A Guide for Enterprises: The Basics of Digital Asset Infrastructure

Etherealize x Chainlink

Table of Contents:

Building a Common Language for the Onchain Economy

Ethereum has entered its institutional era.

Banks, asset managers, and corporations are no longer debating if blockchain will reshape market infrastructure, but instead how it will integrate into their systems.

Despite this momentum, terminology remains fragmented. Terms like atomic settlement, account abstraction, and zero-knowledge proof are used daily, but rarely with a shared understanding.

This guide was created by Etherealize and Chainlink to provide a unified framework that bridges the vocabulary of traditional finance with the architecture of decentralized systems.

Our goal is simple: to make blockchain terminology clear, credible, and interoperable, so that institutions, developers, and policymakers can speak the language of the technology they're building on.

The Foundations of Blockchain Systems

Understanding digital assets begins with understanding the systems that secure and move them.

What Is a Blockchain?

A blockchain is a distributed ledger that is maintained by a network of independent participants rather than a single authority. Transactions are organized into blocks that are cryptographically linked to one another. Once recorded, data cannot be modified without the agreement of the network under its consensus rules.

Because the ledger is replicated across many participants and designed to operate continuously, blockchains provide resilient infrastructure that enables around-the-clock transfer and settlement of digital assets.

Bitcoin introduced the concept of decentralized digital currency. Ethereum extends this model by supporting programmable contracts executed directly on the ledger, enabling a broad range of automated financial applications.

What Is a Ledger?

A ledger is a record of ownership and transactions. In traditional markets, custodians, banks, and clearinghouses maintain ledgers internally. In blockchain systems, the ledger is synchronized across many independent computers (nodes), all verifying the same transaction history for accuracy and resilience.

What Is a Token?

A token is a digital record of ownership stored on a blockchain. It shows who owns what and allows ownership to be transferred securely without relying on a single central authority. Tokens can represent many things: a form of digital money, a claim on an asset like a Treasury bill, or a right to participate in a system or service.

Because tokens are managed by software on the blockchain, they can follow rules automatically. For example, a token can be designed so that it can only be transferred to approved parties, or so that interest payments and redemptions happen on schedule without manual processing. This gives tokens the ability to behave in an automated way, enabling faster settlement, easier tracking, and the ability to divide ownership into small pieces if needed.

What Is an Address?

An address is the location on a blockchain where ownership of assets is recorded. Instead of relying on a financial institution to maintain account records, ownership is established through cryptography. A private key grants the authority to initiate transactions, and anyone with that key can control the assets held at that address.

On Ethereum, addresses operate in two ways. Some are controlled directly by a private key, representing a user or institution acting on the network. Others are controlled by smart contract software, which can hold and transfer assets according to predefined rules. This structure enables both direct ownership and automated financial operations executed through code.

What Is a Wallet?

A wallet is the software or hardware that allows users to interact with blockchain accounts. A wallet does not store the assets themselves. It stores and protects the cryptographic keys that control the ability to move those assets recorded on the blockchain.

Wallets can be non-custodial, where the user controls the keys directly, or custodial, where a provider manages keys and access under defined governance and compliance processes. They may also be hot or cold, depending on how they are connected to networks. Hot wallets are kept online and allow rapid transaction processing. Cold wallets keep keys offline, providing stronger protection against unauthorized access.

What Is Account Abstraction?

Account abstraction upgrades how users authorize transactions. Instead of relying solely on a single private key, authorization can be handled by programmable logic. This enables features such as automated recovery controls, multi-signature authorization, spending limits, or rules for different assets or workflows. By treating accounts more like smart contracts, security policies and operational compliance can be tailored to institutional requirements without changing the underlying blockchain.

What Are Validation and Consensus?

Validation is the process that blockchain networks use to agree on the current state of the ledger. Instead of relying on a single authority, many independent participants review new activity and come to a shared agreement on the official record. When participants in a network have reached agreement on the current state of the ledger, they have reached consensus.
This approach replaces trust in a central operator with trust in a transparent and distributed system, helping ensure the ledger cannot be changed improperly and remains available even if individual participants go offline.

What Is Staking?

Staking is the process by which some blockchains select validators and achieve consensus. Stakers voluntarily lock up a certain amount of the network's digital asset to show they have a stake in the system, and in exchange are given the opportunity to vote on the current state of the ledger. Some protocols reward stakers for their role in helping the network achieve consensus. Stakers can also be penalized if they fail to do their job or violate protocol rules. Staking allows blockchains to remain secure while reducing energy consumption.

What Is Slashing?

In proof-of-stake systems, validators may lose part of their stake for misconduct or failures defined by protocol rules. This potential penalty keeps the network secure for other users.

What Are Gas Fees?

Every action on a blockchain, such as updating balances or running a smart contract, requires computing power from the network. Users pay gas fees to compensate the network for the computing power used to process their transactions.

What Are Smart Contracts?

Smart contracts are computer programs stored on a blockchain that automatically carry out actions when certain conditions are met. They remove the need for manual processing or intermediaries because the rules are built directly into the software. Once deployed, they operate exactly as written, providing a predictable and transparent way to execute agreements such as trades, payments, or asset transfers without relying on a central party to oversee or enforce them.

What Are Layer 2s?

Layer 2s are infrastructure built on top of a base blockchain such as Ethereum in order to handle transactions more efficiently. They process activity separately and then update the main chain with the results. This approach allows Ethereum to scale without altering its core security model. Institutional users can benefit from lower costs, higher throughput, and the ability to customize privacy and execution environments. Layer 2s manage transaction processing, while Ethereum provides settlement finality and protection against disputes. This separation supports high-volume financial activity without compromising trust in the underlying ledger.

Data & Connectivity

Blockchains operate as closed systems, but financial markets do not.
Data connectivity enables smart contracts to execute based on external conditions while preserving blockchain security guarantees.

How Does a Blockchain Interact with External Data?

Because blockchains cannot fetch data from external services on their own, they rely on oracle networks to bring trusted information onchain. These systems source data from multiple providers, validate the information using cryptographic and consensus-based techniques, and then deliver it to smart contracts. This prevents reliance on single data feeds and reduces the risk of manipulation. The result is a secure connection between programmatic settlement and real-world financial signals, allowing everything from collateral valuations to corporate actions to update automatically.

What Is Proof of Reserves and Why Is It Important?

Tokenized assets and stablecoins often depend on offchain reserves such as cash, Treasuries, or commodities. Chainlink Proof of Reserve provides a verifiable link between these reserves and the corresponding supply of digital tokens. By posting cryptographic attestations or automated confirmations onchain, Proof of Reserve allows market participants and regulators to independently verify that assets remain fully backed in near real time. This improves confidence in tokenized instruments and supports more transparent risk management.

What Is Interoperability?

Blockchains are designed as sovereign networks with their own assets and execution environments. Interoperability refers to the standards and mechanisms that enable blockchains to exchange value and data without creating new central points of control. With secure cross-chain infrastructure, institutions can unify operations across fragmented ecosystems, such as transferring collateral where it is most efficiently deployed, accessing liquidity across markets, and optimizing settlement flows globally. This creates a more connected digital infrastructure that aligns with how financial systems operate today.

What Are Attestations?

Attestations serve as cryptographically signed claims that a specific fact is true, such as identity verification, asset ownership, or regulatory status. They allow institutions to confirm eligibility or compliance without exposing underlying sensitive information. Attestations can be reused across applications, reducing redundant onboarding, improving privacy controls, and enabling a more portable and interoperable compliance framework across the onchain economy.

Privacy

Public ledgers are transparent by design, but many institutional activities require confidentiality. Privacy-preserving methods allow sensitive information to remain protected while still enabling independent verification of outcomes. In some cases, these methods enhance privacy protections beyond what is possible in traditional infrastructure, allowing markets to operate with greater efficiency, security, and control over information exposure.

What Is a Zero-Knowledge Proof?

A zero-knowledge proof is a cryptographic method that allows someone to prove that a statement is true without revealing the underlying information. This enables validation of facts, such as identity, asset ownership, or transaction correctness, while keeping sensitive data confidential. For financial institutions, zero-knowledge proofs provide a path to meeting regulatory and reporting requirements while limiting the exposure of client information or proprietary positions. They can be used to verify eligibility, perform balance checks, or confirm compliance conditions directly on a blockchain, without disclosing the underlying details to the public. In this model, transparency applies to the correctness of the system, while privacy applies to the details of individual participants, giving organizations and consumers greater control over what information they share and with whom.

What Is Selective Disclosure?

Selective disclosure allows a participant to reveal only the minimum information required for a specific purpose, such as confirming jurisdiction, accreditation, or exposure thresholds, while withholding other data.

What Are Trusted Execution Environments (TEEs)?

TEEs are secure areas of hardware that execute code privately, protecting sensitive data even from the operator of the system. Inputs are processed inside the protected environment, and only the approved outputs are shared externally. This enables confidential workflows, such as order matching or valuation, while still anchoring trust in the blockchain through verifiable commitments to the results.

What Is the Concept of Data Minimization?

Privacy is not only about protecting what is stored, it is also about limiting what is ever revealed. Data minimization ensures that only the information required for a specific authorization, regulatory check, or settlement event is shared, reducing unnecessary data exposure and long-term storage obligations.

Governance & Upgrades

Some blockchain systems are decentralized, meaning they evolve through processes that distribute decision-making.

What Is Onchain Governance?

Onchain governance uses mechanisms such as token- or identity-based voting to approve parameter changes, treasury actions, or upgrades. The procedures are transparent and verifiable on the ledger.

How Do Upgrades Happen?

Upgrades combine open development, review, and deployment steps that are validated by network participants. The process defines who proposes changes, how they are approved, and how they are safely executed.

What Is a DAO?

A DAO is an arrangement where resources and rules are managed collectively through onchain processes. It formalizes participation and accountability for shared operations or treasuries.

What Is Credible Neutrality?

Credible neutrality is the design principle that infrastructure should not privilege specific users, assets, or jurisdictions. It supports predictable operations and reduces policy or governance bias.

The Application Layer

Blockchains are not just new technologies, they are the foundation of a new market infrastructure. Traditional market functions like settlement, custody, and compliance are now being redefined through programmable code.

What Is Decentralized Finance (DeFi)?

DeFi replicates and extends the functions of traditional finance, such as borrowing, lending, trading, and yield generation, through smart contracts rather than intermediaries. It operates on open, programmable networks, enabling 24/7 access to liquidity, credit, and yield. DeFi protocols are composable, meaning they can integrate seamlessly, allowing users or institutions to stack financial products and automate capital deployment.

What Is Tokenization?

Tokenization is the process of representing ownership of a physical or financial asset on a blockchain. The token serves as an onchain record of the rights associated with the asset, enabling transfers and lifecycle events to be managed through software. When applied to traditional instruments such as Treasuries, funds, or real estate, tokenization provides a new technical framework for how ownership can be recorded, transferred, and integrated with digital infrastructure.

What Are Stablecoins?

Stablecoins are digital tokens pegged to a fiat currency, typically backed by reserves of cash and short-term government securities. They function as the settlement currency of the onchain economy, enabling predictable pricing, stable collateral, and dollar-denominated transactions within decentralized systems. The recent GENIUS Act provides regulation to ensure that issuers maintain offchain reserves and are audited regularly.

What Is Atomic Settlement?

Atomic settlement is a transaction design in which all components of a trade, such as delivery of an asset and payment for that asset, are completed simultaneously. Either the entire transaction succeeds, or none of it does. This removes the possibility that one party fulfills its side of the agreement while the other does not. On blockchains, atomic settlement is enforced by software rather than by intermediaries, allowing transfer of ownership and payment to occur in a single, coordinated update to the ledger.

Glossary

Account Abstraction

Account abstraction is an architectural upgrade that allows accounts to use programmable logic to authorize actions. It enables features such as automated recovery, multi-party authorization, spending limits, and compliance-enforced workflows.

Address

An address is the unique identifier on a blockchain where assets are held. It represents ownership and can be controlled either by a private key (externally owned accounts) or by smart contract code.

Atomic Settlement

A transaction design in which all parts of a trade complete at the same time or not at all. It prevents one side from settling without the other.

Attestation

A signed, verifiable claim that certain data or facts are accurate, which others can check without accessing the underlying details.

Automated Market Maker (AMM)

A trading mechanism that uses pooled liquidity and a formula to set prices instead of a traditional order book.

Bridge

Technology that moves assets or information between otherwise separate blockchains, enabling cross-network use.

Cold Storage

The act of keeping private keys offline to reduce exposure to cyber threats.

Consensus

Consensus is the mechanism through which independent participants in a blockchain network agree on the canonical state of the ledger. It ensures that all parties share the same transaction history without relying on a central authority.

Credible Neutrality

Operating principles and design choices are intended to avoid special treatment of particular users, assets, or jurisdictions.

Custody

Custody refers to the control and safekeeping of private keys and digital assets. It can be performed by the owner (self-custody) or by a regulated third party under defined governance, security, and compliance frameworks.

DAO (Decentralized Autonomous Organization)

A governance arrangement where rules and decisions are managed onchain by participants, typically using tokens.

Data Availability (DA) Layer

Infrastructure that ensures the data behind transactions remains retrievable for verification, even if execution happens off the base chain. This supports scale while preserving auditability.

Data Minimization

Data minimization is a privacy principle that limits the amount of information shared or stored to only what is necessary for a given operation. It reduces exposure risks and long-term custodial obligations.

Decentralized Exchange (DEX)

A protocol that enables users to trade directly through smart contracts without a centralized intermediary.

Digital Asset Treasury (DAT)

A treasury vehicle that holds and manages digital assets. This approach enables digital assets to be incorporated into regulated financial frameworks while maintaining standard governance and oversight.

Digital Identity

A verifiable, cryptography-based identifier that can be used for access control, compliance checks, or attestations.

Execution Environment

An execution environment is the computational context where transactions are processed and smart contracts run. Layer 2s can offer specialized execution environments tailored for cost efficiency, privacy, or institutional workflows.

Gas Fees

Gas fees are payments made by users to compensate the network for the computational work required to execute transactions or run smart contracts. Gas aligns resource usage with cost and helps prevent spam.

Governance Token

A token that conveys voting rights over protocol parameters, upgrades, or treasury decisions.

Hot Wallet

A wallet connected to the internet, which is necessary for performing certain functions requiring prompt online signatures.

Layer 1 (L1)

The base blockchain where transactions are recorded and finalized. It is the primary ledger of ownership and source of security. For the purposes of this glossary, that blockchain is Ethereum.

Layer 2 (L2)

Infrastructure built on top of a Layer 1 that executes transactions more efficiently and then updates the base chain with the results. It aims to increase throughput and reduce cost while relying on L1 for settlement and security.

Liquidity Mining

Distributing tokens or fees to participants who supply assets to a protocol, as an incentive to deepen liquidity.

Liquidity Pool

A smart contract holding assets that others can trade against or borrow from, usually in return for fees or rewards to providers.

Node

A computer that stores the ledger and propagates records of new transactions. Broad, independent participation improves resilience.

Onchain Governance

Decision-making is conducted on a blockchain, typically using tokens or identities to vote on changes.

Oracle Networks

Oracle networks deliver secure external data to smart contracts. They aggregate information from multiple independent sources and provide cryptographic assurances so that blockchain applications can rely on offchain data without introducing new trust dependencies.

Private Key

A private key is a confidential cryptographic credential that grants control over a blockchain address. Anyone with the private key can authorize transactions and move assets, making secure storage essential for institutional operations and key-management policies.

Proof of Reserve

A method for an issuer or custodian to demonstrate that sufficient real assets back the tokens in circulation, using cryptographic or programmatic checks.

Proof of Stake (PoS)

A consensus method in which validators commit assets (“stake”) and may earn rewards for contributing to the security of the network.

Real-World Assets (RWAs)

Offchain assets, such as securities, real estate, or commodities, represented in tokenized form on a blockchain.

Rollup

A Layer 2 approach that processes many transactions and posts a proof or summary to the base chain. This preserves integrity while lowering congestion and cost.

Selective Disclosure

Selective disclosure is a privacy method that allows users or institutions to reveal only the minimum information required for a specific verification, such as jurisdiction or accreditation, while withholding other sensitive details.

Sequencer

A component of some Layer 2s that orders transactions before they are finalized on L1.

Settlement

Settlement is the final transfer of ownership or payment that completes a transaction. In blockchain systems, settlement is executed programmatically and recorded directly on the ledger, reducing reliance on intermediaries and batch processes.

Slashing

A penalty that removes part of a validator's stake for downtime or violating the rules of the protocol.

Stablecoin

A token designed to track the value of a reference asset, commonly a fiat currency, typically supported by reserves.

Tokenization

The representation of ownership or rights to an asset recorded on a blockchain.

Total Value Locked (TVL)

A measure of the assets deposited in a protocol, used as a proxy for scale and liquidity but not a measure of risk.

Trusted Execution Environment (TEE)

A TEE is a secure hardware enclave that executes code in isolation from the rest of the system. It protects sensitive data during processing and provides verifiable outputs that can be anchored onchain.

Validator

A participant that helps a network achieve consensus about the current state of the ledger.

Validation

Validation is the process by which network participants verify that new transactions follow protocol rules. Validators check correctness before data is added to the ledger, supporting network integrity and preventing invalid updates.

Yield

Return generated by deploying assets, for example through staking, lending, or providing liquidity, subject to associated risks.

ZK Circuits

The structured computations used to generate and verify zero-knowledge proofs.

Zero-Knowledge Proof (ZKP)

A method to prove a statement is true without revealing the underlying information, enabling verification with limited disclosure.

Etherealize x Chainlink

Ending Remarks

This glossary is intended to provide clear and consistent language for institutions evaluating or engaging with blockchain-based systems. As terminology continues to develop alongside technology and regulation, definitions will evolve. Our goal is to support informed discussion and decision-making by offering a shared reference point across market participants, policymakers, and service providers.