VF Blockchain

The Most Important Terms - Cypto Lexicon From A-Z

Airdrop:

In an airdrop, free coins are distributed to the community or to a specific group of investors (e.g., Ethereum holders) - a kind of promotional gift, so to speak. This increases the attention and subsequent purchases for young projects.

Altcoin:

When referring to an altcoin, it usually means an alternative coin beside Bitcoin. Examples include Litecoin, Bitcoin Cash, Dash, NEO, Cardano, etc.

Atomic Swap:

An atomic swap is a trade between two different cryptocurrencies that occurs without a third party (cross-chain trading). The transaction is secured by Hash-Time-Locked Contracts (HTLC). HTLCs ensure that the atomic swap is completely trustless, and each party fulfills the terms of the trade agreement. Through an atomic swap, for example, Bob can exchange 70 Litecoins (LTC) for 1 Bitcoin (BTC).

Block and Blockchain:

Transactions are stored in a block and linked together through hashing functions, making them inseparably connected. When the blocks are chained together, they form the blockchain, a decentralized database whose values are immutable.

Consensus Algorithm:

The consensus algorithm is the engine of every blockchain. This algorithm determines how consensus is reached on the blockchain, i.e., what state prevails on the blockchain (who owns many coins, how many coins exist, etc.).

dApp:

Decentralized Application. A dApp does not run centrally on a server but rather decentralized and autonomously on the blockchain, controlled by no one. The app's data is stored on the blockchain. Examples of dApps include CryptoKitties, BitClave, etc.

DEX:

Decentralized Exchange. A DEX is a decentralized trading platform or cryptocurrency exchange. Unlike centralized cryptocurrency exchanges such as Coinbase, Bittrex, and Binance, decentralized exchanges are not controlled by a central company but operate independently and decentralized. Control over the coins lies entirely with the user. Examples include Bitshares, EtherDelta, and NEX. 0x is a protocol for decentralized exchanges.

ERC20 Token:

ERC20 tokens are tokens based on the Ethereum blockchain. These tokens use a standard template, ensuring that they comply with certain rules or specifications to ensure consistent functionality. Examples include OmiseGo, Golem, TenX, which are ERC20 tokens.

FIAT:

Fiat Money. The term describes fiat currencies such as the Euro, US Dollar, British Pound, and other traditional currencies.

FOMO:

Fear of Missing Out. FOMO describes the fear of missing out on an opportunity. This phenomenon often leads market participants to jump into a rising market and buy at inflated prices - therefore, always remain rational.

FUD:

Fear, Uncertainty, and Doubt. When referring to FUD, fear, uncertainty, and doubt are spread to portray a specific project in a negative light. This marketing strategy aims to instill certain fears to persuade investors to sell a particular coin or token.

Hardfork:

A network split, usually necessary when a major update is required that is no longer backward compatible with the existing version of the blockchain. New blocks are found on the new version of the blockchain, but not on the older one. However, both blockchains share the same transaction history.

Hashing:

A hashing function generates a string of characters to encrypt given data using mathematical functions. Hashing functions are one-way functions, meaning you can derive the public key from the private key but not vice versa. A hash is, therefore, a digital fingerprint.

Hashrate:

The hashrate indicates the computational power of the entire network. Each computer in a network has a certain computational power. The hashrate specifically indicates the speed at which a computer can perform a calculation. In the Bitcoin network, for example, this is necessary to solve highly complex mathematical problems. The higher the hashrate, the more secure the network.

Hash-Time-Locked Contracts (HTLC):

Hash-Time-Locked Contracts (HTLC) are a technical implementation of payments using cryptocurrencies, allowing one party to pay another under the condition that the other party cooperates. If the other party does not cooperate, the sender automatically receives their payment back. HTLCs are used to build protocols (rules) for so-called Atomic Swaps.

ICO:

Initial Coin Offering (ICO): A type of IPO in the blockchain sector. Instead of issuing stocks, coins or tokens are issued. This means that the investor sends a cryptocurrency to a smart contract and receives tokens in exchange.

KYC:

Stands for Know Your Customer. Access providers (cryptocurrency exchanges) are legally required to identify customers (address data, etc.).

Lightning Network:

The Lightning Network is a scaling solution for the Bitcoin blockchain, enabling transactions to be processed not on the blockchain itself but initially through so-called payment channels. This leads to a significant relief of the blockchain. Due to marginal transaction fees, the Lightning Network is also suitable for microtransactions.

Mimble Wimble:

Mimble Wimble is primarily a protocol to enhance Bitcoin. Specifically, Mimble Wimble helps improve the scalability of Bitcoin by compressing the information on the blockchain to its essentials - thereby drastically reducing the blockchain size. At the same time, Mimble Wimble introduces anonymous or private transactions to the Bitcoin blockchain. In simplified terms, Mimble Wimble leads to transactions on the Bitcoin blockchain no longer being traceable - similar to what privacy coins already enable.

Mining:

Proof of Work (PoW) is a mechanism where miners compete to solve cryptographic puzzles, with higher computational power (hash power) increasing the chance of finding a block and receiving a block reward. Miners verify transactions on the blockchain by adding new blocks.

Node/Nodes:

A network node (computer) on the blockchain. A full node stores all blockchain transactions ever made. It verifies whether the rules of the blockchain have been followed, ensuring transaction accuracy, proper signing, and correct formatting.

Oracles:

Oracles are components of a blockchain that validate information. Oracles help make data from outside the blockchain world usable. For example, prices or sensor data can be observed using oracles and further processed in the blockchain world. Oracles are essential for the functioning of smart contracts.

Plasma:

Plasma is initially a scaling solution for the Ethereum blockchain. Specifically, Plasma is a 2-layer solution, allowing the Ethereum blockchain to process more data by adding another layer (tree with branches). The actual workload is shifted from the main blockchain to side chains.

Private Key:

The private key, comparable to your PIN or password. Never share your private key with anyone!

Proof of Stake (POS):

Proof of Stake (POS) is a consensus algorithm where the stakeholder (coin owner) locks their coins/tokens in a wallet to generate a block and confirm transactions. The number of coins is crucial here. The more coins owned, the higher the chance of generating a block.

Proof of Work (PoW):

Proof of Work (PoW) is a consensus algorithm where miners compete to solve cryptographic puzzles. The more computational power the miner has, the greater the chance of generating a block.
Pruning: Pruning is an efficient way to save storage space on a node. When pruning is enabled on a node, downloaded block data and already validated transactions are deleted since older data is no longer needed. If something goes wrong, the data can be restored.

Public Key:

The public key is the public address, comparable to your bank account number. For example, a Bitcoin address: 1PxrZp2SJ2GmeX328zWmhodsYWFxzwuG7t.

Raiden Network:

The Raiden Network is a scaling solution and payment system for the Ethereum blockchain. Similar to the Lightning Network, the Raiden Network relies on transactions that occur not on the blockchain but initially in so-called state channels (channels) - alongside the blockchain. This is intended to relieve the main chain.

Relayer:

Relayers are a type of peer-to-peer network (collection points) that organize buy and sell orders in an order book to simulate an exchange without being one. Relayers act as intermediaries between buyers and sellers of cryptocurrencies (ERC20 tokens) - similar to eBay.

Crypto Lexicon

SCAM:
A scam is a fraud. Users are often prompted to send Bitcoin or Ethereum through fake websites, social media addresses, etc. - do not follow these instructions, as it is usually a scam.

Schnorr Signatures:
Schnorr is a cryptographic technique named after the German mathematician Claus-Peter Schnorr, which links private and public keys as well as signatures. Many cryptographers view Schnorr signatures as the best signatures in the market because they are not only highly secure but also easy to verify. Additionally, Schnorr signatures support multiple signatures (multi-signatures).

ScriptSig:
A signature script (ScriptSig) includes both the public key (public address) and the digital signature of the sender for authentication purposes.

Security Token:
A security token is similar to a security (stock) and can represent ownership and participation rights (revenue and profit sharing). In contrast, a utility token does not confer such rights but rather serves as a ticket to transfer value on the blockchain or to use services on the blockchain.

SegWit:
Segregated Witness (SegWit) is a scaling solution for the Bitcoin blockchain, where signatures are segregated to accommodate more transactions in a block. SegWit also serves as the basis for 2-layer solutions like the Lightning Network.

Sidechain:
A sidechain is a separate blockchain that runs alongside the main blockchain (main chain). Typically, tokens used on the main chain can also be used on the sidechain. When switching to the sidechain, it is usually marked to prevent double spending. Sidechains can help scale and relieve blockchains.

Sharding:
Sharding involves dividing the blockchain into multiple sub-segments (shards), so not all nodes (network computers) need to validate all transactions, only specific ones. This significantly speeds up the blockchain.

Smart Contract:
A program on the blockchain that self-executes and cannot be stopped. A smart contract is executed not by a central server but by multiple network nodes on the blockchain. This means once a smart contract is set up and activated, it cannot be stopped. The revolutionary aspect is that a smart contract can hold money and decide what to do with it (if-then sequence).

Softfork:
A softfork is a software update on the blockchain that introduces new features but remains backward compatible with older versions. It is comparable to a new version of Microsoft Word. A softfork usually does not result in a network split.
SPV: Simplified Payment Verification (SPV) is a simplified payment check. It checks whether certain transactions appear in a block, eliminating the need to download the entire blockchain to verify the correctness of a payment.

State Channel:
A State Channel is a channel between 2 users or a user and a service (machine). Each message in this channel is signed by the respective participant, making it irreversible. Transactions initially take place outside the blockchain in the channel (Off-chain), with only the final valid result

of the transactions in this channel being recorded on the blockchain.

Unspent Transaction Output (UTXO):
In the Bitcoin network, there is no account balance or saldo as we know it from our bank account. Instead, in the Bitcoin network, we speak of so-called Unspent Transaction Outputs (UTXO). Translated, this means: These are unspent bitcoins or accumulated bitcoins. Because every transaction in the Bitcoin network always consists of one or more inputs (senders) and outputs (receivers). Each input is also, in turn, an output of a previous transaction. Through the UTXO model, no one can spend more bitcoins than they have themselves.

Utility Token:
A utility token is a kind of ticket for a platform. A utility token does not confer any further rights such as revenue or profit-sharing rights but serves only to transfer value on a blockchain and pay for services. This means a utility token has a specific function on the blockchain, such as paying transaction fees or gaining access to the system or services.
Wallet: Your digital wallet. Your coins are not stored there, but rather the private keys that give you access to your coins on the blockchain.

Whitepaper:
A concept paper that typically describes the blockchain project. It usually contains technical details of the blockchain, as well as information about the number of outstanding coins and their use.

zk-Snarks:
zk-Snarks is a cryptography technique where the contents of a payment transaction are fully encrypted or concealed, so that outsiders cannot see how many coins are sent from whom to where. zk-Snarks effectively provide proof that a transaction is valid without disclosing any information about the transaction itself. Laymen can imagine this as with an unlocked smartphone. The person does not show the password (PIN) or the unlocked phone but instead activates a specific function of the smartphone (e.g., WLAN or camera), thereby proving that they actually have control over the smartphone. What's special about zk-Snarks is that these so-called Zero-Knowledge Proofs can be verified for accuracy within milliseconds and with minimal data.