Course Glossary

Table of contents

This glossary defines key terms used in the course slides. The web version links each term to its first substantive appearance in the slides.

2

2008 financial crisis. The global financial disruption that weakened confidence in banks, financial governance, and centralized risk management. Aliases: 2008 Global Financial Crisis, financial crisis, global financial crisis.

Source: 03-IN - Framing.

21 million cap. Bitcoin's approximate maximum total supply limit of 21 million bitcoin. Aliases: 21 million cap (Bitcoin), 21M cap, hard cap, supply cap.

Source: 01-BF - Monetary Policy.

5

51% attack. An attack where a participant or coalition gains enough consensus power to manipulate accepted history or disrupt normal confirmation. Aliases: 51 percent attack, 51% attack (Bitcoin), 51% attack (blockchain

consensus), 51% attack (proof of work), majority attack, majority hash attack, majority hash power attack.

Source: 03-IN - Why This History Matters.

A

ABI encoding. The Ethereum convention for packing function arguments, return values, and event data into byte sequences. Aliases: ABI encoding (Ethereum), ABI-encoded, encoded arguments.

Source: 04-EF - ABI, Encoding, and Function Selectors.

Access control. Rules that determine who may read data, propose transactions, endorse updates, order entries, or administer the ledger. Aliases: Access control (distributed ledgers), Access control (smart contracts), access-control policy, authorization logic, authorization policy.

Source: 04-DS - Transparency vs. Privacy.

Access list. An optional transaction field that predeclares accounts or storage slots a transaction expects to access. Aliases: Access list (Ethereum transaction), access lists.

Source: 03-EF - Transactions: Structure and Flow.

Access policy. Rules that determine which participants may read, write, submit, approve, or administer specific resources. Aliases: access control policy.

Source: 01-PC - Key Components.

Account model. A ledger model, used by systems such as Ethereum, that tracks mutable account balances instead of discrete spendable outputs. Aliases: Account model (blockchain), Account-centric model (smart contracts), account model, account-based model.

Source: 02-BF - Why the UTXO Model?.

Account model (Ethereum). An accounting and execution model where balances, code, and storage are attached to accounts and updated directly. Aliases: Account model (Ethereum accounting), Account model (Ethereum transaction model), Ethereum Account Model, Ethereum accounts, account-based model, accounts.

Source: 01-EF - Transaction Models: UTXO vs Accounts.

Accuracy. The degree to which reputation scores correlate with actual future peer behavior. Aliases: Accuracy (reputation systems).

Source: 03-DS - Properties of Reputation Systems.

Acknowledgment. A message confirming that another message was received. Aliases: ACK, Acknowledgment (network protocol), acknowledgment, acknowledgments.

Source: 05-IN - Omission Faults.

Activation queue. The waiting process a staked node passes through before becoming an active validator. Aliases: Activation queue (PoS validator lifecycle), activation epoch.

Source: 03-CM - Proof of Stake: The Full Lifecycle.

addr message. A Bitcoin network message that advertises known peer addresses to other nodes. Aliases: addr message (Bitcoin protocol), address message, addrv2 message.

Source: 03-BF - Gossip and Peer Connections.

Address (Bitcoin). A user-facing encoding of spending conditions, typically derived from public-key material, where value can be locked. Aliases: Bitcoin address.

Source: 02-BF - Wallets, Addresses, and Keys.

Address (Ethereum). A 20-byte account identifier used to refer to EOAs, contract accounts, owners, recipients, and callers. Aliases: address.

Source: 04-EF - Types: Value Types.

Address Clustering. The process of grouping addresses or outputs that likely belong to the same actor based on transaction evidence and heuristics. Aliases: Address Clustering (blockchain forensics), Address clustering (forensics), address cluster analysis, clustering, wallet clustering.

Source: 02-FO - Address Clustering.

Address format. A user-facing encoding style for Bitcoin addresses, such as legacy addresses beginning with 1 or SegWit forms such as 3 or bc1. Aliases: Address format (Bitcoin), Base58, Bech32, SegWit address, legacy address.

Source: 02-BF - Where Addresses Come From.

Address freeze. An issuer-controlled function that prevents specified blockchain addresses from moving a stablecoin token. Aliases: Address freeze (stablecoin), blacklist, blacklisting, freeze capability.

Source: 02-AS - Trust Architecture: The Stablecoin Hybrid.

Address gossip. The exchange of known peer addresses among connected Bitcoin nodes. Aliases: Address gossip (Bitcoin network), address relay, peer address gossip.

Source: 03-BF - Joining the Bitcoin Network.

Address payable. A Solidity address type that is allowed to receive ETH through value-transfer operations. Aliases: Address payable (Solidity), address payable, payable address.

Source: 04-EF - Types: Value Types.

Address reuse. The practice of using the same Bitcoin address for multiple transactions, which can leak information about ownership and activity. Aliases: Address reuse (Bitcoin).

Source: 02-BF - What Are Wallets?.

Address zero. A special all-zero Ethereum address commonly used in token events to signal minting or burning rather than transfer from a normal owner. Aliases: 0x0, Address zero (Ethereum), zero address.

Source: 06-EF - What Is Minting?.

Admin certificate. A credential that authenticates administrative authority for managing a Fabric organization or network component. Aliases: Admin certificate (Hyperledger Fabric), admin certificates, administrator certificate.

Source: 01-PC - Case Study: Fabric Lockout.

Administrator. A role with authority to manage configuration, membership, or other network control-plane settings. Aliases: Administrator (permissioned ledger role), admin, network administrator.

Source: 01-PC - Roles and Duties.

Admissibility. Whether evidence can be accepted and relied on in formal legal proceedings. Aliases: Admissibility (legal evidence), court-admissible evidence, legal admissibility.

Source: 02-FO - Attribution: Standards of Evidence and Known Pitfalls.

Admission control. The process for deciding who may join or act in the network before they receive credentials or roles. Aliases: Admission control (permissioned ledger), access admission, membership admission.

Source: 01-PC - What Changes.

Adoption friction. The combined technical, institutional, economic, and user-level barriers that prevent blockchain from spreading broadly. Aliases: Adoption friction (blockchain), accumulated friction, barriers to adoption.

Source: 05-AS - The Real Question.

Adversary. A modeled opponent who may try to read, alter, forge, replay, or otherwise break a cryptographic system. Aliases: attacker.

Source: 01-CP - What Is Cryptography?.

Adversary assumption. The protocol assumption about what faulty or malicious participants are able and willing to do. Aliases: Adversary assumption (consensus), adversary model.

Source: 01-CM - Crash-Fault Tolerance (CFT).

Adverse Selection. A market outcome where hidden information causes lower-quality or riskier participants to dominate.

Source: 04-IN - The "Market for Lemons": When Trust Breaks Down.

AES. A widely used symmetric block cipher standard for encrypting fixed-size blocks with a secret key. Aliases: AES (symmetric cipher), Advanced Encryption Standard.

Source: 03-CP - What Is Symmetric Cryptography?.

Agreement. The guarantee that correct participants converge on the same chosen value or ledger result. Aliases: Agreement (consensus property), Agreement (consensus), consistency.

Source: 01-CM - Foundations of Consensus.

AI error at scale. A failure mode where brittle, hallucinated, or overconfident AI output causes widespread damage when trusted in automated systems. Aliases: AI error at scale (blockchain automation), AI errors at scale.

Source: 05-AS - Risks.

AI-driven exploit. An attack where AI helps discover, prioritize, or execute weaknesses in contracts, wallets, protocols, or public code. Aliases: AI-driven exploit (blockchain security), AI-driven exploits.

Source: 05-AS - Risks.

Algorithm deprecation. The process of retiring an algorithm from trusted use because its security margin or standard status is no longer adequate. Aliases: Algorithm deprecation (cryptography), cryptographic deprecation, deprecated algorithm.

Source: 05-CP - Cryptographic Assumptions Decay Over Time.

Algorithmic design failure. A collapse caused by automated economic or protocol mechanisms that fail under real market pressure. Aliases: Algorithmic design failure (crypto markets), algorithmic failure.

Source: 05-AS - When Blockchain Systems Broke.

Algorithmic stablecoin. A stablecoin design that attempts to maintain its peg through supply adjustments rather than full collateral backing. Aliases: algorithmic.

Source: 02-AS - Stablecoins: Types and Mechanisms.

Ali Baba cave protocol. A teaching analogy where repeated random challenges convince a verifier that a prover knows a secret without revealing it. Aliases: Ali Baba cave, cave protocol.

Source: 05-CP - Ali Baba Cave: The Protocol.

Allowance. A token permission that lets one address or contract spend a limited amount of another address's fungible token balance. Aliases: Allowance (fungible token), allowances, spending allowance, spending allowances.

Source: 05-EF - Fungible vs Non-Fungible — Design Implications.

Allowlist. A preapproved set of addresses allowed to mint during a special window or under special launch rules. Aliases: Allowlist (NFT mint), Allowlist (minting), allow list, allowlists, pre-approved list, preapproved addresses, whitelist.

Source: 05-EF - Minting and Market Design Patterns.

Amount Correlation. Linking possible source and destination flows by comparing amounts after accounting for fees or conversions. Aliases: Amount Correlation (mixer investigations), amount matching, value correlation.

Source: 02-FO - Breaking Mixers: Investigative Countermeasures.

Announce-request-transmit pattern. A relay sequence where a node advertises data, a peer requests it, and the node then sends the full item. Aliases: Announce-request-transmit pattern (Bitcoin relay), announce-request-transmit, inv-getdata relay.

Source: 03-BF - Transaction Relay.

Anomaly detection. A monitoring technique that flags sudden behavior changes that may indicate reputation exploitation. Aliases: Anomaly detection (trust systems).

Source: 03-DS - Threats: On–Off (Reputation Milking).

Anonymity. The condition of acting without linking an action or transaction to an identifiable person. Aliases: anonymous.

Source: 03-IN - The Cypherpunk Movement.

Anonymity layer. A network routing tool or service that obscures a user's real network address from the peers they contact. Aliases: Anonymity layer (network privacy), anonymity network, privacy routing layer.

Source: 04-BF - Mitigating Network Deanonymization.

Anonymity Set. The group of plausible participants among whom a user's action is hidden. Aliases: Anonymity Set (privacy), candidate set.

Source: 02-FO - Counter-Heuristic #1: CoinJoin.

Anti-Money Laundering. Risk-based controls for monitoring, recordkeeping, sanctions screening, suspicious-activity review, and required reporting. Aliases: AML, AML controls, Anti-Money Laundering (crypto compliance).

Source: 04-BF - Off-Chain Controls: KYC and AML.

ApeCoin. A separate ERC-20 governance and utility token used for ApeCoin DAO voting rather than direct BAYC NFT ownership. Aliases: APE, ApeCoin (BAYC ecosystem), ApeCoin DAO.

Source: 06-EF - Case Study: Bored Ape Yacht Club.

Append-only. A record design where new entries are added to the end and past entries are not silently edited in place. Aliases: append-only history, append-only record.

Source: 04-DS - From Logs to Ledgers.

Append-only ledger. A record structure where new entries can be added but past entries are not silently edited or deleted. Aliases: Append-only ledger (Bitcoin), append-only database, global append-only ledger.

Source: 02-IN - What is a Blockchain?.

Append-only shared ledger. A shared record where new entries are added without silently overwriting prior history. Aliases: append-only ledger, append-only shared record.

Source: 01-PC - Why Not A Shared Database?.

Append-only state machine. A model of Ethereum where valid transactions advance a shared global state and accepted history is extended rather than rewritten. Aliases: Append-only state machine (Ethereum), global state machine, shared state machine.

Source: 02-EF - The Ethereum Operational Framework.

Application Binary Interface. The byte-level interface that specifies how callers encode function calls, return values, and event data for a contract. Aliases: ABI, Application Binary Interface (Ethereum).

Source: 04-EF - ABI, Encoding, and Function Selectors.

Approval. A permission that lets another address or contract transfer a user's token under defined rules. Aliases: Approval (token permission), approvals, operator approval, over-broad approvals.

Source: 05-EF - Common Pitfalls in NFT Projects.

Approximate Value Match. A cross-chain comparison that links flows by similar economic value while allowing for fees, price movement, and conversion differences. Aliases: Approximate Value Match (cross-chain forensics), approximate amount match, value match.

Source: 02-FO - Following the Hop: Cross-Chain Forensics.

Arbitrage. An MEV strategy that profits from price differences for the same asset across venues such as decentralized exchanges. Aliases: Arbitrage (MEV).

Source: 03-EF - The Mempool.

Archive mode. A storage mode that retains historical state for each block instead of only the current working state. Aliases: Archive mode (Ethereum), archive sync.

Source: 03-EF - Sync Modes & Data Availability.

Archive node. A full Ethereum node that also retains historical state for past blocks. Aliases: Archive node (Ethereum), archive mode node.

Source: 03-EF - Nodes and Clients.

ARIP. Nigeria's program for onboarding virtual asset service providers into a more formal regulatory process. Aliases: Accelerated Regulatory Incubation Program.

Source: 03-AS - Sub-Saharan Africa: Impact Signals.

Array. An ordered collection of values that may have fixed or dynamic length. Aliases: Array (Solidity), arrays, dynamic array, fixed-size array.

Source: 04-EF - Types: Reference Types.

Artificial Intelligence. Automated systems that analyze data, find patterns, and make or support decisions at scale. Aliases: AI, Artificial Intelligence (blockchain future).

Source: 05-AS - Two Powerful Technologies Collide.

Arweave. A storage protocol used for content-addressed token metadata or media with paid permanence assumptions. Aliases: Arweave (token metadata storage), Arweave TX ID.

Source: 06-EF - Metadata, IPFS, and the Pointer Problem.

ASIC. Specialized hardware built to perform mining computations far more efficiently than general-purpose devices. Aliases: ASIC (mining hardware), Application-Specific Integrated Circuit, purpose-built ASIC.

Source: 02-CM - Hardware Evolution and Centralization Pressures.

ASIC concentration. The concentration of mining power among operators with specialized application-specific mining hardware. Aliases: ASIC centralization, ASIC concentration (mining), specialized hardware concentration.

Source: 04-BF - Bitcoin Gold 51% Attack Discovery.

ASIC miner. Specialized mining hardware designed to compute Bitcoin's SHA-256 hashes far faster and more efficiently than general-purpose devices. Aliases: ASIC, ASIC miner (Bitcoin), application-specific integrated circuit.

Source: 02-BF - Evolution of Mining Hardware.

Asset swap. A token trade, often executed through smart contracts rather than a traditional intermediary. Aliases: Asset swap (DeFi), swap, swap assets, swapping.

Source: 01-AS - What Users Actually Do.

Asset-backed token. A token whose meaning depends on a referenced off-chain asset, custodian, receipt, or legal structure. Aliases: asset-backed tokens, reference token, reference tokens.

Source: 05-EF - A Taxonomy of Digital Assets.

Associated data. Metadata or headers that are authenticated by an AEAD scheme but intentionally left unencrypted. Aliases: AAD, additional authenticated data.

Source: 03-CP - From Confidentiality to Authenticated Encryption (AEAD).

Asymmetric cryptography. A cryptographic model that uses a mathematically linked public key and private key for different operations. Aliases: public key cryptography, public-key cryptography.

Source: 04-CP - The Locked Mailbox Analogy.

Asymmetric difficulty. The property that producing valid proof-of-work is expensive while checking it is cheap. Aliases: Asymmetric difficulty (Proof-of-Work).

Source: 01-CM - Nakamoto (Proof-of-Work) Consensus.

Asynchronous system. A distributed system with no known upper bound on message or processing delay. Aliases: asynchrony, fully asynchronous system.

Source: 01-CM - Timing Models on a Spectrum.

Atomic swap. A cross-chain trade designed so both sides complete or both sides refund without requiring a trusted middleman. Aliases: Atomic Swap (cross-chain trading), Atomic swap (cross-chain), atomic swaps.

Source: 01-FO - Bridges & Swaps: Crossing the Chain Boundary (cont.).

Attack surface. The set of roles, services, credentials, and processes attackers can target to influence or disrupt the network. Aliases: Attack surface (permissioned governance), Attack surface (smart contracts), system attack surface.

Source: 01-PC - Governance Boundary.

Attestation (Ethereum). A validator vote that supports blocks or checkpoints in Ethereum's Proof-of-Stake consensus process. Aliases: Attestation (Ethereum PoS vote), Attestation (Ethereum PoS), attest, attestations, validator attestation, validator vote.

Source: 01-EF - PoW vs PoS: Security Model (Review).

Attestation (Proof of Stake). A stake-weighted validator vote about a block, chain head, or checkpoint relationship. Aliases: Attestation (PoS vote), Attestation (Proof of Stake vote), attest, attestations, validator vote.

Source: 03-CM - The Committee: Attestation and Validation.

Attestation weight. The total validator voting power represented by attestations supporting a block or branch. Aliases: Attestation weight (Ethereum), attested stake weight, stake-weighted votes.

Source: 02-EF - The Ethereum Operational Framework.

Attester. A validator assigned to vote on block validity, chain head, or checkpoint relationships. Aliases: Attester (Ethereum PoS role), attesters, committee attester.

Source: 02-EF - The Ethereum Operational Framework.

Attribution. Linking observed blockchain activity to a real-world actor, organization, infrastructure owner, or operation. Aliases: Attribution (blockchain forensics), actor attribution, entity attribution, identity attribution, real-world attribution.

Source: 01-FO - Future of Forensics: AI-Powered Attribution.

Attribution uncertainty. The remaining doubt when a transaction trace points to an address or cluster but not yet to a confirmed real-world actor. Aliases: Attribution uncertainty (blockchain forensics), attribution risk.

Source: 01-FO - Challenges in Forensic Analysis.

Audit-visible metadata. Information visible enough for auditing while the underlying sensitive payload remains restricted. Aliases: audit metadata, restricted payload metadata.

Source: 01-PC - Privacy.

Auditability. The ability to inspect evidence that records or transactions followed expected rules and were not silently altered. Aliases: Auditability (blockchain use cases), Auditability (distributed ledgers), audit trail, auditable history, auditable record, public auditability.

Source: 04-DS - Case Study B — Public Sector: EBSI & Estonia (KSI){.smaller}.

Audited cryptographic library. A cryptographic implementation reviewed and maintained so applications can rely on safe defaults instead of custom security code. Aliases: OpenSSL, audited libraries, libsodium.

Source: 05-CP - When Good Crypto Goes Bad: Milk Sad (CVE-2023-39910).

Auditor / observer. A role that reviews history or compliance without directly controlling transaction submission or approval. Aliases: Auditor / observer (permissioned ledger role), audit-only participant, auditor, observer.

Source: 01-PC - Roles and Duties.

Austrian Economics. An economic framework that favors hard money, limited intervention, and the liquidation of malinvestment after credit booms.

Source: 04-IN - The Ideological Divide: Austrian vs. Keynesian Economics.

Authenticated encryption with associated data. An encryption design that provides confidentiality, integrity, and authentication in one API while allowing some data to be authenticated but not encrypted. Aliases: AEAD, authenticated encryption.

Source: 03-CP - From Confidentiality to Authenticated Encryption (AEAD).

Authentication path. The ordered list of sibling hashes needed to recompute a Merkle root from a target item. Aliases: Authentication path (Merkle proof), path.

Source: 02-CP - Merkle Proofs (Membership).

Authenticity. A security property that supports checking whether data or a message came from the claimed source. Aliases: authentication.

Source: 01-CP - What Is Cryptography?.

Authorization. The application's decision to grant a role, resource, or session after successful ownership or identity verification. Aliases: Authorization (token gating), access authorization.

Source: 06-EF - Token Gating: Access Flow.

Automated large-scale attack. An attack that uses automation to probe many contracts, protocols, wallets, or users at once. Aliases: Automated large-scale attack (blockchain security), automated attack, large-scale automated attack.

Source: 05-AS - Risks.

Automated market maker. A DEX mechanism where smart contracts price swaps from token reserves instead of matching buyers and sellers through an order book. Aliases: AMM, AMMs.

Source: 01-FO - Decentralized Exchanges (DEXs).

Automated provenance extraction. The automated parsing of on-chain events to recover asset type, amount, source chain, destination chain, and related movement history. Aliases: Automated provenance extraction (blockchain forensics), provenance extraction.

Source: 01-FO - Future of Forensics: Automated Cross-Chain Tracing.

Autonomous economic agent. A software system that evaluates conditions and executes economic actions, such as on-chain transactions, without continuous human direction. Aliases: autonomous economic agents, software agent.

Source: 05-AS - Opportunities.

Autonomous system. A routing domain on the Internet, usually controlled by one organization, that announces paths for reaching networks. Aliases: AS, ASN, Autonomous system (Internet routing), autonomous system number.

Source: 04-BF - Partitioning Attacks.

Autonomy. A design priority favoring user control, censorship resistance, self-custody, permissionless access, and auditability. Aliases: Autonomy (monetary system design).

Source: 04-IN - Design Trade-Offs: Efficiency vs. Autonomy.

Availability. The fraction of time a service is operational during the period users need it. Aliases: Availability (distributed systems), uptime.

Source: 01-DS - Availability, MTTF, and MTTR.

Avalanche effect. The property that a tiny input change causes a large and unpredictable change in the hash output. Aliases: avalanche, avalanche behavior.

Source: 02-CP - Hash Function Properties.

B

b-money. Wei Dai's proposed decentralized money design that anticipated distributed accounting but did not become an operational consensus system. Aliases: b money.

Source: 01-BF - Lessons from Precursors.

Balance attack. A network-layer attack that partitions or delays validators so competing branches gain roughly balanced attestation weight. Aliases: Balance attack (Ethereum PoS), balancing attack.

Source: 02-EF - Balance Attack.

Balance-transfer invariant. The accounting rule that a valid transfer subtracts from one balance and adds to another without creating or losing units unexpectedly. Aliases: Balance-transfer invariant (token contract), conservation of balances.

Source: 04-EF - Example: Coin (Code, Part 2).

Ballot stuffing. A manipulation tactic where fake or coordinated accounts give each other high ratings to inflate reputation scores. Aliases: Ballot stuffing (reputation attack), rating inflation, vote flooding.

Source: 03-DS - PeerTrust: Handling Manipulation.

Bandwidth. The finite data-carrying capacity of network links, shared unevenly across participants. Aliases: Bandwidth (distributed systems), throughput.

Source: 01-DS - Fallacy #3: Bandwidth Is Infinite.

Bank for International Settlements. An international institution described as the central bank for central banks that promotes cooperation among monetary authorities. Aliases: BIS.

Source: 04-IN - The Modern Financial Architect: Central Banks.

Bank Secrecy Act. A U.S. financial-crime law framework requiring covered businesses to maintain records and help detect illicit finance. Aliases: BSA, Bank Secrecy Act (United States).

Source: 04-BF - Off-Chain Controls: KYC and AML.

Base fee. The protocol-determined part of an Ethereum transaction fee that is burned under EIP-1559. Aliases: Base fee (EIP-1559), Base fee (Ethereum fee market), Base fee (Ethereum gas), base-fee burn, base_fee, burned base fee.

Source: 01-EF - Gas: Metering Computation and Storage.

Basis vector. A vector used with others to generate the points of a lattice. Aliases: Basis vector (lattice cryptography), basis vectors.

Source: 05-CP - Lattices: Intuition Without the Math.

Beacon block. The outer consensus-layer block container that validators propose and attest to in post-Merge Ethereum. Aliases: Beacon block (Ethereum consensus layer), Beacon block (Ethereum), beacon blocks.

Source: 02-EF - Beacon Blocks and Execution Payloads.

Beacon Chain. Ethereum's proof-of-stake consensus chain that coordinates validators, fork choice, and finality. Aliases: Beacon Chain (Ethereum), beacon chain.

Source: 03-EF - Two Networks, One Chain.

Beneficial owner. The real person who ultimately owns or controls an account, customer, or legal entity. Aliases: Beneficial owner (KYC), UBO, ultimate beneficial owner.

Source: 04-BF - Off-Chain Controls: KYC and AML.

Best-effort propagation. A message-spreading model where nodes try to relay information but delivery, ordering, and timing are not guaranteed. Aliases: Best-effort propagation (blockchain), best-effort delivery, best-effort transport.

Source: 01-DS - Fallacy #1: The Network Is Reliable.

BGP hijack. An Internet routing attack where traffic is redirected by falsely announcing network paths. Aliases: Border Gateway Protocol hijack, route hijack.

Source: 04-BF - Partitioning Attacks.

Bias. A systematic tendency that shapes what a source notices, values, highlights, or omits. Aliases: Bias (information evaluation), biases, source bias.

Source: 01-AS - Reading Critically.

Binding. The property that it should be infeasible to open one commitment as two different underlying messages. Aliases: Binding (commitment), binding commitment.

Source: 02-CP - Hashing as Commitment.

Birthday paradox. The principle that collisions among random-looking hash outputs become likely after about 2^(n/2) trials for an n-bit digest. Aliases: Birthday paradox (hashing), birthday attack, birthday bound.

Source: 02-CP - Math Spotlight: Birthday Paradox and Work Factors.

Bit gold. Nick Szabo's proposed work-based digital money concept that helped frame scarcity through costly computation. Aliases: bit gold.

Source: 01-BF - Lessons from Precursors.

Bit string. A sequence of 0s and 1s used as the standard representation of digital inputs, outputs, keys, and messages. Aliases: bit strings.

Source: 01-CP - Sets and Functions.

Bitcoin. The first widely adopted blockchain system and a reference point for understanding how blockchain designs became visible to the public. Aliases: Bitcoin (blockchain platform), Bitcoin (historical synthesis), Bitcoin (monetary alternative), Bitcoin (permissionless digital cash system), Bitcoin (technical system), Bitcoin network, bitcoin.

Source: 01-IN - Why A Blockchain Course?.

Bitcoin Core. The open-source reference implementation commonly used to operate a full Bitcoin node.

Source: 03-BF - Setting Up a Full Node.

Bitcoin fork. A chain derived from Bitcoin's code or history that follows different rules or community choices after a split. Aliases: Bitcoin-derived chain, forked chain.

Source: 04-BF - Bitcoin Gold 51% Attack Discovery.

Bitcoin Gold. A 2017 fork of Bitcoin that changed its mining algorithm but kept far less hash rate and economic scale than Bitcoin. Aliases: BTG.

Source: 04-BF - Bitcoin Gold 51% Attack Discovery.

Bitcoin ledger. Bitcoin's public permissionless record of payments, authorized by digital signatures and validated by nodes following common rules. Aliases: Bitcoin's ledger.

Source: 04-DS - Case Study C — Bitcoin Ledger (Permissionless).

Bitcoin overflow bug. A 2010 Bitcoin implementation flaw that allowed a transaction in block 74638 to create about 184 billion BTC. Aliases: 2010 overflow bug, block 74638 overflow bug.

Source: 04-BF - Bitcoin Overflow Bug.

Bitcoin peer-to-peer network. The decentralized network of Bitcoin nodes that connect directly to relay transactions, blocks, and peer information without a central server. Aliases: Bitcoin P2P network.

Source: 03-BF - Bitcoin's Peer-to-Peer Network.

Bitcoin Pizza Day. The May 22, 2010 purchase in which Laszlo Hanyecz paid 10,000 BTC for two pizzas, creating an early real-world price signal. Aliases: 10,000 BTC pizza, pizza purchase.

Source: 01-BF - The 10,000 BTC Pizza.

Bitcoin protocol message. A structured message exchanged between Bitcoin nodes over long-lived TCP connections. Aliases: P2P message.

Source: 03-BF - Communication Protocol Basics.

Bitcoin Script. Bitcoin's stack-based scripting language for defining and validating the conditions required to spend transaction outputs. Aliases: Script.

Source: 03-BF - Introduction to Bitcoin Script.

Bitcoin whitepaper. The 2008 proposal by Satoshi Nakamoto for peer-to-peer electronic cash that does not depend on trusted financial intermediaries. Aliases: Bitcoin whitepaper (Bitcoin), Bitcoin: A Peer-to-Peer Electronic Cash System, whitepaper.

Source: 03-IN - Framing.

Bitfinex Hack. A major 2016 exchange theft whose laundering trail later illustrated peeling chains, chain hopping, KYC subpoenas, OSINT, and cloud evidence. Aliases: 2016 Bitfinex hack, Bitfinex Hack (2016), Bitfinex Hack (case study).

Source: 02-FO - Case Study: The Bitfinex Hack (2016).

Blender.io. A centralized Bitcoin mixer used in the Ronin laundering path after funds were bridged from Ethereum to Bitcoin. Aliases: Blender, Blender.io (mixer).

Source: 01-FO - Ronin: Tracing Through the Mixers.

Blind signature. A cryptographic signing technique that lets a signer authorize a message without learning the message contents. Aliases: blind signatures.

Source: 03-IN - Framing.

Blinded block header. A block header and bid value forwarded without revealing the full transaction body before validator selection. Aliases: Blinded block header (Ethereum MEV), blinded bid, blinded header.

Source: 03-EF - Builder / Relay Stack and MEV.

Blob. A large, temporary data attachment to an Ethereum block that rollups can use for verification but the EVM does not execute. Aliases: Blob (EIP-4844), blob data, blobs.

Source: 01-EF - Proto-Danksharding (EIP-4844) — Blob Data for L2s.

Blob data. Temporary Ethereum data space introduced to make rollup batch publication cheaper without expanding permanent state. Aliases: Blob data (Ethereum scaling), EIP-4844 blob data, blob, blobs.

Source: 04-AS - Layer 2s, Rollups, and Blobs.

Block. A packaged batch of approved operations or transactions plus metadata that links it into the chain. Aliases: Block (blockchain data structure), blocks.

Source: 02-IN - The "Block" in Blockchain.

Block (Bitcoin). A package of transactions that can be appended to the Bitcoin chain after satisfying proof-of-work and validation rules. Aliases: Bitcoin block (data structure), block, blocks.

Source: 01-BF - Primitive 2: The Public Ledger via P2P Networking.

Block assembly. The process where miners or validators select pending transactions, verify them, and package them into a proposed block. Aliases: candidate block assembly.

Source: 02-IN - Step 4: Block Assembly.

Block body. The part of a block that contains the transactions or state updates being recorded in the ledger. Aliases: block transactions, body.

Source: 02-CM - Block Body Anatomy.

Block builder. An actor or component that assembles transactions into a candidate execution payload or block. Aliases: Block builder (Ethereum block building), Block builder (Ethereum), builder, builders.

Source: 03-EF - Review: The Life of an Ethereum Transaction.

Block cipher. A symmetric cipher that transforms fixed-size blocks of data under a secret key. Aliases: block ciphers.

Source: 03-CP - Building Blocks of Block Ciphers.

Block header. The compact metadata portion of a blockchain block that can include a Merkle root committing to the block's transactions. Aliases: Block header (Bitcoin), Block header (blockchain), block headers, header.

Source: 02-CP - Where You'll See Them (Non-Exhaustive).

Block header hash. The hash of a block's header that miners compare to the difficulty target when proving work. Aliases: Block header hash (Bitcoin mining), block hash, header hash.

Source: 01-BF - Primitive 3: Consensus via Proof-of-Work.

Block interval. The intended average time between new blocks in a chain. Aliases: block time, target interval.

Source: 02-CM - Difficulty Adjustment: Control-Loop Intuition.

Block linking. The use of a previous block hash inside a later block so changing earlier data breaks later references. Aliases: Block linking (hashing), hash linking, hash-linked blocks, hash-linked records.

Source: 04-AS - Hashing in Blockchain Practice.

Block log. The durable ordered ledger history that records accepted blocks, including transactions later marked valid or invalid. Aliases: Block log (Hyperledger Fabric), block history, ledger history.

Source: 02-PC - From Permissioned Concepts to Fabric Terms.

Block propagation. The process by which newly found blocks spread across the peer-to-peer network. Aliases: Block propagation (Bitcoin network), block relay.

Source: 02-CM - Block Propagation and Stale/Orphan Blocks.

Block proposer (Ethereum). The validator selected for a slot to build and broadcast a candidate block. Aliases: Block proposer (Ethereum PoS role), Block proposer (Ethereum PoS), proposer, slot proposer.

Source: 02-EF - PoS Overview: Validators, Committees, and Clients.

Block proposer (Proof of Stake). The validator selected for a slot to choose transactions, build a candidate block, and propose it to the network. Aliases: Block proposer (PoS role), leader, proposer.

Source: 03-CM - The Block Proposer: Selection and Building.

Block relay. The process by which newly found blocks spread among Bitcoin nodes and miners. Aliases: Block relay (Bitcoin network), block broadcast, block propagation.

Source: 04-BF - Partitioning Attacks.

Block reward. The miner compensation for finding a valid block, made up of newly issued bitcoin and transaction fees. Aliases: Block reward (Bitcoin), mining reward.

Source: 01-BF - Incentives: Making Honesty Profitable.

Block size. The amount of transaction data a block can carry under the protocol's limits. Aliases: block capacity.

Source: 02-CM - Parameter Choices and Tradeoffs.

Block space. The limited capacity inside blocks that users compete for when they want transactions included. Aliases: Block space (Bitcoin), blockspace.

Source: 01-BF - Monetary Policy.

Block subsidy. Newly issued coins paid to the miner of a valid block as part of the block reward. Aliases: Block subsidy (Bitcoin monetary policy), Block subsidy (Bitcoin), block reward, block reward subsidy, mining subsidy, subsidy.

Source: 02-CM - Security Model and Economics.

Block validation. The independent node process of checking proof-of-work, transaction validity, unspent inputs, and proper chain extension before accepting a block. Aliases: Block validation (Bitcoin), validate block.

Source: 02-BF - After Finding a Valid Block.

Block weight. Bitcoin's consensus measure for block size limits, capped at 4 million weight units. Aliases: Block weight (Bitcoin), weight units.

Source: 02-BF - The Data Structure of a Block.

Block withholding. A pool attack where a miner submits valid shares but hides full valid blocks, reducing the pool's rewards. Aliases: Block withholding (mining pool), pool block withholding.

Source: 02-CM - Block Withholding in Poolsv{.smaller}.

Blockchain. A shared technical system for recording and verifying data without relying only on a central trusted authority. Aliases: blockchains.

Source: 01-IN - Why A Blockchain Course?.

Blockchain abstraction layer. Software or services that hide raw blockchain operations behind wallets, apps, exchanges, or other user-facing tools. Aliases: abstraction layer, interface layer.

Source: 01-AS - What Does a User Actually Interact With?.

Blockchain address. A public identifier for a blockchain wallet or account, often derived by hashing a public key. Aliases: account address, address, addresses, wallet address.

Source: 04-CP - Public Keys as Blockchain Addresses.

Blockchain analytics. The use of ledger data, clustering, and risk scoring to help assess counterparties and transaction flows. Aliases: Blockchain analytics (Bitcoin compliance), blockchain analysis, chain analytics.

Source: 04-BF - How KYC/AML Apply to Bitcoin.

Blockchain forensics. Analysis of blockchain transactions, addresses, and patterns to connect on-chain activity with real-world actors or behavior. Aliases: Blockchain forensics (forensics), Blockchain forensics (investigative analysis), blockchain analytics, forensics, on-chain forensics.

Source: 03-IN - Promises vs. Reality.

Blockchain network. A distributed network of machines that propagate and validate blockchain state without a single central operator. Aliases: blockchain P2P network.

Source: 01-DS - Distributed Computing and Blockchain.

Blockchain network deployment. The practical setup and operation of blockchain nodes or environments so students can observe network behavior directly.

Source: 01-IN - Tools and Setup.

Blockchain stack. The layered combination of cryptography, networking, consensus, ledger structures, and applications that makes a blockchain system work. Aliases: blockchain layers, technical stack.

Source: 04-AS - The Blockchain Stack at a Glance.

Blockchain Trilemma. The design trade-off among decentralization, security, and scalability in blockchain systems. Aliases: decentralization-security-scalability trilemma.

Source: 04-IN - The Engineer's Dilemma: The Blockchain Trilemma.

Blockchain vulnerability. A weakness in blockchain software, protocols, networks, or assumptions that can create security or reliability risk. Aliases: vulnerabilities.

Source: 01-IN - Learning Objectives II.

BLS signature. A signature scheme Ethereum uses because many validator signatures can be aggregated into one compact proof. Aliases: BLS, BLS signature (Ethereum), Boneh-Lynn-Shacham signature.

Source: 02-EF - Slots and Epochs.

BOINC. A generalized volunteer-computing platform that coordinates work distribution, result upload, validation, and credit. Aliases: Berkeley Open Infrastructure for Network Computing.

Source: 01-DS - Volunteer Computing Pipeline: BOINC.

Bootstrap. The process by which new participants enter a trust system and begin earning reputation from low or neutral starting trust. Aliases: Bootstrap (reputation systems), bootstrapping, newcomer handling.

Source: 03-DS - Properties of Reputation Systems.

Bootstrapping. An FHE technique that refreshes noisy ciphertexts so more encrypted operations can be performed. Aliases: Bootstrapping (FHE), noise refresh, noise reset.

Source: 05-CP - Fully Homomorphic Encryption (FHE).

Bored Ape Yacht Club. An Ethereum NFT collection that became a membership club, event network, artwork license system, and entertainment brand. Aliases: BAYC, Bored Ape Yacht Club (membership NFT project).

Source: 06-EF - Case Study: Bored Ape Yacht Club.

Branching factor. The number of child hashes combined at each internal node of a Merkle tree. Aliases: Branching factor (Merkle tree), binary tree, k-ary tree.

Source: 02-CP - Design Choices & Variants.

Bretton Woods. The post-World War II monetary system in which the U.S. dollar was convertible to gold and other major currencies were pegged to the dollar. Aliases: Bretton Woods system.

Source: 04-IN - The Turning Point: Ending Bretton Woods.

Bribery. An attack where an adversary pays validators to vote for, build, or support a chosen block or chain. Aliases: Bribery (PoS attack), validator bribery.

Source: 03-CM - Censorship, Bribery, and Eclipse.

Bridge. Infrastructure that represents or moves assets or messages across chains using contracts, custodians, relayers, or other trust assumptions. Aliases: Bridge (cross-chain infrastructure), Bridge (cross-chain movement), Bridge (cross-chain), blockchain bridge, bridges, cross-chain bridge.

Source: 06-EF - Centralization Chokepoints.

Broad verifiability. The property that ordinary participants can still run nodes and independently check the base layer. Aliases: Broad verifiability (Ethereum L1 design), broadly verifiable, full participation.

Source: 01-EF - The Scaling Problem.

Broadcast. The act of sending a signed transaction or block outward to peers so the wider network can learn about it. Aliases: Broadcast (blockchain network), broadcasting, transmission.

Source: 02-IN - Step 2: The Broadcast.

Broadcast storm. A network condition where repeated or duplicate broadcasts consume so much capacity that useful traffic is crowded out. Aliases: broadcast storms.

Source: 01-DS - Case Study: Gnutella & “Flooding”.

BTC-e. A large early digital currency exchange with weak AML controls that became a major cash-out hub for cybercriminals. Aliases: BTC-e (case study), Bitcoin Exchange.

Source: 01-FO - Case Study: BTC-e.

Builder. A participant that assembles candidate blocks from pending transactions for possible proposal by validators. Aliases: Builder (Ethereum block building), block builder, builders.

Source: 02-EF - Censorship.

Byte-exact hashing. Hashing that depends on the exact serialized bytes, field order, and encoding specified by the protocol. Aliases: bit-for-bit deterministic hashing.

Source: 02-CM - Block Header Anatomy: What Gets Hashed.

Bytecode. The low-level instructions produced from smart contract languages and executed by the EVM. Aliases: Bytecode (EVM), Bytecode (Ethereum), EVM bytecode, compiled bytecode, contract bytecode, unique bytecode.

Source: 01-EF - The Ethereum Virtual Machine (EVM).

Byzantine agreement. A protocol problem where honest participants must settle on one value even while traitors send conflicting values.

Source: 05-IN - Mini-Activity: Byzantine Agreement.

Byzantine fault. A failure where a node behaves arbitrarily, deceptively, or maliciously, including sending conflicting messages to different peers. Aliases: Byzantine faults, arbitrary fault, malicious fault.

Source: 05-IN - Byzantine Faults.

Byzantine fault threshold. The maximum number of Byzantine participants a protocol's quorum math is designed to tolerate. Aliases: Byzantine fault threshold (BFT quorum), fault threshold, t.

Source: 01-CM - Quorums.

Byzantine Fault Tolerance. The ability of a protocol to keep reaching correct agreement even when some participants behave Byzantine. Aliases: BFT, BFT-based systems, Byzantine Fault Tolerance (consensus), Byzantine Fault Tolerant, Byzantine Fault Tolerant consensus protocol, Byzantine fault tolerance (consensus).

Source: 05-IN - Byzantine Faults.

Byzantine Generals Problem. The problem of getting loyal distributed actors to agree on one plan even when some actors or channels are faulty or malicious. Aliases: BGP, Byzantine Generals Problem (Bitcoin), Byzantine agreement problem.

Source: 05-IN - Byzantine Generals Problem.

Byzantine-fault tolerance. A consensus family designed to remain safe when some known participants may lie, equivocate, or act maliciously. Aliases: BFT, BFT orderer, Byzantine fault tolerance, Byzantine-fault tolerance (Hyperledger Fabric ordering).

Source: 01-CM - Byzantine-Fault Tolerance (BFT).

C

C2PA. A content provenance standard that helps creators and platforms preserve media origin and edit history. Aliases: C2PA (content provenance), C2PA standard, Coalition for Content Provenance and Authenticity.

Source: 05-AS - Opportunity: Authenticity and Provenance.

Call frame. The EVM execution context for one call, including its own caller, value, gas budget, memory, and return data. Aliases: Call frame (EVM), execution frame, stack frame.

Source: 04-EF - Calls and Control Flow in the EVM.

Calldata. The read-only input bytes supplied by the caller, including encoded function arguments. Aliases: Calldata (Solidity data location), call data, transaction input payload.

Source: 04-EF - Data Locations: Storage, Memory, Calldata.

Canary validator. A limited validator deployment used to test upgrades before rolling them out to a larger production fleet. Aliases: Canary validator (Ethereum operations), canary validators.

Source: 03-EF - Client Diversity & Pairing Practices.

Candidate block. A block assembled by a participant that still needs consensus approval before becoming official history. Aliases: Candidate block (Bitcoin mining), Candidate block (Bitcoin), block proposal, candidate blocks, proposed block.

Source: 02-IN - Step 4: Block Assembly.

Canonical block. A block treated as the accepted branch by the protocol after receiving enough stake-weighted support. Aliases: Canonical block (PoS), canonical acceptance.

Source: 03-CM - The Committee: Attestation and Validation.

Canonical chain. The ledger branch that honest nodes treat as the accepted history under the consensus rule. Aliases: Canonical chain (blockchain), accepted chain, canonical branch, canonical history, main chain.

Source: 01-CM - Why Consensus Matters in Blockchains.

Canonical history. The transaction history currently accepted by nodes under Bitcoin's chain-selection and validation rules. Aliases: Canonical history (Bitcoin), Canonical history (Ethereum), accepted history, authoritative history, canonical chain, canonical head, shared history, valid history.

Source: 01-BF - Bitcoin, Simplified.

Capability negotiation. The peer handshake step where Ethereum nodes advertise which subprotocol versions and features they support. Aliases: Capability negotiation (Ethereum networking), capabilities.

Source: 03-EF - ETH Execution-Network Message.

Capital at risk. Validator funds locked under protocol rules that can be lost or delayed if the validator misbehaves or fails duties. Aliases: Capital at risk (PoS), bonded capital, locked collateral, staked capital.

Source: 03-CM - Orientation: Proof of Work vs Proof of Stake.

Capital Controls. Legal restrictions on moving money into, out of, or within a financial system during stress or by policy choice.

Source: 04-IN - The Problem of Control: Chokepoints & Censorship.

Capital flow control. State efforts to restrict, monitor, or steer money moving across borders or out of the domestic financial system. Aliases: capital controls.

Source: 02-AS - Why Governments Care.

Casper-FFG. Ethereum's finality gadget that justifies and finalizes checkpoints when enough total stake votes consistently across epochs. Aliases: Casper Friendly Finality Gadget, Casper-FFG (Ethereum finality), FFG, Friendly Finality Gadget.

Source: 02-EF - Gasper: Fork Choice + Finality.

CBDC pilot. A limited operational test of a CBDC design before full-scale production deployment. Aliases: pilot.

Source: 02-AS - Central Bank Digital Currencies (CBDCs).

Censorship. The intentional filtering, dropping, or blocking of messages or transactions by a participant or adversary. Aliases: Censorship (Ethereum), Censorship (PoS attack), Censorship (blockchain), Censorship (distributed systems), soft censorship, transaction censorship.

Source: 05-IN - Why Failures Become Security Risks.

Censorship resistance. The ability of a blockchain design to make it difficult for gatekeepers to block valid participation or transactions. Aliases: Censorship resistance (Bitcoin network), Censorship resistance (blockchain network), Censorship resistance (blockchain), Censorship resistance (decentralization), censorship-resistant.

Source: 02-IN - The Spectrum of Decentralization.

Central authority. A single organization or service that can vouch for participants, enforce rules, or resolve disputes for the network. Aliases: Central authority (P2P trust), central referee.

Source: 03-DS - What Is "Trust" in P2P?.

Central Bank. An institution that manages a fiat monetary system through policy, emergency liquidity, and payment-system oversight. Aliases: central banks.

Source: 04-IN - The Modern Financial Architect: Central Banks.

Central bank digital currency. A digital form of central bank money issued or governed by a monetary authority. Aliases: CBDC, CBDCs, Central Bank Digital Currency (tokenization), central bank digital currencies, central bank digital currency.

Source: 03-IN - Why This History Matters.

Central server. A server that provides a key coordination function for a system, such as indexing files or routing users to resources. Aliases: central index.

Source: 03-IN - P2P Normalizes Decentralization.

Centralization. The concentration of control, speed, or privacy decisions in fewer hands or a single owner. Aliases: Centralization (ledger design), centralized design.

Source: 04-DS - Trade-offs.

Centralization chokepoint. A dependency above or around a decentralized base layer where control, access, or failure risk concentrates in a small number of operators. Aliases: centralization chokepoints, centralized chokepoint.

Source: 06-EF - Centralization Chokepoints.

Centralized architecture. A system design where one authority coordinates work, controls state, and becomes the main trust dependency.

Source: 05-IN - Centralized vs. Distributed Architectures.

Centralized database. A database controlled by a trusted owner or administrator who can define, update, and manage the authoritative record. Aliases: admin-trusted database, central database.

Source: 04-DS - Distributed Ledger vs. Centralized Database (Compare/Contrast).

Centralized digital money system. A digital money arrangement controlled by identifiable operators who can be directly regulated, prosecuted, or shut down. Aliases: centralized digital currency system.

Source: 04-BF - Regulatory Pressure Beyond Bitcoin.

Centralized index. A central service that stores searchable metadata or routing information for many participants. Aliases: central index, centralized discovery.

Source: 01-DS - Client–Server: Centralized Index and Control.

Centralized issuer. A single organization that creates, backs, or administers a digital money system. Aliases: central issuer, centralized company.

Source: 01-BF - Lessons from Precursors.

Centralized system. A system organized around a clear control point that simplifies coordination but creates a point of trust or failure. Aliases: Centralized system (architecture), centralized architecture.

Source: 04-AS - Centralized vs Distributed Architectures.

Centralized trust. A model where users rely on a central institution or authority to validate records, settle disputes, or coordinate agreement.

Source: 01-IN - Learning Objectives I.

Centralized trust model. A model where institutions verify identity, keep records, enforce rules, and resolve disputes on behalf of users. Aliases: centralized trust, digital trust.

Source: 03-IN - Digital Trust: The Centralized Model.

Certificate Authority. An entity trusted to issue and digitally sign certificates that bind public keys to identities. Aliases: CA, Certificate Authority (Hyperledger Fabric), Fabric CA, certificate authority.

Source: 04-CP - Certificates and PKI Hierarchy.

Certificate Revocation List. A published list of certificates that a Certificate Authority has revoked before their normal expiration. Aliases: CRL, certificate revocation lists.

Source: 04-CP - Certificate Validation Process.

Certificate validation. The process of checking a certificate's chain, expiration, subject match, issuer signatures, and revocation status. Aliases: certificate validation process.

Source: 04-CP - Certificate Validation Process.

ChaCha20. A modern stream cipher that generates a fast keystream for symmetric encryption. Aliases: ChaCha20 (symmetric cipher).

Source: 03-CP - What Is Symmetric Cryptography?.

Chain head. The block a node currently treats as the tip of the best chain to extend. Aliases: Chain head (PoS fork choice), current head, head.

Source: 03-CM - Fork Choice Rules.

Chain hopping. Moving assets across different blockchains to force investigators into a new ledger, asset format, or tracing environment. Aliases: Chain Hopping (blockchain forensics), Chain hopping (blockchain forensics), Chain hopping (obfuscation), asset hopping, chain hop, cross-chain hopping, cross-chain laundering.

Source: 01-FO - How Adversaries Hide.

Chain ID. A network identifier included in a transaction signature to bind the transaction to one Ethereum chain. Aliases: Chain ID (Ethereum transaction), chainId.

Source: 03-EF - Transaction Fields and Signatures.

Chain of Custody. The traceable sequence of control or movement that links funds from one address, service, or actor to another. Aliases: Chain of Custody (blockchain forensics), custody chain, fund provenance.

Source: 02-FO - Obfuscation Service: Mixers & Tumblers.

Chain of ownership. The sequence of signed transfers that links a coin's prior transaction to its current authorized owner. Aliases: Chain of ownership (Bitcoin), chain of signatures, signature chain.

Source: 01-BF - Primitive 1: Ownership via Digital Signatures.

Chain reorganization. A short-term replacement of one chain branch with another branch that has more cumulative work. Aliases: Chain reorganization (Bitcoin), block reorganization, chain reorg, ledger rewrite, reorg.

Source: 02-BF - When Is a Transaction Complete?.

Chaincode. Fabric's term for application code that implements business rules and proposes ledger updates during transaction simulation. Aliases: Chaincode (Hyperledger Fabric), Chaincode (enterprise tokenization), Chaincode (permissioned ledgers), Fabric smart contract, assets as chaincode, permissioned chaincode, private chaincode, smart contract.

Source: 02-PC - Fabric-Specific Concepts To Watch For.

Chaincode definition. The channel-level agreement on a chaincode's name, version, sequence number, endorsement policy, and related settings. Aliases: Chaincode definition (Hyperledger Fabric), chaincode approval definition, contract definition.

Source: 02-PC - Chaincode Lifecycle.

Chaincode event. A notification emitted by chaincode so external observers can react to a business action after the transaction is processed. Aliases: Chaincode event (Hyperledger Fabric), Fabric event, event.

Source: 02-PC - Chaincode Example: CreateAsset.

Chaincode lifecycle. The governance process for installing a chaincode package, approving a channel definition, and committing that definition before invocation. Aliases: Chaincode lifecycle (Hyperledger Fabric), Fabric chaincode lifecycle, lifecycle.

Source: 02-PC - Chaincode Lifecycle.

Chaincode package. The deployable artifact containing smart-contract code and metadata needed to run chaincode on endorsing peers. Aliases: Chaincode package (Hyperledger Fabric), deployable chaincode artifact, package.

Source: 02-PC - Chaincode Lifecycle.

Chaining state. The intermediate hash state that is passed from one compression round to the next. Aliases: Chaining state (hashing), final internal state, internal state.

Source: 02-CP - Merkle–Damgård: How SHA-256 is Built.

Change address. A fresh sender-controlled address used to receive the change output from a transaction. Aliases: Change address (Bitcoin).

Source: 02-BF - Change Addresses and Fees.

Change Address Detection. A heuristic process for identifying which output in a UTXO transaction likely returns leftover value to the sender. Aliases: Change Address Detection (Bitcoin forensics), change detection, change output detection.

Source: 02-FO - Heuristic #2: Change Address Detection.

Change output. A new transaction output that returns leftover value to the sender because selected UTXOs must be spent in full. Aliases: Change output (Bitcoin transaction), Change output (Bitcoin), change.

Source: 02-BF - What Are Wallets?.

Channel. A ledger or communication partition that limits which participants can see or interact with a subset of data. Aliases: Channel (Hyperledger Fabric), Channel (permissioned ledger privacy), channels, partition, partitions.

Source: 01-PC - Privacy.

Channel configuration. The governance data that defines channel membership, policies, administrative rules, and related configuration for a Fabric channel. Aliases: Channel configuration (Hyperledger Fabric), channel config, channel policy configuration.

Source: 02-PC - From Permissioned Concepts to Fabric Terms.

Channel MSP definition. The channel-level MSP information that tells a channel which organizations exist and which signatures satisfy their trust rules. Aliases: Channel MSP definition (Hyperledger Fabric), channel MSP, channel MSP definitions.

Source: 02-PC - What is an MSP?.

Checkpoint (Ethereum). An epoch-boundary block used as a target for finality votes. Aliases: Checkpoint (Ethereum finality), checkpoint link, epoch checkpoint.

Source: 02-EF - Gasper: Fork Choice + Finality.

Checkpoint (Proof of Stake). A block at an epoch boundary used as an anchor for finality votes. Aliases: Checkpoint (PoS finality), Checkpoint (Proof of Stake finality), checkpoints, epoch checkpoint, finality anchor.

Source: 03-CM - Epochs and Checkpoints: Organizing Slots.

Checkpoint sync. A synchronization approach that starts from a recent finalized checkpoint instead of replaying the entire chain from genesis. Aliases: Checkpoint sync (Ethereum PoS), checkpoint synchronization.

Source: 03-EF - Sync Modes & Data Availability.

Checks-Effects-Interactions. A defensive ordering pattern that checks preconditions, updates internal state, and performs external calls last. Aliases: CEI, CEI pattern, Checks-Effects-Interactions (smart contract security).

Source: 04-EF - Reentrancy: Anatomy and Defenses.

CHIPS. A private US dollar clearing and settlement system used for large-value payments among banks. Aliases: CHIPS (payment settlement), Clearing House Interbank Payments System.

Source: 02-AS - Global Payment Infrastructure: Overview.

Chokepoint. A central place in a financial network where an authority or intermediary can block, freeze, or redirect activity. Aliases: Chokepoint (blockchain investigations), Chokepoint (financial system), cash-out chokepoint, central chokepoint, chokepoints, investigative chokepoint, single point of control.

Source: 04-IN - The Problem of Control: Chokepoints & Censorship.

Chord. A ring-based distributed hash table where hashed peers and keys are arranged in identifier order and lookups follow shortcut links. Aliases: Chord (DHT).

Source: 02-DS - DHT Example: Chord.

Chosen collision. A collision attack where the attacker deliberately constructs different inputs that hash to the same digest. Aliases: Chosen collision (hashing), chosen-prefix collision, crafted collision.

Source: 05-CP - Hash Fragility: Collision Resistance Isn't Forever.

Churn. The continual joining, leaving, rebooting, moving, and reconnecting of nodes in a distributed network. Aliases: Churn (P2P membership), Churn (P2P networking), Churn (network topology), membership churn, peer churn.

Source: 01-DS - Fallacy #5: Topology Doesn't Change.

Cipher Block Chaining. A block-cipher mode that XORs each plaintext block with the previous ciphertext block before encryption. Aliases: CBC.

Source: 03-CP - Modes of Operation Overview.

Cipher Feedback. A legacy mode that turns a block cipher into a self-synchronizing stream-like construction. Aliases: CFB.

Source: 03-CP - Modes of Operation Overview.

Ciphertext. The encrypted output that should hide the plaintext from anyone without the correct key or keystream. Aliases: Ciphertext (FHE), ciphertexts, encrypted data.

Source: 03-CP - Infinite-length One Time Pad.

CIPS. China's cross-border yuan payment system that combines messaging and settlement for renminbi transactions. Aliases: CIPS (cross-border payment system), Cross-Border Interbank Payment System.

Source: 02-AS - Global Payment Infrastructure: Overview.

Circuit breaker. A safety mechanism that pauses critical operations when data feeds or assumptions appear to fail. Aliases: Circuit breaker (oracle defense), emergency pause, pause mechanism.

Source: 04-EF - Randomness, Oracles, and External Data.

Civil forfeiture. A legal process for taking ownership of assets connected to unlawful activity, even when the assets are discovered later. Aliases: forfeiture.

Source: 01-FO - Silk Road: The Ledger.

Classical consensus. A consensus family that usually assumes known participants, message exchange, quorum rules, and explicit fault models. Aliases: Classical consensus (consensus family), permissioned consensus.

Source: 04-AS - Classical vs Economic Consensus.

Client diversity. The presence of multiple independent software clients participating in the same blockchain network. Aliases: Client diversity (Ethereum network health), Client diversity (Ethereum operations), Client diversity (Ethereum), Client diversity (blockchain), client diversity, consensus client diversity, diverse clients, execution client diversity, multi-client diversity.

Source: 01-DS - Fallacy #8: The Network Is Homogeneous.

Client team. A team that implements Ethereum node software and shapes which protocol changes are practically deployable. Aliases: Client team (Ethereum stakeholder), client teams.

Source: 01-EF - Stakeholders & Decision Making.

Client-server architecture. A centralized design where clients request data or service from a server or server cluster that holds authority. Aliases: client-server, client-server model.

Source: 01-DS - Client–Server: Centralized Index and Control.

Code as speech. The legal argument that source code can be expressive activity protected by the First Amendment.

Source: 03-IN - The Crypto Wars: U.S. Gov Position (1990s).

Code-based cryptography. A post-quantum cryptography family based on hard decoding problems from error-correcting codes.

Source: 05-CP - Post-Quantum Cryptography: The New Toolbox.

Coercive Extraction. Gaining value through theft, extortion, or forced illicit transfer rather than normal market participation.

Source: 03-AS - North Korea: Overview.

Coercive Revenue Generation. A state strategy that turns theft, extortion, or illicit transfer into funding for sanctioned activity. Aliases: coercive crypto revenue.

Source: 03-AS - North Korea: Overview.

Coin selection. The wallet process of choosing which UTXOs to spend as inputs for a new transaction. Aliases: Coin selection (wallet).

Source: 02-BF - What Are Wallets?.

Coinbase transaction. The first transaction in a Bitcoin block, which creates new bitcoin and pays the miner according to protocol rules. Aliases: Coinbase transaction (Bitcoin mining), Coinbase transaction (Bitcoin), coinbase, coinbase tx.

Source: 01-BF - Incentives: Making Honesty Profitable.

Coincidence of Wants. The barter problem where each trader must want what the other trader is offering at the same time.

Source: 04-IN - What is Money? A Social Technology.

CoinJoin. A collaborative transaction technique that combines multiple users' inputs and outputs to make ownership links harder to trace. Aliases: CoinJoin (Bitcoin privacy technique), CoinJoin (Bitcoin privacy).

Source: 04-BF - Mitigating Network Deanonymization.

Collaboration artifact. A shared indicator, evidence record, or analytical product that teams can use across investigations. Aliases: Collaboration artifact (forensics), shared analytical product, shared indicator.

Source: 01-FO - Future of Forensics: Secure Cross-Agency Collaboration.

Collateral. Assets posted to back trading positions and payouts in a market. Aliases: Collateral (prediction markets), market collateral.

Source: 01-AS - Prediction Markets Case: Polymarket.

Collateralized Debt Obligation. A complex financial product built from pools of debt instruments, including mortgage-related securities. Aliases: CDO, collateralized debt obligations.

Source: 04-IN - Case Study: The 2008 Global Financial Crisis.

Collision resistance. The property that it should be infeasible to find any two distinct inputs with the same digest.

Source: 02-CP - Hash Function Properties.

Collusion. A coordinated attack where peers rate each other positively, or rate competitors negatively, to distort reputation scores. Aliases: Collusion (P2P reputation threat), collusion ring, coordinated praise.

Source: 03-DS - Properties of Reputation Systems.

Collusion resistance. A trust system's ability to limit the effect of peers that coordinate ratings to boost themselves or harm others.

Source: 03-DS - EigenTrust: Anchors and Collusion Resistance.

Colonial Pipeline. A U.S. critical-infrastructure ransomware case where a Bitcoin ransom created a live trace that supported rapid FBI recovery efforts. Aliases: Colonial Pipeline (case study).

Source: 01-FO - Case Study: Colonial Pipeline.

Colored Coins. An early Bitcoin-based approach that marked transaction outputs so off-chain participants could treat them as representing non-BTC assets. Aliases: Colored Coins (Bitcoin tokenization), colored coins.

Source: 05-EF - Tokenization History — Early Experiments.

Commission fault. A failure where a node remains active but returns an incorrect or corrupted result. Aliases: commission faults.

Source: 05-IN - Commission Faults.

Commit. The step where a valid ordered transaction is written to the ledger and its effects update world state. Aliases: Commit (Hyperledger Fabric), committing, valid commit.

Source: 02-PC - One Invoke: Proposal to Commit.

Commit phase. The phase where enough matching votes allow the protocol to accept a value as decided for that position. Aliases: Commit phase (consensus), commit, committed.

Source: 01-CM - Rounds and Phases.

Commit-reveal scheme. A protocol where participants first commit to hidden values and later reveal them, reducing opportunities to change inputs after seeing others. Aliases: Commit-reveal scheme (NFT fairness), Commit-reveal scheme (smart contract randomness), commit reveal, commit-reveal.

Source: 04-EF - Randomness, Oracles, and External Data.

Commitment. A compact cryptographic reference that can later prove whether a specific piece of data matches what was recorded. Aliases: Commitment (ledger verification), commitments, hash commitment.

Source: 01-PC - Why Not A Shared Database?.

Committee (Ethereum). A randomly assigned group of validators that attests to block validity, chain head, and checkpoints. Aliases: Committee (Ethereum PoS), committees, validator committee.

Source: 02-EF - PoS Overview: Validators, Committees, and Clients.

Committee (Proof of Stake). A randomly assigned subset of validators that checks a proposed block and votes on it for a slot or epoch. Aliases: Committee (PoS validator group), Committee (Proof of Stake group), committees, validator committee.

Source: 03-CM - The Committee: Attestation and Validation.

Committing peer. A peer acting in the commit role by receiving ordered blocks, rechecking policy and state-version rules, and updating ledger state. Aliases: Committing peer (Hyperledger Fabric), committer, committers, committing peers.

Source: 02-PC - The Big Picture: End-to-End Fabric Path.

Commodity Money. Money whose value is tied to the useful or scarce physical good itself, such as salt, cattle, or shells.

Source: 04-IN - A Brief History of Money's Form.

Common-input ownership heuristic. A heuristic that treats multiple inputs to one transaction as likely controlled by the same actor. Aliases: CIOH, Common-input ownership heuristic (Bitcoin forensics), common-input ownership.

Source: 04-AS - Graph Thinking and Heuristics.

Common-input-ownership heuristic. A tracing rule of thumb that assumes inputs spent together in one transaction are likely controlled by the same entity. Aliases: CIOH, Common-Input-Ownership Heuristic (Bitcoin forensics), Common-input-ownership heuristic (blockchain forensics), common input ownership, common-input heuristic, multi-input heuristic.

Source: 01-FO - Challenges in Forensic Analysis.

Compact block relay. A block propagation protocol that sends compact block information and only transmits full transactions the peer is missing. Aliases: Compact block relay (Bitcoin), cmpctblock, compact blocks.

Source: 03-BF - Block Propagation.

Completeness. The property that an honest prover can convince the verifier when the statement being proved is true. Aliases: Completeness (zero-knowledge proofs).

Source: 05-CP - Zero-Knowledge Proofs: Prove Without Revealing.

Composability. The ability for smart contracts to call and combine with other contracts in a single coordinated workflow. Aliases: Composability (Ethereum), Composability (smart contracts), Composability (tokenization), atomic workflows, composable assets, contract composability, permissionless composability.

Source: 01-EF - From EVM to Programs — Smart Contracts.

Compression function. A fixed-size function that mixes one message block with the current hash state to produce the next state. Aliases: Compression function (hashing), compress.

Source: 02-CP - Merkle–Damgård: How SHA-256 is Built.

Compromised node. A node that has been taken over or corrupted so it may produce bad data or act against the protocol. Aliases: compromise, hijacked node.

Source: 05-IN - Why Failures Become Security Risks.

Computational hardness. The assumption that some problems are so difficult that no efficient known algorithm can solve them at relevant sizes. Aliases: hardness, intractability.

Source: 01-CP - Computational Hardness.

Computational hardness assumption. An assumption that a mathematical problem has no efficient known solution for properly chosen parameters. Aliases: hard problem, hardness assumption.

Source: 04-CP - Computational Hardness Assumptions.

Computational irreversibility. The condition where reversing a transaction becomes infeasible because an attacker would need to redo and surpass accumulated proof-of-work. Aliases: Computational irreversibility (Bitcoin), computationally impractical to reverse, practical irreversibility.

Source: 01-BF - Bitcoin: The Mission Statement.

Computationally infeasible. A security claim that an attack is possible in theory but too expensive for realistic attackers using known methods. Aliases: infeasible.

Source: 02-CP - Pre-Image Resistance.

Concatenation. The operation of joining byte strings in order before hashing them together. Aliases: Concatenation (hash input), parallel operator, ||.

Source: 02-CP - What Is a Merkle Tree?.

Confidential smart contract. A smart contract design that keeps user data or account state private while still allowing contract logic to execute. Aliases: confidential smart contracts.

Source: 05-CP - Fully Homomorphic Encryption (FHE).

Confidentiality. A security property that keeps information hidden from parties who are not authorized to read it.

Source: 01-CP - What Is Cryptography?.

Confidentiality boundary. A Fabric design boundary that limits which members can see ledger data, policies, or private payloads. Aliases: Confidentiality boundary (Hyperledger Fabric), data-separation boundary, visibility boundary.

Source: 02-PC - Channels: Confidentiality Boundary.

Confirmation. A block added after a transaction's block, increasing confidence that the chosen history will remain accepted. Aliases: Confirmation (Bitcoin), Confirmation (blockchain), Confirmation (proof of work), block confirmations, confirmation depth, confirmations.

Source: 01-CM - Why Consensus Matters in Blockchains.

Confirmation requirement. The number of blocks a service waits after a transaction before treating it as sufficiently settled. Aliases: Confirmation requirement (Bitcoin services), confirmation depth, required confirmations.

Source: 04-BF - Bitcoin Gold 51% Attack Discovery.

Confusion. A cipher design goal that obscures the relationship between the secret key and the resulting ciphertext. Aliases: Confusion (Shannon principle).

Source: 03-CP - Shannon's Principles: Confusion and Diffusion.

Consensus. The process a blockchain network uses to agree on valid history or state despite many independent participants. Aliases: Consensus (blockchain layer), Consensus (blockchain mechanism), Consensus (distributed ledger ordering), Consensus (distributed systems), Consensus (distributed-systems goal), agreement, agreement process, consensus mechanism, consensus mechanisms, consensus process, consensus protocol.

Source: 01-IN - Course Structure.

Consensus attack. An attack that tries to manipulate which recent ledger history honest nodes accept as the valid chain. Aliases: Consensus attack (Bitcoin), consensus-layer attack.

Source: 04-BF - What Can Consensus Attacks Achieve?.

Consensus client. Software that runs consensus-layer logic such as duty assignment, block verification, committees, and finality. Aliases: CL client, Consensus client (Ethereum client), Consensus client (Ethereum), beacon node.

Source: 02-EF - PoS Overview: Validators, Committees, and Clients.

Consensus family. A broad category of consensus protocols grouped by identity assumptions, adversary model, and finality style. Aliases: consensus families.

Source: 01-CM - Comparing Consensus Families.

Consensus layer. The Ethereum layer responsible for validators, attestations, fork choice, and finality. Aliases: CL, Consensus layer (Ethereum architecture), Consensus layer (Ethereum).

Source: 02-EF - The Merge: Beacon Chain to PoS.

Consensus mechanism. A rule system that lets many independent participants agree on one accepted result or history. Aliases: Consensus mechanism (blockchain), consensus mechanisms.

Source: 03-IN - Why This History Matters.

Consensus protocol. A protocol that lets distributed nodes agree on shared ledger history or state without relying on one central referee. Aliases: Consensus protocol (blockchain mechanism), consensus, consensus protocols.

Source: 01-CP - How Blockchain Uses Cryptography.

Consensus rules. The protocol rules that determine whether Bitcoin transactions and blocks are valid. Aliases: Consensus rules (Bitcoin), Consensus rules (blockchain), consensus rule, network rules, validity rules.

Source: 03-BF - What Is a Bitcoin Node?.

Consensus tradeoff. A design tension in consensus systems where improving performance, security, or decentralization can make another goal harder. Aliases: consensus tradeoffs.

Source: 01-IN - Learning Objectives I.

Consistency. The property that participants converge on the same correct version of the record despite simultaneous writes or failures. Aliases: Consistency (distributed ledgers).

Source: 04-DS - From Logs to Ledgers.

Consolidation. The gathering of funds from many addresses or outputs into a smaller number of controlled destinations. Aliases: Consolidation (blockchain forensics), UTXO consolidation, fund aggregation.

Source: 02-FO - Graph Motif: The "Fan-In".

Constant product formula. An AMM pricing rule that keeps the product of two token reserves constant as trades change each reserve. Aliases: Constant product formula (AMM), constant product market maker, x*y=k.

Source: 01-FO - Decentralized Exchanges (DEXs).

ConstitutionDAO. A DAO formed to pool funds for a rare U.S. Constitution printing, whose token later persisted as a social symbol after the bid failed. Aliases: ConstitutionDAO (single-purpose DAO), PEOPLE.

Source: 06-EF - Case Study: ConstitutionDAO.

Constructor. A deployment-time function that runs once to initialize contract state before the runtime bytecode is stored on-chain. Aliases: Constructor (Solidity), constructor logic.

Source: 04-EF - Contract Deployment.

Content addressing. A storage addressing model where the address is derived from the content itself, so changing the file changes the address. Aliases: Content addressing (storage), content-addressed storage.

Source: 06-EF - Metadata, IPFS, and the Pointer Problem.

Content authenticity and provenance. Evidence about where digital content came from, how it changed, and who or what issued it. Aliases: authenticity and provenance, content provenance.

Source: 05-AS - Opportunity: Authenticity and Provenance.

Content Credentials. Metadata attached to media to preserve information about origin, edits, ownership, or other provenance claims. Aliases: content credential.

Source: 05-AS - Opportunity: Authenticity and Provenance.

Content hash. A cryptographic fingerprint of a file that lets users detect whether referenced media or metadata has changed. Aliases: Content hash (NFT storage), content hashes, file hash.

Source: 05-EF - NFTs: What Are We Actually Buying?.

Content identifier. A content-addressed identifier derived from data so users can verify they retrieved the expected file. Aliases: CID, CIDs, Content identifier (IPFS), IPFS CID.

Source: 05-EF - Common Pitfalls in NFT Projects.

Content-Addressable Network. A DHT design that maps peers and keys into a virtual coordinate space divided into node-owned zones. Aliases: CAN.

Source: 02-DS - DHT Example: CAN.

Content-addressed data system. A system that identifies stored content by hashes of the content rather than only by location or filename. Aliases: content-addressed data systems, content-addressed storage.

Source: 02-CP - Where You'll See Them (Non-Exhaustive).

Content-addressed storage. A storage model where data is retrieved by its hash rather than by a server location. Aliases: Content-addressed storage (NFT metadata), content addressing, content-addressed.

Source: 05-EF - Metadata and Storage Models.

Context factor. A weighting factor that accounts for the type, stakes, and norms of the transaction being rated. Aliases: context factors, context weight, transaction context.

Source: 03-DS - PeerTrust: How Trust Is Calculated.

Continuous security. The view that auditing, monitoring, upgrades, and migration are ongoing requirements rather than one-time setup tasks. Aliases: Continuous security (blockchain systems), adaptive security, security is continuous.

Source: 05-AS - Key Lessons.

Contract account. An Ethereum account that holds code and storage and runs only when activated by a transaction or contract call. Aliases: Contract account (Ethereum account type), Contract account (Ethereum), contract, contract accounts, contract address, smart contract account.

Source: 01-EF - Accounts & Global State (EOA vs Contract).

Contract address. The Ethereum address where a deployed contract account's code and storage can be reached. Aliases: Contract address (Ethereum), Contract address (NFT verification), contract addresses.

Source: 01-EF - Accounts & Global State (EOA vs Contract).

Contract creation transaction. A transaction with no destination address that deploys new contract code using data carried in the transaction. Aliases: Contract creation transaction (Ethereum), contract creation, to = null.

Source: 03-EF - Transaction Fields and Signatures.

Contract declaration. The Solidity syntax that names the deployable unit of code and state. Aliases: Contract declaration (Solidity), contract Name, contract block.

Source: 04-EF - Solidity: File Structure, From Top to Bottom.

Contract deployment. The process of creating a contract account by sending creation code that runs once and returns runtime bytecode. Aliases: Contract deployment (Ethereum), deployment.

Source: 04-EF - Contract Deployment.

Contract event. A record emitted by smart contract execution that applications and indexers can use to track meaningful activity. Aliases: Contract event (blockchain indexing), contract events, event log, logs.

Source: 01-AS - Indexing: Making Blockchain Usable.

Control loop. A mechanism that observes actual output and changes an input to steer the system toward a target behavior. Aliases: Control loop (difficulty adjustment), feedback loop.

Source: 02-CM - Difficulty Adjustment: Control-Loop Intuition.

Control surface. The part of a token ecosystem through which a holder can actually exercise power or access a privilege. Aliases: Control surface (token governance), control surfaces.

Source: 06-EF - Case Study: Bored Ape Yacht Club.

Convertibility. The right or ability to exchange a monetary claim for a specified amount of an underlying asset.

Source: 04-IN - The Turning Point: Ending Bretton Woods.

Coordination cost. The added effort required for distributed participants to discover one another, exchange information, and stay coherent. Aliases: coordination complexity.

Source: 01-DS - Centralized vs. Decentralized: Trade-offs.

Corda. A permissioned distributed ledger platform named as an example of restricted participation among known entities. Aliases: Corda (permissioned ledger platform).

Source: 02-IN - The Spectrum of Decentralization.

Core EIP. An Ethereum Improvement Proposal that changes Ethereum protocol rules rather than only an application-level interface. Aliases: Core EIP (Ethereum governance), Core EIPs.

Source: 01-EF - Governance & Ethereum Improvement Proposals (EIPs).

Core operation. The day-to-day flow that moves a request from submission and approval to ordered, validated ledger history. Aliases: Core operation (permissioned ledger), transaction operation, transaction path.

Source: 01-PC - Key Components.

Correlated client bug. A defect that affects many nodes or validators at once because they run the same client implementation or version. Aliases: Correlated client bug (Ethereum), client monoculture risk, correlated bug.

Source: 03-EF - Client Diversity & Pairing Practices.

Correlated slashing. A penalty design where validators lose more stake when many validators misbehave in the same period or pattern. Aliases: Correlated slashing (PoS penalty), correlation penalty.

Source: 03-CM - Slashing — Making Misbehavior Expensive.

Correlation. Linking events across systems using patterns such as timing, amount, destination, or infrastructure rather than a direct shared identifier. Aliases: Correlation (forensics), cross-system correlation, event correlation.

Source: 01-FO - Bridges & Swaps: Crossing the Chain Boundary (cont.).

Correlation penalty. A slashing penalty that increases when many validators are slashed in the same period. Aliases: Correlation penalty (Ethereum slashing), correlated slashing penalty.

Source: 02-EF - Nothing-at-Stake.

Correspondent banking. A banking arrangement where banks hold accounts with one another to route international payments. Aliases: correspondent banks.

Source: 02-AS - Global Payment Infrastructure: Overview.

Counter. A value that increments across generator or encryption rounds so each keyed function input is distinct. Aliases: Counter (cryptography), ctr.

Source: 03-CP - Counter-Mode Pseudorandom Generator (PRG).

Counter mode. A block-cipher mode that encrypts counter values to generate a keystream. Aliases: CTR.

Source: 03-CP - Modes of Operation Overview.

Counter-Heuristic. A wallet, protocol, or user behavior designed to break the assumptions behind common forensic heuristics. Aliases: Counter-Heuristic (blockchain forensics), anti-clustering technique, counter heuristic.

Source: 02-FO - Pitfalls & Counter-Heuristics.

Counter-mode PRG. A generator that evaluates a keyed function on successive counter values to produce a keystream. Aliases: CTR-style PRG, counter-mode pseudorandom generator.

Source: 03-CP - Counter-Mode Pseudorandom Generator (PRG).

Crash fault. A failure where a node stops responding completely and sends no further messages. Aliases: crash failure, crash faults.

Source: 05-IN - Crash Faults.

Crash fault tolerance. A consensus fault model that handles nodes stopping or becoming unavailable without assuming malicious behavior. Aliases: CFT, Crash fault tolerance (consensus).

Source: 01-PC - Consensus.

Crash-fault tolerance. A consensus family that tolerates nodes crashing, restarting, or going silent, but not lying or colluding. Aliases: CFT, Crash-fault tolerance (Hyperledger Fabric ordering), crash-fault-tolerant.

Source: 01-CM - Crash-Fault Tolerance (CFT).

CREATE. The standard EVM deployment opcode that derives a new contract address from the creator address and nonce. Aliases: CREATE (EVM opcode).

Source: 04-EF - Contract Deployment.

CREATE2. An EVM deployment opcode that derives a contract address from the creator address, a salt, and the initcode hash. Aliases: CREATE2 (EVM opcode).

Source: 04-EF - Contract Deployment.

Credential. Cryptographic proof that ties an action to a recognized participant, organization, and role. Aliases: Credential (permissioned ledger), credentials, operational certificate.

Source: 01-PC - Key Components.

Credential compromise. The loss of control over a credential that lets an attacker act as an authorized participant or administrator. Aliases: admin compromise, credential theft, key theft.

Source: 01-PC - Threats to Permissioned Systems.

Credential expiration. The point when a credential is no longer valid and must be renewed or replaced before it can authorize actions. Aliases: certificate expiration, expired credentials.

Source: 01-PC - Membership Lifecycle.

Credential revocation. The removal of credentials or access so a participant can no longer act under a prior role. Aliases: revocation, revoke credentials.

Source: 01-PC - Key Components.

Credibility weighting. A defense that scales ratings by the rater's own credibility so untrusted raters have little influence.

Source: 03-DS - PeerTrust: Handling Manipulation.

Credible neutrality. The expectation that applications run under public rules that are not controlled by one privileged operator. Aliases: Credible neutrality (Ethereum).

Source: 01-EF - Beyond Cryptocurrency: Buterin's Vision.

Credit Rating Agency. An institution that evaluates the risk of financial products and assigns ratings such as AAA. Aliases: credit rating agencies.

Source: 04-IN - Case Study: The 2008 Global Financial Crisis.

Critical evaluation. The practice of judging whether a blockchain project actually solves a trust problem better than simpler alternatives.

Source: 03-IN - Why This History Matters.

Cross-chain bridge. Infrastructure that locks, verifies, or represents value from one blockchain so related value can move or appear on another. Aliases: Cross-Chain Bridge (blockchain infrastructure), Cross-chain bridge (blockchain forensics), bridge, bridges, cross-chain bridge contract, smart contract bridge.

Source: 01-FO - How Adversaries Hide.

Cross-Chain Forensics. The practice of correlating exits on one chain with entries on another using timing, value, and service behavior. Aliases: Cross-Chain Forensics (blockchain forensics), cross-chain tracing, following the hop.

Source: 02-FO - Following the Hop: Cross-Chain Forensics.

Cross-chain tracing. Following asset movement across multiple blockchains by matching bridge events, swaps, timings, amounts, and destinations. Aliases: Cross-chain tracing (blockchain forensics), chain-by-chain reconstruction, cross-chain forensics.

Source: 01-FO - Bridges & Swaps: Crossing the Chain Boundary (cont.).

Cross-checking. Comparing claims across independent sources to test whether evidence and interpretations hold up. Aliases: Cross-checking (information evaluation), cross-check, multiple sources.

Source: 01-AS - Reading Critically.

Crypto intermediary. A company or platform that stands between users and blockchain systems by providing custody, trading, lending, or other services. Aliases: crypto intermediaries.

Source: 05-AS - When Blockchain Systems Broke.

Crypto Wars. The 1990s political and legal conflict over whether strong cryptography would remain restricted or become broadly available to the public.

Source: 03-IN - The Crypto Wars: U.S. Gov Position (1990s).

Crypto-collateralized stablecoin. A stablecoin backed by on-chain crypto assets, often requiring over-collateralization to absorb price volatility. Aliases: crypto-backed stablecoin, crypto-collateralized.

Source: 02-AS - Stablecoins: Types and Mechanisms.

Crypto-native environment. A system whose users, assets, and incentives mostly remain on-chain rather than depending on traditional institutions. Aliases: crypto-native ecosystem, crypto-native system.

Source: 05-AS - Future 2: Specialized Crypto Ecosystem.

CryptoAPI. A Windows cryptographic interface whose default key storage behavior mattered in the CryptoDefense failure. Aliases: CryptoAPI (Windows), Windows CryptoAPI.

Source: 05-CP - Case Study: CryptoDefense — Keys Left in Plain Sight.

Cryptocurrency. A digital asset ecosystem built around blockchain-based tokens, markets, and networks. Aliases: Cryptocurrency (digital money), crypto, crypto markets, cryptocurrencies, traditional cryptocurrency.

Source: 01-IN - Why A Blockchain Course?.

CryptoDefense. A ransomware case where private keys were generated with strong RSA but left accessible in the victim's own key store.

Source: 05-CP - Case Study: CryptoDefense — Keys Left in Plain Sight.

Cryptoeconomic penalty. A punishment that combines cryptographic proof of a rule violation with an economic loss imposed by the protocol. Aliases: Cryptoeconomic penalty (PoS), economic penalty, protocol penalty.

Source: 03-CM - Slashing — Making Misbehavior Expensive.

Cryptographic agility. The ability to replace or upgrade cryptographic algorithms without redesigning the whole protocol or application. Aliases: algorithm agility, hash agility, signature agility.

Source: 05-CP - Cryptographic Assumptions Decay Over Time.

Cryptographic assumption. A belief that a cryptographic problem remains too expensive for realistic attackers to solve with known methods and hardware. Aliases: cryptographic assumptions, hardness assumption.

Source: 05-CP - Cryptographic Assumptions Decay Over Time.

Cryptographic commitment. A compact value, often a hash or Merkle root, that binds a system to underlying data without carrying all of that data directly. Aliases: Cryptographic commitment (blockchain), commitment, compact commitment.

Source: 04-AS - Hashing: What Problem Does It Solve?.

Cryptographic hash. A function that turns data into a compact fingerprint that changes dramatically if the input changes. Aliases: digital fingerprint, hash, hashes.

Source: 02-IN - Pillar 1: Cryptography.

Cryptographic hash function. A deterministic algorithm that maps data of any length to a fixed-length digest used for integrity, commitments, and verification. Aliases: Cryptographic hash function (PRG building block), cryptographic hash, hash, hash function.

Source: 02-CP - What Is a Cryptographic Hash Function?.

Cryptographic link. A reference from one block to another using a cryptographic hash so later blocks depend on earlier block contents. Aliases: fingerprint, hash link, mathematical link.

Source: 02-IN - The "Block" in Blockchain.

Cryptographic primitive. A foundational cryptographic building block, such as a hash or signature, used to construct higher-level blockchain behavior. Aliases: cryptographic primitives, primitives.

Source: 02-IN - Looking Ahead: Next Steps.

Cryptographic Proof. Mathematical evidence produced by cryptographic mechanisms that can verify claims without relying solely on institutional trust. Aliases: Cryptographic proof (Bitcoin), cryptographic proof instead of trust, cryptographic proofs.

Source: 04-IN - The Bitcoin Standard: A Digital Return to "Hard Money".

Cryptographic trust. Trust grounded in cryptographic checks that verify identity, authenticity, and message integrity. Aliases: crypto trust layer.

Source: 03-DS - Cryptographic vs. Social Trust.

Cryptographic verification. The use of hashes, signatures, and related checks to confirm data integrity and sender identity.

Source: 03-DS - Trust but Verify: The Complete Trust Loop.

Cryptographically relevant quantum computer. A quantum computer powerful enough to break important public-key cryptographic systems used by today's blockchains. Aliases: CRQC, cryptographically relevant quantum threat.

Source: 05-AS - Cryptographically Relevant Quantum Threat.

Cryptographically secure pseudorandom number generator. A random generator designed so attackers cannot feasibly predict outputs even after seeing other outputs. Aliases: CSPRNG, cryptographically secure PRNG.

Source: 05-CP - When Good Crypto Goes Bad: Milk Sad (CVE-2023-39910).

Cryptography. The mathematical toolkit blockchains use to prove authorization, protect integrity, and make tampering evident. Aliases: Cryptography (blockchain layer), Cryptography (blockchain pillar), Cryptography (mathematical security), crypto.

Source: 02-IN - The Three Pillars.

Cryptography export controls. Government restrictions that limited the export or public distribution of strong cryptographic tools. Aliases: crypto export controls, export controls.

Source: 03-IN - Privacy as a Prerequisite for Open Society.

Cryptography Mailing List. The specialist mailing list where the Bitcoin whitepaper was first circulated to a community already debating privacy, trust, and digital cash.

Source: 01-BF - Satoshi Nakamoto's Whitepaper.

CRYSTALS-Kyber. A lattice-based post-quantum key-establishment scheme presented as a migration path for public-key encryption and key exchange. Aliases: Kyber.

Source: 04-CP - Quantum Threat Preview.

Cumulative work. The total proof-of-work backing a chain of blocks, used to decide which history nodes treat as canonical. Aliases: Cumulative work (Bitcoin), heaviest chain, highest-work chain, most cumulative work, most work.

Source: 01-BF - Bitcoin, Simplified.

Curated participation. A participation model where membership is granted only to approved entities instead of anyone who connects. Aliases: controlled participation, curated admission.

Source: 01-PC - What Changes.

Currency layer. The layer concerned with what unit of value people use, such as dollars, yuan, bitcoin, or a CBDC. Aliases: Currency layer (state control).

Source: 02-AS - The Permission Layer: Three Challenges to State Control.

Custodial failure. A breakdown where a platform holding user assets loses, mismanages, or blocks access to those assets. Aliases: Custodial failure (crypto intermediaries), custody failure.

Source: 05-AS - When Blockchain Systems Broke.

Custodial model. An arrangement where a platform holds the user's keys and provides account access, services, and possible recovery. Aliases: Custodial model (key custody), custodial custody, custodial wallet, platform custody.

Source: 01-AS - Custody Models.

Custody. The safekeeping and control of an underlying asset or keys by a party trusted to support a tokenized claim. Aliases: Custody (asset-backed token), custodian, custodians.

Source: 05-EF - Why Tokenize? Problems and Promises.

Custody proof. Evidence that an asset's custody history satisfies the rules required for a transaction to be accepted. Aliases: Custody proof (embedded provenance), custody chain proof, valid custody proof.

Source: 01-FO - Future of Forensics: Embedded Provenance.

Custom error. A named Solidity failure type that can return structured information when a call reverts. Aliases: Custom error (Solidity), error.

Source: 04-EF - Example: Coin (Code, Part 2).

Cypherpunk Manifesto. Eric Hughes's 1993 public statement arguing that privacy in the electronic age must be built with code rather than granted by institutions. Aliases: A Cypherpunk's Manifesto, Cypherpunk Manifesto.

Source: 03-IN - Framing.

Cypherpunk movement. A community of activists, computer scientists, and cryptographers who argued that strong cryptography could protect privacy and individual autonomy online. Aliases: cypherpunk ethos, cypherpunks.

Source: 03-IN - The Cypherpunk Movement.

Cypherpunk vision. The political and technical belief that cryptography can support privacy, autonomy, decentralization, and resistance to centralized control. Aliases: cypherpunk thinking, original vision.

Source: 05-AS - The Original Vision.

D

DAI. A crypto-collateralized stablecoin governed through MakerDAO rather than a single traditional issuer. Aliases: DAI (stablecoin), MakerDAO DAI.

Source: 02-AS - Types of Digital Money.

Damping. A control on iterative trust propagation that limits drift and keeps global scores tied to trusted reference points. Aliases: Damping (trust propagation).

Source: 03-DS - PeerTrust vs. EigenTrust: Summary.

Dandelion-style relay. A transaction relay approach that first sends a transaction along a short random path before broadcasting it widely. Aliases: Dandelion relay, Dandelion-style relay (Bitcoin privacy), stem-and-fluff relay.

Source: 04-BF - Mitigating Network Deanonymization.

Darknet market. An online illicit marketplace accessed through privacy-focused infrastructure such as Tor. Aliases: dark web market, illicit marketplace.

Source: 01-FO - Case Study: Silk Road.

Data availability. The requirement that transaction or rollup data be available so others can reconstruct and verify the resulting state. Aliases: DA, Data availability (Ethereum scaling), Data availability (Ethereum), Data availability (tokenized assets).

Source: 01-EF - The Scaling Problem.

Data location. A label that specifies where reference-type data lives during execution, such as storage, memory, or calldata. Aliases: Data location (Solidity), data locations.

Source: 04-EF - Data Locations: Storage, Memory, Calldata.

DDoS. An attack that floods or disrupts critical services so they cannot perform their network role. Aliases: DDoS (permissioned ledger risk), denial-of-service attack, distributed denial of service.

Source: 01-PC - Threats to Permissioned Systems.

De facto dollar infrastructure. A system people use in practice to access, price, save, or move dollars even though it is not the official banking rail. Aliases: practical dollar infrastructure.

Source: 02-AS - Case Study: USDT on Tron.

Deanonymization. Linking pseudonymous blockchain activity to a real-world identity, operator, organization, or accountable entity. Aliases: Deanonymization (blockchain forensics), de-anonymization, identity linkage.

Source: 01-FO - BTC-e: Deanonymization.

Decentralization. The distribution of control, validation, or operation across multiple participants rather than one central authority. Aliases: Decentralization (Bitcoin), Decentralization (blockchain design), Decentralization (ledger design), Decentralization (system control), decentralized, decentralized design.

Source: 01-IN - Learning Objectives I.

Decentralized application. An application that runs on or coordinates through a blockchain or related decentralized network rather than a single traditional service. Aliases: DApp, DApps, Dapp, dApp, dApps, dapp, dapps, decentralized app.

Source: 01-IN - Why A Blockchain Course?.

Decentralized Autonomous Organization. A token-governed organization that coordinates voting, treasury control, protocol changes, or shared work through on-chain and off-chain processes. Aliases: DAO, DAOs, decentralized autonomous organization.

Source: 06-EF - Three Patterns: DAOs, Membership NFTs, and Social Tokens.

Decentralized coordination. A system's ability to let many independent participants organize shared activity without a central controller.

Source: 03-IN - P2P Normalizes Decentralization.

Decentralized exchange. An on-chain marketplace where users trade tokens through smart contracts rather than a centralized exchange operator. Aliases: DEX, DEXes, DEXs, Decentralized Exchange (Ethereum), Decentralized exchange (DeFi), decentralized exchanges.

Source: 03-EF - Maximal Extractable Value (MEV).

Decentralized Finance. Smart-contract-based financial applications such as swaps, lending, and token markets that execute on public blockchains. Aliases: DeFi, Decentralized Finance (Ethereum).

Source: 02-FO - Ethereum Forensics: Where the Evidence Hides.

Decentralized infrastructure network. A protocol-based network that coordinates independent providers of services such as data feeds or storage. Aliases: infrastructure network, protocol service network.

Source: 01-AS - Infrastructure as a Use Case.

Decentralized oracle network. An oracle design that aggregates data from multiple sources or participants instead of relying on one trusted feed. Aliases: DON, Decentralized oracle network (oracle design), oracle network.

Source: 01-EF - Oracles: Bridging Blockchains and Reality.

Decentralized physical infrastructure network. A network that coordinates real-world hardware contributions from many independent participants. Aliases: DePIN, decentralized physical infrastructure networks.

Source: 05-IN - Everyday Examples of Distributed Systems.

Decentralized system. A system that spreads authority, operation, or communication across many participants instead of one central controller. Aliases: decentralized design, decentralized network.

Source: 01-DS - Centralized vs. Decentralized: Trade-offs.

Decoupling. A situation where related trends move independently rather than rising and falling together. Aliases: Decoupling (token adoption).

Source: 06-EF - Hidden Infrastructure Growth.

Decryption. The process of recovering plaintext from ciphertext using the correct cryptographic key. Aliases: Decryption (asymmetric cryptography), decrypt.

Source: 03-CP - The Shared Key.

Deep reorganization. A chain reorganization that replaces many recent blocks rather than only one or two competing tips. Aliases: Deep reorganization (proof of work), deep reorg, multi-block reorganization.

Source: 04-BF - Bitcoin Gold 51% Attack Discovery.

Delegatecall. An EVM operation that executes another contract's code while using the caller's storage and execution context. Aliases: Delegatecall (EVM), delegatecall.

Source: 04-EF - Upgradeability and Proxy Patterns.

Delegated minter role. A contract permission that lets a trusted operator or bridge address mint tokens on behalf of the system. Aliases: MINTER_ROLE.

Source: 06-EF - Minting on Ethereum.

Delegation. Assigning voting power to another address without transferring token ownership. Aliases: Delegation (token governance), delegate, delegated voting.

Source: 06-EF - Case Study: ENS DAO.

Denial-of-service attack. An attack that prevents a node or service from responding normally. Aliases: DoS, DoS attack.

Source: 05-IN - Crash Faults.

Denomination Standardization. Forcing withdrawals into fixed amounts to reduce the usefulness of amount-based correlation. Aliases: Denomination Standardization (privacy tooling), fixed output denominations, standard denominations.

Source: 02-FO - Breaking Mixers: Investigative Countermeasures.

Deployment bytecode. The bytecode sent in a deployment transaction that the EVM executes to initialize a contract and produce runtime bytecode. Aliases: Deployment bytecode (Ethereum), creation bytecode, creation code.

Source: 04-EF - Contract Deployment.

Deposit contract. The execution-layer contract where a participant deposits 32 ETH to join the validator set. Aliases: Deposit contract (Ethereum staking), staking deposit contract, validator deposit contract.

Source: 02-EF - PoS Overview: Validators, Committees, and Clients.

DES. An older block cipher that is now treated as legacy because its security margin is no longer adequate. Aliases: DES (legacy symmetric cipher), Data Encryption Standard.

Source: 03-CP - What Is Symmetric Cryptography?.

Design trade-off. A choice where gaining one desirable property requires accepting cost, weakness, or reduced performance in another. Aliases: Design trade-off (blockchain architecture), policy trade-off, trade-off.

Source: 01-FO - Future of Forensics: ForensiBlock & the Design Trade-off.

Determinism. The property that the same input to a hash function always produces the same digest. Aliases: Determinism (chaincode), Determinism (hashing), deterministic, deterministic execution.

Source: 02-CP - What Is a Cryptographic Hash Function?.

Deterministic derivation. The local wallet process of generating many private keys, public keys, and addresses from one seed phrase. Aliases: Deterministic derivation (wallet), derivation, derive.

Source: 02-BF - Where Addresses Come From.

Deterministic execution. Execution where the same input and prior state always produce the same result on every node. Aliases: Deterministic execution (Ethereum), Deterministic execution (smart contracts), determinism, deterministic, deterministic behavior.

Source: 01-EF - Beyond Cryptocurrency: Buterin's Vision.

Deterministic finality. A finality model where a protocol step or ordering service declares an entry final once required conditions are met. Aliases: declared finality, deterministic commit, final commit, immediate finality.

Source: 04-DS - Permissioned vs. Permissionless: Comparison.

devp2p. Ethereum's peer-to-peer networking framework for discovery, encrypted transport, and execution-layer subprotocols. Aliases: devp2p (Ethereum execution layer), devp2p stack.

Source: 03-EF - ETH Execution-Network Message.

Difficulty. The protocol setting that controls how hard it is to find a valid proof-of-work block. Aliases: Difficulty (Proof of Work), difficulty adjustment, difficulty target, target.

Source: 04-AS - Difficulty, Work, and Probabilistic Finality.

Difficulty adjustment. A protocol rule that adjusts the target based on recent block timing so average block intervals stay near the design goal. Aliases: Difficulty adjustment (proof of work), difficulty retargeting, retargeting.

Source: 02-CM - Difficulty Adjustment: Control-Loop Intuition.

Difficulty target. The threshold a block hash must fall below for the block to satisfy the PoW validity rule. Aliases: Difficulty target (Bitcoin mining), Difficulty target (proof of work), difficulty threshold, target, target threshold.

Source: 02-CM - The PoW Rule at a Glance.

Diffie-Hellman key exchange. A protocol that lets two parties derive the same shared secret over an insecure channel without sending the secret itself. Aliases: DH, Diffie-Hellman, Diffie–Hellman key exchange.

Source: 04-CP - Diffie–Hellman Key Exchange Concept.

Diffusion. A cipher design goal that spreads each plaintext bit's influence across many ciphertext bits. Aliases: Diffusion (Shannon principle).

Source: 03-CP - Shannon's Principles: Confusion and Diffusion.

Digest. The fixed-length output of a hash function that acts as a compact fingerprint of the input data. Aliases: Digest (hashing), fingerprint, hash, hash digest, hash output, hash value.

Source: 02-CP - What Is a Cryptographic Hash Function?.

DigiCash. David Chaum's early digital cash company that used blind signatures for private payments but still depended on a central company and banks. Aliases: Chaumian digital cash.

Source: 03-IN - Early Attempts at Digital Money.

Digital asset. A blockchain-recorded item of value or ownership that can be transferred through valid transactions. Aliases: Digital asset (blockchain), digital assets.

Source: 02-IN - Putting it Together: The Lifecycle of a Transaction.

Digital cash. Money represented digitally so it can be transferred online, with Bitcoin aiming to make that transfer work without a trusted bank. Aliases: Digital cash (Bitcoin precursor), decentralized digital cash, digital money, electronic cash, internet-native cash.

Source: 01-BF - The Emergence of Bitcoin.

Digital certificate. A signed data object that binds a public key to an owner, domain, device, or other identity information. Aliases: X.509 certificate, certificate.

Source: 04-CP - Certificates and PKI Hierarchy.

Digital currency. A form of money or payment instrument represented digitally, including systems that governments and central banks may explore. Aliases: digital currencies.

Source: 01-IN - Why A Blockchain Course?.

Digital Euro. The European Central Bank's proposed public digital-money project for euro-area payments. Aliases: digital euro project.

Source: 03-AS - EU: Overview.

Digital money. Money or payment value represented and transferred through digital systems rather than physical cash. Aliases: digital cash, digital currencies, digital currency.

Source: 03-IN - Early Attempts at Digital Money.

Digital Product Passport. A product-linked digital record used to track provenance, compliance, lifecycle, or supply-chain information. Aliases: DPP, Digital Product Passports.

Source: 06-EF - Hidden Infrastructure Growth.

Digital Ruble. Russia's state-run central-bank digital currency project for domestic payment control and possible settlement experiments. Aliases: Russia's digital ruble.

Source: 03-AS - Russia: Overview.

Digital Rupee. India's central-bank-led digital-money project for safer payments, settlement efficiency, and state oversight. Aliases: India's digital rupee, e-rupee.

Source: 03-AS - India: Overview.

Digital Scarcity. Verifiable scarcity in a digital system, such as Bitcoin's protocol-limited supply.

Source: 04-IN - The Bitcoin Standard: A Digital Return to "Hard Money".

Digital signature. A cryptographic proof that a message or transaction was authorized by the holder of a corresponding private key. Aliases: Digital signature (Bitcoin ownership), Digital signature (Bitcoin), Digital signature (Ethereum transaction), digital signatures, signature, signatures, signed payload, signing, unforgeable signature.

Source: 01-IN - Learning Objectives I.

Digital signature workflow. The process of hashing a message, signing the digest with a private key, and verifying the result with a public key. Aliases: sign-and-verify workflow.

Source: 04-CP - Digital Signature Workflow.

Dilithium. A lattice-based post-quantum digital signature scheme presented as a replacement direction for vulnerable signature systems. Aliases: CRYSTALS-Dilithium.

Source: 04-CP - Quantum Threat Preview.

Direct trust. Trust based on a participant's own prior interactions with a peer. Aliases: direct experience, first-hand trust.

Source: 03-DS - Direct vs. Indirect Trust.

Discrete logarithm. The hard problem of recovering a hidden exponent from a public group relation. Aliases: Discrete logarithm (public-key cryptography), discrete log, discrete logarithms.

Source: 05-CP - Shor's Algorithm (1994): Breaking RSA and ECC.

Discrete logarithm problem. The problem of finding an exponent from a base, modulus, and resulting modular power. Aliases: DLP, discrete log.

Source: 04-CP - Computational Hardness Assumptions.

Distributed architecture. A system design where many peer nodes share responsibility for coordination and state without a central hub.

Source: 05-IN - Centralized vs. Distributed Architectures.

Distributed Consensus. Agreement among many independent participants about valid system state or transaction history. Aliases: Distributed Consensus (blockchain).

Source: 04-IN - Design Trade-Offs: Efficiency vs. Autonomy.

Distributed hash table. A structured P2P system that maps keys to responsible peers so data can be found through efficient routing. Aliases: DHT, DHTs, Distributed Hash Table (P2P networking), structured overlay routing.

Source: 02-DS - Structured Overlay Networks.

Distributed Ledger. A record-keeping system replicated across multiple participants rather than maintained only by one central database. Aliases: DLT, distributed ledger technology, distributed ledgers.

Source: 04-IN - The Institutional Counterpoint: The BIS Critique.

Distributed system. A system made of multiple independent computers that coordinate over a network to accomplish shared behavior. Aliases: Distributed system (architecture), distributed architecture, distributed systems.

Source: 02-IN - Looking Ahead: Next Steps.

Distributed trust. A trust model where dependence is spread across participants, cryptography, consensus rules, and incentives instead of one central authority. Aliases: emergent trust.

Source: 05-IN - What is "trust" in digital systems?.

DLS result. The result showing that consensus becomes practical when the network eventually behaves predictably enough for timing assumptions to hold. Aliases: DLS partial synchrony result, Dwork-Lynch-Stockmeyer result.

Source: 01-CM - The Timing Limits — FLP and DLS Results.

DNS seed. A publicly maintained domain name that returns IP addresses for reachable Bitcoin peers during node startup. Aliases: DNS seed (Bitcoin peer discovery), DNS seed (Bitcoin), DNS seeds.

Source: 03-BF - Joining the Bitcoin Network.

Dollar-like Digital Instrument. A digital asset or payment instrument that gives users exposure to U.S. dollar value without necessarily using a traditional bank account. Aliases: digital dollar instrument, dollar-like instrument.

Source: 03-AS - What We're Analyzing Today.

Domain separation. The practice of marking different kinds of hash inputs with distinct constants so they cannot be confused. Aliases: LeafTag, NodeTag, tags.

Source: 02-CP - Building a Merkle Tree.

Doodles. An Ethereum NFT project that evolved toward a media, entertainment, and collectibles brand with holder benefits and limited participation. Aliases: Doodles (membership NFT project).

Source: 06-EF - Case Study: Doodles.

Double attestation. A slashable offense where a validator signs two conflicting attestations for the same target epoch. Aliases: Double attestation (Ethereum slashing), attester equivocation.

Source: 02-EF - Nothing-at-Stake.

Double proposal. A slashable offense where a validator signs two different blocks for the same slot. Aliases: Double proposal (Ethereum slashing), proposer equivocation.

Source: 02-EF - Nothing-at-Stake.

Double spend. An attack where an adversary tries to replace an accepted payment with a conflicting history that excludes or redirects it. Aliases: double-spend attack.

Source: 02-CM - Attacks: Double Spend.

Double spending. An attack goal where a payment is accepted and then a conflicting history is published to erase or reverse it. Aliases: Double spending (Ethereum threat model), double-spend, double-spend attack.

Source: 02-EF - Double Spending (Threat Model).

Double-spend. An attack attempt that uses the same bitcoin value in conflicting payments by reversing, delaying, or replacing a recent transaction. Aliases: Double-spend (Bitcoin), double spend, double-spending.

Source: 04-BF - Why Attack Bitcoin?.

Double-spend attack. An attempt to spend funds and then replace history so the original payment is excluded. Aliases: Double-spend attack (blockchain payments), double spending, double-spend attempt.

Source: 04-AS - Common PoW Attack Themes.

Double-spend check. The validation rule that an output can be consumed at most once. Aliases: Double-spend check (Bitcoin), double-spend prevention.

Source: 02-BF - UTXO Visualized.

Double-spend problem. The digital money problem of preventing the same unit of value from being spent more than once. Aliases: double spending.

Source: 01-CP - Example: The Double-Spend Problem.

Double-spending. The attempt to spend the same digital asset more than once. Aliases: Double-spending (Bitcoin), Double-spending (blockchain), double spend, double spending, double-spend, double-spend attempt, double-spend problem, double-spending problem.

Source: 03-IN - The Synthesis: Bitcoin.

Drex. Brazil's central-bank pilot for tokenized digital financial infrastructure and programmable settlement. Aliases: Brazil Drex, Brazil's Drex pilot.

Source: 03-AS - Latin America: Impact Signals.

Dutch auction. An auction format where the price starts high and decreases until buyers commit or supply is sold. Aliases: Dutch auction (NFT sale), Dutch auctions.

Source: 05-EF - Minting and Market Design Patterns.

Dynamic NFT. A tokenized asset whose metadata, displayed state, or associated rights can change over time. Aliases: dynamic NFTs, dynamic asset, dynamic assets.

Source: 05-EF - Looking Forward: Dynamic Assets.

E

e-CNY. China's retail central-bank digital currency pilot built inside a state-directed payment architecture. Aliases: China's retail CBDC, digital renminbi, digital yuan.

Source: 03-AS - China: Overview.

e-gold. A centralized digital money service that let users transfer ownership of gold-denominated balances. Aliases: E-gold, e-gold.

Source: 03-IN - Early Attempts at Digital Money.

ECDSA. A digital signature scheme used by major blockchains to authorize transactions and prove control of keys. Aliases: ECDSA (blockchain signatures), Elliptic Curve Digital Signature Algorithm.

Source: 05-AS - Cryptographically Relevant Quantum Threat.

Eclipse attack. An attack where a node's peer connections are manipulated so it receives a distorted view of the network. Aliases: Eclipse attack (Bitcoin network), Eclipse attack (Bitcoin), Eclipse attack (Ethereum networking), Eclipse attack (P2P threat), Eclipse attack (network attack), Eclipse attack (network security), eclipse, eclipse attacks, eclipse attempt, eclipse pressure, eclipse-style isolation, eclipsed node, network isolation, network-level eclipse, node isolation attack, peer isolation attack.

Source: 01-DS - Fallacy #4: The Network Is Secure.

Economic consensus. A consensus family that uses scarce resources, incentives, or penalties to shape behavior in open systems. Aliases: Economic consensus (consensus family), blockchain economic consensus.

Source: 04-AS - Classical vs Economic Consensus.

Economic Instrument of Statecraft. The use of financial, trade, monetary, and market tools to project power or impose costs. Aliases: economic instrument of national power, economic statecraft.

Source: 03-AS - Financial Rails Are Power.

Economic Shelter. Use of an asset or instrument to protect savings from inflation, devaluation, or weak local currency conditions. Aliases: savings shelter, stablecoin shelter.

Source: 03-AS - Latin America: Impact Signals.

Ecosystem component. A service around the chain that improves usability, interoperability, performance, or access to outside information. Aliases: Ecosystem component (blockchain systems), supporting component, supporting service.

Source: 01-AS - The Full Blockchain System.

Effective balance. The capped validator balance used by the consensus layer to weight selection probability and voting influence. Aliases: Effective balance (Ethereum staking), effective validator balance.

Source: 02-EF - Validator Selection & Randomness.

Effective gas price. The actual per-gas price paid after applying the sender's fee ceiling, the base fee, and the priority fee. Aliases: Effective gas price (Ethereum fee market), actual per-unit fee.

Source: 03-EF - Transactions: Structure and Flow.

Efficiency. A design priority favoring high speed, low cost, high throughput, and reversibility in payments. Aliases: Efficiency (monetary system design).

Source: 04-IN - Design Trade-Offs: Efficiency vs. Autonomy.

EigenTrust. A global reputation algorithm that normalizes local trust values and iteratively propagates them through the network to produce shared trust scores.

Source: 03-DS - EigenTrust: From Local Opinions to Global Scores.

Eight fallacies of distributed computing. A checklist of common false assumptions engineers make about networks, such as reliability, zero latency, and homogeneous nodes. Aliases: eight fallacies, fallacies of distributed computing.

Source: 01-DS - The Eight Fallacies.

EIP workflow. The staged process by which Ethereum proposals move from idea to draft, review, implementation, testing, and possible adoption. Aliases: EIP workflow (Ethereum governance), proposal workflow, upgrade workflow.

Source: 01-EF - EIP Workflow.

EIP-1559. An Ethereum upgrade that changed transaction fees by introducing a burned base fee plus an optional proposer tip. Aliases: EIP-1559 (Ethereum fee market).

Source: 01-EF - Governance & Ethereum Improvement Proposals (EIPs).

EIP-1559 fee mechanism. Ethereum's fee model that combines an automatically adjusted base fee with a user-selected priority tip and fee ceiling. Aliases: EIP-1559, EIP-1559 fee mechanism (Ethereum fee market), Ethereum Improvement Proposal 1559.

Source: 03-EF - EIP-1559 Fee Mechanics.

EIP-2981. An Ethereum royalty information standard that lets a token contract publish a preferred royalty recipient and percentage. Aliases: EIP-2981 (NFT royalty standard), ERC-2981.

Source: 05-EF - Royalties, Economics, and Marketplace Realities.

Elastic Currency. Money whose supply can be expanded or contracted to meet changing economic needs. Aliases: elastic money.

Source: 04-IN - The Ideological Divide: Austrian vs. Keynesian Economics.

Electronic Codebook. A block-cipher mode that encrypts each block independently under the same key. Aliases: ECB.

Source: 03-CP - Modes of Operation Overview.

Electronic coin. In Nakamoto's framing, a chain of digital signatures that transfers value from one owner to the next. Aliases: Electronic coin (Bitcoin), coin.

Source: 01-BF - Primitive 1: Ownership via Digital Signatures.

Elliptic curve cryptography. A public-key approach that uses arithmetic on elliptic-curve points to create compact keys and signatures. Aliases: ECC, Elliptic Curve Cryptography (quantum vulnerability), elliptic-curve cryptography.

Source: 04-CP - Elliptic Curve Cryptography (ECC).

Elliptic-curve discrete logarithm problem. The problem of finding the scalar that maps one elliptic-curve point to another by point multiplication. Aliases: ECDLP, elliptic curve DL, elliptic-curve discrete log.

Source: 04-CP - Computational Hardness Assumptions.

Embedded provenance. Traceability metadata or proof requirements built directly into a system so asset origin and custody can be verified during use. Aliases: provenance-bearing system.

Source: 01-FO - Future of Forensics: ForensiBlock & the Design Trade-off.

Encrypt-then-MAC. A composition pattern that encrypts data first and then authenticates the ciphertext with a message authentication code.

Source: 03-CP - From Confidentiality to Authenticated Encryption (AEAD).

Encrypted mempool. A proposed transaction pool design that hides transaction contents until ordering or inclusion decisions are harder to censor or exploit. Aliases: Encrypted mempool (Ethereum censorship mitigation), encrypted mempools.

Source: 02-EF - Censorship.

Encryption. Cryptographic math for scrambling data to provide confidentiality, even though public blockchains usually do not encrypt the ledger itself. Aliases: Encryption (asymmetric cryptography), asymmetric encryption, encrypt, symmetric encryption.

Source: 02-IN - Pillar 1: Cryptography.

End-entity certificate. A certificate issued to the final server, user, or device whose identity and public key are being validated. Aliases: leaf certificate, server certificate.

Source: 04-CP - Certificates and PKI Hierarchy.

Endianness. The convention for ordering bytes when serializing numbers or fields before hashing or validation. Aliases: Endianness (block serialization), byte order.

Source: 02-CM - Block Header Anatomy: What Gets Hashed.

Endorsement. An endorser's signed approval of a simulated chaincode result and its read-write set. Aliases: Endorsement (Hyperledger Fabric), endorsements, signed endorsement.

Source: 02-PC - One Invoke: Proposal to Commit.

Endorsement mismatch. A failure where endorsers return different results for the same proposal, preventing the client from satisfying endorsement policy. Aliases: Endorsement mismatch (Hyperledger Fabric), mismatched endorsements.

Source: 02-PC - Determinism and Safety.

Endorsement policy. A rule specifying which peers or organizations must approve a transaction before it can be committed. Aliases: Endorsement policy (Hyperledger Fabric), approval policy, endorsement policies.

Source: 04-DS - Case Study A — Hyperledger Fabric (Permissioned).

Endorsing peer. A peer acting in the approval role by simulating chaincode, producing a read-write set, and signing the proposed result. Aliases: Endorsing peer (Hyperledger Fabric), endorser, endorsers, endorsing peers.

Source: 02-PC - The Big Picture: End-to-End Fabric Path.

Endpoint. A surrounding system such as a wallet, exchange, or smart contract where users interact with a blockchain and where attacks often occur. Aliases: Endpoint (blockchain security), endpoints.

Source: 02-IN - Common Misconceptions: What a Blockchain is NOT.

Endpoint Analysis. Investigating the services and records where users buy, sell, store, or otherwise expose an otherwise private asset. Aliases: Endpoint Analysis (privacy coin forensics), endpoint correlation, on-ramp and off-ramp analysis.

Source: 02-FO - Forensic Limitations & Voluntary Disclosure.

Energy consumption. The electricity and physical resources consumed by blockchain operation, especially proof-of-work mining. Aliases: Energy consumption (proof-of-work blockchains), electricity consumption, resource use.

Source: 05-AS - External Constraints.

Energy externality. A cost or impact of mining energy use that falls outside the protocol's direct accounting, such as grid or emissions effects. Aliases: Energy externality (proof of work), environmental externality, externality.

Source: 02-CM - Energy, Externalities, and Design Responses.

Engine API. The local JSON-RPC interface that lets a consensus client ask an execution client to build or validate payloads. Aliases: Engine API (Ethereum).

Source: 03-EF - Two Networks, One Chain.

ENS DAO. The DAO that governs Ethereum Name Service protocol infrastructure, token voting processes, working groups, and treasury decisions. Aliases: ENS, ENS DAO (protocol governance), Ethereum Name Service DAO.

Source: 06-EF - Case Study: ENS DAO.

Entanglement. A quantum relationship where the state of one qubit is linked with another in a way classical bits cannot reproduce. Aliases: Entanglement (quantum computing).

Source: 05-CP - Quantum Primer: Why It Matters for Cryptography.

Entity Cluster. A set of addresses, UTXOs, or accounts inferred to be controlled by one real-world actor or service. Aliases: Entity Cluster (blockchain forensics), address cluster, cluster, entity.

Source: 02-FO - The Analyst's Mindset: Graph Thinking.

Entropy. A measure of how much unpredictability a source or process provides. Aliases: Entropy (key generation), Entropy (randomness), bad entropy, randomness, randomness quality.

Source: 01-CP - Probability Refresher: Independence & Random Variables.

Entropy quality. The practical unpredictability of the source feeding key, seed, or nonce generation. Aliases: randomness quality.

Source: 05-CP - When Good Crypto Goes Bad: Milk Sad (CVE-2023-39910).

Enum. A value type that restricts a variable to a fixed set of named states. Aliases: Enum (Solidity), enumeration.

Source: 04-EF - Types: Value Types.

Epoch (Ethereum). A group of 32 slots used to reshuffle committees and evaluate finality checkpoints. Aliases: Epoch (Ethereum PoS time unit), epochs.

Source: 02-EF - Slots and Epochs.

Epoch (Proof of Stake). A group of consecutive slots used to organize validator selection, checkpoints, and finality updates. Aliases: Epoch (PoS time unit), epochs.

Source: 03-CM - Proof of Stake: The Full Lifecycle.

Equivocation. The act of sending conflicting protocol messages to different participants. Aliases: Equivocation (Ethereum PoS), Equivocation (PoS offense), Equivocation (consensus), conflicting signatures, conflicting votes, double proposal, double vote, double-signing, equivocate, equivocating.

Source: 01-CM - Failure Models.

ERC-1155. An Ethereum multi-token standard that can represent multiple fungible, semi-fungible, or non-fungible asset types in one contract. Aliases: ERC-1155 (Ethereum token standard), ERC-1155 (token standard), ERC1155.

Source: 05-EF - A Taxonomy of Digital Assets.

ERC-165. An Ethereum standard that lets contracts advertise which interfaces they implement. Aliases: ERC-165 (Ethereum interface standard).

Source: 04-AS - Tokens and Standards.

ERC-20. The Ethereum interface standard commonly used for fungible tokens with balances, transfers, and spending allowances. Aliases: EIP-20, ERC-20 (Ethereum token standard), ERC-20 (token standard), ERC20.

Source: 05-EF - A Taxonomy of Digital Assets.

ERC-20 Transfer Event. The standard log event emitted by an ERC-20 token contract when token balances move between addresses. Aliases: ERC-20 Transfer Event (Ethereum), ERC-20 logs, ERC-20 transfer, Transfer event.

Source: 02-FO - Following Token Flows: ERC-20 Transfers.

ERC-721. The Ethereum interface standard for one-of-one non-fungible tokens identified by unique token IDs. Aliases: ERC-721 (Ethereum token standard), ERC-721 (token standard), ERC721.

Source: 05-EF - A Taxonomy of Digital Assets.

ETH subprotocol. The execution-layer devp2p protocol family that defines messages for exchanging transactions, blocks, and chain data. Aliases: ETH, ETH subprotocol (Ethereum execution layer), eth subprotocol, eth/68.

Source: 03-EF - ETH Execution-Network Message.

Ether. Ethereum's native asset, used to pay gas and represent value on the network. Aliases: ETH, Ether (Ethereum native asset).

Source: 01-EF - The Ethereum Virtual Machine (EVM).

Ethereum. A blockchain platform emphasized in the course for smart contracts, tokens, and application-oriented design. Aliases: Ethereum (blockchain platform), Ethereum (programmable blockchain platform), Ethereum network.

Source: 01-IN - Course Structure.

Ethereum Classic. The chain that continued without the DAO-reversal fork after the Ethereum community split in 2016. Aliases: ETC, Ethereum Classic (Ethereum history).

Source: 04-EF - Case Study: The DAO Hack (2016).

Ethereum Discovery v5. Ethereum's peer discovery protocol, based on Kademlia-like ideas for finding nodes in the P2P layer. Aliases: Discovery v5, Ethereum node discovery.

Source: 02-DS - The Blockchain Link: Efficient Routing.

Ethereum Foundation. An influential organization that helps coordinate Ethereum research and development but does not unilaterally control protocol upgrades. Aliases: EF, Ethereum Foundation (Ethereum stakeholder).

Source: 01-EF - Stakeholders & Decision Making.

Ethereum Improvement Proposal. A public specification for a proposed Ethereum protocol change, process change, or ecosystem standard. Aliases: EIP, EIPs, Ethereum Improvement Proposal (Ethereum governance), Ethereum Improvement Proposals.

Source: 01-EF - Governance & Ethereum Improvement Proposals (EIPs).

Ethereum Node Record. Signed node metadata used by Ethereum peers during discovery. Aliases: ENR, Ethereum Node Record (Ethereum networking), Ethereum Node Records.

Source: 03-EF - Execution-Layer Networking (devp2p / RLPx).

Ethereum Request for Comment. A category of Ethereum standard that defines shared application interfaces such as token or wallet conventions. Aliases: ERC, ERCs, Ethereum Request for Comment (Ethereum standard), Ethereum Request for Comments.

Source: 01-EF - Governance & Ethereum Improvement Proposals (EIPs).

Ethereum Request for Comments. An Ethereum application-level standard that defines shared interfaces such as token contracts and other reusable conventions. Aliases: ERC, ERC standard, ERC standards, ERCs, Ethereum Request for Comments (Ethereum standard).

Source: 04-EF - Ethereum's Advantage for Smart Contracts.

Ethereum Virtual Machine. The stack-based virtual machine that every Ethereum node uses to execute contract bytecode and reproduce state transitions. Aliases: EVM, Ethereum Virtual Machine (Ethereum execution).

Source: 01-EF - The Ethereum Virtual Machine (EVM).

Euler's theorem. A number-theoretic result used to explain why correctly chosen RSA exponents return a value to its original form. Aliases: Euler's theorem (RSA intuition).

Source: 04-CP - Why RSA Works (Intuition).

European Blockchain Services Infrastructure. An EU initiative using shared permissioned ledger infrastructure for trusted cross-border services such as credentials and notarization. Aliases: EBSI.

Source: 04-DS - Case Study B — Public Sector: EBSI & Estonia (KSI){.smaller}.

Event. A contract-declared log format that lets successful transactions emit structured data for off-chain consumers. Aliases: Event (Solidity), event emission, events.

Source: 04-EF - Solidity: File Structure, From Top to Bottom.

Event log. Structured output emitted during transaction execution and recorded in the transaction receipt. Aliases: Event Log (Ethereum), Event log (Ethereum), contract event log, emitted event, emitted logs, event logs, events, logs.

Source: 03-EF - Review: The Life of an Ethereum Transaction.

Event signature hash. The keccak-256 hash of an event signature that appears as the first topic for ordinary Solidity events. Aliases: Event signature hash (Ethereum log), event selector, topic 0.

Source: 04-EF - Events and Logs.

Eventual synchrony. A timing assumption that the network may be unreliable for a while but eventually delivers messages within usable bounds. Aliases: Eventual synchrony (distributed-systems assumption), eventually synchronous network.

Source: 03-CM - Safety and Liveness — PoS Invariants.

EVM sandbox. The restricted execution environment that prevents contracts from directly accessing local files, networks, clocks, or operating-system randomness. Aliases: EVM sandbox (Ethereum execution), isolation, sandboxed EVM, sandboxed execution.

Source: 01-EF - Determinism & Execution Constraints.

Exact lookup. A search for one specific item using its known key, hash, or identifier. Aliases: exact-match search, key-based lookup.

Source: 02-DS - Structured Overlay Networks.

Exchange onboarding. The process by which an exchange collects identity and account information before allowing a customer to use its services. Aliases: Exchange onboarding (Bitcoin), account onboarding, customer onboarding.

Source: 04-BF - How KYC/AML Apply to Bitcoin.

Exchange platform. A service that gives users account-based access to crypto trading, custody, or other blockchain-related products. Aliases: Exchange platform (crypto access), crypto exchange, exchange, platform.

Source: 01-AS - What Does a User Actually Interact With?.

Exclusive OR. A bit operation that outputs 1 when exactly one input bit is 1 and outputs 0 otherwise. Aliases: XOR, ^, .

Source: 03-CP - Exclusive OR (XOR) Logic.

Execute-Order-Validate. A Fabric architecture that separates transaction simulation, ordering, and validation into distinct stages. Aliases: EOV, Execute-Order-Validate (Hyperledger Fabric), Execute-order-validate (Hyperledger Fabric), execute order validate, execute-order-validate architecture.

Source: 04-DS - Case Study A — Hyperledger Fabric (Permissioned).

Execution client. Software that handles Ethereum transactions, state, and EVM execution. Aliases: EL client, Execution client (Ethereum client), Execution client (Ethereum).

Source: 02-EF - PoS Overview: Validators, Committees, and Clients.

Execution layer. The Ethereum layer responsible for transactions, accounts, smart contracts, and state updates. Aliases: EL, Execution layer (Ethereum architecture), Execution layer (Ethereum).

Source: 02-EF - The Merge: Beacon Chain to PoS.

Execution payload. The execution-layer block data inside a post-Merge beacon block, including the header, ordered transactions, and execution data. Aliases: Execution payload (Ethereum), execution block, payload.

Source: 02-EF - Execution Payload: Header Structure.

Execution payload body. The variable-size portion of an execution payload that carries ordered transactions and execution-layer data. Aliases: Execution payload body (Ethereum), body, payload body.

Source: 02-EF - Execution Payload: Header Structure.

Execution payload header. The compact portion of an execution payload containing commitments and metadata for verifying transactions, receipts, and resulting state. Aliases: Execution payload header (Ethereum), header, payload header.

Source: 02-EF - Execution Payload: Header Structure.

Expected work. The average number of hash attempts needed before finding a valid block at a given target. Aliases: Expected work (proof of work), expected hashes, expected trials.

Source: 02-CM - Difficulty, Hash Rate, and Expected Work.

Exposed public key. A public key that has been revealed in a way that could become dangerous if attackers can derive the corresponding private key. Aliases: Exposed public key (quantum threat), exposed public keys.

Source: 05-AS - Cryptographically Relevant Quantum Threat.

Extended UTXO. A smart contract model that adds richer validation logic while preserving a UTXO-style transaction structure. Aliases: Cardano eUTXO, Extended UTXO (smart contract model), eUTXO.

Source: 04-EF - Beyond Ethereum: Other Smart Contract Models.

External call. A call from one contract to another account that hands control to code outside the caller's direct control. Aliases: External call (smart contracts), external interaction.

Source: 04-EF - Calls and Control Flow in the EVM.

External data. Information from outside the blockchain, such as prices, reserves, outcomes, or timestamps, that contracts may need to use. Aliases: External data (oracle input), off-chain data, real-world data.

Source: 01-AS - Oracles: Connecting to the Real World.

Externally Owned Account. An Ethereum account controlled by a private key that can initiate transactions and pay gas. Aliases: EOA, EOAs, Externally Owned Account (Ethereum account type), Externally Owned Account (Ethereum), Externally owned account (Ethereum), externally owned accounts, user account, wallet account.

Source: 01-EF - Accounts & Global State (EOA vs Contract).

Extra nonce. Additional adjustable data in the coinbase transaction that miners change to produce new Merkle roots after exhausting the block-header nonce space. Aliases: Extra nonce (coinbase transaction), coinbase extra nonce.

Source: 02-BF - Evolution of Mining Hardware.

F

Factoring. The problem of finding the prime factors that multiply together to form a given composite number. Aliases: Factoring (hard problem), factoring large primes, integer factoring.

Source: 01-CP - Proofs and Reasoning.

Failover. The process of shifting a critical function to a backup service or path when the primary one fails. Aliases: Failover (permissioned ledger operations), failover plan, planned failover.

Source: 01-PC - Threats to Permissioned Systems.

Failure concentration. The risk that a small number of powerful administrative, ordering, or governance components can disrupt the whole network. Aliases: Failure concentration (permissioned ledger), control-plane concentration, control-plane failure.

Source: 01-PC - What Changes.

Failure model. The set of failure behaviors a protocol assumes it must tolerate. Aliases: fault model.

Source: 01-CM - Failure Models.

Fallback function. A special Solidity function that can run when calldata does not match a known selector or when ETH is received in certain cases. Aliases: Fallback function (Solidity), fallback.

Source: 04-EF - ABI, Encoding, and Function Selectors.

Fallback peer. A known peer address included in node software as a backup way to connect when ordinary discovery is insufficient. Aliases: Fallback peer (Bitcoin), fallback node, hardcoded fallback peer.

Source: 03-BF - Joining the Bitcoin Network.

False Merge. An error where unrelated users or addresses are incorrectly combined into one inferred entity. Aliases: False Merge (blockchain forensics), false clustering, incorrect cluster merge.

Source: 02-FO - Pitfalls & Counter-Heuristics.

False positive. An incorrect match or attribution that wrongly links activity, funds, or identities. Aliases: False positive (forensic analysis), incorrect attribution, incorrect match.

Source: 01-FO - Challenges in Forensic Analysis.

Fan-In. A graph motif where value from many sources is gathered into one destination. Aliases: Fan-In (blockchain forensics), fan in, many-to-one flow.

Source: 02-FO - Graph Motif: The "Fan-In".

Fan-in pattern. A transaction graph pattern where many sources converge into one service, wallet, or cluster. Aliases: Fan-in pattern (graph analysis), fan-in, funds pooling.

Source: 01-FO - BTC-e: Weak KYC Made the Cluster Actionable.

Fan-in/fan-out. A transaction graph pattern showing many inputs converging, many outputs dispersing, or both. Aliases: Fan-in/fan-out (forensics pattern), fan-in, fan-out.

Source: 04-AS - Graph Thinking and Heuristics.

Fan-Out. A graph motif where one source distributes value to many destination addresses or accounts. Aliases: Fan-Out (blockchain forensics), fan out, one-to-many flow.

Source: 02-FO - Graph Motif: The "Fan-Out".

FATF standards. International recommendations for applying anti-money-laundering and counter-terrorist-financing controls to virtual assets and their service providers. Aliases: FATF guidance, FATF standards (virtual assets), Financial Action Task Force standards.

Source: 04-BF - Off-Chain Controls: KYC and AML.

Fault isolation. A design property where a failure in one part of a system is contained instead of spreading through the whole service. Aliases: failure isolation.

Source: 01-DS - Why Distribute? Motivations and Risks.

Fault tolerance. A system's ability to keep operating correctly despite component failures or misbehavior. Aliases: Fault tolerance (Bitcoin network), fault tolerance spectrum, network robustness.

Source: 05-IN - Fault Tolerance Spectrum.

Federal Reserve. The central bank of the United States, responsible in this lesson for pursuing price stability and maximum employment. Aliases: Fed, U.S. Federal Reserve.

Source: 04-IN - The Modern Financial Architect: Central Banks.

Fediverse. A collection of independently operated social-network servers that communicate through shared protocols. Aliases: Mastodon, federated social networks.

Source: 05-IN - Everyday Examples of Distributed Systems.

Fedwire. A US Federal Reserve settlement system where dollar payments are finally transferred between participating institutions. Aliases: Fedwire (payment settlement).

Source: 02-AS - Global Payment Infrastructure: Overview.

Fee estimation. The wallet process of estimating an appropriate miner fee so a transaction is likely to be included in a desired time frame. Aliases: Fee estimation (wallet).

Source: 02-BF - What Are Wallets?.

Fee-adjusted amount matching. A correlation technique that matches likely related transfers after accounting for fees, slippage, or service deductions. Aliases: Fee-adjusted amount matching (cross-chain tracing), amount matching, fee-adjusted matching.

Source: 01-FO - Future of Forensics: Automated Cross-Chain Tracing.

Feedback scope. The amount of interaction history behind a rating or reputation score. Aliases: evidence depth, transaction scope.

Source: 03-DS - PeerTrust: How Trust Is Calculated.

Feedback score. A measure of how satisfied peers were with past interactions with a participant. Aliases: satisfaction, satisfaction score.

Source: 03-DS - PeerTrust: How Trust Is Calculated.

Fiat Money. Government-issued money not backed by a physical commodity and sustained by legal decree, policy, and broad acceptance. Aliases: fiat, fiat currency.

Source: 04-IN - A Brief History of Money's Form.

Fiat off-ramp. A service or path used to convert crypto assets into fiat currency or spendable equivalents. Aliases: Fiat off-ramp (crypto laundering), cash-out path, cash-out venue, off-ramp.

Source: 01-FO - Adversarial Counter-Responses to Regulation.

Fiat-collateralized stablecoin. A stablecoin backed by reserves of fiat currency or cash-equivalent assets intended to support redemption at the peg. Aliases: fiat-backed stablecoin, fiat-collateralized.

Source: 02-AS - Stablecoins: Types and Mechanisms.

Finality. The point at which a ledger entry can reasonably be treated as permanent under the consensus model. Aliases: Finality (blockchain settlement), Finality (consensus), Finality (distributed ledgers), finalization, finalized, ledger finality, settlement, transaction finality.

Source: 04-DS - Immutability Source.

Finality (Ethereum). The point at which Ethereum history becomes economically and explicitly irreversible under the Proof-of-Stake consensus rules. Aliases: Finality (Ethereum PoS), Finality (Ethereum consensus), finalization, finalized, finalized block, finalized checkpoint.

Source: 01-EF - PoW vs PoS: Security Model (Review).

Finality delay. A condition where Ethereum continues producing blocks but lacks enough validator participation to finalize checkpoints. Aliases: Finality delay (Ethereum operations), delayed finality, finality stall.

Source: 02-EF - Real-World Ethereum Security Examples.

Finalization. The protocol step that makes a checkpoint and its prior history economically irreversible under the stated assumptions. Aliases: Finalization (PoS finality), finality, finalized checkpoint.

Source: 03-CM - Finalization: Irreversible History.

Finalized checkpoint. A checkpoint treated as economically irreversible because reverting it would require large-scale slashable validator behavior. Aliases: Finalized checkpoint (Ethereum finality), finality, finalized, finalized history.

Source: 02-EF - Gasper: Fork Choice + Finality.

Financial Exclusion. A condition where an actor is denied practical access to banks, payment networks, settlement systems, or related financial services. Aliases: financial isolation, payment exclusion.

Source: 03-AS - Royal Funds Frozen!.

Financial experiment. A way of understanding blockchain as a live environment for new assets, markets, incentives, and failure modes. Aliases: Financial experiment (blockchain), financial substrate.

Source: 05-AS - What Is Blockchain Really?.

Financial inclusion. Expanding access to useful financial services for people or businesses underserved by existing banking systems.

Source: 02-AS - Why Governments Care.

Financial Rail. A payment or settlement pathway through which value moves between participants. Aliases: financial rails, payment rail, settlement rail.

Source: 03-AS - Financial Rails Are Power.

FinCEN guidance. U.S. regulatory guidance explaining how financial-crime rules apply to money services and virtual-asset business models. Aliases: FinCEN guidance (United States), Financial Crimes Enforcement Network guidance.

Source: 04-BF - Off-Chain Controls: KYC and AML.

Finger table. A Chord node's list of shortcut peers used to jump across the ring toward a target identifier. Aliases: Finger table (Chord), finger tables, shortcuts.

Source: 02-DS - DHT Example: Chord.

First Bitcoin transaction. The January 12, 2009 transfer of 10 BTC from Satoshi Nakamoto to Hal Finney. Aliases: First Bitcoin transaction (Bitcoin), Satoshi-to-Hal transaction.

Source: 01-BF - The Network Comes Alive: The First Blocks.

First principles. A learning approach that starts from core concepts and assumptions before moving to complex systems or applications.

Source: 01-IN - Course Overview.

First-spy heuristic. A deanonymization method that treats the first peer observed relaying a transaction as the best guess for its source. Aliases: First-spy heuristic (Bitcoin forensics), first spy, first-spy.

Source: 04-BF - Timing & Latency Attacks.

Fiscal Policy. Government choices about spending and taxation used to influence economic conditions.

Source: 04-IN - The Ideological Divide: Austrian vs. Keynesian Economics.

Fix fingers. A maintenance task where peers refresh shortcut entries that may have become stale after other peers leave or join. Aliases: Fix fingers (Chord maintenance), finger repair, fix_fingers().

Source: 02-DS - The "Self-Healing" Solutions.

Fixed-supply rule. Bitcoin's monetary rule that the protocol should not permit creation beyond its capped supply schedule. Aliases: Fixed-supply rule (Bitcoin), capped supply, supply cap.

Source: 04-BF - Bitcoin Overflow Bug.

Flash Loan. A loan that is borrowed and repaid within a single transaction, often producing a large inflow followed immediately by repayment. Aliases: Flash Loan (DeFi), flash loans.

Source: 02-FO - Smart Contract Forensics.

Flooding. A forwarding pattern where a peer sends a query to all neighbors, who repeat the process until a limit is reached. Aliases: Flooding (P2P routing), Flooding (P2P search), blind broadcast, flood, flooded query, flooding search, query flooding.

Source: 01-DS - Case Study: Gnutella & "Flooding".

FLP result. The result that deterministic consensus cannot guarantee both safety and liveness in full asynchrony if even one node may fail. Aliases: FLP impossibility, Fischer-Lynch-Paterson result.

Source: 01-CM - The Timing Limits — FLP and DLS Results.

Foreign exchange. The exchange of one currency for another, especially in cross-border payment and settlement workflows. Aliases: FX.

Source: 02-AS - mBridge So Far.

Foreign Reserves. State-held external assets used to support currency stability, international payments, and crisis response. Aliases: international reserves, reserve assets.

Source: 03-AS - Royal Funds Frozen!.

ForensiBlock. An academic framework for enterprise or consortium blockchains that embeds provenance and auditability into the consensus layer.

Source: 01-FO - Future of Forensics: ForensiBlock & the Design Trade-off.

Forensic analysis. The investigation of blockchain activity, artifacts, and transaction patterns to support analysis or attribution. Aliases: Forensic analysis (blockchain), blockchain forensics, forensics.

Source: 01-IN - Course Structure.

Forensic substrate. The persistent, signed, timestamped transaction record that supports later tracing and analysis. Aliases: Forensic substrate (blockchain), auditable financial record.

Source: 06-EF - Analyst Implications.

ForensiCross. A research system described in the lesson for privacy-preserving collaboration across agencies holding overlapping wallet evidence.

Source: 01-FO - Future of Forensics: Secure Cross-Agency Collaboration.

Forged withdrawal request. A withdrawal command that appears valid to a bridge because attackers possess enough required approvals, even though the request is unauthorized. Aliases: Forged withdrawal request (bridge security), forged withdrawal.

Source: 01-FO - Ronin: Key Management.

Fork. A divergence where separated parts of a blockchain network extend different versions of the chain. Aliases: Fork (Bitcoin), Fork (Ethereum PoS), Fork (blockchain partition), blockchain fork, competing branch, competing valid blocks, short-term fork, temporary fork.

Source: 02-DS - The Blockchain Link.

Fork choice. The protocol logic nodes use to choose the current best chain head among competing valid branches. Aliases: Fork choice (Ethereum), fork-choice rule, head selection.

Source: 02-EF - Forks in Proof of Stake — Causes and Resolution.

Fork choice rule (Proof of Stake). The deterministic rule nodes use to choose the current chain head among competing viable branches. Aliases: Fork choice rule (PoS consensus), fork choice, fork-choice rule, fork-choice rules.

Source: 03-CM - Fork Choice Rules.

Fork race. A competition between competing valid branches where whichever branch spreads and gains work faster becomes the accepted history. Aliases: Fork race (proof of work), fork-race win, race between branches.

Source: 04-BF - Selfish Mining.

Fork-choice state. The consensus client's view of the current head, safe, and finalized blocks used to guide chain selection. Aliases: Fork-choice state (Ethereum consensus), fork choice.

Source: 03-EF - Two Networks, One Chain.

Formal verification. The use of mathematical methods to prove that code satisfies specified properties or rules. Aliases: Formal verification (smart contracts).

Source: 04-EF - Beyond Ethereum: Other Smart Contract Models.

Formalization. Movement from informal or lightly governed activity into licensed, recognized, and supervised channels. Aliases: formal integration, regulatory formalization.

Source: 03-AS - Sub-Saharan Africa: Overview.

FPIC. A blockchain-oriented vocabulary that maps closely to safety, liveness, validity, and agreement. Aliases: finality, progress, integrity, consistency.

Source: 01-CM - Consensus Properties: SLVA and FPIC.

Fractionalization. Dividing exposure to an asset into smaller tokenized units that can be owned or traded separately. Aliases: Fractionalization (tokenization), fractional ownership.

Source: 05-EF - Why Tokenize? Problems and Promises.

Fragmentation. The splitting of users, assets, standards, and infrastructure across many partially incompatible chains or platforms. Aliases: Fragmentation (crypto ecosystem), ecosystem fragmentation, market fragmentation.

Source: 01-AS - Complications and Risks.

Fragmented adoption. A future where blockchain use survives unevenly across isolated sectors, regions, or communities without one coherent ecosystem. Aliases: Fragmented adoption (blockchain futures), constrained adoption, fragmentation.

Source: 05-AS - A Spectrum of Futures.

Fragmented Oversight. A regulatory condition where several agencies or institutions share authority without one unified rulemaking center. Aliases: fragmented regulation, fragmented supervision.

Source: 03-AS - United States: Overview.

Fraud detection and monitoring. Using models and transaction analysis to identify suspicious flows, risky patterns, or possible abuse in blockchain activity. Aliases: Fraud detection and monitoring (blockchain analytics), fraud monitoring, transaction monitoring.

Source: 05-AS - Opportunities.

Fraud proof. Evidence submitted during a dispute window to show that an optimistic rollup's claimed state transition was incorrect. Aliases: Fraud proof (Layer 2 verification), Fraud proof (optimistic rollup), challenge, fraud proofs.

Source: 01-EF - L2 Operator Models.

Free identity. The condition in an open P2P network where creating new peer identities has little or no cost. Aliases: Free identity (P2P security), cheap identity, identity is free.

Source: 02-DS - The Great P2P Weakness: Sybil & Eclipse Attacks.

Friends With Benefits. A Web3-focused social DAO where application review and FWB token ownership gate membership spaces and participation. Aliases: FWB, Friends With Benefits (social DAO).

Source: 06-EF - Case Study: Friends With Benefits.

Frosties. An NFT project whose January 2022 sellout raised about $1.1 million before operators abandoned the project and drained proceeds. Aliases: Frosties (rug pull case study).

Source: 06-EF - The Frosties Rug Pull.

Full node. A blockchain node that downloads and validates every transaction and block, often serving data to weaker peers. Aliases: Full node (blockchain network), full nodes, validating node.

Source: 01-DS - The Blockchain Link.

Full node (Bitcoin). A Bitcoin node that independently enforces validity rules and rejects invalid transactions or blocks. Aliases: Full node (Bitcoin network), full nodes, full validating node, node.

Source: 01-BF - Security Model & Threats.

Full node (Ethereum). An Ethereum node that runs execution and consensus clients, stores current state, and verifies every new block. Aliases: full node.

Source: 03-EF - Nodes and Clients.

Full sync. A synchronization mode that replays blocks from genesis to independently derive current chain state. Aliases: Full sync (Ethereum), full synchronization.

Source: 03-EF - Sync Modes & Data Availability.

Full validation. Verification of the entire relevant transaction and block history under Bitcoin consensus rules. Aliases: Full validation (Bitcoin).

Source: 03-BF - Types of Nodes.

Fully Homomorphic Encryption. Encryption that lets a system compute directly on encrypted data and later decrypt the result to the same answer as a plaintext computation. Aliases: FHE, fully-homomorphic encryption.

Source: 05-CP - Fully Homomorphic Encryption (FHE).

Function. A rule that maps each input from one set to one output in another set. Aliases: Function (mathematics), functions.

Source: 01-CP - Sets and Functions.

Function modifier. A Solidity construct used to add reusable checks or behavior around function execution. Aliases: Function modifier (Solidity), modifier, modifiers.

Source: 04-EF - Solidity: File Structure, From Top to Bottom.

Function mutability. A function annotation that communicates whether a function may read contract state, write contract state, or avoid state entirely. Aliases: Function mutability (Solidity), mutability, pure, view.

Source: 04-EF - Visibility, Mutability, and Payable.

Function selector. The first four bytes of the keccak-256 hash of a function signature, used to route calldata to the intended function. Aliases: 4-byte selector, Function selector (Ethereum ABI), selector.

Source: 04-EF - ABI, Encoding, and Function Selectors.

Function signature. The canonical function name and parameter-type string that is hashed to derive a function selector. Aliases: Function signature (Ethereum ABI), name(types).

Source: 04-EF - ABI, Encoding, and Function Selectors.

Function visibility. A function or variable annotation that controls whether code can be accessed externally, internally, by derived contracts, or only within the same contract. Aliases: Function visibility (Solidity), external, internal, private, public, visibility.

Source: 04-EF - Visibility, Mutability, and Payable.

Fungible token. A token type where each unit is interchangeable with any other unit of the same asset. Aliases: ERC-20 token, ERC-20 tokens, Fungible token (tokenization), fungible tokens.

Source: 05-EF - A Taxonomy of Digital Assets.

G

Galois/Counter Mode. A modern mode that combines CTR-style encryption with an authentication tag. Aliases: AES-GCM, GCM.

Source: 03-CP - Modes of Operation Overview.

Gas (Ethereum). The unit Ethereum uses to measure and charge for computation, storage, and other EVM operations. Aliases: Gas (Ethereum execution), Gas (Ethereum resource unit), gas metering.

Source: 01-EF - Gas: Metering Computation and Storage.

Gas budget. The amount of gas available to a call frame before execution fails from running out of gas. Aliases: Gas budget (EVM call frame), available gas.

Source: 04-EF - Calls and Control Flow in the EVM.

Gas estimation. Simulated execution used to predict how much gas a transaction is likely to consume. Aliases: Gas estimation (Ethereum), estimated gas.

Source: 03-EF - Gas Strategy and UX.

Gas limit. A cap on how much gas a transaction or block may consume. Aliases: Gas limit (Ethereum transaction), Gas limit (Ethereum), block gas limit, gasLimit, gas_limit, transaction gas limit.

Source: 01-EF - Gas: Metering Computation and Storage.

Gas metering. The EVM rule that charges gas for operations so contract execution consumes bounded network resources. Aliases: Gas metering (EVM), Gas metering (Ethereum), gas-metered computation, metering computation.

Source: 01-EF - The Ethereum Virtual Machine (EVM).

Gasper. Ethereum's consensus protocol combining LMD-GHOST fork choice with Casper-FFG finality. Aliases: Ethereum full consensus protocol, Gasper (Ethereum consensus).

Source: 02-EF - Gasper: Fork Choice + Finality.

Gateway control. A regulatory strategy that shapes use by constraining exchanges, custodians, liquidity, or access points rather than changing a protocol. Aliases: Gateway control (regulation), access constraint, gateway constraint.

Source: 04-BF - Regulatory Pressure Beyond Bitcoin.

Genesis Block. The first Bitcoin block, mined by Satoshi Nakamoto on January 3, 2009. Aliases: Block 0, Genesis Block (Bitcoin), genesis block.

Source: 01-BF - The Network Comes Alive: The First Blocks.

GENIUS Act. The 2025 U.S. framework establishing a federal path for regulated payment stablecoins.

Source: 03-AS - United States: Impact Signals.

getdata message. A Bitcoin protocol message used to request full data for an announced transaction or block. Aliases: getdata, getdata message (Bitcoin protocol).

Source: 03-BF - Communication Protocol Basics.

Getter. A read function that returns contract state, sometimes generated automatically for public state variables. Aliases: Getter (Solidity), auto-generated getter, getter function.

Source: 04-EF - Example: SimpleStorage (Code).

Gitcoin. A Web3 funding ecosystem that uses grants, matching pools, and token governance to support open-source and public-goods work. Aliases: GTC, Gitcoin (public-goods DAO).

Source: 06-EF - Case Study: Gitcoin.

Global coordination. Cooperation across agencies, countries, and private firms to share intelligence and pursue actors who operate across borders. Aliases: Global coordination (crypto regulation), international coordination, public-private partnership.

Source: 01-FO - Policy & Regulatory Response.

Global settlement layer. A blockchain-based or blockchain-inspired layer for settling payments, tokenized claims, and financial obligations across institutions. Aliases: shared settlement system.

Source: 05-AS - Future 1: Global Settlement Layer.

Global state. The shared Ethereum record of account balances, nonces, code, and storage after accepted transactions are applied. Aliases: Ethereum state, Global state (Ethereum), shared global state.

Source: 01-EF - Accounts & Global State (EOA vs Contract).

Global trust vector. The final EigenTrust score set in which each entry represents a peer's global reputation. Aliases: global reputation vector, trust vector.

Source: 03-DS - EigenTrust: From Local Opinions to Global Scores.

Gnutella. An early decentralized P2P file-sharing network that searched by forwarding queries through peers instead of using a central index. Aliases: Gnutella (case study).

Source: 01-DS - Case Study: Gnutella & "Flooding".

Gold-Exchange Standard. A monetary arrangement where currencies are linked to a reserve currency that is itself convertible into gold.

Source: 04-IN - The Turning Point: Ending Bretton Woods.

Gossip. A propagation method where nodes forward new transactions or blocks to a small set of peers, who validate and relay them onward. Aliases: Gossip (P2P propagation), Gossip (blockchain network), controlled flood, gossip protocol, gossiping.

Source: 01-DS - Gossip in a Blockchain Network.

Gossip membership. A maintenance technique where peers exchange small samples of known peers to keep neighbor lists fresh. Aliases: membership gossip, peer-list gossip.

Source: 02-DS - The P2P Playbook: Surviving Churn.

Gossip protocol. A propagation method where each node forwards valid messages to neighboring peers until information spreads through the network. Aliases: Gossip protocol (Bitcoin network), gossip, peer relay.

Source: 02-IN - Pillar 2: Peer-to-Peer Networks.

Gossip relay. A dissemination pattern where peers forward new transactions or blocks broadly through neighbor-to-neighbor communication. Aliases: Gossip relay (P2P networking), gossip, gossip propagation, unstructured relay.

Source: 04-AS - Gossip vs DHTs.

Gossip topic. A named message channel in GossipSub for a class of consensus messages such as blocks or attestations. Aliases: Gossip topic (Ethereum consensus layer), topic, topics.

Source: 03-EF - Consensus-Layer Networking (libp2p / GossipSub).

GossipSub. A topic-based gossip protocol used by Ethereum consensus clients to disseminate blocks, attestations, and other messages. Aliases: GossipSub (Ethereum consensus layer), gossipsub.

Source: 03-EF - Block Production: Anatomy of a Slot.

Governance. The rules and institutions that decide membership, upgrades, dispute handling, and who can change the system. Aliases: Governance (distributed ledgers), decision rights, ledger governance.

Source: 04-DS - Distributed Ledger vs. Centralized Database (Compare/Contrast).

Governance boundary. The line around decisions that can change members, rules, thresholds, configuration, or upgrade behavior. Aliases: governance security boundary.

Source: 01-PC - Governance Boundary.

Governance committee. The authorized group that votes or decides on network changes according to the permissioned system's policy. Aliases: Governance committee (permissioned ledger), authorized governance members.

Source: 01-PC - Governance Actions.

Governance coordination. The social process of reaching agreement on protocol changes, upgrades, or responses to system problems. Aliases: Governance coordination (blockchain protocols), coordination and agreement, protocol coordination.

Source: 05-AS - Human & Economic Constraints.

Governance manipulation. Attempts to distort protocol decisions through bribery, messaging, voting strategies, or other pressure on governance processes. Aliases: Governance manipulation (token-governed systems), governance attack, voting manipulation.

Source: 05-AS - Risks.

Governed membership. A participation model where admission, authorization, and membership changes are handled by governance outside the voting protocol. Aliases: controlled membership, known participants.

Source: 01-CM - Byzantine-Fault Tolerance (BFT).

Graceful degradation. A failure-handling approach where a system keeps providing reduced service instead of collapsing completely.

Source: 01-DS - Why Distribute? Motivations and Risks.

graffiti. An optional 32-byte metadata field in a beacon block. Aliases: graffiti (beacon block field), graffiti field.

Source: 02-EF - Beacon Blocks and Execution Payloads.

Graph Analysis. The practice of modeling on-chain actors and value flows as nodes and edges to detect patterns of control and movement. Aliases: Graph Analysis (blockchain forensics), graph thinking, transaction graph analysis.

Source: 02-FO - The Analyst's Mindset: Graph Thinking.

Graph Motif. A recurring graph shape that suggests a possible behavior, service role, or laundering tactic. Aliases: Graph Motif (blockchain forensics), motif, transaction pattern.

Source: 02-FO - The Analyst's Mindset: Graph Thinking.

Great Inflation. The high and volatile inflation period from about 1965 to 1982 highlighted as a post-Bretton Woods policy stress.

Source: 04-IN - The Problem of Value: The Specter of Inflation.

Greedy routing. A forwarding rule that sends a query to the neighboring zone that appears closest to the target coordinate. Aliases: Greedy routing (CAN), greedy walk.

Source: 02-DS - DHT Example: CAN.

Grover's Algorithm. A quantum search algorithm that gives a quadratic speedup for unstructured search problems. Aliases: Grover's algorithm.

Source: 05-CP - Grover's Algorithm (1996).

Gwei. A common subunit of Ether, where one ETH equals one billion gwei. Aliases: Gwei (Ether unit).

Source: 01-EF - The Ethereum Virtual Machine (EVM).

H

Halting Problem. The undecidable problem of determining whether any arbitrary program will eventually stop or run forever. Aliases: Halting Problem (computation).

Source: 01-EF - The Halting Problem.

Halving. The scheduled event that cuts Bitcoin's block subsidy in half every 210,000 blocks, roughly every four years. Aliases: Halving (Bitcoin monetary policy), Halving (Bitcoin), halvings, reward halving, subsidy halving.

Source: 01-BF - Monetary Policy.

Hard fork. An incompatible protocol change that can split a network into separate chains if different groups keep following different rules. Aliases: DAO fork, Hard fork (Ethereum governance), Hard fork (blockchain governance), Hard fork (blockchain protocol), Hard fork (governance), chain split, fork, hard-fork split, network split, protocol fork.

Source: 04-DS - Governance Models.

Hard Money. Money with a difficult-to-expand and predictable supply, often contrasted with discretionary fiat currency.

Source: 04-IN - The Problem of Value: The Specter of Inflation.

Hardware security module. A dedicated device or service designed to protect private keys and perform cryptographic operations without exposing raw key material. Aliases: HSM, HSMs.

Source: 05-CP - Case Study: CryptoDefense — Keys Left in Plain Sight.

Hardware wallet. A device that stores cryptocurrency private keys separately from general-purpose computers and signs transactions without exposing the key. Aliases: hardware wallets.

Source: 05-CP - Case Study: CryptoDefense — Keys Left in Plain Sight.

Harvest Now, Decrypt Later. An attack strategy where encrypted data is collected today so it can be decrypted later if future cryptanalytic or quantum advances break its protection. Aliases: HNDL, Harvest Now, Decrypt Later (privacy coin forensics), harvest-now-decrypt-later.

Source: 05-CP - Quantum Primer: Why It Matters for Cryptography.

Hash anchor. A hash recorded on the shared channel so peers can verify that private data has not been silently changed. Aliases: Hash anchor (private data), hash anchoring, integrity anchor.

Source: 02-PC - Private Data Collections.

Hash collision. A case where two distinct inputs produce the same hash digest. Aliases: collision, collisions.

Source: 02-CP - What Is a Cryptographic Hash Function?.

Hash commitment. A published digest that binds someone to underlying data while allowing the data to remain hidden until later disclosure. Aliases: commitment, hashing as commitment.

Source: 02-CP - Hashing as Commitment.

Hash function. A function that maps data to a compact value used to identify data and detect changes. Aliases: cryptographic hashing, hash functions, hashing.

Source: 01-CP - Sets and Functions.

Hash pointer. A hash reference in a block header that points to the previous block and links the chain together. Aliases: Hash pointer (Bitcoin), previous block hash, previous block header hash.

Source: 02-BF - The Data Structure of a Block.

Hash power. The amount or share of proof-of-work computation controlled by a miner, pool, or network. Aliases: Hash power (proof of work), hash rate, hash share, mining power.

Source: 04-BF - Selfish Mining.

Hash puzzle. A PoW puzzle where miners search for a nonce so the hash of candidate data falls below a target. Aliases: hash-based puzzle.

Source: 02-CM - Proof-of-work Puzzles.

Hash rate. The number of hash attempts miners can perform per second, either individually or across the whole network. Aliases: H, network hash rate.

Source: 02-CM - Difficulty, Hash Rate, and Expected Work.

Hash Time-Locked Contract. A contract pattern that locks funds behind a hash preimage and a timeout so cross-chain swap participants can claim or refund funds. Aliases: HTLC, HTLCs.

Source: 01-FO - Bridges & Swaps: Crossing the Chain Boundary (cont.).

Hash-based cryptography. A post-quantum approach, especially for signatures, that builds security from hash-function assumptions. Aliases: Hash-based cryptography (post-quantum), hash-based signatures.

Source: 05-CP - Post-Quantum Cryptography: The New Toolbox.

Hash-chaining. A chain of hashes where each later entry depends on earlier data, causing past edits to break later links. Aliases: Hash-chaining (immutability source), hash chain, hash-chained history.

Source: 04-DS - Immutability Source.

Hash-linked chain. A sequence of blocks where each block includes the hash of the previous block, making earlier changes visible and costly to repair. Aliases: Hash-linked chain (Bitcoin), chain, cryptographically linked chain.

Source: 01-BF - How Double-Spending is Solved.

Hash-linking. A structure where each entry commits to the previous entry with a hash so later history depends on earlier contents. Aliases: Hash-linking (distributed ledgers), cryptographic linking, cryptographic links, hash linking.

Source: 04-DS - From Logs to Ledgers.

Hashcash. An anti-spam system that used computational work to make abuse costly and later influenced Bitcoin's Proof-of-Work design.

Source: 03-IN - Framing.

Hashing. A cryptographic process that turns data into a fixed-size value used to identify, compare, and protect information. Aliases: hash.

Source: 01-IN - Learning Objectives I.

Heaviest chain. The valid chain with the most accumulated proof-of-work, used as the surviving history in Nakamoto-style consensus. Aliases: Heaviest chain (Proof-of-Work), most-work chain.

Source: 01-CM - Why Consensus Matters in Blockchains.

Helium. A decentralized wireless network built from individual hotspots that provide connectivity over unlicensed radio frequencies. Aliases: Helium (IoT network).

Source: 05-IN - Everyday Examples of Distributed Systems.

Heterogeneity. The normal condition that network participants differ in hardware, software, operating systems, and connection quality. Aliases: Heterogeneity (distributed systems), heterogeneous network, heterogeneous nodes.

Source: 01-DS - Fallacy #8: The Network Is Homogeneous.

Heuristic. An evidence-based rule of thumb used to infer likely relationships or behavior when direct proof is unavailable. Aliases: Heuristic (forensic analysis), Heuristic (forensics), forensic heuristic, heuristics, inference rule, rule of thumb.

Source: 01-FO - Challenges in Forensic Analysis.

Hidden infrastructure. The services users usually do not see, such as RPC providers, nodes, indexers, oracles, bridges, and scaling layers. Aliases: Hidden infrastructure (blockchain applications), behind-the-scenes infrastructure, supporting infrastructure.

Source: 01-AS - What Users Actually Do.

Hierarchical trust. A trust model where authority flows downward from a root authority to intermediaries and users. Aliases: hierarchical trust model.

Source: 02-AS - Trust Architecture: CBDCs vs Permissionless Systems.

Hivemapper. A decentralized mapping network where contributors collect imagery to update a shared global map. Aliases: Hivemapper (mapping network).

Source: 05-IN - Everyday Examples of Distributed Systems.

HMAC. A standard hash-based MAC construction that uses inner and outer keyed hashes to authenticate messages safely. Aliases: Hash-based Message Authentication Code, hash-based message authentication code.

Source: 02-CP - Aside: HMAC.

Holder. The party that stores a verifiable credential and presents it when proof is needed. Aliases: Holder (verifiable credentials), credential holder.

Source: 01-AS - Identity Case: Verifiable Credentials.

Homomorphic encryption. Encryption that allows computation on encrypted data without first decrypting it. Aliases: FHE, fully homomorphic encryption.

Source: 04-DS - Transparency vs. Privacy.

Homomorphic evaluation. The operation of applying a function to ciphertexts so the encrypted output corresponds to the function's plaintext result. Aliases: Eval, homomorphic Eval.

Source: 05-CP - FHE at a Glance.

Honest supermajority. An assumption that enough stake follows the protocol, commonly two-thirds or more for finality decisions. Aliases: Honest supermajority (PoS assumption), honest 2/3 stake, honest majority.

Source: 03-CM - Safety and Liveness — PoS Invariants.

Honest work. Proof-of-work contributed by miners following the protocol, which Bitcoin assumes outweighs attacker work. Aliases: Honest work (Bitcoin security), honest majority work, majority of honest work.

Source: 01-BF - Security Model & Threats.

Hot wallet. A cryptocurrency wallet whose private keys are kept on an internet-connected system for operational use. Aliases: Hot wallet (exchange forensics), central hot wallet, exchange hot wallet, hot wallets.

Source: 05-CP - Case Study: CryptoDefense — Keys Left in Plain Sight.

Hub-Building. Attracting firms, capital, and infrastructure to make a jurisdiction a regional or global center. Aliases: crypto hub-building, regulated hub-building.

Source: 03-AS - Gulf States: Overview.

Hybrid architecture. A CBDC design that combines multiple technical approaches, such as centralized components and distributed ledger components, within one controlled system. Aliases: Hybrid architecture (CBDC), hybrid CBDC architecture.

Source: 02-AS - CBDC Technical Platforms.

Hybrid cryptographic system. A transition design that combines existing cryptography with post-quantum methods to reduce migration risk. Aliases: Hybrid cryptographic system (quantum transition), hybrid cryptographic systems, hybrid cryptography.

Source: 05-AS - What Can Be Done.

Hybrid cryptosystem. A design that uses asymmetric cryptography to establish trust or keys and symmetric cryptography for fast bulk encryption. Aliases: hybrid cryptographic system, hybrid system.

Source: 04-CP - Symmetric vs Asymmetric Comparison.

Hybrid P2P model. A design that combines centralized services such as indexing or login with direct peer-to-peer data transfer. Aliases: hybrid peer-to-peer model.

Source: 01-DS - Case Study: Napster.

Hybrid Posture. A strategy combining market participation with deliberate state steering, taxation, supervision, and constraints. Aliases: state-guided hybrid posture.

Source: 03-AS - India: Overview.

Hybrid signature. A migration technique that combines a classical signature with a post-quantum signature so both protections can be checked during rollout. Aliases: Hybrid signature (post-quantum migration), hybrid deployment, hybrid signatures.

Source: 05-CP - PQC Migration in Blockchain Systems.

Hybrid trust. A trust model where centralized issuer powers coexist with permissionless network participation. Aliases: Hybrid trust (stablecoin), stablecoin hybrid.

Source: 02-AS - Trust Architecture: The Stablecoin Hybrid.

Hybrid trust system. A design that combines a global reputation baseline with local, context-aware personalization. Aliases: hybrid design.

Source: 03-DS - PeerTrust vs. EigenTrust: Summary.

Hyperledger. A family of enterprise-oriented blockchain technologies often associated with permissioned network designs. Aliases: Hyperledger (blockchain framework).

Source: 01-IN - Course Structure.

Hyperledger Fabric. A permissioned blockchain framework named as an example of restricted enterprise or consortium participation. Aliases: Fabric, HLF, Hyperledger Fabric (permissioned ledger platform), Hyperledger Fabric (permissioned ledger).

Source: 02-IN - The Spectrum of Decentralization.

I

Idempotent operation. An operation that can be safely repeated without causing duplicate or unintended effects. Aliases: idempotency, idempotent operations.

Source: 01-DS - Fallacy #1: The Network Is Reliable.

Identity and membership. The mechanisms that establish who a participant is and what standing they have in the network. Aliases: membership identity.

Source: 01-PC - Key Components.

Identity check. The step that verifies a requester has a valid credential and role before a request can proceed. Aliases: Identity check (transaction path), credential check, role check.

Source: 01-PC - Transaction Path.

Identity model. The protocol assumption about who can participate and how participants are recognized. Aliases: Identity model (consensus), membership model.

Source: 01-CM - Crash-Fault Tolerance (CFT).

Identity theft risk. The risk created when a stolen identity grants an attacker the permissions attached to that role. Aliases: Identity theft risk (permissioned ledger), identity compromise risk.

Source: 01-PC - Identity Theft Risks.

Identity verification. The repeated process of checking that a Fabric action is backed by a valid identity and a signature that satisfies the relevant policy. Aliases: Identity verification (Hyperledger Fabric), identity check, signature verification.

Source: 02-PC - The Big Picture: End-to-End Fabric Path.

Immutability. The practical resistance of accepted blockchain history to unnoticed revision because later blocks depend on earlier hashes. Aliases: Immutability (Ethereum contracts), Immutability (blockchain), Immutability (distributed ledgers), contract immutability, immutable, immutable contract, immutable history, strict immutability.

Source: 02-IN - Step 6: Chaining the Block.

Immutable chain. A hash-linked history where changing an earlier block would require changing later references and rebuilding later proof-of-work. Aliases: Immutable chain (Bitcoin), tamper-evident chain.

Source: 02-BF - Linking Blocks into a Chain.

Immutable code. Deployed contract logic that cannot be altered in place without a separate upgrade mechanism or replacement deployment. Aliases: Immutable code (smart contracts), deployed immutable contract code.

Source: 01-FO - Ronin: Legal Battles.

Immutable ledger. A replicated blockchain record that is very difficult to alter retroactively once transactions are widely confirmed. Aliases: Immutable ledger (blockchain forensics), permanent public record, public ledger.

Source: 01-FO - The Immutable Ledger.

Implementation bug. A flaw in the code that enforces a protocol, even when the abstract design rule is sound. Aliases: implementation flaw, software bug.

Source: 04-BF - Implementation vs. Design.

Improvement proposal. A formal proposal for changing a permissionless protocol, such as a Bitcoin Improvement Proposal or Ethereum Improvement Proposal. Aliases: BIP, BIPs, EIP, EIPs, Improvement proposal (permissionless governance).

Source: 04-DS - Governance Models.

Inactivity leak. A mechanism that gradually reduces the balances of offline validators during extended non-participation so the chain can recover liveness. Aliases: Inactivity leak (Ethereum PoS), Inactivity leak (Ethereum finality recovery), Inactivity leak (PoS penalty), inactivity leak mechanism, inactivity leak penalty, inactivity penalty.

Source: 03-CM - Nothing-at-Stake and Economic Security.

Incentive. A reward or cost structure that encourages participants to behave in ways that support the system. Aliases: Incentive (information sources), Incentive (network design), economic incentives, incentives, source incentive.

Source: 03-IN - P2P Normalizes Decentralization.

Incentive design. The design of rewards, penalties, governance rights, and market pressures that shape participant behavior. Aliases: Incentive design (blockchain systems), incentives shape outcomes.

Source: 05-AS - Key Lessons.

Incentives. Protocol rewards and fees that make honest block production more profitable than attacking or abandoning the system. Aliases: Incentives (Bitcoin security), economic incentives, miner incentives.

Source: 01-BF - Bitcoin, Simplified.

Inclusion list. A proposed mechanism for requiring proposers to include specified pending transactions. Aliases: Inclusion list (Ethereum censorship mitigation), inclusion lists.

Source: 02-EF - Censorship.

Inclusion proof. A short set of sibling hashes that lets a verifier confirm an item is included under a known Merkle root. Aliases: Inclusion proof (Merkle tree), Merkle proof, lightweight client proof, membership proof.

Source: 04-AS - Why the Merkle Root Matters.

Independence. A relationship where the outcome of one event does not change the probability of another event. Aliases: Independence (probability), independent events.

Source: 01-CP - Probability Refresher: Independence & Random Variables.

Independent validation. The practice of checking transactions and blocks against Bitcoin rules on one's own node instead of trusting another party. Aliases: Independent validation (Bitcoin), local validation.

Source: 03-BF - What Is a Bitcoin Node?.

Independent verification. The ability for participants to check the record and its changes for themselves rather than trusting another party's private assertion. Aliases: Independent verification (distributed ledgers), independently verifiable, verification.

Source: 04-DS - The Shared Notebook Problem.

Indexed field. An event parameter stored as a log topic so off-chain clients can search or filter by it. Aliases: Indexed field (Solidity event), indexed, indexed parameter.

Source: 04-EF - Events and Logs.

Indexer. An off-chain service that reads blockchain data and organizes it for search, display, analytics, or application use. Aliases: Indexer (blockchain application), Indexer (blockchain data), indexers, indexing service.

Source: 05-EF - System Architecture — Where Everything Lives.

Indictment. A formal criminal charge issued after investigators and prosecutors assemble a legally supportable theory of the case. Aliases: Indictment (legal process), criminal charge.

Source: 01-FO - BTC-e: Indictment.

Indirect trust. Trust extended through recommendations from other peers rather than through personal experience. Aliases: hearsay, recommendation-based trust.

Source: 03-DS - Direct vs. Indirect Trust.

Indistinguishability. A property where no efficient algorithm can reliably tell one distribution, such as PRG output, from another, such as true randomness. Aliases: Indistinguishability (cryptography), computational indistinguishability, indistinguishable.

Source: 01-CP - Probability Refresher: Events and Outcomes.

Inflation. A rise in general prices that reduces a currency's purchasing power.

Source: 04-IN - The Problem of Value: The Specter of Inflation.

Inflation hedging. Using a stablecoin or other asset to preserve purchasing power when a local currency is rapidly losing value. Aliases: Inflation hedging (stablecoin), inflation hedge.

Source: 02-AS - Major Stablecoins and Use Cases.

Information Asymmetry. A situation where one side of a transaction knows more about quality or risk than the other side.

Source: 04-IN - The "Market for Lemons": When Trust Breaks Down.

Information isolation. A condition where each participant sees only the messages sent directly to them rather than the whole system view.

Source: 05-IN - Byzantine Generals Problem.

Infrastructure centralization. A concentration of important network services in a small number of operators or implementations. Aliases: Infrastructure centralization (Ethereum security), builder centralization, relay centralization.

Source: 02-EF - Censorship.

Infrastructure chokepoint. A concentrated dependency where many users or apps rely on one provider, creating availability, censorship, or visibility risk. Aliases: centralized dependency, chokepoint, service dependency.

Source: 01-AS - RPC Providers: The Access Layer.

Infrastructure concentration. A condition where users, applications, or value rely heavily on a small number of providers, keys, bridges, or data feeds. Aliases: concentrated infrastructure.

Source: 06-EF - Centralization Chokepoints.

Infrastructure-scale adoption. A future where blockchain-style systems become part of major settlement, payment, and institutional infrastructure. Aliases: Infrastructure-scale adoption (blockchain futures), global infrastructure, infrastructure-scale blockchain adoption.

Source: 05-AS - A Spectrum of Futures.

Initcode. The contract creation code executed during deployment, including constructor logic, before returning runtime bytecode. Aliases: Initcode (Ethereum), init code, initialization code.

Source: 04-EF - Contract Deployment.

Initial block download. The first synchronization process in which a full node downloads and verifies blockchain history from the beginning. Aliases: IBD, Initial block download (Bitcoin).

Source: 03-BF - Setting Up a Full Node.

Initial Coin Offering bubble. A period of speculative token fundraising in which many projects raised money without durable products or value. Aliases: ICO bubble, ICO speculation.

Source: 05-AS - When Blockchain Systems Broke.

Initialization vector. A public value supplied with ciphertext so repeated plaintexts encrypt differently under modes that require freshness. Aliases: IV.

Source: 03-CP - Padding and Initialization Vectors.

Insider. A participant who appears to belong to the group but secretly acts against the group's shared objective. Aliases: Insider (adversarial participant), malicious insider.

Source: 05-IN - Opening Exercise: The Insider.

Institutional control. The influence of banks, firms, regulators, exchanges, and other organized actors over how blockchain systems are used and governed. Aliases: Institutional control (blockchain adoption), control and regulation, institutional adoption.

Source: 05-AS - What Actually Happened.

Institutional phenomenon. The way blockchain affects organizations, markets, governance, and trust relationships beyond its code. Aliases: Institutional phenomenon (blockchain).

Source: 01-IN - Course Overview.

Institutional skepticism. A cautious or critical view from regulators and financial institutions that blockchain may offer limited net benefit or unacceptable risk. Aliases: Institutional skepticism (blockchain adoption), skeptical institutional critique.

Source: 05-AS - Future 3: Decline or Fragmentation.

Institutional Trust. Confidence that financial institutions, regulators, and intermediaries are accurately managing risk and honoring obligations.

Source: 04-IN - Case Study: The 2008 Global Financial Crisis.

Integer factorization. The problem of recovering the prime factors of a composite number. Aliases: Integer factorization (public-key cryptography), factor large integers, factoring, factorization.

Source: 04-CP - Computational Hardness Assumptions.

Integer overflow. A programming error where a number exceeds the range a field can represent and wraps into an unintended value. Aliases: Integer overflow (software implementation), overflow.

Source: 04-BF - Bitcoin Overflow Bug.

Integrity. A security property that lets users detect whether data or messages have been changed. Aliases: Integrity (distributed ledgers), data integrity, message integrity.

Source: 01-CP - What Is Cryptography?.

Intellectual property. Legal rights over creative or informational works that are separate from control of a blockchain token. Aliases: IP, IP rights, Intellectual property (NFT rights), copyright.

Source: 05-EF - NFTs: What Are We Actually Buying?.

Intelligence Fusion. Combining multiple evidence streams to produce a stronger conclusion than any one source could support alone. Aliases: Intelligence Fusion (blockchain attribution), evidence fusion, multi-source fusion.

Source: 02-FO - Attribution: From Cluster to Identity.

Interactive consistency. A Byzantine agreement goal requiring loyal actors to reach the same plan despite faulty or malicious actors.

Source: 05-IN - The Byzantine Generals Problem (formal).

Interference. The quantum effect algorithms use to amplify useful answers and suppress wrong paths in certain computations. Aliases: Interference (quantum computing), quantum interference.

Source: 05-CP - Quantum Primer: Why It Matters for Cryptography.

Intermediary. A middle party such as a bank, card network, government, exchange, or platform that helps verify and enforce a transaction. Aliases: intermediaries, trusted middle party, trusted third parties, trusted third party.

Source: 03-IN - Digital Trust: The Centralized Model.

Intermediate CA. A Certificate Authority authorized by a higher CA to issue certificates below it in the hierarchy. Aliases: delegated signer, intermediate certificate authority.

Source: 04-CP - Certificates and PKI Hierarchy.

Internal Trace. A record of contract-to-contract execution steps that occur inside a single Ethereum transaction. Aliases: Internal Trace (Ethereum), contract trace, internal call trace, internal transaction trace.

Source: 02-FO - Reminder: Ethereum's Account Model.

Interoperability. The ability of a ledger system to work with external systems, institutions, or standards. Aliases: Interoperability (blockchain systems), Interoperability (ledger design), Interoperability (settlement infrastructure), cross-chain interoperability, external interoperability, interconnected systems, interoperable systems.

Source: 04-DS - Case Study B — Public Sector: EBSI & Estonia (KSI){.smaller}.

InterPlanetary File System. A peer-to-peer storage and sharing network where files are located by cryptographic hash rather than by one central server location. Aliases: IPFS, InterPlanetary File System (NFT storage).

Source: 05-IN - Everyday Examples of Distributed Systems.

Invalid transaction. A transaction that remains in the block log for audit but does not update world state because validation failed. Aliases: Invalid transaction (Hyperledger Fabric), invalidated transaction, marked invalid.

Source: 02-PC - Phase B: Ordering, Validation, and Commit.

Invariant. A condition that should remain true after every valid contract call. Aliases: Invariant (smart contracts), accounting invariant, contract invariant.

Source: 04-EF - Example: Coin (Code, Part 1).

Inventory message. A Bitcoin protocol message used to announce that a node has a transaction or block available. Aliases: Inventory message (Bitcoin network), Inventory message (Bitcoin protocol), inv, inv message, inv(tx).

Source: 03-BF - Communication Protocol Basics.

Invoke. A client-requested transaction flow that proposes a chaincode action, gathers endorsements, submits for ordering, and reaches validation and commit. Aliases: Fabric invoke, Invoke (Hyperledger Fabric), transaction invoke.

Source: 02-PC - One Invoke: Proposal to Commit.

Irreversible history. Blockchain history that cannot be reverted without large-scale slashable validator misconduct. Aliases: Irreversible history (PoS finality), finalized history, irreversibility.

Source: 03-CM - Finalization: Irreversible History.

Irreversible transaction. A transaction that cannot normally be undone once accepted by the network. Aliases: Irreversible transaction (blockchain risk), irreversible settlement, irreversible transactions.

Source: 01-AS - Fraud and Scams.

Issuer. The party that creates and signs a verifiable credential. Aliases: Issuer (digital money), Issuer (verifiable credentials), credential issuer, issuers.

Source: 01-AS - Identity Case: Verifiable Credentials.

Issuer control. The power of a stablecoin issuer to mint, redeem, blacklist, freeze, or otherwise enforce rules at the token level. Aliases: Issuer control (stablecoin).

Source: 02-AS - Case Study: USDT on Tron.

Issuer layer. The stablecoin component controlled by the issuer, including minting, redemption, reserves, and address-freeze authority. Aliases: Issuer layer (stablecoin).

Source: 02-AS - Trust Architecture: The Stablecoin Hybrid.

Iterative propagation. Repeatedly passing trust values through the network until the scores converge and stabilize. Aliases: trust propagation.

Source: 03-DS - EigenTrust: From Local Opinions to Global Scores.

J

JSON Web Token. A compact token format that can carry identity or authorization claims protected by a digital signature. Aliases: JSON Web Tokens, JWT.

Source: 04-CP - Real-World Failure: The pac4j-jwt Auth Bypass.

JSON-RPC. A remote procedure call format used by Ethereum clients for structured requests and responses. Aliases: JSON-RPC (Ethereum client).

Source: 03-EF - Two Networks, One Chain.

JSON-RPC endpoint. A network address that accepts JSON-RPC requests for chain data such as balances, blocks, logs, or transaction submission. Aliases: API endpoint, JSON-RPC endpoint (blockchain access), JSON-RPC endpoints, endpoint.

Source: 01-AS - RPC Providers: The Access Layer.

Jurisdictional arbitrage. Routing activity through countries or services with weaker enforcement, weaker AML rules, or lower cooperation with investigators. Aliases: Jurisdictional arbitrage (crypto regulation), jurisdiction shopping, regulatory arbitrage.

Source: 01-FO - Policy & Regulatory Response.

Justification. The state reached when a supermajority of total stake votes for a link between checkpoint epochs. Aliases: Justification (PoS finality), justified link, supermajority vote link.

Source: 03-CM - Justification: Supermajority Vote Links.

Justified checkpoint. A checkpoint that has received at least two-thirds of total stake voting for the required source-to-target link. Aliases: Justified checkpoint (Ethereum finality), justification, justified.

Source: 02-EF - Gasper: Fork Choice + Finality.

K

Kademlia. A DHT design family that uses prefix-like distance logic for efficient peer and content lookup.

Source: 02-DS - The Blockchain Link: Efficient Routing.

Keccak-256. Ethereum's SHA-3-related hash function using pre-standardization Keccak padding rather than standardized SHA3-256 padding. Aliases: Keccak, Keccak sponge construction, Keccak-256 (Ethereum).

Source: 02-CP - Sponge Construction: How SHA-3 is Built.

Key compromise. A failure where an attacker gains control of private keys or administrator credentials used to authorize ledger actions. Aliases: Key compromise (ledger operations), compromised keys, credential compromise.

Source: 04-DS - Threats to Distributed Ledgers (cont.).

Key distribution problem. The challenge of securely sharing secret keys with many parties before encrypted communication can begin. Aliases: key distribution crisis, key-distribution problem.

Source: 04-CP - The Impossible Secret.

Key Encapsulation Mechanism. A public-key mechanism for securely establishing shared key material, often used as a building block in modern encrypted protocols. Aliases: KEM, key encapsulation mechanisms.

Source: 05-CP - Post-Quantum Cryptography: The New Toolbox.

Key handling. The operational discipline of generating, storing, using, rotating, and protecting cryptographic keys. Aliases: key management, private-key handling.

Source: 05-CP - Case Study: CryptoDefense — Keys Left in Plain Sight.

Key hygiene. The operational practices for generating, storing, rotating, backing up, and revoking cryptographic keys. Aliases: key management, key management hygiene.

Source: 04-CP - Compromised Keys and Revocation Failures.

Key management. The operational practice of securely distributing, storing, using, and replacing symmetric keys. Aliases: Key management (blockchain operations), Key management (blockchain users), Key management (symmetric cryptography), Key management (wallet usability), key distribution, key rotation, key-management, private key management, private-key management, wallet recovery.

Source: 03-CP - Why Symmetric Crypto.

Key manager. The wallet role that creates, stores, and organizes private keys, often from a seed phrase. Aliases: Key manager (wallet).

Source: 02-BF - What Are Wallets?.

Key mixing. A block-cipher step that combines data with a round key, commonly using XOR. Aliases: round-key mixing.

Source: 03-CP - Building Blocks of Block Ciphers.

Key pair. A matched public key and private key whose mathematical relationship enables asymmetric cryptographic operations. Aliases: Key pair (asymmetric cryptography), Key pair (permissionless identity), key pairs, public-private key pair, public/private key pair.

Source: 04-CP - Enter Public-Key Cryptography.

Key space. The set of possible keys or seeds an attacker would need to search. Aliases: keyspace.

Source: 05-CP - When Good Crypto Goes Bad: Milk Sad (CVE-2023-39910).

Key store. A storage mechanism intended to hold cryptographic keys with access controls and platform protection. Aliases: OS-protected keystore, key store, keystore.

Source: 05-CP - Case Study: CryptoDefense — Keys Left in Plain Sight.

Keyless Signature Infrastructure. Estonia's hash-linked integrity infrastructure for proving that government and healthcare records have not been altered. Aliases: Estonia KSI, KSI.

Source: 04-DS - Case Study B — Public Sector: EBSI & Estonia (KSI){.smaller}.

Keynesian Economics. An economic framework that supports active government and central-bank intervention to manage recessions and demand.

Source: 04-IN - The Ideological Divide: Austrian vs. Keynesian Economics.

Keystream. A sequence of key-derived bits or bytes combined with plaintext, often by XOR, to produce ciphertext. Aliases: pseudorandom stream.

Source: 03-CP - Pseudo-Random Generators.

Know Your Customer. A compliance process that identifies a customer and, when required, the beneficial owner before or during service. Aliases: KYC, Know Your Customer (crypto compliance), Know Your Customer (identity), identity checks, mandatory ID checks.

Source: 04-BF - Off-Chain Controls: KYC and AML.

Knowledge graph. A structured network of entities and relationships used to connect addresses, tags, actors, services, and evidence. Aliases: Knowledge graph (AI attribution), entity graph.

Source: 01-FO - Future of Forensics: AI-Powered Attribution.

KYC Subpoena. Legal process compelling an exchange or service to reveal the identified customer behind an account or deposit address. Aliases: KYC Subpoena (blockchain attribution), KYC records, Know Your Customer subpoena, exchange subpoena.

Source: 02-FO - The Final Step: Attribution.

KYC/AML. Compliance processes that collect or use customer identity and transaction information at financial services. Aliases: Anti-Money Laundering, KYC/AML (forensics and compliance), Know Your Customer.

Source: 04-AS - Attribution.

KYC/AML compliance. Identity and financial-crime controls that require institutions to know customers and monitor for illicit finance risks. Aliases: AML, Anti-Money Laundering, KYC, Know Your Customer.

Source: 03-IN - Digital Trust: The Centralized Model.

L

Labeled Dataset. A database mapping blockchain addresses or clusters to known services, markets, mixers, sanctioned entities, or other actors. Aliases: Labeled Dataset (blockchain analytics), address labels, analytics firm labels, labeled addresses.

Source: 02-FO - The Final Step: Attribution.

Large Language Model. An AI model that can process large volumes of text to extract clues such as crypto addresses, actor names, and contextual links. Aliases: LLM, LLMs, Large Language Model (AI attribution).

Source: 01-FO - Future of Forensics: AI-Powered Attribution.

Last-revealer bias. The small ability of the final randomness contributor to withhold its reveal and marginally influence the resulting seed. Aliases: Last-revealer bias (RANDAO), last revealer advantage.

Source: 02-EF - Global Randomness: RANDAO + VDF Beacons.

Latency. The time it takes for information to travel across a network or complete a protocol step. Aliases: Latency (distributed systems), Latency (ledger performance), network delay, propagation delay, transaction latency.

Source: 01-DS - Fallacy #2: Latency Is Zero.

Lattice. A repeating high-dimensional grid of points generated by basis vectors. Aliases: Lattice (cryptography), lattices.

Source: 05-CP - Lattices: Intuition Without the Math.

Lattice-based cryptography. A post-quantum cryptography family based on hard problems in high-dimensional lattices. Aliases: lattice cryptography.

Source: 05-CP - Post-Quantum Cryptography: The New Toolbox.

Laundering Chain. A sequence of services, assets, and transfers used to obscure the origin of funds before use or cash-out. Aliases: laundering infrastructure, laundering network.

Source: 03-AS - North Korea: Impact Signals.

Layer 1. The base blockchain that provides consensus, ordering, settlement, and data availability. Aliases: L1, Layer 1 (Ethereum scaling), Layer 1 (scaling), base blockchain, base chain, base layer.

Source: 01-EF - Introducing L2.

Layer 2. A separate execution environment built on top of a Layer 1 that processes transactions off the main chain and posts data or proofs back. Aliases: L2, L2s, Layer 2 (Ethereum scaling), Layer 2 system, Layer 2s.

Source: 01-EF - Introducing L2.

Layer 2 network. A system that processes many user transactions away from the base chain while depending on that chain for settlement, data, or verification. Aliases: L2, L2 network, Layer 2, Layer 2 network (scaling), rollup.

Source: 01-AS - Scaling and Interoperability.

Layering. Splitting and routing funds through multiple transactions to bury the original source under a more complex transaction history. Aliases: Layering (crypto laundering), transaction layering.

Source: 01-FO - How Adversaries Hide.

Lazarus Group. A North Korea-linked threat group used in the lesson as the attributed actor behind the Ronin Bridge theft. Aliases: DPRK-linked Lazarus Group, Lazarus, Lazarus Group (threat actor), North Korea's Lazarus Group.

Source: 01-FO - Policy & Regulatory Response.

Lazy mint. A minting pattern where a signed off-chain voucher authorizes token creation only when a buyer submits it on-chain. Aliases: lazy minting, signature-based mint.

Source: 06-EF - Minting on Ethereum.

Leader. The participant responsible for coordinating a round by putting forward the next candidate value. Aliases: Leader (consensus), proposer.

Source: 01-CM - Consensus in the Real World.

Leader election. The process of selecting one node to coordinate a round or period of consensus activity.

Source: 05-IN - Classical Consensus Approaches.

Leaf node. A lower-capacity peer that connects to a supernode rather than participating heavily in network-wide flooding. Aliases: Leaf node (P2P network), leaf, leaf nodes.

Source: 01-DS - Gnutella's Fix: Supernodes & "Smart Flooding".

Leaf set. A Pastry node's set of numerically nearby peers used to finish routing once a lookup reaches the target neighborhood. Aliases: Leaf set (Pastry).

Source: 02-DS - DHT Example: Pastry.

Learning With Errors. A lattice-related problem based on solving noisy linear equations that are easy to generate but hard to recover. Aliases: LWE.

Source: 05-CP - Lattices: Intuition Without the Math.

Least significant byte. The final byte of a binary value, used in the toy PRG as the emitted output for each round. Aliases: LSB_8, last byte.

Source: 03-CP - Simple Pseudorandom Generator.

Ledger. An append-only record with added mechanisms for maintaining integrity, ordering, and agreement across participants. Aliases: Ledger (blockchain data structure), ledger history, ledgers, shared ledger.

Source: 04-DS - From Logs to Ledgers.

Ledger convergence. The process by which honest nodes settle on the same accepted ledger history. Aliases: chain convergence, history convergence.

Source: 01-CM - Why Consensus Matters in Blockchains.

Ledger split. A condition where different parts of the network temporarily see incompatible versions of the ledger. Aliases: Ledger split (Bitcoin), conflicting ledger views, network split.

Source: 04-BF - What Can Consensus Attacks Achieve?.

Legacy Bank Rail. Traditional financial infrastructure such as SWIFT messaging and correspondent banking used to move and settle value. Aliases: legacy bank rails, legacy banking rails.

Source: 03-AS - Competing Financial Infrastructures.

Legal jurisdiction. The authority of a court or agency to act over a server, entity, person, or asset within its legal reach. Aliases: jurisdiction.

Source: 01-FO - Colonial Pipeline: Payment Recovery.

Legal tender. Money that must be accepted for debts or payments under the law of an issuing jurisdiction.

Source: 02-AS - CBDCs vs Cryptocurrencies.

Lender of Last Resort. An institution that can provide emergency liquidity to prevent bank panics or wider financial collapse.

Source: 04-IN - The Modern Financial Architect: Central Banks.

Length-extension attack. An attack on some Merkle-Damgard-based constructions where a known digest can be used as a starting state to append data. Aliases: length extension.

Source: 02-CP - Aside: Length-Extension Attack.

libp2p. The modular peer-to-peer networking framework used by Ethereum consensus clients. Aliases: libp2p (Ethereum consensus layer).

Source: 03-EF - Two Networks, One Chain.

License. The explicit permission terms that state how NFT-associated content may be used, copied, commercialized, or restricted. Aliases: License (NFT rights), license terms, licensing.

Source: 05-EF - NFTs: What Are We Actually Buying?.

Light client. A blockchain participant that does not download the full chain and instead queries a full node for needed network data. Aliases: Light client (blockchain network), light clients, light node, light nodes.

Source: 01-DS - The Blockchain Link.

Light client (Bitcoin). A Bitcoin client that downloads block headers and uses proofs from full nodes instead of storing and validating every block. Aliases: SPV client, lightweight client.

Source: 03-BF - Bitcoin's Peer-to-Peer Network.

Light client (Ethereum). A resource-minimized client that tracks headers and requests proofs instead of storing and validating all state locally. Aliases: light clients.

Source: 03-EF - Nodes and Clients.

Lightweight client. A client that verifies selected blockchain facts using compact proofs and headers instead of storing every transaction. Aliases: Lightweight client (blockchain verification), light client, lightweight clients.

Source: 04-AS - Why the Merkle Root Matters.

Linear cost. A scaling pattern where message cost grows roughly in proportion to the number of peers. Aliases: Linear cost (network scalability), O(N), linear message cost.

Source: 02-DS - Scalability Challenges{.smaller}.

Linux.Encoder. A ransomware case where AES keys were derived from predictable clock-seeded randomness. Aliases: Linux.Encoder.1.

Source: 05-CP - Case Study: Linux.Encoder RNG Failure.

Liquidation. The closing of an undercollateralized loan position, often with a reward or discount for the liquidator. Aliases: Liquidation (DeFi), liquidations.

Source: 03-EF - The Mempool.

Liquidity. The availability of buyers, sellers, and trading depth that lets an asset be exchanged without large price disruption. Aliases: Liquidity (crypto markets), market liquidity.

Source: 04-BF - Lessons: Small Community Risks.

Liquidity pool. A smart-contract reserve of tokens used to execute swaps and determine prices in an automated market maker. Aliases: Liquidity pool (AMM), pool, token pool.

Source: 01-FO - Decentralized Exchanges (DEXs).

Liveness. The guarantee that the system continues making progress and is not permanently stalled. Aliases: Liveness (Ethereum consensus), Liveness (consensus property), Liveness (consensus), availability, block-production liveness, consensus liveness, progress.

Source: 05-IN - Consensus as the Core Goal.

Liveness failure. A failure mode where the network cannot make progress, often because the ordering service stalls or loses quorum. Aliases: Liveness failure (Hyperledger Fabric), liveness, ordering-service stall.

Source: 02-PC - Where Consensus Can Still Fail.

LMD-GHOST. Ethereum's fork-choice rule that follows the branch with the greatest weight from validators' latest attestations. Aliases: LMD-GHOST (Ethereum fork choice), Latest-Message-Driven Greedy Heaviest-Observed SubTree, fork-choice rule.

Source: 02-EF - Forks in Proof of Stake — Causes and Resolution.

Local MSP configuration. The MSP material a peer, orderer, or client uses locally to identify itself and verify trusted identities. Aliases: Local MSP configuration (Hyperledger Fabric), local MSP, local trust material.

Source: 02-PC - What is an MSP?.

Local satisfaction ratio. A peer's direct record of successful versus failed interactions with another peer. Aliases: local satisfaction ratios, net satisfaction.

Source: 03-DS - EigenTrust: From Local Opinions to Global Scores.

Location addressing. A storage addressing model where the address names a server location, so the operator can change or remove the content behind it. Aliases: Location addressing (storage), location-addressed storage.

Source: 06-EF - Metadata, IPFS, and the Pointer Problem.

Location-addressed storage. A storage model where data is retrieved from a specific domain and path, such as an HTTPS URL. Aliases: HTTPS URL storage, Location-addressed storage (NFT metadata), location addressing.

Source: 05-EF - Metadata and Storage Models.

Locking script. The script condition attached to an output that defines what must be provided later to spend that output. Aliases: Locking script (Bitcoin Script), Locking script (Bitcoin), script condition, scriptPubKey.

Source: 02-BF - Transactions and the UTXO Model.

Lockout. An operational failure where required credentials or authority are unavailable, preventing normal management actions. Aliases: Lockout (permissioned ledger operations), lockout situation, network lockout.

Source: 01-PC - Case Study: Fabric Lockout.

Log. A time-ordered record of events or actions that preserves history by adding new entries rather than rewriting old ones. Aliases: Log (Ethereum), Log (distributed ledgers), audit trail, event log, log entry, logs.

Source: 04-DS - From Logs to Ledgers.

Logarithmic cost. A scaling pattern where each network doubling adds only a small number of extra routing hops. Aliases: Logarithmic cost (network scalability), O(log N), logarithmic routing cost.

Source: 02-DS - Scalability Challenges{.smaller}.

Logarithmic verification. The scaling pattern where Merkle proof length and verification work grow with tree depth rather than total dataset size. Aliases: Logarithmic verification (Merkle proof), O(log n) verification, logarithmic proof size.

Source: 02-CP - Why Proofs Are Efficient.

Logic contract. The contract that contains executable code used by a proxy while the proxy keeps the persistent state. Aliases: Logic contract (proxy pattern), implementation, implementation contract, logic.

Source: 04-EF - Upgradeability and Proxy Patterns.

Logical clock. An abstract ordering mechanism that helps distributed systems reason about event sequence without relying on one perfect physical clock. Aliases: logical clocks.

Source: 05-IN - Timing Faults.

Logical ring. Chord's circular identifier space where peers and keys are placed according to hash-derived IDs. Aliases: Logical ring (Chord), clock, ring.

Source: 02-DS - DHT Example: Chord.

Long-range attack. An attack that uses old credentials or stake to construct an alternative version of distant ledger history. Aliases: Long-range attack (PoS), Long-range attack (Proof of Stake attack), Long-range attack (distributed ledgers), fabricated alternative history, history rewrite attack, long-range attacks, long-range history rewrite, old-key attack.

Source: 04-DS - Threats to Distributed Ledgers (cont.).

Longest chain rule. The convention that nodes accept the valid chain with the most cumulative proof-of-work as the current ledger history. Aliases: Longest chain rule (Bitcoin), chain selection rule, most cumulative proof-of-work rule.

Source: 01-BF - How Double-Spending is Solved.

Longest Proof-of-Work chain. The valid chain backed by the most accumulated proof-of-work, which Bitcoin nodes treat as the agreed history. Aliases: Longest Proof-of-Work chain (Bitcoin), highest-work chain, longest PoW chain, longest chain.

Source: 01-BF - A Practical Solution to Byzantine Generals.

Longest valid chain. The protocol-selected branch of valid blocks that represents the most accepted accumulated work under the chain-selection rule. Aliases: Longest valid chain (proof of work), heaviest chain, heaviest valid chain, longest chain.

Source: 02-CM - The PoW Rule at a Glance.

Longest-chain selection. The rule of favoring the valid chain with the greatest accumulated proof-of-work. Aliases: Longest-chain selection (Bitcoin consensus), longest chain, most accumulated work.

Source: 04-AS - Bitcoin's Core Design Synthesis.

Low Time Preference. A preference for saving and long-term investment over immediate consumption.

Source: 04-IN - The Bitcoin Standard: A Digital Return to "Hard Money".

M

Machine-readable provenance chain. A structured history of content or credential changes that software systems can inspect rather than relying only on human judgment. Aliases: provenance chain.

Source: 05-AS - Opportunity: Authenticity and Provenance.

Mainnet. The live Ethereum network where real transactions, smart contracts, balances, and fees operate. Aliases: Ethereum mainnet, Mainnet (Ethereum).

Source: 01-EF - Ethereum's History.

Majority attack. An attack where one actor or coalition gains enough validating influence to control recent ledger history or approve fraudulent activity. Aliases: 51% attack, Majority attack (distributed ledgers), collusion attack, majority hash attack.

Source: 04-DS - Threats to Distributed Ledgers.

Majority attack economics. The security idea that attacking Bitcoin requires controlling enough work to outpace the honest network, making many attacks economically difficult. Aliases: Majority attack economics (Bitcoin), majority attack, majority-work economics.

Source: 01-BF - Lessons from Precursors.

Majority hash-power attack. An attack where dominant mining power can outcompete honest miners and replace recent chain history. Aliases: 51 percent attack, Majority hash-power attack (Proof of Work), majority hash attack.

Source: 04-AS - Common PoW Attack Themes.

Majority voting. A decision rule where the value supported by most participants is accepted as the group's result. Aliases: majority decision.

Source: 05-IN - Strategies for Handling Suspicion.

Malicious actor. A participant that intentionally tries to mislead, disrupt, or subvert the network. Aliases: adversary, malicious participant.

Source: 05-IN - Why Suspicion Matters.

Malicious smart contract. A smart contract intentionally designed to deceive users, drain assets, or trigger harmful approvals or transfers. Aliases: malicious contract, scam contract.

Source: 01-AS - Fraud and Scams.

Managed Anonymity. A privacy model where small transactions may receive limited privacy while larger or suspicious flows remain traceable to authorities. Aliases: anonymity for small value and traceable for high value.

Source: 03-AS - China: Impact Signals.

Managed membership. A participation model where admitted identities are known and governed instead of allowing open anonymous entry. Aliases: Managed membership (permissioned ledgers), curated membership, known identities.

Source: 02-PC - How Fabric Avoids Public-Chain Consensus Costs.

Mapping. A key-value lookup table commonly used for balances, permissions, registries, and other sparse associations. Aliases: Mapping (Solidity), key-value lookup, mapping(Key => Value).

Source: 04-EF - Types: Reference Types.

Market churn. Rapid creation, disappearance, or turnover of crypto assets that makes discovery, due diligence, liquidity, and risk assessment harder. Aliases: Market churn (crypto assets), cryptocurrency churn, token churn.

Source: 01-AS - Finance (High-Level Overview).

Market for Lemons. A market failure where uncertainty about quality drives good participants away and leaves worse options behind. Aliases: lemons problem.

Source: 04-IN - The "Market for Lemons": When Trust Breaks Down.

Market resolution. The process that determines which event outcome won and how positions should be paid. Aliases: Market resolution (prediction markets), outcome resolution, resolution.

Source: 01-AS - Prediction Markets Case: Polymarket.

Mathematical security. Security based on precise definitions, assumptions, and proofs rather than on hiding how the system works. Aliases: security through mathematics.

Source: 01-CP - Cryptography: From Obscurity to Mathematical Security.

Max fee per gas. The sender's ceiling on the total per-gas price they are willing to pay for a transaction. Aliases: Max fee per gas (Ethereum fee market), max fee, maxFeePerGas, max_fee_per_gas.

Source: 03-EF - Transactions: Structure and Flow.

Max priority fee per gas. The sender's maximum per-gas tip offered to the block proposer for including the transaction. Aliases: Max priority fee per gas (Ethereum fee market), maxPriorityFeePerGas, max_priority_fee_per_gas, priority fee, tip.

Source: 03-EF - Transactions: Structure and Flow.

Maximal Extractable Value. Value a block builder or proposer can gain from transaction ordering, inclusion, or exclusion choices. Aliases: MEV, Maximal Extractable Value (Ethereum block building), Maximal Extractable Value (Ethereum block production), Maximal Extractable Value (block proposal), maximal extractable value.

Source: 03-CM - The Block Proposer: Selection and Building.

mBridge. A multi-central-bank CBDC platform for direct cross-border settlement in participating sovereign digital currencies. Aliases: Project mBridge, mBridge (CBDC platform), mBridge Ledger.

Source: 02-AS - CBDC Technical Platforms.

Mean Time To Failure. The average time a system runs before failing. Aliases: MTTF.

Source: 01-DS - Availability, MTTF, and MTTR.

Mean Time To Repair. The average time needed to recover from a failure and restore service. Aliases: MTTR.

Source: 01-DS - Availability, MTTF, and MTTR.

Median-time-past. A timestamp rule that compares a new block's time against the median of recent block times to limit manipulation. Aliases: MTP, Median-time-past (blockchain timestamps).

Source: 02-CM - Retargeting: Technical Implementation.

Medium of Exchange. A function of money that lets people trade through a commonly accepted instrument instead of direct barter.

Source: 04-IN - What is Money? A Social Technology.

Membership / Admin identity. A high-authority identity that can add members, change policy, or alter network configuration. Aliases: Membership / Admin identity (permissioned ledger role), admin identity, configuration identity, membership identity.

Source: 01-PC - Identity Theft Risks.

Membership lifecycle. The ongoing process of verifying, issuing, using, reviewing, renewing, rotating, and revoking participant access. Aliases: membership management.

Source: 01-PC - Membership Lifecycle.

Membership NFT. An NFT used as a key for access to content, events, community spaces, or other member privileges. Aliases: membership NFTs.

Source: 06-EF - Three Patterns: DAOs, Membership NFTs, and Social Tokens.

Membership policy. Rules that determine who may add, remove, renew, or revoke participants and credentials. Aliases: member policy.

Source: 01-PC - Key Components.

Membership Service Provider. A Fabric component or role that connects participants to verifiable organizational identities, often using certificates. Aliases: MSP, MSPs, Membership Service Provider (Hyperledger Fabric), membership service provider.

Source: 04-DS - Permissioned Ledgers.

Memory. The temporary workspace available during one call and cleared afterward. Aliases: Memory (Solidity data location), temporary memory.

Source: 04-EF - Data Locations: Storage, Memory, Calldata.

Memory-hard puzzle. A PoW puzzle designed to require substantial memory as well as computation, making some hardware specialization harder. Aliases: memory-hard PoW.

Source: 02-CM - Proof-of-work Puzzles.

Mempool. A node's waiting area for valid transactions that have been seen by the network but not yet included in a block. Aliases: Mempool (blockchain network), memory pool, pending transaction pool, transaction pool.

Source: 02-IN - Step 3: The Mempool.

Mempool (Bitcoin). A node's local collection of known pending transactions waiting to be included in a block. Aliases: memory pool, pending transaction pool.

Source: 01-BF - Primitive 3: Consensus via Proof-of-Work.

Mempool (Ethereum). The set of pending transactions relayed through the network before a validator includes them in a block. Aliases: Mempool (Ethereum transactions), memory pool, pending transaction pool, transaction pool.

Source: 01-EF - Transaction Lifecycle (PoS Era).

Merkle internal node. A non-leaf hash computed from child hashes inside a Merkle tree. Aliases: internal node, parent node.

Source: 02-CP - What Is a Merkle Tree?.

Merkle leaf. A hash of an individual data item at the bottom layer of a Merkle tree. Aliases: leaf, leaf hash, leaves.

Source: 02-CP - What Is a Merkle Tree?.

Merkle proof. A compact proof that a data item is included in a Merkle tree with a particular root. Aliases: Merkle inclusion proof, Merkle proof (allowlist), inclusion proof, membership proof.

Source: 02-CP - Merkle Proofs (Membership).

Merkle root. The top hash in a Merkle tree that commits to all leaves below it. Aliases: Merkle root (Bitcoin), root, root hash, transaction root.

Source: 02-CP - Merkle Trees: Motivation.

Merkle tree. A hash-based data structure that summarizes many pieces of data efficiently and supports compact verification. Aliases: Merkle tree (Bitcoin), Merkle trees, hash tree, tree of hashes.

Source: 01-IN - Learning Objectives I.

Merkle-Damgard construction. An iterative hash design that processes message blocks through a compression function and carries the resulting state forward. Aliases: Merkle-Damgård, Merkle–Damgård, Merkle–Damgård construction.

Source: 02-CP - Merkle–Damgård: How SHA-256 is Built.

Merkle-Patricia trie. Ethereum's hash-linked key-value data structure used to commit compactly to ordered protocol data such as state, transactions, and receipts. Aliases: MPT, Merkle Patricia trie, Merkle-Patricia trie (Ethereum), trie.

Source: 02-EF - Execution Payload: Header Structure.

Mersenne Twister. A fast general-purpose PRNG useful for simulations but unsuitable for generating cryptographic secrets. Aliases: Mersenne Twister (not for secrets), mt19937, std::mt19937.

Source: 05-CP - When Good Crypto Goes Bad: Milk Sad (CVE-2023-39910).

Mesh. The changing set of peers that relay a GossipSub topic to balance bandwidth, diversity, and resilience. Aliases: Mesh (GossipSub), rotating mesh.

Source: 03-EF - Consensus-Layer Networking (libp2p / GossipSub).

Mesh topology. A network shape where nodes maintain multiple overlapping peer connections rather than relying on one central hub. Aliases: Mesh topology (Bitcoin network), peer mesh.

Source: 03-BF - Gossip and Peer Connections.

Message authentication code. A keyed tag used to verify both message integrity and knowledge of a shared secret. Aliases: MAC.

Source: 02-CP - Aside: Length-Extension Attack.

Message call. An invocation that asks an account or contract function to execute with specific input data, value, gas, and caller context. Aliases: Message call (EVM), call, contract call.

Source: 04-EF - Ethereum Accounts and Contract Review.

Message hash. A fixed-length digest of a message that is signed instead of signing the entire raw message directly. Aliases: Message hash (digital signatures), digest, hash, message digest.

Source: 04-CP - Digital Signature Workflow.

Message header. The part of a Bitcoin protocol message that identifies the command, payload length, and checksum. Aliases: Message header (Bitcoin protocol), protocol message header.

Source: 03-BF - Communication Protocol Basics.

Message integrity. The property that data has not been altered in transit or storage. Aliases: data integrity, integrity.

Source: 03-DS - Cryptographic vs. Social Trust.

Message payload. The message-specific data carried inside a Bitcoin protocol message. Aliases: Message payload (Bitcoin protocol), payload.

Source: 03-BF - Communication Protocol Basics.

Metadata. Descriptive data associated with a token, often including names, traits, images, media links, or other references. Aliases: Metadata (NFT), Metadata (tokenization), metadata JSON, token metadata.

Source: 05-EF - A Taxonomy of Digital Assets.

Metadata pointer problem. The integrity gap created when an on-chain token points to off-chain metadata or media that may be mutable, unavailable, or controlled by another system. Aliases: pointer problem.

Source: 06-EF - Metadata, IPFS, and the Pointer Problem.

Metallic Standard. A monetary form based on scarce metals such as gold or silver, often issued as coins. Aliases: metallic standards.

Source: 04-IN - A Brief History of Money's Form.

MEV relay. An off-chain coordination service that checks built blocks and forwards blinded bids from builders to validators. Aliases: MEV relay (Ethereum MEV), relay, relays.

Source: 03-EF - Builder / Relay Stack and MEV.

MEV-Boost. Middleware that lets validators receive builder-created blocks through relays without directly building every block themselves. Aliases: MEV-Boost (Ethereum MEV), MEV-Boost (Ethereum block building), maximal extractable value boost.

Source: 02-EF - Censorship.

MiCA. The European Union's unified regulatory framework for crypto issuers, exchanges, stablecoins, and service providers. Aliases: Markets in Crypto-Assets, Markets in Crypto-Assets regulation.

Source: 03-AS - EU: Overview.

Milk Sad. A wallet seed generation failure in Libbitcoin Explorer where weak randomness made supposedly large key spaces enumerable. Aliases: CVE-2023-39910, Milk Sad (wallet entropy case), Milk Sad vulnerability.

Source: 05-CP - When Good Crypto Goes Bad: Milk Sad (CVE-2023-39910).

Miner. A participant that helps produce blocks in systems such as Proof of Work by competing under the protocol's rules. Aliases: Miner (Bitcoin network), Miner (Bitcoin), Miner (blockchain role), miners, mining node.

Source: 02-IN - Pillar 3: Consensus.

Miner fee. The value left unassigned to transaction outputs, calculated as total inputs minus total outputs and claimed by the miner. Aliases: Miner fee (Bitcoin), fee, transaction fee.

Source: 02-BF - Change Addresses and Fees.

Minimum viable product. A usable early-stage system suitable for broader testing but not yet a mature production deployment. Aliases: MVP.

Source: 02-AS - mBridge So Far.

Mining. The Proof-of-Work process through which participants compete to add blocks or history to the Bitcoin ledger. Aliases: Bitcoin mining, Mining (Bitcoin), Mining (Proof of Work), mine, miners.

Source: 03-IN - The Synthesis: Bitcoin.

Mining concentration. A condition where a small number of large mining pools or operators control a large share of block production. Aliases: Mining concentration (Bitcoin network), mining centralization.

Source: 03-BF - Network Growth and Concerns.

Mining hardware. The specialized computing equipment used to perform SHA-256 hashing in the search for valid blocks. Aliases: Mining hardware (Bitcoin), mining rigs.

Source: 02-BF - Evolution of Mining Hardware.

Mining pool. A group of miners who combine hash power and share rewards according to a payout rule. Aliases: Mining pool (Bitcoin mining), Mining pool (Bitcoin), mining pools, pool, pooled mining.

Source: 02-CM - Mining Pools, Variance, and Payouts.

Minter. An authorized account that can create new token-like units in the example contract. Aliases: Minter (token contract), minting role.

Source: 04-EF - Example: Coin (Code, Part 1).

Minting. The process of creating or issuing a token under a contract's rules, often during a planned NFT launch. Aliases: Minting (NFT), Minting (token), Minting (tokens), mint, mint NFTs, minting transaction, mints, token minting.

Source: 05-EF - Minting and Market Design Patterns.

Mixer. A service or protocol that pools funds from multiple users to obscure direct transaction links between sources and destinations. Aliases: Mixer (blockchain forensics), Mixer (blockchain obfuscation), crypto mixer, mixer pool, mixers, mixing service, tumbler, tumblers.

Source: 01-FO - How Adversaries Hide.

Mode of operation. A rule set that applies a fixed-size block cipher safely to longer messages or data streams. Aliases: Mode of operation (block cipher), block-cipher mode, mode, modes of operation.

Source: 03-CP - Modes of Operation Visual.

Modular arithmetic. Arithmetic where results wrap around after division by a fixed modulus. Aliases: mod arithmetic, modulo arithmetic.

Source: 04-CP - Mathematical Backdrop: Modular Exponentiation.

Modular exponentiation. The operation of raising a value to an exponent and reducing the result modulo a chosen number. Aliases: exponentiation modulo n, modular power.

Source: 04-CP - Mathematical Backdrop: Modular Exponentiation.

Modular scaling. A scaling approach that separates responsibilities so L1 focuses on consensus, ordering, and data availability while L2s handle execution. Aliases: Modular scaling (Ethereum roadmap), modular blockchain scaling.

Source: 01-EF - Modular Scaling.

Monero. A privacy-by-default cryptocurrency that hides sender, receiver, and amount using ring signatures, stealth addresses, and RingCT. Aliases: Monero (privacy coin), XMR.

Source: 02-FO - Monero (XMR): Privacy by Default.

Monetary Hierarchy. The existing ordering of monetary and payment power among states, currencies, institutions, and infrastructures. Aliases: monetary hierarchies, payment hierarchy.

Source: 03-AS - Closing the Geopolitical Discussion.

Monetary Policy. Central-bank action, such as setting interest rates, used to influence money conditions and the broader economy. Aliases: Monetary policy (Bitcoin), issuance policy, supply rule.

Source: 04-IN - The Modern Financial Architect: Central Banks.

Monetary sovereignty. A state's ability to issue and govern its currency and transmit monetary policy through its financial system.

Source: 02-AS - Why Governments Care.

Money. A social coordination tool that works by serving as a medium of exchange, unit of account, and store of value.

Source: 04-IN - What is Money? A Social Technology.

Money Flower. A BIS taxonomy that classifies forms of money by issuer, form, access, and technology. Aliases: BIS Money Flower.

Source: 04-IN - A Taxonomy for the Future: The "Money Flower".

Money laundering. The process of moving illicit funds through layers of transactions or services to hide their criminal source. Aliases: Money laundering (blockchain forensics), crypto laundering, laundering.

Source: 01-FO - Permissionless Finance.

Mortgage-Backed Security. A financial security created by bundling mortgage loans into an investable product. Aliases: MBS, mortgage-backed securities.

Source: 04-IN - Case Study: The 2008 Global Financial Crisis.

msg.sender. The Solidity context variable that identifies the immediate caller of the current call frame. Aliases: immediate caller, msg.sender (Solidity).

Source: 04-EF - Ethereum Accounts and Contract Review.

msg.value. The Solidity context variable that reports how much ETH was attached to the current call. Aliases: msg.value (Solidity).

Source: 04-EF - Ethereum Accounts and Contract Review.

Multi-signature authorization. A spending condition that requires multiple valid signatures from a defined set of public keys. Aliases: Multi-signature authorization (Bitcoin Script), multi-signature, multisig, multisignature.

Source: 03-BF - Why Bitcoin Script Exists.

Multi-signature wallet. A control mechanism requiring multiple approved signers before an administrative action can execute. Aliases: Multi-signature wallet (upgrade governance), multi-sig, multisig.

Source: 04-EF - Upgradeability and Proxy Patterns.

Multi-source aggregation. Combining data from multiple sources to reduce reliance on one reporter or feed. Aliases: Multi-source aggregation (oracle defense), multi-source oracle, oracle aggregation.

Source: 04-EF - Randomness, Oracles, and External Data.

Multi-version concurrency control. A commit-time check that asks whether the keys read during simulation still have the same versions when the transaction is validated. Aliases: MVCC, MVCC check, Multi-version concurrency control (Hyperledger Fabric), state-version check.

Source: 02-PC - Peers: Two Jobs, One Node Type.

Multisig. A control arrangement where a threshold of multiple keys must approve an action such as moving funds or administering infrastructure. Aliases: Multisig (bridge security), multi-sig, multisignature, multisignature wallet.

Source: 06-EF - Centralization Chokepoints.

Multisignature. An authorization scheme requiring several distinct keys or signatures to approve one action. Aliases: multi-signature, multisig.

Source: 01-FO - Ronin: Key Management.

Multivariate cryptography. A post-quantum family based on the difficulty of solving systems of multivariate polynomial equations. Aliases: multivariate cryptography.

Source: 05-CP - Post-Quantum Cryptography: The New Toolbox.

Munition. A legal classification that treated strong cryptographic software like export-controlled military technology. Aliases: Munition (cryptography export control), munitions classification.

Source: 03-IN - The Crypto Wars: U.S. Gov Position (1990s).

Mutable database. A database whose owning organization can directly update or overwrite records under normal administrative control. Aliases: Mutable database (system choice), mutable DB, traditional database.

Source: 01-PC - Recap: Three Approaches Compared.

Mutual Legal Assistance Treaty. A formal government-to-government process for requesting evidence across national borders. Aliases: MLAT, MLATs, Mutual Legal Assistance Treaty (cross-border investigations).

Source: 02-FO - Forensic Limitations & Voluntary Disclosure.

Mutual suspicion. A design posture where each participant verifies others because they may be faulty, compromised, or hostile.

Source: 05-IN - Why Suspicion Matters.

N

Nakamoto consensus. A permissionless consensus style where scarce work and the heaviest valid chain guide nodes toward one history over time. Aliases: Nakamoto-style consensus, PoW consensus, Proof-of-Work consensus.

Source: 01-CM - Nakamoto (Proof-of-Work) Consensus.

Named identity. An identity tied to a known participant rather than only to a pseudonymous key or economic stake. Aliases: Named identity (permissioned ledger), authenticated identity, recognized identity.

Source: 01-PC - What Changes.

Napster. An early P2P file-sharing system that used centralized servers for metadata search while transferring files directly between users. Aliases: Napster (case study).

Source: 01-DS - Case Study: Napster.

NAT traversal. A networking technique that helps peers communicate even when routers or firewalls hide their local addresses.

Source: 01-DS - Communications Application: Skype's P2P Telephony.

Native coin. A blockchain's built-in asset used to secure the chain and pay for computation or data, such as ETH on Ethereum. Aliases: ETH, native asset, native coins.

Source: 05-EF - A Taxonomy of Digital Assets.

Negligible advantage. An advantage over random guessing so small that it is treated as practically unusable by any efficient adversary. Aliases: negligible probability.

Source: 01-CP - Probability Refresher: Events and Outcomes.

Neighbor capture. A Sybil tactic in which fake identities occupy a target's peer connections so the attacker can shape what the target sees. Aliases: capturing neighbor slots.

Source: 03-DS - Threats: Sybil Attacks.

Neighbor list. The set of peers a node currently knows about or connects to for sending and receiving network information. Aliases: Neighbor list (P2P node), peer list, peer table.

Source: 02-DS - The Eclipse Attack.

Network congestion. A condition where heavy demand for network capacity slows activity or raises the cost of getting transactions processed. Aliases: Network congestion (blockchain).

Source: 03-IN - Promises vs. Reality.

Network control. The ability to govern or restrict the underlying blockchain validators, routing, and participation rules. Aliases: Network control (stablecoin).

Source: 02-AS - Case Study: USDT on Tron.

Network deanonymization. The process of linking a Bitcoin transaction to the node, IP address, user, or service that likely created it. Aliases: Network deanonymization (Bitcoin), deanonymization, transaction-origin deanonymization.

Source: 04-BF - Mitigating Network Deanonymization.

Network latency. Delay in message delivery across a network. Aliases: latency.

Source: 05-IN - Why Decentralization Is Harder.

Network layer. The blockchain infrastructure on which stablecoin tokens are held and transferred. Aliases: Network layer (stablecoin).

Source: 02-AS - Trust Architecture: The Stablecoin Hybrid.

Network partition. A communication split where parts of a distributed network cannot reliably exchange messages with each other. Aliases: Network partition (Bitcoin), Network partition (distributed ledgers), network partitions, partition, partitioned network, partitioning, partitions.

Source: 05-IN - Centralized vs. Distributed Architectures.

Network threat. An attack or failure mode that affects communication among blockchain participants and can disrupt propagation, validation, or availability. Aliases: Network threat (blockchain), network threats.

Source: 01-IN - Learning Objectives II.

Network verification. The process by which participating nodes independently check transactions and blocks against Bitcoin's rules. Aliases: Network verification (Bitcoin), network validation.

Source: 01-BF - Lessons from Precursors.

Neutral infrastructure. Protocol infrastructure that processes valid transactions without enforcing user identity or compliance checks at the base layer. Aliases: Neutral infrastructure (blockchain), base-layer neutrality.

Source: 01-FO - Permissionless Finance.

Niche ecosystem. A future where blockchain remains useful inside limited communities or markets without replacing mainstream systems. Aliases: Niche ecosystem (blockchain futures), bounded niche, specialized ecosystem.

Source: 05-AS - A Spectrum of Futures.

Nixon Shock. President Nixon's August 15, 1971 suspension of the U.S. dollar's convertibility to gold.

Source: 04-IN - The Turning Point: Ending Bretton Woods.

No cash-out economy. An illicit ecosystem where actors spend cryptocurrency directly instead of converting it to fiat. Aliases: No cash-out economy (illicit finance), crypto-denominated underground market.

Source: 01-FO - Adversarial Counter-Responses to Regulation.

Node. An individual computer running blockchain software and participating in relaying, checking, or storing network data. Aliases: Node (blockchain network), Node (distributed network), Node (distributed systems), nodes, participant, peer, peer node, peers.

Source: 02-IN - Pillar 2: Peer-to-Peer Networks.

Node (Bitcoin). A computer running Bitcoin software that receives, relays, checks, or stores transactions and blocks. Aliases: Bitcoin node, Node (Bitcoin network), node, nodes.

Source: 01-BF - Primitive 2: The Public Ledger via P2P Networking.

Node (Permissioned Ledgers). A software instance run by an organization to submit, approve, order, validate, or store ledger activity. Aliases: Node (permissioned ledger), network node, software instance.

Source: 01-PC - Identity.

Node consolidation. A reduction in independently operated full nodes that can weaken network diversity and resilience. Aliases: Node consolidation (Bitcoin network).

Source: 03-BF - Network Growth and Concerns.

Node operator. A person or organization that runs and configures a Bitcoin node. Aliases: Node operator (Bitcoin), operator.

Source: 03-BF - Node Operator Responsibilities.

Non-faulty process. A participant that follows the protocol rules and is not exhibiting the fault behavior under discussion. Aliases: correct node, honest node, honest participant.

Source: 01-CM - Foundations of Consensus.

Non-fungible token. A token with a unique identifier that distinguishes it from other tokens, often linking to metadata, media, or specific rights. Aliases: NFT, NFTs, Non-fungible token (tokenization), non-fungible tokens.

Source: 05-EF - A Taxonomy of Digital Assets.

Non-interactive proof. A proof format where the prover publishes one proof that anyone can verify without back-and-forth challenge rounds. Aliases: Non-interactive proof (zero-knowledge proofs), non-interactive ZK, non-interactive proof.

Source: 05-CP - Zero-Knowledge Proofs: Prove Without Revealing.

Non-KYC instant exchange. An automated crypto swap service that does not require account creation or identity verification before exchanging assets. Aliases: automated swap service, instant exchange.

Source: 01-FO - Bridges & Swaps: Crossing the Chain Boundary (cont.).

Non-repudiation. A property that makes it difficult for someone to deny having authorized a message or transaction.

Source: 03-IN - Exercise.

Nonce. A one-time value used to provide freshness and prevent dangerous reuse in cryptographic operations. Aliases: Nonce (Proof of Work), Nonce (block header), extra-nonce, nonce field, nonces.

Source: 01-CP - What Is Randomness?.

Nonce (Bitcoin). A value miners change while repeatedly hashing a candidate block header to search for a valid proof-of-work. Aliases: Nonce (Bitcoin mining), nonces.

Source: 01-BF - Primitive 3: Consensus via Proof-of-Work.

Nonce (Cryptography). A value that must not repeat with the same key in modes such as CTR and GCM. Aliases: unique nonce.

Source: 03-CP - Counter-Mode Pseudorandom Generator (PRG).

Nonce (Ethereum). A per-account counter used in Ethereum state, including in address derivation and transaction sequencing. Aliases: Nonce (Ethereum account), account nonce, sequence number.

Source: 01-EF - Accounts & Global State (EOA vs Contract).

Nonpayable. The default Solidity behavior where a function reverts if ETH is attached to the call. Aliases: Nonpayable (Solidity), nonpayable function.

Source: 04-EF - Visibility, Mutability, and Payable.

Normalization. The step that converts a peer's positive local experiences into bounded trust values whose total influence is limited. Aliases: Normalization (EigenTrust), normalized local trust.

Source: 03-DS - EigenTrust: From Local Opinions to Global Scores.

Not Turing-complete. A design constraint where the language avoids unbounded computation such as arbitrary loops. Aliases: Not Turing-complete (Bitcoin Script), non-Turing-complete.

Source: 03-BF - Introduction to Bitcoin Script.

Nothing-at-stake. The incentive problem where validators can cheaply sign multiple competing forks unless penalties make that behavior costly. Aliases: Nothing-at-stake (PoS attack incentive), Nothing-at-stake (PoS risk), Nothing-at-stake (Proof of Stake attack), nothing at stake, nothing-at-stake incentives.

Source: 03-CM - Nothing-at-Stake.

Nouns DAO. An NFT-native DAO where one new Noun is auctioned roughly daily and each Noun acts as membership and one governance vote. Aliases: Nouns, Nouns DAO (NFT governance).

Source: 06-EF - Case Study: Nouns DAO.

O

Obfuscation. Techniques or services used to make blockchain tracing and attribution more difficult. Aliases: Obfuscation (blockchain tracing), obfuscation service, obfuscation services.

Source: 04-AS - Obfuscation and Countermeasures.

Observability. The practice of using logs, block history, and world-state queries to determine which Fabric transaction stage succeeded or failed. Aliases: Observability (Hyperledger Fabric), live observation, troubleshooting evidence.

Source: 02-PC - Observability: What to Watch Live.

Odd-leaf rule. A published convention for handling a tree level with an odd number of hashes. Aliases: Odd-leaf rule (Merkle tree), carry it up, duplicate last hash, odd number of leaves.

Source: 02-CP - Building a Merkle Tree.

OFAC. The U.S. Treasury office whose sanctions list shaped the Tornado Cash censorship episode discussed in the lesson. Aliases: OFAC (policy), Office of Foreign Assets Control.

Source: 02-EF - Censorship.

Off-chain. Dependent on systems, institutions, or files outside the blockchain's consensus process. Aliases: Off-chain (blockchain), off chain.

Source: 06-EF - On-Chain vs. Off-Chain.

Off-chain blind spot. An area of crypto activity recorded inside private systems such as exchanges or OTC desks rather than on a public blockchain. Aliases: Off-chain blind spot (blockchain forensics), off-chain ledger, private ledger blind spot.

Source: 01-FO - Challenges in Forensic Analysis.

Off-chain consumer. A system outside Ethereum consensus that reads receipts, logs, or state to react to on-chain activity. Aliases: Off-chain consumer (Ethereum), off-chain observer.

Source: 03-EF - Review: The Life of an Ethereum Transaction.

Off-chain data. Data kept outside the ledger while hashes or commitments on the ledger support later verification. Aliases: off-chain sensitive data.

Source: 01-PC - Why Not A Shared Database?.

Off-chain enforcement. Reliance on legal agreements, custodians, registries, or institutions outside the blockchain to make a tokenized claim meaningful. Aliases: Off-chain enforcement (tokenization), off-chain enforcement.

Source: 05-EF - Real-World Assets (RWAs) and Tokenization.

Off-chain evidence. Information outside the blockchain, such as exchange records, devices, accounts, OSINT, or institutional records, used to support attribution. Aliases: Off-chain evidence (forensics), external evidence, off-chain identity links, off-chain links.

Source: 04-AS - Attribution.

Offset. The position in a pad or generated stream where encryption or decryption begins. Aliases: Offset (keystream position), counter position.

Source: 03-CP - Pseudo-Random Generators.

Omission fault. A failure where a node remains active but fails to send or receive some messages. Aliases: message omission, omission faults.

Source: 05-IN - Omission Faults.

On-chain. Recorded or enforced through blockchain consensus, such as token ownership, IDs, transfer history, and contract execution. Aliases: On-chain (blockchain), on chain.

Source: 06-EF - On-Chain vs. Off-Chain.

On-chain analysis. The examination of blockchain transactions, addresses, contracts, and flows using data recorded directly on a public ledger. Aliases: On-chain analysis (blockchain forensics), ledger analysis, on-chain ledger analysis.

Source: 01-FO - Forensic Countermeasures.

On-chain attestation. A verifiable on-chain record or token asserting a credential, reputation claim, membership status, or other statement. Aliases: On-chain attestation (credential systems), on-chain attestations.

Source: 06-EF - Analyst Implications.

On-chain community. A community coordinated through blockchain accounts, tokens, smart contracts, or governance mechanisms. Aliases: on-chain communities, token community.

Source: 05-AS - Future 2: Specialized Crypto Ecosystem.

On-chain linkability. The ability to connect addresses, inputs, outputs, or transactions using patterns visible on the public ledger. Aliases: On-chain linkability (Bitcoin), linkability.

Source: 04-BF - Mitigating Network Deanonymization.

On-chain randomness. Random-looking values generated or consumed by contracts inside the blockchain execution environment. Aliases: On-chain randomness (smart contracts), blockchain randomness.

Source: 04-EF - Randomness, Oracles, and External Data.

On-chain state. The blockchain-maintained record of balances, ownership, approvals, or other contract data treated as authoritative by the system. Aliases: On-chain state (token architecture), canonical state, contract state.

Source: 05-EF - System Architecture — Where Everything Lives.

On-chain storage. A storage model where token metadata or media bytes are written directly into blockchain state or contract data. Aliases: On-chain storage (NFT metadata), on-chain media, on-chain metadata.

Source: 05-EF - Metadata and Storage Models.

On-chain token. A blockchain record controlled by smart contract or protocol rules that represents value, rights, or a reference to another asset. Aliases: blockchain token, token.

Source: 05-EF - Digital Assets, Tokenization, and NFTs.

On-off attack. An attack pattern where a participant behaves well long enough to gain trust, then switches to harmful behavior before disappearing. Aliases: on-off exploitation, reputation milking attack.

Source: 03-DS - Threats: On–Off (Reputation Milking).

On/off ramp. A service or process that moves users between fiat money and Bitcoin or back again. Aliases: On/off ramp (Bitcoin), fiat gateway, off-ramp, on-ramp.

Source: 04-BF - How KYC/AML Apply to Bitcoin.

One-time pad. An encryption method that XORs plaintext with truly random key material of equal length that is never reused. Aliases: OTP, random pad.

Source: 03-CP - Infinite-length One Time Pad.

One-way function. A function that is easy to compute in the forward direction but infeasible to invert with available algorithms and resources. Aliases: One-way function (public-key cryptography), mathematical one-way function, one-way, one-way property.

Source: 01-CP - Sets and Functions.

Online Certificate Status Protocol. A protocol for checking the current revocation status of a certificate with an authority or responder. Aliases: OCSP.

Source: 04-CP - Certificate Validation Process.

OP_CHECKLOCKTIMEVERIFY. A Bitcoin Script opcode that prevents spending until an absolute block height or timestamp condition is satisfied. Aliases: CLTV, OP_CHECKLOCKTIMEVERIFY (Bitcoin Script).

Source: 03-BF - Script Primitives.

OP_CHECKMULTISIG. A Bitcoin Script opcode that validates multiple signatures against a set of public keys. Aliases: OP_CHECKMULTISIG (Bitcoin Script).

Source: 03-BF - Script Primitives.

OP_CHECKSEQUENCEVERIFY. A Bitcoin Script opcode that enforces relative time-lock conditions between transactions. Aliases: CSV, OP_CHECKSEQUENCEVERIFY (Bitcoin Script).

Source: 03-BF - Script Primitives.

OP_CHECKSIG. A Bitcoin Script opcode that verifies a single digital signature against a public key. Aliases: OP_CHECKSIG (Bitcoin Script).

Source: 03-BF - Script Primitives.

OP_HASH160. A Bitcoin Script opcode that hashes data with SHA-256 and then RIPEMD-160. Aliases: HASH160, OP_HASH160 (Bitcoin Script).

Source: 03-BF - Script Primitives.

OP_RETURN. A Bitcoin transaction field used to include small amounts of metadata without making that data spendable. Aliases: OP RETURN, OP_RETURN (Bitcoin).

Source: 05-EF - Tokenization History — Early Experiments.

Opaque transaction graph. A transaction structure that hides or obscures relationships among senders, recipients, and amounts. Aliases: Opaque transaction graph (privacy assets), hard-to-trace transaction graph, opaque ledger graph.

Source: 04-BF - Regulatory Pressure Beyond Bitcoin.

Opcode. A primitive instruction in Bitcoin Script that performs a small operation such as checking a signature, hashing data, or comparing values. Aliases: Opcode (Bitcoin Script), Script opcode, operation code.

Source: 03-BF - Script Primitives.

Open Blockchain Rail. Public-chain, stablecoin, or exchange-linked infrastructure used to move value outside purely legacy or state-run systems. Aliases: crypto rail, crypto rails, open blockchain rails.

Source: 03-AS - Competing Financial Infrastructures.

Open membership. A participation model where many independent or unknown actors can join the network. Aliases: open network.

Source: 05-IN - Why Decentralization Is Harder.

Open membership enumeration. The ability to read a token-gated community's membership list from public on-chain ownership data. Aliases: Open membership enumeration (token community), membership enumeration.

Source: 06-EF - Analyst Implications.

Open participation. A model where nodes can join or leave without prior admission by a central membership authority. Aliases: Open participation (consensus), open membership, permissionless participation.

Source: 01-CM - Nakamoto (Proof-of-Work) Consensus.

Open Source Intelligence. Publicly available information from sources such as social media, forums, code repositories, paste sites, and business records. Aliases: OSINT, Open Source Intelligence (blockchain attribution).

Source: 02-FO - The Final Step: Attribution.

Open-source intelligence. Intelligence gathered from publicly available sources such as websites, forums, social media, records, and other open data. Aliases: OSINT, open source intelligence.

Source: 01-FO - Forensic Countermeasures.

Open-source review. The practice of publicly inspecting source code so flaws can be found, discussed, and fixed by a broader community. Aliases: open review, public code review.

Source: 04-BF - Implementation vs. Design.

Operational complexity. The coordination, monitoring, key rotation, upgrade, and incident-response work required to run a ledger across organizations. Aliases: Operational complexity (distributed ledgers), operational burden.

Source: 04-DS - Common Pitfalls (cont.).

Operational finality. The practical finality Fabric gives after a valid commit under normal managed-membership and crash-fault assumptions. Aliases: Fabric finality, Operational finality (Hyperledger Fabric), immediate finality.

Source: 02-PC - How Fabric Avoids Public-Chain Consensus Costs.

Operational security. The discipline of avoiding behavior or infrastructure mistakes that expose an actor's identity, location, or control of assets. Aliases: OpSec, Operational security (forensics), operational security mistake.

Source: 01-FO - The Immutable Ledger.

Operational Security Failure. A preventable user or operator mistake that exposes identity, infrastructure, or intent. Aliases: OpSec failure, Operational Security Failure (blockchain forensics), opsec failure.

Source: 02-FO - Breaking Mixers: Investigative Countermeasures.

Opt-in governance. A governance reality where participants choose which Ethereum software and chain rules to run or support. Aliases: Opt-in governance (Ethereum), opt-in coordination.

Source: 01-EF - Stakeholders & Decision Making.

Optimistic rollup. A rollup model where Ethereum accepts posted results unless someone challenges them during a dispute window. Aliases: Optimistic rollup (Ethereum L2), Optimistic rollup (Ethereum scaling), optimistic rollups.

Source: 01-EF - L2 Operator Models.

Oracle. An external system that brings off-chain facts on-chain so smart contracts can use them deterministically. Aliases: Oracle (blockchain external data), Oracle (blockchain), Oracle (smart contract dependency), Oracle (smart contracts), data feed, oracle network, oracles.

Source: 01-EF - Oracles: Bridging Blockchains and Reality.

Orderer / sequencer. A participant or service role that establishes a consistent order for accepted transactions. Aliases: Orderer / sequencer (permissioned ledger role), orderer, ordering role, sequencer.

Source: 01-PC - Roles and Duties.

Orderer cluster. The Fabric service that establishes one agreed transaction sequence for a channel and delivers ordered blocks to peers. Aliases: Orderer cluster (Hyperledger Fabric), orderer, orderers, ordering service.

Source: 02-PC - From Permissioned Concepts to Fabric Terms.

Ordering. The agreed sequence in which ledger entries are placed, especially when conflicting or simultaneous actions depend on who went first. Aliases: Ordering (distributed ledgers), event ordering, shared ordering.

Source: 04-DS - From Logs to Ledgers.

Ordering service. A service or small cluster that places accepted requests into one consistent sequence for validation and commit. Aliases: Ordering service (Hyperledger Fabric), Ordering service (permissioned ledger), leader-based cluster, orderer, ordering cluster, ordering services.

Source: 01-PC - What Changes.

Organization. A recognized consortium member, such as a carrier, port, regulator, or insurer, that participates in the network. Aliases: Organization (permissioned ledger identity), consortium member, member organization.

Source: 01-PC - Identity.

Organizational sponsorship. A model where known organizations are accountable for the representatives who participate under their name. Aliases: sponsorship.

Source: 01-PC - Sybil Resistance.

Orphaned branch. A competing branch that loses the consensus race and is no longer treated as the accepted ledger history. Aliases: Orphaned branch (blockchain), orphaned fork, pruned fork, stale branch.

Source: 01-CM - Why Consensus Matters in Blockchains.

OSINT. Publicly available information used to connect blockchain activity with real-world behavior or identities. Aliases: OSINT (forensics), open-source intelligence.

Source: 04-AS - Attribution.

Out-of-band fix. A recovery action performed outside the normal on-ledger or policy-controlled management path. Aliases: Out-of-band fix (permissioned ledger recovery), manual recovery, out-of-band recovery.

Source: 01-PC - Case Study: Fabric Lockout.

Outbound connection. A peer connection that a Bitcoin node initiates to another node. Aliases: Outbound connection (Bitcoin node), outbound peer connection.

Source: 03-BF - Joining the Bitcoin Network.

Overlay maintenance. The recurring protocol work peers perform to repair neighbor links, refresh routing information, and preserve data availability. Aliases: background maintenance, self-healing.

Source: 02-DS - The “Self-Healing” Solutions.

Overlay network. A logical network built on top of the physical internet that defines which peers know about each other and how application messages move. Aliases: logical topology, overlay.

Source: 02-DS - What is an “Overlay Network?”.

P

P2P overlay. A logical network of peer connections built on top of the underlying internet or transport network. Aliases: overlay network, peer-to-peer overlay.

Source: 01-DS - Centralized vs. P2P.

Pad reuse. The unsafe use of the same one-time-pad segment or keystream position for more than one encryption. Aliases: keystream reuse, offset reuse.

Source: 03-CP - Infinite-length One Time Pad.

Padding. Extra bytes added so plaintext fits the exact block size required by a block cipher mode. Aliases: PKCS#7 padding, Padding (block cipher).

Source: 03-CP - Padding and Initialization Vectors.

parent_root. A beacon-block field committing to the parent block that the current beacon block extends. Aliases: parent root, parent_root (beacon block field).

Source: 02-EF - Beacon Blocks and Execution Payloads.

Parity multisig. A widely used multisignature wallet system whose 2017 bugs caused major ETH theft and later froze funds. Aliases: Parity multisig (Ethereum incident), Parity multisig library, Parity multisig wallet.

Source: 02-EF - Security Risk: Smart Contract Code Reuse.

Partial failure. A failure mode where some components or links are broken while others continue running, creating inconsistent views of system health. Aliases: partial outage.

Source: 01-DS - Distributed Failures.

Partially synchronous system. A system where timing may be unstable for a while but eventually becomes bounded enough for timeouts to be useful. Aliases: partial synchrony, partially synchronous network.

Source: 01-CM - Timing Models on a Spectrum.

Partition. A condition where groups of nodes cannot reliably exchange messages with each other. Aliases: Partition (distributed network), network partition, sub-partition.

Source: 02-EF - Balance Attack.

Partition resistance. A design goal of keeping blockchain peers connected enough that the network avoids isolated islands and inconsistent chain views. Aliases: Partition resistance (blockchain networking), partition-resistant.

Source: 02-DS - The Blockchain Link.

Partitioning attack. An attack that attempts to split the network into disconnected regions so information and consensus updates are delayed. Aliases: Partitioning attack (Bitcoin network), network partition attack, routing partition.

Source: 03-BF - Fault Tolerance.

Pastry. A structured overlay that routes toward a target by matching more digits of the target identifier at each hop. Aliases: Pastry (DHT).

Source: 02-DS - DHT Example: Pastry.

Path-dependent adoption. A pattern where blockchain's future role depends on earlier choices by institutions, users, regulators, and developers. Aliases: Path-dependent adoption (blockchain futures), path dependency.

Source: 05-AS - What Does the Future Hold?.

Paxos. A classical consensus algorithm that uses leader election and majority logic to reach agreement despite crashes or lost messages.

Source: 05-IN - Classical Consensus Approaches.

Pay-Per-Last-N-Shares. A pool payout model where block rewards are distributed across the recent window of submitted shares when a block is found. Aliases: PPLNS.

Source: 02-CM - Pool Payout Model: Pay-Per-Last-N-Shares (PPLNS).

Pay-Per-Share. A pool payout model where miners receive a fixed payment for each valid share regardless of when the pool finds blocks. Aliases: PPS.

Source: 02-CM - Pool Payout Model: Pay-Per-Share (PPS).

Pay-to-PubKey-Hash. A standard Bitcoin script pattern requiring a public key that matches a stored hash and a valid signature from that key. Aliases: P2PKH, Pay-to-PubKey-Hash (Bitcoin Script), pay to public key hash.

Source: 03-BF - Bitcoin Script Basics.

Payable. A Solidity annotation that permits a function or address to receive ETH. Aliases: Payable (Solidity), payable function.

Source: 04-EF - Visibility, Mutability, and Payable.

Payload validation status. The execution client's response indicating whether a payload executed correctly, failed validation, or cannot yet be checked. Aliases: INVALID, Payload validation status (Ethereum Engine API), SYNCING, VALID.

Source: 03-EF - Two Networks, One Chain.

Payment Censorship. The blocking of financial transactions by banks, payment processors, or other intermediaries for policy, political, or business reasons.

Source: 04-IN - The Problem of Control: Chokepoints & Censorship.

Payment Chokepoint. A point in a payment system where access, surveillance, or blockage can be applied. Aliases: financial chokepoint, payment bottleneck.

Source: 03-AS - What We're Analyzing Today.

Payment infrastructure layer. The rails and intermediaries that move money, distinct from the currency unit being moved. Aliases: Payment infrastructure layer (state control), payment layer.

Source: 02-AS - The Permission Layer: Three Challenges to State Control.

Payment messaging. The transmission of payment instructions about who should pay whom, separate from the final movement of value. Aliases: messaging.

Source: 02-AS - Global Payment Infrastructure: Overview.

Payment rails. The messaging, settlement, and intermediary systems that move money between institutions and across borders. Aliases: payment infrastructure, rails.

Source: 02-AS - Global Payment Infrastructure: Overview.

Payment Stablecoin. A stablecoin designed for payments and backed by reserves under supervisory standards. Aliases: payment stablecoins, regulated payment stablecoin.

Source: 03-AS - United States: Impact Signals.

Payment system modernization. Efforts to make payment systems faster, cheaper, more resilient, and better suited to digital commerce.

Source: 02-AS - Why Governments Care.

Peel chain. A laundering pattern where small amounts are peeled off through a sequence of transactions while the remaining balance continues onward. Aliases: Peel chain (crypto laundering), peel chains, peeling chain.

Source: 01-FO - How Adversaries Hide.

Peeling Chain. A repeated UTXO pattern where small amounts are peeled off to destinations while most funds continue to a new change address. Aliases: Peeling Chain (Bitcoin forensics), Peeling chain (forensics pattern), peel chain, peeling chains.

Source: 02-FO - Heuristic #3: Peeling Chains.

Peer. A participant in a peer-to-peer network that can request, provide, rate, or verify resources without relying on a central server. Aliases: Peer (Hyperledger Fabric), Peer (P2P network), node, participant, peers.

Source: 03-DS - Intro: "The Bad Download".

Peer and orderer logs. Runtime records from peers and orderers that show which transaction stage is happening and where a failure occurred. Aliases: Fabric logs, Peer and orderer logs (Hyperledger Fabric), container logs.

Source: 02-PC - Observability: What to Watch Live.

Peer discovery. The process a peer uses to find other peers it can connect to in a decentralized network. Aliases: Discovery v4, Discovery v5, Peer discovery (Bitcoin network), Peer discovery (Ethereum networking), Peer discovery (P2P networking), discovery, node discovery, peer finding.

Source: 02-DS - From P2P Models to P2P Design.

Peer diversity. The practice of maintaining varied peer connections so one attacker, region, or failure mode is less likely to dominate a node's view. Aliases: Peer diversity (Bitcoin network), Peer diversity (P2P security), address diversity, connection diversity, diverse peers, route diversity.

Source: 02-DS - The Eclipse Attack.

Peer scoring. A local heuristic for rewarding useful peers and penalizing peers that send bad data, spam, or fail to respond. Aliases: Peer scoring (Ethereum networking), peer reputation, reputation score.

Source: 03-EF - Execution-Layer Networking (devp2p / RLPx).

Peer table. A node's local record of known or connected peers used to decide which network connections to maintain. Aliases: Peer table (Bitcoin network), address table, peer list.

Source: 04-BF - Sybil Attacks.

Peer-to-peer design. The engineering of how peers discover each other, route messages, maintain membership, and resist manipulation without a central coordinator. Aliases: P2P design, P2P network design.

Source: 02-DS - From P2P Models to P2P Design.

Peer-to-peer electronic cash. A payment system where parties can transact directly online without routing payment authority through a financial institution. Aliases: P2P electronic cash, Peer-to-peer electronic cash (Bitcoin), peer-to-peer cash.

Source: 01-BF - Bitcoin: The Mission Statement.

Peer-to-peer gossip. A propagation pattern where Ethereum nodes forward transactions or blocks through direct peer connections. Aliases: P2P gossip, Peer-to-peer gossip (Ethereum), gossip.

Source: 03-EF - Review: The Life of an Ethereum Transaction.

Peer-to-peer network. A network design where nodes exchange information directly with peers instead of depending on one central server. Aliases: P2P, P2P net, P2P network, P2P networking, Peer-to-peer network (Bitcoin), Peer-to-peer network (blockchain layer), Peer-to-peer network (blockchain pillar), peer-to-peer, peer-to-peer file sharing network, peer-to-peer networking.

Source: 02-IN - The Three Pillars.

Peer-to-peer networking. A network design where participants communicate directly with one another instead of routing all activity through one central server. Aliases: P2P networking, peer-to-peer network.

Source: 01-IN - Learning Objectives I.

PeerTrust. A context-aware reputation model that calculates trust from weighted feedback, rater credibility, transaction scope, and contextual factors.

Source: 03-DS - PeerTrust: How Trust Is Calculated.

Peg. The mechanism or target relationship intended to keep a stablecoin's price aligned with a reference asset. Aliases: Peg (stablecoin), stablecoin peg.

Source: 02-AS - Stablecoins: Types and Mechanisms.

Penalty calibration. The process of setting rewards and punishments strong enough to deter attacks without making honest operation too risky. Aliases: Penalty calibration (PoS protocol design), penalty tuning.

Source: 03-CM - Nothing-at-Stake and Economic Security.

Perfect secrecy. A security property where ciphertext alone reveals no information about the plaintext.

Source: 03-CP - Infinite-length One Time Pad.

Permission layer. The practical control layer that determines who may issue, access, transfer, freeze, or route money. Aliases: Permission layer (state control).

Source: 02-AS - The Permission Layer: Three Challenges to State Control.

Permissioned chain. A blockchain network where participation, validation, or access is restricted to approved entities. Aliases: permissioned blockchain, permissioned chains.

Source: 01-IN - Course Structure.

Permissioned consensus. A consensus model where known participants use roles, signatures, quorums, and policy to agree on ledger updates. Aliases: known-membership consensus.

Source: 01-PC - Consensus.

Permissioned distributed ledger. A distributed ledger where only approved entities can join, validate, or perform specific roles. Aliases: permissioned DLT, private distributed ledger.

Source: 02-AS - CBDC Technical Platforms.

Permissioned ledger. A blockchain design where access, transaction submission, or validation is limited to approved entities. Aliases: Permissioned ledger (enterprise tokenization), consortium blockchain, consortium ledger, permissioned blockchain, permissioned distributed ledger, permissioned ledgers, permissioned system, private blockchain.

Source: 02-IN - What is a Blockchain?.

Permissioned System. A system where access depends on approval, eligibility, or compliance with a gatekeeper's rules. Aliases: Permissioned System (financial access), Permissioned system (CBDC), Permissioned system (blockchain participation), consortium ledger, permissioned blockchain, permissioned by definition, permissioned financial system, permissioned infrastructure, permissioned ledger.

Source: 04-IN - The Problem of Control: Chokepoints & Censorship.

Permissionless finance. Financial activity on open blockchain networks where users can create wallets and transact without prior approval from a central gatekeeper. Aliases: Permissionless finance (blockchain), permissionless access, permissionless systems.

Source: 01-FO - Permissionless Finance.

Permissionless ledger. A blockchain design where broad participation is allowed, including reading, writing, or helping reach consensus. Aliases: open ledger, permissionless blockchain, permissionless ledgers, permissionless system, public blockchain.

Source: 02-IN - What is a Blockchain?.

Permissionless network. A network where peers can join without central approval, so each node must locally evaluate peer behavior. Aliases: Permissionless network (Ethereum), open permissionless network.

Source: 03-EF - Aside: Trust Mechanisms in Ethereum Networking.

Permissionless Participation. The ability to use or join a system without prior approval from a gatekeeper. Aliases: Permissionless participation (Bitcoin), open participation, permissionless access.

Source: 04-IN - Design Trade-Offs: Efficiency vs. Autonomy.

Permissionless system. A blockchain system where users can generate keys, broadcast transactions, and participate without prior authorization. Aliases: Permissionless system (blockchain governance), Permissionless system (blockchain participation), Permissionless system (blockchain), open blockchain, permissionless blockchain, permissionless network, permissionless systems, public blockchain.

Source: 02-AS - Trust Architecture: CBDCs vs Permissionless Systems.

Permutation box. A bit-reordering step in a block cipher that spreads influence across positions to create diffusion. Aliases: P-box, permutation.

Source: 03-CP - Building Blocks of Block Ciphers.

Persistent state. Contract data that remains in Ethereum state after execution and can affect future calls. Aliases: Persistent state (smart contract), Persistent state (smart contracts), contract state, contract storage, on-chain state, persistent storage.

Source: 01-EF - From EVM to Programs — Smart Contracts.

PGP. Strong encryption software released by Phil Zimmermann in 1991 that became a flashpoint in debates over public access to cryptography. Aliases: Pretty Good Privacy.

Source: 03-IN - Framing.

Phishing. A deceptive message, website, or workflow that tricks users into revealing secrets or approving harmful actions. Aliases: Phishing (crypto fraud), fake website, phishing attack.

Source: 01-AS - Fraud and Scams.

Physical entropy. Unpredictability gathered from real-world physical processes such as thermal noise, user input, or network jitter. Aliases: entropy source, physical entropy source.

Source: 01-CP - Sources of Randomness.

Physical topology. The underlying internet connectivity beneath an overlay, such as routers, links, and physical network paths. Aliases: physical network topology.

Source: 02-DS - What is an "Overlay Network?".

Pinning. Keeping content available in a content-addressed storage system by ensuring at least one service or node continues to host it. Aliases: Pinning (IPFS), pin, pinned content.

Source: 05-EF - Metadata and Storage Models.

Pivot point. The moment when broad or ambiguous evidence becomes specific enough to support action against a person, device, or service. Aliases: Pivot point (investigation), break point, investigative break.

Source: 01-FO - Silk Road: The Break.

Plaintext. The original readable data before encryption or after successful decryption. Aliases: message.

Source: 03-CP - Infinite-length One Time Pad.

Policy and governance. The rules and decision processes that define who may act, approve, administer, and change the network. Aliases: governance policy.

Source: 01-PC - Key Components.

Policy Friction. Deliberate regulatory or tax burdens that shape activity without fully banning it. Aliases: regulatory friction, tax friction.

Source: 03-AS - India: Impact Signals.

Policy layer. A set of explicit rules that define who may read, submit, approve, govern, or change the network. Aliases: Policy layer (permissioned ledger), policy controls, policy layers.

Source: 01-PC - Policy Layers.

Policy literacy. The ability to understand how technical design choices connect to law, regulation, governance, and public debate.

Source: 03-IN - Why This History Matters.

Policy Spectrum. A range of recurring state approaches rather than a single pro-crypto or anti-crypto classification. Aliases: crypto policy spectrum.

Source: 03-AS - Strategic Approaches to Cryptocurrency.

Policy threshold. An endorsement rule requiring a specified number of organizations or roles from a larger set to sign a transaction result. Aliases: OutOf, OutOf policy, Policy threshold (endorsement), threshold policy.

Source: 02-PC - Endorsement Policies as Trust Logic.

Political system. A way of understanding blockchain as a debate over decentralization, control, governance, and censorship resistance. Aliases: Political system (blockchain), political project.

Source: 05-AS - What Is Blockchain Really?.

Polynomial time. A runtime that grows by a polynomial function of input size and is treated as the practical side of cryptographic feasibility. Aliases: efficient algorithm.

Source: 01-CP - Desirable Properties of PRGs.

Post-order invalidation. A transaction failure after ordering when committing peers mark the transaction invalid during validation. Aliases: Post-order invalidation (Hyperledger Fabric), commit-time invalidation, post-order failure.

Source: 02-PC - Where Consensus Can Still Fail.

Post-quantum cryptography. Cryptography designed around hard problems believed to resist attacks by both classical and quantum computers. Aliases: PQC, post-quantum algorithms, post-quantum crypto, quantum-safe cryptography.

Source: 04-CP - Computational Hardness Assumptions.

Post-quantum migration. The coordinated transition from vulnerable cryptographic assumptions to quantum-resistant alternatives in live systems. Aliases: PQC migration, Post-quantum migration (blockchain governance), cryptographic migration.

Source: 04-AS - Cryptographic Challenges Moving Forward.

Pragma. A source-code directive that constrains the Solidity compiler version and expected language behavior. Aliases: Pragma (Solidity), compiler directive, pragma solidity.

Source: 04-EF - Solidity: File Structure, From Top to Bottom.

Pragmatic Adoption. Uptake driven by immediate usefulness rather than abstract commitment to a technology or ideology. Aliases: practical adoption, utility-driven adoption.

Source: 03-AS - Latin America: Overview.

Pre-image resistance. The property that, given a digest, it should be computationally infeasible to find any input that hashes to it. Aliases: one-way property, preimage resistance.

Source: 02-CP - Hash Function Properties.

Pre-order rejection. A transaction failure before ordering caused by issues such as insufficient endorsements, invalid identity, or policy mismatch. Aliases: Pre-order rejection (Hyperledger Fabric), pre-order failure.

Source: 02-PC - Where Consensus Can Still Fail.

Pre-trusted anchor. A trusted starting peer used to ground a global reputation calculation and constrain how trust propagates. Aliases: anchor, anchor node, pre-trusted peer, trusted reference point.

Source: 03-DS - EigenTrust: Anchors and Collusion Resistance.

Predictable monetary policy. A supply schedule whose issuance rules and cap are visible in the protocol rather than changed by discretionary authority. Aliases: Predictable monetary policy (Bitcoin), transparent issuance.

Source: 01-BF - Benefits of Bitcoin's Design.

Prediction market. A market where users trade positions tied to real-world outcomes, so prices can reflect collective expectations. Aliases: event market, prediction markets.

Source: 01-AS - Prediction Markets Case: Polymarket.

Prefix matching. A routing strategy where each hop chooses a peer whose identifier shares a longer prefix with the target. Aliases: Prefix matching (DHT routing), prefix-based routing.

Source: 02-DS - DHT Example: Pastry.

Preimage resistance. The property that it is computationally hard to recover an input from only its hash digest. Aliases: pre-image resistance.

Source: 04-AS - Hash Properties That Matter for Blockchain.

Previous block hash. The header field that points to the prior block and links a Bitcoin block into the chain. Aliases: Previous block hash (Bitcoin block header), prev block hash.

Source: 04-AS - Bitcoin Block Structure.

Price risk. The exposure buyers and merchants face when bitcoin's price changes before a transaction reaches sufficient finality. Aliases: Price risk (Bitcoin payments), exchange-rate uncertainty.

Source: 02-BF - Transaction Challenges.

Price volatility. Large and unpredictable changes in crypto-asset prices that can undermine trust in their use as money or savings. Aliases: Price volatility (crypto assets), high price volatility, volatility.

Source: 05-AS - External Constraints.

Primary market. The initial sale or minting phase where NFTs are first distributed to buyers. Aliases: Primary market (NFT), mint sale, primary sale, primary sales.

Source: 05-EF - Royalties, Economics, and Marketplace Realities.

Primary source. A source close to the original event, dataset, protocol decision, or official action being described. Aliases: Primary source (crypto research), primary sources.

Source: 01-AS - Key Sources.

Priority fee. The per-gas amount paid to the proposer as an incentive to include a transaction. Aliases: Priority fee (Ethereum fee market), max priority fee, tip.

Source: 03-EF - EIP-1559 Fee Mechanics.

Privacy. Controls that limit who can see sensitive ledger data while still preserving appropriate verification. Aliases: Privacy (distributed ledgers), confidentiality.

Source: 04-DS - Transparency vs. Privacy.

Privacy channel. A permissioned-ledger mechanism for limiting visibility of data or transactions to an authorized subset of participants. Aliases: Privacy channel (permissioned ledger), privacy channels, private channel.

Source: 05-EF - Enterprise Tokenization and Permissioned Ledgers.

Privacy coin. A cryptocurrency designed to provide stronger transaction privacy than transparent ledgers such as Bitcoin. Aliases: Monero, Privacy Coin (blockchain forensics), Privacy coin (blockchain design), XMR, ZEC, Zcash, privacy asset, privacy coins, privacy-preserving blockchain, privacy-preserving cryptocurrency.

Source: 03-IN - Why This History Matters.

Privacy controls. Mechanisms that separate who can participate from who can see particular data or proofs. Aliases: Privacy controls (permissioned ledger), selective disclosure, selective visibility.

Source: 01-PC - Privacy.

Privacy Pools. An experimental mixer-like design that uses zero-knowledge proofs to preserve privacy while letting users prove separation from known illicit deposits. Aliases: Privacy Pools (privacy protocol).

Source: 02-FO - The Next Generation: Privacy Pools.

Privacy through cryptography. The use of cryptographic tools to protect personal autonomy and private activity in digital systems. Aliases: cryptographic privacy.

Source: 05-AS - The Original Vision.

Privacy-aware design. A system design goal that protects user anonymity and data while still preserving enough accountability for trust decisions. Aliases: privacy-aware.

Source: 03-DS - Key Considerations in System Design.

Privacy-enhancing asset. A cryptoasset designed to make transaction tracing, screening, or identity linkage harder than on transparent ledgers. Aliases: Privacy-enhancing asset (cryptoasset), privacy asset, privacy coin.

Source: 04-BF - Regulatory Pressure Beyond Bitcoin.

Privacy-Preserving Blockchain. A blockchain whose core protocol intentionally conceals transaction details such as sender, receiver, or amount. Aliases: Privacy-Preserving Blockchain (blockchain forensics), privacy chain, privacy-native blockchain, privacy-preserving ledger.

Source: 02-FO - The Shift in Strategy: Privacy-Preserving Blockchains.

Privacy-preserving record linkage. A method for identifying overlapping records across parties while limiting disclosure of each party's full dataset. Aliases: secure record linkage.

Source: 01-FO - Future of Forensics: Secure Cross-Agency Collaboration.

Private audit. A compliance workflow where an organization proves rules were satisfied without revealing sensitive transaction details. Aliases: Private audit (zero-knowledge), private audits.

Source: 05-CP - Zero-Knowledge in Blockchain Practice.

Private data channel. A permissioned-ledger mechanism that limits sensitive data visibility to selected participants. Aliases: Private data channel (permissioned ledgers), private channel, private channels.

Source: 04-DS - Permissioned Ledgers.

Private data collection. A Fabric privacy mechanism that restricts sensitive transaction data to a defined subset of participants. Aliases: PDC, Private data collection (Hyperledger Fabric), collections, private collections, private data collections.

Source: 04-DS - Case Study A — Hyperledger Fabric (Permissioned).

Private exponent. The RSA private-key exponent computed from the public exponent and phi of the modulus. Aliases: Private exponent (RSA), d.

Source: 04-CP - RSA Key Generation Overview.

Private key. The secret credential a user controls to authorize blockchain actions such as signing a transaction. Aliases: Private key (Bitcoin ownership), Private key (Bitcoin), Private key (wallet control), private keys, private signing key, secret key.

Source: 02-IN - Pillar 1: Cryptography.

Private set intersection. A cryptographic protocol that reveals only the overlap between parties' sets without revealing the rest of either set. Aliases: PSI.

Source: 01-FO - Future of Forensics: Secure Cross-Agency Collaboration.

Private transaction submission. Sending a transaction directly to a builder or private service instead of broadcasting it through the public mempool. Aliases: Private transaction submission (Ethereum), direct submission, private submission.

Source: 03-EF - The Mempool.

Private-key compromise. A failure state where an attacker obtains a private key and can act as the key holder. Aliases: compromised private key, key compromise.

Source: 04-CP - Compromised Keys and Revocation Failures.

Probabilistic Finality. A settlement model where confidence that a transaction will not be reversed increases over time rather than becoming immediately absolute. Aliases: Probabilistic finality (Bitcoin), Probabilistic finality (Proof of Work), probabilistic confirmation, probabilistic security, probabilistic settlement.

Source: 04-IN - The Institutional Counterpoint: The BIS Critique.

Probabilistic Lead. An inference that helps guide an investigation but does not by itself prove ownership, intent, or identity. Aliases: Probabilistic Lead (blockchain forensics), heuristic lead, investigative lead.

Source: 02-FO - Pitfalls & Counter-Heuristics.

Probability space. A mathematical model of possible outcomes and events used to reason about uncertainty. Aliases: sample space.

Source: 01-CP - Probability Refresher: Events and Outcomes.

Problem fit. The match between a system design and the scenario's trust boundary, governance needs, performance demands, and verification requirements. Aliases: Problem fit (ledger design), best fit, tool choice.

Source: 01-PC - When To Use What?.

Process. An independently running participant in a distributed consensus protocol. Aliases: Process (consensus), node, participant.

Source: 01-CM - Foundations of Consensus.

Programmability. The ability to encode asset behavior, settlement rules, access conditions, or compliance logic in software. Aliases: Programmability (tokenization), programmable assets.

Source: 05-EF - Why Tokenize? Problems and Promises.

Programmable claim. A claim whose creation, ownership, transfer, or state changes are governed by code rather than manual recordkeeping.

Source: 06-EF - What Is a Token?.

Programmable coordination. The use of shared rules, consensus, verification, and smart contracts to coordinate activity among participants. Aliases: Programmable coordination (blockchain technology).

Source: 05-AS - What Is Blockchain Really?.

Programmable money. Money or payment instruments that can execute rules, conditions, or automated logic as part of transfer and settlement. Aliases: programmable payments.

Source: 05-AS - Future 1: Global Settlement Layer.

Programmable rights. Rights or claims whose access, transfer, or behavior can be controlled by software rules rather than only manual administration. Aliases: Programmable rights (tokenization), programmable claims, programmable right.

Source: 05-EF - Looking Forward: Dynamic Assets.

Programmable spending condition. A rule encoded in a Bitcoin output that specifies what must be provided before that output can be spent. Aliases: Programmable spending condition (Bitcoin Script), spending condition.

Source: 03-BF - Introduction to Bitcoin Script.

Programmable state. Shared blockchain state that can be changed by on-chain logic rather than only by simple payments. Aliases: Programmable state (Ethereum), general-purpose programmable state.

Source: 04-AS - Ethereum's Goals.

Project Aber. A UAE-Saudi central-bank experiment testing whether a shared wholesale digital currency could improve cross-border interbank settlement. Aliases: Aber.

Source: 03-AS - Gulf States: Impact Signals.

Project mBridge. A multi-central-bank platform for testing faster and more direct cross-border settlement using shared digital rails. Aliases: mBridge.

Source: 03-AS - Gulf States: Impact Signals.

Proof of Stake. A consensus approach where participants prove eligibility to help add or confirm blocks by staking assets under protocol rules. Aliases: PoS, Proof of Stake (Ethereum consensus), Proof of Stake (Ethereum post-Merge consensus), Proof of Stake (consensus cost), Proof of Stake (consensus mechanism), Proof of Stake (consensus), Proof-of-Stake, proof-of-stake.

Source: 02-IN - Pillar 3: Consensus.

Proof of Work. A consensus approach where participants prove eligibility to add a block by performing computational work. Aliases: PoW, Proof of Work (Bitcoin consensus), Proof of Work (Bitcoin), Proof of Work (Ethereum pre-Merge consensus), Proof of Work (consensus cost), Proof of Work (consensus mechanism), Proof of Work (consensus), Proof-of-Work, Proof-of-Work (Bitcoin consensus mechanism), proof of work, proof-of-work, work.

Source: 02-IN - Pillar 3: Consensus.

Proof-of-space puzzle. A resource-binding puzzle where participants prove they have committed storage rather than repeatedly burning computation. Aliases: proof of space, storage-based puzzle.

Source: 02-CM - Proof-of-work Puzzles.

Proof-of-useful-work. A PoW design goal where the expensive computation also produces externally useful scientific or computational output. Aliases: useful proof of work.

Source: 02-CM - Proof-of-work Puzzles.

Proof-of-work puzzle. A computational challenge that is expensive to solve but quick for other nodes to verify. Aliases: PoW puzzle.

Source: 02-CM - Proof-of-work Puzzles.

Propagation asymmetry. Uneven message delivery that gives different validators different views of blocks or attestations at the same time. Aliases: Propagation asymmetry (Ethereum network), attestation delay, message delay.

Source: 02-EF - Balance Attack.

Proposal. A signed client request sent to endorsing peers asking them to simulate a chaincode action. Aliases: Proposal (Hyperledger Fabric), signed proposal, transaction proposal.

Source: 02-PC - One Invoke: Proposal to Commit.

Proposal simulation. The pre-order execution step where endorsers run chaincode against current state to compute a proposed result without committing it. Aliases: Proposal simulation (Hyperledger Fabric), chaincode simulation, simulation.

Source: 02-PC - Chaincode: What It Is and How It Runs.

Propose phase. The phase in a round where the leader suggests the candidate value for participants to consider. Aliases: Propose phase (consensus), propose.

Source: 01-CM - Rounds and Phases.

Proposer boost. A fork-choice weight bonus for the current slot's block when validators see it on time. Aliases: Proposer boost (Ethereum fork choice), proposer boost timing.

Source: 02-EF - Balance Attack.

Proposer-builder separation. A block production design that separates the validator duty of proposing a block from the specialized work of building it. Aliases: PBS, Proposer-builder separation (Ethereum MEV).

Source: 03-EF - Builder / Relay Stack and MEV.

proposer_index. A beacon-block field identifying the validator selected to propose that block. Aliases: proposer index, proposer_index (beacon block field).

Source: 02-EF - Beacon Blocks and Execution Payloads.

Proto-Danksharding. An Ethereum upgrade that introduced temporary blob data for rollups as a step toward cheaper data availability. Aliases: EIP-4844, Proto-Danksharding (Ethereum scaling upgrade), proto-danksharding.

Source: 01-EF - Proto-Danksharding (EIP-4844) — Blob Data for L2s.

Protocol coordination. Aligning many independent participants through shared rules and incentives instead of central management. Aliases: protocol-governed coordination.

Source: 01-AS - Infrastructure as a Use Case.

Protocol governance friction. The difficulty of changing Bitcoin's protocol because broad agreement is needed across a decentralized ecosystem. Aliases: Protocol governance friction (Bitcoin), governance friction, slow adoption.

Source: 01-BF - Limitations and Trade-Offs.

Protocol migration strategy. A planned process for moving a blockchain network, wallets, clients, exchanges, and users to new cryptographic or protocol rules. Aliases: Protocol migration strategy (quantum transition), migration strategy, staged upgrade.

Source: 05-AS - What Can Be Done.

Provenance. A verifiable history of ownership, transfers, or state changes associated with an asset. Aliases: Provenance (supply chain), Provenance (tokenization), asset history, asset provenance, origin history, ownership history, product history.

Source: 05-EF - Why Tokenize? Problems and Promises.

Provenance graph. A graph of ownership and transfer relationships used to inspect an asset's history and spot suspicious or fake activity. Aliases: Provenance graph (NFT verification), provenance graphs.

Source: 05-EF - Common Pitfalls in NFT Projects.

Provenance marker. A recorded attribute or event that helps reconstruct an asset's origin, custody, compliance status, or transformation history. Aliases: Provenance marker (embedded provenance), provenance metadata, semantic context.

Source: 01-FO - Future of Forensics: Embedded Provenance.

Prover. An L2 operator role that produces a proof or claim that Ethereum can later check under the rollup's rules. Aliases: Prover (L2 operator), provers.

Source: 01-EF - L2 Operator Models.

Proxy Contract. A contract that forwards calls to a separate implementation contract where the actual execution logic lives. Aliases: EIP-1967 proxy, Proxy Contract (Ethereum), proxy contracts.

Source: 02-FO - Smart Contract Forensics.

Proxy pattern. An upgrade design that keeps state and the user-facing address in a proxy while delegating execution to replaceable logic code. Aliases: Proxy pattern (smart contract upgradeability), proxy contract, upgradeable proxy.

Source: 04-EF - Upgradeability and Proxy Patterns.

Pseudonymity. A privacy model where public addresses appear on-chain instead of real names, but activity can still be linked and analyzed. Aliases: Pseudonymity (Bitcoin), Pseudonymity (blockchain forensics), Pseudonymity (blockchain privacy), Pseudonymity (blockchain), ownership without identity, pseudonymous, pseudonymous address, pseudonymous identity.

Source: 02-IN - Common Misconceptions: What a Blockchain is NOT.

Pseudonymous. Identified by addresses or keys rather than real-world names, while activity may still be visible on-chain. Aliases: Pseudonymous (blockchain identity), pseudonymity.

Source: 02-AS - Types of Digital Money.

Pseudonymous coordination. Decision-making and value transfer among participants identified by addresses or handles rather than verified legal identities. Aliases: Pseudonymous coordination (token governance), pseudonymous coordination at scale.

Source: 06-EF - Analyst Implications.

Pseudonymous identity. Identity represented by cryptographic keys rather than verified real-world names. Aliases: Pseudonymous identity (permissionless ledgers), pseudonymity, pseudonymous keys.

Source: 04-DS - Permissioned vs. Permissionless: Comparison.

Pseudorandom function. A keyed function whose outputs should be computationally indistinguishable from random for anyone without the key. Aliases: PRF, keyed pseudorandom function.

Source: 03-CP - Counter-Mode Pseudorandom Generator (PRG).

Pseudorandom generator. An algorithm that expands a short random seed into a longer sequence that should appear random to efficient observers. Aliases: PRG, PRNG, pseudorandom number generator.

Source: 01-CP - Sets and Functions.

Pseudorandom number generator. A deterministic generator that produces random-looking outputs from a seed but may not be secure against prediction. Aliases: PRNG, Pseudorandom number generator (implementation failure), general-purpose PRNG.

Source: 05-CP - When Good Crypto Goes Bad: Milk Sad (CVE-2023-39910).

Pub/Sub overlay. A networking layer where peers subscribe to message topics and receive broadcasts relevant to those topics. Aliases: Pub/Sub overlay (Ethereum consensus layer), pub/sub, publish-subscribe overlay.

Source: 03-EF - Consensus-Layer Networking (libp2p / GossipSub).

Public auditability. The property that anyone can inspect the public ledger history to check recorded transactions and validation outcomes. Aliases: Public auditability (Bitcoin), publicly auditable transactions.

Source: 04-DS - Case Study C — Bitcoin Ledger (Permissionless).

Public Blockchain. A blockchain network that is broadly accessible and not operated as a closed internal ledger by one institution. Aliases: open blockchain, public chain.

Source: 03-AS - How Blockchain Changes State Power.

Public exponent. The RSA public-key exponent chosen to work with the private exponent and the modulus. Aliases: Public exponent (RSA), e.

Source: 04-CP - RSA Key Generation Overview.

Public goods. Work or infrastructure that benefits an ecosystem broadly but is difficult to monetize through ordinary markets. Aliases: Public goods (Gitcoin), public-goods funding.

Source: 06-EF - Case Study: Gitcoin.

Public key. The key that others can use to verify a signature made with the corresponding private key. Aliases: Public key (Bitcoin ownership), Public key (Bitcoin), public keys, public verification key, verification key.

Source: 02-IN - Pillar 1: Cryptography.

Public key hash. The hash of a public key that a P2PKH locking script requires the spender to match. Aliases: Public key hash (P2PKH), pubKeyHash.

Source: 03-BF - Bitcoin Script Basics.

Public Key Infrastructure. The certificate and identity-management infrastructure used to bind participants or organizations to cryptographic credentials. Aliases: PKI, Public Key Infrastructure (permissioned ledgers), Public Key Infrastructure (trust model), public key infrastructure.

Source: 04-DS - Common Pitfalls.

Public ledger. The publicly propagated record of transactions and blocks that nodes use to agree on one history. Aliases: Public ledger (Bitcoin), global history, shared ledger, shared public record, transparent ledger.

Source: 01-BF - Bitcoin, Simplified.

Public legitimacy. The social and political acceptance needed for a technology to be trusted, permitted, and adopted at scale. Aliases: Public legitimacy (blockchain adoption), legitimacy.

Source: 05-AS - External Constraints.

Public mempool. The default state in which pending Ethereum transactions can be observed by anyone running appropriate node infrastructure. Aliases: Public mempool (Ethereum), public pending transaction pool.

Source: 03-EF - The Mempool.

Public mint. A minting pattern where anyone can call the mint function, usually constrained only by price, timing, or supply cap. Aliases: open mint.

Source: 06-EF - Minting on Ethereum.

Public verifiability. The property that validator assignments, votes, and punishment evidence can be checked by other participants from public protocol data. Aliases: Public verifiability (PoS), publicly verifiable.

Source: 03-CM - Orientation: Proof of Work vs Proof of Stake.

Public-key cryptography. A cryptographic model that separates a private signing key from public material used to verify signatures. Aliases: asymmetric crypto, asymmetric cryptography.

Source: 04-AS - Asymmetric Crypto and Digital Signatures.

Public-Key Infrastructure. A system of certificates, authorities, and validation rules that binds identities to public keys. Aliases: PKI, public key infrastructure.

Source: 04-CP - Certificates and PKI Hierarchy.

Pull payment. A payment design where recipients withdraw funds themselves instead of the contract pushing funds during unrelated logic. Aliases: Pull payment (smart contract security), pull over push payments, withdrawal-based payment.

Source: 04-EF - Reentrancy: Anatomy and Defenses.

Purchasing Power. The amount of goods or services a given amount of money can buy.

Source: 04-IN - The Problem of Value: The Specter of Inflation.

Q

Quadratic funding. A matching-fund mechanism where broad support from many contributors can receive more weight than a few large donations.

Source: 06-EF - Case Study: Gitcoin.

Quantum computing. A computing model that uses quantum effects to speed up certain structured problems that underlie cryptographic security. Aliases: Quantum computing (cryptography), quantum computers.

Source: 05-CP - Quantum Primer: Why It Matters for Cryptography.

Quantum error correction. Techniques for protecting fragile quantum computations from noise long enough to run useful algorithms. Aliases: error correction.

Source: 05-CP - Shor's Algorithm (1994): Breaking RSA and ECC.

Quantum risk. The risk that future quantum algorithms could undermine current public-key systems more severely than hash functions. Aliases: Quantum risk (cryptography), post-quantum risk, quantum threat.

Source: 04-AS - Cryptographic Challenges Moving Forward.

Qubit. A quantum information unit that can participate in superposition and entanglement rather than storing only a classical 0 or 1. Aliases: qubits.

Source: 05-CP - Quantum Primer: Why It Matters for Cryptography.

Quorum. A required amount of participant support before a protocol treats a proposal or decision as valid. Aliases: Quorum (consensus), Quorum (permissioned consensus), quorum rule, quorum threshold, threshold.

Source: 01-CM - Consensus in the Real World.

Quorum certificate. Portable evidence that a round gathered enough matching votes to move forward safely. Aliases: QC, Quorum Certificate (PoS vote aggregation), Quorum certificate (consensus), aggregate signature, aggregated signatures, quorum certificate.

Source: 01-CM - Rounds and Phases.

Quorum disruption. An attack or outage that prevents enough authorized approvers from participating to meet a quorum rule. Aliases: approval disruption, preventing quorum.

Source: 01-PC - Threats to Permissioned Systems.

Quorum overlap. The property that any two valid quorums share enough membership to include at least one honest participant. Aliases: quorum intersection.

Source: 01-CM - Practical Consensus Design.

Quorum rule. A validation rule that accepts a result only after enough independent participants agree. Aliases: Quorum rule (volunteer computing), quorum rules.

Source: 01-DS - Volunteer Computing Pipeline: BOINC.

Quorum size. The number of matching participants required to form a valid BFT quorum for a given fault threshold. Aliases: $2t + 1$, Quorum size (BFT).

Source: 01-CM - Quorums.

Quorum system. A protocol rule requiring a minimum number of consistent responses before treating a decision as authoritative. Aliases: quorum, quorums.

Source: 05-IN - Strategies for Handling Suspicion.

R

Raft. A classical consensus algorithm designed to make leader-based replicated consensus easier to understand and implement. Aliases: Raft (Hyperledger Fabric ordering), Raft consensus, Raft ordering.

Source: 05-IN - Classical Consensus Approaches.

Rail Competition. Rivalry among different systems for moving and settling value at scale. Aliases: financial rail competition, payment rail competition.

Source: 03-AS - Competing Financial Infrastructures.

Rainbow table. A precomputed table of candidate inputs and hashes used to speed up guessing against unsalted hashes. Aliases: precomputed lookup table, rainbow table attack.

Source: 02-CP - Aside: Hash Salting.

RANDAO. Ethereum's production mechanism for building shared randomness from proposer reveals over time. Aliases: RANDAO (Ethereum PoS), RANDAO (Ethereum randomness), RANDAO seed, rolling randomness.

Source: 02-EF - Validator Selection & Randomness.

randao_reveal. A proposer's BLS signature included in a beacon block and mixed into Ethereum's rolling randomness state. Aliases: RANDAO reveal, randao reveal, randao_reveal (beacon block field).

Source: 02-EF - Beacon Blocks and Execution Payloads.

Random variable. A numeric value assigned to the outcome of a random process. Aliases: random variables.

Source: 01-CP - Probability Refresher: Independence & Random Variables.

Randomness. Unpredictability with no discernible pattern from the perspective of an observer or attacker. Aliases: true randomness.

Source: 01-CP - Probability Refresher: Events and Outcomes.

Ransomware extortion. A criminal payment demand made after malware disrupts or threatens a victim's systems or data. Aliases: Ransomware extortion (illicit finance), ransom demand, ransomware payment.

Source: 01-FO - Permissionless Finance.

Ransomware-as-a-service. A criminal model where operators provide ransomware tooling or infrastructure to affiliates who conduct attacks. Aliases: RaaS.

Source: 01-FO - Case Study: Colonial Pipeline.

Rater credibility. The trustworthiness of the peer providing a rating, used to decide how much that rating should affect the final score. Aliases: reviewer credibility.

Source: 03-DS - PeerTrust: How Trust Is Calculated.

Reachable node. A Bitcoin node that accepts inbound network connections from other peers. Aliases: Reachable node (Bitcoin network), listening node, publicly reachable node.

Source: 03-BF - Elements of the Bitcoin Network.

Read-write set. The proposed transaction output listing which ledger keys were read, which versions were observed, and which values should be written. Aliases: RW set, Read-write set (Hyperledger Fabric), read write set, read-write set.

Source: 02-PC - Chaincode: What It Is and How It Runs.

Real-world asset. An off-chain asset such as fiat currency, commodities, securities, invoices, or property represented by a tokenized claim. Aliases: RWA, RWAs, Real-world asset (tokenization), real-world assets.

Source: 05-EF - A Taxonomy of Digital Assets.

Rebranding attack. An attack where a peer with a bad reputation abandons its identity and rejoins as a new participant. Aliases: clean slate attack, identity reset.

Source: 03-DS - Threats: Rebranding Attacks.

receipts_root. The header commitment to execution results such as status, gas used, and emitted logs. Aliases: receipts root, receipts_root (Ethereum execution payload).

Source: 02-EF - Execution Payload: Header Structure.

Receive function. A special Solidity function that handles plain ETH transfers sent without calldata. Aliases: Receive function (Solidity), receive.

Source: 04-EF - ABI, Encoding, and Function Selectors.

Recency weighting. A scoring method that gives recent behavior more influence than older behavior. Aliases: recency decay.

Source: 03-DS - Threats: On–Off (Reputation Milking).

Recommender credibility. A measure of how much weight to give a peer's recommendation based on that peer's own trustworthiness. Aliases: recommender quality.

Source: 03-DS - Direct vs. Indirect Trust.

Recursive Length Prefix. Ethereum's legacy byte encoding format for deterministic serialization of nested lists and byte strings. Aliases: RLP, RLP encoding, Recursive Length Prefix (Ethereum encoding).

Source: 03-EF - ETH Execution-Network Message.

Redemption. The process of exchanging a token for the underlying off-chain asset, cash value, or legally recognized claim. Aliases: Redemption (real-world asset token), redeem, redemption gates.

Source: 05-EF - Real-World Assets (RWAs) and Tokenization.

Redemption risk. The risk that holders cannot reliably exchange a stablecoin for the reference asset at the expected value. Aliases: Redemption risk (stablecoin).

Source: 02-AS - Stablecoins: Types and Mechanisms.

Reduction. A logical transformation showing that breaking one scheme would also solve another problem believed to be hard. Aliases: Reduction (cryptographic proof), security reduction.

Source: 01-CP - Proofs and Reasoning.

Redundancy. The use of extra components or copies so a system can keep operating when one component fails. Aliases: Redundancy (permissioned ledger operations), redundant services.

Source: 05-IN - Crash Faults.

Reentrancy. A vulnerability pattern where an external call lets another contract call back into the original contract before the first execution finishes safely. Aliases: Reentrancy (smart contract risk), Reentrancy (smart contract security), recursive call pattern, reentrancy bug, reentrant call, reentrant execution, reentry.

Source: 04-EF - Reentrancy: Anatomy and Defenses.

Reentrancy vulnerability. A bug where external calls let an attacker reenter contract logic before state such as balances is safely updated. Aliases: Reentrancy vulnerability (smart contract security), recursive withdraw bug, reentrancy.

Source: 02-EF - Real-World Ethereum Security Examples.

ReentrancyGuard. A library-style guard that blocks a protected function from being entered again before the first call finishes. Aliases: ReentrancyGuard (smart contract security), mutex, nonReentrant, reentry lock.

Source: 04-EF - Reentrancy: Anatomy and Defenses.

Reference type. A Solidity type category for larger data structures whose behavior depends on where the data is stored. Aliases: Reference type (Solidity), reference types.

Source: 04-EF - Types: Reference Types.

Regulated intermediary. A business such as an exchange, custodian, broker, or payment processor that must apply legal compliance controls around Bitcoin activity. Aliases: Regulated intermediary (Bitcoin), covered intermediary, regulated gateway.

Source: 04-BF - Off-Chain Controls: KYC and AML.

Regulated perimeter. The boundary where activity enters services subject to identity, monitoring, and reporting obligations. Aliases: Regulated perimeter (Bitcoin), compliance perimeter, regulated edge.

Source: 04-BF - How KYC/AML Apply to Bitcoin.

Regulation and compliance. The legal rules and required controls that shape who may build, issue, custody, transact, or scale blockchain systems. Aliases: Regulation and compliance (blockchain adoption), compliance, regulatory compliance.

Source: 05-AS - External Constraints.

Regulatory chokepoint. A service or interface where rules can be enforced because crypto activity touches banks, exchanges, bridges, or other identifiable operators. Aliases: Regulatory chokepoint (crypto policy), chokepoint, compliance chokepoint, regulated chokepoint.

Source: 01-FO - Forensic Countermeasures.

Regulatory classification. The legal categorization of an asset or service, such as security or commodity, that determines which rules apply. Aliases: Regulatory classification (digital assets), asset classification, legal classification.

Source: 01-AS - Regulation and Uncertainty.

Regulatory surface. The parts of a system where regulators can impose rules, supervision, sanctions compliance, or enforcement. Aliases: Regulatory surface (stablecoin).

Source: 02-AS - Stablecoins: Types and Mechanisms.

Regulatory uncertainty. Unsettled or uneven legal treatment that makes user access, platform behavior, and market outcomes harder to predict. Aliases: Regulatory uncertainty (crypto markets), legal uncertainty, unclear rules.

Source: 01-AS - Regulation and Uncertainty.

Relay. Infrastructure that passes builder-created candidate blocks to validators, often through MEV-Boost. Aliases: MEV relay, Relay (Ethereum block building), relays.

Source: 02-EF - Censorship.

Relay policy. A node's local rules for which valid transactions it will keep, filter, rate-limit, or forward to peers. Aliases: Relay policy (Bitcoin node), mempool policy, policy rules.

Source: 03-BF - Decisions Nodes Make.

Remote Procedure Call. A request-response interface that wallets and apps use to ask blockchain nodes for data or to submit transactions. Aliases: RPC, Remote Procedure Call (blockchain access).

Source: 01-AS - Walking a Transaction Step-by-Step.

Reorg risk. The risk that a recent accepted branch will be replaced by another valid branch with more cumulative work. Aliases: Reorg risk (Bitcoin), chain reorg risk, reorganization risk.

Source: 01-BF - Security Model & Threats.

Reorganization. A change in the canonical chain where nodes replace one recent branch with a longer or heavier competing branch. Aliases: Reorganization (blockchain), chain reorg, reorg, reorgs.

Source: 02-CM - Attacks: Double Spend.

Replacement transaction. A transaction that reuses the same account nonce with a higher fee to supersede an earlier pending transaction. Aliases: Replacement transaction (Ethereum), replace-by-fee, transaction replacement.

Source: 03-EF - The Mempool.

Replication. The practice of maintaining multiple copies or instances so answers can be compared and service can continue after failures. Aliases: Replication (P2P storage), Replication (distributed ledgers), Replication (distributed systems), data replication, replica, replicas, replicate, replicated components, replicated copy, replicated state.

Source: 05-IN - Commission Faults.

Representative Money. Money that represents a redeemable claim on an underlying asset held elsewhere, such as gold or silver in a vault.

Source: 04-IN - A Brief History of Money's Form.

Reputation. A summary of a peer's past behavior used to estimate whether that peer is likely to behave correctly in the future. Aliases: Reputation (P2P trust).

Source: 03-DS - What Is "Trust" in P2P?.

Reputation milking. A strategy where a peer builds a good track record on low-risk actions and then exploits that reputation for a more damaging failure. Aliases: milking reputation.

Source: 03-DS - PeerTrust: Handling Manipulation.

Reputation system. A scoring system that aggregates evidence about peer behavior so participants can choose whom to trust. Aliases: trust system.

Source: 03-DS - Properties of Reputation Systems.

Reputation-based selection. Choosing peers for an interaction based on established track records and trust scores.

Source: 03-DS - Trust but Verify: The Complete Trust Loop.

Require check. A Solidity guard that stops execution and reverts when a required condition is not true. Aliases: Require check (Solidity), precondition check, require.

Source: 04-EF - Example: Coin (Code, Part 1).

Required approvals. The policy-defined set of organizations or nodes that must approve a proposed action. Aliases: Required approvals (transaction policy), approval requirements, organizational signoffs.

Source: 01-PC - Transaction Path.

Reserve. The assets or collateral meant to support confidence that a stablecoin can be redeemed at its target value. Aliases: Reserve (stablecoin), backing assets, reserves.

Source: 02-AS - Stablecoins: Types and Mechanisms.

Reserve Currency. A currency widely held and used by governments and institutions for international settlement and reserves. Aliases: world reserve currency.

Source: 04-IN - The Turning Point: Ending Bretton Woods.

Retail CBDC. A public-facing central bank digital currency intended for citizens, businesses, and everyday payments. Aliases: retail CBDCs, retail central bank digital currency, retail central-bank digital currency.

Source: 02-AS - Central Bank Digital Currencies (CBDCs).

Retry. A resilience pattern where a failed or uncertain operation is attempted again, usually with limits or backoff. Aliases: Retry (distributed systems), retries, retrying.

Source: 01-DS - Availability, MTTF, and MTTR.

Reversibility. The ability of a trusted institution to undo or correct a transaction, especially when fraud occurs.

Source: 03-IN - Digital Trust: The Centralized Model.

Revert. The rollback of state changes from a failed EVM execution while gas already spent remains charged. Aliases: Revert (EVM execution), Revert (EVM), Revert (Ethereum execution), reversion, reverted, reverted transaction, reverts, state revert, transaction revert.

Source: 01-EF - Transaction Lifecycle (PoS Era).

Right-click save critique. The claim that copying NFT-linked media defeats NFT ownership, which confuses copying a file with controlling the token record. Aliases: Right-click save critique (NFT misconception), right click save, right-click save.

Source: 05-EF - Critiques and Misunderstandings.

Ring Signature. A signature scheme that proves one member of a group signed without revealing which member was the true signer. Aliases: Ring Signature (Monero), Ring signature (Monero privacy), ring signatures.

Source: 02-FO - Monero (XMR): Privacy by Default.

RingCT. Monero's confidential transaction mechanism that hides transaction amounts while still allowing supply validity checks. Aliases: Ring Confidential Transactions, RingCT (Monero privacy), RingCT (Monero), confidential transactions.

Source: 02-FO - Monero (XMR): Privacy by Default.

RLPx. The encrypted session layer used by devp2p peers to authenticate, frame, and multiplex execution-layer traffic. Aliases: RLPx (Ethereum execution layer), RLPx transport.

Source: 03-EF - ETH Execution-Network Message.

Robustness. The ability of a reputation system to resist manipulation by fake identities, collusion, slander, and other attacks. Aliases: Robustness (reputation systems).

Source: 03-DS - Properties of Reputation Systems.

Role-based access control. An access-control method where permissions are assigned to roles rather than individually to every action. Aliases: RBAC.

Source: 01-PC - Privacy.

Role-based trust. A trust model where participants are allowed to perform only the actions assigned to their verified roles. Aliases: role-based trust model.

Source: 01-PC - Open vs Curated Admission.

Rollback. A coordinated move to abandon a chain segment and reorganize onto an earlier valid branch. Aliases: Rollback (blockchain incident response), chain rollback, rollback past a block.

Source: 04-BF - Emergency Response to the Overflow Bug.

Rollup. A Layer 2 system that batches execution off-chain and posts enough data, claims, or proofs back to Ethereum for verification. Aliases: Rollup (Ethereum L2), Rollup (Ethereum scaling), rollup-style L2, rollups.

Source: 01-EF - L2 Operator Models.

Ronin Bridge. An Ethereum-linked bridge for the Axie Infinity ecosystem that was drained after attackers compromised enough validator approvals. Aliases: Ronin, Ronin Bridge (case study).

Source: 01-FO - Case Studey: Ronin Bridge.

Root CA. A self-signed Certificate Authority at the top of a PKI hierarchy that acts as an ultimate trust anchor. Aliases: root certificate authority, trust anchor.

Source: 04-CP - Certificates and PKI Hierarchy.

Root of trust. The ultimate authority in a system whose decisions establish the validity of lower-level participants or credentials.

Source: 02-AS - Trust Architecture: CBDCs vs Permissionless Systems.

Rough consensus. An informal adoption process where independent operators converge on a protocol change without being forced by a central authority. Aliases: Rough consensus (permissionless governance), operator consensus.

Source: 04-DS - Governance Models.

Round. One repeated step of a block cipher that combines operations such as substitution, permutation, and key mixing. Aliases: Round (block cipher), rounds.

Source: 03-CP - Building Blocks of Block Ciphers.

Round key. A per-round key value derived from the main secret key for use inside a block cipher. Aliases: round keys.

Source: 03-CP - Building Blocks of Block Ciphers.

Round trip. A request-and-response exchange whose delay accumulates when a protocol requires many sequential steps. Aliases: Round trip (network protocol), back-and-forth exchange, round trips.

Source: 01-DS - Fallacy #2: Latency Is Zero.

Route leak. An Internet routing incident where routes are incorrectly propagated, causing traffic to take unintended paths. Aliases: routing leak.

Source: 04-BF - Partitioning Attacks.

Routing bias. A connection-selection flaw that makes peers over-connect within one region or group and under-connect to the rest of the network.

Source: 02-DS - Partitions & Healing.

Routing state. The local neighbor and shortcut information a peer maintains so it can forward messages toward useful next hops. Aliases: Routing state (P2P overlay), routing information, routing table state.

Source: 02-DS - Structured Overlay Networks.

Royalty. A creator payment preference associated with NFT resales that marketplaces may choose to honor or bypass. Aliases: Royalty (NFT marketplace), creator royalties, creator royalty, royalties.

Source: 05-EF - Royalties, Economics, and Marketplace Realities.

Royalty signaling. A contract-level declaration of royalty recipient and basis points for secondary sales, without guaranteeing marketplace enforcement. Aliases: EIP-2981, NFT royalty signaling, Royalty signaling (NFT).

Source: 06-EF - Minting on Ethereum.

RPC node. A node interface that lets clients or services submit requests to blockchain infrastructure. Aliases: RPC node (bridge security), gas-free RPC node, remote procedure call node.

Source: 01-FO - Ronin: Key Management.

RPC provider. A service that lets wallets and dApps read from and send transactions to Ethereum nodes through an API. Aliases: RPC provider (Ethereum infrastructure), RPC provider (access layer), RPC providers, node provider, node providers, remote procedure call provider.

Source: 06-EF - Centralization Chokepoints.

RSA. A public-key cryptosystem based on the difficulty of factoring large composite numbers. Aliases: RSA (quantum vulnerability), Rivest-Shamir-Adleman.

Source: 04-CP - RSA Emerges.

RSA modulus. The public composite number produced by multiplying RSA's two secret primes. Aliases: modulus n, n.

Source: 04-CP - RSA Key Generation Overview.

RSA padding. A structured encoding added around RSA inputs so real deployments avoid the weaknesses of raw textbook RSA equations. Aliases: OAEP, RSA-PSS, padding scheme.

Source: 04-CP - RSA Encryption & Decryption.

RSA signature. An RSA-based signature that applies the private exponent to a message digest and is checked with the public exponent. Aliases: RSA digital signature.

Source: 04-CP - Example: RSA Signature.

Rug pull. A project-driven exit scam or abandonment in which operators collect user funds or value and then disappear, drain assets, or break promised utility. Aliases: Rug pull (token project), exit scam, rug pulls.

Source: 06-EF - The Frosties Rug Pull.

Runtime bytecode. The bytecode that remains stored at a contract address after deployment and is executed by future calls. Aliases: Runtime bytecode (Ethereum), runtime code.

Source: 04-EF - Contract Deployment.

S

Safety. The guarantee that honest nodes do not finalize conflicting values or contradictory system states. Aliases: Safety (consensus property), Safety (consensus), consensus safety, consistency, safety property.

Source: 05-IN - Consensus as the Core Goal.

Salt. An added random value that makes otherwise similar inputs produce different cryptographic results. Aliases: Salt (hashing), hash salting, salting, salts.

Source: 01-CP - What Is Randomness?.

Sanctioning infrastructure. Targeting services, contracts, or operational tools that enable laundering rather than only the original theft actor. Aliases: Sanctioning infrastructure (crypto policy), infrastructure sanctions, sanctioning the infrastructure.

Source: 01-FO - Ronin: From Trace to Takedown.

Sanctions. Legal restrictions that bar interaction with designated entities, actors, contracts, or infrastructure. Aliases: Sanctions (crypto policy), designation, economic sanctions, financial sanctions, sanctions enforcement.

Source: 01-FO - Policy & Regulatory Response.

Sanctions evasion. The use of financial paths or infrastructure to bypass formal economic restrictions on designated actors, entities, or jurisdictions. Aliases: Sanctions evasion (illicit finance), sanctions avoidance.

Source: 01-FO - Permissionless Finance.

Sanctions power. The ability to restrict financial activity by controlling access to payment networks, settlement systems, or banking relationships. Aliases: Sanctions power (payment infrastructure), sanctions enforcement, sanctions leverage.

Source: 02-AS - Global Payment Infrastructure: Overview.

Sanctions Resilience. The ability to keep operating economically despite external restrictions on payments, banking, reserves, or trade. Aliases: sanctions resistance.

Source: 03-AS - How Blockchain Changes State Power.

Sanctions screening. The process of checking customers, counterparties, or transaction exposure against sanctions restrictions and risk lists. Aliases: Sanctions screening (AML), sanctions exposure screening.

Source: 04-BF - How KYC/AML Apply to Bitcoin.

Sandwich attack. An MEV strategy that places transactions before and after a user's swap to profit from the induced price movement. Aliases: Sandwich attack (MEV), front/back-run, sandwiching.

Source: 03-EF - The Mempool.

Satoshi. The smallest bitcoin unit, equal to 0.00000001 BTC. Aliases: Satoshi (Bitcoin), sat.

Source: 02-BF - Transactions and the UTXO Model.

Satoshi Nakamoto. The pseudonymous author who released the Bitcoin whitepaper and early software, with the real identity still unknown. Aliases: Nakamoto.

Source: 01-BF - Satoshi Nakamoto's Whitepaper.

Scalability. A blockchain system's ability to handle greater usage while maintaining acceptable cost, speed, and reliability. Aliases: Scalability (Bitcoin), Scalability (blockchain systems), Scalability (blockchain), Scalability (reputation systems), scaling, throughput.

Source: 01-IN - Learning Objectives II.

Scalability trilemma. The design tension where security, decentralization, and scalability are difficult to maximize at the same time. Aliases: Scalability trilemma (blockchain design), blockchain trilemma.

Source: 01-EF - The Scaling Problem.

Scalar multiplication. The elliptic-curve operation of repeatedly adding a point to itself according to a private integer. Aliases: Scalar multiplication (ECC), kP, point multiplication.

Source: 04-CP - Elliptic Curve Cryptography (ECC).

Scaling layer. An additional protocol or system that improves transaction throughput or cost while depending on another chain or trust model. Aliases: L2, Scaling layer (blockchain), layer 2, scaling layers.

Source: 05-AS - Technical Constraints.

Scarcity. The design property that bitcoin issuance is limited and tied to costly work rather than unlimited creation. Aliases: Scarcity (Bitcoin), costliness.

Source: 01-BF - Lessons from Precursors.

Script execution stack. The stack on which Bitcoin nodes evaluate unlocking data and locking-script operations to decide whether a spend is valid. Aliases: Script execution stack (Bitcoin Script), execution stack, stack.

Source: 03-BF - Bitcoin Script Basics.

Searcher. An off-chain actor that scans pending transactions and market state for profitable MEV opportunities. Aliases: MEV searcher, Searcher (MEV), searchers.

Source: 03-EF - The Mempool.

Second pre-image resistance. The property that, given one known input, it should be infeasible to find a different input with the same digest. Aliases: second-preimage resistance.

Source: 02-CP - Hash Function Properties.

Second-preimage resistance. The property that it is hard to find a different input with the same digest as a chosen existing input. Aliases: second preimage resistance, second-pre-image resistance.

Source: 04-AS - Hash Properties That Matter for Blockchain.

Secondary market. Trading that happens after the initial NFT mint or sale, usually through marketplaces and open offers. Aliases: Secondary market (NFT), resale market, secondary markets.

Source: 05-EF - Royalties, Economics, and Marketplace Realities.

Secret key. A private value used with a public algorithm to control encryption, authentication, signing, or other cryptographic behavior. Aliases: key, secret keys.

Source: 01-CP - From Secrecy to Integrity.

Security. The difficulty an attacker faces in compromising the network or reversing transactions. Aliases: Security (blockchain trilemma property).

Source: 04-IN - The Engineer's Dilemma: The Blockchain Trilemma.

Security bit-strength. A shorthand measure of the computational effort an attacker is expected to need, expressed as an equivalent number of key or digest bits. Aliases: bit-strength, security bits.

Source: 05-CP - Grover's Algorithm (1996).

Security budget. The ongoing rewards that sustain honest mining, mainly block subsidies and transaction fees. Aliases: PoW security budget, Security budget (PoS), Security budget (proof of work), chain security budget.

Source: 02-CM - Security Model and Economics.

Security margin. The gap between the best known attack cost and the level of effort a system is meant to withstand. Aliases: Security margin (cryptography), security margins.

Source: 05-CP - Cryptographic Assumptions Decay Over Time.

Security proof. A formal argument that a cryptographic claim follows from stated assumptions and logical rules. Aliases: proof, proofs.

Source: 01-CP - Proofs and Reasoning.

Security through obscurity. A fragile security model that depends on keeping the method itself secret rather than relying on openly analyzable assumptions and keys. Aliases: obscurity.

Source: 01-CP - Cryptography: From Obscurity to Mathematical Security.

Security-by-design. A design approach that builds security or auditability into a system's architecture rather than adding it only after incidents occur. Aliases: security by design.

Source: 01-FO - Future of Forensics: ForensiBlock & the Design Trade-off.

Seed. The initial input that determines the output sequence of a pseudorandom generator. Aliases: Seed (PRG input), Seed (randomness), initial seed, random seed.

Source: 01-CP - Sources of Randomness.

Seed phrase. A human-readable backup phrase that can regenerate the private keys managed by a wallet. Aliases: Seed phrase (wallet recovery), backup phrase, recovery phrase.

Source: 02-BF - What Are Wallets?.

Seizure. Legally taking control of assets connected to criminal, stolen, or sanctioned activity. Aliases: Seizure (asset recovery), asset seizure, fund recovery.

Source: 01-FO - Colonial Pipeline: Payment Recovery.

Selective disclosure. A privacy approach where people reveal identity or information only when it is necessary or desired. Aliases: Selective Disclosure (privacy compliance), Selective disclosure (ledger privacy), limited disclosure.

Source: 03-IN - Privacy as a Prerequisite for Open Society.

Self-Custody. Holding and controlling one's own assets instead of relying on a custodian such as a bank or exchange. Aliases: Self-custody (Bitcoin), Self-custody (key custody), key management, non-custodial control, non-custodial custody, self custody, self-custodial wallet.

Source: 04-IN - Design Trade-Offs: Efficiency vs. Autonomy.

Self-inverse. A property where applying the same XOR value twice cancels it out and restores the original input. Aliases: Self-inverse (XOR property), XOR reversibility.

Source: 03-CP - Exclusive OR (XOR) Logic.

Self-policing. A design approach where decentralized participants and mechanisms provide moderation, storage, or computation without central enforcement.

Source: 03-DS - Key Considerations in System Design.

Selfish mining. A mining strategy where a coalition withholds found blocks and releases them strategically to earn more than its fair share. Aliases: Selfish mining (Bitcoin), Selfish mining (Proof of Work), block withholding, strategic withholding.

Source: 02-CM - Selfish Mining: Strategic Withholding.

Semantic security. A confidentiality property where repeated encryption should not reveal whether plaintexts are equal.

Source: 03-CP - Padding and Initialization Vectors.

Separation of duties. A design practice that assigns submission, approval, ordering, administration, and audit responsibilities to distinct roles. Aliases: Separation of duties (permissioned ledger), role separation.

Source: 01-PC - Roles and Duties.

Sequencer. An L2 operator role that orders user transactions into batches before posting results or data back to L1. Aliases: L2 sequencer, Sequencer (L2 operator), Sequencer (Layer 2), sequencers.

Source: 01-EF - L2 Operator Models.

Sequencing. The act of placing endorsed transactions into one agreed order for a specific channel. Aliases: Sequencing (Hyperledger Fabric ordering), block sequence, ordering, transaction sequence.

Source: 02-PC - Orderer Cluster and Raft Quorum.

Serial identity strategy. An identity attack pattern where an adversary uses one identity at a time and discards it when its reputation is damaged. Aliases: serial strategy.

Source: 03-DS - Threats: Rebranding Attacks.

Service cluster. A group of addresses inferred to belong to one service, entity, or platform. Aliases: Service cluster (exchange forensics), entity cluster, exchange cluster.

Source: 01-FO - Case Study: BTC-e.

Session key. A temporary symmetric key used to protect data after a secure session has been established. Aliases: session keys.

Source: 03-CP - Why Symmetric Crypto.

Set. A collection of distinct elements used to describe spaces such as all possible keys or all possible messages. Aliases: Set (mathematics), sets.

Source: 01-CP - Mathematics — The Language of Trust.

Setter. A function that updates contract state. Aliases: Setter (Solidity), setter function.

Source: 04-EF - Example: SimpleStorage (Code).

Settlement. The final completion of a payment or transfer obligation through the actual movement of value. Aliases: Settlement (payment).

Source: 02-AS - Global Payment Infrastructure: Overview.

Settlement policy. An operational rule for deciding when a service treats a transaction as settled, based in this lesson on finalized checkpoints. Aliases: Settlement policy (Ethereum operations), finality-based settlement, settlement rule.

Source: 02-EF - Double Spending (Threat Model).

SHA-1. An older Secure Hash Algorithm with 160-bit outputs that is deprecated because practical collisions have been found.

Source: 02-CP - Collision Resistance.

SHA-256. A 256-bit member of the SHA-2 family widely used for integrity checks and Bitcoin hashing.

Source: 02-CP - What Is a Cryptographic Hash Function?.

SHA-3. A modern Secure Hash Algorithm family based on a sponge construction rather than Merkle-Damgard iteration. Aliases: SHA3.

Source: 02-CP - Collision Resistance.

Sharding. A scaling technique that splits workload or data across parallel pieces of a system instead of forcing every node to process everything. Aliases: Sharding (scaling).

Source: 01-EF - Proto-Danksharding (EIP-4844) — Blob Data for L2s.

Share. A partial proof of work meeting an easier pool-set difficulty, used to measure a miner's contributed work. Aliases: Share (mining pool), pool share, valid share.

Source: 02-CM - Pool Payout Model: Pay-Per-Share (PPS).

Shared database. A database shared across organizations but still controlled by one administrator or broad admin access model. Aliases: Shared database (permissioned-ledger contrast), central shared database.

Source: 01-PC - Why Not A Shared Database?.

Shared handoff record. A common record of custody transfers, approvals, and related documents that multiple organizations can rely on. Aliases: shared custody record, shared record.

Source: 01-PC - Scenario.

Shared history. The common record of events or state that honest nodes converge on after transactions are validated and accepted. Aliases: Shared history (blockchain), shared reality, shared truth.

Source: 02-IN - What is a Blockchain?.

Shared key. A secret key known to the communicating parties and used to protect their messages. Aliases: pre-shared secret, shared secret key, unique shared key.

Source: 04-CP - The Key-Distribution Crisis.

Shared randomness. A common random seed that all honest consensus participants can compute and use for validator assignments. Aliases: Shared randomness (Ethereum consensus), deterministic seed, global randomness.

Source: 02-EF - Global Randomness: RANDAO + VDF Beacons.

Shared record. A common record that multiple organizations or participants rely on without assigning one party as the sole owner of truth. Aliases: Shared record (distributed ledgers), shared log, shared notebook.

Source: 04-DS - The Shared Notebook Problem.

Shared secret. A secret value independently derived by both parties from their private exponents and exchanged public values. Aliases: Shared secret (Diffie-Hellman), shared key, shared value.

Source: 04-CP - Diffie–Hellman Key Exchange Concept.

Shared secret key. A secret value known to the communicating parties that enables both encryption and decryption. Aliases: secret key, shared key.

Source: 03-CP - The Shared Key.

Shared state. The common view of system data or action that honest nodes agree to treat as authoritative. Aliases: Shared state (blockchain systems), Shared state (blockchain), shared ledger state, single shared state.

Source: 05-IN - Consensus as the Core Goal.

SHAttered. A practical SHA-1 collision demonstration that showed two different files could share the same SHA-1 digest. Aliases: SHAttered attack.

Source: 05-CP - Hash Fragility: Collision Resistance Isn't Forever.

Shielded Address. A Zcash address type where sender, receiver, and amount can be hidden inside the shielded pool. Aliases: Shielded Address (Zcash), shielded address, shielded addresses, z-addr.

Source: 02-FO - Zcash (ZEC): Optional Privacy.

Shielded Pool. The set of funds and transactions using Zcash shielded functionality, which determines the practical anonymity set. Aliases: Shielded Pool (Zcash), anonymity pool, shielded pool activity.

Source: 02-FO - Zcash (ZEC): Optional Privacy.

Shielded transaction. A transaction that proves validity while hiding details such as sender, receiver, or amount. Aliases: shielded transactions.

Source: 05-CP - Zero-Knowledge in Blockchain Practice.

Shor's algorithm. A quantum algorithm that can solve integer factorization and discrete logarithm problems efficiently on sufficiently capable quantum computers. Aliases: Shor algorithm, Shor's Algorithm (quantum computing), Shor's algorithm (quantum cryptanalysis), Shor's quantum algorithm, Shor's algorithm.

Source: 04-CP - Computational Hardness Assumptions.

Short transaction ID. A compact identifier for a transaction used so peers can reconstruct a block from transactions already in their mempool. Aliases: Short transaction ID (compact block relay), short TX ID.

Source: 03-BF - Block Propagation.

Shortest Vector Problem. A lattice problem asking for the shortest nonzero vector in a lattice. Aliases: SVP.

Source: 05-CP - Lattices: Intuition Without the Math.

Sibling hash. A neighboring hash supplied at each tree level so a verifier can hash upward toward the Merkle root. Aliases: Sibling hash (Merkle proof), sibling hashes.

Source: 02-CP - Merkle Proofs (Membership).

Sidechain. A separate blockchain linked to a main chain for asset or message transfer. Aliases: linked chain.

Source: 01-FO - Case Studey: Ronin Bridge.

Signature chain. A linked sequence of certificate signatures that connects an end-entity certificate to a trusted Root CA. Aliases: Signature chain (PKI), certificate chain, chain of trust.

Source: 04-CP - Certificate Validation Process.

Signature verification. The public-key check that confirms whether a signature matches a message and the claimed signer's public key. Aliases: verification, verify.

Source: 04-CP - Digital Signature Workflow.

Signature verification bypass. A failure where software accepts a signed object without actually enforcing the required signature check. Aliases: auth bypass, authentication bypass, verification bypass.

Source: 04-CP - Real-World Failure: The pac4j-jwt Auth Bypass.

Signed approval. A cryptographically signed authorization from a known member that counts toward policy or consensus requirements. Aliases: Signed approval (permissioned consensus), approved signature, signed approvals.

Source: 01-PC - Consensus.

Signed message. An off-chain message signed by a wallet to prove key control without sending a transaction or paying gas. Aliases: Signed message (wallet authentication), signature challenge, signed challenge.

Source: 06-EF - How Token Gating Works.

Signed voucher. An off-chain authorization signed by a deployer or issuer that a buyer can submit to mint a token. Aliases: Signed voucher (lazy minting), mint voucher, voucher.

Source: 06-EF - Minting on Ethereum.

Signer. The wallet role that produces digital signatures authorizing a transaction to spend controlled outputs. Aliases: Signer (wallet).

Source: 02-BF - What Are Wallets?.

Signing key. The online key a validator uses to sign block proposals, attestations, and other consensus messages. Aliases: Signing key (PoS validator operations), validator signing key.

Source: 03-CM - Becoming a Validator.

Silk Road. A major darknet market that relied on Bitcoin and became an early landmark case for blockchain-supported criminal investigation. Aliases: Dread Pirate Roberts market, Silk Road (case study).

Source: 01-FO - Case Study: Silk Road.

Simple Serialize. A deterministic serialization format used in newer Ethereum contexts to encode structured data. Aliases: SSZ, Simple Serialize (Ethereum encoding).

Source: 03-EF - Transaction Fields and Signatures.

Simplified Payment Verification. A lightweight Bitcoin verification method that checks block headers and Merkle proofs rather than validating the full blockchain. Aliases: SPV.

Source: 03-BF - Setting Up a Light Client.

Single point of failure. A concentrated institution, server, or process whose compromise or shutdown can disrupt the whole system. Aliases: SPOF, central point of failure, chokepoint, single points of failure.

Source: 03-IN - Digital Trust: The Centralized Model.

Single-purpose DAO. A DAO organized around one concrete objective rather than ongoing protocol or community governance. Aliases: single purpose DAO.

Source: 06-EF - Case Study: ConstitutionDAO.

Slander. A coordinated attack that floods an honest peer with false negative ratings to damage its reputation. Aliases: Slander (P2P reputation threat), false negative feedback, smear campaign.

Source: 03-DS - Properties of Reputation Systems.

Slashing (Ethereum). A protocol penalty that removes some staked ETH when a validator provably violates consensus rules. Aliases: Slashing (Ethereum PoS penalty), slash, slashed.

Source: 01-EF - PoW vs PoS: Security Model (Review).

Slashing (Proof of Stake). A protocol penalty that removes validator stake when cryptographic evidence proves misbehavior. Aliases: Slashing (PoS penalty), Slashing (Proof of Stake penalty), slash, slashed, slashing penalty, stake penalty.

Source: 03-CM - Slashing — Making Misbehavior Expensive.

Slashing evidence. Cryptographic proof included in consensus-layer data that a validator committed slashable behavior. Aliases: Slashing evidence (Ethereum), attester slashings, proposer slashings, slashings.

Source: 02-EF - Beacon Blocks and Execution Payloads.

Slot. A specific position in the ordered history where a protocol chooses one value or block. Aliases: Slot (consensus log), height, position, slot (beacon block field), slot field.

Source: 01-CM - Traditional BFT-Style Finality.

Slot (Ethereum). A 12-second Ethereum consensus time window in which at most one block may be proposed and a committee may attest. Aliases: Slot (Ethereum PoS time unit), Slot (Ethereum PoS), slots.

Source: 02-EF - Slots and Epochs.

Slot (Proof of Stake). The basic PoS time unit in which a block proposer may be selected and a committee may attest to the proposed block. Aliases: Slot (PoS time unit), slots.

Source: 03-CM - Proof of Stake: The Full Lifecycle.

Slow confirmation. A delay in block inclusion caused by low fees, crowded mempools, or miner selection preferences. Aliases: Slow confirmation (Bitcoin).

Source: 02-BF - Transaction Challenges.

SLVA. The academic shorthand for the four core consensus properties: safety, liveness, validity, and agreement. Aliases: safety, liveness, validity, agreement.

Source: 01-CM - Foundations of Consensus.

Smart contract. Program logic deployed to a blockchain that can execute rules or update state according to platform conditions. Aliases: Smart contract (application layer), on-chain contract, on-chain program, on-chain programs, smart contracts.

Source: 01-IN - Tools and Setup.

Smart contract auditing. Reviewing smart contract code to identify vulnerabilities, risky patterns, or unintended behavior before or after deployment. Aliases: contract auditing, smart-contract audit.

Source: 05-AS - Opportunities.

Smart contract code reuse. The deployment of many contracts from the same or closely related code patterns. Aliases: Smart contract code reuse (Ethereum security), contract code reuse, template reuse.

Source: 02-EF - Security Risk: Smart Contract Code Reuse.

Smart contract randomness. Randomness used by smart contracts for outcomes such as lotteries, games, or NFT reveals. Aliases: on-chain randomness.

Source: 05-CP - Case Study: Linux.Encoder RNG Failure.

Smart flooding. A more selective flooding strategy where stronger peers forward queries to other hubs instead of every weak participant. Aliases: Smart flooding (P2P search), smart flood.

Source: 01-DS - Gnutella's Fix: Supernodes & "Smart Flooding".

Smart wallet. A wallet design that reduces seed-phrase or key-management burden by adding programmable recovery or account features. Aliases: Smart wallet (wallet usability), smart wallets.

Source: 01-AS - Usability Challenges.

Smart-contract exploit. The use of a flaw in smart contract logic to drain assets, change system behavior, or undermine a decentralized application. Aliases: contract exploit, smart contract exploit.

Source: 05-AS - When Blockchain Systems Broke.

Snap sync. A faster sync mode that downloads state snapshots and verifies them with Merkle proofs. Aliases: Snap sync (Ethereum), snapshot sync.

Source: 03-EF - Sync Modes & Data Availability.

SNARK. A succinct non-interactive proof system often used to prove computation correctness with short proofs. Aliases: zk-SNARK, zkSNARK.

Source: 05-CP - Zero-Knowledge Proofs: Prove Without Revealing.

Social consensus. Agreement among developers, node operators, validators, users, and ecosystem participants about which software and rules to adopt. Aliases: Social consensus (Ethereum governance), rough social consensus.

Source: 01-EF - Governance & Ethereum Improvement Proposals (EIPs).

Social impact. The effect a blockchain system can have on institutions, incentives, users, and communities outside the protocol itself.

Source: 01-IN - Learning Objectives II.

Social layer. The communication, culture, moderation, reputation, and norms that surround a token system but are not enforced by the chain. Aliases: Social layer (token community), off-chain social layer.

Source: 06-EF - Two-Layer Community Architecture.

Social Technology. A human-made coordination system whose usefulness depends on shared expectations and acceptance.

Source: 04-IN - What is Money? A Social Technology.

Social token. A fungible token used to coordinate identity, status, rewards, access, or participation around a community or creator. Aliases: social tokens.

Source: 06-EF - Three Patterns: DAOs, Membership NFTs, and Social Tokens.

Social trust. Trust based on observed honesty and reliability over time rather than on cryptographic identity alone. Aliases: behavioral trust, social (behavioral) trust.

Source: 03-DS - Cryptographic vs. Social Trust.

Socio-technical system. A system whose behavior depends on both technical mechanisms and human incentives, institutions, and coordination. Aliases: socio-technical design.

Source: 01-BF - And Now, Bitcoin.

Soft fork. A rule change that tightens what counts as valid without forcing the same kind of chain split as a hard fork. Aliases: Soft fork (blockchain protocol), soft-fork tightening.

Source: 04-BF - Lessons: Small Community Risks.

Solidity. A smart contract programming language that compiles into EVM bytecode. Aliases: Solidity (Ethereum programming), Solidity (Ethereum).

Source: 01-EF - From EVM to Programs — Smart Contracts.

Solo mining. Mining independently without pooling hash power or sharing rewards with other miners. Aliases: independent mining.

Source: 02-CM - Mining Pools, Variance, and Payouts.

Soulbound Token. A token minted with transfer disabled so it is intended to remain bound to one wallet. Aliases: SBT, SBTs, soulbound token, soulbound tokens.

Source: 06-EF - Soulbound Tokens.

Sound Money. Money that reliably holds value over time, especially because its supply is predictable or difficult to manipulate.

Source: 04-IN - The Bitcoin Standard: A Digital Return to "Hard Money".

Soundness. The property that a cheating prover cannot convince the verifier of a false statement except with negligible probability. Aliases: Soundness (zero-knowledge proofs).

Source: 05-CP - Zero-Knowledge Proofs: Prove Without Revealing.

Source checkpoint. The earlier checkpoint named in a validator vote that links one epoch boundary to another. Aliases: Source checkpoint (PoS finality vote), source epoch.

Source: 03-CM - Justification: Supermajority Vote Links.

Source-code verification. The off-chain process of matching published source code and compiler settings to deployed contract bytecode. Aliases: Source-code verification (Ethereum), contract verification, verified source.

Source: 04-EF - Contract Deployment.

Sovereign Decentralized Settlement. Final transfer of value through a decentralized system without relying on banks or governments as trusted intermediaries. Aliases: decentralized settlement.

Source: 04-IN - The Bitcoin Standard: A Digital Return to "Hard Money".

Sovereign participant. A node that independently chooses and enforces the rules and policies it accepts. Aliases: Sovereign participant (Bitcoin node).

Source: 03-BF - Decisions Nodes Make.

Sparse tree. A Merkle tree design for very large key spaces where most possible leaves are empty. Aliases: Sparse tree (Merkle tree), sparse Merkle tree, sparse trees.

Source: 02-CP - Design Choices & Variants.

Speculation. Market behavior driven mainly by expected price changes rather than present utility or fundamentals. Aliases: Speculation (crypto markets), market speculation, speculative behavior.

Source: 01-AS - Fragmentation and Speculation.

Speculative layer. The visible trading and price-speculation activity around tokens, especially secondary-market NFT collections. Aliases: NFT speculative layer, Speculative layer (token markets).

Source: 06-EF - Hidden Infrastructure Growth.

Spending authority. The practical ability to control bitcoin by possessing the private keys or seed material needed to produce valid signatures. Aliases: Spending authority (Bitcoin), authority to spend.

Source: 02-BF - From Wallet to Block.

Spending policy. Wallet decision logic for choices such as coin selection, fee estimation, change outputs, and address reuse. Aliases: Spending policy (wallet).

Source: 02-BF - What Are Wallets?.

SPFS. Russia's financial messaging system built as an alternative to SWIFT after sanctions pressure. Aliases: SPFS (payment messaging), System for Transfer of Financial Messages.

Source: 02-AS - Global Payment Infrastructure: Overview.

Sponge capacity. The hidden portion of a sponge hash state that provides the construction's security margin. Aliases: capacity, capacity bits.

Source: 02-CP - Sponge Construction: How SHA-3 is Built.

Sponge construction. A hash design that absorbs input into a larger internal state and then squeezes output while keeping part of the state hidden. Aliases: sponge.

Source: 02-CP - Sponge Construction: How SHA-3 is Built.

Sponge rate. The portion of a sponge hash state that receives message blocks and from which output bits are extracted. Aliases: rate, rate bits.

Source: 02-CP - Sponge Construction: How SHA-3 is Built.

Stabilize. A maintenance task where peers check nearby neighbors so successor links stay correct as membership changes. Aliases: Stabilize (Chord maintenance), stabilization, stabilize().

Source: 02-DS - The "Self-Healing" Solutions.

Stablecoin. A token designed to track a reference asset such as the U.S. dollar. Aliases: stablecoins.

Source: 02-FO - Ethereum Forensics: Where the Evidence Hides.

Stablecoin Issuer. An entity that creates and manages stablecoins, usually by promising reserve backing or redemption rules. Aliases: stablecoin issuers.

Source: 03-AS - How Blockchain Changes State Power.

Stack-based scripting language. A programming model where operations consume and produce values on a last-in, first-out stack. Aliases: Stack-based scripting language (Bitcoin Script), stack language.

Source: 03-BF - Introduction to Bitcoin Script.

Stake. Locked value that gives a validator weight in consensus and can be reduced if the validator violates protocol rules. Aliases: Stake (PoS), Stake (Proof of Stake), bonded stake, staked capital, staked collateral.

Source: 03-CM - Orientation: Proof of Work vs Proof of Stake.

Stake deposit. The locked funds a participant provides to enter the validator set and become economically accountable. Aliases: Stake deposit (PoS validator lifecycle), deposit stake, validator deposit.

Source: 03-CM - Proof of Stake: The Full Lifecycle.

Stake-weighted selection. A selection process where validator assignment is random but the chance of selection is proportional to stake. Aliases: Stake-weighted selection (PoS), stake-weighted lottery, stake-weighted randomness.

Source: 03-CM - The Block Proposer: Selection and Building.

Staking rewards. Protocol payments that compensate validators for participating honestly and performing assigned duties. Aliases: Staking rewards (PoS incentives), validator rewards.

Source: 03-CM - Nothing-at-Stake and Economic Security.

Stale block. A valid block that is not included in the ultimately canonical chain after a competing branch wins. Aliases: orphan block, stale/orphan block.

Source: 02-CM - Block Propagation and Stale/Orphan Blocks.

Staleness check. A validation rule that rejects oracle data older than an acceptable time or block threshold. Aliases: Staleness check (oracle defense), freshness check.

Source: 04-EF - Randomness, Oracles, and External Data.

STARK. A transparent, scalable non-interactive proof family used for succinct verification of computation. Aliases: zk-STARK, zkSTARK.

Source: 05-CP - Zero-Knowledge Proofs: Prove Without Revealing.

State. The current agreed condition of the ledger, such as account balances or other recorded facts, after valid updates are applied. Aliases: State (blockchain).

Source: 02-IN - What is a Blockchain?.

State Capacity. A government's practical ability to observe, regulate, enforce, and influence outcomes.

Source: 03-AS - How Blockchain Changes State Power.

State Digital Rail. Official digital payment or settlement infrastructure such as CBDCs and shared central-bank platforms. Aliases: central-bank digital rail, state digital rails.

Source: 03-AS - Competing Financial Infrastructures.

State growth. The accumulation of on-chain state that full nodes must continue storing and verifying over time. Aliases: State growth (Ethereum scaling), state bloat, storage pressure.

Source: 01-EF - State Growth & Storage Pressure.

State machine. A rule-governed system that moves from one agreed state to the next when valid transactions are applied. Aliases: State machine (blockchain), state machines.

Source: 02-IN - What is a Blockchain?.

State overhead. The storage burden created by the trust data a system must keep, such as ratings, scores, histories, or matrices.

Source: 03-DS - Key Considerations in System Design.

State variable. A variable stored in contract storage whose value can persist between calls. Aliases: State variable (Solidity), state variables.

Source: 04-EF - Solidity: File Structure, From Top to Bottom.

State visibility. The degree to which government authorities can observe participants, balances, and transactions in a money system. Aliases: State visibility (digital money).

Source: 02-AS - Types of Digital Money.

State-Observable Payment Architecture. A payment design that gives state authorities practical visibility into activity under government-defined rules. Aliases: state-managed payment architecture, state-observable payments.

Source: 03-AS - China: Overview.

state_root. The header commitment to Ethereum's global state after the block's transactions execute. Aliases: state root, state_root (Ethereum execution payload).

Source: 02-EF - Execution Payload: Header Structure.

Stealth Address. A one-time destination address derived so outside observers cannot publicly link the transaction to the recipient's main address. Aliases: Stealth Address (Monero), Stealth address (Monero privacy), one-time address, stealth addresses.

Source: 02-FO - Monero (XMR): Privacy by Default.

Storage. The persistent on-chain data area where contract state remains across transactions. Aliases: Storage (Solidity data location), contract storage, persistent storage.

Source: 04-EF - Data Locations: Storage, Memory, Calldata.

Storage layout. The ordered arrangement of state variables in storage that upgradeable contracts must preserve across logic versions. Aliases: Storage layout (proxy pattern), storage layout discipline.

Source: 04-EF - Upgradeability and Proxy Patterns.

Store of Value. A function of money that allows purchasing power to be saved for future use.

Source: 04-IN - What is Money? A Social Technology.

Strategic Autonomy. The ability to preserve key capabilities without excessive dependence on outside powers or platforms.

Source: 03-AS - EU: Overview.

Strategic disruption. An attack goal focused on causing instability, fear, or market movement rather than directly stealing coins. Aliases: economic disruption, price dislocation.

Source: 04-BF - Why Attack Bitcoin?.

Strategic Posture. A government's overall stance toward crypto and digital finance based on its interests, risks, and desired control points. Aliases: crypto posture, state posture.

Source: 03-AS - Strategic Approaches to Cryptocurrency.

Stream cipher. A symmetric cipher that generates a keystream and encrypts data bit by bit or byte by byte. Aliases: stream ciphers.

Source: 03-CP - Block vs Stream Ciphers.

Strong cryptography. Cryptographic tools that are difficult for outsiders, including governments or attackers, to break in practice. Aliases: strong encryption.

Source: 03-IN - The Cypherpunk Movement.

Struct. A custom grouped record type that combines multiple fields into one named data structure. Aliases: Struct (Solidity), structs.

Source: 04-EF - Types: Reference Types.

Structured overlay network. A P2P overlay that deliberately organizes peers and data so lookups can move toward a target instead of broadcasting everywhere. Aliases: structured overlay.

Source: 02-DS - Structured Overlay Networks.

Structured round. A named unit of protocol progress that keeps one proposal and its supporting evidence organized together. Aliases: Structured round (consensus), consensus round, round.

Source: 01-CM - Practical Consensus Design.

Structuring. Breaking value into smaller movements to reduce attention, detection, or perceived risk. Aliases: Structuring (financial crime), smurfing, structured movement.

Source: 02-FO - Heuristic #3: Peeling Chains.

Subpoena. A legal demand requiring an organization or person to provide records or testimony relevant to an investigation. Aliases: Subpoena (legal process).

Source: 01-FO - BTC-e: Deanonymization.

Subprime Mortgage. A higher-risk home loan made to a borrower considered less likely to repay. Aliases: subprime mortgage loans.

Source: 04-IN - Case Study: The 2008 Global Financial Crisis.

Substitution box. A nonlinear mapping in a block cipher that replaces input values to create confusion. Aliases: S-box, substitution.

Source: 03-CP - Building Blocks of Block Ciphers.

Success probability. The chance that an adversary succeeds at a specified attack or guessing task. Aliases: adversary success probability.

Source: 01-CP - Probability Refresher: Events and Outcomes.

Successor. The first peer at or after a key's identifier on the Chord ring, responsible for storing or answering for that key. Aliases: Successor (Chord), successor node.

Source: 02-DS - DHT Example: Chord.

Supernode. A high-capacity peer that acts as a hub for weaker peers by handling more indexing, routing, or relay work. Aliases: Supernode (P2P network), supernodes, ultrapeer, ultrapeers.

Source: 01-DS - Gnutella's Fix: Supernodes & "Smart Flooding".

Supernode hierarchy. A P2P design where more capable peers form a higher-capacity backbone that helps weaker peers route or search. Aliases: supernode model, supernodes.

Source: 02-DS - Scalability Challenges{.smaller}.

Superposition. The quantum behavior where a system can represent overlapping possible states until measurement. Aliases: Superposition (quantum computing).

Source: 05-CP - Quantum Primer: Why It Matters for Cryptography.

Supply cap. Bitcoin's protocol-designed limit on total issuance, commonly described as 21 million BTC. Aliases: 21 million BTC limit, 21 million bitcoin limit, Supply cap (Bitcoin monetary policy).

Source: 04-AS - Bitcoin Monetary Policy and Difficulty.

Supply chain traceability. The use of shared records to follow product origin, handling, location, or certification across organizations. Aliases: Supply chain traceability (blockchain use case), food traceability, traceability.

Source: 01-AS - Supply Chain Case.

Surround vote. A slashable voting pattern where one checkpoint vote improperly surrounds or wraps around a prior vote. Aliases: Surround vote (Ethereum slashing), Surround vote (PoS offense), protocol-violating vote pattern, surround votes, surround voting.

Source: 03-CM - Slashing — Making Misbehavior Expensive.

Suspicious Activity Report. A formal report filed by a regulated institution when activity appears abnormal or potentially linked to crime. Aliases: SAR, SARs, Suspicious Activity Report (crypto compliance), required reporting.

Source: 01-FO - Policy & Regulatory Response.

SWIFT. A global bank-to-bank financial messaging network that carries payment instructions but does not settle funds itself. Aliases: SWIFT (payment messaging), Society for Worldwide Interbank Financial Telecommunication.

Source: 02-AS - Global Payment Infrastructure: Overview.

Sybil attack. An attack where one adversary creates many fake peer identities to distort peer selection, routing, or consensus influence. Aliases: Sybil attack (Bitcoin network), Sybil attack (P2P threat), Sybil attacks, Sybil flood, Sybil pressure, Sybils, fake identities, fake peer attack.

Source: 02-DS - The Great P2P Weakness: Sybil & Eclipse Attacks.

Sybil resistance. Mechanisms that make it expensive for one actor to create many identities and overwhelm an open network. Aliases: Sybil defense, Sybil resistance (permissioned ledger), Sybil resistance through economics, anti-Sybil control, anti-Sybil mechanism, sybil resistance.

Source: 04-DS - Permissionless Ledgers.

Sybil risk. The risk that one actor can join or impersonate many participants to gain outsized influence. Aliases: Sybil attack, Sybil-style risk.

Source: 05-IN - Why Decentralization Is Harder.

Sybil-resistant leader election. A method for choosing who may propose a block that limits fake identities by requiring an expensive scarce resource. Aliases: Sybil resistant leader election.

Source: 02-CM - Proof of Work: Purpose and Agenda.

Symmetric cryptography. A cryptographic approach where the same shared secret key is used to encrypt and decrypt data. Aliases: symmetric crypto, symmetric encryption.

Source: 03-CP - The Shared Key.

Synchronized state. The condition where honest nodes update their local ledgers to reflect the same accepted result. Aliases: Synchronized state (blockchain), same synchronized state, shared state.

Source: 02-IN - The Result: A Shared Truth.

Synchronous system. A system whose message and processing delays are bounded and known in advance. Aliases: synchronous network, synchrony.

Source: 01-CM - Timing Models on a Spectrum.

Systemic trust shock. A broad loss of confidence caused by failures that cascade through an entire financial or institutional system.

Source: 03-IN - A Crisis of Trust: 2008.

T

Tamper evidence. The property that changing any committed item changes hashes along its path and therefore changes the Merkle root. Aliases: Tamper evidence (Merkle tree), tamper detection, tamper-evident.

Source: 02-CP - Merkle Trees: Motivation.

Tamper-evident. A property where unauthorized changes become detectable rather than silently hidden. Aliases: tamper evidence.

Source: 02-IN - Pillar 1: Cryptography.

Tamper-evident ledger. A record whose structure makes unauthorized changes detectable by participants who verify the cryptographic links and rules. Aliases: decentralized ledger, tamper evidence, tamper-evident history.

Source: 01-CP - How Blockchain Uses Cryptography.

Target checkpoint. The later checkpoint named in a validator vote that a source checkpoint is being linked to. Aliases: Target checkpoint (PoS finality vote), target epoch.

Source: 03-CM - Justification: Supermajority Vote Links.

Target rule. The validity rule that a candidate block's hash must be numerically below the current target threshold. Aliases: Target rule (proof of work), hash $<$ target, hash-below-target rule.

Source: 02-CM - Visualizing the Target Rule.

Technical architecture. The structural design of blockchain components, including how data, networks, cryptography, and agreement mechanisms fit together. Aliases: Technical architecture (blockchain).

Source: 01-IN - Course Overview.

Temporary fork. A short-lived split where different valid blocks at the same height are seen by different parts of the network. Aliases: Temporary fork (proof of work), competing branch, short-lived fork.

Source: 02-CM - Block Propagation and Stale/Orphan Blocks.

The Bitcoin Standard. Saifedean Ammous's framing of Bitcoin as a modern digital successor to gold and hard-money economics. Aliases: Bitcoin Standard, The Bitcoin Standard (book and thesis).

Source: 04-IN - The Bitcoin Standard: A Digital Return to "Hard Money".

The DAO hack. A 2016 Ethereum exploit that abused an external-call-before-state-update bug to drain funds from The DAO. Aliases: DAO attack, The DAO exploit, The DAO hack (Ethereum history).

Source: 04-EF - Case Study: The DAO Hack (2016).

The Merge. The September 15, 2022 Ethereum upgrade that moved block production from Proof of Work to Proof of Stake while preserving existing state. Aliases: Beacon Chain merge, Merge, The Merge (Ethereum upgrade), The Merge (Ethereum).

Source: 01-EF - The Merge (Sept 15, 2022).

Thin history. A small amount of interaction evidence that is not yet enough to support high confidence in a peer's reputation. Aliases: low feedback scope.

Source: 03-DS - PeerTrust: Handling Manipulation.

Threat model. The set of failures, attackers, and assumptions a system is designed to withstand. Aliases: threat models.

Source: 05-IN - Fault Tolerance Spectrum.

Threat modeling. A structured way to identify what can go wrong in a system, who might attack it, and which weaknesses matter most.

Source: 03-IN - Why This History Matters.

Throughput. The rate at which a ledger or database can process accepted writes or transactions. Aliases: Throughput (ledger performance), transaction throughput, write throughput.

Source: 04-DS - Permissioned Ledgers.

Time lock. A spending condition that prevents an output from being spent until a specified block height, time, or sequence condition is met. Aliases: Time lock (Bitcoin Script), time-locked output, timelock.

Source: 03-BF - Why Bitcoin Script Exists.

Time-seeded PRNG. A pseudorandom generator seeded from the current time, making outputs guessable within a narrow time window. Aliases: clock-seeded PRNG, srand(time()).

Source: 05-CP - Case Study: Linux.Encoder RNG Failure.

Time-to-Live. A counter or limit that prevents a forwarded message from spreading forever through a network. Aliases: TTL, Time-to-Live (network messages).

Source: 01-DS - Case Study: Gnutella & "Flooding".

Time-warp attack. A coordinated timestamp manipulation attack that tricks the difficulty control loop into lowering difficulty or mismeasuring time. Aliases: time warp.

Source: 02-CM - Timestamp Manipulation and Time-Warp Attacks.

Timelock. A delay mechanism that forces an upgrade or administrative action to wait before it can take effect. Aliases: Timelock (upgrade governance), time lock.

Source: 04-EF - Upgradeability and Proxy Patterns.

Timeout. A waiting limit that lets nodes turn prolonged silence or delay into a protocol recovery event. Aliases: Timeout (consensus), timeouts.

Source: 01-CM - Consensus in the Real World.

Timestamp manipulation. Miner behavior that sets block timestamps within allowed limits to influence how the protocol measures elapsed time. Aliases: timestamp games.

Source: 02-CM - Timestamp Manipulation and Time-Warp Attacks.

Timestamping. A technique for recording data so others can later verify that the data existed at a particular time.

Source: 01-IN - Why A Blockchain Course?.

Timing Analysis. Correlating deposits and withdrawals by comparing when they occur, especially in low-volume pools. Aliases: Timing Analysis (mixer investigations), time correlation, timing correlation.

Source: 02-FO - Breaking Mixers: Investigative Countermeasures.

Timing attack. An attack that exploits when transactions or blocks are first observed to infer origin, gain advantage, or affect confidence. Aliases: Timing attack (Bitcoin network), latency attack, timing and latency attack.

Source: 04-BF - Timing & Latency Attacks.

Timing correlation. An analytic method that compares transaction timing across flows, services, or chains to infer likely relationships. Aliases: Timing correlation (forensics), timing analysis.

Source: 04-AS - Obfuscation and Countermeasures.

Timing fault. A failure where a node returns correct information too late or outside the required ordering window. Aliases: timing faults.

Source: 05-IN - Timing Faults.

Timing model. The assumptions a protocol makes about message and processing delays. Aliases: timing assumption.

Source: 01-CM - Timing Models on a Spectrum.

Timing window. A bounded time interval used to match likely related deposits and withdrawals across chains or services. Aliases: Timing window (cross-chain tracing), timing windows.

Source: 01-FO - Future of Forensics: Automated Cross-Chain Tracing.

Tip. The optional part of an Ethereum transaction fee paid to the block proposer to encourage inclusion. Aliases: Tip (EIP-1559), priority fee, proposer tip.

Source: 01-EF - Gas: Metering Computation and Storage.

Token. A blockchain-based representation of value, rights, or other state managed by platform rules or smart contracts. Aliases: Token (blockchain), tokens.

Source: 01-IN - Learning Objectives I.

Token gate. An access rule that grants or denies entry based on whether a wallet holds a specified token or balance. Aliases: token gating, token-gated access.

Source: 06-EF - Token-Based Communities.

Token ID. The unique number or identifier that distinguishes one NFT or asset instance from others in the same contract. Aliases: Token ID (NFT), identifier, token identifier, unique identifier, unique identifiers.

Source: 05-EF - Fungible vs Non-Fungible — Design Implications.

Token incentive. A reward or ownership structure created through tokens that shapes how participants behave in a blockchain system. Aliases: economic incentive, token incentives.

Source: 05-AS - Human & Economic Constraints.

Token standard. A shared contract interface that wallets, markets, indexers, and applications rely on to interpret and interact with tokens. Aliases: ERC standard, ERC standards, Token standard (Ethereum), standards, token standards.

Source: 06-EF - Fungible vs. Non-Fungible.

Token-based community. A community that uses token ownership to control membership, access, participation, or governance. Aliases: token community, token-based communities.

Source: 06-EF - Token-Based Communities.

Token-weighted governance. A governance model where voting power is based on the amount or number of governance tokens a participant controls. Aliases: token-weighted voting.

Source: 06-EF - Two-Layer Community Architecture.

Tokenization. The process of representing a digital or real-world claim as an on-chain token with programmable ownership and transfer behavior. Aliases: Tokenization (application layer), tokenize, tokenized assets.

Source: 05-EF - Digital Assets, Tokenization, and NFTs.

Tokenized asset. A real-world or digital claim represented as an on-chain token. Aliases: tokenized assets, tokenized claim.

Source: 01-AS - Finance (High-Level Overview).

Tokenized Financial Infrastructure. Financial infrastructure that represents claims, assets, or settlement processes as digital tokens. Aliases: tokenized finance, tokenized-finance pathway.

Source: 03-AS - Latin America: Impact Signals.

tokenURI. A common NFT contract interface that returns the location or content-addressed reference for a token's metadata. Aliases: metadata pointer, token URI, tokenURI (NFT metadata), tokenURI function.

Source: 05-EF - System Architecture — Where Everything Lives.

Top-Level Transaction. The outer Ethereum transaction record showing fields such as sender, recipient, ETH value, gas use, and status. Aliases: Top-Level Transaction (Ethereum), main transaction record, top-level tx.

Source: 02-FO - Ethereum Forensics: Where the Evidence Hides.

Topic. A 32-byte indexed field in an Ethereum log used by clients to filter events efficiently. Aliases: Topic (Ethereum log), indexed topic, log topic.

Source: 04-EF - Events and Logs.

Tor network. A privacy-focused network that routes traffic to obscure users' network locations and enable hidden services. Aliases: Tor.

Source: 01-FO - Case Study: Silk Road.

Tornado Cash. An Ethereum privacy protocol whose 2022 sanctions became a major case study in relay and builder censorship pressure. Aliases: Tornado Cash (Ethereum policy case), Tornado Cash (mixer).

Source: 02-EF - Censorship.

Traceability. The degree to which a movement of funds can be reconstructed and defended from available on-chain and off-chain evidence. Aliases: Traceability (blockchain forensics), traceability level, traceable.

Source: 02-FO - Not All Hops Are Equally Opaque.

Traceable execution. The ability to follow and verify actions recorded by blockchain transactions and smart contracts. Aliases: Traceable execution (blockchain systems), verifiable execution.

Source: 05-AS - Two Powerful Technologies Collide.

Transaction. A proposed change to blockchain state, such as transferring value or invoking a contract, that must be validated by the network. Aliases: Transaction (blockchain), script operations, transactions.

Source: 01-IN - Learning Objectives I.

Transaction (Bitcoin). A signed message proposing that bitcoin value move from current control to a new owner or destination. Aliases: Bitcoin transaction, payment, transaction, transactions, tx.

Source: 01-BF - Primitive 1: Ownership via Digital Signatures.

transaction (Ethereum). A signed message from an account that requests a state change on Ethereum. Aliases: Ethereum transaction (Ethereum), transaction.

Source: 03-EF - Review: The Life of an Ethereum Transaction.

Transaction bundle. A group of ordered transactions submitted together to a builder with an associated bid or value estimate. Aliases: Transaction bundle (MEV), bundle, bundles.

Source: 03-EF - Builder / Relay Stack and MEV.

Transaction censorship. The deliberate delay or exclusion of selected transactions from relay or confirmation. Aliases: Transaction censorship (Bitcoin), censorship, selective censorship.

Source: 04-BF - Why Attack Bitcoin?.

Transaction fee. A cost paid to have a blockchain transaction included or processed by the network. Aliases: Transaction fee (Bitcoin), Transaction fee (mining incentives), fees, miner fees, transaction fees.

Source: 03-IN - Promises vs. Reality.

Transaction graph. The network of relationships among transactions, inputs, outputs, and addresses visible from blockchain data. Aliases: Transaction graph (Bitcoin), Transaction graph (forensics), graph structure, on-chain graph, payment graph, transaction graph structure.

Source: 04-BF - Mitigating Network Deanonymization.

Transaction input. A reference to a previous UTXO plus the unlocking data needed to spend it in a new transaction. Aliases: Transaction input (Bitcoin), input.

Source: 02-BF - Transactions and the UTXO Model.

Transaction lifecycle. The end-to-end path from a user's signed intent through broadcast, waiting, block inclusion, consensus, and final chain update. Aliases: Transaction lifecycle (blockchain), end-to-end transaction, lifecycle of a transaction, transaction flow.

Source: 02-IN - Putting it Together: The Lifecycle of a Transaction.

Transaction ordering. The proposer's ability to decide which pending transactions appear in a block and in what order. Aliases: Transaction ordering (Bitcoin), Transaction ordering (block proposal), global transaction ordering, order of transactions, ordering power, transaction inclusion.

Source: 03-CM - The Block Proposer: Selection and Building.

Transaction output. A newly created spendable value record that locks bitcoin to a recipient, change address, or other script condition. Aliases: Transaction output (Bitcoin), output.

Source: 02-BF - Transactions and the UTXO Model.

Transaction path. The sequence from identity check through proposal, approval, ordering, validation, and commit. Aliases: Transaction path (permissioned ledger), generic path, transaction pipeline.

Source: 01-PC - Transaction Path.

Transaction pipeline. The end-to-end path from a user action through wallet signing, RPC broadcast, node validation, propagation, and on-chain recording. Aliases: Transaction pipeline (blockchain), transaction flow, transaction path.

Source: 01-AS - Walking a Transaction Step-by-Step.

Transaction policy. Rules that determine which organizations or roles must approve a transaction before it can be committed. Aliases: approval policy, endorsement policy.

Source: 01-PC - Key Components.

Transaction propagation. The spreading of a valid transaction across network peers after it is submitted to a node. Aliases: Transaction propagation (blockchain network), propagation, transaction relay.

Source: 01-AS - Walking a Transaction Step-by-Step.

Transaction receipt. The record produced after Ethereum transaction execution that reports status, gas used, and emitted logs. Aliases: Transaction receipt (Ethereum), receipt.

Source: 03-EF - Review: The Life of an Ethereum Transaction.

Transaction relay. The peer-to-peer process where signed transactions move from wallets to nodes and then across the network. Aliases: Transaction relay (Bitcoin network), Transaction relay (Bitcoin), broadcast, gossip, transaction propagation.

Source: 02-BF - Where Does a Transaction Go?.

Transaction selection. The miner's choice of which valid transactions to include when assembling a block. Aliases: Transaction selection (mining), block assembly policy, miner discretion.

Source: 02-CM - Censorship and Transaction Selection.

Transaction signing. Using a private key to create cryptographic authorization for a blockchain action. Aliases: signed transaction, signing, wallet signature.

Source: 01-AS - Wallets: The Control Layer.

Transaction Trace. Detailed execution data showing the internal calls and contract behavior that occurred during an Ethereum transaction. Aliases: Transaction Trace (Ethereum), debug_traceTransaction, trace-level data.

Source: 02-FO - Smart Contract Forensics.

Transaction validation. The software process nodes use to check whether a transaction follows Bitcoin's rules before accepting it. Aliases: Transaction validation (Bitcoin), Transaction validation (blockchain), transaction checks, validate transactions, validation, validation logic.

Source: 04-BF - Bitcoin Overflow Bug.

transactions_root. The header commitment to the exact ordered list of transactions included in an execution payload. Aliases: transaction root, transactions root, transactions_root (Ethereum execution payload).

Source: 02-EF - Execution Payload: Header Structure.

Transfer history. The immutable record of prior token transfers and owners visible from on-chain state and events. Aliases: Transfer history (token), ownership history.

Source: 06-EF - What Is a Token?.

Transitive trust. Trust extended through another trusted relationship rather than verified directly.

Source: 05-IN - Trust.

Transparency. The ability for participants or permitted members to verify state changes and rule compliance. Aliases: Transparency (distributed ledgers), verifiability.

Source: 04-DS - Transparency vs. Privacy.

Transparency log. A public append-only record that uses Merkle roots and proofs to support auditing of inclusion and history. Aliases: append-only log, transparency logs.

Source: 02-CP - Where You'll See Them (Non-Exhaustive).

Transparent Address. A Zcash address type whose transactions are publicly visible and traceable like Bitcoin transactions. Aliases: Transparent Address (Zcash), t-addr, transparent address, transparent addresses.

Source: 02-FO - Zcash (ZEC): Optional Privacy.

Transparent Ledger. A ledger where transaction relationships are publicly visible and can be analyzed as a graph. Aliases: Transparent Ledger (blockchain forensics), public transaction graph, transparent blockchain.

Source: 02-FO - The Shift in Strategy: Privacy-Preserving Blockchains.

Transport cost. The monetary and resource cost of moving, relaying, storing, or processing data across a network. Aliases: Transport cost (distributed systems), egress cost, relay cost.

Source: 01-DS - Fallacy #7: Transport Cost Is Zero.

Trapdoor function. A function that is easy to compute in one direction but infeasible to reverse unless the secret trapdoor information is known. Aliases: trapdoor one-way function.

Source: 04-CP - Trapdoor Functions.

Treasury disbursement. The release of community or protocol funds according to contract rules, votes, or other governance processes. Aliases: Treasury disbursement (DAO), treasury release, treasury spending.

Source: 06-EF - Two-Layer Community Architecture.

Tron. A public blockchain network that carries a large share of USDT transfers, especially where low fees matter. Aliases: TRON, Tron (stablecoin network).

Source: 02-AS - Case Study: USDT on Tron.

Trust. A system dependency on an entity behaving correctly under stated conditions. Aliases: Trust (P2P reputation), Trust (security engineering).

Source: 05-IN - Trust.

Trust anchor. A trusted starting point used to validate a chain of trust decisions. Aliases: trust-anchor model.

Source: 05-IN - Trust.

Trust architecture. The design of who must trust whom, how authority is assigned, and who can authorize, revoke, or validate activity. Aliases: trust model.

Source: 02-AS - Trust Architecture: CBDCs vs Permissionless Systems.

Trust assumption. A condition about which actors, code, infrastructure, or cryptography must behave correctly for a system to remain safe. Aliases: Trust assumption (blockchain design), trust assumptions.

Source: 05-AS - Technical Constraints.

Trust boundary. The line around the people, institutions, or mechanisms that the system assumes are trustworthy enough. Aliases: Trust boundary (ledger design), boundary of trust.

Source: 04-DS - Trade-offs.

Trust but verify. A workflow that uses reputation to choose peers, cryptographic checks to verify results, and verified outcomes to update reputation. Aliases: complete trust loop, trust but verify pattern.

Source: 03-DS - Properties of Reputation Systems.

Trust matrix. A structured table of normalized trust values showing how much each peer trusts other peers. Aliases: C matrix.

Source: 03-DS - EigenTrust: From Local Opinions to Global Scores.

Trust mechanism. A system feature that turns uncertain peer behavior into signals, scores, or rules that help participants choose safer partners. Aliases: trust mechanisms.

Source: 03-DS - Intro: "The Bad Download".

Trust minimization. A design goal that reduces how much users must rely on a trusted institution or leader for the system to work. Aliases: Trust minimization (blockchain), minimized trust, trust-minimized, trust-minimized alternative.

Source: 03-IN - A Crisis of Trust: 2008.

Trust model. The explicit answer to who or what participants must trust for the system's record to remain correct. Aliases: Trust model (system design), trust assumption, trust assumptions.

Source: 04-DS - Distributed Ledger vs. Centralized Database (Compare/Contrast).

Trust relocation. The idea that blockchain changes where trust is placed, moving it into code, operators, infrastructure, incentives, and institutions. Aliases: Trust relocation (blockchain systems), relocated trust, trust shifts.

Source: 05-AS - Key Lessons.

Trust-Minimized Protocol. A protocol designed to reduce the need to rely on a central institution or intermediary behaving correctly. Aliases: trust-minimized protocols.

Source: 04-IN - Design Trade-Offs: Efficiency vs. Autonomy.

Trusted bootstrap paradox. The tension that a decentralized node still needs some initial peer-discovery source that may be centralized or compromisable. Aliases: bootstrap dependency.

Source: 02-CM - Eclipse and Network-Level Attacks.

Trusted checkpoint. A recent finalized block reference obtained from trusted or diverse sources before syncing a PoS node. Aliases: Trusted checkpoint (PoS bootstrapping), checkpoint hash, recent trusted checkpoint.

Source: 03-CM - Weak Subjectivity.

Trusted Intermediary. An institution or actor that users rely on to process, validate, or settle transactions correctly. Aliases: financial intermediary, trusted arbiter, trusted intermediaries, trusted third party.

Source: 04-IN - The Bitcoin Standard: A Digital Return to "Hard Money".

Trusted third party. An external actor that others rely on to vouch for identity, attributes, or correct behavior. Aliases: TTP, certificate authority, certification authority, third party.

Source: 05-IN - Trust.

Trustless. A misleading shorthand for systems that reduce reliance on specific institutions while still depending on explicit assumptions and mechanisms. Aliases: Trustless (blockchain claim), trustless system.

Source: 05-IN - What is "trust" in digital systems?.

Trustless coordination. Coordination among parties who do not need personal trust because cryptographic checks and protocol rules make agreement verifiable.

Source: 01-CP - Why Cryptography Matters Today.

Trustless model. A system model where participants rely on verifiable rules and mathematical proof instead of a central authority or personal trust. Aliases: trustless system, trustless systems.

Source: 01-CP - Cryptography and Trustless Systems.

Trustlessness. The claim that a system reduces the need to trust specific people or institutions by relying on code, cryptography, and consensus. Aliases: Trustlessness (blockchain claims), trustless system, trustlessness claim.

Source: 05-AS - Key Lessons.

Turing complete. A language property that supports general computation with control flow such as loops, branching, and function calls. Aliases: Turing complete (smart contract language), Turing completeness.

Source: 04-EF - From Bitcoin Script to Solidity.

Two-party trust. A direct trust relationship where one party expects another party to behave as promised. Aliases: bilateral trust.

Source: 05-IN - Trust.

Two-Phase Commit. A coordination protocol where a central coordinator first asks participants if they are ready and then issues a final commit only if all agree. Aliases: 2PC, two-phase commit.

Source: 05-IN - Classical Consensus Approaches.

U

Unauthenticated messages. Messages that do not cryptographically prove who sent them or that they were not forged. Aliases: oral messages.

Source: 05-IN - The Byzantine Generals Problem (formal).

Unbonding period. A delay after validator exit during which stake remains locked before withdrawal is allowed. Aliases: Unbonding period (PoS validator lifecycle), cooldown, unbonding.

Source: 03-CM - Proof of Stake: The Full Lifecycle.

Unconfirmed transaction. A transaction the network has received but that has not yet become part of accepted blockchain history. Aliases: pending transaction, unconfirmed.

Source: 02-IN - Step 3: The Mempool.

Unforgeable. A property where attackers cannot practically create valid proofs or authorizations without the required cryptographic secret.

Source: 02-IN - Pillar 1: Cryptography.

Unified provenance graph. A graph that links related asset movements across chains into one traceable history. Aliases: Unified provenance graph (blockchain forensics), provenance graph.

Source: 01-FO - Future of Forensics: Automated Cross-Chain Tracing.

Uniform distribution. The expectation that hash outputs are spread evenly across the output space without useful patterns or biases. Aliases: Uniform distribution (hashing), uniform distribution of output, uniform output.

Source: 02-CP - Hash Function Properties.

Unit of Account. A function of money that provides a common yardstick for pricing and comparing value.

Source: 04-IN - What is Money? A Social Technology.

Unlicensed money transmitter. A money services operator that transfers value without the authorization required by law.

Source: 03-IN - Early Attempts at Digital Money.

Unlocking data. Data such as a signature and public key that satisfies an output's locking script so the referenced UTXO can be spent. Aliases: Unlocking data (Bitcoin), scriptSig, witness.

Source: 02-BF - Transactions and the UTXO Model.

Unlocking script. The script or data supplied by a spender to satisfy a previous output's locking script. Aliases: Unlocking script (Bitcoin Script), scriptSig.

Source: 03-BF - Bitcoin Script Basics.

Unpredictability. A property where seeing part of a sequence does not make the next value feasibly guessable. Aliases: Unpredictability (PRG property), predictability.

Source: 01-CP - Probability Refresher: Independence & Random Variables.

Unsigned integer. A nonnegative integer type commonly used for balances, counters, timestamps, and range checks. Aliases: Unsigned integer (Solidity), uint, uint256, unsigned int.

Source: 04-EF - Types: Value Types.

Unspent transaction output. A transaction output that has not yet been spent and can be consumed only by satisfying its attached spending conditions. Aliases: UTXO, UTXOs, Unspent transaction output (Bitcoin), unspent output.

Source: 03-BF - Introduction to Bitcoin Script.

Unstructured overlay network. A P2P overlay where peers form mostly random neighbor connections rather than maintaining a precise searchable structure. Aliases: random mesh, unstructured overlay.

Source: 02-DS - Unstructured Overlay Networks.

Usability. How safely and easily ordinary users can understand, operate, and recover from interactions with blockchain systems. Aliases: UX, Usability (blockchain systems), user experience.

Source: 05-AS - The Real Question.

USDC. A dollar-referenced stablecoin issued by Circle with a US-regulated, sanctions-compliant posture. Aliases: Circle USDC, USD Coin, USDC (stablecoin).

Source: 02-AS - Types of Digital Money.

USDT. A dollar-referenced stablecoin issued by Tether that dominates many high-volume and emerging-market payment flows. Aliases: Tether, USDT (stablecoin).

Source: 02-AS - Types of Digital Money.

User / Operator. A person or service acting on behalf of an organization inside the permissioned network. Aliases: User / Operator (permissioned ledger identity), operator, service operator, user.

Source: 01-PC - Identity.

User experience. How people actually encounter, understand, and navigate blockchain systems through products and interfaces. Aliases: UX, User experience (blockchain applications).

Source: 01-AS - From Theory to Reality.

Utility layer. Operational token uses such as product passports, supply-chain records, loyalty systems, credentials, and asset records. Aliases: Utility layer (token infrastructure), operational utility layer.

Source: 06-EF - Hidden Infrastructure Growth.

Utility NFT. An NFT whose value is tied to access, participation, functionality, identity, or benefits rather than only collectibility. Aliases: utility NFTs.

Source: 05-EF - From Experiments to NFTs — A Combined Timeline.

Utility-Driven Crypto Adoption. Crypto adoption motivated by practical needs such as remittances, dollar access, inflation pressure, or unreliable payment infrastructure. Aliases: high-utility adoption, necessity-driven use.

Source: 03-AS - Sub-Saharan Africa: Overview.

UTXO. A discrete unspent output from an earlier transaction that can be used as an input to a later transaction. Aliases: UTXO (Bitcoin), Unspent Transaction Output, spendable output, unspent output.

Source: 02-BF - What Are Wallets?.

UTXO model (Bitcoin). An accounting model where value is tracked as discrete unspent outputs that transactions consume and create. Aliases: Bitcoin UTXO Model, UTXO, UTXO model (Bitcoin accounting), UTXO model (Bitcoin transaction model), unspent transaction output, unspent transaction output model.

Source: 01-EF - Transaction Models: UTXO vs Accounts.

UTXO set. The current collection of unspent transaction outputs that nodes use to determine whether transaction inputs are spendable. Aliases: UTXO set (Bitcoin).

Source: 02-BF - UTXO Visualized.

V

Validation. The peer-side process that rechecks endorsement policy, MVCC constraints, and transaction well-formedness after ordering. Aliases: Validation (Hyperledger Fabric), commit-time validation, transaction validation.

Source: 02-PC - One Invoke: Proposal to Commit.

Validation against policy. The check that an ordered request still satisfies the relevant policy and state rules before commit. Aliases: Validation against policy (transaction path), policy validation.

Source: 01-PC - Transaction Path.

Validation Event. Outside evidence that confirms what an on-chain heuristic previously suggested. Aliases: Validation Event (blockchain forensics), corroborating event, external validation.

Source: 02-FO - Breaking the Obfuscation: Account Clustering.

Validator. A participant that helps validate, propose, or confirm blocks under a consensus system such as Proof of Stake. Aliases: Validator (block production), Validator (blockchain role), block producer, miner, miners, validators.

Source: 02-IN - Pillar 3: Consensus.

Validator (Ethereum). A Proof-of-Stake participant that helps propose, check, attest to, and finalize blocks using staked ETH. Aliases: Validator (Ethereum PoS role), Validator (Ethereum PoS), validators.

Source: 01-EF - The Merge (Sept 15, 2022).

Validator (Proof of Stake). A participant that has staked capital and performs PoS duties such as proposing blocks, attesting, and voting on checkpoints. Aliases: Validator (PoS role), Validator (Proof of Stake role), validators.

Source: 03-CM - Orientation: Proof of Work vs Proof of Stake.

Validator / endorser. A participant role that approves transactions according to the network's policy. Aliases: Validator / endorser (permissioned ledger role), approver, endorser, validator.

Source: 01-PC - Roles and Duties.

Validator process. Software that signs the validator duties assigned by the consensus client. Aliases: Validator process (Ethereum client), validator client.

Source: 02-EF - PoS Overview: Validators, Committees, and Clients.

Validator selection. The consensus-layer process that assigns validators to proposer and committee duties for slots and epochs. Aliases: Validator selection (Ethereum PoS), duty assignment, validator assignment.

Source: 02-EF - Validator Selection & Randomness.

Validator set. The group of nodes authorized to approve bridge actions such as withdrawals. Aliases: Validator set (bridge security), validator nodes.

Source: 01-FO - Ronin: Key Management.

Validity. The guarantee that only proposed values satisfying the protocol rules can be committed. Aliases: Validity (consensus property), Validity (consensus), integrity.

Source: 01-CM - Foundations of Consensus.

Validity proof. A cryptographic proof that a state transition was computed correctly according to the rollup's rules. Aliases: Validity proof (Layer 2 verification), Validity proof (ZK rollup), ZK proof, cryptographic validity proof, validity proofs, zero-knowledge proof.

Source: 01-EF - Rollups — Optimistic vs ZK{.smaller}.

Value Stability. The ability of a monetary asset to maintain relatively stable purchasing power or price over time.

Source: 04-IN - The Institutional Counterpoint: The BIS Critique.

Value type. A Solidity type category whose values are copied when assigned or passed to functions. Aliases: Value type (Solidity), value types.

Source: 04-EF - Types: Value Types.

VARA. Dubai's dedicated authority for licensing and supervising virtual-asset activity under a state-defined rulebook. Aliases: Dubai Virtual Assets Regulatory Authority, Virtual Assets Regulatory Authority.

Source: 03-AS - Gulf States: Impact Signals.

Variance. The unpredictability of mining income caused by the lottery-like timing of finding valid blocks. Aliases: Variance (mining payouts), payout variance, reward variance.

Source: 02-CM - Mining Pools, Variance, and Payouts.

Verifiability. The ability for anyone running appropriate software to check Bitcoin's rules and history for themselves. Aliases: Verifiability (Bitcoin), independent verification.

Source: 01-BF - Benefits of Bitcoin's Design.

Verifiable credential. A digitally checkable claim, such as a diploma or identity attribute, whose authenticity can be verified across organizations. Aliases: VC, VCs, Verifiable credential (digital identity), Verifiable credential (public-sector ledgers), verifiable credentials.

Source: 04-DS - Case Study B — Public Sector: EBSI & Estonia (KSI){.smaller}.

Verifiable Delay Function. A proposed time-locked computation that is slow to produce but easy to verify, reducing the ability to compute randomness outcomes early. Aliases: VDF, VDF beacon, Verifiable Delay Function (Ethereum randomness proposal).

Source: 02-EF - Global Randomness: RANDAO + VDF Beacons.

Verifiable Random Function. A cryptographic method that produces randomness with a proof that the output was generated correctly. Aliases: VRF, VRFs, Verifiable Random Function (smart contract randomness), Verifiable random function (NFT fairness).

Source: 04-EF - Randomness, Oracles, and External Data.

Verifiable randomness oracle. A service that supplies randomness with a proof that the output was generated correctly. Aliases: Chainlink VRF, VRF oracle.

Source: 05-CP - Case Study: Linux.Encoder RNG Failure.

Verification-weighted feedback. Feedback that is weighted more heavily when it is backed by checked outcomes rather than unsupported claims.

Source: 03-DS - Threats: Slander.

Verified outcome. An interaction result that has been checked with evidence such as hashes, signatures, or successful task completion. Aliases: verified outcomes, verified result.

Source: 03-DS - Trust but Verify: The Complete Trust Loop.

Verifier. The party that checks a presented verifiable credential and decides whether to accept the claim. Aliases: Verifier (verifiable credentials), credential verifier.

Source: 01-AS - Identity Case: Verifiable Credentials.

Version negotiation. A compatibility process where participants determine which protocol versions or features they can safely use together. Aliases: protocol negotiation.

Source: 01-DS - Fallacy #6: There Is One Administrator.

Versioned address format. A blockchain address design that marks which cryptographic scheme or account format the address uses. Aliases: Versioned address format (blockchain), address version, new address versions, versioned address formats.

Source: 05-CP - PQC Migration in Blockchain Systems.

View change. A recovery step where nodes move to a new view with a new leader after enough evidence of a stall. Aliases: View change (consensus), leader rotation, view changes.

Source: 01-CM - The Timing Limits — FLP and DLS Results.

View Key. A read-only key that lets a third party inspect transaction history without authorizing spending. Aliases: View Key (privacy coin compliance), read-only key, view keys.

Source: 02-FO - Forensic Limitations & Voluntary Disclosure.

Virtual Asset Service Provider. A business that provides services such as exchange, custody, transfer, or other virtual-asset activity for users. Aliases: CASP, VASP, crypto asset service provider, virtual asset service providers.

Source: 03-AS - Sub-Saharan Africa: Impact Signals.

Virtual coordinate space. CAN's logical map where keys hash to coordinates and peers own regions of the space. Aliases: Virtual coordinate space (CAN), coordinate space, grid, logical map.

Source: 02-DS - DHT Example: CAN.

Virtual Currency Exchange. A service where users trade or cash out crypto assets and where account records can become attribution evidence. Aliases: VCE, VCEs, Virtual Currency Exchange (blockchain investigations), crypto exchange.

Source: 02-FO - Breaking the Obfuscation: Account Clustering.

Virtual-asset service provider. A business that provides covered virtual-asset services such as exchange, transfer, custody, or administration for customers. Aliases: VASP, Virtual-asset service provider (FATF), virtual asset service provider.

Source: 04-BF - Off-Chain Controls: KYC and AML.

Volunteer computing. A distributed-computing model where many volunteers contribute idle machine resources to process large workloads. Aliases: volunteer distributed computing.

Source: 01-DS - Scientific Applications.

Vote phase. The phase where replicas or validators sign support for a candidate value. Aliases: Vote phase (consensus), vote, voting.

Source: 01-CM - Rounds and Phases.

W

Wallet. Software or hardware that manages blockchain keys and helps users create or authorize transactions. Aliases: Bitcoin wallet, Wallet (Bitcoin), Wallet (DApp architecture), Wallet (blockchain software), crypto wallet, hardware wallet, software wallet, wallets.

Source: 01-IN - Learning Objectives I.

Wallet application. A user-facing tool that manages keys, displays balances, and prepares or signs blockchain transactions. Aliases: crypto wallet, wallet, wallet app.

Source: 01-AS - What Does a User Actually Interact With?.

Wallet authentication. A login or access pattern where a user proves control of a blockchain address by signing a challenge. Aliases: wallet auth.

Source: 06-EF - How Token Gating Works.

Wallet Fingerprinting. Inferring wallet software or behavior from patterns such as output order, script type, or change address habits. Aliases: Wallet Fingerprinting (Bitcoin forensics), wallet behavior fingerprinting.

Source: 02-FO - Heuristic #2: Change Address Detection.

Wallet graph. A network view of wallets and the transfers among them used to trace flows, clusters, and relationships. Aliases: Wallet graph (forensics), address graph, operator wallet graph.

Source: 06-EF - Rug Pull Operator Wallet Graph.

Wallet reuse. The repeated use of the same wallet or related wallet cluster across activities, creating a link analysts can trace. Aliases: Wallet reuse (forensics), address reuse.

Source: 06-EF - The Frosties Rug Pull.

Wallet seed. Secret seed material from which a cryptocurrency wallet derives private keys. Aliases: seed phrase, wallet seeds.

Source: 05-CP - When Good Crypto Goes Bad: Milk Sad (CVE-2023-39910).

Wallet software. Software that helps a user create transactions and apply the private key needed to authorize them. Aliases: wallet, wallets.

Source: 02-IN - Step 1: Creation and Signing.

Wash trading. Trading in which related parties or the same actor buy and sell to themselves to inflate apparent price or volume. Aliases: Wash trading (NFT market), wash trade, wash trades.

Source: 05-EF - Royalties, Economics, and Marketplace Realities.

Weak subjectivity. The PoS property that new or long-offline nodes need a recent trusted checkpoint to identify the canonical chain safely. Aliases: Weak subjectivity (Ethereum PoS), Weak subjectivity (PoS bootstrapping), Weak subjectivity (Proof of Stake), weak subjectivity checkpoint.

Source: 03-CM - Weak Subjectivity.

WebAssembly. A portable low-level runtime target used by some smart contract platforms to run code compiled from languages such as Rust or Go. Aliases: WASM, Wasm, WebAssembly (smart contracts).

Source: 04-EF - Beyond Ethereum: Other Smart Contract Models.

Welcoming bootstrap. An onboarding approach that lets honest newcomers build reputation gradually without giving attackers immediate influence. Aliases: fair onboarding, safe onboarding.

Source: 03-DS - Key Considerations in System Design.

Wholesale CBDC. A central-bank digital instrument intended for settlement among financial institutions rather than general public use. Aliases: wholesale CBDCs.

Source: 02-AS - Central Bank Digital Currencies (CBDCs).

Wholesale Digital Currency. A digital currency designed for use by banks or financial institutions rather than ordinary retail users. Aliases: shared wholesale digital currency, wholesale CBDC.

Source: 03-AS - Gulf States: Impact Signals.

Withdrawal key. The offline key or credential used to control validator fund withdrawal and recovery. Aliases: Withdrawal key (PoS validator operations), withdrawal credential.

Source: 03-CM - Becoming a Validator.

Withdrawal pattern. A contract flow where users claim funds from recorded balances, commonly vulnerable if payment happens before accounting updates. Aliases: Withdrawal pattern (reentrancy), withdraw pattern.

Source: 04-EF - Reentrancy: Anatomy and Defenses.

Witness. The private information that makes a statement true and lets the prover generate a convincing proof. Aliases: Witness (zero-knowledge proofs), secret witness.

Source: 05-CP - Zero-Knowledge Proofs: Prove Without Revealing.

Work factor. The amount of computation an attacker is expected to need to succeed against a cryptographic property. Aliases: attack cost.

Source: 02-CP - Math Spotlight: Birthday Paradox and Work Factors.

Work unit. A packaged piece of computation assigned to a participant in a distributed volunteer-computing pipeline. Aliases: Work unit (volunteer computing), work units.

Source: 01-DS - Scientific Applications.

Workaround Rail. An alternative path used when mainstream financial infrastructure becomes unavailable, risky, or politically constrained. Aliases: alternative payment rail, alternative trade rail.

Source: 03-AS - Russia: Impact Signals.

World state. A query-friendly snapshot of the latest valid ledger values derived from the block log. Aliases: World state (Hyperledger Fabric), current state, current-value snapshot.

Source: 02-PC - From Permissioned Concepts to Fabric Terms.

Wrapped Asset. A token representation of value that is locked, controlled, or otherwise backed on another chain. Aliases: Wrapped Asset (cross-chain infrastructure), Wrapped asset (bridging), bridge-issued asset, linked token, wrapped equivalent, wrapped token.

Source: 02-FO - Mechanisms for Chain Hopping.

Wrapped token. A token representation of an asset from another chain that lives on the current chain's ledger. Aliases: Wrapped Monero, wrapped asset.

Source: 01-FO - Bridges & Swaps: Crossing the Chain Boundary.

X

XSema. A research system described in the lesson that automates cross-chain provenance extraction from bridge logs and related evidence.

Source: 01-FO - Future of Forensics: Automated Cross-Chain Tracing.

Z

Zcash. A cryptocurrency that supports both transparent transactions and shielded transactions using zero-knowledge proofs. Aliases: ZEC, Zcash (privacy coin).

Source: 02-FO - Zcash (ZEC): Optional Privacy.

Zero Knowledge rollup. A rollup model where Ethereum checks a cryptographic proof that the posted state transition was correct. Aliases: ZK rollup, ZK rollups, Zero Knowledge rollup (Ethereum L2), validity rollup, validity rollups.

Source: 01-EF - L2 Operator Models.

Zero-Knowledge Proof. A proof that convinces a verifier a statement is true without revealing the secret witness or other private information behind it. Aliases: ZK proof, ZKP, Zero-Knowledge Proof (cryptography), zero knowledge proof, zero-knowledge proof, zero-knowledge proofs, zero-knowledge proof.

Source: 05-CP - Zero-Knowledge Proofs: Prove Without Revealing.

ZK circuit. A constraint representation of a computation that a zero-knowledge proof system can prove was satisfied. Aliases: ZK circuits, zero-knowledge circuit.

Source: 05-CP - Zero-Knowledge in Blockchain Practice.

ZK rollup. A scaling design that batches many transactions off chain and posts a succinct validity proof for on-chain verification. Aliases: ZK rollup (Ethereum scaling), ZK rollups, validity rollup, zero-knowledge rollup.

Source: 05-CP - Zero-Knowledge in Blockchain Practice.

zk-SNARK. A compact zero-knowledge proof system used by Zcash to verify shielded transactions without revealing their private details. Aliases: zero-knowledge succinct non-interactive argument of knowledge, zk-SNARK (Zcash), zk-SNARK (privacy proof), zk-SNARKs.

Source: 02-FO - Zcash (ZEC): Optional Privacy.