

#	TIP	DEFINITION
1	Block	A block is a computer file that keeps a record, or ledger, of cryptocurrency transactions completed during a given period and is worth a specified number of coins. For example, one block in the Bitcoin blockchain is worth 6.25 Bitcoins, a number which will halve every four years until 2140 when the last block is created. Blocksize varies between blockchains. Bitcoin's theoretical limit is 4MB, while Bitcoin Cash allows anything from 8MB to 32MB.
2	Blockchain	A network of independent but connected blocks, copies of which are distributed within a decentralized computer network. One Bitcoin transactions are added to a block and the new block is created, that transaction is verified and updated throughout the blockchain.
3	Distributed Ledger	Another name for a blockchain.
4	Genesis Block	The first block of a blockchain which contains unspendable coins. Bitcoin's genesis block was created on Jan 3 2009 with 50 Bitcoins.
5	Block Height	The total number of connected blocks in a blockchain.
6	Peer-to-Peer	The direct networking of two or more computers with each other without a centralized third-party acting as an intermediary. Blockchains run on Peer to Peer networks, i.e., decentralized networks.
7	Protocol	The software that links the blocks together and provides the rules under which new blocks are added to the decentralized network.
8	Algorithm	The recipe, or formula, used to generate keys that keep transactions secure. Cryptocurrencies rely on three main keys: Hash, Public Key and Private Key (see below).
9	Encryption	The process by which legible text is converted into illegible text called a hash or a key by use of an algorithm. This process, also known as cryptography, is the origin of the name cryptocurrencies.
10	Hash	A string of letters and numbers that represents a verified and submitted transaction. It is usually called Hash or TxID.
11	Hash Rate	The speed at which a computer verifies and submits a transaction, thereby generating a new Hash. It is literally the average speed at which a blockchain creates new Hashes, and is calculated in units of hash/second.
12	Public Key	A string of letters and numbers which identifies the address of your wallet in the Blockchain. This information is shareable with others in order to receive cryptocurrency, just like your email address or bank account number.
13	Private Key	A string of letters and numbers which unlocks your wallet. This is personal information and must never be shared, just like your password or PIN.
14	Seed Phrase	A 12, 18, or 24-word phrase that you and only you have access to and which acts as a backup to your private keys. If you forget or lose your private key, a seed phrase will help you recover it.
15	Wallet	A file in the blockchain that stores and receives your cryptocurrency, just like your email inbox receives and stores emails. It is operated by both a Public Key and a Private Key.
16	Cold Wallet	The storage of the Public and Private Keys of your wallet offline by printing them on a piece of paper, or saving them in an external hard drive that is not connected to the internet, in order to prevent loss through hacking. Cold storage is recommended when you have a large number of coins in your wallet.
17	Hot Wallet	Your wallet's public and private keys are stored on an app that's connected to the internet and is used to access your wallet. Your keys can be stolen if your computer or phone is hacked.
18	Mining	The process by which transactions are verified by a computer or a group of computers. When all the computers on the network accept the transaction, two things happen: a new block is added to the chain and new coins are created and added to the new block.

19	Consensus	The algorithm by which transactions are verified and submitted. The main types of consensus algorithms are Proof of Work (PoW), Proof of Authority (PoA) and Proof of Stake (PoS).
20	Mempool	A collection of verified and submitted transactions that are waiting to be confirmed by all computers in the Bitcoin network; a "waiting area" for valid blocks. A high mempool size indicates congestion; a traffic jam of blocks waiting to be added to the blockchain.
21	Proof of Work (PoW)	An algorithm that enables multiple computers in a blockchain to compete to mine blocks. The first computer to mine a block must prove that it has used a certain amount of energy to do so before the new block is accepted by all the other computers in the blockchain.
22	Proof of Authority (PoA)	An algorithm that gives a trusted computer or a specific group of trusted computers the authority to mine blocks. This is a much faster method than PoW.
23	Proof of Stake (PoS)	An algorithm that allows a computer to mine blocks in proportion to how many coins it holds. For instance, a computer that owns 2% of the coins available can mine a maximum of 2% of all blocks.
24	Proof of Activity (PoA)	An algorithm that uses both Proof of Work (PoW) and Proof of Stake (PoS) to verify transactions. The system starts with PoW and then switches to PoS after a block is successfully added.
25	Proof of Burn (PoB)	An algorithm that allows computers to mine blocks based on how many coins they "burn". Coins are burned by sending them to an unspendable address. The more coins burned, the more chances to mine.
26	Non-Fungible Token	A file that is stored within a block and which cannot be copied or replaced, meaning each NFT is as unique as a fingerprint. This is why NFTs are attached to digital assets, such as a JPEG picture or a digital painting, to prove ownership of the asset or provide access to the asset.
27	Fiat Currency	Currency that is created by a government and circulated via banks. In contrast, cryptocurrencies are invented within computers and are circulated via a peer-to-peer network, i.e., a blockchain.
28	Node	A computer that is part of a blockchain. A blockchain is therefore a network of nodes.
29	Faucet	A reward system on a website or app that offers free cryptocurrency for signing up or completing certain tasks. Some of these offers (not all) are scams and one must be careful before they sign up or share any data.
30	Whale	People or entities that hold a huge number of coins of a particular cryptocurrency. In Bitcoin, the minimum number of coins needed to qualify as a Whale is 1,000. Smaller holders are called a Dolphin or a Fish.
31	Nonce	A random number that is generated and used only once to verify new blocks. When a block is submitted, a nonce is attached to it to confirm that it is indeed a new block and not an old block being re-submitted to the chain.
32	Smart Contracts	Pieces of code that live within the blockchain whose purpose is to execute on a logic that the developer has programmed. When certain information is submitted to the blockchain, the code does what it is programmed to do; for example, make a payout.
33	Solidity	The programming language used to create Ethereum-based smart contracts.
34	Oracle	A piece of code that takes data from multiple sources both inside and outside the blockchain, then verifies, analyses and feeds the results into a smart contract for further action. Smart contracts rely on data from oracles to perform actions.
35	Token	A type of cryptocurrency that represents an asset, or has a specific use with a blockchain ecosystem. Some tokens are used for governance, allowing holders to vote on changes to the blockchain.
36	Chain Linking	The process of linking two different Blockchains, for example Bitcoin and Ethereum, so that crypto coins can be transferred between them. For a successful transfer, the transaction must be recorded and verified in both blockchains at the same time.

37	Block Explorer	A search engine that enables you to participate in blockchain transactions and provides access to data in blockchains. Examples include blockchain.com, blockstream.info, blockexplorer.com, blockcypher.com and btc.com.
38	Application-Specific Integrated Circuit (ASIC)	A specialized circuit designed for computers that mine a specific type of cryptocurrency only and perform no other function. A Bitcoin ASIC circuit can only mine Bitcoin and not Ethereum.
39	Altcoins	Because Bitcoin was the first cryptocurrency, any cryptocurrency that is not Bitcoin (like Ethereum, Litecoin and Cardano) is called an altcoin. There are thousands of altcoins; some legitimate, while others are used as conduits of financial crime.
40	Decentralized Finance (DeFi)	A financial service that is based on blockchains and relies on smart contracts to facilitate access to financial and banking services. Because DeFis are automated, they provide everyone with access to services that were previously exclusionary.
41	Exchange	A website that enables you to exchange cryptocurrency for fiat currencies like dollars or euros, exchange fiat currency for cryptocurrency, or trade one cryptocurrency for another.
42	Bitcoin	The first cryptocurrency. Launched in 2009, it was the first-ever crypto coin and remains the most valuable and largest cryptocurrency.
43	SATS	The smallest unit of Bitcoin, equivalent to 0.00000001 BTC. SATS, also known as Satoshi's, refer to Satoshi Nakamoto, the alleged creator of bitcoin.
44	Ethereum	Ethereum is a blockchain based on its own coin called Ether. Unlike the Bitcoin blockchain, Ethereum allows decentralized applications to be built onto it, which enables Ethereum to go beyond mining and offer other functions such as decentralized financial services, games and all kinds of decentralized apps.
45	Ether (ETH)	The native cryptocurrency of the Ethereum network. However, Ethereum accepts other cryptocurrencies, including Bitcoin.
46	Gwei	The smallest unit of an Ether. 1 gwei is equal to 0.000000001 ETH (10 ⁻⁹ ETH). Accordingly, 1 ETH is equivalent to 1 billion gwei.
47	Gas	The fee a miner earns for verifying and submitting transactions on the Ethereum network. Requiring Gas for every transaction prevents hackers from clogging Ethereum with invalid transactions.
48	dApps (Decentralized Apps)	Apps or programs that run on a blockchain and outside of the control of a central authority. For example, if Twitter was a dApp, once a message is posted, no one could delete it, including Twitter.
49	Unspent Transaction Output (UTXO) Model	A payment system where a transaction involves two separate actions; the first action sends the required number of coins to the recipient and the second action sends the remaining coins, known as unspent balance, to a different address in the sender's wallet. The total number of coins in the wallet is calculated by adding up all the unspent balances in the wallet.
50	Account/Balance Model	A payment system where a transaction involves two simultaneous actions; the balance in the owner's wallet is reduced by the exact number of coins sent out and the balance in the recipient's wallet is increased by coins received; there is no list of unspent balances, just an overall balance. This model is used in Ethereum while the UTXO model is used on Bitcoin.
51	Fork	A split that occurs when the blockchain's algorithm is updated. If there is disagreement amongst the different computers (miners) on whether to accept a new algorithm, one group updates to the new algorithms while another group continues to use the old, resulting in two different blockchains with a common origin.
52	Hard Fork	A permanent update to the blockchain. Computers running the previous version of the blockchain are kicked out of the updated blockchain.
53	Soft Fork	A permanent change to the protocol that requires computers to update their software. Those that fail to update remain in the blockchain, but they cannot submit new blocks.

54	Market Capitalization	The total value of a cryptocurrency is calculated by multiplying the number of coins in circulation by the current market price of a single coin. This number can run into the hundreds of billion or trillions of dollars.
55	The Flipping	The expected date when Ethereum overtakes Bitcoin in terms of market capitalization.
56	Exchange	A website or app, for example Binance, that allows you to open an account and buy cryptocurrencies using bitcoins, altcoins, or fiat currencies like dollars or Euros. Funds are sent to your account via the usual methods, e.g., PayPal or wire transfer.
57	Arbitrage	Buying cryptocurrency on one exchange and selling it for a higher price on another exchange.
58	Stablecoin	A cryptocurrency whose value is attached to the value of a fiat currency, a commodity like Gold or whose supply is controlled by an algorithm, thus ensuring the value of the currency remains stable. The best known stablecoin is Tether, the value of which is equivalent to approximately 1 US dollar.
59	Memecoin	A cryptocurrency based on a joke. Memecoins have no real-world utility and have value only because they are considered funny by many who buy them for this reason. The best known is Dogecoin.
60	Dollar Cost Averaging (DCA)	The practice of buying a fixed amount of cryptocurrency on a weekly, monthly or annual basis regardless of price fluctuations. This removes emotions from the investment process and maintains consistency and benefits from price falls.
61	Casascius Coin	Actual metal bitcoins created by Bitcoin user Casascius (Mike Caldwell) which are embedded with a piece of paper that contains the private key for a specific number of Bitcoin. A total of 27,673 Casascius coins were minted, worth a total 59,383.9 BTC.
62	Coin Mixer	A software that makes bitcoin transactions anonymous and untraceable. It achieves this by taking one transaction, mixing it up with others, and then sending it back to the owner on a different address and in different amounts.
63	Initial Coin Offering (ICO)	The offering of a new cryptocurrency to people in return for fiat currency, bitcoins, or altcoins. Participants of the ICO hope that the new crypto they have acquired will become widely used and raise its value.
64	Anti-Money Laundering (AML)	Policies and legislation to protect against money laundering.
65	Know your Customer (KYC)	The procedures used to verify the identity of a crypto user and link it to their wallet.
66	Double Spend	An attempt to send the same payment of cryptocurrency to two different wallets.
67	Escrow	A third party within a blockchain, like BitPay, that holds cryptocurrency safely until the seller receives payment before they are released to the buyer.
68	HODL	A famous misspelling of "hold," this means holding on to your cryptoassets when the market is down until prices come back up.
69	FOMO (Fear of Missing Out)	Selling other assets to buy into a cryptocurrency whose value is rising.
70	FUD (Fear, Uncertainty, and Doubt)	FUD is usually existent in those outside the crypto community.
71	Rekt	Borrowed from wrecked, meaning suffering devastating losses
72	Bull Market	An extended period during which the price of a cryptocurrency is rising
73	Mooning	A cryptocurrency whose price is skyrocketing—going to the moon due to a long bull market run
74	Pump and Dump	The practice of buying a cryptocurrency in large numbers to drive up its price and encourage others to invest, then selling all of it when the price rises and there is a profit to be made.

75	Shill	Someone who promotes an altcoin so that they can personally benefit when it rises in value.
76	Bear Market	An extended period during which the price of a cryptocurrency is falling
77	Bagholder	An investor that holds a coin that is worth significantly less than they paid for it.
78	Capitulation	Selling a cryptocurrency at a significant loss due to loss of hope that its value will ever go up
79	White Paper	A document that explains to potential users of a blockchain the various aspects of the blockchain and how it will work. A white paper precedes the launch of a blockchain.
80	51% Attack	This refers to a computer or group of computers having the ability to verify more than 50% of all transactions in a network. This enables them to reverse transactions, spend coins more than once, and manipulate which blocks are added and which are not.
81	Satoshi Nakamoto	The person or group of persons that created Bitcoin. The identity or identities of Satoshi Nakamoto have never been confirmed.
82	Nick Szabo	Developer of smart contract technology and the Bit Gold algorithm, cryptologist and lawyer. Rumored to also be Satoshi Nakamoto.
83	Craig Wright	Australian entrepreneur who has claimed more than 150 patents related to distributed registry technology, smart contracts, and six cryptocurrencies. Claims to be Satoshi Nakamoto.
84	Vitalik Buterin	Founder of Ethereum.
85	Changpen Zhao	The founder of Hong Kong based cryptocurrency exchange Binance.
86	Pavel Durov	Founder of the Telegram Open Network, the Gram cryptocurrency and the TON blockchain platform.
87	Brian Armstrong	Founder and CEO of Coinbase, a California based cryptocurrency exchange.
88	Jack Dorsey	CEO of mobile payments company Square (and Twitter), which allows its customers to trade Bitcoin.
89	Brandon Chaz	Founder of Coinmarketcap, the largest online cryptocurrency aggregator. This site consolidates data from all exchanges and based on this data determines the value of cryptocurrency.
90	Elizabeth Rossiello	Founder of BitPesa, a Kenyan based cryptocurrency exchange.
91	David A. Marcus	Director of Libra, a cryptocurrency developed by Facebook and other companies.
92	Cameron and Tyler Winklevoss	Owners of crypto exchange Gemini and digital art auction platform Nifty Gateway
93	Matthew Roszak	Chairman of Bloq, a blockchain infrastructure company.
94	Degen Spartan	DeFi Twitter Influencer
95	Laura Shin	Founder and Host of Unchained and Unconfirmed cryptocurrency podcasts
96	Charlie Lee	Founder of the third cryptocurrency in history: Litecoin.
97	Justin Sun	Founder of the TRON cryptocurrency.
98	Charles Hoskinson	Co-founder of Ethereum, Founder of Cardano (ADA).
99	Sergey Nazarov	Co-founder of Chainlink, the first blockchain oracle.