A Glossary of Blockchain Terms*

Airdrop	An airdrop is a distribution of a cryptocurrency token or coin, usually for free, to numerous wallet addresses for marketing purposes.
Atomic swap	An atomic swap is a smart contract technology enabling the exchange of one cryptocurrency for another without using centralized intermediaries.
Bitcoin	Bitcoin is a type of digital currency that runs on the peer-to-peer (P2P) network without the need for central authority or intermediaries.
Block	A block is a collection of transactions that has not yet been recorded in any prior blocks.
Blockchain	A blockchain is a decentralized public ledger that uses cryptography to record transactions among a network's participating agents. It permits transactions to be gathered into blocks and recorded cryptographically into chain blocks in chronological order, and allows all users in the network to access the ledger. A central authority does not own, control, or manage this distributed database.
Blockchain application	A blockchain application is a P2P system for validating, time stamping, and permanently storing transactions and agreements on a shared ledger that is distributed to all participating nodes.
Byzantine fault tolerance (BFT)	BFT is the property of a system that can resist the class of failures derived from the Byzantine Generals' Problem, which is a logical dilemma that illustrates how a group of Byzantine generals may have communication problems when trying to agree on their next move. Thus, a BFT system can continue to operate even if some of the nodes fail or act maliciously.
Central bank digital currency (CBDC)	A CBDC is fiat money of a particular nation or region, issued and regulated by a country's monetary authority. Thus, CBDC is money that a government establishes and backs through its central bank in a virtual form.

*H. Kent Baker and Hak J. Kim compiled this glossary.

(Continued)

Cold wallet	A cold wallet is a component of hardware or other type of physical device that enables investors to access crypto-asset holdings.
Consensus protocol (algorithm or mechanism)	Consensus protocol is the set of rules and mechanisms implemented in a blockchain to consolidate the preferences and decisions of users and to manage decision-making of the network. It determines how users reach consensus on that blockchain in achieving the necessary agreement on a single data value or a single state of the network among distributed processes.
Consortium blockchain	A consortium blockchain is a system that is "semiprivate" with a controlled user group, but works across different organizations. The protocol layer is under the control of a consortium of firms that must govern according to legal frameworks and agreements external to the blockchain code. A consortium blockchain is a hybrid between the "low trust" offered by public blockchains and the "single highly trusted entity" model of private blockchains. Thus, a consortium blockchain is permissioned, semidecentralized, and has a multiparty consensus.
Crosschain	A crosschain is the interoperability between two relatively independent blockchains. It enables blockchains to speak to one another because they are built in a standardized way.
Cryptocurrency	A cryptocurrency is a digital or virtual currency that uses encryption techniques to regulate the generation of units of currency and verify the transfer of funds. It operates independently of a central bank. Many cryptocurrencies such as bitcoin are decentralized networks based on blockchain technology.
Cryptocurrency agnostic	Cryptocurrency agnostic means that projects are built to work with a multitude of tokens, cryptos, and altcoins, which allow users from different ecosystems to participate, further expanding building capacity across existing and new cryptocurrency projects.
Cryptoeconomics	Cryptoeconomics is using incentives and cryptography to design new kinds of systems, applications, and networks. It also studies economic interaction in adversarial environments.
Cryptographic hashing	Cryptographic hashing is the procedure of repeatedly inserting a random string of digits into hashing formula until finding a desirable output. It produces a single fixed length output. Some examples of hash function algorithms are MD5, MD4, or SHA-256.

(Continued)

Cypherpunk	A cypherpunk is someone who believes in privacy-enhancing technology.
Cryptography	Cryptography is a mathematical algorithm used to encrypt and decrypt information. In blockchain, it is used for creating wallets, signing transactions, and verifying the block.
Crypto tokens	A crypto token, also called a cryptocurrency or crypto asset, is a special kind of virtual currency token residing on its own blockchain and representing an asset or utility.
Decentralized application (dApp)	A decentralized application is a computer application that runs on a distributed computing system.
Decentralized autonomous organization (DAO)	A DAO is a virtual organization embodied in computer code and executed on a distributed ledger or blockchain.
Decentralized network	A decentralized network refers to a network in which anyone can transact on the ledger. The network is decentralized in the sense that no centralized entity governs the network.
Delegated Proof of Stake (DPoS)	DPoS is a consensus protocol that provides dependable verification and approval of transactions in a blockchain.
Distributed hash table (DHT)	DHT is a key-value store where the keys are hashes and widely used to coordinate and maintain metadata about P2P systems. Key-value pairs are stored in a DHT, and any participating node can efficiently retrieve the value associated with a given key.
Distributed ledger	A distributed ledger is a database that is shared across multiple sites or geographies accessible by multiple people. It allows transactions to open to the participants publicly. The participant at each node of the network can access the records shared across that network and can own an identical copy of it. Any changes or additions made to the ledger are reflected and copied to all participants.
Double spending	Double spending is the result of successfully spending digital currency more than once. Blockchain protects against double spending by verifying each transaction in the network. It ensures that the inputs for the transaction had not previously already been spent.
Encryption	Encryption refers to the process of converting data to an unrecognizable or "encrypted" form. A common use of encryption is to protect sensitive information, so that only authorized parties can view it.

(Continued)

	Blockchain encryption prevents sensitive information from getting into the wrong hands and being misused or forged. Thus, only authorized parties can view the information. Although various blockchains use different cryptography algorithms, the Bitcoin blockchain uses the SHA-256 algorithm, which produces a 32-byte hash that has proven resistant to hacking attempts to date.
Genesis block	Genesis block is the name of a blockchain's first block. It is the prototype of all other blocks in the blockchain as the common ancestor of them. If any block is followed the chain backward in time, it eventually leads to the genesis block.
Hard fork	A hard fork occurs when a cryptocurrency on a distributed ledger undergoes a protocol change resulting in a permanent diversion from the legacy or existing distributed ledger. This radical change to the protocol of a blockchain network makes previously invalid blocks/transactions valid or vice versa. Thus, a hard fork is a backward incompatible upgrade to the blockchain network.
Hashing	Hashing is a mathematical function that miners perform on blocks to make the network secure. It is a transaction's unique identifier.
Hash rate	Hash rate is the computational power that miners contribute to secure the network in exchange for block rewards and transaction fees.
Hot wallet	A hot wallet is an online portal that allows investors or merchants to access crypto holdings via an online platform or application.
Hybrid blockchain	A hybrid blockchain is a mix of public and private blockchains. It can host an application or service on an independent permissioned blockchain while leveraging a public blockchain for security and settlement.
Hybrid PoW (Proof of Work)/ PoS (Proof of Stake)	A hybrid PoW/PoS consensus mechanism uses elements of both PoW and PoS models when determining transaction validation rights.
Hyperledger	Hyperledger is an open source blockchain project designed to promote collective advancement of blockchain projects as opposed to disparate proprietary systems.
Immutability	Immutability is the inability of a block to be deleted or modified once it is in the blockchain.

(Continued)

Initial coin offering (ICO)	An ICO is a mechanism used to raise external funding through the emission of tokens in exchange for cryptocurrencies. It is often a form of crowdfunding, but a private ICO that does not seek public investment is also possible.
Interoperability	Interoperability refers to the exchange of data and information compatibly across varied complex systems.
InterPlanetary File System (IPFS)	IPFS is a protocol and P2P network for storing and sharing data in a distributed file system.
Lightning network	A lightning network is a series of off-chain payment channels where two people can conduct a very fast low-cost transaction or series of transactions, which are later settled on-chain. It adds another layer to Bitcoin's blockchain enabling users to create payment channels between any two parties on that extra layer.
Merkle (hash) tree and root	A Merkle tree or hash tree is a tree-like structure that organizes large amounts of data using hashes. It consists of raw data, leaves, and a root. In blockchain, a Merkle tree serves to encode data and to verify it as blockchain signatures (hashing) more efficiently and securely. A Merkle root is the hash of all the hashes of all the transactions that are part of a block in a blockchain network.
Miner	A miner is a node on the network that is actively involved in the consensus process used to verify transactions before these transactions are batched in blocks. Miners participate in performing the block verification process by determining whether each transaction is legitimate. Miners are incentivized to participate in this process with the ability to earn compensation from either confirming blocks as they are added to the blockchain or processing transactions.
Mining	Mining is the process of adding new transaction records to a block and verifying a block created by other miners. It allows nodes to reach a secure, tamper-resistant consensus. Miners collect transaction fees and are rewarded for their services.
Node	A node is any kind of device such as a computer, laptop, or server that connects to the blockchain network. It stores, spreads, and preserves the blockchain data. All nodes on a blockchain network are connected and constantly exchange the latest data with each other.

(Continued)

Nonce	A nonce, an abbreviation for "number only used once," is a pseudo-random number that is used as a counter during the mining process. It is a number added to a hashed or encrypted block in a blockchain that, when rehashed, meets the difficulty level restrictions. Thus, a nonce is the number that blockchain miners are trying to solve.
Off-chain transaction	Off-chain refers to a cryptocurrency transaction that happens outside of a main blockchain and is not published there.
On-chain transaction	On-chain refers to a cryptocurrency transaction that occurs on the blockchain.
Oracle	An oracle is a way for a blockchain or smart contract to interact with external data. As third-party services, blockchain oracles serve as bridges between blockchains and the outside world.
Orphan block	An orphan block is a validated block that is not accepted into the blockchain network due to a time lag in the acceptance of the block in question into the blockchain. For example, assume two blocks are validated at a similar time. Once one block gets accepted in the node, then the other block is discarded, which is an orphan block. Thus, an orphan block is a valid and verified block but have been rejected by the chain
Peer-to-peer (P2P)	In blockchain, a P2P network is one where peers can communicate and do transactions directly with other network members without having to rely on an intermediary or a third party to perform confirmations or other verification processes
Private (permissioned) blockchain	A private blockchain is closed and invitation-only such that specific users or entities on a blockchain have authorizing powers over others, allowing them to appoint members or validators. It has centralized authorities and is often deployed in the area of internal business operations.
Private key	A private key is a cryptography allowing a user access to his or her cryptocurrency or transaction. It is equivalent to a password and thereby helps to protect a user from theft and unauthorized access to funds.
Proof of Activity (PoA)	POA is another hybrid of PoW and PoS that attempts to combine the best features of both mechanisms.

(Continued)

Proof of Burn (PoB)	POB is an alternative consensus algorithm that tries to address the high energy consumption issue of a PoW system.
Proof of Capacity (PoC)	POC is a consensus mechanism that uses a process called plotting.
Programmatic Proof of Work (ProgPoW)	ProgPow is a blockchain protocol consensus algorithm designed to reduce the mining efficiency advantage of specialized hardware like ASIC miners over less-advanced machines like a standard CPU, meaning average individual crypto participants can mine coins.
Proof of Elapsed Time (PoET)	PoET is a consensus algorithm that prevents high resource utilization and keeps the process more efficient by following a fair lottery system. For example, each participating node in the network is required to wait for a randomly chosen time period, and the first one to complete the designated waiting time wins the new block. Each node in the blockchain network generates a random wait time and goes to sleep for that specified duration. The one with the shortest wait time commits a new block to the blockchain, broadcasting the necessary information to the whole peer network. The same process then repeats for the discovery of the next block.
Proof of Retrievability (PoR)	PoR is a compact proof by a file system (prover) to a client (verifier) that a target file is intact in the sense that the client can fully recover it.
Proof of Storage	Proof of Storage is a consensus protocol used primarily to verify the integrity of a remote file.
Proof of Work (PoW)	PoW is the original consensus algorithm in a blockchain network. In a PoW algorithm, the miners compete against each other to validate a block and the first miner who presents validation for a block gets rewarded. For example, a miner repeatedly inserts transaction data (block) and a random string of digits (nonce of block) into a hashing formula, until the miner finds a desirable outcome – the PoW. Other miners can verify the PoW by taking the alleged input string and applying it to the same formula to see if the outcome is what the initial minor presented. Some view PoW as a controversial consensus algorithm because of the electricity costs involved in performing the formula calculations.

(Continued)

Proof of Stake (PoS)	PoS is a consensus algorithm that asks users to prove ownership of a certain amount of currency that is their stake in the currency. PoS gives the miners who hold coins (e.g., bitcoin) the ability to mine or validate transactions. In other words, the power of mining is proportional to the amount of coins a miner owns. Thus, the PoS process rewards larger stakeholders in the network.
Public (permissionless) blockchain	A public or permissionless blockchain is a decentralized ledger that is accessible to any user. Users do not need permission from anyone on the network to perform certain actions such as joining the network, receiving/sending transaction data, and participating in the consensus process to determine what blocks get added to the chain.
Public key	A public key is a cryptographic code or address used to facilitate transactions between parties that allow users to receive cryptocurrencies in their accounts. It enables the agent to access specific information, comparable to an access code.
Record	A record is a combination of transactions.
SHA-256	SHA-256 stands for Secure Hash Algorithm 256-bit, and it is used for cryptographic security. SHA-256 generates an almost-unique 256-bit signature for a text. Bitcoin uses SHA-256 for mining and creating addresses.
Sidechain	A sidechain is a mechanism allowing tokens and other digital assets from one blockchain to be securely used in a separate blockchain and then be moved back to the original blockchain if needed.
Smart contract	A smart contract is computer code operationalized within blockchain that automatically moves digital assets according to prespecified rules. Thus, smart contracts are codes that are built into the software that enable automation of certain job tasks or processes.
Soft fork	A soft fork is a change to the bitcoin protocol that makes only previously valid blocks or transactions invalid.
Stablecoin	A stablecoin is a crypto asset that normally takes the form of a coin or token that is connected or supported by an underlying asset including currencies or basket of commodities. The basic goal of stablecoins is to aid in developing of an alternative financial system with currency units not dependent or controlled by a government or other centralized entity.

(Continued)

Stale block	A stale block is a block that is no longer part of the current best blockchain because it was overridden by a longer chain.
Tamper-resistant ledger	A tamper-resistant or immutable ledger is a record (data stored on the blockchain) that cannot be changed due to using of encryption and digital signatures.
Wallet	A wallet is the primary storage platform for crypto assets.