Blockchain glossary

Blockchain A type of distributed digital ledger to which data is recorded sequentially and permanently in ’blocks’. Each new block is linked to the immediately previous block with a cryptographic signature, forming a ‘chain’. This tamper-proof self-validation of the data allows transactions to be processed and recorded to the chain without recourse to a third party certification agent. The ledger is not hosted in one location or managed by a single owner, but is shared and accessed by anyone with the appropriate permissions – hence ‘distributed’.

Block A package of data containing multiple transactions over a given period of time.

Chain The cryptographic link that keeps blocks together using a ‘hash’ function.

Data mining The process of solving cryptographic problems using computer hardware to add newly hashed blocks to a public blockchain such as bitcoin. In fulfilling this function, successful data miners keep the blockchain actively recording transactions and, as an incentive, are awarded newly minted bitcoins for their trouble.

Ethereum A public blockchain system developed as an open-source project, its architecture running remotely on the Ethereum Virtual Machine. It uses ‘ethers’, a cryptocurrency, as its token and supports the storage and execution of ‘smart contracts’.

Hash The result of applying an algorithmic function to data in order to convert them into a random string of numbers and letters. This acts as a digital fingerprint of that data, allowing it to be locked in place within the blockchain.

Hyperledger An umbrella project set up by the Linux Foundation comprising various tools and systems for building open-source blockchains.

Node A copy of the ledger operated by a participant with a blockchain network.

Oracle A bridge from a blockchain to an external data source that allows a smart contract to complete its business by referencing timely real-world information. An oracle might allow a smart contract to access consumer energy usage, live train timetables, election results, and so on.

Peer-to-peer (P2P) The direct sharing of data between nodes on a network, as opposed to via a central server.

Permissioned ledger A large, distributed network using a native token, with access restricted to those with specific roles.

Private blockchain A closely controlled network operated by consortia in which the data is confidential and is accessed only by trusted members. Private blockchains do not require a toke

Private key	A unique string of data that represents proof of identification within the blockchain, including the right to access and own that participant's wallet within a cryptocurrency. It must be kept secret: it is effectively a personal password.
Proof of stake	The mechanism by which participants earn the right to add new blocks and so earn new tokens, based on how much of that currency they already hold.
Proof of work	Repeatedly running a hash function, the mechanism by which data miners win the right to add blocks to a bitcoin-style blockchain.
Public blockchain	A large distributed network using a native token (such as bitcoin), open to everyone to participate and maintain.
Public key	A unique string of data that identifies a participant within the blockchain. It can be shared publicly.
Smart contracts	Custom software logic that executes automated events when data is written to the blockchain according to rules specified in the contract.
Token	The means of exchange to give value to a transaction,; typically a native cryptocurrency. Some non-currency blockchain architectures can be tokenless.