CompTIA Blockchain Advisory Council

Blockchain Terminology:
A GLOSSARY FOR BEGINNERS

Learn the basic terminology for blockchain technology from CompTIA. We have the entire list of terms beginners need to know.

51% Attack
When more than 50% of the miners in a blockchain launch an attack on the rest of the nodes/users to attempt to steal assets or double spend.

Address
Much like a URL, a blockchain address is the location to or from which transactions occur on the blockchain.

Alt-coin
Any coin or token other than Bitcoin.

Attestation Ledger
A register or account book created for the purpose of providing support/evidence of individual transactions. Normally, an attestation ledger is used to verify that a transaction has been carried out, or to verify the authenticity of products or transactions.

Bitcoin
The first and most popular cryptocurrency based on DLT technology developed from a whitepaper written by Satoshi Nakamoto in 2008.

Block
A group of transactions entered into a blockchain; analogous to a page of a ledger or record book.

Blockchain
A mathematical structure for storing digital transactions or data in an immutable, distributed, decentralized digital ledger consisting of blocks that are linked via cryptographic signature that is nearly impossible to fake, hack or disrupt.

Blockchain (Private a.k.a. Permissioned)
A blockchain that resides on a private network of computers that is only accessible to those with permission.

Blockchain (Public a.k.a. Permissionless)
A blockchain that resides on a network of computers around the world that is accessible to everyone.

Byzantine Fault Tolerance (BFT)
A property of a distributed, decentralized system to resist complete failure even when some of the nodes fail or act maliciously.

Centralized
A system or process for which there is a singular (i.e., central) source of authority, control and/or truth.

Chain of Custody
The entire chain of documentation of ownership of a product during its lifecycle from raw materials to the final end user.

Chaincode
Another name for a smart contract.

Consensus Mechanism - Proof of Authority (PoA)
PoA is an alternative form to the PoS algorithm. Instead of staking cryptocurrency (wealth), in PoA you stake your identity. This means voluntarily disclosing who you are in exchange for the right to validate blocks. Any malicious actions you undertake as a validator will reflect back on your identity. PoA blockchains require a thorough form of KYC (Know Your Customer - a verification process that determines you actually are who you claim to be).

Consensus Mechanism - Proof of Burn (PoB)
PoB allows the miners to "burn" or destroy cryptocurrency which grants them the right to add blocks in proportion to the coins destroyed. Essentially, miners burn coins/tokens to buy virtual mining rigs that give them the power to mine blocks. The more currency burned by the miner, the bigger the ensuing virtual mining rig. To burn, miners send currency to a verifiably un-spendable address. This process does not consume many resources, thus PoB is often called PoW without energy waste.

Depending upon the implementation, miners are allowed to burn the native currency or the currency of an alternative chain, and in exchange, they receive a reward in the native currency of the blockchain.

Consensus Mechanism - Proof of Capacity (PoC)
PoC allows the mining devices in the network to use their available hard drive space to decide the mining rights, instead of using the mining device's computing power (as in PoW) or the miner's stake in the cryptocurrency (as in PoS).

Consensus Mechanism - Proof of Stake (PoS)
In PoS, miners put up(i.e., "stake") some of the blockchain's cryptocurrency (e.g., ether for the Ethereum blockchain) in order to increase their chances of being selected to validate a block. The stake is locked up as a deposit to ensure the miner validates the block according to the rules. If the miner violates the rules, the deposit will be "burned" or destroyed. PoS is less resource intensive than PoW since fewer miners are racing to solve the mathematical formula.

Consensus Mechanism - Proof of Work (PoW)
In PoW, transaction data (block) + a random strings of digits (nonce of block) are repeatedly applied to a (hashing) mathematical formula by miners, until a desirable outcome is found (the proof of work). Other miners then verify the proof of work by taking the alleged input string and applying it to the same formula to see if the outcome is indeed that what was presented. If the results are the same, the transaction is verified and added to the blockchain. As many miners are racing to solve the formula which requires a great deal of computing power, PoW is resource intensive.

Consensus Mechanism (a.k.a. Consensus Protocol)
The process used to validate a transaction across a distributed blockchain network designed to achieve Byzantine Fault Tolerance.

Cryptocurrency
Digital money which uses encryption and consensus algorithms to regulate the generation of coins/tokens and transfer of funds. Cryptocurrencies are generally decentralized, operating independently of central authorities.

Cryptography
The science of securing communication using individualized codes so only the participating parties can read the messages.

DAO (Decentralized Autonomous Organization)
A governance structure without a central authority which rewards good behavior and penalizes bad behavior by a set of pre-defined rules which can only be changes by a vote, which typically requires a stake, adding risk to the process to discourage bad actors, amongst the participants.

DApp
Software which does not rely on a central system or database but can share information amongst its users via a decentralized database, such as a blockchain.

Decentralization/Decentralized
A system with no single point where the decision is made. Every node makes a decision for its own behavior and the resulting system behavior is the aggregate response.

Digital Identity (a.k.a. Self-Sovereign Identity)
The network or Internet equivalent to the real identity of a person or entity (like a business or government agency). Advocates of blockchain-based digital identity is to return ownership and control of personal information to the individuals. In any given transaction, personal information is not disclosed, but rather the information required by one party is verified by the digital identity application.

Digital Signature
A mathematical scheme for verifying digital messages or documents satisfy two requirements - they have authenticity (from a known sender) and integrity (were not altered in transit.

Digital Signature - Multi-signature
In order to increase security, multisig addresses require more than one digital signature (and therefore multiple keys) to sign a transaction or message.

Digital Signature - Ring
A digital signature that can be performed by any of a group of people that each have keys. A property of a ring signature is that it is impossible to determine which of the group signed the transaction.

Distributed
As opposed to decentralized, a distributed system shares processing and/or data across multiple nodes, but the decisions may still be centralized and use complete system knowledge.

Distributed Ledger Technology (DLT)
The larger class of technology of which blockchain is a subset. A digital system for recording the transaction of assets in which the transactions and their details are recorded in multiple identical copies at the same time with no central data store or administration.

Double Spending
A unique problem to cryptocurrency where the same coins or tokens are spent or traded twice.

Ethereum
A public blockchain that supports smart contracts.

Fiat
Legal tender the value for which is backed by a government or governmental body (e.g., US dollars, Euros)

Fork
A collectively agreed upon software update by all nodes in a distributed network. Sometimes, the previous version continues in parallel with the new version.

Fungible
The property an item of being exchangeable with other like items. For example, USD and Euros are fungible. The value of USD can be expressed in Euros.

Gas
A fee charged to write a transaction to a public blockchain. The gas is used to reward the miner which validates the transaction.

Genesis Block
The first or first few blocks of a blockchain.

Governance
Establishment of policies and continuous monitoring of their proper implementation of an organization or system.

Hash Function
A function that receives an input of any size and returns a unique string of a uniform length.

Hyperledger Fabric
IBM's private (permissioned) blockchain toolset.

Identity
The information on an entity used by computer systems to uniquely represent a person, organization, application, or device.

Immutable/Immutability
The property of being unchangeable. Once a transaction has been added to a block and written to a blockchain, it cannot be changed and therefore is immutable.

Initial Coin Offering (ICO)
The first sale of a blockchain coin or token.

Interoperability
The ability of two or more systems to communicate and exchange data. Due to various design decisions (e.g., consensus protocol) most blockchains are not interoperable, however there are many projects that are working to connect various blockchains.

IPFS (Interplanetary File System)
A peer-to-peer hypermedia protocol for storing and sharing data in a distributed file system using content-addressing to uniquely identify each file in a global namespace connecting all computing devices.

Know Your Customer (KYC)
The legal process of a business identifying and verifying the identity of its clients. KYC requirements vary from jurisdiction to jurisdiction.

Liquidity
The ease of converting an asset (or, in this case, cryptocurrency) to cash (fiat).

Mainnet
The production version of a blockchain.

Merkle Tree/Hash Tree
In cryptography and computer science, a Merkle or hash tree is a tree in which every leaf node is labeled with the hash of a data block, and every non-leaf node is labeled with the cryptographic hash of the labels of its child nodes.

Mining
In a public blockchain, the process of verifying a transaction and writing it to the blockchain for which the successful miner is rewarded in the cryptocurrency of the blockchain.

Node
A computer which holds a copy of the blockchain ledger.

Non-Fungible
The property an item of not being exchangeable with other like items. For example, USD and Euros are fungible. For example, a Stratovarius violin is non-fungible because the value of it cannot be expressed in a number of other violins.

Off-chain
Data stored external to the blockchain.

On-chain
Data stored within the blockchain.

Open Source
Software products that include permission to use, enhance, reuse or modify the source code, design documents, or content of the product.

Oracle
An application that connects blockchain applications to legacy applications.

Peer-to-Peer (P2P)
A direct connection between two participants in a system - can be computer to computer or person to person.

Provenance
The entire history of a product during its lifecycle including its chain of custody and all documentation of value added services and activities which were used to produce that product or service.

Public/Private Key
A public key is a unique string of characters derived from a private key which is used to encrypt a message or data. The private key is used to decrypt the message or data.

Satoshi Nakamoto
The name used by the person or entity who developed bitcoin, authored the bitcoin white paper, and created and deployed bitcoin's original reference implementation. As part of the implementation, Nakamoto also devised the first blockchain database.

Seed Phrase
A random sequence of words which can be used to restore a lost wallet.

Sharding
A type of database partitioning that separates very large databases the into smaller, faster, more easily managed parts called data shards. Sharding can potentially be used to improve blockchain performance

Sidechain
A discrete blockchain that is linked to a main blockchain via two-way pegs which enable assets to be interchanged between the main blockchain and the sidechain. Sidechains are a method to enable scaling and increase transaction speed by only performing necessary transactions on the main blockchain.

Smart Contract
Self-executing computer code deployed on a blockchain to perform a function, often, but not always, the exchange of value between a buyer and a seller.

Solidity
A JavaScript-like object-oriented programming language for Ethereum for implementing smart contracts on the Ethereum blockchain.

Stablecoin
A cryptocurrency which is underwritten by an asset or assets (e.g., fiat currency, commodities, etc.) designed to minimize the volatility of the price of the coin/token.

State Channel
A process by which blockchain transactions are executed off-chain, collected and then written to the main chain as a single transaction in order to improve performance and reduce cost.

Testnet
A staging blockchain environment for testing application before being put into production (or onto the mainnet)

Token
Cryptographic tokens represent programmable assets or access rights, managed by a smart contract and an underlying distributed ledger. They are accessible only by the person who has the private key for that address and can only be signed using this private key.

Token Generation Event
The creation and first sale of a blockchain coin or token.

Token Type - ERC-20
A type of fungible Ethereum token (i.e., smart contract) standard which is defined by a series of functions that must be supported, including functions to retrieve the total supply, transfer from one wallet to another, and approve a transaction. Typically, any given ERC-20 token has many copies which are held in a variety of crypto wallets.

Token Type - ERC-721
A type of non-fungible Ethereum token (i.e., smart contract) standard which is defined by a series of functions that must be supported, including functions to retrieve the total supply, transfer from one wallet to another, and approve a transaction. Each ERC-721 token is unique and non-interchangeable with other tokens (i.e., non-fungible).

Token/Coin Exchange
An application to buy, sell and trade cryptocurrencies.

Tokenless Ledger
A ledger that doesn't require a native currency to operate.

Tokenomics
The study, design and implementation of monetary management and distribution based on blockchain technology.

Transactions Per Second (TPS)
A measurement of the speed of a blockchain. The low TPS of most blockchains is a significant barrier to using blockchain for business, especially financial, applications.

Transparency
A primary property of public blockchains whereby any participant in a system or transaction can view the transactions on the blockchain.

Trust
Confidence in the integrity of an entity (e.g., person, organization, etc.).

Trustless
The elimination of trust from a transaction. Blockchain is called a trustless system because the two entities performing a transaction do not need to trust one another. The properties of blockchain - digital signatures, cryptography, etc. - provide the trust.

Vyper
A Python-like programming language for the Ethereum blockchain built for security, language and compiler simplicity, and auditability.

Wallet
A digital file that holds coins and tokens held by the owner. The wallet also has a blockchain address to which transactions can be sent.

Wallet (Cold)
A wallet disconnected from the internet.

Wallet (Hot)
A wallet connected to the Internet.

Wallet (Multisignature)
A wallet that requires multiple digital signatures to execute a transaction.

Zeppelin/Open Zeppelin
A community of like-minded Smart Contract developers.