A

- **Address (Wallet Address)**: A string of letters and numbers that represents a destination on the blockchain. You give this to someone so they can send you cryptocurrency, similar to sharing a bank account number for crypto transfers. Each address is unique and is derived from a public key.
- **Airdrop**: A promotional event where a blockchain project distributes free coins or tokens to users. Often used to raise awareness, an airdrop might reward users with tokens for tasks like signing up or joining a community.
- **All-Time High (ATH)**: The highest price or market value a cryptocurrency has ever reached in its history. For example, Bitcoin's ATH refers to its record high price.
- **All-Time Low (ATL)**: The lowest price point a cryptocurrency has ever fallen to since it began trading.
- **Altcoin**: Short for "alternative coin", it refers to any cryptocurrency other than Bitcoin. Examples include Ethereum, Litecoin, and thousands of other coins that followed Bitcoin.
- **ASIC (Application-Specific Integrated Circuit)**: Specialised computer hardware designed to perform a specific task. In crypto, ASICs are built to efficiently perform the hashing required for Proof-of-Work mining (for example, Bitcoin mining) much faster than normal computers.
- **Ape / Aping In**: Slang for impulsively buying into a coin or NFT project without proper research, often driven by hype or FOMO.

B

- **Bear Market**: A period of declining prices in a financial market. In crypto, a bear market is marked by widespread pessimism, prices fall, and many investors expect them to drop further. (Those who expect prices to fall are called "bears", and a negative outlook is described as bearish).
- **Bitcoin (BTC)**: The first decentralised cryptocurrency, launched in 2009. Bitcoin runs on its own blockchain and introduced the concept of a peer-to-peer digital currency that operates without a central authority.
- **Blockchain**: A decentralised digital ledger that records transactions across many computers in a way that the records are permanent and tamper-proof. Data is stored in blocks that are linked in a chain using cryptography. In simple terms, a blockchain is like a public database that no single party controls, where all participants collectively verify and agree on updates.
- **Block**: A batch of transactions recorded together on the blockchain. Each block is like a page in the ledger containing multiple transactions, and blocks are added sequentially to the chain. A new block must be validated (by miners or validators) before it joins the chain.

- **Block Reward**: The new coins awarded to miners or validators for successfully adding a block to the blockchain. For example, Bitcoin miners currently earn a fixed number of new bitcoins as the block reward each time they mine a block (this reward halves every few years in an event called the halving).
- **Bull Market**: A period of rising prices and optimistic sentiment. In a crypto bull market, asset prices climb, and investors generally expect continued growth. (Investors who expect prices to rise are called "bulls", and an optimistic outlook is described as bullish).
- **Bridging / Cross-Chain Bridge**: A tool or protocol that allows tokens or data to move between different blockchain networks. Used for cross-chain DeFi, NFTs, or liquidity.
- **Burn / Coin Burn**: A process of permanently removing coins from circulation, typically by sending them to an unusable address. Burned tokens are effectively destroyed to reduce the supply, often with the aim of increasing scarcity or value of the remaining coins.
- **BIP (Bitcoin Improvement Proposal)**: A formal document used to propose changes or improvements to the Bitcoin protocol. BIPs go through community review and consensus.

C

- **CBDC (Central Bank Digital Currency)**: A digital form of fiat money issued by a country's central bank. Unlike cryptocurrencies, CBDCs are centralised and represent traditional money (like a digital dollar), but use some of the technology of cryptocurrencies.
- **Centralised Exchange (CEX)**: A cryptocurrency exchange operated by a company or central entity (e.g. Coinbase or Binance). Users trade by depositing funds into the exchange, which holds their assets and facilitates the trades. While easy to use, CEXes require trust in the company (and usually require KYC checks).
- **Confirmation**: The number of blocks added to the chain after a transaction's block. More confirmations mean more certainty that the transaction is final and cannot be reversed.
- **Consensus Mechanism**: The method by which a blockchain network reaches agreement on the state of the ledger and validates new blocks. It ensures all honest participants (nodes) agree on which transactions are valid. Examples include Proof-of-Work and Proof-of-Stake, which use different approaches to achieve consensus. In short, a consensus mechanism is what keeps a distributed network of computers in sync and secure without a central authority.
- **CoinJoin**: A privacy-enhancing technique that combines multiple Bitcoin transactions into one, making it harder to trace individual payments.
- **Cryptocurrency**: A digital or virtual currency that uses cryptography for security and operates on a blockchain network, typically without a central authority. Examples are Bitcoin, Ether, and Litecoin. Cryptocurrencies enable peer-to-peer transactions over the internet, and ownership of coins is proven by cryptographic keys.

- **Cold Wallet / Cold Storage**: Storing cryptocurrency offline, away from any internet connection, for security purposes. Examples include hardware wallets or paper wallets. Because it's offline, a cold wallet is much harder for hackers to access. (By contrast, see Hot Wallet under H).
- **Coin**: In casual use, "coin" can refer broadly to any cryptocurrency, but more strictly it means a cryptocurrency that runs on its own native blockchain (e.g. Bitcoin is a coin on the Bitcoin blockchain, Ether is the coin of the Ethereum blockchain). (See also Token under T for assets that run on another coin's platform).
- **CeFi (Centralised Finance)**: Crypto services provided by centralised companies (e.g. Celsius, BlockFi) that manage custody and user assets, similar to traditional banks.
- **Custodial vs. Non-Custodial**: A custodial service (or wallet) is one where a third party (like an exchange) holds your private keys and funds on your behalf, similar to a bank holding your money. Non-custodial means you control your private keys and funds directly. Most crypto enthusiasts recommend non-custodial wallets (e.g. your own wallet app or hardware wallet) so that you have full control (hence the saying "not your keys, not your coins").

D

- **DApp (Decentralised Application)**: An application run by many users on a decentralised network (like a blockchain) rather than a single, centralised server. For example, a decentralised finance app on Ethereum is a Dapp, it uses smart contracts on the blockchain as its back end, meaning no single company controls the core functionality.
- **DAO (Decentralised Autonomous Organisation)**: An organisation governed by code and blockchain-based smart contracts, with no central leadership. Decisions in a DAO are made collectively by the members (often by voting with tokens) according to pre-defined rules on the blockchain. In essence, it's like an internet community with a shared bank account and rules enforced by software.
- **Dust**: A tiny amount of cryptocurrency (usually less than the transaction fee) that's left behind in wallets and often unusable.
- **DCA (Dollar-Cost Averaging)**: An investment strategy where one invests a fixed amount of money at regular intervals, regardless of the asset's price. Using DCA, an investor might buy a set dollar amount of Bitcoin every week or month, reducing the impact of volatility by averaging out purchase prices.
- **DeFi (Decentralised Finance)**: An umbrella term for financial services (like lending, borrowing, trading, earning interest) that are built on blockchain networks and operate without traditional banks or intermediaries. DeFi platforms often use smart contracts on networks like Ethereum to recreate banking and trading services in an open, permissionless way.

- **Delegated Proof-of-Stake (DPoS)**: A variation of Proof-of-Stake where stakeholders elect a small number of delegates (or witnesses) to validate blocks on their behalf. It's a consensus mechanism designed to be faster and more efficient by using voting and a limited set of validators.
- **DEX (Decentralized Exchange)**: A cryptocurrency exchange that operates through smart contracts on a blockchain, without a central company. On a DEX (like Uniswap or SushiSwap), users trade directly from their wallets, and trades are executed by code (smart contracts) on the blockchain. This removes the need for an intermediary and allows users to retain control of their funds.
- **Difficulty (Mining Difficulty)**: A measure of how hard it is for miners to find the next valid block in a Proof-of-Work blockchain. Higher difficulty means it takes more computing power on average to mine a block. Bitcoin's network adjusts its mining difficulty roughly every two weeks to keep block production steady as miner power (hash rate) changes.
- **Digital Signature**: A cryptographic mechanism used to verify authenticity of digital messages or transactions. In cryptocurrency, when you send a transaction, you "sign" it with your private key. This produces a digital signature that proves you own the funds (without revealing your private key) and that the transaction hasn't been tampered with.
- **Double Spend**: An attempt to spend the same cryptocurrency twice. Blockchains like Bitcoin are designed to prevent double spending through their consensus rules, once a transaction is confirmed in a block, the network will reject any other transaction trying to use the same coins. (Double spending was a big problem for earlier digital currencies that Bitcoin's design solved).
- **DYOR (Do Your Own Research)**: A common mantra in the crypto community, urging investors to research and understand projects before investing, rather than relying solely on others' opinions. It's a reminder to be vigilant, as the crypto space can be rife with hype and misinformation.

E

- **Ethereum (ETH)**: A popular blockchain platform known for its smart contract functionality. Ethereum is the second-largest cryptocurrency network after Bitcoin. Its native currency is Ether (ETH), and the platform enables developers to build decentralised applications (DApps) and tokens (like ERC-20 tokens) on top of its blockchain.
- **EVM (Ethereum Virtual Machine)**: The runtime environment for executing smart contracts on Ethereum. It ensures consistent execution across all Ethereum nodes.
- **Exchange**: A platform for buying, selling, or trading cryptocurrencies. Centralised exchanges (CEX) are run by companies (they hold users' funds and match orders on their servers), whereas decentralised exchanges (DEX) use blockchain smart contracts to facilitate peer-to-peer trading without a central operator. Exchanges typically offer to convert crypto to crypto, or crypto to fiat and vice versa.

- **Encryption**: The process of converting information into code to prevent unauthorised access. In crypto, encryption (along with other cryptographic techniques) is used to secure transactions and wallets, for instance, your private key is often stored encrypted, and only you have the password to decrypt it.
- **ERC-20**: A widely used technical standard for creating tokens on the Ethereum blockchain. An ERC-20 token is basically a cryptocurrency that isn't Ether but runs on Ethereum's network (examples include Chainlink's LINK or USDC stablecoin). The standard ensures compatibility so these tokens can be easily exchanged and work with Ethereum wallets and DApps.
- **ERC-721**: The technical standard on Ethereum for non-fungible tokens (**NFTs**). ERC-721 tokens are unique and not interchangeable one-to-one, which makes them suitable for representing one-of-a-kind assets like digital art or collectibles.
- **Escrow**: A financial arrangement where a third party temporarily holds funds or assets on behalf of two other parties in a transaction until certain conditions are met. In crypto, escrow can be implemented with smart contracts (for example, holding funds until services are delivered) or via trusted intermediaries for peer-to-peer trades to prevent fraud.

F

- **FOMO (Fear of Missing Out)**: An emotional state in which an investor feels anxiety about missing a potential opportunity, leading them to jump into a rising market for fear of missing gains. In crypto, FOMO often happens when prices spike rapidly, and people rush to buy so they don't "miss out" on the run up.
- **Flash Loan**: A DeFi feature that allows users to borrow large sums of crypto without collateral, as long as the loan is repaid within a single blockchain transaction.
- **FUD (Fear, Uncertainty, and Doubt)**: A strategy (or simply a mood) of spreading negative, misleading, or false information to instil fear and uncertainty. In crypto communities, accusing someone of spreading "FUD" implies they are exaggerating risks or bad news to discourage investment in a coin.
- **Fiat**: Short for fiat currency, it refers to government-issued currency like USD, EUR, JPY, etc. Fiat currencies are traditional money we use daily, which are backed by governments but not by physical commodities. In crypto, you'll often see "fiat on-ramps" (services to convert fiat to crypto) or discussions of crypto vs fiat.
- **Fork**: A change or split in a blockchain's protocol. Soft forks are backward-compatible updates (old nodes still recognise new blocks), whereas hard forks are not backward-compatible and result in a permanent divergence, potentially creating a new blockchain that departs from the original. (See Hard Fork under H and Soft Fork under S for more details).

- **Full Node**: A computer on the network that fully validates all rules of the blockchain. A full node downloads and verifies the entire blockchain and helps relay transactions. Running a Bitcoin full node, for instance, means you independently verify every block and transaction, contributing to the network's decentralisation and security.
- **Futures**: A type of financial contract or derivative where two parties agree to buy or sell an asset at a predetermined future date and price. Crypto futures allow traders to speculate on the future price of a coin (like Bitcoin) without actually holding it, often using leverage. They are commonly used in advanced trading but can be risky due to price volatility.

G

- **Gas (Gas Fee)**: In Ethereum, "gas" is the unit measuring the computational work of running transactions or smart contracts. Every action on Ethereum (like sending ETH or interacting with a DeFi contract) requires a gas fee paid in Ether. The gas price (usually in Gwei) is how much one is willing to pay per unit of gas, and the gas limit is the maximum gas one will use for a transaction. In simple terms, gas fees are like transaction fees or "fuel" costs for using the Ethereum network.
- **Gas War**: A period of extremely high Ethereum gas fees caused by intense competition for block space, often during NFT mints or token launches.
- **Genesis Block**: The very first block of a blockchain. Every blockchain has a genesis block (block number 0 or 1) that is hardcoded into the network software. For example, Bitcoin's genesis block was mined by Satoshi Nakamoto in January 2009 and contains a famous embedded message.
- **GPU (Graphics Processing Unit)**: A specialised processor originally designed for rendering graphics, which is also effective at performing the repetitive calculations needed for mining certain cryptocurrencies. Before ASICs became common, many cryptocurrencies (like Ethereum in its early days) were mined with GPUs. Some coins are still GPU-mined, meaning they use an algorithm designed to be efficiently solvable by GPUs.
- **Gwei**: A denomination of Ether (ETH). 1 Gwei is 0.000000001 ETH. Gas prices on Ethereum are often quoted in Gwei. For example, saying the gas price is 30 Gwei means 30 billionths of an Ether per unit of gas.
- **Governance Token**: A token that gives holders the ability to vote on proposals affecting a blockchain project or protocol (e.g. UNI in Uniswap governance).

H

- **Halving**: A programmed event in certain cryptocurrencies (notably Bitcoin) that cuts the block reward in half. For Bitcoin, halving occurs roughly every 4 years. It slows the creation of new BTC and reduces the miner reward, increasing scarcity over time. Historically, Bitcoin halving events have been associated with significant market interest due to the reduction in new supply.

- **Hard Fork**: A major change to a blockchain's protocol that is not backward compatible. A hard fork requires all participants to upgrade to the new rules; otherwise, a split can occur, resulting in two separate blockchains. A famous example is the split of Ethereum and Ethereum Classic after The DAO hack in 2016, or Bitcoin and Bitcoin Cash in 2017, in each case, a new coin was created via hard fork.
- **Hash / Hashing**: In crypto, hashing refers to using a mathematical algorithm to transform input data into a fixed-length alphanumeric string (a hash). A hash is effectively a digital fingerprint of the data, even a tiny change in the input produces a completely different hash. Hashing is used in securing blockchains: each block contains the hash of the previous block, linking them, and miners in Proof-of-Work must find a hash below a target value by trying many inputs (this is the "puzzle" in mining). SHA-256, for instance, is the hash algorithm Bitcoin uses.
- **Hash Rate**: The measuring unit of a miner's computational power, or collectively the power of the entire network. It's the number of hash computations performed per second by miners. A higher hash rate means more total computing power is working on that blockchain's Proof-of-Work, generally increasing security (as it'd require more power to attack). For example, if Bitcoin's hash rate is 100 EH/s, it means the network is performing 100 quintillion hashing operations every second.
- **Hash Function**: A cryptographic algorithm that turns input data into a fixed-length output (a hash). Used for securing data and linking blockchain blocks.
- **HODL**: A popular slang term in the crypto community meaning "hold" (do not sell) your cryptocurrency instead of trading it. It originated from a typo of "hold" in a forum post, and it means "Hold On for Dear Life". Telling someone to HODL means to stay invested for the long term despite volatility.
- **Hard Cap**: The absolute maximum number of coins that will ever be created for a cryptocurrency. For example, Bitcoin's hard cap is 21 million BTC.
- **Hot Wallet**: A cryptocurrency wallet that is connected to the internet. Examples are mobile wallets, web wallets, or exchange wallets. Hot wallets are convenient for frequent access and transactions, but because they are online, they are more vulnerable to hacking compared to cold wallets (offline storage).
- **Hardware Wallet**: A physical device (like a USB stick) that securely stores a user's cryptocurrency private keys offline. Examples include Ledger and Trezor devices. Hardware wallets are a popular form of cold wallet, they keep keys off your computer/phone, signing transactions internally when you need to send funds, which adds a strong layer of security against malware or hackers.

I

- **ICO (Initial Coin Offering)**: A fundraising method in which a new cryptocurrency project sells its own tokens or coins to early backers in exchange for capital (often using Bitcoin, Ether, or even fiat). It's analogous to an IPO in stocks. ICOs were extremely popular around 2017, allowing startups to raise money, but many ICOs were speculative or scams. (Related: IEO meaning Initial Exchange Offering, a variation where the token sale is conducted on a crypto exchange's platform rather than directly by the project).
- **Immutable**: Incapable of being changed. Blockchains are often described as immutable ledgers, meaning once data (transactions) are recorded in a block and added to the chain, they cannot be altered or deleted. This property is what gives blockchain transactions finality and trustworthiness.
- **Impermanent Loss**: A temporary loss of funds that liquidity providers can experience in a liquidity pool due to volatility in the token pair's price. It happens when the value of the tokens you deposited changes compared to when you deposited them, resulting in fewer dollar-equivalent when you withdraw than if you'd just held the tokens separately. If prices return to the original levels, the loss can diminish ("impermanent"), but if not, the loss becomes permanent relative to holding.
- **Inflation**: In crypto, inflation refers to the increase in the supply of a coin over time (which can lower its value if not met with equal demand). Some cryptocurrencies have a fixed supply (no inflation, like Bitcoin), while others continuously add new coins as rewards (leading to a steady inflation rate). Inflation can also refer to general price inflation in fiat terms, which sometimes drives interest in crypto as a hedge.
- **Interoperability**: The ability of different blockchain systems or networks to communicate and work with each other. High interoperability means you could, for example, move assets or data from one blockchain to another smoothly. Projects aimed at interoperability include Polkadot, Cosmos, and cross-chain bridges that connect different chains.
- **IPFS (InterPlanetary File System)**: A decentralised file storage and sharing network that works peer-to-peer. It's often used in the crypto world to store large data (like NFT images or website data) off-chain while still having content addressed by a hash. IPFS ensures files are distributed across many nodes rather than relying on a central server.

J

- **JOMO (Joy of Missing Out)**: The opposite of FOMO. It's a feeling of contentment about not participating in something. In crypto, people express JOMO when they are glad they didn't invest in a hype coin that then crashed, or happy to sit out during chaotic market swings. Essentially, it's being relieved about missing a potentially bad investment.

K

- **KYC (Know Your Customer)**: A process used by financial businesses (including many crypto exchanges) to verify the identity of their clients. KYC procedures often involve providing personal information and identification documents. It's done to comply with regulations and prevent illicit activities like money laundering. In crypto, using a centralised exchange usually requires KYC, while decentralised platforms often do not.
- **Key / Key Pair**: In cryptography and crypto wallets, you have a key pair consisting of a private key and a public key. The private key is secret and lets you authorise transactions (like a password), and the public key (or address) is shareable and lets you receive funds. (See Private Key and Public Key under P).
- **Keylogger**: A form of malware that secretly records keyboard input. It can be used to steal private keys, passwords, or seed phrases.

L

- **Ledger**: A record of financial transactions. A blockchain is essentially a distributed ledger, an ever-growing list of records (blocks) that is shared and maintained by many participants. "Ledger" in crypto often refers to the transaction history that all nodes have a copy of. (It's also the name of a popular hardware wallet company, but here we mean the general concept).
- **Layer 1 (L1)**: The base blockchain protocol layer (e.g. Bitcoin, Ethereum). It handles consensus and transaction settlement.
- **Lightning Network**: A "Layer 2" payment protocol that operates on top of Bitcoin (and some other blockchains) to enable faster and cheaper transactions. The Lightning Network allows users to open payment channels between parties; transactions within these channels are instant and the net result is later settled on the main blockchain. This helps Bitcoin scale by handling small or frequent transactions off-chain, then recording the final state on-chain.
- **Layer 2 (L2)**: A secondary protocol built on top of a Layer 1 blockchain to improve scalability, speed, and cost-efficiency (e.g. Lightning Network, Arbitrum).
- **Liquidity**: How easily an asset can be bought or sold in a market without dramatically affecting its price. In crypto, a coin that has high liquidity can be traded quickly at stable prices (lots of buyers and sellers are available). Low liquidity might mean price slippage when trading (the act of buying/selling moves the price noticeably due to scarce orders).
- **Liquidity Pool**: In DeFi, a liquidity pool is a collection of funds (usually two tokens) locked in a smart contract, used to enable trading on a decentralised exchange or other protocol. Users known as liquidity providers contribute tokens to the pool (e.g. ETH and DAI in a pool) and in return earn fees or rewards. These pools use algorithms (automated market makers) to price assets based on the ratio in the pool. Liquidity pools are fundamental to many DEXs instead of traditional order books.

- **Liquidity Mining**: A process where users provide liquidity to DeFi protocols and earn token rewards in return.
- **Long (Long Position)**: A trading position or bet that the price of an asset will go up. "Going long" on Bitcoin means you buy (or use a derivative) expecting the price to rise so you can sell later at a profit. In simpler terms, if you are long on a coin, you are bullish on it. (Opposite of Short, where you bet the price will fall).
- **Lambo ("When Lambo?")**: A slang phrase used humorously to ask when a cryptocurrency investment will pay off so much that the holders can afford a Lamborghini sports car. It exemplifies the get-rich-quick mindset of some crypto traders. Asking "When Lambo?" is basically asking when a coin will moon (hit a very high price). It's a tongue-in-cheek way to express excitement or impatience for big gains.

M

- **Market Cap (Market Capitalisation)**: The total value of a cryptocurrency's circulating supply. It's calculated as price per coin times number of coins in circulation. For example, if a coin is $100 and there are 5 million coins circulating, the market cap is $500 million. Market cap is used to compare the relative size of cryptocurrencies (e.g. Bitcoin has the largest market cap in crypto).
- **Mining**: The process of using computational power to validate transactions and add new blocks to a Proof-of-Work blockchain (like Bitcoin). Participants who do this are called miners. In mining, computers compete to solve a cryptographic puzzle (finding a hash below a target); the first to solve it gets to create the next block and earns a block reward plus transaction fees.
- **Mining Pool**: A group of miners who combine their computing resources to mine blocks together and share the rewards proportional to the contributed power. Mining pools give more regular payouts to small-scale miners, as finding blocks solo can be very infrequent when difficulty is high. Essentially, it's teamwork for miners to reduce variance in earnings.
- **Multichain**: Refers to platforms, apps, or wallets that operate across multiple blockchains rather than being limited to just one.
- **Moon / To the Moon**: Slang for a cryptocurrency price shooting upward dramatically, as if heading to the moon. If someone says, "Doge is going to the moon!", they mean the price is skyrocketing or they believe it will. When moon? is a common meme phrase investors use to ask when a coin will hit a peak or extremely high value.
- **Multisig (Multi-Signature)**: A security feature where a crypto wallet or address is controlled by more than one key. Transactions from a multisig wallet require multiple independent approvals (signatures) before they are valid. For example, a 2-of-3 multisig wallet might require any 2 of 3 designated private keys to sign a transaction. This prevents any single party from moving funds unilaterally and is often used for added security or shared accounts.

- **Memecoin**: A cryptocurrency that started as a joke or meme but gained popularity. They often have fun or viral branding rather than serious utility. The most famous example is Dogecoin (inspired by the Doge meme). Memecoins can still attain high market values due to community enthusiasm and speculation, but they are considered highly risky and volatile.
- **Metaverse**: A broad term for immersive virtual worlds where users can interact, play, and transact. In the crypto context, "metaverse" often refers to blockchain-based virtual environments that incorporate digital assets (like NFTs for virtual land, items, or avatars). The metaverse envisions a future internet of augmented and virtual reality spaces with their own economies, many of which use cryptocurrency for exchange.
- **MEV (Maximal Extractable Value)**: Profit that a miner or validator can extract by reordering, including, or excluding transactions in a block.

N

- **NFT (Non-Fungible Token)**: A unique digital asset recorded on a blockchain. "Non-fungible" means it's not interchangeable one-for-one with any other token (unlike, say, one Bitcoin is equal to any other Bitcoin). NFTs are often used to represent digital collectibles, art, music, virtual real estate, or any item where uniqueness is important. Owning an NFT typically means you have a provably unique token that represents ownership or authenticity of an associated digital or physical item.
- **Node**: A computer that is connected to a blockchain network. Nodes can serve different functions, but generally each node keeps a copy of the blockchain and helps validate and relay transactions. Full nodes store the entire blockchain and enforce all the rules, while light nodes (or SPVs) might store only some data and rely on full nodes for verification. A robust network has many nodes spread across the world, which keeps the system decentralised.
- **Non-Custodial**: Refers to a service or wallet where the user retains full control of their private keys (and thus their crypto). A non-custodial wallet (like many mobile or hardware wallets) means you are not trusting a third party to secure your funds, you are responsible for them. (Contrast with Custodial under C, where another entity holds the keys).
- **Network**: In crypto, "the network" often refers to the entire system of nodes that participate in running a blockchain. For example, "the Ethereum network" is all the computers (nodes) that enforce Ethereum's rules and maintain its blockchain.

O

- **Oracle**: A bridge between a blockchain and the outside world. Oracles provide external data to smart contracts, so the contracts can react to real-world events or information not available on the blockchain. For instance, a smart contract bet on tomorrow's weather needs an oracle to input the actual temperature. Oracles can be decentralised services (like Chainlink) that feed data like price feeds to DeFi apps.

- **On-Chain**: Actions or data recorded directly on the blockchain ledger. These are transparent and immutable.
- **OTC (Over The Counter)**: Direct trading of crypto between two parties, outside of public exchanges. OTC trades are often used for large volume transactions to avoid slippage on open markets. These private deals can be facilitated by brokers or done peer-to-peer, and prices/terms are negotiated rather than matching on an exchange order book. Essentially, OTC is "off-exchange" trading.
- **Off-Chain**: Actions or data processed outside the blockchain. Off-chain methods are used for speed, privacy, or cost savings.
- **Open Source**: Software for which the original source code is made freely available and may be redistributed and modified. Most major crypto projects (like Bitcoin, Ethereum) are open source, meaning anyone can inspect the code for security and contribute to improvements. This transparency builds trust, as the community can audit how the system works.
- **Orphan Block**: A block that was mined but not accepted into the main blockchain, usually because another block at the same height was added to the chain instead (perhaps due to two miners finding a block simultaneously). Orphan blocks (also called stale blocks) are those that the network dropped in favour of a longer chain path. Their transactions usually end up in the accepted chain's blocks later, but the orphaned block's miner doesn't get a reward.

P

- **Paper Wallet**: A physical printout (or handwritten note) of your cryptocurrency private key and address, often represented as QR codes. It's a form of cold storage. By keeping this paper safe and offline, your funds can't be hacked digitally. However, paper wallets must be kept secure from physical loss or damage, and imported to a software wallet when you want to spend the funds.
- **Peer-to-Peer (P2P)**: A network model where participants interact directly with each other without a central intermediary. Cryptocurrencies operate on P2P networks, transactions are sent directly from person to person through their nodes/wallets, and nodes collectively validate and propagate these transactions. This is in contrast to client-server models (like traditional banks, where a central server mediates all transfers).
- **Private Key**: A secret alphanumeric string that allows you to access and spend your cryptocurrency. It's like the password that controls your funds. Anyone with your private key can spend your coins, so it must be kept absolutely secret. Wallet software typically manages private keys for you (often represented as a seed phrase, see S), so you usually deal with a 12-24 word backup rather than the raw key.

- **Public Key**: An alphanumeric string derived from the private key, which you can share with others as an address to receive funds. The public key (or its shorter form, the address) is like your bank account number or email address for crypto, people can send you money with it. Thanks to cryptography, the public key does not reveal the private key, but it is mathematically linked in a way that allows the network to verify that a signature (made by the private key) is valid for that address.

- **Proof-of-Stake (PoS)**: A consensus mechanism where validators stake (lock up) their coins to secure the network and validate new blocks. In PoS, instead of expending energy on solving puzzles, the chance to create the next block often depends on how many coins one holds and has staked (or sometimes randomness). Honest validators are rewarded (usually with more coins), while malicious behaviour can be penalised by slashing their stake. PoS is used by networks like Ethereum (after "the Merge"), Cardano, and others, generally resulting in far less energy usage than Proof-of-Work.

- **Phishing**: A type of scam where attackers impersonate legitimate services to trick users into revealing sensitive information like passwords or seed phrases.

- **Proof-of-Work (PoW)**: The original blockchain consensus mechanism, used by Bitcoin and others. In PoW, miners compete to solve a computational puzzle (finding a hash) to add the next block. Solving the puzzle proves they expended computational effort (work). The winner broadcasts their block, and it becomes part of the blockchain. PoW is very secure but energy-intensive, it's what makes Bitcoin decentralised and tamper-resistant at the cost of significant electricity usage.

- **Protocol**: A set of rules that define how data is transmitted and how the network operates. In cryptocurrency, the protocol refers to the underlying code and rules of the blockchain (e.g. Bitcoin protocol, Ethereum protocol). This covers how nodes find consensus, how blocks are structured, how transactions work, etc. Protocol updates (especially if not backward compatible) can lead to forks.

- **Pump and Dump**: A form of fraud or market manipulation where a group coordinates to inflate the price of an asset (the "pump") through hype or buying, and then quickly sells off (the "dump") once the price is high. Late buyers get left with losses as the price crashes back down. Unfortunately, low-liquidity altcoins are sometimes subject to pump-and-dump schemes organised in chat groups, a practice that is unethical and often illegal in regulated markets.

Q

- **QR Code**: A square barcode that can encode information, often used in crypto to easily share wallet addresses. Scanning a crypto QR code (with a wallet app's camera, for instance) can fill in the recipient's address automatically, helping avoid the risk of mistyping the long string. Almost all mobile wallets can display your address as a QR code for convenient receiving.

- **Quantum Computing (Risk)**: An emerging field of computing that uses quantum mechanics to perform certain computations much faster than classical computers. A sufficiently powerful quantum computer in the future could theoretically break some forms of cryptography, including the Elliptic Curve signatures used in Bitcoin and many others, posing a risk to cryptocurrency security. This is a long-term concern; crypto developers are monitoring it and researching quantum-resistant algorithms well before practical quantum attacks become possible.

R

- **REKT**: Slang for "wrecked," meaning severely damaged or ruined. In crypto lingo, to get rekt means to suffer a heavy financial loss, for example, someone who bought a coin at the top and saw it crash 90% might say they got rekt. It's often used humorously or empathetically in trading communities.
- **ROI (Return on Investment)**: A measure of the profit or loss made on an investment relative to the amount of money invested. In crypto, people calculate ROI to see how much they've gained (or lost) on a coin in percentage terms. For example, a 200% ROI means your investment's value tripled. (Be cautious: very high ROI promises are often too good to be true).
- **Rug Pull**: A type of scam in the crypto world where a team suddenly abandons a project and runs away with investors' money. Typically, it refers to when developers of a DeFi project or token lure people to invest, then abruptly withdraw all liquidity or funds, causing the token's price to collapse to near zero. The term comes from the idea of "pulling the rug out" from under investors' feet.
- **Ripple (XRP)**: Ripple is a company (Ripple Labs) known for a payments protocol, and XRP is the digital asset associated with it. XRP is a cryptocurrency designed for fast, low-cost international transfers. The Ripple company has used XRP and its network in collaborations with banks for cross-border payment solutions. (Note: The terms Ripple and XRP are often used interchangeably in casual conversation, but technically Ripple is the company and network, XRP is the token).
- **Rewards (Staking/Mining Rewards)**: In crypto, rewards refer to the coins earned by participants who help secure the network. Mining rewards (for PoW miners) and staking rewards (for PoS validators) are incentives given for block production or validation. For example, Ethereum stakers earn ETH as a reward for securing the network, and Bitcoin miners get BTC when they find new blocks (plus transaction fees).

S

- **Satoshi (unit)**: The smallest fraction of Bitcoin, equal to 0.00000001 BTC (one hundred-millionth of a Bitcoin). Often used when discussing tiny amounts of BTC. The unit is named after Satoshi Nakamoto, Bitcoin's creator.

- **Satoshi Nakamoto**: The pseudonym used by Bitcoin's mysterious creator (or creators). Satoshi Nakamoto authored the Bitcoin whitepaper in 2008 and launched the network in 2009, but their identity remains unknown. Satoshi mined some of the early bitcoins and then disappeared from public communication by 2011.
- **Scam**: Unfortunately common in the crypto space, scams can take many forms, fake giveaways, phishing sites, pyramid schemes, and more. Always be cautious: if something sounds too good to be true (e.g. "guaranteed 10x returns" or free ETH from a random link), it likely is. Use DYOR and never share your private keys.
- **SEC**: The U.S. Securities and Exchange Commission. While not a crypto term per se, the SEC often comes up in discussions about regulation of cryptocurrencies and ICOs (determining if certain tokens are unregistered securities, etc.). Global equivalents include regulators like the FCA (UK) or ESMA (EU).
- **Slashing**: A penalty in Proof-of-Stake systems where a validator loses some or all of their staked tokens for dishonest or harmful behaviour.
- **Seed Phrase (Recovery Phrase)**: A sequence of typically 12 or 24 words that is the backup to your crypto wallet. This phrase is your private key, expressed in words for convenience. Anyone with your seed phrase can access your funds, so it must be kept secret and safe. If your device or wallet is lost, you can recover your funds by inputting the seed phrase into a compatible wallet app. Never share it with anyone and beware of phishing attempts asking for it.
- **Sharding**: A scaling technique (notably planned for Ethereum 2.0) where the blockchain's data is partitioned into smaller pieces called shards. Each shard is like a mini-blockchain with its own subset of data and validators, allowing the network to process many transactions in parallel rather than every node handling everything. Sharding aims to increase transaction throughput.
- **Shilling**: Promoting a cryptocurrency (often exaggeratedly) as a great investment, usually for one's own benefit. Someone "shilling" a coin might hype it up on social media or forums to drive the price higher (perhaps because they already hold a lot of it). It's considered bad form unless the promotion is transparent and honest (e.g. "he's just shilling his bags" means he's hyping a coin he owns and wants to sell high).
- **Shitcoin**: A vulgar slang term for a cryptocurrency that is deemed worthless or without a serious purpose. People use this term for coins they believe have no viable future or were made as cash grabs. It's subjective, one person's promising project might be another's "just another shitcoin" if they're sceptical. (Use of the term is common in informal chats but obviously not polite).
- **Smart Contract**: Self-executing code on the blockchain that automatically enforces agreements or triggers actions when certain conditions are met. Smart contracts run on platforms like Ethereum and enable complex applications like DeFi or NFTs. They are "trustless" in the sense that you don't need to trust a middleman, the code itself ensures the

terms are fulfilled. (For example, a simple smart contract could say if Bob pays 1 ETH into the contract, then release a digital asset to Bob).

- **Soft Fork**: A network upgrade or change to a blockchain protocol that is backward-compatible. In a soft fork, updated nodes follow new rules but old nodes (that haven't upgraded) still see the new blocks as valid (as long as the new rules don't violate the old rules). This means a soft fork doesn't split the chain, it's a gentle upgrade. An example was Bitcoin's SegWit upgrade; non-upgraded nodes still functioned, they just ignored the SegWit part of transactions.
- **Stablecoin**: A cryptocurrency designed to maintain a stable value, usually pegged to a fiat currency like the US dollar (e.g. 1 token = $1). Examples include USDT (Tether), USDC, and DAI. Stablecoins achieve stability through various means: fiat reserves, over-collateralised crypto loans, or algorithmic mechanisms. They are widely used in trading and DeFi as a way to park value without leaving the crypto ecosystem.
- **Staking**: Locking up your cryptocurrency in a Proof-of-Stake network to support its operations (validating transactions, securing the network) in return for rewards. It's analogous to mining but without heavy hardware, instead, your "stake" (coins) and honest behaviour are what qualify you to earn new coins. Staking can often be done via wallets or exchanges and typically yields a percentage return over time.
- **Slippage**: The difference between the expected price and actual execution price of a trade, often caused by low liquidity or high volatility.
- **Solidity**: The primary programming language used for writing smart contracts on Ethereum and several other blockchains. It's a high-level language with a syntax similar to JavaScript, designed to implement smart contracts that run on the Ethereum Virtual Machine (EVM).
- **Spam Attack**: On blockchains, this refers to someone flooding the network with a high volume of transactions (often low value) to slow the network and increase fees, or to bloat the blockchain's size. These attacks aim to disrupt normal usage or test the network's limits.
- **Snapshot**: A record of blockchain data at a specific point in time. Used for airdrops, governance votes, or token distributions.
- **Sybil Attack**: A type of attack on a network where one entity creates many fake identities (nodes) to gain disproportionate influence. In crypto, consensus mechanisms like PoW and PoS are designed to make Sybil attacks costly (you'd need a lot of mining power or a lot of coins to fake many identities with influence).

T

- **TA (Technical Analysis)**: An approach to evaluating investments (like crypto prices) by analysing statistical trends gathered from trading activity, such as past prices and volume. Traders who do TA use charts and indicators (like moving averages, RSI, etc.) to try to predict future movements. It's often contrasted with fundamental analysis, which focuses on the underlying project fundamentals.

- **Tornado Cash**: A privacy tool for Ethereum that uses zero-knowledge technology to obscure the source of funds. It was later sanctioned by the U.S. government.
- **Testnet**: A parallel blockchain used for testing new features or applications without risking real assets. For example, Ethereum's testnets (like Goerli or Sepolia) allow developers to deploy contracts and users to try things using test ETH (worth nothing) before it goes live on the mainnet. Think of it as a sandbox version of the blockchain.
- **Token**: A general term for any cryptocurrency that is not a native coin of its own blockchain but operates on another chain (or any crypto asset in general). For instance, UNI is a token on Ethereum (an ERC-20 token). "Token" is also used broadly to refer to any crypto asset, including coins. Tokens can represent value, utility, or even assets and rights within a platform. (All coins can be called tokens, but not all tokens are standalone coins with their own chain).
- **Tokenomics**: A portmanteau of "token" and "economics", referring to the economic design of a crypto project's token. It includes the token's supply and distribution, inflation/emission schedule, use cases, and incentive mechanisms. Good tokenomics are important for a project's long-term viability (for example, how a token gains value, how supply is controlled, etc.).
- **Turing-Complete**: Describes a system capable of performing any computational logic. Ethereum is Turing-complete, enabling complex smart contracts.
- **Total Value Locked (TVL)**: A metric popular in DeFi that represents the total assets (value) deposited in a protocol, for example, in all the liquidity pools, lending contracts, or vaults of that platform. It indicates how much money is "locked" up and being used by the protocol's smart contracts. TVL is often used to gauge the popularity or size of a DeFi project (higher TVL generally = more usage).
- **TPS (Transactions Per Second)**: How many transactions a blockchain can process each second, used as a measure of performance or throughput. For instance, Bitcoin handles around 5–7 TPS, Ethereum about 10-15 TPS (in its current form), whereas some blockchains or Layer 2 solutions claim thousands of TPS. Higher TPS means more capacity for activity, but often comes with trade-offs in decentralization or security.
- **Trading Volume**: The total amount of an asset traded during a given time period (often 24 hours for crypto stats). High trading volume means many coins are changing hands, which can indicate high interest and also often correlates with better liquidity (easier to buy/sell without moving the price).
- **Transaction**: The basic unit of operation on a blockchain, the act of sending value (or data) from one address to another, recorded on the ledger. A transaction typically includes the sender's address, recipient's address, the amount, and a digital signature proving the sender authorised it. On platforms like Ethereum, transactions can also trigger smart contract function calls (which might do things beyond value transfer).

- **Transaction Fee**: A small amount paid to use the network, given as a reward to miners/validators for processing the transaction. Fees help prevent spam and allocate limited space in each block, when a network is busy, users often compete by paying higher fees to get their transactions included faster.
- **Trustless**: A term describing a system (like a blockchain) where you do not need to trust any single intermediary or counterparty for it to function as intended. Instead, the rules of the system and consensus mechanism ensure honesty. For example, Bitcoin is trustless in the sense that you don't have to trust any particular miner, bank, or government, the network's protocol and widespread distribution mean it operates by math and consensus, not personal trust.

U

- **UTXO (Unspent Transaction Output)**: A concept in Bitcoin and similar cryptocurrencies. Each Bitcoin transaction consumes previous outputs and creates new outputs. A UTXO is a chunk of Bitcoin that you own and can spend, essentially an output of a transaction that has not yet been used as input in another transaction. The sum of all your UTXOs equals your total balance. UTXO-based models are like having many coins of various denominations in your wallet that together make up your total funds.
- **Utility Token**: A token designed to have a specific use or utility within a platform or service, rather than serving as just a general currency. For example, a token might grant access to a service, enable governance voting, or pay for fees in a DApp. Utility tokens are not intended to be investments per se (though they often trade on the market), but rather fuel for an ecosystem (like gas is the utility token for the Ethereum network in the form of ETH).
- **Uniswap**: A popular decentralised exchange (DEX) protocol on Ethereum that uses an automated market maker model and liquidity pools (rather than an order book) to facilitate trading of ERC-20 tokens. (Included here because Uniswap has become nearly synonymous with decentralised trading).
- **Unlocking**: In token sales or vesting schedules, this refers to tokens becoming available for use/trading after a lock-up period. For instance, team or investor tokens might be locked for a year and then gradually "unlocked" (released) each month thereafter, to prevent a sudden flood of supply on the market.

V

- **Validator**: In Proof-of-Stake systems, a node that is responsible for verifying transactions and creating new blocks, typically by staking tokens as collateral. Validators are randomly (or pseudo-randomly) chosen to propose the next block, with their odds often proportional to the amount they've staked. Honest behaviour is rewarded (with block rewards or fees), whereas dishonesty can be penalised by losing some of their staked tokens.

- **Volatility**: How much an asset's price moves up and down over time. A highly volatile asset like many cryptocurrencies can see large price swings in short periods (rapid and unpredictable changes). Volatility is often measured by standard deviation or variance of returns; in simpler terms, when someone says, "Bitcoin is volatile", it means its price can change a lot in a short time (which implies risk but also opportunity for traders).
- **Vitalik Buterin**: The co-founder of Ethereum (included as an important figure). Vitalik authored the Ethereum whitepaper and is a prominent developer and thought leader in the crypto space.
- **Vesting**: A token distribution mechanism where tokens are gradually released over time to prevent early investors from dumping large amounts immediately.

W

- **Wallet**: Software or hardware that stores your cryptocurrency keys and allows you to send, receive, and manage your coins. A wallet doesn't actually hold coins inside it; it holds private keys that prove your ownership of coins recorded on the blockchain. There are hot wallets (online, connected to the internet for convenience) and cold wallets (offline, for security). Examples: mobile app wallets, hardware wallets, paper wallets.
- **Wallet Address**: It's the public identifier you share to receive funds.
- **Web3**: The idea of a new, decentralised internet built on blockchain and cryptographic technologies. In Web3, users can own their data, digital assets, and identity, and services are often run by decentralised networks (DAOs, smart contracts) rather than centralised companies. Web1 was read-only, Web2 is read-write (but data is centralised on platforms), and Web3 is read-write-own, meaning users have a stake and control via tokens and decentralised protocols.
- **Whale**: Slang for an individual or organisation that holds a huge amount of cryptocurrency, enough that their trades might sway the market. For example, a Bitcoin whale might have tens of thousands of BTC. When whales buy or sell, they can cause noticeable price movements due to the large volume.
- **Whitelist**: In crypto contexts, a list of approved participants for something. For example, ICOs or NFT mints might require you to be whitelisted to participate (often by being an early community member or passing KYC). If you're on the whitelist, you get early or guaranteed access to buy.
- **Whitepaper**: A document (often academic style) that outlines a problem and how a particular project or technology solves it. In cryptocurrency, the whitepaper usually describes the protocol, technical details, and purpose of the coin or project. The most famous example is the Bitcoin Whitepaper written by Satoshi Nakamoto in 2008, which explained the concept of Bitcoin. Reading a project's whitepaper is part of doing due diligence (see DYOR).

- **Wrapped Token**: A token that represents another asset, often used to bring non-native assets into a different blockchain ecosystem. For example, Wrapped Bitcoin (WBTC) is an ERC-20 token on Ethereum that is backed 1:1 by actual Bitcoin kept in reserve. It allows BTC holders to use their bitcoin within Ethereum's DeFi apps. "Wrapping" typically involves a custodian or smart contract that locks the original asset and issues an equivalent amount of the wrapped version on the other chain.
- **Wash Trading**: A market manipulation tactic where a trader buys and sells the same asset to inflate volume or mislead others about real demand.

X

- **XRP (Ripple)**: A cryptocurrency created by Ripple Labs for fast, low-cost international payments. XRP runs on the XRP Ledger, a blockchain that doesn't use mining (it uses a consensus protocol among a set of trusted validators). XRP gained popularity as a bridge currency for bank and remittance networks. It's known for its quick settlement (seconds) and high throughput, though its degree of decentralisation is often debated.
- **XBT**: An alternative ticker symbol for Bitcoin, used on some exchanges or platforms (much like gold is "XAU" and silver "XAG" under ISO conventions). "BTC" is more commonly used, but you might see XBT in certain contexts, it means the same thing.
- **XRP Ledger**: The underlying blockchain network on which XRP transacts. The XRP Ledger reaches consensus through its unique consensus algorithm (not PoW/PoS) and is maintained by a network of validators. It's designed for speed and efficiency in value transfer.

Y

- **Yields (Yield Farming)**: In crypto, "yield" refers to the return earned on an investment, often expressed as an annual percentage. Yield farming is the practice of moving assets around various DeFi platforms to earn the best returns, such as interest or new token rewards. For example, providing liquidity on a DEX might earn trading fees and additional token incentives. Yield farmers often chase high APYs, but those can come with higher risks.
- **YTD (Year-to-Date)**: A common financial term meaning from the start of the current year up until today. You might see YTD returns for a coin (e.g. "Bitcoin is up 120% YTD"), but it's not crypto-specific. Included here as it appears in some crypto dashboards for performance metrics.
- **YSK**: Short for "You Should Know". Sometimes used in forums or social media to preface a helpful tip or piece of info related to crypto.

Z

- **Zero Confirmation**: A state where a transaction has been broadcast to the network but not yet included in a block (thus zero confirmations). Such transactions are seen in wallets as

"unconfirmed". They are not yet final and could be double-spent or cancelled until a miner includes them in a block.

- **Zero-Knowledge Proof (ZKP)**: A cryptographic technique where one party (the prover) can prove to another (the verifier) that a statement is true without revealing any additional information about it. In simpler terms, it's like proving you know a secret without revealing the secret. Zero-knowledge proofs have big implications for privacy in crypto, for example, Zcash uses zk-SNARKs to allow transactions that reveal no addresses or amounts, and Ethereum layer-2 solutions use ZK proofs to bundle and verify transactions off-chain. This technology can enable verification of data while keeping that data completely private.
- **Zk-SNARK**: Stands for "Zero-Knowledge Succinct Non-Interactive Argument of Knowledge," which is a specific type of zero-knowledge proof. Zk-SNARKs allow a proof that something is true, with the proof itself being very short and quick to verify, and without interaction between prover and verifier. Zcash made this term famous by using zk-SNARKs for private transactions.
- **Zk-Rollup**: A Layer 2 scaling solution for blockchains (especially discussed in Ethereum) that uses zero-knowledge proofs. A zk-rollup bundles hundreds of transactions off-chain and then posts a summary proof (a ZK proof) on-chain. This proof attests to the validity of all those transactions. The result is much higher throughput and lower cost, while the security is inherited from the main chain's verification of the proof.
- **51% Attack**: (Even though it starts with a number, this is an important concept often discussed). A scenario where a single entity or coalition gains more than 50% of a network's mining (or staking) power, allowing them to potentially manipulate the blockchain. In a 51% attack, the attacker could temporarily prevent new transactions from confirming, halt payments between some or all users, or double-spend their own coins. However, they cannot create money from nothing or steal others' coins directly, they can only rewrite recent history and censor/replace transactions. In major networks like Bitcoin or Ethereum, a 51% attack is extremely difficult due to the immense cost and resources required.