

Onyx

onyx.org

Cryp2Nova

Archived copy · cryp2nova.com

Onyx

Contents

Introducing Onyx 07

Architecture 13

Tokenization 25

Security 39

Economics 43

Tokenomics 47

Governance 50

Keeping Onyx Fair 55

Enterprise Features 57

Creating Trust 62

Potential Use Cases 66

Final Notes 73

CRYP2NOVA

Archived copy · cryp2nova.com



Onyx is creating a secure and inclusive digital infrastructure that empowers individuals and enterprises to interact, build, and transact with confidence. From financial grade products to creative and commercial applications, our ecosystem ensures privacy, trust, and equitable access for all.

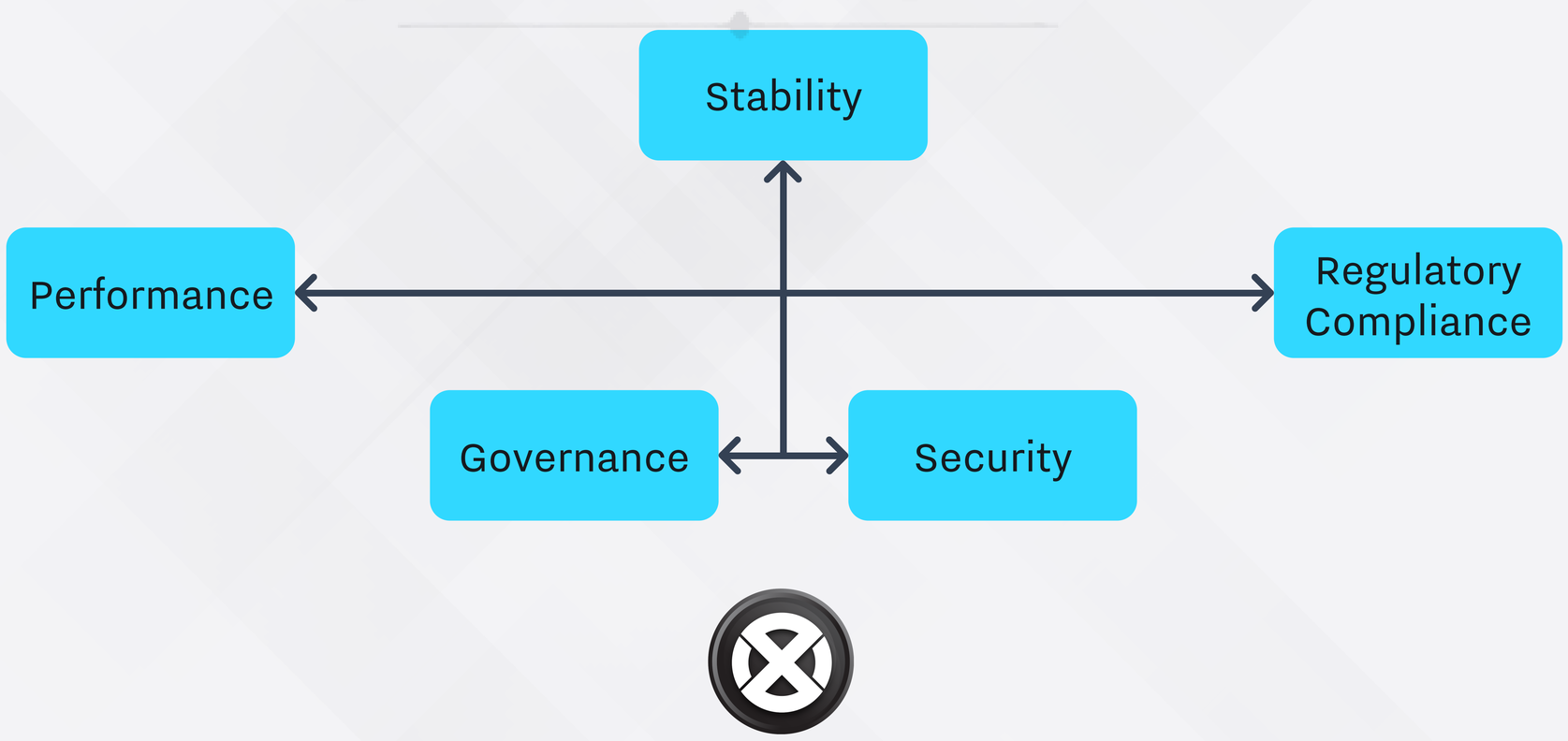
Archived copy · cryp2nova.com

Distributed ledger technologies (DLTs) have the potential to transform industries at scale, but realizing this promise requires overcoming five core challenges that currently hinder enterprise adoption. A viable platform must deliver high transactional performance, formally verified security, decentralized and expert-driven governance, enforceable mechanisms for systemic stability, and robust tools for regulatory compliance. This whitepaper explores these critical requirements and assesses how Onyx addresses them through a technically rigorous, scalable, and trustworthy framework.

To support trillions in digital value transfer, public DLTs must withstand persistent adversarial threats with mathematically proven consensus mechanisms, ensuring uncompromised security without sacrificing decentralization. Compliance with evolving regulations, including GDPR and sanctions enforcement, demands built-in identity and data governance capabilities.

At the same time, enterprise-scale applications require throughput of hundreds of thousands of transactions per second and consensus finality within seconds, performance levels that exceed those of most current platforms. Sustainable governance must be decentralized, globally representative, and equipped with legal, technical, and economic expertise. Finally, long-term stability depends on both resilient infrastructure and enforceable decisions that uphold consensus and policy integrity.

Only through the convergence of these capabilities can a distributed ledger achieve the trust and functionality necessary for widespread adoption in mainstream markets.



Archived copy · cryp2nova.com

Onyx

Onyx is a public network and decentralized governance framework architected to meet the technical, regulatory, and operational requirements of mainstream market adoption. The Onyx network will be governed by the Onyx DAO (Decentralized Autonomous Organization) consisting of XCN holders on the Ethereum ERC-20 Blockchain. These holders can shape the direction of the Onyx DAO and Onyx through their participation in Onyx Improvement Proposals (OIPs).

This governance framework is designed to ensure a secure and trusted digital environment, one that relies on decentralized entities rather than centralized entities exerting disproportionate control. Decision-making authority is distributed among XCN holders, each possessing voting rights over critical platform policies and technical direction proportionate to how many XCN tokens they hold.

The Onyx network is a distributed ledger platform engineered to address the principal limitations hindering mainstream adoption of public DLT systems. Onyx maintains platform stability through a carefully designed combination of technical safeguards and Governance frameworks, ensuring consistent operation and reinforcing trust across its ecosystem. Onyx delivers near-optimal bandwidth efficiency, enabling the network to process hundreds of thousands of transactions per second within a single shard, a tightly connected mesh of peer-to-peer nodes.

Upon launch, Onyx is projected to handle approximately 100,000 cryptocurrency transactions per second, with final consensus reached in seconds, setting a new performance benchmark far beyond that of traditional public distributed ledger technologies.

Security is foundational to Onyx’s architecture. Onyx achieves asynchronous Byzantine Fault Tolerance (aBFT), the highest known level of security for distributed consensus. Unlike other protocols that rely on centralized coordinators, leaders, or timeouts which introduce vulnerabilities to Distributed Denial of Service (DDoS) attacks, Onyx leaderless model is inherently resilient. This approach ensures robust security, even at scale, and marks a significant advancement in the field of distributed systems.

Onyx also guarantees both Fair Access and Fair Ordering of transactions. It ensures that no single participant can censor transaction submission or manipulate the transaction ordering in consensus. Transactions are ordered according to their actual receipt times by the network, preserving fairness in both inclusion and sequencing.

Archived copy · cryp2nova.com

Onyx's technical architecture supports two core capabilities essential for the secure and compliant operation of a distributed ledger.

First, Onyx employs a shared state mechanism that enables software clients to verify the integrity and provenance of Onyx before engaging with it. This mechanism prevents network nodes from forking the official platform and propagating unauthorized modifications. In the event of divergent changes to the original and a modified copy, clients can deterministically identify and reject the invalid version, ensuring ledger consistency and tamper resistance.

Second, Onyx enables coordinated, deterministic software updates across all network nodes, as specified by the Onyx DAO. This mechanism enables the Onyx DAO to specify the exact content and timing of protocol changes and to verify their implementation across the network.

Upon release, updates are applied simultaneously to all participating nodes. Any node failing to implement the authorized update is excluded from consensus participation and cannot propagate an alternative ledger state, thereby preserving protocol uniformity and network integrity.

The Onyx codebase will be governed by XCN holders through the Onyx DAO and made publicly available for review with the release of Version 1. Use of the Onyx platform will not require a license, including for developing applications, integrating services, or deploying smart contracts. Developers will be able to create either open-source or proprietary applications without seeking permission or approval from the Onyx DAO.

The Onyx technical architecture incorporates controlled mutability of network state and supports the attachment of supplementary data to transactions, including identity certificates. These capabilities enable optional features, such as the deletion of personal data and the use of verified identity mechanisms, all governed by the end-user's consent. Onyx is committed to engaging with regulatory bodies and promoting the development of tools that support enterprises in meeting their consumer protection and regulatory compliance requirements.

This approach ensures transparency while enforcing the consistency and trust required for the broad market adoption of a publicly distributed ledger.

The integration of these controls equips the DAO with the necessary mechanisms to enforce effective governance and maintain protocol coherence. This framework establishes the operational and regulatory stability deemed essential for the widespread adoption of the platform.

Archived copy · cryp2nova.com

Introducing Onyx



Archived copy · cryp2nova.com

The Onyx data structure and consensus algorithm constitute a novel framework for achieving distributed consensus. This introduction outlines the operational principles of Onyx and highlights its key properties. The primary objective of a distributed consensus algorithm is to enable a network of participants, without mutual trust, to agree on the chronological ordering of transactions. Onyx accomplishes this objective through a fundamentally distinct approach, establishing trust in adversarial or trustless environments.

A blockchain functions as a linear structure analogous to a tree that undergoes continuous pruning to prevent divergent branches and maintain a single authoritative chain of blocks. In contrast, Onyx retains all information by integrating concurrent events directly into the ledger, eliminating the need for pruning and preserving the full history of network activity.

In both blockchain and systems like Onyx, users can initiate transactions that are subsequently encapsulated within a data structure, referred to as a “block” in blockchain systems, and propagated across the distributed network for eventual inclusion in the shared ledger.

In blockchain systems, blocks are designed to form a single, linear chain of data. When multiple blocks are produced concurrently, network consensus protocols dictate that one branch will be selected for continuation. In contrast, the others are discarded to prevent a forked or divergent ledger state. This process results in the continual elimination of alternative valid paths, preserving only a singular, authoritative sequence of blocks.

With Onyx, all blocks of transactions are retained and integrated into the ledger, none are discarded, resulting in greater efficiency compared to blockchain architectures. Rather than eliminating concurrent event histories, Onyx preserves and merges them into a unified, non-linear structure, ensuring that all valid contributions are permanently reflected in the consensus.

Moreover, blockchain systems encounter limitations when new blocks are generated too rapidly, as the resulting proliferation of branches can exceed the system’s ability to resolve them into a single chain. To mitigate this, mechanisms such as proof-of-work are employed to constrain block production rates artificially.

Archived copy · cryp2nova.com

In contrast, Onyx imposes no such restriction; the data structure accommodates rapid growth without loss of information. All events are preserved, and participants may submit transactions and event blocks freely without compromising consensus integrity or system performance.

Finally, because Onyx incorporates all transaction events without discarding potential forks, it enables stronger formal guarantees than traditional consensus models. Specifically, Onyx achieves Byzantine fault tolerance along with fairness in transaction ordering, capabilities not simultaneously provided by other systems. While other protocols offer Byzantine agreement without fairness, and blockchain provides neither, Onyx delivers a consensus framework that is fair, Byzantine, high-performance, ACID-compliant, resource-efficient, cost-effective, timestamped, and resistant to denial-of-service attacks.

Throughput

Onyx achieves high throughput, constrained primarily by network bandwidth rather than computational overhead. If each node possesses sufficient bandwidth to transmit and receive a specified volume of transactions per second, the overall network can process a comparable transaction load. In practice, even a standard high-speed residential internet connection can support an Onyx node capable of handling transaction volumes comparable to those of global-scale payment systems, such as the VISA network.

Cost

An Onyx-based distributed ledger offers significantly lower operational costs compared to traditional blockchain systems, as it eliminates the need for energy-intensive consensus mechanisms such as proof-of-work. Operating an Onyx node does not require investment in specialized mining hardware; instead, nodes can be deployed on standard, commercially available computing infrastructure, reducing both capital and energy expenditures.

Archived copy · cryp2nova.com

Efficiency

Onyx achieves 100% efficiency as defined within the blockchain domain, wherein no computational effort is wasted. In blockchain systems, resources are often expended on mining blocks that are subsequently orphaned and discarded. In contrast, all transaction events in Onyx are permanently incorporated into the ledger, eliminating such inefficiencies. The protocol is also bandwidth-efficient: it requires only minimal additional overhead beyond the basic dissemination of transactions to establish consensus timestamps and determine transaction order.

Once a transaction is submitted to the network, all nodes reach a deterministic agreement on its position within the transaction history within seconds, with finality and 100% certainty.

Crucially, each node also possesses common knowledge of this consensus state; that is, every node knows that all other nodes have reached the same conclusion. As a result, the network can apply the transaction's effects immediately and, unless required for auditing or regulatory compliance, discard the transaction data. In a minimal cryptocurrency implementation, this allows nodes to maintain only the current balances of non-empty accounts without retaining the complete transactional history back to the genesis block.

Scaling

The Onyx network, governed by the Onyx DAO, is designed to decentralize progressively over time, starting from a foundation of trusted node operators and evolving into a fully permissionless ecosystem. Initially, the Onyx DAO Treasury will proxy-stake XCN to DAO-operated nodes, while users may also delegate their stake to these nodes. As the network matures, node operation will expand to include additional operators. While anonymous node operators will not receive proxy stake from the DAO or default wallet configuration unless sanctioned through additional Onyx Improvement Proposals, third-party wallets may enable such delegation.

This staged decentralization strategy, supported by ongoing token distribution from the Treasury, strategic incentives, and a growing pool of existing XCN holders aims to facilitate a competitive, open market for proxy staking, where wallet providers and node operators compete to attract stake in a fully decentralized environment.

Archived copy · cryp2nova.com

Staking and Proxy Staking

While XCN will still maintain its presence on Ethereum as an ERC-20 token with staking support for DAO Governance, Onyx introduces new utility for XCN in the form of staking as it will utilize a proof-of-stake (PoS) consensus mechanism with native XCN where a node's influence on consensus decisions is directly proportional to the amount of XCN staked to it.

A transaction achieves consensus when validated by nodes collectively representing more than two-thirds of the total network stake. Ensuring that a substantial portion of the XCN supply is actively staked on Onyx is essential to maintaining the integrity and liveness of the network.

In the network's initial phase, the Onyx DAO Treasury will contribute by proxy-staking XCN to select nodes, thereby enabling consensus formation while adoption increases.

As XCN becomes more widely distributed to nodes, mitigating the risk that any individual or coordinated group could gain control of one-third of the total supply, the network will by default operate under its permissionless design, allowing anyone to host a node. To participate, a node must declare one or more accounts it controls and cryptographically prove ownership of the corresponding private keys. The aggregate balance of those accounts determines the node's voting weight in the Onyx voting algorithm, and nodes are compensated based on this weight.

Importantly, staked XCN remains fully liquid. They can be spent at any time, thereby avoiding one of the primary drawbacks of traditional bonded proof-of-stake systems, which often lock assets and reduce liquidity.

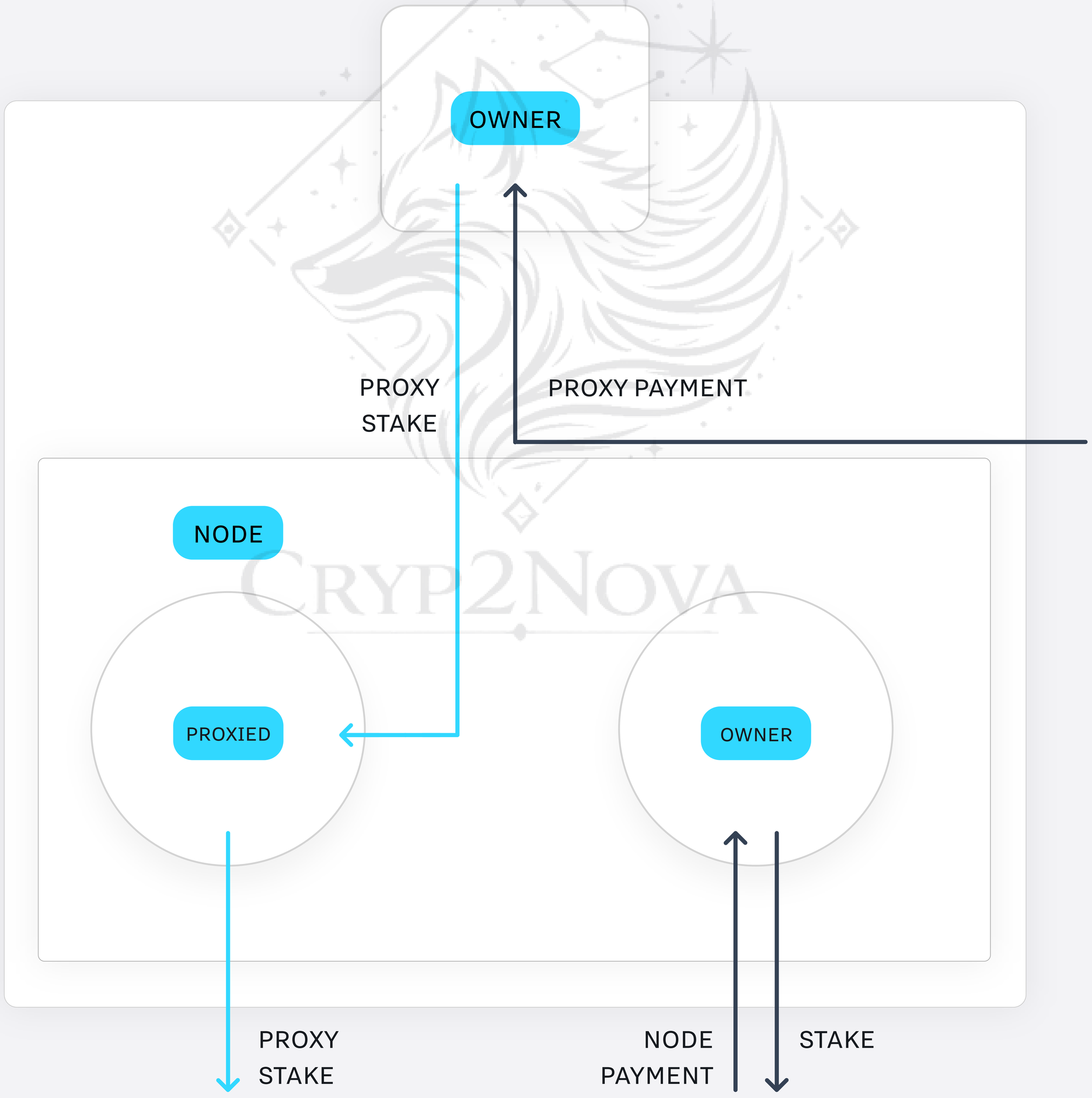
Onyx also introduces proxy staking, a mechanism that allows users who do not operate nodes to still contribute to consensus and earn rewards. By proxy staking, a user assigns their XCN to a participating node, increasing the node's stake weight.

The node's rewards are then shared with the XCN owner that is proxy-staking. Proxy-staked XCN remains entirely under the owner's control, allowing them to withdraw, reassign, or spend them at any time. Proxy staking does not grant the node spending authority.

Finally, all nodes must maintain a non-zero XCN balance to participate in consensus and to cover transaction fees incurred when submitting messages to the ledger.

Archived copy · cryp2nova.com

The diagram below shows the proxy staking model, where a node's stake includes both the XCN it owns and any XCN delegated to it by proxy stakers. Rewards from this combined stake are shared between the node operator and proxy stakers. This allows users to earn rewards without running a node, strengthens network security by distributing stake more broadly, and helps node operators increase their revenue.



Archived copy · cryp2nova.com



Architecture

CRYP2NOVA

Archived copy · cryp2nova.com

The Onyx network is a multi-layered, modular system designed to support decentralized applications at scale with uncompromising performance, security, and flexibility. Its architecture is composed of distinct but interlocking layers, each responsible for a critical set of functions ranging from secure message transmission to consensus, file storage, and programmable logic.

At its foundation, Onyx leverages conventional internet infrastructure while eliminating common points of failure such as DNS, enabling resilient peer-to-peer connectivity. Above this transport layer, Onyx's consensus protocol establishes a deterministic, timestamped ordering of all network transactions, ensuring data consistency across a decentralized node set.

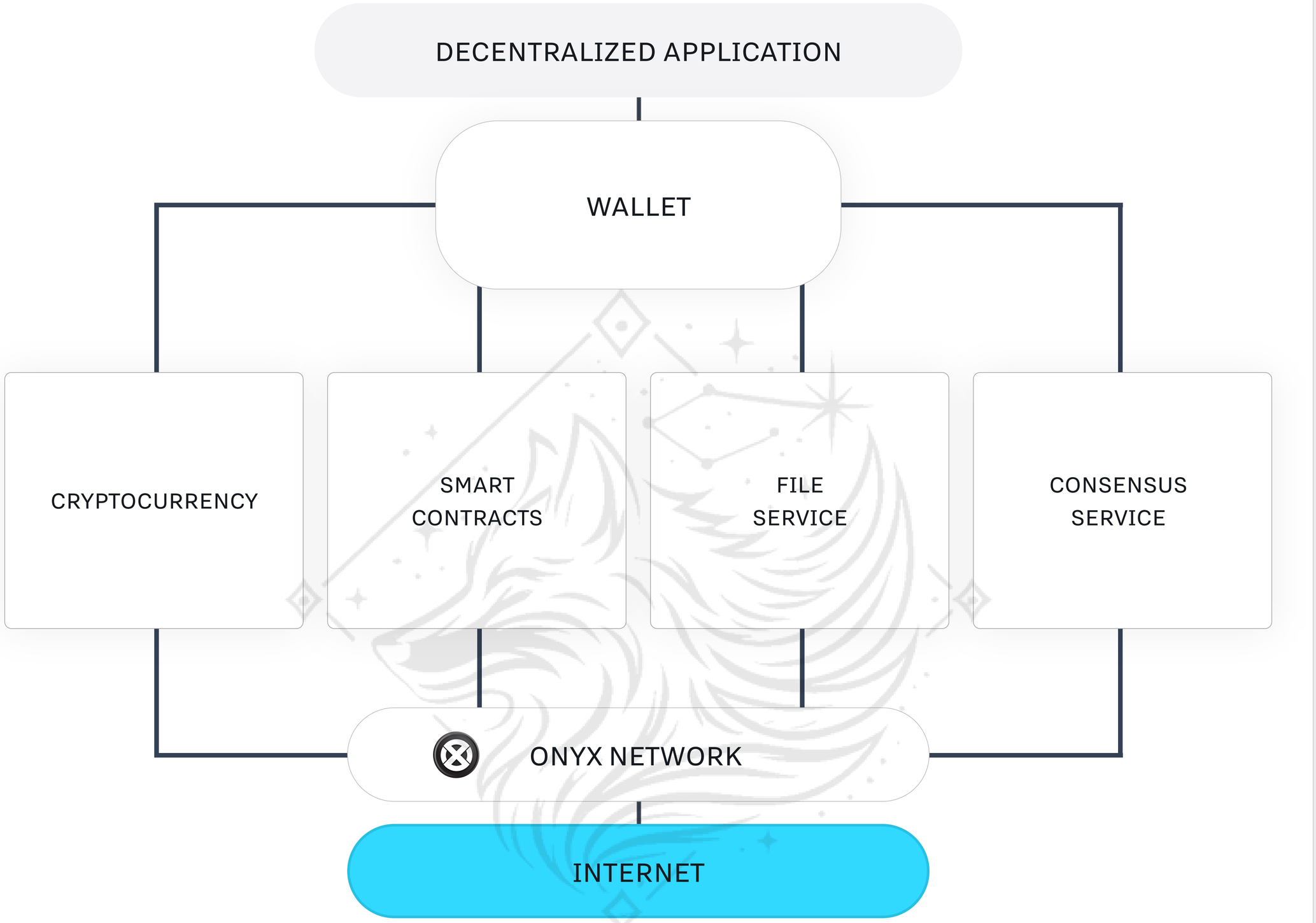
On top of this core, the Services Layer introduces a suite of capabilities, native cryptocurrency, smart contract execution, distributed file storage, and a high-performance consensus service, all accessible via a unified API governed by the Onyx DAO, and in turn XCN holders. To support scalability and real-time responsiveness, Onyx incorporates sharding and a consensus node network that distributes read-access efficiently across the ecosystem.

Together, these components create a robust platform for building secure, auditable, and high-throughput decentralized systems, suitable for applications in finance, identity, logistics, IoT, and beyond.



Archived copy · cryp2nova.com

Internet layer



Onyx network nodes are internet-connected computers that communicate over standard TCP/IP protocols, with all data transmissions secured using Transport Layer Security (TLS). This encryption protocol incorporates ephemeral cryptographic keys, which are generated for each session and discarded afterward, providing perfect forward secrecy.

This means that even if a node’s long-term private key is compromised, past communications remain secure and indecipherable.

Archived copy · cryp2nova.com

Each node within the Onyx network is uniquely identified by its IP address and port number rather than relying on domain names or the Domain Name System (DNS). By avoiding DNS entirely, the network eliminates a significant point of vulnerability common in many distributed systems, namely, DNS hijacking, poisoning, or other forms of name resolution attacks.

This architectural decision enhances the network's resilience against censorship, surveillance, and disruption, making it more robust and more challenging to tamper with or take offline using conventional attack vectors.

Onyx Consensus Layer

Nodes in the Onyx network act as active participants in both the intake and distribution of transactions submitted by clients. When a client submits a transaction to any node, that node immediately begins disseminating the transaction to its peers through a fast and fault-tolerant algorithm. This ensures that every valid transaction is rapidly propagated throughout the network in a redundant and decentralized manner, making the system highly resilient to node failures or network partitions.

Once transactions are widely disseminated, each node independently executes the Onyx consensus algorithm, a deterministic protocol designed to establish a unified view of the network's history. Through this process, nodes collaboratively determine a consensus timestamp for each transaction and reach an agreement on a definitive, total ordering of all transactions across the network. This ensures that, regardless of when or where a transaction is first received, all nodes reach the same conclusion about its place in the Onyx network.

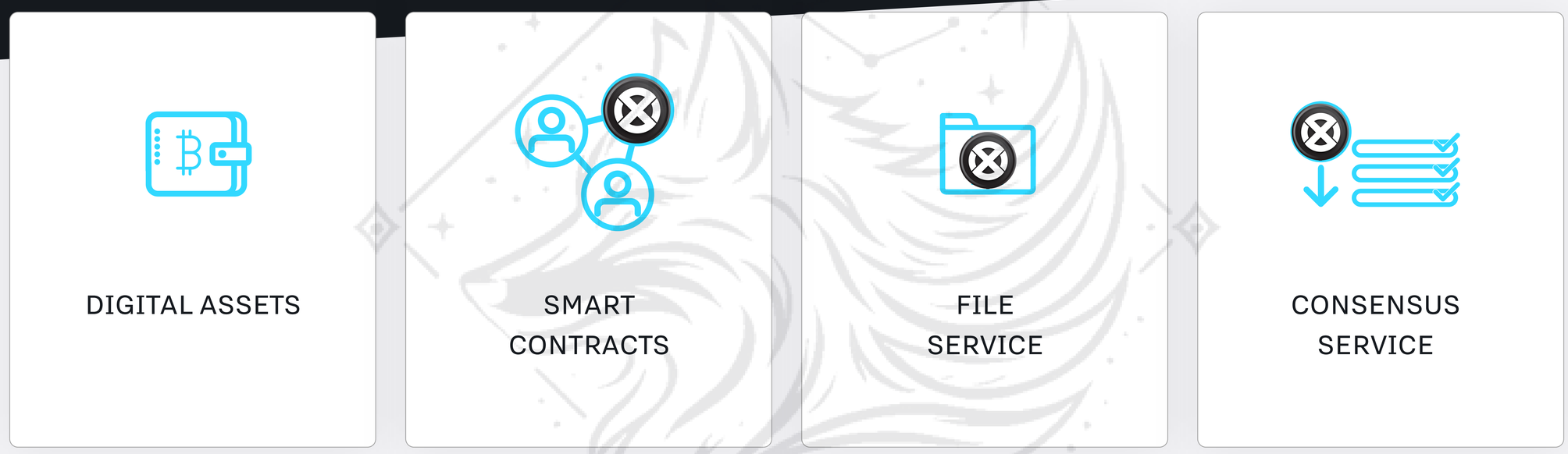
After consensus is achieved, each node applies the transactions to its local copy of Onyx in the exact order defined by the consensus. This synchronized application process updates the shared state in a consistent and verifiable way. As a result, all nodes within a given shard maintain identical views of Onyx current state, ensuring complete data consistency and enabling trustless coordination across the network.

Archived copy · cryp2nova.com

Services Layer

The Onyx Services Layer represents the operational heart of the platform, a modular suite of network-native capabilities built atop Onyx's consensus protocol. These services expose core functionality to developers and applications, enabling decentralized execution, secure storage, digital asset management, and trustless event ordering.

Each service is designed to leverage the performance, fairness, and security guarantees of the underlying consensus engine, while remaining flexible enough to support diverse enterprise and public-sector use cases.



Native Currency

Onyx native cryptocurrency is XCN. This bridged implementation of XCN is engineered for high throughput and low latency, resulting in low transaction fees that make microtransactions economically viable. Network participation will be open to any user, who may operate a node and receive compensation for contributing to consensus.

Users can create accounts by generating a public-private key pair, with no requirement to associate personally identifiable information such as a name or address. However, the platform supports optional identity binding through the attachment of hashed identity certificates, issued by third-party certificate or identity authorities selected by the user. This mechanism is intended to facilitate regulatory compliance in jurisdictions requiring adherence to Know Your Customer (KYC) or Anti-Money Laundering (AML) obligations.

Archived copy · cryp2nova.com

Smart Contracts

Onyx offers robust support for executing smart contracts written in Solidity, the industry-standard programming language widely used across Ethereum-compatible ecosystems. Thanks to this compatibility, developers can seamlessly deploy existing Solidity codebases, including extensive libraries and complex smart contracts onto Onyx without the need for modification or refactoring.

This interoperability not only preserves the value of established tooling and frameworks but also significantly accelerates the development and deployment of decentralized applications. As a result, teams can leverage familiar development workflows while taking advantage of Onyx's performance and consensus guarantees.

File Storage

Onyx file system enables users to store data with network-wide consensus on both the content and existence of each file. All nodes within a shard store identical copies, ensuring fault tolerance and preventing data loss if any single node fails. Deletion permissions are enforced through access control, allowing only authorized parties to remove stored data.

This functionality allows the file system to operate as a revocation service. For example, consider a scenario where a professional certification body issues a digital accreditation to a licensed engineer. A hash of the certification document, co-signed by both the certifying authority and the engineer, is submitted to the ledger. Both parties are granted the right to remove the hash if necessary.

To verify the credential, the engineer may present the certification file to an employer or client, who can then check whether the hash remains recorded on the ledger. If the certification is later revoked due to expiration or disciplinary action, the certifying body can delete the hash, indicating the credential is no longer valid. If the engineer attempts to resubmit the hash without the certifier's signature, it will be evident that the entry was not authorized, and thus not a valid representation of the original certification.

Files on the Onyx network are internally represented as Merkle trees, but developers interact with them through a simplified interface. Onyx provides Java classes that abstract the underlying structure, enabling developers to manipulate files as if working within a conventional file system with directories, subdirectories, and files.

Archived copy · cryp2nova.com

Developers can rename directories, modify file contents, and perform operations like moving, copying, and pasting. Behind the scenes, all changes are automatically structured and stored as Merkle trees.

This architecture enables the platform to generate cryptographic proofs that a file is part of the consensus state. Entire directory structures can be stored in this manner.

Additionally, Onyx supports Merkle Directed Acyclic Graphs (DAGs). This allows for deduplication: when two files share identical byte segments, only one copy of the shared data is physically stored, improving storage efficiency.

Files can be accessed in two distinct ways:

> By hash, guaranteeing immutability, since the hash directly reflects the file's contents.

> By File ID, enabling mutability, as the File ID can be redirected by the file's owner to point to a newer version.

This dual-access model means files are both immutable and updatable, depending on how they are accessed. Access by hash ensures permanence, while access by File ID ensures that the latest version is always retrieved.

The Onyx Mesh

The Onyx Mesh provides a powerful, high-performance alternative to traditional smart contracts and on-chain data storage, offering decentralized, trust-based ordering of events.

Through The Onyx Mesh, applications can submit messages to the Onyx public network, where each message is deterministically timestamped and ordered using the Onyx Mesh algorithm. This process ensures fairness, transparency, and cryptographic verifiability while offloading commercial logic and data storage to external systems.

Archived copy · cryp2nova.com

The Onyx Mesh is part of the broader Onyx Network, a public distributed ledger governed by the Onyx DAO composed of XCN holders and built on Onyx. Alongside cryptocurrency, file storage, and smart contracts, The Onyx Mesh serves as a key network service enabling decentralized consensus for various use cases.

Clients submit messages tagged with a thread ID to the Onyx mainnet. These messages, containing data such as bids, logs, or event notifications, are distributed across nodes until consensus is reached. Each message receives a consensus timestamp, sequence number, and is incorporated into a running hash that provides a cryptographic fingerprint of all messages for that thread.

Once consensus is established, the message and metadata are streamed to consensus nodes.

These consensus nodes are read-only and do not participate in consensus. They receive messages from the mainnet, and depending on configuration, can store full transaction records, selected threads, or even all consensus data, offering flexibility in data management.

This decoupled architecture empowers applications to process data off-chain while relying on Onyx for trusted ordering. Developers can build commercial logic into consensus nodes or application servers, using consensus timestamps to drive real-time operations or generate cryptographic proofs of event ordering.

Onyx Mesh architecture defines three roles.

Mainnet Nodes

Reach consensus and assign timestamps to messages.

Consensus Nodes

Propagate, store, and allow querying of consensus messages. They cannot submit transactions or vote.

Commercial Nodes

Maintain local state, execute commercial logic, and manage access to decrypted content.

Archived copy · cryp2nova.com

A commercial application network may subscribe to an Onyx Mesh thread to receive and decrypt encrypted messages. These networks benefit from Onyx's decentralized ordering while maintaining control over sensitive data and execution.

Onyx Mesh is particularly well-suited for use cases where data privacy regulations, such as GDPR, apply. In the Onyx Mesh model, personal data is encrypted before being submitted to the mainnet. The Onyx network stores this encrypted payload briefly (approx. 3 minutes), while consensus nodes may store it longer. Because only commercial application nodes hold the decryption keys, control over data access is preserved.

This architecture ensures that raw personal data is stored only where legally justified, while consensus nodes retain encrypted, immutable records that support compliance through cryptographic proofs. If deletion is required, commercial nodes may delete the data and keys, rendering encrypted records effectively inaccessible while maintaining the integrity of the consensus history.

The Onyx Mesh bridges the gap between public decentralized trust and private enterprise control. It delivers fast, fair, and secure consensus without requiring full on-chain data storage, dramatically reducing operational costs and complexity. Whether used in financial services, healthcare, IoT, or identity management, Onyx Mesh brings auditability, integrity, and efficiency to distributed systems.

As adoption grows, Onyx Mesh stands to become a cornerstone in the evolution of compliant, scalable, and decentralized application infrastructure.

Archived copy · cryp2nova.com

Consensus Network

The Onyx consensus network comprises a set of nodes that replicate the core validation and state-tracking functions of the main Onyx network while excluding the ability to influence consensus or submit transactions. Consensus nodes participate in the network's peer-to-peer communication protocol, receiving all transaction data in real-time, performing signature verification, and computing consensus outcomes. However, they do not create events and, therefore, do not alter the structure of Onyx. As such, consensus nodes possess no voting authority and are unable to submit transactions through the Onyx API, functioning effectively as read-only nodes.

Despite their restricted role in consensus, Consensus Nodes may implement custom APIs to offer enhanced services or tailored data access. The consensus network provides a scalable and efficient mechanism for disseminating ledger state and transaction data to external clients and distributed applications without burdening the throughput of the main network.

This architecture enables decentralized applications (dApps) to operate their own consensus nodes, allowing them to monitor specific events, filter relevant transactions, and respond to network activity in near real-time. For example, a dApp managing smart contracts may deploy a consensus node to listen for contract-specific events, ignore unrelated data, and trigger appropriate application logic in response.

Archived copy · cryp2nova.com

Sharding

The Onyx network will initially operate as a single shard composed of a limited number of nodes.

As the network matures and more nodes join, it will evolve to support multiple shards, each functioning independently to establish consensus. Sharding boosts performance by enabling parallel processing, as each node processes only the transactions relevant to its shard.

Each shard contains a randomly assigned subset of nodes that maintain a consistent shard-specific state, a portion of the full network ledger. These nodes utilize the Onyx consensus algorithm to determine the transaction order within their shard.

Every shard can store accounts and files and execute smart contracts. Transactions that involve only one shard (e.g., transferring XCN within that shard or storing a file) are processed immediately upon reaching consensus.

To support cross-shard activity, the network implements trust-based inter-shard communication.

A transaction that spans multiple shards, such as moving cryptocurrency from an account in shard X to an account in shard Y, triggers the generation of inter-shard messages. Each shard maintains a queue of outbound messages tagged with sequence numbers to ensure ordered processing. Messages are “pushed” by randomly selected nodes from the source shard to nodes in the destination shard, accompanied by cryptographic proof of consensus.

The receiving shard verifies the message, checks its sequence number, and integrates it into its consensus state if valid. Duplicate messages are ignored, and processing occurs strictly in sequence. Once confirmation is received that a message has been processed, the source shard removes it from its outbound queue.

Complex, multi-shard transactions (e.g., one-to-many or many-to-one transfers) may involve atomic operations, such as placing “holds” on balances until all conditions are met. For example, a transaction that transfers coins from two source accounts in different shards to one destination account involves holds being placed on both sources. Only if all holds are successful are balances updated and funds transferred to the destination. If any hold fails, all are released, and no transfer occurs. This guarantees atomicity across shards.

Archived copy · cryp2nova.com

A master shard oversees node assignment, ensuring balanced stake distribution and periodically reallocating nodes to shards. The system ensures no single node controls too much stake within a shard, preserving Byzantine fault tolerance.

Finality is often achieved as quickly as consensus within the initiating shard. For most single-source transactions, this means users can rely on near-instant certainty.

In more complex, multi-shard interactions, finality may take slightly longer due to required inter-shard confirmations, but it remains efficient and secure.

By ensuring every inter-shard message is cryptographically bound to the consensus state of the originating shard, the network preserves asynchronous Byzantine fault tolerance across the entire platform. This architecture allows Onyx to scale horizontally while maintaining security, consistency, and trust.



CRYP2NOVA

Archived copy · cryp2nova.com

Tokenization



Archived copy · cryp2nova.com

Before exploring how Onyx implements tokenization, it’s important to first understand several foundational concepts, including the different types of tokens and the technical parameters that define their behavior.

Fungible Tokens

Fungible tokens such as stablecoins, governance tokens, and other value-pegged assets are inherently interchangeable, with each unit holding equal value, much like the dollars in a bank account. While every dollar might be represented digitally or tracked with different identifiers, each functions identically in practice. These tokens are typically managed through account-based models, where an account reflects a balance of indistinguishable units.

Thanks to their uniformity and simplicity, fungible tokens are ideal for high-throughput use cases such as payments, rewards, and liquidity provisioning.

Non-fungible tokens (NFTs)

Non-fungible tokens (NFTs) are inherently unique, with each token distinguishable by attributes such as a name, serial number, or embedded metadata. This uniqueness makes NFTs individually identifiable and non-interchangeable. Often linked to specific digital or physical assets like digital art, virtual real estate, or proof of ownership.

NFTs are typically implemented using a token-based model, where each token stands alone with a defined owner. Due to their individualized nature, NFTs are best suited for lower throughput use cases that involve high-value or asset-specific interactions, particularly in scenarios where traceability and uniqueness are essential.

Use Cases

The range of token use cases continues to expand rapidly, touching nearly every industry from finance and gaming to supply chains, identity, and governance. This growing diversity has shaped the design of platforms like the Onyx Layer 1, which supports multiple token types tailored to distinct purposes and audiences. At one end of the spectrum are utility tokens, which grant holders access to specific products or services such as cloud computing credits, event tickets, or subscription-based offerings. At the other are security tokens, which represent ownership in real-world assets like company equity, real estate shares, or other financial instruments. These tokens are regulated and must comply with securities laws, as their value is directly tied to the assets they represent.

Archived copy · cryp2nova.com

Another emerging category includes memecoins, which are often created for community-driven engagement, experimentation, or entertainment. While they may lack intrinsic utility or asset backing, memecoins frequently serve as cultural artifacts or social signals within digital communities. Despite their lighthearted origins, some have demonstrated significant economic impact and adoption. Together, these varied token types highlight the flexibility and breadth of tokenization, enabling both practical and expressive use cases across permissioned and public networks.

States

Once a token contract is developed and deployed, it results in the creation of a token that can be transferred between accounts, typically as part of a commercial process or triggered event. Each account's balance and transaction history are captured within the overall state of the token system.

Onyx Layer 1	Onyx Mesh
Token state is maintained on the public ledger by Onyx mainnet nodes.	Token state resides on permissioned network nodes, which stay synchronized using Onyx Mesh messages published to a specific thread.

Token Contracts

A Token Contract is the code that defines a token's roles, rules, and behaviors. It is typically authored by the token issuer and made publicly accessible either by open-sourcing the code or deploying it as a smart contract on a public network. This transparency ensures that the token's behavior is verifiable, eliminating the need to rely on opaque, third-party systems. Onyx approach to Token Contracts varies by deployment model.

Archived copy · cryp2nova.com

Token Contracts

A Token Contract is the code that defines a token's roles, rules, and behaviors. It is typically authored by the token issuer and made publicly accessible either by open-sourcing the code or deploying it as a smart contract on a public network. This transparency ensures that the token's behavior is verifiable, eliminating the need to rely on opaque, third-party systems. Onyx approach to Token Contracts varies by deployment model.

Onyx Layer 1	Onyx Mesh
The token contract is embedded directly within the token's definition parameters.	The token contract is implemented in application logic, executed by permissioned nodes that maintain the network state.

Accounts

Accounts are uniquely identified entities such as public keys or user IDs that hold token balances and can participate in sending or receiving tokens. These accounts may be controlled by individuals, organizations, or automated systems. Depending on the use case, tokens can be used for payments, access to services, or transferring ownership.

Onyx Layer 1	Onyx Mesh
Utilizes Onyx-native accounts managed by the Onyx mainnet.	Relies on custom account identifiers, typically public keys, defined within the permissioned network.

Archived copy · cryp2nova.com

Onyx supports two primary models for tokenization: the Onyx Layer 1 for issuing tokens natively on the Onyx public ledger, and the Onyx Mesh for constructing permissioned networks that synchronize state with publicly verifiable ordering.

These models offer distinct benefits tailored to different deployment scenarios, ranging from public-facing stablecoins and NFTs to private, regulator-compliant asset networks.

Tokenization, the process of converting real-world assets or rights into digital representations on a distributed ledger, is reshaping trillion-dollar industries from finance to supply chains. The primary benefit of tokenization is the creation of more transparent, efficient, and accessible markets.

Assets can be fractionalized, transferred, and settled with unprecedented speed and minimal friction. As use cases for tokenization expand across securities, utility tokens, stablecoins, NFTs, and more, the infrastructure supporting it must offer enterprise-grade performance, compliance features, and low operational cost.

Onyx's dual tokenization architecture addresses these demands through:

Onyx Layer 1 for native tokenization with high throughput and decentralized trust.

Onyx Mesh for customizable, permissioned token networks using Onyx's consensus ordering.

CRYP2NOVA

Archived copy · cryp2nova.com

Onyx Layer 1: Native Tokenization on Onyx

The Onyx Layer 1 allows token issuers to define, issue, and manage tokens directly on Onyx's public mainnet. These tokens inherit key characteristics of the Onyx network: asynchronous Byzantine fault tolerance (aBFT), finality in seconds, and low-cost transaction fees fixed in USD.



Key Features:

High Throughput

Thousands of token transactions per second.

Low and Predictable Costs

Transactions cost less than $0.01.

Public Verifiability

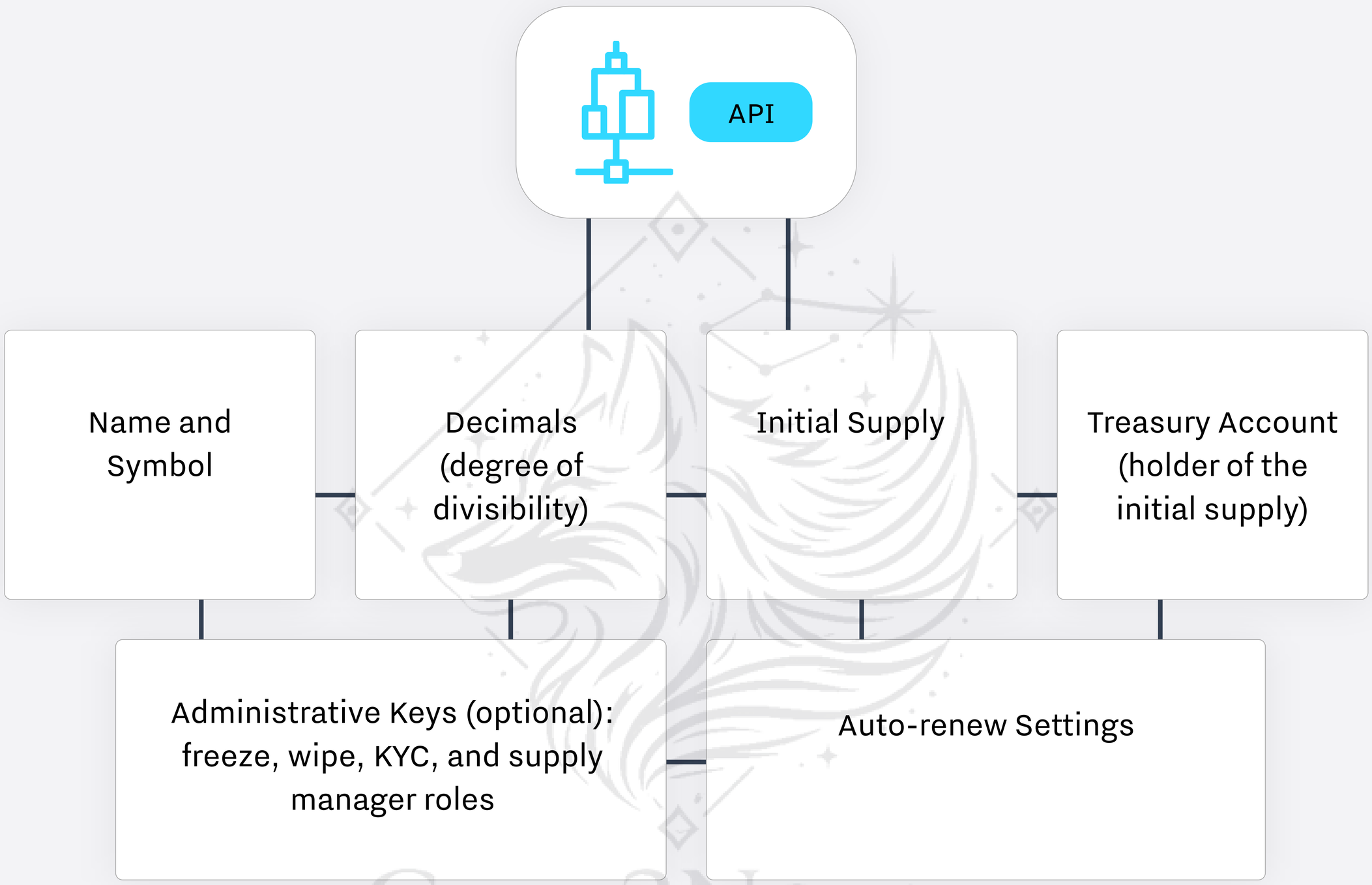
Every transaction is recorded in the ledger and can be audited via consensus nodes.

No Forks

Unlike many blockchain platforms, Onyx's consensus does not fork.

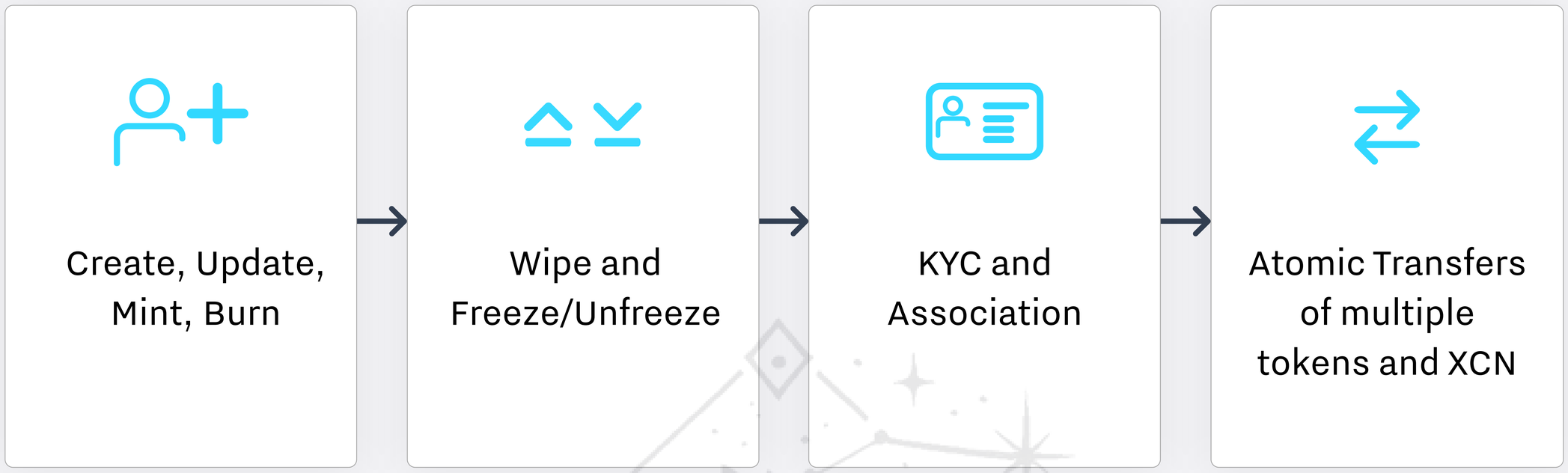
Archived copy · cryp2nova.com

The Onyx Layer 1 provides an API-driven interface that developers use to define token properties. All tokens are issued as native objects on the network.



The Onyx Layer 1 supports a comprehensive set of on-chain operations that enable flexible and secure asset management. Some of the transaction types available to token issuers and holders include lifecycle actions such as creation and updates, supply control through minting and burning, compliance features like KYC and token association, as well as advanced capabilities like atomic transfers involving multiple tokens and XCN in a single transaction.

Archived copy · cryp2nova.com



Consensus nodes track all activity on the Onyx Layer 1, allowing third parties to independently verify token balances, transfer histories, and metadata with full transparency.

These nodes are designed for ease of deployment and provide seamless integration support for external systems such as wallets, custodians, and exchanges. By reflecting the consensus-established state of the Onyx network, consensus nodes offer a decentralized source of truth that enhances auditability and trust.

Additionally, they serve as a critical foundation for interoperability, enabling future cross-network bridges and integration with other distributed ledger technologies (DLTs).

Archived copy · cryp2nova.com

Ease of Deployment

Integration Support with wallets, custodians, and exchanges

Decentralized Trust from the Onyx network's consensus

Interoperability with future bridges and other DLTs

The Onyx Layer 1 API

The Onyx Layer 1 also features the Onyx API which is defined using protocol buffers and serves as the interface for interacting with Onyx network services and functions. Publicly accessible and designed for broad applicability, The Onyx Layer 1 API enables a wide range of commercial and technical use cases.

The Onyx Layer 1 builds on existing network primitives, allowing users to create and interact with tokens as native entities within the Onyx ecosystem. Like other Onyx entities such as accounts, files, smart contracts, and threads, tokens are uniquely identified using the shard.realm.num format. The Onyx Layer 1 introduces a new entity type: the token type entity, which uses this same identifier structure.

Each Onyx account can hold XCN (the native cryptocurrency) alongside multiple custom token types. However, accounts must explicitly opt in to each token type by signing and associating with it before holding or transacting that token. XCN transfers remain independent of token interactions, users can continue to send and receive XCN regardless of the other tokens held by their account.

Archived copy · cryp2nova.com

The Onyx Layer 1 functions inherit Onyx advanced key architecture, supporting flexible configurations including single keys, key lists, threshold keys, and even nested key structures, enabling fine-grained control over token issuance, management, and transfer.

In addition, The Onyx Layer 1 introduces new fields within transaction receipts, records, and state proofs. These responses can be independently captured, verified, and stored by third parties, allowing token operations to inherit Onyx ABFT (Asynchronous Byzantine Fault Tolerance) security model. Token transfer consensus is reached fairly, without the need for a central leader, and transaction finality is achieved within seconds, resulting in an immutable, verifiable log of token activity.

Consensus nodes receive updated record streams and account balance files that include token balances and transfers for Onyx Layer 1 issued tokens.

Onyx Mesh: Tokenization for Permissioned Networks

Onyx Mesh allows applications to submit messages to the Onyx network, which timestamps and orders them using Onyx consensus. The ordered messages can then be consumed by permissioned networks that maintain their own ledger state. This approach is ideal for use cases requiring enhanced control, privacy, or jurisdictional governance such as regulated financial markets or central bank digital currencies (CBDCs).

Architecture Overview:

Clients submit messages (e.g., token transfers) to a specified Onyx Mesh thread	Onyx Mainnet timestamps, orders, and cryptographically verifies these messages	Consensus Nodes relay the message stream to permissioned nodes	Permissioned Nodes apply application logic (the token contract) to update their local state

Archived copy · cryp2nova.com

Token Contract

A token contract defines the core logic of a token, handling minting, burning, role management, and permissions. Unlike the standardized model used in Onyx Layer 1, Onyx Mesh supports fully customizable contracts that can be tailored to meet specific commercial, regulatory, or jurisdictional needs.

These contracts listen to a specific ThreadID on the Onyx Mesh, receiving ordered messages that are validated against the token's rules. Nodes execute the logic to update local state verifying signatures, enforcing restrictions, and managing balances.

Beyond basic operations, contracts can support advanced features like atomic swaps, event triggers, or oracle integration, offering both flexibility and consistency within a permissioned environment.

Token Message Standard

Onyx Mesh tokenization, known as the Token Message Standard, provides a foundational approach for issuing, transferring, and managing digital tokens in a consistent and secure manner across distributed networks. This standard ensures that all token-related messages are well-structured and tamper-proof, enabling seamless synchronization among participating nodes. It not only guarantees message integrity and interoperability, but also unlocks powerful capabilities such as atomic swaps, hold-and-release mechanisms, and automated commercial logic.

These features allow for complex transaction flows, regulatory compliance, and customizable token behaviors, making the Token Message Standard a key enabler for enterprise-grade tokenization and decentralized finance solutions.

The Token Message Standard provides a detailed and flexible framework for defining and enforcing roles and behaviors within a tokenized system. These roles are optional and can be selectively implemented based on the governance, regulatory, or commercial requirements of a specific deployment. The design closely mirrors the capabilities of the Onyx Layer 1 but is extended to support custom implementations, particularly within permissioned environments using the Onyx Mesh. Through this model, token issuers can incorporate fine-grained controls around token creation, distribution, compliance, and lifecycle management, all while maintaining a consistent and interoperable taxonomy across network participants.

Archived copy · cryp2nova.com

At the center of this system is the Administrator role. The Administrator is responsible for initializing the token contract by defining core attributes such as the token's name, symbol, decimal precision, and which roles are enabled for governance. In addition to initial setup, the Administrator has authority to update the token contract, including modifying role assignments, changing governance policies, or rotating keys tied to specific roles. Any such updates require not only the Administrator's signature but also that of the new Keypair Owner, the entity controlling the private key associated with the updated role. This dual-signature requirement ensures deliberate and secure governance transitions. Administrators can also propose and execute changes to other role-based keys (e.g., for the Supply Manager, Compliance Officer, or Enforcement role), further enabling structured yet flexible control over the token's lifecycle.

The Supply Manager role governs the creation (minting) and destruction (burning) of tokens. This role is particularly useful for tokens that require dynamic supply adjustments, such as stablecoins, securities, or programmable financial instruments. Supply Managers can also initiate token transfers, allowing them to manage treasury operations, distribute rewards, or settle internal flows. The token contract can be designed so that minting or burning is only triggered under specific commercial conditions or events, ensuring that the supply logic aligns with the broader operational context of the tokenized asset.

The Compliance role enforces the regulatory requirements of the token network. It provides mechanisms to manage identity verification (KYC), freeze or unfreeze accounts, and remove or reinstate compliance status. These capabilities are essential in environments where Anti-Money Laundering (AML) regulations, sanctions enforcement, or access controls are required. Typically, the Compliance role may be assigned to a trusted third-party provider, such as a financial institution or compliance service, that performs identity verification and monitors for suspicious activity.

The Enforcement role enables more direct intervention in token balances through a process known as clawback. This is executed via a wipe transaction, which irreversibly removes a specified number of tokens from a user's account and simultaneously burns them from the total supply. This function may be used in exceptional situations such as regulatory enforcement actions, fraud recovery, or dispute resolution processes. The ability to revoke tokens directly enhances the network's responsiveness to legal and operational risks.

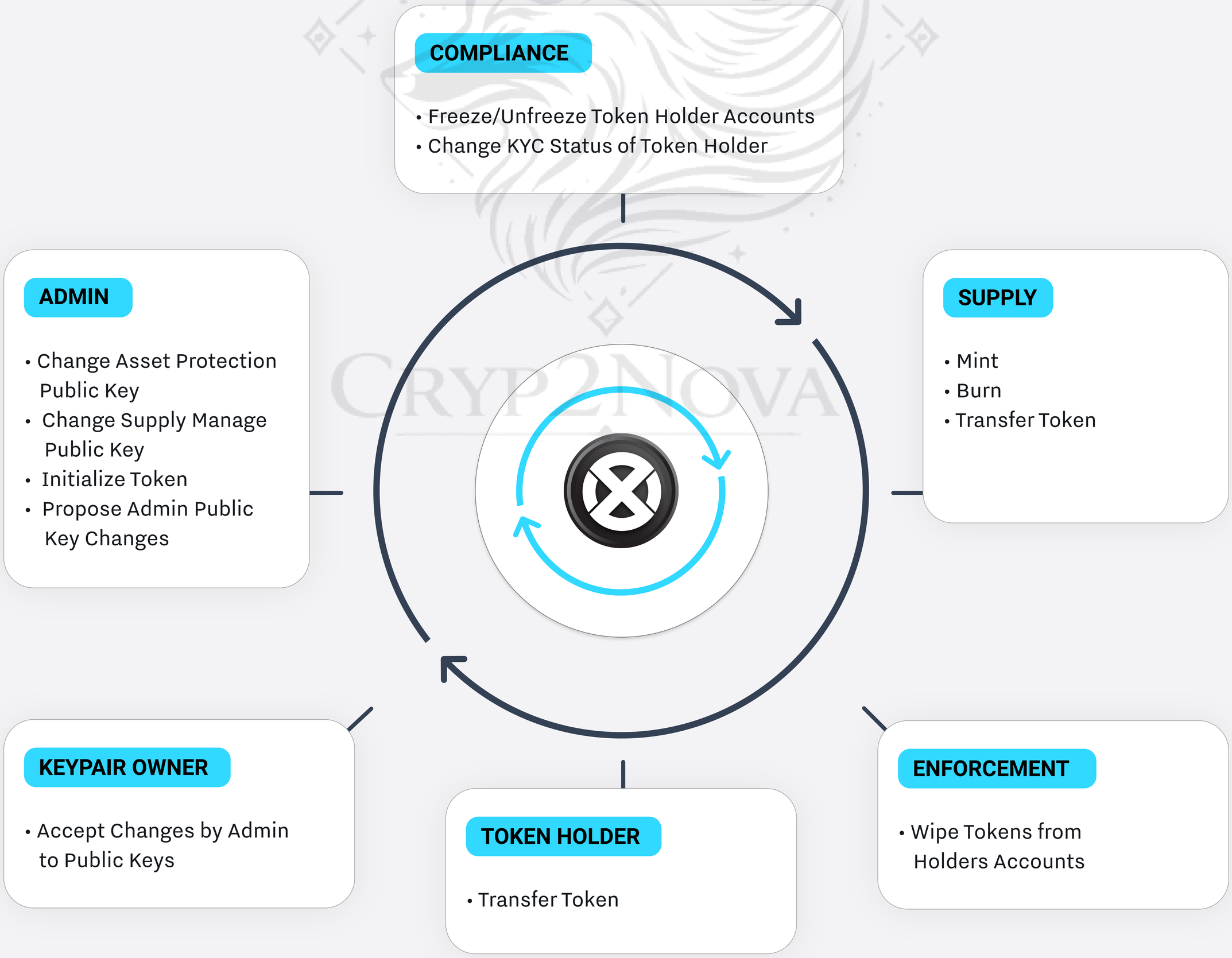
Lastly, the Token Holder is the most common and fundamental role in any token ecosystem. Token Holders are end users or systems that own tokens and can transfer them up to the balance they control. Each Token Holder manages access to their tokens through a cryptographic key pair, enabling decentralized custody and user-level control without intermediaries. This role ensures that participation in the network remains open and permissionless for users, while still being governed by the rules enforced through the token contract.

Archived copy · cryp2nova.com

Altogether, the Token Message Standard offers a powerful and adaptable model for structuring token systems. Its role-based architecture provides enterprises and developers with a comprehensive toolkit for implementing secure, compliant, and commercial-aligned token functionality, whether in public, permissioned, or hybrid network environments. By decoupling token behavior from rigid infrastructure, it allows each role to be flexibly defined, updated, and enforced according to evolving requirements, enabling sustainable token ecosystems with built-in governance.

Customization Possibilities

The platform offers extensive customization options, allowing for jurisdictional constraints, enhanced privacy, and seamless integration with enterprise blockchain frameworks.



Archived copy · cryp2nova.com

Token Node Operation

Token Nodes maintain ledger state, expose APIs for clients, and sync via Onyx Mesh.

Onboarding new nodes involves deploying the token contract and subscribing to the relevant thread. Nodes can reconstruct state from historical Onyx Mesh messages via consensus nodes. This has several benefits.



Full Control	Privacy	Scalability	Governance Flexibility
Define bespoke token behavior without mainnet constraints	Sensitive data can be encrypted and handled only by trusted nodes	High throughput with decentralized ordering	Determine who can join and maintain the network

Onyx offers a powerful dual approach to tokenization through its two core services: Onyx Layer 1 and Onyx Mesh.

Onyx Layer 1 provides the simplicity, speed, and transparency of public network deployment, ideal for issuing stablecoins, loyalty points, and governance tokens that users can easily access via Onyx wallets or integrated applications. In contrast, Onyx Mesh delivers the flexibility, privacy, and custom governance required for complex enterprise use cases such as private marketplaces, regulated financial networks, and supply chain consortia, offering full control over token logic, onboarding, compliance, and data residency.

Both models are underpinned by the same core strengths: fast finality, aBFT security, and predictable pricing. Whether launching consumer-facing assets or building sovereign-grade token economies, Onyx provides the trusted infrastructure to do so with performance and flexibility.

Archived copy · cryp2nova.com

Security



CRYP2NOVA

Archived copy · cryp2nova.com

Cryptography

All communications within the Onyx network are secured using TLS 1.2, and all transactions are authenticated through digital signatures. The Onyx data structure itself is formed using cryptographic hashes.

All cryptographic algorithms and key lengths implemented in the Onyx platform conform to the Commercial National Security Algorithm (CNSA) Suite, the standard mandated for securing U.S. government Top Secret information. These algorithms include RSA 3072 for digital signatures, AES-256 for encryption, ECDSA/ECDH with the P-384 curve, and SHA-384 for hashing in addition to using ephemeral keys for ensuring perfect forward secrecy.

Asynchronous Byzantine Fault Tolerance (aBFT)

The Onyx algorithm provides asynchronous Byzantine Fault Tolerance (aBFT), ensuring that no individual node or colluding subset of nodes can prevent the network from reaching consensus or alter it after finalization.

Each Onyx node deterministically arrives at a point of certainty, recognizing that consensus has been definitively achieved across the network. In contrast, blockchain systems lack formal Byzantine agreement guarantees; consensus is probabilistic and subject to reversal. Additionally, blockchain protocols are not inherently resilient to network partitions, isolated subsets of miners may independently extend conflicting chains, resulting in forks and inconsistencies in transaction ordering.

It is important to clarify that the term Byzantine Fault Tolerant (BFT) is occasionally applied in a weakened form to describe limited resistance to adversarial behavior in some consensus protocols. In contrast, Onyx adheres to the original, stronger definition of BFT: even under conditions where (1) a subset of malicious actors colludes to disrupt or distort consensus, and (2) adversaries exert partial control over the network infrastructure, such as delaying or obstructing message delivery, the system will still reach consensus, and all nodes will eventually have certainty that consensus has been achieved.

Archived copy · cryp2nova.com

Onyx satisfies this robust definition of Byzantine Fault Tolerance. Provided that malicious entities control less than one-third of the total staked XCN, they cannot halt consensus, manipulate transaction ordering, or bias consensus timestamps.

Byzantine Fault Tolerance (BFT) encompasses varying degrees of robustness, determined by the underlying assumptions about network behavior and message transmission. Weaker forms of BFT assume synchronous or partially synchronous networks with bounded message delays, while stronger forms, such as asynchronous BFT, make no timing assumptions and tolerate arbitrary delays in message delivery. The strength of a BFT protocol is directly correlated with its ability to maintain consensus in increasingly adversarial or unpredictable network conditions.

The strongest form of Byzantine Fault Tolerance is asynchronous BFT, which ensures that consensus can be reached even if adversaries have the capability to delay or selectively suppress message transmission across the network. This model assumes only that more than two-thirds of nodes behave honestly and that, over time, messages repeatedly sent between nodes will eventually be delivered. Unlike partially asynchronous systems which rely on assumptions such as fixed maximum message delays (e.g., ten seconds), asynchronous BFT remains secure even under unpredictable network conditions. Partially asynchronous protocols may fail under real-world threats such as botnets, Distributed Denial of Service (DDoS) attacks, or malicious firewalls, as these can invalidate the timing assumptions critical to their correctness.

ACID Compliance

Onyx is ACID compliant when employed as the consensus layer for a distributed database.

ACID, Atomicity, Consistency, Isolation, Durability, defines a set of properties required for reliable transaction processing.

Onyx enables a network of nodes to reach final consensus on the chronological order of transactions. Once consensus is achieved, each node applies the transactions to its local database instance in the same deterministic order. If the local databases conform to ACID principles, the network as a whole functions as a unified, ACID-compliant distributed system.

In contrast, blockchain platforms lack definitive finality; because consensus is probabilistic and reversible, they cannot guarantee ACID compliance.

Archived copy · cryp2nova.com

Distributed Denial-of-Service Attack Resilience

One form of Denial-of-Service (DoS) attack involves an adversary overwhelming an honest network node with superfluous or malicious messages, impairing its ability to process legitimate traffic and fulfill its protocol responsibilities.

A Distributed Denial-of-Service (DDoS) attack escalates this threat by leveraging a large number of compromised devices or public services to amplify the volume and reach of the attack, making it significantly more difficult to mitigate and potentially disruptive to network-wide operations.

In a distributed ledger network, a Distributed Denial-of-Service (DDoS) attack may target the nodes responsible for participating in the consensus process. By overwhelming these critical nodes with excessive traffic, an adversary could impair their functionality or isolate them from the network, thereby disrupting or delaying the establishment of consensus and compromising the reliability and availability of the ledger.

Onyx is inherently resilient to Distributed Denial-of-Service (DDoS) attacks due to its fully decentralized consensus architecture, in which no single node or subset of nodes holds privileged roles or responsibilities in establishing consensus.

Similar to Bitcoin in its distributed structure, Onyx allows the network to remain operational even if individual nodes are targeted and temporarily disconnected. For an adversary to meaningfully disrupt the system, a large fraction of the network would need to be simultaneously affected, which is significantly more complex and resource-intensive.

By contrast, alternative consensus models that rely on designated leaders, coordinators, or round-robin schemes introduce structural vulnerabilities. In such systems, targeting the current leader with a DDoS attack, and switching to each successive leader as they are elected can effectively halt network progress while attacking only one node at a time.

Onyx circumvents this limitation by eliminating the need for leadership roles altogether, thereby maintaining consensus integrity without incurring the energy costs associated with proof-of-work mechanisms.

Archived copy · cryp2nova.com

Economics



Archived copy · cryp2nova.com

Users incur fees when utilizing the Onyx platform for operations such as cryptocurrency transfers, data storage, or submitting transactions to the network.

Due to Onyx's high-throughput architecture and the absence of proof-of-work, these fees are expected to be significantly lower than those on many existing public distributed ledger platforms.

Nodes participating in the Onyx network are compensated for the computational, bandwidth, and storage resources they expend in supporting consensus and delivering network services. The platform categorizes fees and payments into several distinct categories, each corresponding to different aspects of network activity and resource consumption.

Node Fee

When a user or application initiates an action on the Onyx platform, it transmits the corresponding transaction to a single node, which is responsible for submitting that transaction to the network. This submission process incurs a small computational and energy cost for the node. To compensate for this effort, Node Fees are paid. These fees serve both to reimburse resource consumption and to incentivize nodes to perform this essential network function.

Initially, the Onyx DAO will set standardized Node Fee rates; however, over time, fee determination will be delegated to individual nodes, allowing them to set their rates based on market dynamics or service offerings. Node Fees are paid directly by the end user to the account of the submitting node, providing a direct economic relationship between users and infrastructure providers.

Network Fee

Once a transaction is submitted to the network, it is disseminated to participating nodes, which first validate digital signatures and then temporarily store the transaction in memory while the network reaches consensus.

Users pay a Network Fee to compensate nodes for the computational, memory, and communication resources required to process and finalize the transaction within the consensus protocol.

Archived copy · cryp2nova.com

The resource cost and thus the Network Fee may vary depending on factors such as the size of the transaction payload and the number of associated digital signatures. Users pay Network Fees into an Onyx Treasury account, from which a portion of the collected fees is distributed daily to participating nodes as Node Reward Payments, reflecting their contribution to consensus operations.

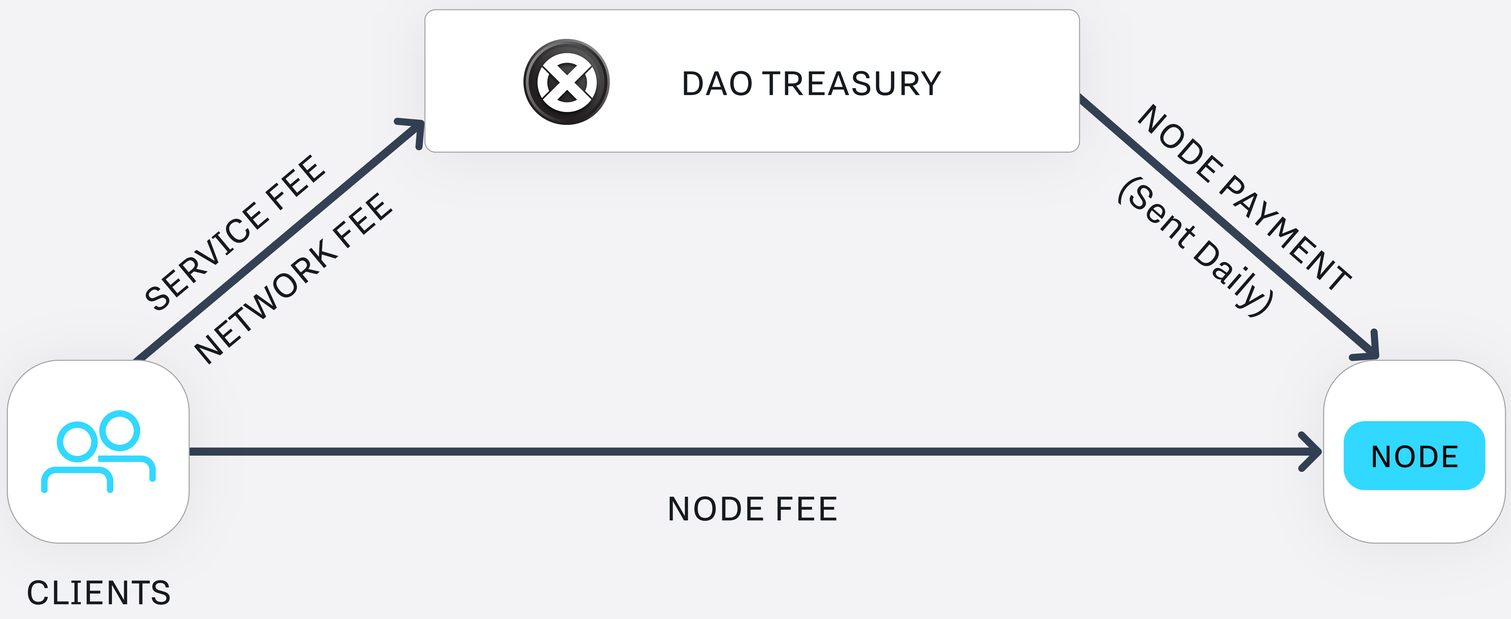
Service Fee

Service Fees are designed to compensate nodes for the ongoing resource commitments required to maintain or support the outcomes of a transaction. For example, in the case of a file storage transaction, all nodes are responsible for storing the file on persistent storage for a defined duration. The Service Fee for such a transaction is calculated based on the file size and the length of the storage period.

For transactions involving smart contract execution, the Service Fee reflects the computational effort required to execute the contract and any additional storage costs associated with persisting its results on the network. Users pay Service Fees into the Onyx Treasury account.

As with Network Fees, a portion of the collected Service Fees is redistributed daily to participating nodes as Node Reward Payments based on their contribution to fulfilling service-related responsibilities.

Onyx collects Service Fees and Transaction Fees on behalf of the nodes that execute transactions and deliver associated services. These fees are aggregated into the Onyx Treasury and are subsequently used to fund incentive payments to participating nodes. This ensures that nodes are compensated proportionally for their contributions to consensus, computation, storage, and other operational responsibilities across the network.



Archived copy · cryp2nova.com

Node Reward Payment

Once per day, incentive payments are distributed from the Onyx Treasury account to participating nodes to compensate and incentivize their continued operation. To qualify for payment, a node must meet availability thresholds established by the Onyx DAO, for example, by contributing at least one event to 90% or more of the consensus rounds during the preceding 24-hour period.

Payments are proportional to the total amount of XCN staked to the node, including both the node's own stake and any proxy-staked XCN assigned to it by other account holders. The fee and reward model is intentionally structured to align economic incentives, ensuring that costs, participation requirements, and risks are distributed fairly among network participants.

The most significant resource expenses on the Onyx network such as file storage or smart contract execution are covered by service fees, which must be paid upfront. For instance, if a client wants to store a file for 30 days, they must prepay the full storage cost at the time the file is created.

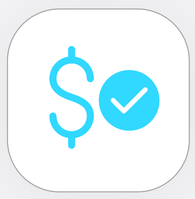
The smaller resource costs, including propagating transactions and reaching consensus, are covered by network fees. When a node receives a transaction from a client, it first checks if the account has enough funds to cover the fees. However, there is a minor risk: the account balance might drop before the transaction is finalized, resulting in some network effort going uncompensated.

To manage this, the system uses a transaction fee parameter set by the client, indicating the maximum amount they are willing to pay. The receiving node conducts a precheck using a published fee schedule that multiplies expected resource usage (e.g., bandwidth, CPU, storage) by defined coefficients to estimate the actual fee. If the client's balance and max fee are sufficient, the transaction proceeds.

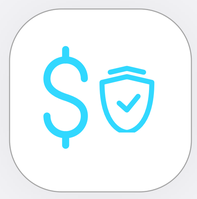
Once submitted, all nodes process the transaction, apply it to the consensus state if payment is confirmed, and distribute the applicable fees accordingly.



Nodes only compensated for processing transactions correctly.



Clients only pay for delivered services.



No services are performed without payment, avoiding risk.

Archived copy · cryp2nova.com

Tokenomics



Archived copy · cryp2nova.com

The XCN tokenomics model is designed to provide long-term economic sustainability, balancing supply, utility, and incentives within the Onyx ecosystem. The distribution and allocation of XCN ensure a structured approach to network growth, governance participation, and staking rewards.

XCN was issued with a fixed total supply at genesis, ensuring a predictable economic model without the risk of unexpected inflation. The supply is carefully managed through governance decisions, staking incentives, and controlled emissions. The total supply is structured to support network incentives while maintaining scarcity over time. The current structure of the XCN token is itemized below:

Max Supply	Predefined at initial deployment to ensure the amount does not exceed 68,892,071,757 units based on the prior conversions.
Total Supply	The current total supply of XCN stands at approximately 48.4B which has been reduced from the initial max supply.
Circulating Supply	The amount of XCN in units currently in the market which is approximately 33.5B. This number dynamically adjusts based on staking participation, token burns, and emissions.
Burn Mechanism	Implemented through transaction fees and governance-approved mechanisms to maintain a total supply deflationary model.
Emission Control	Governance-driven mechanisms regulate token distribution to staking participants and ecosystem contributors. The emission of XCN is regulated by on-chain and off-chain mechanics to ensure a predictable distribution rate until total supply is reached.
Bridged Supply Management	XCN exists natively on Ethereum but can be bridged to base via Superbridge and BSC via Wormhole. These bridged XCN tokens require onchain validation of the equivalent issued amount to be locked to maintain transparency and to ensure conformance to the total supply of XCN.

Archived copy · cryp2nova.com

A portion of XCN total supply is allocated to the Onyx Treasury, managed by the Onyx DAO. These funds are used to support protocol development, grants, liquidity incentives, and strategic partnerships. The Treasury's allocation is governed by on-chain voting, ensuring decentralized oversight of fund utilization. Treasury-controlled funds may be deployed in:

Ecosystem Grants

Supporting developers, research initiatives, and infrastructure improvements.

Liquidity Incentives

Providing rewards to liquidity providers across DeFi protocols integrated with Onyx.

Protocol Upgrades

Funding technical improvements and security audits.

Strategic Partnerships

Engaging with institutional and DeFi partners to drive adoption.

Tokenomics parameters, including staking rewards, treasury allocations, and token burns, are fully controlled by the Onyx DAO. The governance model ensures that token supply mechanics evolve based on the needs of the network and economic conditions, balancing incentive distribution with long-term sustainability. By maintaining a structured and governance-driven tokenomics model, XCN ensures a sustainable economic framework for network participants while aligning incentives for validators, stakers, and ecosystem contributors.

Archived copy · cryp2nova.com

Governance



Archived copy · cryp2nova.com

Onyx is governed as a DAO using the XCN ERC-20 token on Ethereum where holders can participate in decisions relating to the protocol. Onyx expands governance further by using XCN for governance of its network.

A governance model for a public distributed ledger must define the rules governing the evolution of node software, the issuance and allocation of native tokens, and the incentive structures for network participants. It must also account for and balance the interests of diverse stakeholders, including node operators, developers, enterprises, end-users, and regulatory authorities.

Onyx utilizing XCN for governance means that each XCN holder holds equal voting rights with the number of tokens that they hold determining their vote weight in the governance process. This structure is designed to promote diversity of thought, operational transparency, and institutional trustworthiness with a deliberate emphasis on decentralization, accountability, and long-term sustainability.

To reinforce transparency and operational oversight, Onyx Improvement Proposals (OIP) are used to ratify major changes to the overall Onyx DAO and Onyx as a network.

XCN serving as the governance token of the Onyx DAO means enabling decentralized, on-chain governance where token holders can propose, vote on, and execute protocol changes. The governance framework is implemented via smart contracts, ensuring a secure, transparent, and permissionless decision-making process. All governance operations, including proposal creation, voting, and execution, are automated and enforced by the governance contract deployed on Ethereum.

The Onyx DAO utilizes a structured on-chain governance mechanism, where governance weight is determined by the amount of XCN staked. The governance contract enforces the following workflow:



Archived copy · cryp2nova.com

1. Proposal Creation

- Any address holding at least 100,000,000 XCN in governance weight can submit proposals.
- Proposals can include protocol upgrades, economic parameter adjustments, treasury allocations, and smart contract modifications.
- The proposal payload must define the target contract address, function calls, execution parameters, and rationale.
- Proposals are initiated using the `propose()` function in the governance contract.

2. Voting Process

- Once submitted, proposals enter a 3-day voting period.
- Staked XCN determines voting power, meaning votes are weighted based on the amount of XCN committed to the governance contract.
- Participants cast votes using the `castVote()` function, which records votes onchain and tallies results in real time.
- The voting options are For, Against, or Abstain.

3. Quorum and Approval

- A proposal is considered successful if it meets the approval threshold of at least 200,000,000 XCN votes in favor.
- If the quorum is met and a majority vote is achieved, the proposal moves to the execution phase.

Archived copy · cryp2nova.com

4. Timelock Execution

- Approved proposals enter a 2-day timelock, enforced by the governance contract to allow for final review.
- After the timelock expires, the `execute()` function is called, finalizing the proposal and enacting changes to the protocol.
- The timelock contract prevents immediate governance takeovers, ensuring a secure and deliberate execution process.

The Onyx DAO governance logic is fully on-chain, defined by the governance smart contract deployed on Ethereum. Key contract functions include:

```
// Function to create a new proposal
targets, values, signatures, calldatas, description
function propose(

      Address[] memory targets,
      uint256[] memory values,
      string[] memory signatures,
      bytes[] memory calldatas,
) external returns (uint256);

// Function to cast a vote
Function castVote(uint256 proporsalId, uint8 support) external;

// Function to queue an approved proposal
Function queue(uint256 proporsalId) external;

// Function to execute an after timelock
Function execute(uint256 proporsalId) external;
```


Archived copy · cryp2nova.com

These functions collectively enable decentralized governance, ensuring that proposals follow a structured workflow from initiation to execution. The Onyx DAO is responsible for making critical protocol decisions, including but not limited to:

Protocol Upgrades	Economic Policies	Security Enhancements
Implementing improvements to Onyx, optimizing performance, and enhancing security throughout the ecosystem.	Adjusting staking parameters, transaction fees, and node incentives.	Modifying node rules, consensus policies, and other configurations.

By participating in on-chain voting, staking XCN for governance weight, and submitting proposals, token holders actively contribute to the evolution and security of the Onyx ecosystem.

Open Consensus

Onyx's consensus protocol is distinct from its governance structure. Initially, all consensus nodes will be operated by the Onyx DAO to ensure consistency and security during early network deployment. Over time, node participation will expand to include external operators, who will be compensated for maintaining the Onyx network.

The open consensus model supports scalability and decentralization, with a long-term objective of enabling a globally distributed network of potentially millions of nodes. Consensus influence is determined by stake-weighted voting, wherein each node's voting power is proportional to its holdings of Onyx's native cryptocurrency, XCN. This mechanism mitigates the risk of collusion, protects against attacks such as double-spending or unauthorized ledger modification, and ensures that no small set of actors can control transaction ordering.

The open consensus model of Onyx is designed to enhance trust, transparency, and resilience. It provides the institutional accountability necessary for global adoption, while creating an inclusive and decentralized technical infrastructure that everyone can participate in.

Archived copy · cryp2nova.com

Keeping Onyx Fair



Archived copy · cryp2nova.com

Onyx provides fairness in consensus by eliminating centralized control over transaction ordering and timestamp assignment. No node, including those participating in consensus, holds privileged authority to determine when or in what order transactions are accepted. Instead, all consensus decisions are made collectively through voting, embedded within the Onyx algorithm. This decentralized structure supports three key dimensions of fairness:

Fair Access

Onyx is architected to provide inherently equitable transaction submission, ensuring that all participants have a fair opportunity to interact with the network without bias or obstruction. Unlike systems where centralized intermediaries or privileged nodes can influence message flow, Onyx's decentralized communication protocol prevents any single node from censoring or unduly delaying the transmission of a transaction. Even in the presence of a malicious actor attempting to suppress or stall dissemination, the protocol's randomized peer-to-peer structure ensures that the transaction rapidly finds alternate paths through the network.

This design preserves liveness, enhances robustness, and offers strong resistance to localized disruptions or targeted interference, safeguarding the open and inclusive nature of the platform.

Fair Timestamps

Each transaction is assigned a consensus timestamp based on the median of the times reported by nodes upon first receiving it. This timestamp is determined collectively, rather than unilaterally, making it resistant to manipulation. Assuming more than two-thirds of participating nodes are honest and operate with reasonably synchronized clocks, the resulting timestamp is both accurate and Byzantine fault tolerant. This property is particularly relevant in contexts requiring verifiable time-bound execution, such as regulatory deadlines or contractual obligations.

Fair Transaction Order

The final ordering of transactions is derived from their fair consensus timestamps. Because timestamp assignment itself is fair and tamper-resistant, the resulting transaction order preserves this fairness.

This is essential in applications such as financial markets, where transaction ordering can impact market outcomes. Unlike blockchain systems where a miner can arbitrarily prioritize, reorder, or exclude transactions within a block, Onyx ensures that ordering reflects network-wide agreement, not individual discretion. Competitive advantage is limited to factors such as network latency, rather than access to privileged consensus roles.

Archived copy · cryp2nova.com

Enterprise Features



Archived copy · cryp2nova.com

Onyx is designed with enterprise-grade capabilities at its core, offering a feature set tailored to meet the complex requirements of regulated industries and large-scale organizations. From compliance-enabling tools like controlled mutability and opt-in identity verification to robust governance, privacy management, and real-time auditability through consensus nodes, Onyx provides the infrastructure necessary for businesses to operate confidently in demanding regulatory environments. These features position Onyx as a robust foundation for enterprises seeking secure, compliant, and scalable distributed applications.

Regulatory Compliance

It is anticipated that governments will continue to impose regulatory and policy requirements on users, enterprises, and developers operating on public ledgers and engaging with associated cryptocurrencies and tokens. A core objective of the Onyx network is to provide the technical capabilities and governance structures necessary to support compliance with applicable legal and regulatory frameworks, including established regimes such as the European Union's General Data Protection Regulation (GDPR) and anti-money laundering (AML) standards.

Onyx is committed to ensuring the platform remains adaptable to evolving legal requirements.

Self-Custody

As with most distributed ledger technologies, all transactions that modify the state of an Onyx account must be authorized by a digital signature generated using the account's private key. This ensures that end users who maintain control of their private keys retain exclusive authority over their accounts and assets. At no point does Onyx, or any associated developer or enterprise, assume custody of user funds.

Cryptocurrency transfers on the Onyx network are executed in a fully peer-to-peer manner, with no intermediaries required to hold or transfer XCN on behalf of users. Developers have the flexibility to implement self-custody solutions, enabling users to manage their own private keys, or to offer custodial services, in which case they must adhere to all relevant regulatory requirements associated with the management of user assets.

Archived copy · cryp2nova.com

Data Self Sovereignty

Unlike most distributed ledger platforms, Onyx supports controlled mutability, enabling data modification or deletion under predefined conditions. When data is submitted to the network, the publisher may specify an authorization policy that designates which cryptographic keys are permitted to modify or remove the data in the future.

This feature allows developers to design applications that comply with regulatory requirements such as the “right to erasure” under the European Union’s General Data Protection Regulation (GDPR). It also enables users to retain granular control over the visibility and persistence of their data, supporting flexible data governance within a decentralized framework.

Privacy Management

The Onyx network provides a flexible identity management framework that allows users to maintain control over their identity and transaction requirements.

By default, accounts are pseudonymous, consistent with most distributed ledger systems. However, the Onyx architecture supports future implementations that enable users to bind verified identity attributes issued by a trusted Certificate Authority to their ledger accounts. This capability facilitates compliance with Know Your Customer (KYC) and other regulatory requirements. Counterparties may condition transaction acceptance on receiving proof of specific identity attributes (e.g., legal name, age, or jurisdiction) in accordance with their compliance obligations. Users retain full control over their personal information, deciding whether to disclose identity proofs or attributes on a per-transaction basis.

The system operates on an opt-in model. Users must explicitly choose to associate their real-world identity with their account. Those who elect not to participate will retain pseudonymity, though doing so may restrict access to regulated services or counterparties that require verified identity for transaction acceptance.

Archived copy · cryp2nova.com

Government oversight

Security

Individual privacy

Comparable to presenting a verified employee ID when accessing a secure facility, Onyx model enables users to attach a hash of a digital certificate created by a recognized identity provider to their account. This attachment takes the form of a transaction sent to the network.

This transaction:

1. May require authorization from both the user’s private key and the identity provider’s key

2. Can define which entities are permitted to subsequently access or verify the certificate

As long as the binding between an account and its associated certificate remains active i.e., not revoked by either the user or the identity provider, it can serve as verifiable evidence that the account is linked to a known individual whenever funds are transferred into or out of that account.

If necessary, the identity provider may revoke this binding by submitting a signed transaction to the network.

Archived copy · cryp2nova.com

For illustrative purposes, consider a user attempting to transfer funds from their Onyx account to a U.S. bank. The user would supply the bank with the digital certificate and their account address. The bank would verify that the account contains the corresponding hash of the certificate and confirm that the certificate was issued by a recognized and trusted identity authority. Only upon successful validation of these elements would the bank authorize the transaction and accept the funds.

In accordance with regulatory obligations, the bank may be required to report the certificate and transaction details to the appropriate government authority, either in real time (e.g., for high-value transfers) or according to a predetermined reporting schedule.

Anti Money-Laundering

Certain developers and enterprises operating on the Onyx network may be subject to anti-money laundering (AML) reporting obligations. For these entities, a compliance framework can be constructed using on-network identity certificates in conjunction with network data accessed via consensus nodes. Consensus nodes are designed to function as read-only observers of network activity and, in the long term, may be operated by any participant. These nodes enable the collection, storage, and analysis of public transaction data, facilitating investigations and the identification of potentially suspicious behavior.

Onyx is committed to working with the broader distributed ledger technology community and regulatory bodies to ensure that compliance obligations can be met without compromising privacy or security.

The Onyx consensus algorithm and data structure deliver a uniquely strong combination of throughput and fault tolerance. Through the Onyx platform and Onyx DAO, the network offers transparency, open innovation, long-term stability, opt-in identity and compliance mechanisms, and governance informed by cross-industry, globally distributed expertise.

Archived copy · cryp2nova.com

Creating Trust



Archived copy · cryp2nova.com

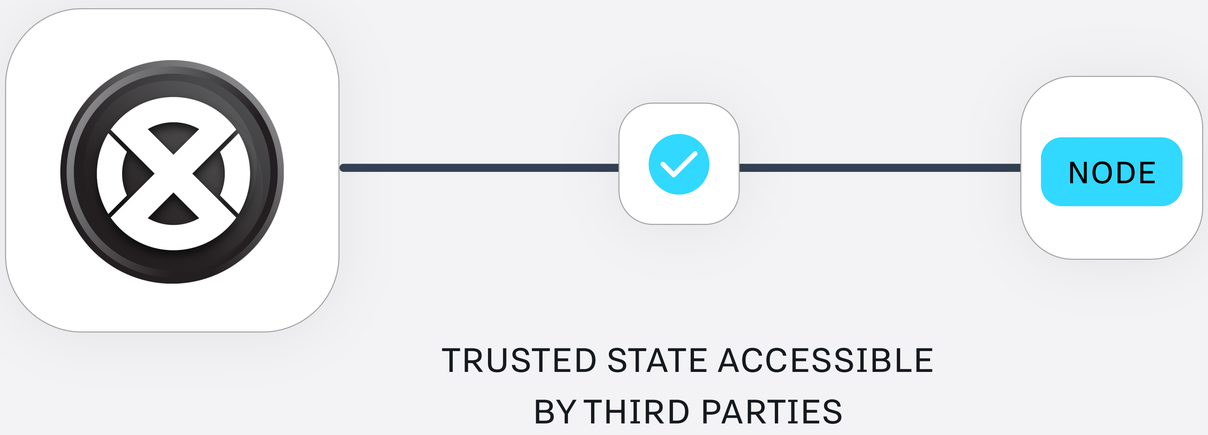
Signed State Proofs

All nodes in the Onyx network maintain a complete and synchronized copy of the current ledger state, for example, the balances of all cryptocurrency accounts. At the conclusion of each round of consensus, every node independently computes the updated state by processing all transactions finalized during that round and all preceding rounds. Each node then generates a cryptographic hash of the resulting state, signs it digitally, embeds the signature in a transaction, and disseminates it to other nodes. Nodes subsequently aggregate these signatures to establish collective validation of the shared state.

When a client queries any component of the state, nodes can construct and return a compact proof file containing the aggregated signatures and accompanying cryptographic artifacts. This allows the client, or any third party, to verify that the returned data corresponds to the consensus state recognized by the entire network.

The state itself is structured as a Merkle tree, enabling efficient and verifiable proofs. A third party can be provided with a Merkle proof consisting of a minimal subset of state data, the Merkle path to the root (including sibling hashes), the set of digital signatures over the root hash, and the historical address book necessary to verify public keys. This cryptographic construct allows the verifier to confirm that the state fragment is authentic and consistent with the globally agreed-upon network state.

CRYP2NOVA



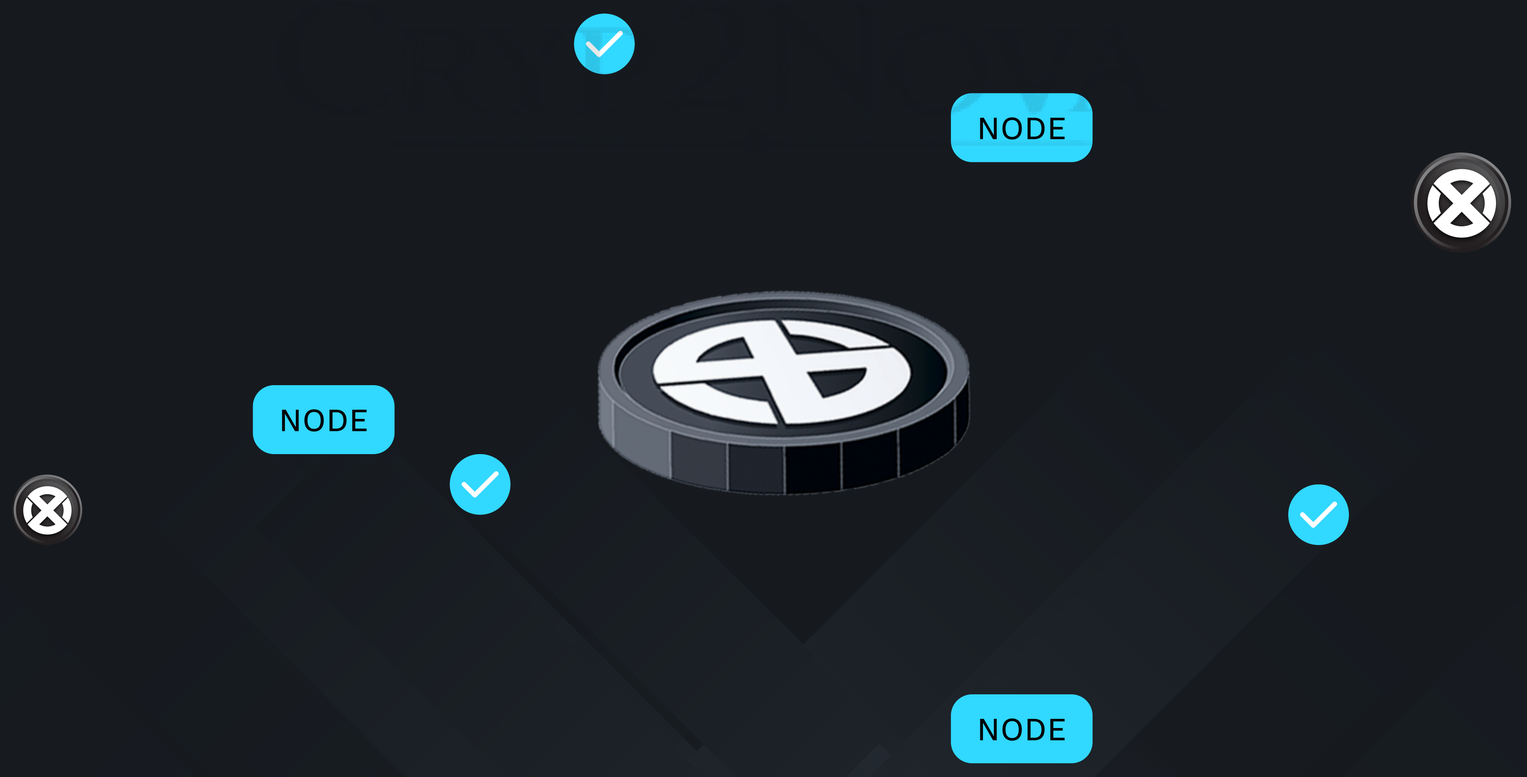
Archived copy · cryp2nova.com

Ledger ID

The cryptographic proof provided by an Onyx node will include an address book, which contains the public keys of all participating nodes along with their associated stake. This address book is essential for any third party to verify the digital signatures affixed to the state or subset of the state returned by a node.

To ensure verifiability over time, the proof also incorporates an address book history, a sequential chain of address books, where each version is digitally signed by nodes from the immediately preceding address book. The validity of each address book in the sequence is contingent on being signed by a supermajority (more than two-thirds) of the total stake, as recorded in the prior address book. This recursive signature structure forms an unbroken chain of trust that extends back to the genesis address book, which was signed by the initial cohort of nodes at the ledger's inception.

The hash of the genesis address book serves a critical function: it acts as a cryptographic anchor and globally unique identifier for the ledger. It defines the origin and identity of the network and is used to establish continuity and authenticity across the entire address book history. This mechanism ensures that clients and third parties can verify not only the current state, but also the historical legitimacy of the network's consensus framework.



Archived copy · cryp2nova.com

Handling Forks

If a small subset of nodes attempts to fork the Onyx network by creating a new ledger based on the current state, they may be able to replicate the data and initiate a technically valid fork.

However, they will be unable to reproduce the address book history that links back to the genesis address book, as the majority of nodes, those not participating in the fork, will not sign the subsequent address books of the forked network. This means the forked ledger must generate a new genesis address book, and thus a new unique identifier, effectively establishing it as a distinct and unrelated network. As a result, the fork cannot masquerade as the original ledger.

When a client submits a transaction to the Onyx network, the node responds with a cryptographic proof demonstrating that the transaction was incorporated into the consensus state. In the case of value transfers, both sender and recipient receive verifiable confirmation that the transaction succeeded. This proof includes a signed chain of state hashes extending back to the genesis address book, thereby validating not only the transaction’s correctness but also its association with the authentic ledger.

In the event of a hypothetical 50/50 network split by stake, neither resulting group would be able to generate a continuous, signed address book history to the original genesis. Rather than a fork, this would constitute a full network deconstruction, yielding two entirely new and independent ledgers. This would destroy continuity, invalidate the original currency, and severely reduce the value of the network, as neither group could claim legitimacy or retain access to the original client base. The resulting loss of transaction fees and market trust provides a powerful economic disincentive against forking.

Thus, Onyx’s technical architecture and cryptographic mechanisms make it practically impossible to create a deceptive or ambiguous fork. Illegitimate copies cannot produce valid state proofs and will be immediately identifiable as such.

Users can unambiguously verify that they are interacting with the authoritative ledger. Moreover, these same mechanisms are essential for enabling secure sharding, allowing different shards to exchange authenticated messages, each with proof that the message originates from the consensus of its source shard. This ensures consistency and trust across a multi-shard ecosystem.

Archived copy · cryp2nova.com

Potential Use Cases



Archived copy · cryp2nova.com

Onyx is a powerful consensus infrastructure designed to bring transparency, fairness, and tamper resistance to digital systems across industries. By providing cryptographic timestamping, deterministic ordering, and decentralized verification through consensus nodes, Onyx enables a wide range of high-integrity applications, from finance and legal records to healthcare, governance, and supply chain management. Its ability to integrate seamlessly with existing systems while offering provable audit trails and regulatory compliance positions it as a foundational layer for trust in both public and private digital ecosystems.

Underpinning all these capabilities is a design focused on privacy, data governance, and regulatory compliance. Onyx's Consensus Service maintains data immutability by anchoring encrypted records to decentralized consensus nodes, while ensuring that sensitive personal data remains securely within commercially-controlled environments.

This architecture allows organizations to comply with right-to-erasure mandates by deleting associated encryption keys without compromising auditability. Data residency is preserved, giving enterprises full control over where decrypted data is stored and who can access it.

Importantly, Onyx nodes, including consensus nodes, never access unencrypted personal information. This makes Onyx uniquely suited for GDPR-aligned deployments and enterprise-grade privacy requirements, enabling decentralized trust without sacrificing localized data control.

The following sections explore how Onyx empowers specific use cases across key domains.

Cross-Border Payment Infrastructure

Onyx makes it possible to achieve low-cost, high-speed international remittances and settlement across banks, remittance platforms, and mobile wallets. Its deterministic finality and consensus timestamps make it possible to provide cryptographic proof of transaction time and ordering, supporting regulatory audits and reconciliation.

By enabling high throughput for mass transfers, leveraging asynchronous Byzantine Fault Tolerance (aBFT) for tamper resistance and finality, and offering fair timestamps for compliance and fee settlement, Onyx opens the door to a more efficient and transparent global financial ecosystem.

Archived copy · cryp2nova.com

Government and Public Records Systems

Onyx makes it possible to store hashes of official records such as land titles, birth certificates, commercial registrations, and judicial rulings for long-term, tamper-proof verification. It enables public verifiability without exposing the underlying data, ensuring transparency while preserving privacy.

With support for provable deletion, Onyx also makes it possible to comply with right-to-erasure regulations. Through permissioned integration using its Consensus Service, it allows for jurisdictional control, making it a strong fit for government and institutional use cases that demand both security and regulatory alignment.

Decentralized Stock Markets

Participants can submit bids and asks to Onyx Mesh, gaining a new level of fairness through precise, timestamp-based sequencing. This ensures that every order is recorded and processed in the exact order it was received, eliminating front-running and manipulation.

Consensus nodes then organize and process these orders by thread, enabling order-matching logic to follow a transparent, verifiable, and tamper-resistant sequence of events, laying the groundwork for more trustworthy and efficient marketplaces.

Decentralized Voting and Governance Auditing

Onyx can be used to record votes and proposals for DAOs, public elections, corporate governance, or university boards, ensuring both the integrity of vote ordering and the privacy of participants. Its fair ordering mechanism guarantees that votes are counted in the exact sequence they’re received, eliminating disputes around timing and manipulation. Transparent consensus nodes offer real-time auditability, allowing stakeholders to independently verify the process.

Additionally, Onyx supports advanced features like proxy delegation and identity-verification mechanisms, making it a versatile foundation for secure and accountable decision-making across a wide range of governance models.

Archived copy · cryp2nova.com

Decentralized Identity

Onyx Mesh enhances decentralized identity frameworks by providing trusted, tamper-resistant timestamps for identity-related artifacts. While the actual identity data remains securely stored within commercial-controlled systems, Onyx ensures that the ordering and verification of these events is handled through a decentralized and transparent layer.

This separation of concerns allows organizations to maintain control over sensitive data while benefiting from the trust, auditability, and integrity that Onyx's consensus layer brings to identity ecosystems.

Trade Finance and Invoice Factoring

Onyx can be used to timestamp and verify critical trade documents such as invoices, bills of lading, and letters of credit, helping reduce fraud, accelerate early payments, and enable automated settlements through smart contracts.

Its Consensus Service provides tamper-proof sequencing, ensuring that every document is recorded in an immutable, verifiable order. Provenance trails created through this process offer powerful tools for risk mitigation and compliance, while consensus nodes support seamless cross-organization integration, allowing multiple stakeholders to share a trusted, real-time view of trade workflows.

Consent Receipts and Provable Deletion

Businesses can leverage Onyx Mesh to record consent grants and withdrawals, creating a verifiable, timestamped history of data processing agreements. This ensures that consent management is not only transparent but also provably compliant with regulatory requirements.

In scenarios requiring provable deletion, key steps in the data removal process can be logged to Onyx Mesh, establishing an auditable, tamper-resistant timeline. This approach strengthens accountability and trust in data governance by providing clear evidence of when and how data-related actions were taken.

Archived copy · cryp2nova.com

Credentialing and Education Verification

Universities, training platforms, and certification bodies can use Onyx to timestamp, verify, and, when necessary, revoke digital credentials, ensuring long-term trust and authenticity.

Onyx supports optional revocation and deletion, allowing institutions to manage credentials flexibly while maintaining compliance. Its privacy-preserving design enables proof-of-existence without revealing sensitive information, protecting learners' identities. Backed by Merkle tree–based storage, Onyx offers scalable, efficient verification, making it ideal for large volumes of credentials across diverse education and training ecosystems.

Escrow and Dispute Resolution

Onyx can be used to deploy escrow smart contracts with built-in transparency, where audit trails are clear and conditions are enforced by consensus-based ordering. Timestamps provide a reliable mechanism to resolve disputes, ensuring clarity around who acted first in any transaction.

Onyx's fair ordering eliminates the risk of timestamp manipulation, while deterministic state proofs enable trusted third-party arbitration when needed. With secure contract logic written in Solidity and backed by Onyx's Consensus Service, parties can engage in escrow arrangements with confidence, knowing that every action is verifiable and tamper-resistant.

Fair Play in Online Gaming

Onyx ensures tamper-proof logging of in-game events, player rankings, and match outcomes, helping to prevent cheating and manipulation in esports and play-to-earn ecosystems. Its consensus-based timestamps guarantee fair and transparent sequencing, so every action is recorded exactly as it occurred.

With high throughput, Onyx can support real-time gaming environments, while its secure off-chain storage combined with verifiable ordering ensures that performance and integrity go hand in hand. This creates a trusted foundation for competitive and reward-driven digital gameplay.

Archived copy · cryp2nova.com

Healthcare Data Audit Trails

Onyx can be used to track consent, access logs, and critical events within Electronic Health Records (EHR) systems, ensuring transparency and accountability without compromising sensitive patient data. By logging events with precise timestamps, Onyx supports compliance with HIPAA, GDPR, and other regulatory frameworks, offering a clear audit trail for every interaction.

Sensitive data remains under the control of commercial systems, while Onyx's decentralized consensus nodes provide external, immutable verification. This separation of data control and auditability creates a powerful foundation for secure, privacy-preserving healthcare data management.

IoT and Supply Chains

Onyx Mesh can timestamp sensor readings and asset handoffs across global supply chains, creating a trusted and tamper-resistant record of events. This verifiable timeline supports compliance with regulatory standards, enhances provenance tracking for quality assurance and sustainability claims, and enables automation through smart contracts that react to real-world conditions.

By anchoring key supply chain events in a decentralized, transparent layer, Onyx brings new levels of trust, traceability, and efficiency to even the most complex logistics networks.

Real-Time ESG and Carbon Credit Tracking

Onyx can be used to timestamp, order, and publicly audit environmental actions such as carbon offset events or broader ESG-related disclosures. By anchoring these actions to a transparent yet secure proof layer, Onyx enables trusted accountability without compromising sensitive data.

It supports verification by multiple stakeholders, allowing regulators, NGOs, and investors to independently confirm the timing and authenticity of reported activities. With tamper-resistant audit trails, Onyx helps build confidence in ESG commitments and fosters greater transparency across sustainability-focused initiatives.

Archived copy · cryp2nova.com

Financial Systems and Token Transfers

Onyx Mesh supports secure and transparent ordering for tokenized assets, making it ideal for maintaining integrity across complex digital asset ecosystems. For example, Onyx can be used to record token transfers with fair sequencing, ensuring that transactions are processed in the exact order they occur.

This decentralized ordering layer preserves cross-network consensus integrity and prevents manipulation. Additionally, atomic swaps between different ledgers can be reliably triggered based on Onyx-assigned timestamps, enabling seamless, trustless interoperability across blockchain platforms.

Legal Document Provenance and Smart Contracts

Onyx could be used to timestamp legal agreements, contracts, and notarized documents, creating decentralized evidence chains that support court admissibility and long-term legal integrity. Its immutable sequence logs ensure that every action whether signing, amendment, or revocation, is recorded in a verifiable, tamper-proof order.

Onyx also supports provable deletion, allowing expired or voided contracts to be clearly marked while maintaining an auditable history. With built-in support for digital signatures and identity linkage via consensus, Onyx offers a secure, transparent foundation for managing legally binding records in a decentralized world.

CRYP2NOVA

Archived copy · cryp2nova.com

Final Notes



Archived copy · cryp2nova.com

To support adoption and integration of the Onyx protocol, a full suite of developer resources will be published in coordination with the network's official launch. These resources will include:

Precise API specifications for interacting with Onyx Layer 1 and Onyx Mesh, including message formats, transaction types, and endpoint definitions.

Reference implementations and contract templates for token issuance, transfer logic, and access control models.

Supported SDK libraries and language bindings for common development environments.

Integration guides and architecture patterns for building application-layer services on top of Onyx.

Formal interface definitions for clients, indexers, and relay services interacting with Onyx nodes and subnets.

All technical documentation will be hosted on a modular, versioned documentation portal that supports live updates, code snippets, and version tracking to ensure alignment with protocol upgrades and implementation milestones.

This documentation is designed to meet the requirements of both independent developers and enterprise engineering teams seeking to integrate Onyx-based infrastructure. Its release schedule will align with the final testnet evaluations and production readiness milestones.

Archived copy · cryp2nova.com



Cryp2Nova

Archived copy · cryp2nova.com