Association of International Certified Professional Accountants™

AICPA® CIMA®

Blockchain Universal Glossary

Note: This glossary was developed as a reference for all Association blockchain and digital assets related content. Terms that are incorporated in this document encompass those from the *AICPA blockchain CPE courses*, *the Digital Assets Practice Aid*, as well as the *Implications of the Use of Blockchain in SOC for Service Organization Examinations*. As those documents are updated or modified, this glossary will be updated accordingly.

Access control mechanism (access control). A control that allows only authorized persons, organizations, or nodes to participate and/or transact on a given blockchain network. Access control is one of the key differences between public and private blockchains.

Airdrop. An allocation of digital assets, to one or more blockchain addresses often done without any consideration from the receiving blockchain addresses. Entity's often employ airdrops as a method of generating awareness or interest in a digital asset and may impose certain criteria to receive or claim the airdropped digital assets.

Bad actor. Those participating in the digital asset ecosystem who may have illegal or fraudulent intentions.

Bitcoin. An example of a crypto asset. (see **crypto asset**)

Block. A collection of digital asset transactions to be recorded on a blockchain.

Blockchain technology. A technology that records a list of records, referred to as blocks, that are linked using cryptography. Each block contains a cryptographic hash of the previous block, a timestamp and transaction data.

Block explorer. Specialized software or web-based browser for searching and viewing details of transactions, blocks, and addresses.

Consensus mechanism. Defines the steps to achieve consensus (e.g., the agreement on the values recorded by the various participants in a blockchain) using a set of rules (protocols) or algorithms. (Also referred to as consensus algorithm or consensus protocol.)

Crypto asset. A type of digital asset that:

- functions as a medium of exchange and
- has all the following characteristics:
  - They are not issued by a jurisdictional authority (for example, a sovereign government).
  - They do not give rise to a contract between the holder and another party.
  - They are not considered a security under the Securities Act of 1933 or the Securities Exchange Act of 1934.

These characteristics are not all-inclusive, and other facts and circumstances may need to be considered. Examples of crypto assets meeting these characteristics include bitcoin, bitcoin cash and ether.

Cryptographic key (key). A string of bits used by a cryptographic algorithm to transform plain text into an encrypted message. Cryptographic key pairs are the public and private keys needed to decode and encode encrypted messages on a blockchain network.

- Private key. A cryptographic key that is privately held and is required to be used in conjunction with a public key to decipher encrypted messages.
- Public key. A cryptographic key that is available to anyone to encrypt messages intended for a recipient.

Cryptography. A technique to secure communication or data.

Digital asset. A digital record made using cryptography for verification and security purposes on a digital decentralized ledger (referred to as a blockchain). A digital asset is characterized by its ability to be used for a variety of purposes, including as a means of exchange, as a representation to provide or access goods or services, or as a financing vehicle, such as a security, among other uses.

Digital asset ecosystem. All entities participating or involved with digital assets. This may include entities engaged in various elements of the ecosystem, including development, maintenance, use (e.g., the purchase, sale, investment, trading, or exchange); custody or security (e.g., hot or cold wallet providers, qualified custodians, or other custodial services); or validation.

Digital signature. The combination of the private key, public key, message and hashing generates a digital signature. A digital signature is unique for every transaction and is a way to prove that the originator of the message has access to the private key.

Distributed ledger technology (DLT). A broad umbrella term covering all blockchain technology and variations of the technology that does not use blocks or blockchains. All blockchains are DLT, but not all DLT are blockchains.

Encryption. The process of encoding data in such a way to prevent unauthorized access.

Ethereum. A blockchain platform and smart contract platform upon which other applications may be built. Ether is the crypto asset that runs on Ethereum. (see crypto asset and blockchain technology)

Exchanges. Platforms for buying and selling digital assets, including crypto assets. (Also referred to as digital asset exchanges.)

Fiat currency. Generally accepted legal tender issued by a sovereign government (e.g., dollar, pound and euro).

Fork. A change to the consensus protocol.

- Hard fork. A fork that may not be backwards compatible with older versions of the consensus protocol, such that computers using the legacy consensus protocol will reject transactions created under the new consensus protocol.
- Soft fork. A fork that is backwards compatible with older versions of the consensus protocol, such that transactions created using the new consensus protocol are accepted by computers using a legacy consensus protocol.

Hashing. A process used to convert data into a string of numbers and letters.

Hybrid blockchain. A network with a combination of characteristics of public and private blockchains where a blockchain may incorporate select privacy, security and auditability elements required by the implementation. (see public blockchain and private blockchain)

Immutability. The characteristic of not being capable of or susceptible to change. In a blockchain network, this refers to the notion that certain features of blockchain technology prevent a transaction that has been previously validated from being subsequently modified or changed.

Key generation or key ceremony. The process to generate public and private keys. (see cryptographic key)

Key management risk. The risk that private keys are not properly secured or backed up, resulting in a loss of data or digital assets.

Node. A participant that downloads and maintains a full or partial copy of the blockchain, validates blocks and can relay transactions.

Off-chain transactions. Transactions recorded outside the underlying blockchain (e.g., transfers by third-party wallet service providers between their users that are not recorded on a public blockchain).

On-chain transactions. Transactions recorded on the underlying blockchain.

Peer-to-peer network. A decentralized network where participants have equal privileges and make certain resources directly available to other network participants.

Privacy coins. Blockchain digital asset with limited ability to determine the identities of the transacting parties by observing the blockchain.

Private blockchain (permissioned). A restricted access network controlled by an entity or group which is similar to a traditional centralized network.

Pseudo-anonymous. Used to describe the circumstance whereby, in blockchain environments, digital assets are exchanged between blockchain addresses, and specific names and identities of those parties transacting are not explicitly identified with those addresses.

Public address (blockchain address). A unique identifier which is used to record receipts of digital assets on a public blockchain. Blockchain addresses are derived from cryptographic manipulation (that is, hashing) of the public key and can be shared with anyone to receive messages.

Public blockchain (permissionless). An open network where participants can view, read and write data, and no one participant has control (e.g., Bitcoin, Ethereum).

Sharding. Using encryption techniques to split data.

Smart contracts. A digital code containing a set of rules under which the participants agree to interact with each other. If and when the predefined rules are met, the agreement is automatically enforced by the code. The smart contract code facilitates, verifies and enforces the performance of an agreement or transaction after which the results of the transaction are written in a blockchain.

Stablecoins. Digital assets that include mechanisms designed to minimize price volatility by linking their values (e.g., a "peg") to the value of another asset such as a fiat currency, a commodity, a digital asset or basket of assets. (see digital asset)

Validator. A participant in a blockchain network and component of a consensus mechanism responsible for validating transactions. For certain blockchains that use Proof of Work, validators are referred to as miners. (see consensus mechanism)

Wallet. A medium used to store private keys and their associated public keys or blockchain addresses, some of which allow participants to send transactions to the peer-to-peer network and receive digital assets from others. There are different types of wallets as follows:

- Cold storage wallet. A wallet that is not connected to the internet, also referred to as an offline wallet.
- Hardware wallet. A hardware (physical) device that generates private keys instead of software.
- Hot storage wallet. A wallet that is accessible to the internet. This is the most common implementation of a wallet, which may be referred to as just a wallet.
- Mobile wallet. A wallet that is accessed via a mobile app.
- Multisig (multisignature) wallet. A wallet that requires two or more signatures to transfer a digital asset from a wallet address.
- Physical wallet. Any medium used to store keys offline in physical form (e.g., paper wallet).
- Software wallet. Refers to anything other than a hardware or physical wallet.
- Third-party hosted wallet service. A third-party service provider who holds an entity's digital assets, also referred to as custodial wallet.