VF BLOCKCHAIN

CRYPTO LEXICON

The Most Important Terms - From A to Z

Airdrop: In an airdrop, free coins are given to the community or to a specific group of investors (e.g., Ethereum holders) — like a promotional gift. This helps create interest and future buying for new projects.

Altcoin: Altcoin stands for "alternative coin" and refers to any coin other than Bitcoin. Examples are Litecoin, Bitcoin Cash, Dash, NEO, Cardano, and others.

Atomic Swap: An atomic swap is a trade between two different cryptocurrencies that doesn't need a third party. This is called cross-chain trading. The trade is protected by something called Hash-Time-Locked Contracts (HTLCs). These make sure the swap is fair and no one can cheat.

Block and Blockchain: Transactions are saved in blocks. These blocks are linked together using special math functions, making them impossible to change. The chain of these blocks is called the blockchain. It's a shared database that can't be changed.

Consensus Algorithm: This is the system that helps all users agree on what is true on the blockchain. It decides things like who owns coins and how many coins there are.

dApp: A dApp (decentralized app) doesn't run on one central server. Instead, it runs on the blockchain and is not controlled by one person or company. All the app's data is stored on the blockchain.

DEX (Decentralized Exchange): A DEX is a crypto trading platform that doesn't rely on a central company like Coinbase or Binance. Instead, users trade directly with each other. The coins stay in the user's control. Examples include Bitshares, EtherDelta, and NEX. 0x is a protocol used by some DEXs.

ERC20 Token: ERC20 tokens are coins that follow a standard set of rules on the Ethereum blockchain. This helps them work with wallets, exchanges, and apps.

FIAT: Fiat money is regular currency like the Euro, US Dollar, or British Pound. It's money made and controlled by governments.

FOMO (Fear of Missing Out): FOMO means the fear of missing out on something good. In crypto, this often makes people buy too quickly when prices go up—sometimes at bad prices. Always stay calm and think carefully.

FUD (Fear, Uncertainty, and Doubt): FUD is when someone spreads fear or bad news—often on purpose—to hurt a crypto project or drive down prices. It's used to make people panic and sell their coins.

Hardfork: A hardfork is a split in a blockchain network. It happens when a big update makes the new version not compatible with the old one. After the fork, both versions run separately but share the same history up to the fork.

Hashing: Hashing uses math to turn data into a fixed-size string of numbers and letters (a hash). It's a one-way function: you can't figure out the original data just from the hash. Hashes are like digital fingerprints.

Hashrate: The hashrate shows how much computing power is in the network. The more powerful the network, the faster it can solve the math problems that run the blockchain—and the safer it becomes.

Hash-Time-Locked Contracts (HTLC): HTLCs are a way to send cryptocurrency only if the other person does what they're supposed to. If they don't, you get your money back. HTLCs are used in things like atomic swaps.

ICO (Initial Coin Offering): An ICO is like an IPO (stock market launch), but for crypto. Instead of stocks, people get tokens. You send cryptocurrency (like Ether) to a smart contract and get project tokens in return.

KYC (Know Your Customer): KYC means crypto exchanges have to collect customer info—like name and address—for legal reasons. It helps stop fraud and crime.

Lightning Network: The Lightning Network is a tool for making Bitcoin faster and cheaper. It moves small payments off the main blockchain into special payment channels, then adds the final result later. It's great for fast and tiny payments.

MimbleWimble: MimbleWimble is a system to make blockchains smaller and more private. It cuts out extra data and hides who sent what to whom. This helps Bitcoin work better and more privately.

Mining: Mining is when computers solve hard math puzzles to add new blocks to the blockchain. This process is called Proof of Work (PoW). Miners check transactions and get rewards when they find a new block.

Node / Nodes: A node is a computer in the blockchain network. A full node stores all past transactions and checks if everything follows the rules.

Oracles: Oracles bring real-world data into the blockchain. They let smart contracts use outside information—like prices, weather, or sports scores.

Plasma: Plasma is a system that makes Ethereum faster by adding extra chains (like branches on a tree). Most of the work is done off the main blockchain to help it run more smoothly.

Private Key: A private key is like your password for your crypto. It gives access to your coins. Never share it with anyone.

Proof of Stake (PoS): In PoS, you don't mine with computing power. Instead, you lock your coins to help run the network. The more coins you lock, the higher your chance to create new blocks and earn rewards.

Proof of Work (PoW): PoW is a way blockchains agree on what's real. Computers compete to solve puzzles. The fastest one adds a block and gets a reward. More computer power means a better chance to win.

Pruning: Pruning is a way to save space on your computer. It deletes old data from a blockchain node that's no longer needed. You can always download it again if necessary.

Public Key: The public key is your blockchain address, like a bank account number. People use it to send you coins. Example: 1PxrZp2SJ2GmeX328zWmhodsYWFxzwuG7t

Raiden Network: Raiden is a tool for Ethereum that works like the Lightning Network. It moves payments off the main blockchain using "state channels." This helps Ethereum work faster and cost less.

Relayer: Relayers help people trade tokens without a central exchange. They collect buy/sell offers (in an order book) and match users. They don't touch your tokens—they just help you trade.

SCAM: A scam is a trick. Sometimes fake websites or social media accounts ask you to send Bitcoin or Ethereum. Don't do it—it's a scam trying to steal your money.

Schnorr Signatures: Schnorr is a secure signature method that connects private keys, public keys, and digital signatures. Many experts think it's one of the best. It also works well with group (multi-) signatures.

ScriptSig: A ScriptSig is part of a Bitcoin transaction. It shows the sender's public key and digital signature to prove the sender owns the coins.

Security Token: A security token is like a digital stock. It can show ownership in a company or share in profits. Unlike utility tokens, security tokens have legal rights.

SegWit (Segregated Witness): SegWit is a Bitcoin update that moves the signature part of transactions out of the main block. This lets more transactions fit and helps tools like the Lightning Network work better.

Sidechain: A sidechain is a second blockchain that runs alongside the main one. You can move coins between them. Sidechains help blockchains work faster and avoid double spending.

Sharding: Sharding breaks a blockchain into smaller pieces (shards). Each computer only checks its part, not the whole chain. This helps the system work much faster.

Smart Contract: A smart contract is a program that runs by itself on the blockchain. Once started, it can't be changed. It follows rules like "if this happens, then do that," and it can even hold and move money.

Softfork: A softfork is a small update to the blockchain that still works with old versions. It adds new features without splitting the network.

SPV (Simplified Payment Verification): SPV is a light way to check payments on the blockchain. It only looks at part of the data, not the whole thing, which saves time and space.

State Channel: A state channel is like a private line between two users or a user and a service. They sign all messages to prove they happened. The final result is saved on the blockchain, but the steps in between are done off-chain.

UTXO (Unspent Transaction Output): Bitcoin doesn't use account balances like banks. Instead, it uses UTXOs—these are pieces of coins that haven't been spent yet. They make sure no one spends more than they have.

Utility Token: A utility token is a digital ticket for using a service. It doesn't give you profits or ownership. It's used to pay for things on the blockchain, like fees or access.

Wallet: A wallet is a digital place where you keep your private keys. It doesn't hold your coins directly—it holds the keys that give you access to them on the blockchain.

Whitepaper: A whitepaper is a document that explains a blockchain project. It includes technical details, how many coins there will be, and how they'll be used.

zk-SNARKs: zk-SNARKs is a way to hide all details of a crypto payment. No one can see who sent coins, how many were sent, or where they went. But it still proves the payment is real. Think of it like turning on your phone's flashlight without showing your password—people can see it works without knowing your code.