Offline Storage.

One Cancels The Other Order (OCO):
A situation where two orders for cryptocurrency are placed simultaneously, with a rule in place to enforce that if one is accepted, the other is cancelled.

Open/Close:
The price at which a cryptocurrency opens at a time period, for example at the start of the day; the price at which a cryptocurrency closes at a time period, for example at the end of the day. In general, these terms were more useful in traditional financial markets as there are fixed hours of the day in which trading occurs.

Open Source:
Open source software is a type of software released under a license in which the copyright holder grants users the rights to study, change, and distribute the software to anyone and for any purpose. It is also a philosophy, with participants believing in the free and open sharing of information in pursuit of the greater common good.

Oracles:

An agent that finds and verifies information, bridging the real world and the blockchain by providing data to smart contracts for execution of said contracts under specified conditions.

Orphan:
A valid block on the blockchain that is not part of the main chain. They may come into existence when two miners produce blocks at similar times, or caused by an attacker attempting to reverse transactions. This is sometimes also known as a “detached block.”

Overbought:
When a cryptocurrency has been purchased by more and more investors over time, with its price increasing for an extended period of time. When this happens without any justifiable reason, the cryptocurrency is considered overbought, and a period of selling is expected.

Oversold:
When a cryptocurrency has been sold by more and more investors over time, with its price decreasing for an extended period of time. When this happens without any justifiable reason, the cryptocurrency is considered oversold, and a period of buying is expected.

P

Paper Wallet:
A physical document containing your private key or seed phrase.

Peer to Peer (P2P):
The decentralized interactions between parties in a distributed network, partitioning tasks or workloads between peers.

Permissioned Ledger:
A ledger designed with restrictions, such that only people or organizations requiring access have permission to access it.

Phishing:
When a scammer pretends to be a trusted institution or person to trick people into revealing sensitive information such as Social Security numbers, passwords, banking details, etc., often through a malware link disguised as legitimate.

Ponzi Scheme:
A fraudulent investment involving the payment of purported returns to existing investors from funds contributed by new investors.

Portfolio:
A collection of cryptocurrencies or crypto assets held by an investment company, hedge fund, financial institution or individual.

Pre-mine:
When some or all of a coin’s initial supply is generated during or before the public launch, rather than being generated over time through mining or inflation. They may be used for legitimate purposes, such as crowdfunding or marketing.

Pre-sale:
A sale that takes place before an ICO is made available to the general public for funding.

Private Key / Secret Key:
A piece of code generated in asymmetric-key encryption process, paired with a public key, to be used in decrypting information hashed with the public key.

Proof-of-Authority (PoA):
A blockchain consensus mechanism that delivers comparatively fast transactions using identity as a stake.

Proof-of-Burn (PoB):
A blockchain consensus mechanism aiming to bootstrap one blockchain to another with increased energy efficiency, by verifying that a cost was incurred in “burning” a coin by sending it to an unspendable address.

Proof-of-Developer (PoD):
Any verification that provides evidence of a real, living software developer who created a cryptocurrency, in order to prevent an anonymous developer from making away with any raised funds without delivering a working model.

Proof-of-Stake (PoS):

A blockchain consensus mechanism involving choosing the creator of the next block via various combinations of random selection and wealth or age of staked coins or tokens. *see Proof-of-Work (PoW).

Proof-of-Work (PoW):
A blockchain consensus mechanism involving solving of computationally intensive puzzles to validate transactions and create new blocks. *see Proof-of-Stake (PoS).

Protocol:
The set of rules that define interactions on a network, usually involving consensus, transaction validation, and network participation on a blockchain.

Pseudonymous:
Writing under a false name, such as "Satoshi Nakamoto."

Public Address:
A public address is the cryptographic hash of a public key, allowing the user to use it as an address to request for payment.

Public Blockchain:
A blockchain that can be accessed by anyone.

Pump and Dump (P&D) Scheme:
A form of securities fraud involving the artificial inflation of the price of a cryptocurrency with false and misleading positive statements in order to sell previously-cheaply purchased stock at a higher price.

Q

QR Code:
A machine-readable label that shows information encoded into a graphical black-and-white pattern. For cryptocurrencies, it is often used to easily share wallet addresses with others.

R

Raiden Network:
An off-chain scaling solution aiming to enable near-instant, low-fee and scalable payments on the Ethereum blockchain. It is similar to Bitcoin's proposed Lightning Network.

Replicated Ledger:
A copy of a distributed ledger in a network that is distributed to all participants in a cryptocurrency network.

Ring Signature:
A method of increasing privacy by fusing inputs of multiple signers with that of the original sender to authorize a transaction.

ROI:
Short for "Return on Investment," the ratio between the net profit and cost of investing.

Relative Strength Index (RSI):
A form of technical analysis that serves as a momentum oscillator, measuring the speed and change of price movements, developed by J. Welles Wilder. It oscillates between zero and 100, where a cryptocurrency is considered overbought when the indicator is above 70 and oversold when below 30.

S

Satoshi (SATS):
The smallest unit of bitcoin with a value of 0.00000001 BTC.

Satoshi Nakamoto:
The individual or group of individuals that created Bitcoin. The identity of Satoshi Nakamoto has never been confirmed.

Scam:
A fraudulent or deceptive cryptocurrency or ICO.

Scrypt:
An alternative proof-of-work (PoW) algorithm to SHA-256, used in Bitcoin mining. Scrypt mining relies more heavily on memory than on pure CPU power, aiming to reduce the advantage that ASICs have and hence increasing network participation and energy efficiency.

Second-Layer Solutions:
A set of solutions built on top of a public blockchain to extend its scalability and efficiency, especially for micro-transactions or actions. Examples include: Plasma, TrueBit, Lightning Network and more.

Securities and Exchange Commission (SEC):
An independent agency of the United States federal government, responsible for enforcing federal securities laws, proposing securities rules, and regulating the securities industry, the nation's stock and options exchanges, and other related activities and organizations.

Seed:
A single starting point when deriving keys for a deterministic wallet. It is usually presented as a series of words to enable the owner to quickly backup or restore a wallet.

Segregated Witness (SegWit):
A Bitcoin Improvement Proposal (BIP) that aimed to fix transaction malleability on Bitcoin. In the past, when changing the “witness” information (signatures) on blocks, it would change the transaction ID and its subsequent hash. SegWit was aiming to fix this by segregating signature and block content: a side effect of this change was smaller block sizes and the ability to support second layer solutions.

Selfish Mining:
A situation in which a miner mines a new block but does not broadcast this new block to the other miners. If this miner is able to find a second block faster than all other miners, then they would have created the longest public chain, invalidating all other blocks discovered in the time it took to execute this attack.

Sell Wall:
A situation where a large limit order has been placed to sell when a cryptocurrency reaches a certain value. This can sometimes be used by traders to create a certain impression in the market, preventing a cryptocurrency from rising above that value, as supply will likely outstrip demand when the order is executed.

Side Chain:
A blockchain ledger that runs in parallel to a primary blockchain, where there is a two-way link between the primary chain and sidechain. This allows the sidechain to operate independently of the primary blockchain, using their own protocols or ledger mechanisms.

Simplified Payment Verification (SPV):
A lightweight client to verify blockchain transactions, downloading only block headers and requesting proof of inclusion to the blockchain in the Merkle Tree.

SHA-256:
A cryptographic hash function that generates a 256-bit signature for a text, used in Bitcoin proof-of-work (PoW). Standing for “Secure Hash Algorithm,” it is one of the SHA-2 algorithms, first designed by the NSA.

Sharding:
Sharding is a scaling approach that enables splitting of blockchain states into partitions containing states and transaction history, so that each shard can be processed in parallel.

Short:
A trading technique in which a trader borrows an asset in order to sell it, with the expectation that the price will continue to decline. In the event that the price does decline, the short seller will then buy the asset at this lower price in order to return it to the lender of the asset, making the difference in profit.

Silk Road:
An online black market that existed on the dark web, now shut down by the FBI. It had accepted bitcoins for transactions.

Smart contract:

A smart contract is a computer protocol intended to facilitate, verify, or enforce a contract on the blockchain without third parties.

Soft Cap:
The minimum amount that an initial coin offering (ICO) wants to raise. Sometimes, if the ICO is unable to raise the soft cap amount, it may be called off entirely. *see Hard Cap.

Soft Fork (Blockchain):
A protocol upgrade where only previously valid transactions are made invalid, with most soft forks requiring miners to upgrade their mining software in order to enforce it. *see Hard Fork.

Solidity:
The programming language used by Ethereum for developing smart contracts.

Spoon (Blockchain):
A hard spoon is a meta-protocol that exists on top of a blockchain, essentially creating a new blockchain with tokens that inherit the original blockchain's token balances. A spoon, like a fork, can be hard or soft, although the implementations of spoons thus far have been hard, i.e. the 2018 Tendermint hard spoon. While a hard spoon has no competition with the underlying blockchain, a soft spoon would compete as a branch of a protocol within the same blockchain. * See Fork.

Spot Market:
A public market in which cryptocurrencies are traded for immediate settlement. It contrasts with a futures market, in which settlement is due at a later date.

Stablecoin:
A cryptocurrency with extremely low volatility, sometimes used as a means of portfolio diversification. Examples include gold-backed cryptocurrency or fiat-pegged cryptocurrency.

Staking:
Participation in a proof-of-stake (PoS) system to put your tokens in to serve as a validator to the blockchain and receive rewards.

Stale Block:
A block which was successfully mined but not included on the current longest blockchain, usually because another block at the same height was added to the chain first.

State Channel:
A second-layer scaling solution that reduces the total on-chain transactions necessary, moving the transactions off-chain and letting participants sign to the main chain after multiple off-chain transactions.

T

Taint:
The percentage of cryptocurrency in an account that can be traced to another account.

Tangle:
The Tangle is a blockchain alternative developed by IOTA, using directed acyclic graphs which only builds in one single direction and in a way that it never repeats, and is quantum-computing resistant.

Testnet:
An alternative blockchain used by developers for testing.

Technical Analysis / Trend Analysis (TA):
An evaluation method involving statistical analyses of market activity, such as price and volume. Charts and other tools are used to identify patterns to underpin and drive investment decisions.

Timelock / Locktime:
A condition for a transaction to only be processed at a certain time or block on the blockchain.

Timestamp:
A form of identification for when a certain transaction occurred, usually with date and time of day and accurate to fractions of a second.

Token Generation Event:
The time at which a token is issued.

Tokenize:
The process by which real-world assets are turned into something of digital value called a token, often subsequently able to offer ownership of parts of this asset to different owners.

Tor:
Tor is free software for enabling anonymous communication. The name is derived from an acronym for the original software project name "The Onion Router." It consists of a network of volunteer relays to conceal users' location and usage.

Total Supply:
The total amount of coins in existence right now, minus any coins that have been verifiably burned. *see Circulating Supply and Max Supply.

Transaction Fee:
A payment for using the blockchain to transact.

Trustless:
A property of the blockchain, where no participant needs to trust any other participant for transactions to be enforced as intended.

Tumbler:
Another name for a mixing service.

Turing-Complete:
Turing-complete refers to the ability of a machine to perform calculations that any other programmable computer is capable of. An example of this is the Ethereum Virtual Machine (EVM).

U

Unconfirmed:
A state in which a transaction has not been appended to the blockchain.

Unpermissioned Ledger:
A public blockchain.

Unspent Transaction Output:
An output of a blockchain transaction that has not been spent, and can be used as an input for new transactions.

V

Validator:
A participant on a proof-of-stake (PoS) blockchain, involved in validating blocks for rewards.

Vanity Address:
A cryptocurrency public address with custom letters and numbers, usually picked by its owner.

Vaporware:
A cryptocurrency project that is never actually developed.

Venture Capital:
A form of private equity provided to fund small, early-stage firms considered to have high growth potential.

Virgin Bitcoin:
A bitcoin that has never been spent.

Volatility:

A statistical measure of dispersion of returns, measured by using the standard deviation or variance between returns from that same security or market index.

W

Wallet:
A cryptocurrency wallet is a secure digital wallet used to store, send, and receive digital currency, and are divided into two categories: hosted wallets and cold wallets.

Wash Trade:
A form of market manipulation in which investors create artificial activity in the marketplace by simultaneously selling and buying the same cryptocurrencies.

Wei:
The smallest fraction of an Ether, with each Ether to 1000000000000000000 Wei.

Whitelist:
A list of interested participants in an ICO, who registered their intent to take part or purchase in a sale.

Whitepaper:
A document prepared by an ICO project team to interest investors with its vision, cryptocurrency use and cryptoeconomic design, technical information, and a roadmap for how it plans to grow and succeed.

Z

Zero Confirmation Transaction:
Alternative phrasing for an unconfirmed transaction.

Zero Knowledge Proof:
In cryptography, a zero-knowledge proof enables one party to provide evidence that a transaction or event happened without revealing private details of that transaction or event.

Zk-SNARKs:
Zk-SNARKs (Zero-Knowledge Succinct Non-Interactive Argument of Knowledge) are the proof construction that one can verify information, like a secret key, both without disclosing the information itself or requiring any interaction between the prover and verifier.

Crypto Indices
Interest
Disclaimer
Privacy
Terms
FAQ
Methodology
About

Blog
Newsletter
Headlines
Facebook
Twitter
Telegram
Instagram
Interactive Chat