

# Glossary of Terms

A comprehensive reference guide for navigating the digital asset ecosystem — 74 terms across eight categories.

mycryptoguides.com

## BLOCKCHAIN FUNDAMENTALS

- Blockchain**  
A distributed, append-only ledger composed of cryptographically linked blocks of transaction data. Each block contains a hash of the previous block, creating an immutable chain.
- Block**  
A container of transaction data. Each block includes a header (with metadata such as a timestamp, nonce, and previous block hash) and a body of validated transactions.
- Block Height**  
The sequential number of a block within a blockchain, measured from the genesis (first) block at height 0.
- Consensus Mechanism**  
The protocol by which all nodes in a decentralized network agree on a single version of truth. Common mechanisms include Proof of Work and Proof of Stake.
- Distributed Ledger (DLT)**  
An umbrella term for any database that is replicated, shared, and kept in sync across many nodes without a central administrator. **Blockchain is one specific type of DLT** — one that groups transactions into blocks and chains them together sequentially with cryptographic hashes. Not all DLTs are blockchains: systems like IOTA's Tangle or Hedera Hashgraph use a directed acyclic graph (DAG) instead of a linear chain, allowing transactions to be validated in parallel rather than one block at a time.
- Interoperability**  
The ability of distinct blockchains and DLTs — which may use entirely different consensus mechanisms or data structures — to communicate, verify each other's state, and move data or value between one another. Cross-chain bridges, atomic swaps, and messaging standards like IBC (Inter-Blockchain Communication) are common approaches, each with its own trust and security trade-offs.
- Genesis Block**  
The very first block in a blockchain, hardcoded into the protocol. Bitcoin's genesis block was mined by Satoshi Nakamoto on January 3, 2009.

- Hash / Hash Function**  
A cryptographic function that converts any input into a fixed-length alphanumeric string. Even a minor change to the input produces a completely different hash (avalanche effect).
- Immutability**  
The property of blockchain data that, once written and confirmed, cannot be altered or deleted without invalidating all subsequent blocks.

- Node**  
Any computer participating in a blockchain network by maintaining a copy of the ledger and/or validating transactions. Full nodes store the entire chain; light nodes store only headers.
- Merkle Tree**  
A binary tree of hashes used to efficiently summarize and verify all transactions in a block. The root hash (Merkle root) is stored in the block header.

## NETWORK & VALIDATION

- Decentralization**  
The distribution of control and data across many independent participants so no single entity can unilaterally alter the ledger or censor transactions.
- Finality**  
The point at which a transaction is considered permanently settled and irreversible. Probabilistic finality (Bitcoin) improves with each confirmation; absolute finality (some PoS chains) is immediate.
- Fork (Hard / Soft)**  
A change to blockchain rules. A soft fork is backward-compatible; a hard fork creates a permanent divergence, potentially splitting the chain into two (e.g., Bitcoin and Bitcoin Cash in 2017).
- Mempool**  
Short for 'memory pool.' The waiting area where unconfirmed transactions reside until miners or validators include them in a block.
- Mining**  
The Proof of Work process of competing to solve a computationally expensive puzzle to earn the right to add the next block and receive block rewards plus transaction fees.
- Proof of Work (PoW)**  
A consensus mechanism requiring nodes (miners) to expend computational energy to propose new blocks. Makes attacks prohibitively expensive. Used by Bitcoin.
- Proof of Stake (PoS)**  
A consensus mechanism where validators lock up (stake) collateral to earn block-proposal rights proportional to their stake. More energy-efficient than PoW. Used by Ethereum post-Merge.
- Validator**  
In Proof of Stake systems, a node that has staked collateral and is responsible for proposing and attesting to new blocks. Slashed (penalized) for dishonest behavior.
- 51% Attack**  
A scenario where a single entity controls the majority of a network's hash rate or stake, enabling double-spend attacks and transaction censorship.

## DIGITAL ASSETS & TOKENS

- Altcoin**  
Any cryptocurrency other than Bitcoin. The term is broad and includes everything from Ethereum to memecoins.
- Cryptocurrency**  
A digital currency secured by cryptography and operating on a decentralized network, enabling peer-to-peer value transfer without intermediaries.
- Digital Asset**  
A broad category encompassing any value-bearing item that exists in digital form and can be owned, transferred, or traded — including cryptocurrencies, tokens, NFTs, and stablecoins.
- ERC-20**  
The dominant token standard on Ethereum defining a common interface for fungible tokens, enabling seamless interoperability across wallets and decentralized applications.

- Fungibility**  
The property of an asset where each unit is interchangeable with any other unit of the same type (e.g., one BTC = any other BTC). Compare with NFTs, which are non-fungible.
- NFT (Non-Fungible Token)**  
A unique, indivisible token on a blockchain representing ownership of a distinct item — digital art, collectibles, in-game assets, real-world asset certificates, etc.
- Stablecoin**  
A token designed to maintain a stable value, typically pegged 1:1 to a fiat currency (e.g., USD). May be fiat-backed (USDC), crypto-collateralized (DAI), or algorithmic.
- Token**  
A digital asset issued on an existing blockchain (vs. a coin, which is native to its own chain). Tokens can represent utility, governance rights, ownership, or financial instruments.
- Utility Token**  
A token that grants access to a specific product, service, or ecosystem function — not primarily designed as an investment vehicle.
- Governance Token**  
A token that confers voting rights in a decentralized protocol, allowing holders to propose and vote on changes to the code, parameters, or treasury.

SMART CONTRACTS & DEFI

- Automated Market Maker (AMM)**  
A type of DEX protocol that uses algorithmic pricing formulas (e.g.,  $x * y = k$ ) and liquidity pools instead of order books to facilitate token swaps.
- Composability**  
The ability for smart contracts and DeFi protocols to interact with each other like financial 'Lego bricks,' enabling complex stacked applications without permission.
- Decentralized Exchange (DEX)**  
A non-custodial protocol enabling peer-to-peer token trading directly from users' wallets, without a centralized intermediary holding funds.
- Decentralized Finance (DeFi)**  
Financial services — lending, borrowing, trading, yield generation — built on public blockchains and governed by smart contracts rather than banks or brokers.
- Escrow (On-Chain)**  
A smart contract that holds funds and releases them automatically when predefined conditions are met, eliminating the need for a trusted third-party escrow agent.
- Liquidity Pool**  
A smart contract holding reserves of two or more tokens, funded by liquidity providers, enabling decentralized trading and earning fees for providers.
- Oracle**  
A middleware service that fetches real-world data (prices, weather, sports results) and delivers it on-chain in a tamper-resistant way for smart contracts to consume.
- Slippage**  
The difference between the expected and actual execution price of a trade, caused by low liquidity or market movement between order placement and execution.
- Smart Contract**  
Self-executing code deployed on a blockchain that automatically enforces the terms of an agreement when predefined conditions are met — no intermediary required.
- Yield Farming**  
The practice of strategically deploying assets across DeFi protocols to maximize returns from interest, fees, and incentive token rewards.

WALLETS & CUSTODY

- Cold Wallet / Cold Storage**  
A wallet whose private keys are never connected to the internet, providing maximum security against remote hacks. Hardware wallets and paper wallets are common forms.
- Custodial Wallet**  
A wallet where a third party (exchange or service) holds the private keys on behalf of the user. Convenient but introduces counterparty risk ('not your keys, not your coins').
- Hardware Wallet**  
A dedicated physical device (e.g., Ledger, Trezor) that stores private keys offline and signs transactions in a secure enclave, combining security with usability.
- Hot Wallet**  
A wallet connected to the internet, enabling fast access for frequent transactions. More convenient but more vulnerable to online attacks than cold storage.
- Multi-Signature (Multisig)**  
A security scheme requiring multiple private key holders to sign a transaction before it broadcasts, eliminating single points of failure for high-value wallets.
- Private Key**  
A secret 256-bit number that cryptographically proves ownership of blockchain assets and authorizes transactions. Must never be shared or lost.
- Public Key / Address**  
Derived from a private key via one-way cryptography, the public address is safe to share and acts as the destination for incoming funds.
- Seed Phrase (Recovery Phrase)**  
A human-readable sequence of 12 or 24 words (BIP-39 standard) from which all wallet keys are derived. The ultimate backup — must be stored offline and securely.
- Self-Custody**  
The practice of controlling your own private keys rather than delegating custody to an exchange or third party.

CROSS-BORDER & PAYMENTS

- Agentic Payments**  
Transactions initiated, negotiated, and executed autonomously by AI agents acting on a user's or business's behalf — authorizing purchases, subscriptions, or transfers within programmable spending limits. Digital assets and stablecoins are emerging as a preferred settlement rail for agentic payments because smart contracts can enforce spending rules and settle instantly, 24/7, without waiting on traditional banking rails or human approval at every step.
- CBDC (Central Bank Digital Currency)**  
A digital form of a nation's fiat currency issued directly by the central bank, combining the programmability of crypto with government backing.
- Correspondent Banking**  
The traditional system where banks hold accounts at other banks to facilitate international transfers — typically slow (2-5 days) and expensive (3-7% fees).
- Liquidity Bridge**

In cross-border crypto payments, a mechanism (like XRP's On-Demand Liquidity) that uses a digital asset as a bridge currency to settle between two fiat currencies in real time.

### On-Demand Liquidity (ODL)

Ripple's payment product using XRP as a real-time bridge asset so financial institutions can settle cross-border transactions without pre-funding nostro accounts.

### Nostro / Vostro Account

Pre-funded accounts banks maintain at foreign correspondent banks to enable international payments. They tie up billions in idle capital that blockchain solutions aim to eliminate.

### SWIFT

The Society for Worldwide Interbank Financial Telecommunication — the dominant messaging network for international bank transfers, processing trillions in daily volume but often slowly.

### Settlement Finality

The irreversible completion of a payment transfer. Blockchain-based settlements can achieve finality in seconds vs. days in traditional correspondent banking.

### Stellar (XLM)

An open-source blockchain network optimized for fast, low-cost cross-border payments and asset issuance, used by financial institutions for remittances.

## ORACLES & DATA

---

### Data Feed

A continuous stream of off-chain information (e.g., BTC/USD price) published on-chain by an oracle network for smart contracts to reference.

### Decentralized Oracle Network (DON)

A network of independent oracle nodes that aggregate data from multiple sources, reaching consensus before delivering it on-chain to prevent single points of failure.

### Hybrid Smart Contract

A smart contract that combines on-chain logic with off-chain data via oracles, enabling complex real-world applications like parametric insurance or derivatives.

### LINK (Chainlink)

The native token of the Chainlink network, used to pay oracle node operators for data delivery services and to stake as collateral ensuring data integrity.

### Off-Chain Data

Information that originates outside a blockchain (prices, weather, sports scores, IoT sensor readings) and must be bridged on-chain via oracles for smart contracts to use.

### Price Feed

A specific type of oracle data feed providing asset prices, aggregated from multiple exchanges and data providers to resist manipulation.

### Sybil Resistance

A property of oracle networks preventing a single actor from creating many fake identities to manipulate the data consensus.

### The Oracle Problem

The fundamental challenge that blockchains cannot natively access external data — smart contracts are deterministic systems that can only read what's already on-chain.

### VRF (Verifiable Random Function)

A cryptographic oracle service (provided by Chainlink VRF) that generates provably fair and tamper-proof random numbers for on-chain use cases like NFT minting or gaming.

## STORE OF VALUE

---

### Bitcoin (BTC)

The first and largest cryptocurrency by market cap, designed as a scarce, decentralized digital store of value with a fixed supply of 21 million coins.

### Digital Gold

A metaphor comparing Bitcoin's properties — scarcity, durability, portability, divisibility, and resistance to censorship — to physical gold as a monetary store of value.

### Halving

A programmed event (approximately every 4 years for Bitcoin) that cuts the block subsidy reward in half, reducing the rate of new supply issuance and historically catalyzing price appreciation.

### Inflation Hedge

An asset whose value is expected to maintain or grow purchasing power as fiat currencies inflate. Bitcoin's fixed supply makes it a candidate for this role.

### Scarcity

The property of having a limited supply. Bitcoin's 21 million coin cap, enforced by code, creates digital scarcity analogous to precious metals.

### Sound Money

Money that cannot be arbitrarily inflated by any authority, maintains purchasing power over time, and serves reliably as a medium of exchange, unit of account, and store of value.

### Stock-to-Flow (S2F)

A model measuring scarcity by dividing existing supply (stock) by annual new production (flow). Bitcoin's S2F ratio approaches gold's after each halving.