AICPA & CIMA

Together as the Association of International Certified Professional Accountants

Blockchain universal glossary

Note: This glossary was developed as a reference for all AICPA® & CIMA® blockchain and digital assets-related content. The terms in this document encompass those from the AICPA blockchain CPE courses, the Accounting for and Auditing of Digital Assets Practice Aid, the Implications of the Use of Blockchain in SOC for Service Organization Examinations, as well as the Blockchain Risk: Considerations for Professionals. This glossary will be updated accordingly as these documents are updated or modified.

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. Entities often employ airdrops to generate 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 be doing so in bad faith (for example, unethical, inappropriate, illegal, or fraudulent intentions).

bitcoin — An example of a crypto asset. (see crypto asset)

block — A collection of digital asset transactions recorded on a blockchain. (See blockchain technology)

blockchain protocol — The software that manifests the instructions for nodes on the network that will include instructions for the consensus mechanism (that is, the rules that define how data is exchanged and transmitted between the nodes). (See consensus mechanism)

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 sequential transaction data.

block depth — The number of blocks that have been added to the blockchain after the block in question. (See block)

block explorer — Specialized software or web-based browser tools for searching and viewing details of transactions, blocks, and addresses on public blockchains.

block height — The number of blocks added to the blockchain since the genesis block. (See genesis block)

block signer — A validator. (See validator)

block size — The allowable amount of data in one block. (See block)

block reward — The predetermined reward given to a miner after the miner has successfully added a transaction block to the blockchain.

block timestamps — Data stored in each block indicating the time the block was validated.

commingled public address — A public address that includes digital assets of multiple parties and does not represent a single entity's holdings.

consensus mechanism — Defines the steps to achieve consensus (for example, 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. The two most common consensus algorithms include the following:

- proof of stake — Only holders of the digital asset can validate transactions but must choose to do so.
- proof of work — Participants use computational power to solve a mathematical puzzle to validate transactions and append a new block to the blockchain.

crypto asset — A type of digital asset that:

- function as a medium of exchange and
- have 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.

crypto asset mining — The processes by which a validator adds blocks of transactions to a distributed ledger and earns a block reward and transaction fees in the form of the native crypto asset, typically for blockchain networks that use proof-of-work consensus mechanisms. (See validator; block reward; transaction fees; proof-of-work)

crypto asset staking — The process whereby a validator contributes a specified number of crypto assets for a period of time to the blockchain for a chance to earn the right to add blocks of transactions to a distributed ledger and earn a block reward and transaction fees in the form of the native crypto asset, typically for blockchain networks that use proof-of-stake consensus mechanisms. Some networks may use a variation of the proof-of-stake protocol that allows owners of crypto assets to delegate their stake to another party that acts as a validator. (See validator; block reward; transaction fees; proof-of-stake)

Note: We acknowledge that the term "staking" may sometimes refer to committing crypto assets to a smart contract for purposes other than supporting the integrity of the validation of transactions on a blockchain. For instance, crypto assets might be deposited to a decentralized finance protocol to provide the depositor an incentive reward for using the protocol. We exclude such activities for purposes of this definition.

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 sign/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 between two parties such that any third party is prevented from accessing or gaining any information about the 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 (for example, the purchase, sale, investment, trading, or exchange), custody or security (for example, hot or cold wallet providers, qualified custodians, or other custodial services), or validating.

digital signature — The combination of the public key, message, hashing, and the private key 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. A distributed ledger is a type of data store that spreads across multiple sites, countries, or institutions and in which records are stored sequentially in a continuous ledger. 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 public blockchain and smart contract platform upon which other applications may be built. Ether is the crypto asset that runs on Ethereum. (See crypto asset; blockchain technology).

fiat currency — Legal tender (that is, money that is legally valid for the payment of debts and that must be accepted for that purpose when offered) issued by a sovereign government (for example, U.S. dollar, pound, euro, eYuan)

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. In the instance of a contentious hard fork, this can create two versions of a blockchain network.
- 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.

fungible token — A token that is not unique.

gas — The fee that is required to process a transaction or execute a smart contract on the Ethereum blockchain. Senders could offer higher gas fees to accelerate transaction processing. Other blockchains may have a similar fee structure but may refer to the fee using a different term.

genesis block — The first block created in a blockchain.

hash collision attack — An attempt to find two inputs that create the same hash value for the purpose of compromising the data on a blockchain.

hash function — A function that can take a string of data and convert that data to a fixed size. Examples of has functions include SHA256 and MD5. Also referred to as hashing.

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; 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.

intermediary systems — Those systems between a blockchain and other systems.

key compromise protocol — Protocols that may include an inventory of keys, processes and procedures, knowledgeable personnel and authenticated communication channels to be executed for the mitigation of damages when an encryption key has or may have been compromised.

key generation or key ceremony — The process to generate public and private keys (key pairs).

key management lifecycle — The operations and controls necessary to securely create, maintain, protect, control, rotate, and retire cryptographic keys.

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

mempool transactions — Those transactions waiting to be confirmed.

mining pools — A group of miners that combine computational power or resources and work together to perform crypto asset mining, sharing the block reward and transaction fees. (See crypto asset mining; crypto asset staking)

multi-sig (multi-signature) — The requirement of more than one signature to authorize a transaction.

node — A participant that maintains a full or partial copy of the blockchain and may perform other functions.

non-fungible token — A token that is unique.

non-standard transactions — Transactions that are not aligned with the blockchain design or use case.

off-chain transactions — Transactions that are recorded outside the underlying blockchain (for example, transfers by third-party wallet service providers between their users that are not recorded on a blockchain).

on-chain transactions — Transactions that are recorded on the underlying blockchain.

oracle — An oracle provides a smart contract with information that does not natively reside on the same distributed ledger that the smart contract is developed on. This allows the smart contract to better fulfill a variety of use cases.

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

private blockchain (permissioned) — A restricted access network controlled by an entity or group which is like a traditional centralized network. A private blockchain requires a verification process for new participants. A private blockchain may also limit which individuals are able to participate in consensus of the blockchain network.

privacy coins — Digital assets that are transacted on a blockchain that have added privacy features to limit viewable transactional information of participating parties.

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 (for example, Bitcoin, Ethereum).

seed phrase — List of words used to gain access to a digital asset wallet, typically used as backup to a participant's password.

sharding — Using encryption techniques to split data (for example, a private key).

side chains — Secondary blockchain that is connected to the main blockchain that has its own consensus protocol.

signature operations — The process of signing a transaction to validate a transaction.

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 executed by the code.

stablecoins — Digital assets that include mechanisms designed to minimize price volatility by linking (or pegging) their values to the value of another asset such as a fiat currency, a commodity, a digital asset, or basket of assets. (See digital asset)

tokenization — The process of digitally representing something of value, whether physical or intangible, for use on a blockchain (that is, the creation of a token).

transaction fees — A fee charged to users of blockchain. Transaction fees are a key incentive to network participants to validate transactions on a network as part of its consensus mechanism. The incentive is different based upon the design of the consensus protocols.

unconfirmed transactions — Transactions that have not yet been processed and incorporated into the blockchain.

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; proof of work)

wallet — A medium used to store private keys and their associated public keys or blockchain addresses. There are different types of wallets, some of which allow participants to send transactions to the peer-to-peer network and receive digital assets from others as follows (categories are not mutually exclusive):

- cold storage wallet — A wallet that is not connected to the internet. Also referred to as an off-line wallet.
- hot storage wallet — A wallet that is accessible to the internet. Most common implementation of a wallet that may be referred to as just a "wallet."
- hardware wallet — A hardware device (physical device) that generates and stores private keys.
- software wallet — Refers to anything other than a hardware or physical wallet.
- multi-sig (multi-signature) wallet — A wallet that requires two or more signatures to authorize a digital asset transaction from a wallet address.
- third-party hosted wallet service — A third-party service provider who holds an entity's digital assets. Also referred to as a custodial wallet.