SEALCOIN

Powering the Machine Economy

WHITEPAPER

A Peer-to-Peer Protocol for Real-Time Machine-to-Machine Transactions

Jonathan LLamas, November 20, 2024

Version updated on June 9, 2026

CRYP2NOVA

info@sealcoin.ai

Archived copy · cryp2nova.com

Table of Content

Table of Content *2*

1. Executive Overview *6*

1.1 Vision: Infrastructure for the Autonomous Machine Economy 6

1.2 From Connected Devices to Autonomous Economic Agents 7

1.3 Hardware-Anchored Trust for Machine Transactions 8

1.4 The Role of QAIT in Machine-to-Machine Settlement 8

1.5 Overview of SEALCOIN Vertical Marketplaces 9

2. Problem Statement *11*

2.1 Fragmentation of the IoT Ecosystem 11

2.2 Lack of Trusted Device Identity 12

2.3 Limitations of Current Machine Payment Systems 13

2.4 Data Authenticity Challenges in Machine-Generated Data 13

2.5 Infrastructure Demand for Artificial Intelligence and Distributed Compute 14

2.6 Regulatory and Compliance Challenges in Machine Transactions 15

3. SEALCOIN Protocol Architecture *17*

3.1 Overview of the SEALCOIN Network 18

3.2 Device Identity Architecture 19

3.3 Root of Trust and Secure Device Environments 19

3.4 Device Authentication and Certificate Framework 20

3.5 Secure Transaction Layer 21

3.6 Service Discovery and Device Interaction 21

3.7 Compliance Supervision Framework 22

4. Key Technologies *23*

4.1 Distributed Ledger Infrastructure 23

4.2 Cryptographic Foundations 24

4.3 Secure Elements and Trusted Execution Environments 25

4.4 Hardware Root of Trust and Post-Quantum Readiness 25

Archived copy · cryp2nova.com

4.5 Device Public Key Infrastructure (PKI)....26

4.6 Smart Contracts and Autonomous Transactions....27

4.7 Machine Identity and Data Integrity....27

5. Machine Economies and Vertical Marketplaces....29

5.1 Concept of SEALCOIN Vertical Marketplaces....29

5.2 Marketplace Architecture Model....30

5.3 Machine-to-Machine Transaction Flow....32

5.4 SEALCOIN Space Communication Marketplace....33

5.4.1 Purpose and Scope....33

5.4.2 Transactional Logic....34

5.4.3 QAIT Configuration in Space Context....34

5.5 SEALCOIN Energy and Electric Mobility Marketplace....34

5.5.1 Purpose and Scope....34

5.5.2 Device-Level Energy Autonomy....35

5.5.3 Regulatory and Grid Integration....35

5.5.4 QAIT Configuration in Energy and Mobility Context....35

5.6 SEALCOIN Distributed Compute Marketplace....36

5.6.1 Purpose and Scope....36

5.6.2 Compute Transaction Model....36

5.6.3 QAIT Configuration in Distributed Compute Context....36

5.7 SEALCOIN Premium Data Marketplace....37

5.7.1 Purpose and Scope....37

5.7.2 Data Transaction Model....37

5.7.3 QAIT Configuration in Data Context....37

5.8 Cross-Marketplace Interoperability and Strategic Positioning....38

6. QAIT Token and Economic Layer....39

6.1 Role of QAIT in the SEALCOIN Ecosystem....39

6.2 Utility Principles of the QAIT Token....40

6.3 Fiat-Referenced Pricing and QAIT Settlement....41

6.4 Proof-of-Security (PoSy) Framework....41

6.5 Machine Prevalidation and Secure Onboarding....42

6.6 PoSy Pools and Device Networks....43

6.7 Transaction-Based Incentive Mechanism....43

6.8 Security Enforcement and Penalty Mechanisms....44

Archived copy · cryp2nova.com

6.9 Smart-Contract Governed Pools....44
6.10 Token Holder Participation and Ecosystem Alignment....45
6.11 Economic Integration Across Vertical Marketplaces....45
7. Governance and Ecosystem Structure....*46*
7.1 Structural Overview of the Ecosystem....46
7.2 SEALCOIN AG: Infrastructure and Technology Provider....47
7.3 QAIT Association: Token Issuer and Crypto-Economic Governance....48
7.4 Activities and Non-Activities of Ecosystem Entities....49
7.5 Regulatory Positioning....50
8. Compliance Framework....*51*
8.1 Identity Verification and Participant Onboarding....51
8.2 Anti–Money Laundering (AML) and Risk Monitoring....52
8.3 Transaction Traceability and Transparency....52
8.4 Compliance Supervision within the Ecosystem....53
8.5 Compliance in Autonomous Machine Economies....53
9 SEALCOIN Protocol Core Development Team....*55*
10. Ecosystem Participants....*60*
10.1 Device Manufacturers....60
10.2 Infrastructure Operators....61
10.3 Autonomous AI Agents....61
10.4 Enterprises and Service Providers....62
10.5 Developers and Technology Integrators....62
10.6 Device Owners and Individual Participants....63
10.7 Collaborative Ecosystem Dynamics....63
11. Development Roadmap....*64*
11.1 SEALCOIN Platform....65
11.2 Wallet and Deposit Workflow....66
11.3 Platform Dashboard and Operational Visibility....67
11.4 Device Registry and Device Lifecycle Management....68
11.5 Certificate Management....68

Archived copy · cryp2nova.com

11.6 Proof-of-Security Pool Participation **69**

11.7 Marketplace Interface **70**

11.8 Future Platform Evolution **71**

12. QAIT Token Generation and Distribution ***72***

12.1 Token Generation Event **72**

12.2 Token Allocation **73**

12.3 Allocation Breakdown **74**

12.4 Emission and Vesting Structure **76**

13. Ecosystem Partnerships ***78***

13.1 WISeKey **78**

13.2 WISeSat.Space **78**

13.3 SEALSQ **79**

13.4 Hedera Hashgraph LLC **80**

13.5 The Hashgraph Group **80**

14. Conclusion ***81***

15. Appendices ***83***

15.1 Glossary **83**

15.2 Legal Disclaimer **90**

CRYP2NOVA

Archived copy · cryp2nova.com

1. Executive Overview

1.1 Vision: Infrastructure for the Autonomous Machine Economy

Digital infrastructure is undergoing a fundamental transformation driven by the convergence of connected devices, distributed computing, artificial intelligence, and decentralized economic coordination. Billions of machines already interact with the physical world, generating data, executing operations, and supporting industrial processes across sectors including energy, transportation, manufacturing, and space infrastructure. Despite their growing presence, these machines remain largely dependent on centralized platforms and human supervision to exchange services, validate data, and settle economic transactions.

SEALCOIN protocol introduces a new foundational infrastructure designed to enable a secure and decentralized machine economy. Within this architecture, devices and artificial intelligence agents can operate as autonomous economic actors capable of discovering services, negotiating value, executing transactions, and settling payments without requiring direct human coordination.

The SEALCOIN protocol combines hardware-anchored device identity, decentralized transaction infrastructure, programmable smart contracts, and token-based settlement to create a trusted environment for machine-to-machine interactions. This infrastructure allows devices to securely authenticate themselves, establish verifiable trust relationships, and participate in economic exchanges across multiple industry domains.

SEALCOIN therefore provides a hardware-anchored, post-quantum-ready infrastructure enabling authenticated machines and AI agents to discover services, negotiate value, and settle transactions autonomously. By introducing cryptographic identity and programmable economic logic at the device level, the platform enables machines to become participants in digital marketplaces rather than passive endpoints in centralized networks.

The long-term objective of the SEALCOIN ecosystem is to support the emergence of a global machine economy in which infrastructure systems, industrial equipment, consumer devices, and artificial intelligence agents can interact within secure and interoperable economic environments.

Archived copy · cryp2nova.com

1.2 From Connected Devices to Autonomous Economic Agents

The first generation of connected devices primarily focused on remote monitoring and centralized data collection. Devices such as sensors, industrial controllers, and connected appliances transmitted information to centralized cloud platforms where analysis and operational decisions were performed. While this architecture improved operational visibility, it did not fundamentally change the economic role of machines.

In contrast, the next generation of connected infrastructure requires devices to perform more complex functions. Modern systems increasingly require devices to coordinate directly with each other, exchange services, and allocate resources dynamically. Energy systems must balance distributed generation and consumption. Mobility infrastructure must coordinate charging, routing, and resource allocation. Satellite networks must dynamically allocate bandwidth and relay capacity. Artificial intelligence systems require access to distributed data and compute resources.

These emerging scenarios require machines to possess three fundamental capabilities that traditional IoT architectures do not provide:

First, devices must possess a secure and verifiable digital identity. Without cryptographic identity anchored in secure hardware or protected environments, machines cannot establish trust relationships with other devices or systems.

Second, machines must be able to negotiate and execute service transactions autonomously. This requires programmable transaction infrastructure capable of encoding service agreements, validating execution conditions, and enforcing economic settlement.

Third, devices require an economic mechanism allowing them to exchange value without relying on traditional payment systems designed for human actors.

SEALCOIN protocol addresses these requirements by providing a unified infrastructure enabling machines to authenticate themselves, interact through programmable service agreements, and settle transactions using a token-based economic layer.

Archived copy · cryp2nova.com

1.3 Hardware-Anchored Trust for Machine Transactions

Trust is the fundamental prerequisite for autonomous machine interaction. Without strong guarantees regarding the authenticity of devices and the integrity of their cryptographic identities, decentralized machine economies cannot operate securely.

The SEALCOIN protocol architecture therefore establishes trust beginning at the device level. Participating devices anchor their cryptographic identities within protected execution environments designed to prevent unauthorized access to private keys. These environments may include secure elements, trusted execution environments, embedded security modules, or secure microcontrollers integrated during device manufacturing.

By protecting cryptographic keys within tamper-resistant environments, SEALCOIN protocol ensures that device identities cannot be forged, duplicated, or manipulated through software attacks. This hardware-rooted trust model provides the foundation for verifiable device authentication across the ecosystem.

In addition to protecting cryptographic identities, the SEALCOIN protocol architecture anticipates future developments in cryptography. As advances in quantum computing may eventually weaken certain classical cryptographic algorithms, the protocol is designed to support hardware and software environments capable of adopting post-quantum cryptographic schemes as they mature.

The combination of hardware-anchored identity, strong cryptographic protocols, and future-ready security architecture establishes a robust trust framework enabling machines to interact autonomously in open economic environments.

1.4 The Role of QAIT in Machine-to-Machine Settlement

Autonomous service interactions between machines require an economic settlement mechanism capable of supporting high-frequency transactions, automated execution, and global interoperability. Traditional financial systems are not optimized for this type of interaction, particularly when transactions involve very small values and occur between devices rather than human users.

Archived copy · cryp2nova.com

The SEALCOIN protocol therefore introduces the QAIT token as the settlement mechanism for machine-to-machine transactions within the network. QAIT enables automated payment execution through smart contracts, allowing devices to settle services immediately after verifying execution conditions.

To support predictable service pricing where needed, transactions within the SEALCOIN network and its marketplaces can be priced using fiat currency references, while settlement is performed in QAIT. In such cases, devices or service providers may define the economic value of a service in a stable reference unit, and the corresponding QAIT amount can be determined dynamically at the time of execution through an external price conversion mechanism.

This approach separates the economic value of services from the volatility often associated with digital assets. Service providers and consumers can rely on predictable pricing while still benefiting from the efficiency and programmability of token-based settlement.

The QAIT token therefore functions as both a utility and payment instrument within the ecosystem. It enables access to network services, supports transaction settlement, and provides incentive mechanisms encouraging participation in the infrastructure.

1.5 Overview of SEALCOIN Vertical Marketplaces

While the SEALCOIN infrastructure provides the technical foundation for autonomous machine interaction, economic activity within the network is organized through sector-specific marketplaces referred to as Vertical Marketplaces.

Each marketplace represents an economic environment in which devices operating within a particular industry can discover services, negotiate transactions, and exchange value according to the operational logic of that sector.

The first generation of SEALCOIN marketplaces focuses on four strategic domains where machine-to-machine economic coordination can generate significant efficiency gains.

The Space Communication Marketplace enables satellites, ground stations, and connected infrastructure to exchange communication services such as bandwidth allocation, relay capacity, and data transmission.

Archived copy · cryp2nova.com

The Energy and Electric Mobility Marketplace supports autonomous energy transactions between distributed energy assets such as solar panels, batteries, smart meters, electric vehicles, and charging infrastructure.

The Distributed Compute Marketplace enables computing devices such as laptops, workstations, and edge compute nodes to contribute processing capacity to distributed workloads including artificial intelligence inference and scientific computing.

The Premium Data Marketplace allows authenticated machine-generated data to be exchanged as verifiable digital assets, enabling secure data markets across industrial, environmental, and infrastructure applications.

Together, these marketplaces demonstrate how the SEALCOIN infrastructure can support multiple interconnected machine economies operating across different sectors.

CRYP2NOVA

Archived copy · cryp2nova.com

2. Problem Statement

The rapid expansion of connected devices, industrial automation, artificial intelligence systems, and distributed digital infrastructure is transforming the way physical and digital systems interact. Billions of machines now operate across energy networks, transportation systems, industrial production lines, environmental monitoring infrastructures, and global communication networks. These machines continuously generate data, execute automated operations, and increasingly perform tasks that were historically managed by human operators.

Despite this technological progress, the current digital infrastructure supporting connected devices remains largely fragmented and insufficient to support autonomous machine economies. Existing systems were designed primarily for centralized data collection and remote device control rather than for decentralized service exchange between machines. As a result, machines cannot easily authenticate each other, exchange services, negotiate economic value, or settle transactions autonomously.

The absence of a unified infrastructure for secure machine interaction limits the potential of connected devices and artificial intelligence systems. To enable a global machine economy, devices must be capable of operating within a trusted environment where identity, service discovery, transaction execution, and economic settlement are handled programmatically and securely.

The SEALCOIN protocol addresses these challenges by providing a framework in which machines can securely authenticate themselves, discover services, execute transactions, and settle value autonomously across sector-specific marketplaces.

2.1 Fragmentation of the IoT Ecosystem

The current Internet of Things landscape is characterized by a high degree of fragmentation. Device manufacturers, software vendors, and platform providers have developed proprietary systems that operate in isolated technological environments. Devices deployed within one ecosystem often cannot interact with devices from another ecosystem without complex integrations or centralized intermediary platforms.

Archived copy · cryp2nova.com

This fragmentation creates barriers to interoperability, increases infrastructure complexity, and prevents devices from participating in open economic environments. Instead of interacting directly with each other, most devices rely on centralized cloud platforms to mediate communications, manage data flows, and coordinate operations.

Such centralized architectures introduce several limitations. They create dependency on single infrastructure providers, increase operational costs, and restrict the ability of devices to interact dynamically with other systems outside their immediate platform environment. Furthermore, centralized platforms limit innovation by controlling the rules under which devices can access services or exchange information.

The SEALCOIN protocol addresses this fragmentation by introducing a decentralized framework in which devices can authenticate themselves, interact securely, and exchange services across open marketplaces without relying on proprietary platforms.

2.2 Lack of Trusted Device Identity

A fundamental requirement for autonomous machine interaction is the ability for devices to verify each other's identities. Without a secure and verifiable identity framework, machines cannot establish trust relationships or safely exchange services and data.

Many connected devices today operate without strong identity protection. Device credentials are often stored in software environments that are vulnerable to manipulation or extraction. In some cases, devices share common credentials across large fleets, increasing the risk of impersonation and unauthorized access.

This lack of robust identity management creates significant vulnerabilities. Malicious actors can impersonate devices, inject falsified data into networks, or execute unauthorized operations within critical infrastructure systems. These vulnerabilities are particularly concerning in sectors such as energy networks, transportation infrastructure, industrial automation, and satellite communication systems.

The SEALCOIN infrastructure addresses this challenge by introducing a cryptographically secure device identity architecture anchored in protected execution environments. Through hardware-based or secure-environment key protection and certificate-based

Archived copy · cryp2nova.com

authentication, the SEALCOIN protocol enables machines to verify the authenticity of their counterparties before engaging in service transactions.

This identity framework forms the foundation for trusted machine-to-machine interaction across the SEALCOIN network.

2.3 Limitations of Current Machine Payment Systems

Autonomous machine economies require an economic settlement mechanism that allows devices to exchange value programmatically and at scale. However, traditional financial systems are not designed for automated transactions between machines.

Conventional payment infrastructures typically involve multiple intermediaries, manual verification procedures, and settlement processes that operate on timeframes unsuitable for machine-to-machine interactions. Transaction costs and operational complexity further limit their applicability for high-frequency or low-value transactions.

In machine economies, transactions may occur continuously as devices allocate resources, consume services, or exchange data. Examples include energy devices negotiating electricity flows, computing devices sharing processing capacity, or satellites providing communication services. These interactions require a settlement mechanism capable of supporting automated execution, global interoperability, and programmable transaction logic.

The SEALCOIN protocol addresses these limitations by integrating a token-based settlement layer designed specifically for machine-to-machine transactions. Within the SEALCOIN network infrastructure, devices can execute smart contracts that automate service validation and economic settlement, allowing machines to exchange value without reliance on traditional payment rails.

2.4 Data Authenticity Challenges in Machine-Generated Data

Machine-generated data is becoming an increasingly valuable resource for industries such as environmental monitoring, logistics optimization, scientific research, and artificial

Archived copy · cryp2nova.com

intelligence training. However, the reliability of this data often depends on the ability to verify its origin and integrity.

Many data collection systems lack mechanisms that ensure the authenticity of information generated by devices. Data may be transmitted through multiple intermediaries before reaching its destination, creating opportunities for manipulation or loss of provenance. Without cryptographic verification of the originating device, it becomes difficult to determine whether a dataset can be trusted.

These limitations reduce the economic value of machine-generated data. Organizations that rely on data for decision-making or machine learning applications must invest additional resources to validate and verify data sources.

The SEALCOIN Agent addresses this challenge by enabling devices to cryptographically sign data at the point of generation. By binding device identity to cryptographic signatures anchored in secure key environments, the SEALCOIN protocol enables data consumers to verify the authenticity and provenance of machine-generated information.

This capability establishes the foundation for secure data marketplaces in which authenticated machine data can be exchanged with confidence.

2.5 Infrastructure Demand for Artificial Intelligence and Distributed Compute

The rapid advancement of artificial intelligence technologies has significantly increased the demand for computing resources. Training large-scale models and executing inference workloads require substantial processing capacity across CPUs, GPUs, and specialized hardware accelerators.

At the same time, a large portion of global computing infrastructure remains underutilized. Personal computers, workstations, and edge devices often possess idle processing capacity that could contribute to distributed workloads if appropriate coordination mechanisms were available.

Existing distributed computing solutions have attempted to leverage this unused capacity, but they often rely on centralized coordination systems and lack robust economic incentives

Archived copy · cryp2nova.com

for device owners. In addition, many systems do not provide secure identity verification for participating devices, which limits trust in the computational results they produce.

The SEALCOIN protocol addresses these limitations by enabling authenticated computing devices to participate in distributed compute marketplaces. Within this environment, devices can contribute processing capacity to computational workloads while receiving automated compensation through programmable transaction settlement.

This approach creates a decentralized compute economy in which secure device identity, service discovery, and token-based settlement enable distributed computing resources to be allocated efficiently across global networks.

2.6 Regulatory and Compliance Challenges in Machine Transactions

As machines begin to execute economic transactions autonomously, regulatory and compliance considerations become increasingly important. Financial transactions, digital asset issuance, and value exchange mechanisms must operate within regulatory frameworks addressing anti-money laundering requirements, identity verification procedures, and transaction monitoring obligations.

The emergence of machine economies introduces new challenges for regulatory compliance. Transactions may occur automatically between devices operating in different jurisdictions, and economic interactions may involve large numbers of small transactions executed in rapid succession.

To ensure that machine economies can operate within appropriate legal frameworks, infrastructure providers must integrate compliance mechanisms directly into their network architecture. Identity verification processes, transaction monitoring systems, and governance structures must be designed to support regulatory oversight without compromising the efficiency of automated interactions.

The SEALCOIN infrastructure incorporates compliance supervision mechanisms designed to support regulatory alignment while enabling decentralized machine interaction. Through the integration of identity frameworks, transaction monitoring capabilities, and governance structures involving dedicated ecosystem entities, the SEALCOIN protocol supports the

Archived copy · cryp2nova.com

development of machine economies that can operate within established regulatory environments.

By addressing the technological, economic, and regulatory challenges outlined in this section, the SEALCOIN protocol provides the foundation for secure and scalable machine-to-machine economic systems.

Archived copy · cryp2nova.com

3. SEALCOIN Protocol Architecture

The SEALCOIN protocol provides the foundational architecture enabling machines, physical devices, and autonomous AI agents to interact within decentralized economic environments. As connected infrastructure expands across industries such as energy, mobility, communications, and computing, machines increasingly require the ability to authenticate themselves, discover services, negotiate economic terms, and execute transactions autonomously.

Traditional digital infrastructures were not designed to support such interactions between machines. Most connected devices today operate within centralized ecosystems where authentication, service coordination, and economic settlement are mediated by centralized platforms. These architectures limit interoperability and prevent devices from participating in open economic environments.

The SEALCOIN protocol introduces a decentralized architecture designed to overcome these limitations. By combining secure device identity, programmable economic logic, and standardized communication frameworks, the protocol enables machines to function as autonomous participants in digital marketplaces.

The architecture of the SEALCOIN protocol is organized around three fundamental components:

The SEALCOIN Platform, which provides the operational environment for device onboarding, identity registration, marketplace coordination, and ecosystem governance.

The SEALCOIN Agent, a specialized software application installed directly on participating devices, responsible for managing device identity, executing transactions, and interacting with other agents across the network.

The SEALCOIN Messaging Protocol, a standardized communication layer that enables agents to negotiate service agreements, exchange information, and coordinate transactions before settlement occurs.

Together, these three pillars enable machines to securely discover services, negotiate agreements, and execute economic transactions within decentralized marketplaces.

Archived copy · cryp2nova.com

SEALCOIN AG develops and maintains the technological implementation of the SEALCOIN protocol and operates the SEALCOIN Platform supporting device onboarding, identity management, and service discovery across the ecosystem.

3.1 Overview of the SEALCOIN Network

The SEALCOIN network is designed to support a global ecosystem in which machines and AI agents interact economically through secure digital identities and programmable transaction mechanisms.

Within the network, devices participating in the ecosystem install the **SEALCOIN Agent**, which acts as the operational interface between the device and the SEALCOIN protocol. The Agent manages the device's cryptographic identity, executes secure communications with other agents through the SEALCOIN Messaging Protocol, and performs economic transactions through its integrated wallet functionality.

Once authenticated within the network, devices can participate in marketplace environments where they can discover services, offer resources, and execute economic transactions autonomously.

The **SEALCOIN Platform** enables this functionality by coordinating the interaction between devices, marketplace services, and settlement mechanisms. Acting as the ecosystem's registry and indexing layer, the platform allows users to onboard devices, configure operational parameters, and publish service availability across sector-specific marketplaces.

Through this architecture, the SEALCOIN protocol separates device-level execution from platform-level coordination. The SEALCOIN Agent performs the operational functions required for autonomous interaction, while the SEALCOIN Platform organizes marketplace participation and discovery across the ecosystem.

This modular design allows the SEALCOIN network to scale across industries and device categories while maintaining security, interoperability, and decentralized coordination.

Archived copy · cryp2nova.com

3.2 Device Identity Architecture

Secure device identity is the cornerstone of the SEALCOIN protocol. Every device participating in the network must possess a verifiable cryptographic identity enabling it to authenticate itself and establish trusted communication with other machines.

Within the SEALCOIN architecture, device identities are generated through cryptographic key pairs stored in protected environments within the device. These keys are associated with digital certificates that bind the device identity to recognized authentication standards.

The **SEALCOIN Agent** manages this identity at the device level. Upon installation, the Agent initializes the device's cryptographic environment, generates or registers cryptographic keys, and associates the device identity with the SEALCOIN Platform registry.

Once registered, the device can authenticate itself within the SEALCOIN protocol and interact securely with other authenticated devices through the SEALCOIN Messaging Protocol.

This identity framework ensures that every machine participating in the network possesses a verifiable and cryptographically secure identity, enabling trusted machine-to-machine communication across decentralized marketplaces.

3.3 Root of Trust and Secure Device Environments

The SEALCOIN protocol relies on a strong root of trust to guarantee the authenticity and integrity of device identities. This root of trust begins with the secure protection of private cryptographic keys within the device.

Devices participating in the SEALCOIN network protect their keys within isolated environments designed to prevent unauthorized extraction or manipulation. These environments may include hardware-based secure elements, trusted execution environments integrated within device processors, or secure microcontrollers embedded during device manufacturing.

The SEALCOIN protocol supports a flexible security architecture allowing different categories of devices to adopt security mechanisms appropriate to their operational environment. High-value infrastructure systems such as satellites, energy infrastructure components, and industrial equipment may integrate dedicated secure hardware modules,

Archived copy · cryp2nova.com

while consumer devices may rely on trusted execution environments integrated into their operating systems.

The **SEALCOIN Agent** interacts with these secure environments to manage cryptographic operations without exposing private keys. By ensuring that private keys remain protected within isolated execution environments, the SEALCOIN protocol preserves the integrity of device identities and prevents impersonation or unauthorized transaction execution.

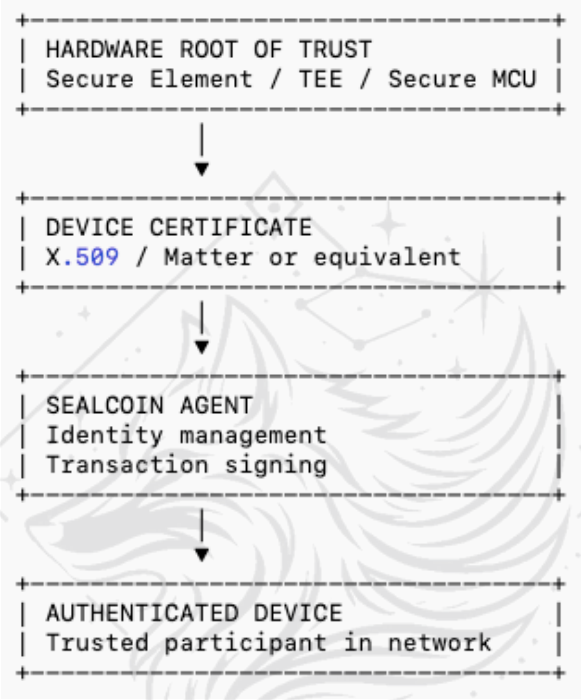


Figure 1: Device Identity and Trust Model

3.4 Device Authentication and Certificate Framework

Authentication within the SEALCOIN network is performed through a certificate-based framework aligned with established public key infrastructure standards.

Each device registered through the SEALCOIN Platform receives a digital certificate linking its cryptographic identity to a verifiable authentication record. These certificates enable devices to prove their identity when communicating with other agents within the network.

The SEALCOIN Agent manages the lifecycle of these certificates. It stores device credentials securely, executes authentication procedures when initiating communications, and validates the certificates of counterpart devices before executing service agreements.

Archived copy · cryp2nova.com

Through this mechanism, agents establish secure communication channels using **Mutual Transport Layer Security (mTLS)**, ensuring that both participants in a transaction can verify each other's identities.

By combining cryptographic identity with certificate validation, the SEALCOIN protocol ensures that all transactions originate from authenticated devices operating within trusted execution environments.

3.5 Secure Transaction Layer

The SEALCOIN protocol enables devices to execute service transactions through programmable smart contract mechanisms that automate economic settlement and enforce service conditions.

Before a transaction is executed, participating agents negotiate service parameters through the **SEALCOIN Messaging Protocol**. These negotiations may involve price discovery, resource availability verification, and agreement on service-level conditions.

Once both parties accept the negotiated terms, the transaction is formalized through the settlement layer associated with the SEALCOIN protocol.

The **SEALCOIN Agent** coordinates this process at the device level. It verifies the negotiated parameters, signs the transaction using the device's cryptographic identity, and executes the settlement through the integrated wallet.

This automated transaction model enables machines to exchange services autonomously while ensuring that execution conditions and payment obligations are enforced programmatically through the protocol's transaction logic.

3.6 Service Discovery and Device Interaction

For machines to exchange services efficiently, they must be able to identify and discover counterpart devices capable of fulfilling specific operational requests.

The **SEALCOIN Platform** provides service discovery mechanisms that allow devices to identify available resources across sector-specific marketplaces. Through the platform registry, devices can publish available services or discover counterpart devices offering relevant capabilities.

Archived copy · cryp2nova.com

Examples of such services include energy supply from distributed generation assets, satellite communication capacity, machine-generated data streams, or distributed computing resources.

The SEALCOIN Agent performs discovery operations on behalf of the device. It queries the platform registry, evaluates available service offers, and initiates negotiations with selected counterpart agents using the SEALCOIN Messaging Protocol.

Through this discovery and negotiation process, machines can dynamically allocate resources across the network and establish service relationships in real time.

3.7 Compliance Supervision Framework

As machine-to-machine transactions involve the exchange of economic value, the SEALCOIN ecosystem incorporates mechanisms designed to support regulatory compliance and operational governance.

Within the SEALCOIN architecture, the SEALCOIN Platform supports identity registration, device onboarding procedures, and transaction monitoring capabilities that facilitate compliance supervision across the ecosystem.

The SEALCOIN protocol enables traceability of transactions through cryptographic verification and verifiable transaction records, while the SEALCOIN Agent ensures that devices execute transactions within the operational parameters defined by their operators through the platform.

Compliance responsibilities are distributed across ecosystem entities according to their respective operational roles. While the SEALCOIN protocol provides the technological framework enabling secure machine interaction, governance structures associated with the ecosystem oversee regulatory alignment and operational compliance.

Through the integration of identity verification mechanisms, transaction monitoring capabilities, and governance coordination processes, the SEALCOIN ecosystem enables machine economies to operate within regulatory environments while preserving the decentralized operational model of the protocol.

Archived copy · cryp2nova.com

4. Key Technologies

The SEALCOIN protocol relies on a set of complementary technologies designed to enable secure identity, trusted communication, and programmable economic transactions between machines. These technologies collectively support the operation of the SEALCOIN Platform, the execution capabilities of the SEALCOIN Agent, and the communication framework provided by the SEALCOIN Messaging Protocol.

Unlike traditional distributed systems that primarily focus on human users, the SEALCOIN protocol is designed specifically for machine-to-machine interaction. Devices participating in the network must be able to authenticate themselves autonomously, establish secure communication channels, negotiate service agreements, and execute transactions with minimal latency and without centralized coordination.

To support these requirements, the SEALCOIN protocol integrates cryptographic identity frameworks, distributed ledger infrastructure, secure hardware environments, and programmable smart contract systems. These technologies together create a trusted environment in which devices and autonomous software agents can exchange services and value securely across decentralized marketplaces.

The following sections describe the core technological foundations supporting the SEALCOIN protocol architecture.

4.1 Distributed Ledger Infrastructure

The SEALCOIN protocol relies on distributed ledger technology to provide a transparent and tamper-resistant record of economic transactions executed within the network. The ledger functions as the settlement layer of the protocol, recording finalized service agreements and the associated transfer of economic value between participating devices.

Unlike traditional centralized databases, distributed ledgers replicate transaction records across multiple nodes participating in the network. This architecture provides resilience against single points of failure and ensures that transaction histories cannot be altered retroactively without consensus among network participants.

Archived copy · cryp2nova.com

Within the SEALCOIN ecosystem, the distributed ledger is used primarily for the execution and verification of economic transactions. Negotiation and service coordination occur off-chain through the SEALCOIN Messaging Protocol, while finalized agreements are recorded through ledger-based settlement mechanisms.

This hybrid architecture separates real-time negotiation from economic settlement. By keeping negotiation processes off-chain while using the ledger only for final settlement and verification, the SEALCOIN protocol achieves both scalability and transparency.

The distributed ledger therefore provides the trust anchor for economic exchanges between machines while allowing the broader network to operate with the speed and flexibility required for autonomous device interaction.

4.2 Cryptographic Foundations

Secure machine interaction requires robust cryptographic mechanisms capable of protecting device identities, verifying communications, and securing transaction execution. The SEALCOIN protocol relies on modern cryptographic primitives to ensure that all interactions within the ecosystem can be verified and authenticated.

Elliptic Curve Cryptography (ECC) forms the basis of the current cryptographic framework used for device identity generation, transaction signing, and certificate verification. ECC provides strong security guarantees while maintaining relatively low computational requirements, making it well suited for deployment across a wide range of device categories, including constrained embedded systems.

Within the SEALCOIN protocol, cryptographic keys are used to establish secure communication channels, sign transaction payloads, and validate service agreements negotiated between agents. The SEALCOIN Agent performs these cryptographic operations locally on the device, ensuring that private keys remain under the control of the device operator.

Through the integration of these cryptographic primitives, the SEALCOIN protocol ensures that every interaction between machines can be authenticated and verified before any economic transaction occurs.

Archived copy · cryp2nova.com

4.3 Secure Elements and Trusted Execution Environments

The security of the SEALCOIN protocol depends on the ability of devices to protect their cryptographic keys against unauthorized access or extraction. To achieve this, devices participating in the SEALCOIN network rely on secure execution environments designed to isolate sensitive cryptographic operations from the rest of the device software environment.

Several types of secure environments may be used depending on the device category and operational requirements. These environments include dedicated hardware secure elements, trusted execution environments integrated within device processors, embedded security modules, or secure microcontrollers integrated during device manufacturing.

Secure elements provide hardware-level protection for cryptographic keys by isolating them from the device's main operating system. Trusted execution environments provide a protected runtime environment within the device processor where sensitive operations can be executed securely.

The SEALCOIN Agent interacts with these secure environments to perform cryptographic operations without exposing private keys to application-level software. This architecture significantly reduces the risk of key compromise and strengthens the integrity of device identities within the SEALCOIN protocol.

By allowing multiple secure environment implementations, the SEALCOIN protocol maintains flexibility while preserving the requirement that private keys remain protected within isolated execution contexts.

CRYP2NOVA

4.4 Hardware Root of Trust and Post-Quantum Readiness

The concept of a hardware root of trust plays a central role in the SEALCOIN security architecture. A root of trust establishes the foundational security boundary that guarantees the authenticity of a device's identity and the integrity of its cryptographic operations.

In the SEALCOIN protocol, this root of trust begins with the secure storage and protection of private cryptographic keys within hardware-based or isolated environments. Devices

Archived copy · cryp2nova.com

participating in the ecosystem must ensure that their keys are generated, stored, and used within environments designed to resist tampering and unauthorized extraction.

In addition to current security mechanisms, the SEALCOIN protocol anticipates the evolution of cryptographic threats associated with the development of quantum computing. Certain classical cryptographic algorithms may eventually become vulnerable to large-scale quantum attacks, requiring the adoption of new cryptographic standards capable of resisting quantum computational capabilities.

To address this long-term challenge, the SEALCOIN technology framework is designed to support the future integration of post-quantum cryptographic algorithms. Devices equipped with secure microcontrollers or cryptographic hardware capable of supporting post-quantum schemes will be able to adopt these mechanisms as standards mature.

The ability to transition toward quantum-resistant cryptographic frameworks ensures that the SEALCOIN protocol can maintain the security of device identities and economic transactions over long operational horizons.

4.5 Device Public Key Infrastructure (PKI)

The SEALCOIN protocol relies on a certificate-based Public Key Infrastructure (PKI) to manage device identities and authentication across the network. PKI enables devices to prove their identities through digital certificates issued by recognized certificate authorities or trusted identity frameworks.

CRYP2NOVA

Within the SEALCOIN ecosystem, each device registered through the SEALCOIN Platform receives a certificate linking its cryptographic key pair to its registered identity. These certificates allow other devices and agents within the network to verify the authenticity of their counterparties before initiating communication or executing transactions.

The SEALCOIN Agent manages certificate storage and validation processes on behalf of the device. When establishing communication with another agent, the SEALCOIN Agent verifies the counterpart certificate and establishes a secure communication channel using Mutual Transport Layer Security.

Archived copy · cryp2nova.com

This certificate-based authentication mechanism ensures that only verified devices can participate in service transactions within the SEALCOIN protocol.

4.6 Smart Contracts and Autonomous Transactions

Smart contracts provide the programmable logic that enables autonomous service transactions within the SEALCOIN ecosystem. These contracts define the rules governing service execution, payment conditions, and transaction settlement between participating devices.

Within the SEALCOIN protocol architecture, smart contracts operate as the enforcement mechanism ensuring that economic agreements negotiated through the SEALCOIN Messaging Protocol are executed according to their defined conditions.

Once agents have negotiated a service agreement, the SEALCOIN Agent signs the transaction and submits it to the settlement layer of the protocol. The associated smart contract verifies that the transaction meets the required conditions before executing the economic settlement.

This programmable transaction model ensures that service agreements between machines can be executed automatically without requiring centralized oversight.

4.7 Machine Identity and Data Integrity

In addition to enabling secure transactions, the SEALCOIN protocol provides mechanisms ensuring the integrity and authenticity of machine-generated data.

Devices participating in the ecosystem can cryptographically sign the data they generate using their device identities. These signatures allow data consumers to verify both the origin and integrity of the information they receive.

By binding data signatures to device identities verified through the SEALCOIN protocol, the ecosystem enables the creation of trusted data markets in which machine-generated information can be exchanged as verifiable digital assets.

Archived copy · cryp2nova.com

This capability is particularly important in sectors such as environmental monitoring, industrial automation, space infrastructure, and artificial intelligence training, where the reliability and provenance of data directly impact operational decision-making.

Through the combination of cryptographic identity, certificate validation, and secure signing mechanisms, the SEALCOIN protocol ensures that both transactions and data exchanges within the ecosystem maintain a high level of trust and verifiability.

Archived copy · cryp2nova.com

5. Machine Economies and Vertical Marketplaces

The SEALCOIN protocol provides a secure transactional foundation for machines. It enables authenticated IoT devices and AI agents to negotiate, execute, and settle service-for-payment transactions using QAIT.

A protocol, however, is not a market. It enables interaction but does not define economic structure. To transform technical capability into organized economic activity, the SEALCOIN ecosystem introduces **Vertical Marketplaces**: sector-specific environments where industry rules, pricing structures, and token configurations are formalized on top of the common authentication and settlement layer.

This separation is intentional. The SEALCOIN protocol secures identity, certificates, wallets, and settlement, while each marketplace defines how value is created and exchanged within a specific industry context.

5.1 Concept of SEALCOIN Vertical Marketplaces

A SEALCOIN Vertical Marketplace is a sector-specific economic environment built on the SEALCOIN protocol where authenticated devices and AI agents interact under defined industry rules.

Each marketplace groups devices by functional domain, applies sector-specific smart contract logic, configures QAIT utility according to business context, and defines pricing and incentive models that reflect that vertical's operational realities. This is how the ecosystem moves from "machines can transact" to "machines transact in structured, sector-native economies."

Archived copy · cryp2nova.com

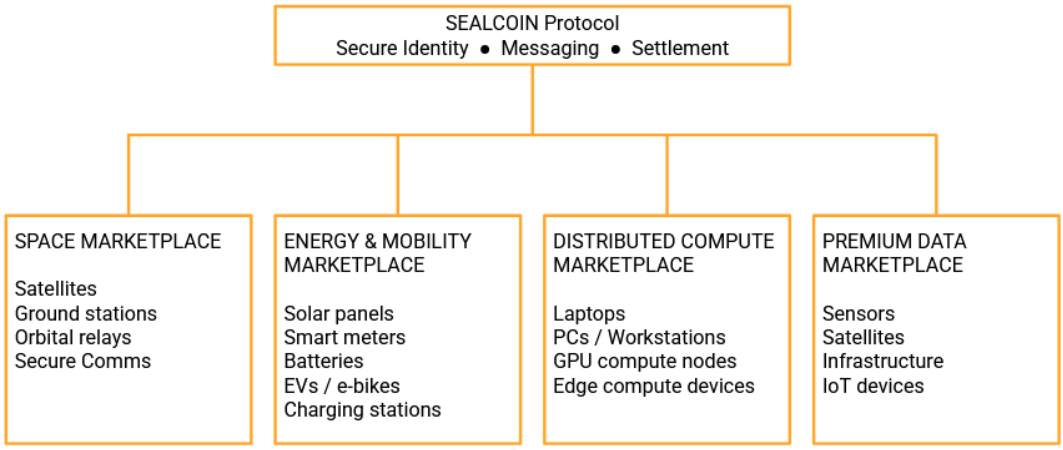


Figure 2: Sealcoin Machine Economy Verticals

5.2 Marketplace Architecture Model

Every SEALCOIN Vertical Marketplace operates across six structural layers, beginning at the hardware trust layer and extending to economic configuration and sector governance.

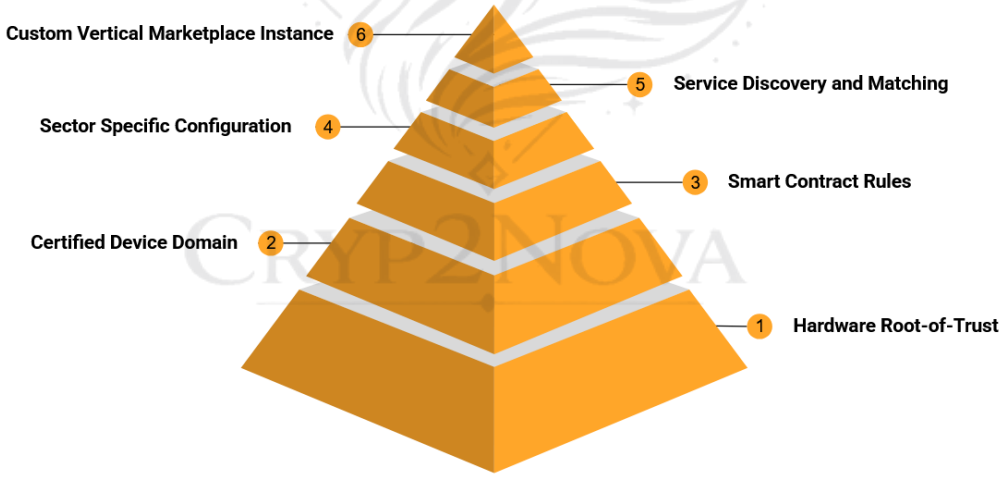


Figure 3: Sealcoin Vertical Marketplace Architecture

Layer 1: Hardware-Rooted Trust and Secure Identity Foundation

The reference security model across SEALCOIN marketplaces is a hardware-anchored Root of Trust. At its strongest level, device identity is protected within tamper-resistant hardware

Archived copy · cryp2nova.com

such as post-quantum-ready secure microcontrollers, dedicated Secure Elements, eSIM-based secure identity modules, ARM TrustZone environments, or other certified hardware security modules. In high-security sectors, private keys are embedded and protected at manufacturing level to ensure long-term cryptographic resilience, including resistance to future quantum computing threats.

SEALCOIN also recognizes proportional security: in constrained or cost-sensitive deployments, the secure environment can be adapted to lighter trusted execution contexts or, in limited contained scenarios, abstracted to hardened software isolation, provided private keys remain protected in an isolated and controlled environment appropriate to the use case.

Layer 2: Certified Device Domain

On top of the hardware-rooted or securely isolated identity layer, every device must be provisioned with a valid digital certificate compliant with recognized standards such as X.509 or Matter Alliance specifications (or equivalent frameworks). Certificate-based authentication is the minimum non-negotiable security framework across all machine economies, ensuring every transaction originates from a certificate-backed, cryptographically verifiable identity.

Layer 3: Business Logic Layer

Each vertical defines smart contract templates adapted to its sector. The protocol-level primitives remain consistent, while contract logic changes by industry: bandwidth allocation differs from kWh settlement, and data licensing differs from grid balancing. This layer is what turns secure identity into programmable economic behavior.

Layer 4: QAIT Economic Configuration

Each Vertical Marketplace defines its own economic parameters for QAIT-based transactions. Pricing logic, token locking requirements, incentive redistribution mechanisms, and PoSy Pool participation models adapt to the business environment in which devices operate.

Critically, all services and data across the SEALCOIN ecosystem are priced and labeled in U.S. dollars or relevant local fiat currencies for economic clarity and stability, while transactions are executed and settled in QAIT. This makes QAIT the settlement layer rather

Archived copy · cryp2nova.com

than the pricing unit and removes volatility risk from service pricing while preserving token-based settlement efficiency and programmability.

Layer 5: Service Discovery and Matching

Within each vertical, devices discover counterparties in clearly structured economic boundaries: a satellite discovers a ground station, an EV discovers a charging station, a solar panel discovers a local buyer, and a sensor lists a data stream for acquisition. This layer operationalizes real-time matching and negotiation at machine speed.

Layer 6: Optional Private Vertical Marketplace Instances

Enterprises may operate private PoSy Pools or restricted marketplace instances with customized governance, regulatory, or compliance constraints. This enables sector-specific adaptation without fragmenting the protocol layer.

Taken together, the architectural outcome is a consistent stack across industries: security begins in silicon, identity is anchored in certificates, logic is encoded in smart contracts, value is priced in fiat and settled in QAIT, and machine economies emerge from authenticated interaction.

5.3 Machine-to-Machine Transaction Flow

The following example illustrates how two authenticated devices interact within a SEALCOIN Vertical Marketplace. In this scenario, an EV charging station requests energy settlement from a solar panel installation.

Archived copy · cryp2nova.com

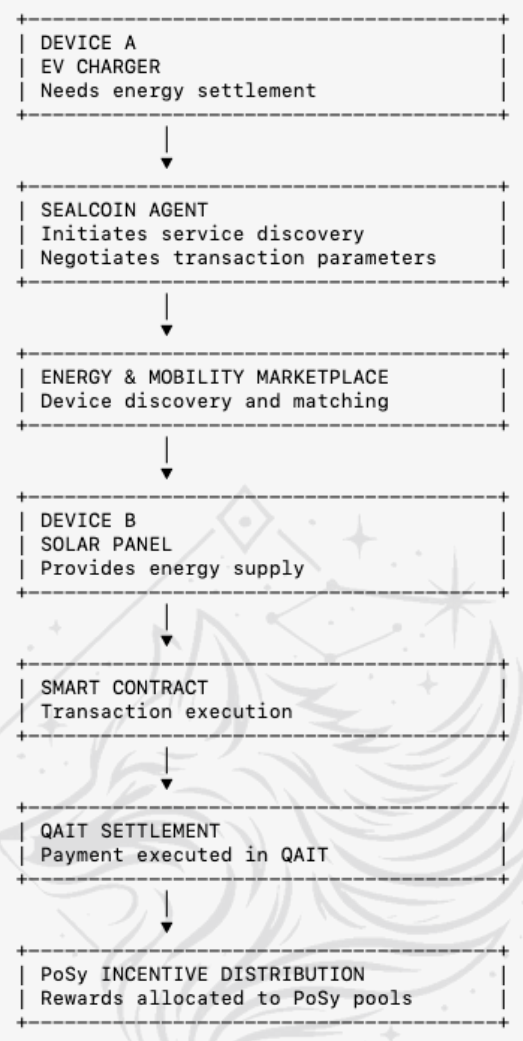


Figure 4: M2M Transaction Flow

CRYP2NOVA

5.4 SEALCOIN Space Communication Marketplace

5.4.1 Purpose and Scope

The SEALCOIN Space Communication Marketplace structures economic activity around satellite infrastructure and orbital communication services. It enables satellites, ground stations, IoT devices, and AI agents to autonomously transact services such as bandwidth allocation, secure communication channels, relay capacity, and space-derived data transmission.

Archived copy · cryp2nova.com

The onboarding of WISESAT satellites establishes the first operational infrastructure within this marketplace. Once certified and registered, satellites become autonomous economic actors capable of pricing and settling services without human intervention.

5.4.2 Transactional Logic

Transactions are driven by orbital constraints and communication demand. Bandwidth may be allocated dynamically, transmission windows can be reserved, and priority access can be priced differently from bulk data relay. AI agents may negotiate satellite access based on latency requirements or mission urgency.

Each transaction is authenticated via device certificates and settled in QAIT through smart contracts executed on the decentralized ledger.

5.4.3 QAIT Configuration in Space Context

The token logic reflects the economics of space infrastructure. Pricing may be time-based, priority-based, latency-sensitive, or volume-based, and token packages can include prepaid bandwidth, scheduled relay windows, emergency priority access, or enterprise-level communication agreements.

The structural shift is that satellites are no longer passive infrastructure. They become programmable service providers operating within a decentralized economic layer.

CRYP2NOVA

5.5 SEALCOIN Energy and Electric Mobility Marketplace

5.5.1 Purpose and Scope

The SEALCOIN Energy and Electric Mobility Marketplace structures real-time energy transactions between authenticated devices operating within distributed grids and mobility networks. Participants include smart meters, solar panels, stationary battery systems, grid operators, energy providers, electric vehicles, e-scooters, e-bikes, and charging stations.

From a systems perspective, electric vehicles and light electric mobility devices are mobile energy storage units with embedded metering and communication capabilities. In many

Archived copy · cryp2nova.com

cases, especially with emerging bidirectional charging standards, EVs can both consume and inject energy into the grid.

5.5.2 Device-Level Energy Autonomy

Transactions occur directly at device level. A smart meter can detect surplus solar production and initiate a sale. An EV can negotiate charging price at a station in real time. A fleet of e-scooters can settle charging costs autonomously. A grid operator can incentivize distributed storage devices to inject power during peak demand.

Devices authenticate one another through certificates, negotiate price per kilowatt-hour, and settle in QAIT through smart contracts. This removes manual reconciliation layers and enables machine-speed energy balancing.

5.5.3 Regulatory and Grid Integration

Energy markets operate under regulatory constraints. Settlement logic may incorporate geographic restrictions, compensation for grid transporters, or compliance conditions defined by utilities.

Energy providers and smart meter manufacturers may operate private PoSy Pools to embed compliance and governance rules into their device networks, allowing decentralization without regulatory anarchy.

5.5.4 QAIT Configuration in Energy and Mobility Context

Energy markets involve high transaction frequency and strict price stability requirements. Services and data pricing are indexed in fiat currencies to reduce volatility while settlement occurs in QAIT; token locking mechanisms may guarantee delivery capacity or provide priority grid access.

Electric mobility strengthens adoption because EV charging is a clear and widely understood use case: when an EV autonomously negotiates and settles charging, machine-based energy commerce becomes tangible.

Archived copy · cryp2nova.com

5.6 SEALCOIN Distributed Compute Marketplace

5.6.1 Purpose and Scope

The SEALCOIN Distributed Compute Marketplace enables authenticated computing devices to participate in decentralized compute infrastructure by sharing CPU and GPU capacity. Personal computers, laptops, workstations, and edge devices equipped with secure identity and SEALCOIN agents can contribute idle compute capacity to a distributed network where computational tasks are executed and settled autonomously.

This marketplace allows individuals and organizations to transform everyday computing devices into economic actors capable of providing computational services. Instead of remaining idle during large portions of their lifecycle, devices can allocate unused processing resources to workloads originating from enterprises, AI systems, research institutions, or decentralized applications.

The work conducted with laptop manufacturers illustrates this principle: consumer-grade devices can securely participate in a distributed compute marketplace where users actively contribute CPU or GPU resources and receive compensation for services performed by their machines.

5.6.2 Compute Transaction Model

Within this marketplace, devices advertise available compute capacity that can be consumed by authorized workloads. Compute requests are matched to authenticated devices capable of executing tasks; results can be attributed to the executing device through verifiable identity, and settlement is automated through smart contract execution.

5.6.3 QAIT Configuration in Distributed Compute Context

Compute services are priced according to capacity and workload characteristics (for example CPU/GPU time allocation, execution duration, and latency or priority requirements), while pricing remains fiat-referenced and settlement is executed in QAIT under the same stability principle applied across marketplaces. This enables enterprises

Archived copy · cryp2nova.com

and AI systems to source distributed compute without operating centralized infrastructure, while device owners monetize unused processing capacity.

5.7 SEALCOIN Premium Data Marketplace

5.7.1 Purpose and Scope

The SEALCOIN Premium Data Marketplace formalizes the trade of authenticated, cryptographically signed machine-generated data. Its defining principle is integrity: only data produced by certified and authenticated devices can be listed and exchanged.

Each data stream is signed by the device's Secure Element, linked to a verifiable certificate, timestamped on the decentralized ledger, and cryptographically auditable. This transforms raw sensor output into a verifiable digital asset.

5.7.2 Data Transaction Model

Devices such as environmental sensors, industrial machines, satellites, smart grids, and mobility systems can list data streams for purchase, and buyers may include enterprises, research institutions, AI systems, or smart contracts requiring verified real-world inputs.

Transactions are executed via smart contracts, and payment in QAIT is released upon successful data delivery and verification. Unlike conventional data markets, authenticity is enforced through certificate-based identity and secure key environments.

CRYP2NOVA

5.7.3 QAIT Configuration in Data Context

Pricing structures may include pay-per-stream access, subscription-based feeds, dataset licensing, real-time oracle integration, and AI training data packages. In this vertical, QAIT monetizes verified origin and enables a premium segment for authenticated machine data rather than competing with bulk aggregation platforms.

Archived copy · cryp2nova.com

5.8 Cross-Marketplace Interoperability and Strategic Positioning

Devices are not confined to a single vertical. The architecture is designed for multi-vertical participation: a satellite can participate in Space Communication and Premium Data; a solar panel can participate in Energy and Premium Data; mobility devices can participate in Energy and broader mobility extensions; and AI agents can transact across multiple verticals. This interoperability is enabled by the shared trust and settlement stack, where discovery and negotiation occur within vertical boundaries while settlement remains consistent through QAIT.

Strategically, the Vertical Marketplace framework formalizes SEALCOIN's evolution from a secure transactional protocol into vertical marketplace infrastructure. The protocol secures identity and settlement, while the marketplaces structure economic behavior into sector-native machine economies.

CRYP2NOVA

Archived copy · cryp2nova.com

6. QAIT Token and Economic Layer

The SEALCOIN protocol enables authenticated machines and AI agents to discover services, negotiate economic terms, and execute autonomous transactions across sector-specific Vertical Marketplaces. While the protocol and platform provide the technical infrastructure for identity, communication, and transaction execution, economic settlement within the ecosystem is performed through the **QAIT token**.

QAIT functions as the programmable settlement instrument that allows machines to exchange value once service agreements are negotiated through the SEALCOIN Messaging Protocol and executed by SEALCOIN Agents operating on participating devices.

Within the SEALCOIN ecosystem architecture, a clear functional separation exists between infrastructure and token governance. SEALCOIN AG develops and operates the technological environment supporting device authentication, service discovery, and transaction execution, while the **QAIT Association acts as the independent issuer and governance body responsible for token issuance, distribution, and token-related economic policies**.

This separation ensures that the technological infrastructure enabling machine economies remains distinct from token issuance and crypto-economic governance.

The QAIT token is designed to support a decentralized machine economy where authenticated devices and AI agents transact services autonomously across multiple vertical industries. Its economic design integrates a **Proof-of-Security (PoSy)** mechanism that aligns device onboarding, network security, token utility, and ecosystem incentives.

6.1 Role of QAIT in the SEALCOIN Ecosystem

QAIT acts as the economic backbone of the SEALCOIN ecosystem, enabling machines to settle service transactions securely and autonomously. Devices equipped with the SEALCOIN Agent hold QAIT through integrated non-custodial wallets that allow them to execute programmable payments once service agreements have been fulfilled.

Within Vertical Marketplaces, devices negotiate services such as communication bandwidth, energy supply, compute resources, or authenticated data streams. These

Archived copy · cryp2nova.com

negotiations occur through the SEALCOIN Messaging Protocol and are executed by SEALCOIN Agents representing the participating machines.

Once service conditions are verified, economic settlement is performed using QAIT through smart contract execution. This architecture enables machines to complete transactions autonomously while maintaining cryptographic verification and transparent transaction records.

Beyond payment functionality, QAIT also plays a critical role in securing the ecosystem through the **Proof-of-Security framework**, which governs device onboarding, security guarantees, and economic incentives associated with machine activity.

The native issuance of QAIT is implemented on the Hedera network using the Hedera Token Service (HTS), which provides the primary settlement infrastructure for the SEALCOIN ecosystem.

To support broader accessibility, interoperability, decentralized liquidity, and exchange integrations, QAIT may also be made available on additional blockchain networks through cross-chain interoperability infrastructure and interoperable token representations.

6.2 Utility Principles of the QAIT Token

The QAIT token serves multiple complementary roles within the SEALCOIN ecosystem, linking network security, device identity validation, and machine-to-machine economic activity.

First, QAIT supports the secure onboarding of IoT devices and AI agents into the ecosystem. Devices must meet minimum authentication standards and possess valid certificates before they can interact within the network. The token locking mechanisms associated with the PoSy framework reinforce this security requirement by ensuring that device onboarding is economically secured.

Second, QAIT validates machine intercommunication and data interchange across the network. Transactions between devices, including service exchanges and data transfers, are cryptographically recorded and economically settled through the token.

Third, QAIT enables decentralized machine-to-machine payments. Autonomous devices executing services within Vertical Marketplaces rely on QAIT as the programmable settlement instrument that allows economic transactions to occur without centralized intermediaries.

Archived copy · cryp2nova.com

Together, these utility principles ensure that QAIT is not merely a transactional token but a foundational element supporting the integrity, security, and economic functionality of the SEALCOIN ecosystem.

6.3 Fiat-Referenced Pricing and QAIT Settlement

Machine economies require predictable pricing structures that align with real-world economic conditions. For this reason, the SEALCOIN ecosystem separates service pricing from token settlement.

Across all Vertical Marketplaces, services and data are priced and labeled in U.S. dollars or relevant local fiat currencies. Devices negotiating services therefore reference stable economic units consistent with the industries in which they operate.

Once service terms are agreed upon, the equivalent value is settled in QAIT through the token settlement layer of the protocol. This design ensures economic stability for service providers and infrastructure operators while preserving the efficiency and programmability of token-based settlement.

By decoupling pricing from token volatility, the SEALCOIN ecosystem enables enterprises and infrastructure operators to integrate autonomous machine transactions without exposing operational pricing to fluctuations in digital asset markets.

6.4 Proof-of-Security (PoSy) Framework

The economic and security architecture of the SEALCOIN ecosystem is built around the **Proof-of-Security (PoSy)** mechanism. PoSy is designed to align token utility, device and AI Agents onboarding, and ecosystem security by linking token locking with the secure registration and operation of machines within the network.

Under the PoSy framework, participants lock QAIT tokens in order to secure the registration of devices and AI agents. These locked tokens establish a security commitment that guarantees the integrity and accountability of machines operating within the ecosystem.

The PoSy mechanism therefore serves several functions simultaneously:

Archived copy · cryp2nova.com

- securing machine onboarding,
- aligning economic incentives with network security,
- rewarding participants contributing to ecosystem integrity.

By requiring economic commitment through token locking, PoSy mitigates the risk of malicious machines behavior while encouraging long-term participation in the network.

6.5 Machine Prevalidation and Secure Onboarding

Device and AI Agents onboarding within the SEALCOIN ecosystem follows a structured security model. Machines must possess valid authentication certificates and meet minimum security standards before being allowed to operate within the network.

Machines (devices or AI agents) may join the ecosystem through two primary onboarding mechanisms:

1. direct onboarding through certificate registration, or
2. onboarding through participation in a PoSy pool.

In the PoSy model, token locking creates **prevalidation capacity** for machines. The number of devices or AI agents that may be registered through a pool is determined by the quantity of QAIT tokens locked within that pool.

CRYP2NOVA

This mechanism ensures that machine registration capacity is economically secured. Tokens must remain locked for the entire duration during which associated device slots are used, creating a direct link between token commitment and network security.

Prevalidation slots are limited and released progressively in order to maintain balanced growth of the ecosystem and to ensure that onboarding capacity remains aligned with network security requirements.

Archived copy · cryp2nova.com

6.6 PoSy Pools and Device Networks

PoSy pools represent coordinated security groups responsible for managing the onboarding and operation of devices within the ecosystem.

Participants may lock QAIT tokens within a pool, allowing the pool to register and secure multiple devices on their behalf. Pools therefore act as decentralized coordination mechanisms that manage device onboarding while reinforcing network security.

Organizations may also operate private PoSy pools to manage the onboarding of machines within specific infrastructures. For example, energy providers may deploy pools governing smart meters, energy storage systems, and electric mobility infrastructure within their networks.

Each pool must maintain a minimum quantity of locked QAIT tokens in order to operate and to ensure that sufficient security coverage exists for the devices and AI agents registered through the pool.

The relationship between locked tokens and registered machines establishes the **ratio**, which ensures that the number of devices operating within the network remains proportionate to the economic commitment securing their activity.

6.7 Transaction-Based Incentive Mechanism

The PoSy framework also incorporates a transaction-based reward model designed to incentivize active participation within the ecosystem.

CRYP2NOVA

When registered machines execute service transactions within Vertical Marketplaces, a small fraction of the transaction fees generated by those activities is allocated to the security reward pool associated with the PoSy framework.

Participants who contribute locked tokens to a PoSy pool receive rewards derived from the transaction activity generated by machines secured within that pool. The magnitude of rewards depends on several factors, including the number of devices and AI agents registered in the pool, the volume of transactions generated by those, and the value of the transactions executed.

Archived copy · cryp2nova.com

This mechanism ensures that economic rewards are directly linked to productive machine activity within the network. Devices generating higher transaction volumes contribute proportionally more to the incentive pool, aligning economic incentives with ecosystem growth.

6.8 Security Enforcement and Penalty Mechanisms

Maintaining the integrity of the machine economy requires mechanisms capable of discouraging malicious behavior or invalid transaction activity.

Within the PoSy framework, devices that submit invalid or malicious transactions may trigger penalties affecting the locked QAIT tokens associated with their security pool. In such cases, a portion of the locked tokens may be subject to enforcement actions defined by the PoSy framework and smart-contract rules (including, where applicable, penalty mechanisms).

This mechanism creates strong economic incentives for participants to maintain the integrity of devices operating under their supervision. By linking security enforcement directly to token commitments, the PoSy framework strengthens the overall reliability of the SEALCOIN ecosystem.

6.9 Smart-Contract Governed Pools

PoSy pools operate through smart contract governance mechanisms that enforce the rules governing token locking, device registration, and reward distribution.

Pools may operate under different locking configurations. In some pools, tokens may be withdrawn at any time, although withdrawal may result in the associated devices being paused or requiring reassignment to alternative security coverage.

Other pools may implement predefined locking periods, during which tokens remain committed for a fixed duration. When the lock period expires, the tokens are reallocated automatically unless the participant opts out of the automatic reallocation.

All token locking operations enforced by smart contracts, ensuring that token ownership remains under the control of participants at all times.

Archived copy · cryp2nova.com

6.10 Token Holder Participation and Ecosystem Alignment

To encourage long-term engagement and ecosystem development, the SEALCOIN economic model introduces participation tiers for token holders based on the amount of QAIT tokens committed within the PoSy framework.

A tiered approach enables participants to access different operational privileges within the ecosystem, including device onboarding capacity, marketplace participation features, governance influence, and advanced service capabilities.

By linking ecosystem participation to token commitment and device activity, the QAIT token model creates strong alignment between network growth, security guarantees, and economic incentives.

6.11 Economic Integration Across Vertical Marketplaces

The economic mechanisms described above operate across all SEALCOIN Vertical Marketplaces. Whether devices exchange satellite communication services, energy resources, computing capacity, or authenticated data streams, settlement occurs through QAIT while security guarantees are enforced through the PoSy framework.

Through the integration of programmable settlement, security-anchored token locking, and marketplace-driven transaction activity, the QAIT token enables the emergence of autonomous machine economies operating across multiple industries.

The combination of the SEALCOIN protocol, the SEALCOIN Agent architecture, and the QAIT PoSy framework establishes a scalable economic model capable of supporting global machine-to-machine commerce.

Archived copy · cryp2nova.com

7. Governance and Ecosystem Structure

The SEALCOIN ecosystem operates through a structured governance model designed to ensure a clear separation between technological infrastructure and token-related economic activities. This model establishes distinct responsibilities for network operation, protocol development, and token issuance, while maintaining coordinated compliance supervision across the ecosystem.

The governance structure is built around two complementary entities: **SEALCOIN AG** and the **QAIT Association**. Each entity performs specific roles that together support the operation of the SEALCOIN protocol, the deployment of Vertical Marketplaces, and the economic activity enabled through the QAIT token.

This separation ensures that the development and maintenance of the technological infrastructure remain independent from token issuance and crypto-economic governance, creating a transparent and compliant operational framework for the ecosystem.

7.1 Structural Overview of the Ecosystem

The SEALCOIN ecosystem follows a dual-entity governance model that separates infrastructure management from token issuance.

Within this structure, **SEALCOIN AG** acts as the technology provider responsible for developing and maintaining the infrastructure supporting the SEALCOIN protocol. Its responsibilities include building the technical components that enable device identity, secure communication, and autonomous machine transactions.

In parallel, the **QAIT Association** acts as the issuer and governance body responsible for the QAIT token and its associated economic mechanisms. The Association oversees token issuance, distribution policies, and token-related governance decisions.

This dual-entity structure provides a clear functional separation between technology infrastructure and token economic management while allowing both components to operate cohesively within the SEALCOIN ecosystem.

Archived copy · cryp2nova.com

SEALCOIN AG Technology Provider	QAIT ASSOCIATION Token Issuer
• Develops SEALCOIN protocol • Operates the platform • Maintains infrastructure • Ensures technical security • Supervises compliance systems Does NOT: • Issue tokens • Control token supply	• Issues the QAIT token • Manages token governance • Oversees token distribution • Manages token treasury • Oversees crypto-economic logic Does NOT: • Develop the protocol • Operate the network

Table 1: Token Governance

7.2 SEALCOIN AG: Infrastructure and Technology Provider

SEALCOIN AG is responsible for the development, integration, and maintenance of the technological infrastructure supporting the SEALCOIN protocol. Its role focuses exclusively on the technical environment required to enable secure machine interaction and autonomous economic transactions.

The responsibilities of SEALCOIN AG include the design and development of the protocol architecture, the integration of hardware and software components necessary for device authentication, and the operation of the SEALCOIN Platform that coordinates device onboarding and service discovery across Vertical Marketplaces.

In addition to infrastructure development, SEALCOIN AG implements cybersecurity safeguards, operational resilience mechanisms, and system integrity controls designed to maintain the reliability of the network.

SEALCOIN AG also supervises compliance mechanisms applied within the ecosystem. This includes monitoring the implementation of identity verification procedures, overseeing transaction monitoring frameworks, and coordinating compliance standards across ecosystem participants.

Importantly, SEALCOIN AG does not issue the QAIT token and does not control token supply or token treasury mechanisms. Its role is limited to providing the technological environment through which token-based transactions can occur.

This separation ensures that the technological infrastructure enabling machine economies operates independently from token issuance and crypto-economic governance.

Archived copy · cryp2nova.com

7.3 QAIT Association: Token Issuer and Crypto-Economic Governance

The QAIT Association serves as the issuer and governance authority responsible for the QAIT token and its associated economic mechanisms.

The Association defines token issuance policies, oversees token distribution processes, and manages the crypto-economic parameters governing token circulation within the SEALCOIN ecosystem. These responsibilities include establishing token governance frameworks, supervising treasury-related functions, and ensuring that token-related activities comply with applicable regulatory standards.

In addition to token issuance and governance, the QAIT Association implements identity verification and anti–money laundering controls related to token distribution and participation in token-related activities. These procedures ensure that participants interacting with the token economy meet the compliance standards required within the ecosystem.

The QAIT token is designed as a **hybrid** token combining both **utility and payment** characteristics. It enables access to services within the SEALCOIN ecosystem while also functioning as the settlement mechanism for machine-to-machine transactions executed across Vertical Marketplaces.

By managing token issuance and economic governance independently from the protocol infrastructure, the QAIT Association ensures that the economic layer of the ecosystem remains transparent, accountable, and aligned with regulatory expectations.

Governance Structure

The QAIT Association operates under a governance framework defined by its Articles of Association and supervised through its governing bodies, including the General Meeting and the Association Board. The Association was established with two Founding Members, Jonathan LLamas and Andrew Forson, who contributed to the creation of the governance framework and the initial strategic direction of the ecosystem.

As the SEALCOIN ecosystem evolves, the Association is designed to expand its membership base by welcoming additional participants from industry, technology, academia, and the broader ecosystem. These members participate in the governance of the Association through the General Meeting and may contribute to advisory committees or governance bodies supporting the development of the ecosystem.

Archived copy · cryp2nova.com

This evolving governance structure ensures that the stewardship of the QAIT token economy progressively reflects a broader ecosystem representation while maintaining continuity in the strategic development of the SEALCOIN protocol and its associated marketplaces.

7.4 Activities and Non-Activities of Ecosystem Entities

The SEALCOIN ecosystem governance model clearly defines the activities performed by each entity as well as the activities that fall outside their operational scope.

SEALCOIN AG performs technological and compliance-related functions associated with the operation of the network infrastructure. These include protocol development, platform integration, cybersecurity safeguards, infrastructure maintenance, and the supervision of compliance frameworks implemented across the ecosystem.

The QAIT Association performs token-related functions, including token issuance, distribution to verified participants, crypto-economic governance, and treasury oversight related to the QAIT token.

Equally important are the activities that neither entity performs. The ecosystem does not engage in the issuance of investment tokens, equity tokens, or debt instruments. It does not operate as a banking institution, does not accept public deposits, and does not manage investment portfolios or collective investment schemes.

Furthermore, the ecosystem does not operate brokerage services, trading venues, or over-the-counter trading platforms. It does not provide regulated custody services for third-party assets and does not offer financial advisory or investment recommendation services.

Participation in the ecosystem also requires verifiable identity. Anonymous participation or privacy-enhanced untraceable transactions are not permitted.

By clearly defining both operational activities and non-activities, the governance structure reinforces the technological and infrastructural nature of the SEALCOIN ecosystem while avoiding activities associated with regulated financial intermediaries.

Archived copy · cryp2nova.com

7.5 Regulatory Positioning

The governance structure of the SEALCOIN ecosystem is designed to align with regulatory expectations while supporting the operation of decentralized machine economies.

Within this structure, the QAIT token is positioned as a hybrid digital asset combining utility and payment characteristics. Its primary function is to enable access to services within the ecosystem and to provide a programmable settlement mechanism for machine-to-machine transactions.

The QAIT Association acts as the issuer responsible for token-related crypto activities, including issuance, distribution, and compliance procedures associated with token participation.

SEALCOIN AG operates as the technology provider responsible for the protocol infrastructure and supervises compliance frameworks applied to the ecosystem.

This separation between token issuance and infrastructure operation provides a governance model that supports regulatory transparency while enabling the SEALCOIN ecosystem to function as a technological platform facilitating autonomous machine economies.

CRYP2NOVA

Archived copy · cryp2nova.com

8. Compliance Framework

The SEALCOIN ecosystem is designed to enable autonomous machine-to-machine economic activity while operating within a framework that supports regulatory compliance and responsible network governance. As devices and AI agents begin to transact value autonomously, the infrastructure enabling these transactions must incorporate mechanisms that support identity verification, transaction traceability, and risk monitoring.

The SEALCOIN protocol integrates compliance capabilities at multiple levels of the ecosystem architecture. These mechanisms ensure that economic activity generated by machines operating through SEALCOIN Agents and participating in Vertical Marketplaces remains aligned with applicable legal and regulatory expectations.

The compliance framework combines technological safeguards embedded within the protocol architecture with governance structures coordinated by ecosystem entities responsible for infrastructure operation and token issuance.

8.1 Identity Verification and Participant Onboarding

A foundational element of the SEALCOIN protocol compliance model is the requirement that ecosystem participants operate through verified identities.

Devices and AI agents participating in the network must be associated with authenticated operators. This requirement ensures that machine-generated transactions can be linked to accountable entities and that ecosystem participation remains consistent with applicable identity verification standards.

Device identities are anchored through certificate-based authentication mechanisms described in earlier sections of this document. Devices must possess valid authentication certificates before they can interact with other machines or participate in service transactions within Vertical Marketplaces.

Participants interacting with token-related functions within the ecosystem, including token distribution or token-based economic participation, are subject to identity verification procedures implemented by the QAIT Association as part of its token issuance and distribution responsibilities.

Archived copy · cryp2nova.com

This layered identity model combines device-level authentication with participant-level verification to ensure that economic activity generated within the ecosystem remains traceable and accountable.

8.2 Anti–Money Laundering (AML) and Risk Monitoring

Machine economies introduce new forms of automated value exchange. As such, transaction monitoring mechanisms are required to ensure that the economic flows generated within the ecosystem do not facilitate illicit financial activity.

The SEALCOIN ecosystem integrates transaction monitoring capabilities designed to detect anomalous activity patterns and to support the implementation of anti–money laundering controls associated with token circulation.

Token-related onboarding and distribution procedures implemented by the QAIT Association incorporate AML compliance processes that verify participant identities and assess potential risk factors associated with token participation.

In parallel, SEALCOIN AG supervises the technological infrastructure supporting transaction monitoring within the network environment. This supervision ensures that token-related flows occurring through the SEALCOIN protocol remain observable and that risk monitoring capabilities can be applied when required.

Through the combination of issuer-level compliance procedures and infrastructure-level monitoring capabilities, the ecosystem supports the implementation of AML frameworks appropriate for a decentralized machine economy.

CRYP2NOVA

8.3 Transaction Traceability and Transparency

The SEALCOIN protocol is designed to provide verifiable records of machine-generated transactions. Each service exchange executed within the ecosystem is recorded through cryptographic verification mechanisms associated with the distributed ledger settlement layer.

These records provide a transparent and immutable history of economic interactions between devices. By linking transactions to authenticated device identities and cryptographic signatures generated by SEALCOIN Agents, the ecosystem ensures that transaction provenance can be verified when necessary.

Archived copy · cryp2nova.com

Traceability mechanisms play a critical role in maintaining the integrity of the machine economy. They allow ecosystem participants, regulators, and authorized entities to verify the origin and authenticity of transactions without compromising the decentralized architecture of the network.

8.4 Compliance Supervision within the Ecosystem

Compliance responsibilities within the SEALCOIN ecosystem are distributed according to the governance structure defined earlier in this document.

The QAIT Association implements identity verification and AML procedures related to token issuance, token distribution, and participation in token-related economic activities.

SEALCOIN AG supervises compliance mechanisms integrated within the network infrastructure. This supervision includes monitoring the operation of identity frameworks, overseeing transaction monitoring capabilities, and coordinating compliance standards applied across ecosystem participants.

By combining issuer-level compliance procedures with infrastructure-level supervision, the ecosystem establishes a governance model capable of supporting regulatory alignment while maintaining the decentralized operational model of the SEALCOIN protocol.

8.5 Compliance in Autonomous Machine Economies

The emergence of machine-to-machine economies introduces new operational paradigms in which devices act as autonomous economic agents. In this context, compliance mechanisms must operate alongside automated transaction execution.

Within the SEALCOIN ecosystem, SEALCOIN Agents execute transactions on behalf of devices while remaining bound by the operational policies configured by device operators through the SEALCOIN Platform. These policies may include transaction limits, service pricing parameters, and operational constraints that guide machine behavior within the network.

By combining programmable transaction logic with identity verification and compliance supervision mechanisms, the SEALCOIN protocol enables machines to transact autonomously while maintaining accountability and traceability.

Archived copy · cryp2nova.com

This approach allows the SEALCOIN ecosystem to support the growth of decentralized machine economies without compromising the governance standards required for responsible digital infrastructure.

Archived copy · cryp2nova.com

9 SEALCOIN Protocol Core Development Team

The technological development of the SEALCOIN protocol is led by **SEALCOIN AG**, the entity responsible for the design, development, and operation of the SEALCOIN protocol and platform.

SEALCOIN AG develops the infrastructure that enables autonomous machine-to-machine transactions across decentralized marketplaces. This includes the development of the SEALCOIN platform, the SEALCOIN Agent architecture, the messaging protocol, and the integration of marketplace verticals operating on top of the protocol.

The SEALCOIN development team combines expertise in cybersecurity, distributed systems, decentralized infrastructure, digital identity technologies, and enterprise software engineering.

The following individuals constitute the core development team of SEALCOIN protocol.

Carlos Moreira

Chief Executive Officer

Carlos Moreira is the founder, Chairman, and CEO of WISeKey and SEALSQ, publicly listed cybersecurity and semiconductor companies specializing in digital identity, cybersecurity, and secure IoT technologies.

He has more than twenty-five years of experience in cybersecurity and digital trust infrastructure. His work focuses on enabling secure digital identities and trusted infrastructures for the Internet and the Internet of Things.

Carlos Moreira has served as a United Nations expert on cybersecurity and has been a member of the World Economic Forum Global Agenda Council on the Future of Information Technology.

Within the SEALCOIN ecosystem, he provides strategic leadership supporting the development of secure digital infrastructure and trusted machine identity frameworks.

Jonathan Llamas

Archived copy · cryp2nova.com

Chief Product and Strategy Officer

Jonathan Llamas is responsible for product architecture and ecosystem strategy for the SEALCOIN platform.

Before joining SEALCOIN, he founded a blockchain venture studio in Switzerland where he worked with Fortune 500 companies and academic institutions on distributed ledger initiatives.

He previously built a decentralized personal data management platform enabling hundreds of thousands of users to control and monetize their personal data using blockchain infrastructure.

Within SEALCOIN, he leads the development of the marketplace architecture and the machine-to-machine economic framework enabled by the protocol.

Jeremy Pansier

Chief Technology Officer

Jeremy Pansier is responsible for the technical architecture of the SEALCOIN platform.

He is a cybersecurity engineer specializing in cryptography and distributed systems. Prior to becoming CTO of SEALCOIN, he led the development of the project's proof-of-concept and initial platform architecture.

Jeremy oversees the development of the SEALCOIN protocol stack, including the platform infrastructure, agent architecture, and integration with decentralized ledger technologies.

CRYP2NOVA

John O'Hara

Chief Financial Officer

John O'Hara is Chief Financial Officer of WISeKey and SEALSQ and brings more than twenty years of experience in finance, governance, and corporate operations.

He previously served as International Controller for WISeKey and has held finance leadership roles at Marsh & McLennan, Deloitte, Yum! Restaurants International, and Chelsea Football Club.

Within SEALCOIN, he oversees financial governance and operational financial planning.

Archived copy · cryp2nova.com

Andreas Moreira

Chief Innovation Officer

Andreas Moreira leads innovation initiatives within the WISeKey ecosystem and contributes to the development of security and digital identity frameworks supporting SEALCOIN.

His work focuses on cybersecurity, trusted IoT infrastructures, and secure digital ecosystems.

Within SEALCOIN, he contributes to innovation strategy and the integration of secure identity technologies within decentralized machine networks.

Bacem Ben Achour

Embedded Software Engineer

Bacem Ben Achour is a software engineer specializing in embedded systems and distributed application development. He contributes to the engineering and implementation of the SEALCOIN platform, focusing on the integration of device-level software with the broader protocol architecture.

Working closely with the Chief Technology Officer and the engineering team, he participates in the development of core platform components supporting device onboarding, marketplace operations, and secure transaction flows within the SEALCOIN ecosystem.

His work includes the implementation of software modules enabling interaction between connected devices, the SEALCOIN Agent architecture, and the smart contract layer supporting autonomous machine-to-machine transactions. Through this role, he contributes to ensuring the reliability, scalability, and security of the SEALCOIN platform as the ecosystem expands.

Micha Roon

Head of Engineering

Micha Roon is Head of Engineering at The Hashgraph Group and contributes engineering leadership to the SEALCOIN ecosystem.

He has more than twenty years of experience in distributed systems and decentralized infrastructure development.

Archived copy · cryp2nova.com

Within SEALCOIN, he contributes to the architecture and implementation of distributed systems and decentralized platform infrastructure.

Jeet Parekh

Web3 Architect

Jeet Parekh is a blockchain architect specializing in distributed ledger technologies, including Hedera.

His experience includes the development of financial infrastructure systems, digital asset platforms, and smart contract architectures.

Within SEALCOIN, he contributes to the architecture and integration of Web3 components supporting the ecosystem.

Eduardo Valenzuela

Scrum Master

Eduardo Valenzuela is an experienced IT project manager and Scrum Master specializing in agile development environments.

He coordinates development teams and manages the delivery lifecycle of the SEALCOIN platform.

CRYP2NOVA

Alex Stadnik

Backend Engineer and DevOps Lead

Alex Stadnik specializes in backend infrastructure and cloud architecture.

He has more than ten years of experience developing distributed systems and scalable infrastructure using technologies such as Kubernetes, AWS, and containerized environments.

Within SEALCOIN, he leads backend platform development and DevOps architecture.

Archived copy · cryp2nova.com

Jakub Poliszuk

Full Stack Engineer

Jakub Poliszuk is a senior full-stack developer with extensive experience in distributed systems and modern web technologies.

Within SEALCOIN, he contributes to platform development, marketplace interfaces, and application architecture.

CRYP2NOVA

Archived copy · cryp2nova.com

10. Ecosystem Participants

The SEALCOIN ecosystem is designed to support a broad range of participants contributing to and benefiting from autonomous machine economies. The architecture of the SEALCOIN protocol enables devices, infrastructure operators, developers, enterprises, and autonomous software agents to interact through a shared framework of secure identity, programmable service negotiation, and token-based economic settlement.

Unlike traditional digital platforms where human users act as the primary participants, the SEALCOIN ecosystem introduces a model in which machines themselves operate as transactional actors. Through the SEALCOIN Agent, devices and AI systems can negotiate services, execute agreements, and settle transactions autonomously within sector-specific Vertical Marketplaces.

Human participants, whether individuals, enterprises, or developers, interact with the ecosystem primarily through the configuration, deployment, and governance of the devices and systems that operate within the network.

The following categories describe the principal participants that contribute to the operation and growth of the SEALCOIN ecosystem.

10.1 Device Manufacturers

Device manufacturers represent a foundational participant category within the SEALCOIN ecosystem. By integrating SEALCOIN-compatible identity mechanisms and the SEALCOIN Agent into their hardware products, manufacturers enable devices to participate directly in machine-to-machine economic transactions.

Manufacturers may embed secure identity environments within their devices, such as secure elements, trusted execution environments, or post-quantum–ready cryptographic modules. These components allow devices to generate and protect cryptographic keys that establish their identity within the SEALCOIN protocol.

Once integrated, devices can be registered through the SEALCOIN Platform and participate in Vertical Marketplaces corresponding to their operational capabilities. Examples include solar energy systems participating in energy markets, satellites participating in

Archived copy · cryp2nova.com

communication infrastructure markets, or sensors generating data streams within authenticated data marketplaces.

Through this integration model, manufacturers transform connected devices into economic actors capable of generating new service-based revenue streams.

10.2 Infrastructure Operators

Infrastructure operators deploy and manage physical systems that provide services within Vertical Marketplaces. These operators may manage energy networks, satellite constellations, data collection infrastructure, distributed compute resources, or other operational environments in which machines exchange services.

By deploying devices equipped with SEALCOIN Agents, infrastructure operators enable their systems to negotiate service agreements and settle transactions autonomously. For example, a satellite operator may allocate communication bandwidth dynamically through the Space Communication Marketplace, while an energy provider may allow smart meters and distributed energy resources to participate in real-time energy transactions.

Infrastructure operators may also establish private PoSy pools or restricted marketplace environments that govern the devices operating within their infrastructure. These mechanisms allow operators to implement sector-specific compliance rules and security policies while maintaining interoperability with the broader SEALCOIN ecosystem.

10.3 Autonomous AI Agents

Artificial intelligence systems represent an emerging participant category within machine economies. AI agents operating through the SEALCOIN protocol can interact with devices and services autonomously, negotiating service agreements and executing transactions without human intervention.

These AI agents may perform tasks such as resource allocation, automated service procurement, predictive infrastructure optimization, or data acquisition for analytical systems. By interacting with devices through the SEALCOIN Messaging Protocol and executing transactions through SEALCOIN Agents, AI systems can participate directly in the economic activity generated within Vertical Marketplaces.

Archived copy · cryp2nova.com

The ability of AI agents to operate as autonomous economic actors expands the potential scope of machine economies, enabling automated coordination between intelligent systems and physical infrastructure.

10.4 Enterprises and Service Providers

Enterprises and service providers participate in the SEALCOIN ecosystem by deploying infrastructure, offering services through Vertical Marketplaces, or consuming services generated by machines operating within the network.

Examples include energy providers offering electricity through distributed energy markets, satellite communication providers allocating bandwidth through the Space Communication Marketplace, or enterprises purchasing authenticated data streams for analytical and operational purposes.

Enterprises may also deploy their own networks of devices within the SEALCOIN ecosystem. These devices can operate autonomously within the economic framework provided by the protocol, enabling enterprises to automate service transactions and optimize operational efficiency.

By leveraging the capabilities of the SEALCOIN protocol, enterprises can integrate machine-driven economic activity directly into their operational infrastructure.

10.5 Developers and Technology Integrators

Developers and technology integrators contribute to the expansion of the SEALCOIN ecosystem by building software tools, integration frameworks, and applications that leverage the capabilities of the protocol.

Developers may create applications that interact with the SEALCOIN Platform registry, develop custom service negotiation algorithms executed through SEALCOIN Agents, or build analytics tools that process data generated by devices operating within the ecosystem.

Technology integrators play a critical role in connecting existing infrastructure systems with the SEALCOIN protocol. By integrating SEALCOIN-compatible identity frameworks and agent software into existing devices or enterprise systems, integrators facilitate the adoption of autonomous machine transactions across multiple industries.

Archived copy · cryp2nova.com

10.6 Device Owners and Individual Participants

Individual device owners represent an important participant group in the emerging machine economy. As consumer devices increasingly incorporate secure identity and connectivity features, individuals may deploy devices capable of participating in Vertical Marketplaces.

Examples include electric vehicle owners whose vehicles participate in energy transactions, users contributing computing capacity through personal computers in distributed compute marketplaces, or individuals operating sensor networks that generate authenticated data streams.

Through the SEALCOIN ecosystem, individual participants can monetize the capabilities of their devices while contributing to the broader infrastructure of decentralized machine economies.

10.7 Collaborative Ecosystem Dynamics

The SEALCOIN ecosystem operates through the interaction of these participant categories within a shared technological and economic framework. Devices, infrastructure operators, AI agents, enterprises, developers, and individual participants contribute complementary capabilities that together enable the operation of decentralized machine marketplaces.

By combining secure device identity, programmable service negotiation, and token-based economic settlement, the SEALCOIN protocol enables a collaborative environment in which machines and organizations can exchange services efficiently and securely.

As the number of connected devices and autonomous systems continues to grow, the participation of diverse ecosystem actors will play a critical role in expanding the scale and functionality of the SEALCOIN machine economy.

Archived copy · cryp2nova.com

11. Development Roadmap

The development of the SEALCOIN ecosystem follows a pragmatic deployment approach focused on progressively enabling real-world machine transactions. Rather than presenting a purely theoretical roadmap, the SEALCOIN project has already reached several operational milestones that demonstrate the feasibility of its architecture.

The ecosystem development began with the implementation of the core protocol infrastructure, including the SEALCOIN Platform, the SEALCOIN Agent architecture, and the integration of decentralized settlement capabilities. These foundational components enable devices to establish secure identities, negotiate services, and execute economic transactions autonomously.

The first operational milestone of this architecture was the launch of the **SEALCOIN Platform Minimum Viable Product (MVP) in January 2025**, which introduced the initial operational interface allowing organizations to onboard devices, and manage certificates. The first official version of the platform was released in October 2025, including additional features such as marketplace and PoSy functionalities, and using the QAIT token issued on the Hedera mainnet.

This platform represents the first functional layer of the machine economy infrastructure described throughout this whitepaper. It demonstrates how the protocol, platform, agent, and token mechanisms interact in practice to support device authentication, secure onboarding, and economic activity across the ecosystem.

CRYP2NOVA

Archived copy · cryp2nova.com

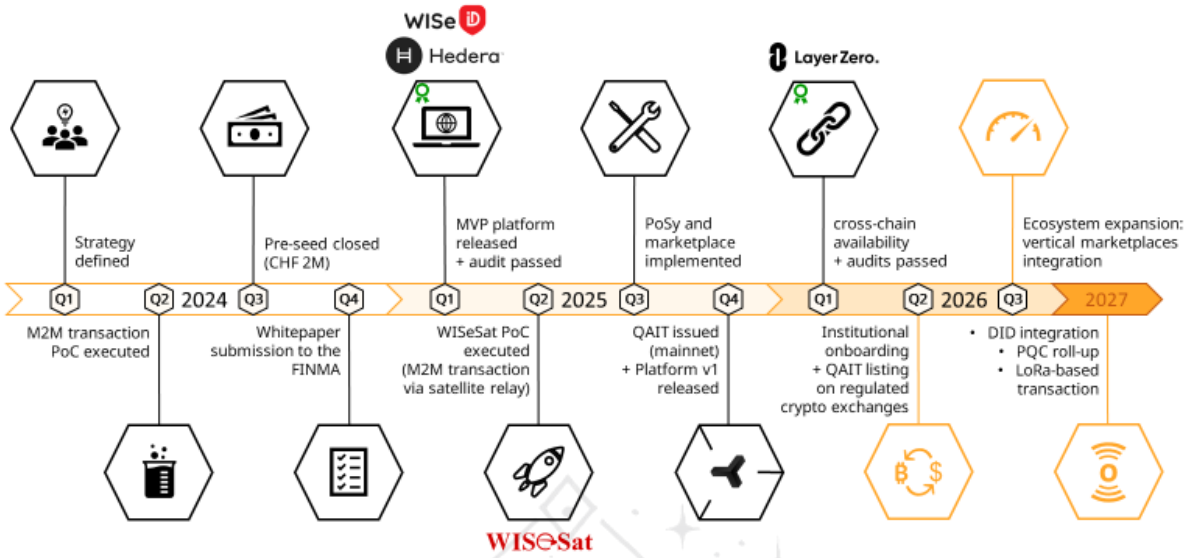


Figure 5: Sealcoin Roadmap

11.1 SEALCOIN Platform

The platform acts as the operational gateway through which users interact with the SEALCOIN protocol. Through this interface, organizations can configure devices, manage cryptographic identities, and monitor economic activity generated by machines operating within the network.

At the core of the platform architecture is a modular design that reflects the lifecycle of transactional IoT deployments. Devices are onboarded, secured through certificates, linked to PoSy pools where applicable, and ultimately connected to marketplace environments where they can exchange services and data.

CRYP2NOVA

Archived copy · cryp2nova.com

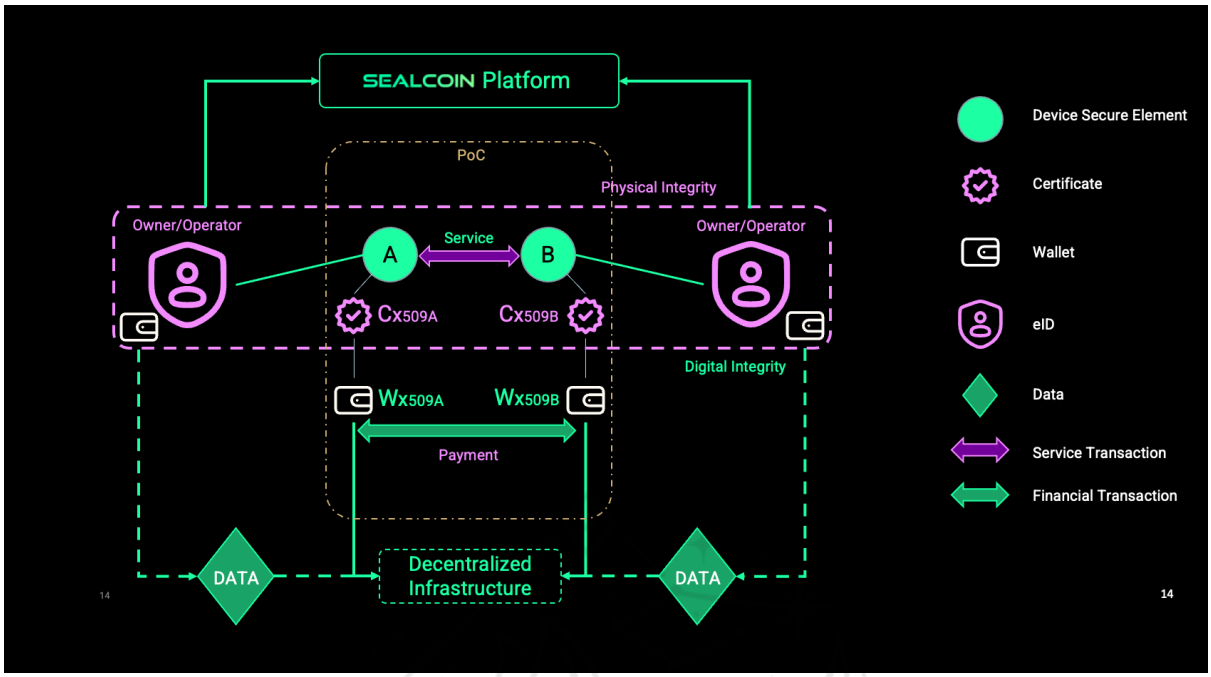


Figure 6: Illustration of Sealcoin PoC Ecosystem

11.2 Wallet and Deposit Workflow

Participation in the SEALCOIN ecosystem requires organizations to maintain token balances that enable operational activities such as device registration, certificate issuance, and marketplace transactions.

Within the platform, organizations are provided with integrated wallet functionality allowing them to manage their token balances and prepare for on-ledger transactions. The wallet interface supports the management of both QAIT tokens and network transaction tokens used for distributed ledger operations.

The deposit workflow enables users to transfer tokens into their platform wallets in order to activate operational capabilities. Once tokens are available within the wallet environment, they can be allocated to activities such as certificate issuance, participation in PoSy pools, or marketplace service transactions.

This mechanism ensures that all economic actions executed through the platform remain cryptographically verifiable and transparently recorded within the underlying distributed ledger environment.

Archived copy · cryp2nova.com

11.3 Platform Dashboard and Operational Visibility

The SEALCOIN Platform provides an operational dashboard that gives organizations immediate visibility into their ecosystem activity.

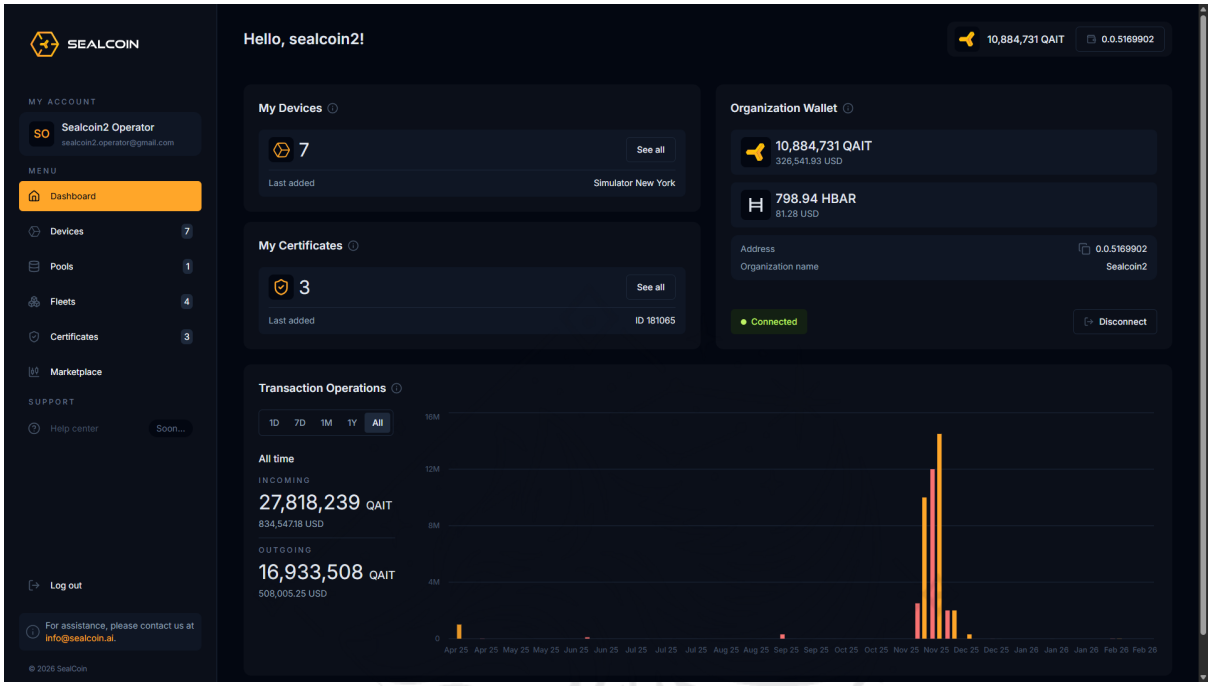


Figure 7: Screenshot of Sealcoin Platform Dashboard Page

Through the dashboard interface, users can monitor wallet balances, including QAIT and ledger transaction tokens, ensuring that sufficient resources are available for device onboarding and marketplace participation. The dashboard also displays the connectivity status of the organization's infrastructure, allowing operators to verify that devices and agents remain properly connected to the network.

Operational metrics presented on the dashboard include the number of registered devices, issued certificates, and recent transaction activity. These metrics can be observed across selectable time ranges, enabling organizations to monitor ecosystem participation and machine transaction throughput.

This interface provides organizations with a high-level operational overview of their participation within the SEALCOIN ecosystem.

Archived copy · cryp2nova.com

11.4 Device Registry and Device Lifecycle Management

Device management is handled through a dedicated registry within the SEALCOIN Platform. This registry enables organizations to onboard and manage devices that will participate in machine-to-machine transactions within the ecosystem.

Devices are registered with the connectivity and identity attributes required for operational participation. Once registered, devices can be associated with certificates, linked to PoSy pools when applicable, and integrated into marketplace environments aligned with their capabilities.

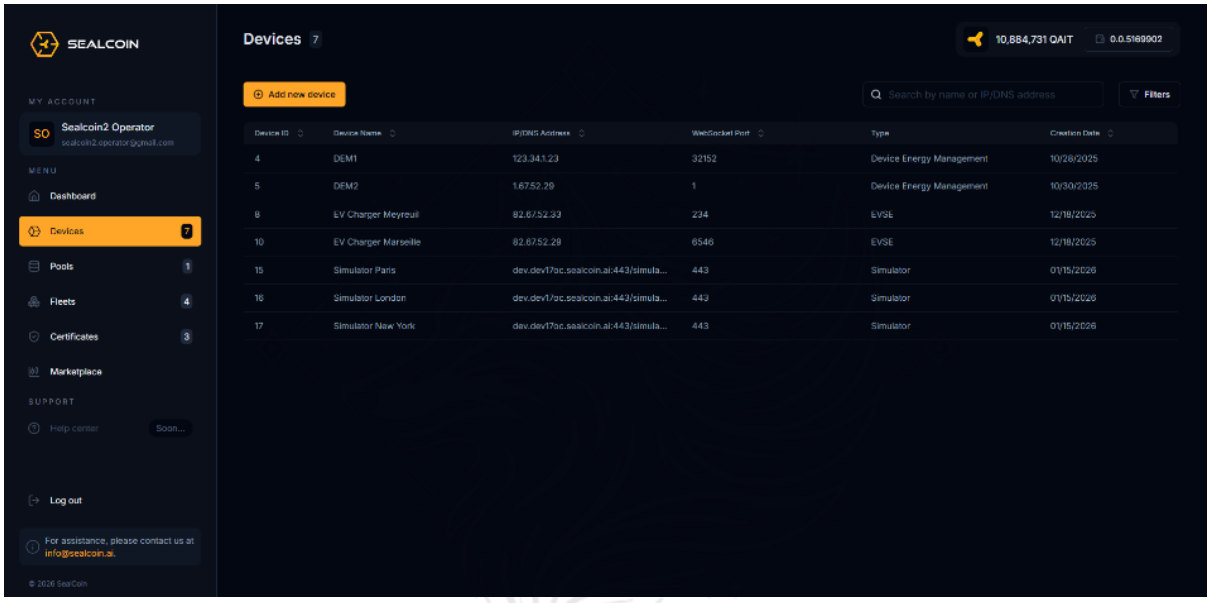


Figure 8: Screenshot of Sealcoin Platform Devices Page

The device registry therefore acts as the foundation for controlled device onboarding within the SEALCOIN ecosystem. It provides organizations with a structured interface through which the lifecycle of their connected infrastructure can be managed.

11.5 Certificate Management

Certificates represent a critical security element within the SEALCOIN architecture. Devices must possess valid authentication certificates before they can interact with other machines or participate in marketplace activity.

Archived copy · cryp2nova.com

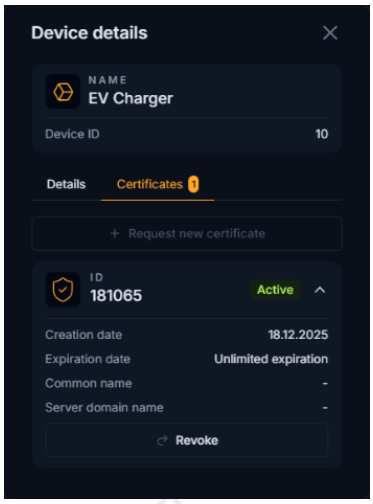


Figure 9: Screenshot of Sealcoin Device Details Modal

The platform includes certificate management capabilities that allow organizations to track issued certificates and manage the security posture of their devices. Certificates are treated as operational assets within the platform, enabling organizations to monitor certificate issuance, expiration, and usage.

By integrating certificate management directly into the platform interface, SEALCOIN ensures that device identity and authentication remain central to the operational lifecycle of the ecosystem.

11.6 Proof-of-Security Pool Participation

The SEALCOIN Platform provides a dedicated interface through which users can interact with Proof-of-Security pools.

Through the Pools module, users can discover available pools, evaluate pool participation conditions, and monitor pool occupancy. The interface provides visibility into the user's participation status within a pool, including the quantity of tokens locked, the number of secured devices associated with the pool, and the rewards generated through device activity.

Operational actions such as claiming rewards or withdrawing participation (when permitted under the pool's rules) can also be performed through this module.

Archived copy · cryp2nova.com

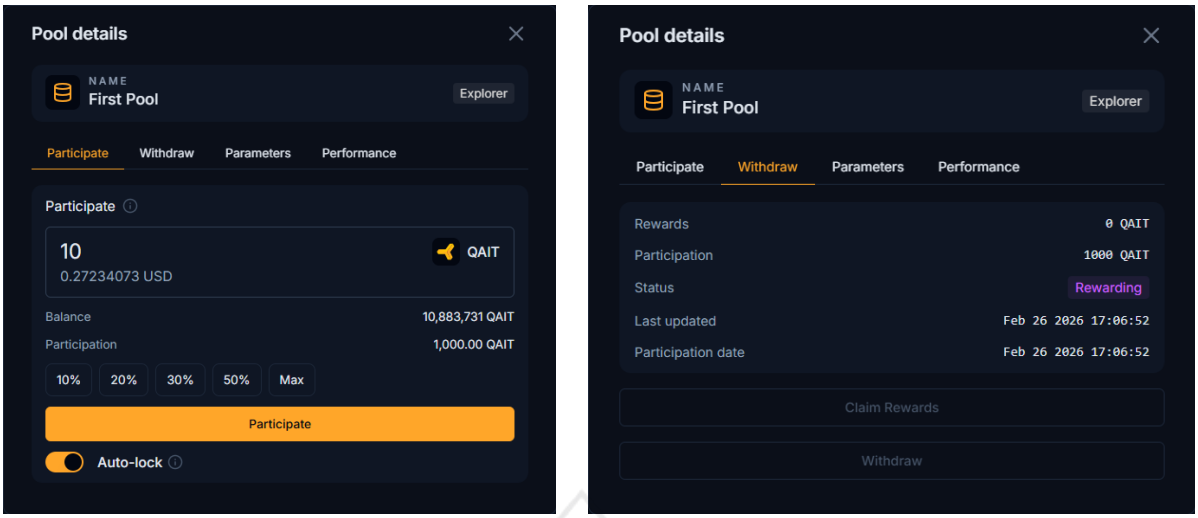


Figure 10: Screenshots of the Pool participation and Pool details Tabs

This functionality connects the PoSy security framework with concrete operational workflows, enabling participants to actively manage the security commitments associated with device onboarding.

11.7 Marketplace Interface

The Marketplace module of the SEALCOIN Platform provides the interface through which service trading occurs within the ecosystem.

Services available within the marketplace are aligned with device types and service categories defined by the Vertical Marketplace architecture. Users can filter available services according to device type, service category, or pricing conditions.

The interface allows participants to observe current pricing levels, review the order book for buy and sell offers, and manage their organization's active orders. Through this environment, organizations can publish service offers or procure services generated by other devices operating within the ecosystem.

Archived copy · cryp2nova.com

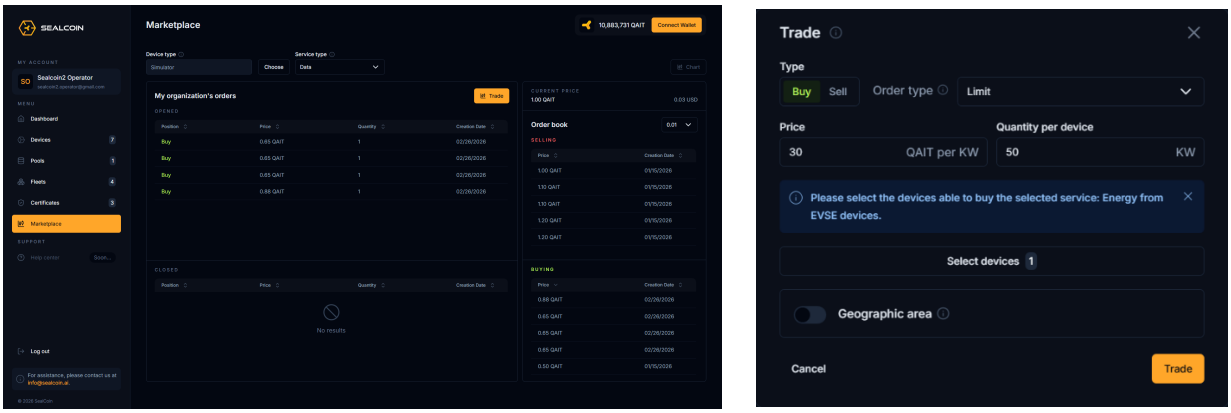


Figure 11: Screenshots of the Marketplace page and Trade form

The marketplace interface therefore enables practical service trading workflows for machine-to-machine service exchange while maintaining transparent price discovery mechanisms.

11.8 Future Platform Evolution

While the platform demonstrates the operational foundation of the SEALCOIN ecosystem, it will continue to evolve as additional device categories and Vertical Marketplaces are integrated.

Future development will focus on expanding device onboarding capabilities, improving automation of machine-to-machine transaction workflows, and strengthening interoperability between Vertical Marketplaces. As the number of connected devices operating through SEALCOIN Agents increases, the platform will support progressively larger volumes of autonomous service transactions.

Through this phased development approach, the SEALCOIN Platform is expected to evolve from an operational management interface into a global infrastructure layer supporting autonomous machine economies across multiple industries.

Archived copy · cryp2nova.com

12. QAIT Token Generation and Distribution

The QAIT token constitutes the settlement asset used within the SEALCOIN ecosystem. While the economic functions of the token, including service settlement, Proof-of-Security (PoSy) participation, and marketplace transactions, are described in Section 6, this section defines the structure through which the token supply is issued and distributed.

The QAIT token supply is fixed and subject to predefined allocation and release mechanisms designed to support the long-term growth of the SEALCOIN ecosystem. The token generation framework ensures that ecosystem incentives, protocol development, and marketplace expansion can be supported while maintaining predictable supply dynamics.

The issuance and distribution of QAIT tokens are governed by the **QAIT Association**, which supervises token supply management, incentive mechanisms, and economic policies associated with the token.

12.1 Token Generation Event

The QAIT Token Generation Event (TGE) represents the initial creation of the token supply used within the SEALCOIN ecosystem.

At the time of the TGE, the total token supply is minted according to predefined parameters and distributed across multiple allocation categories supporting ecosystem development, network participation, infrastructure expansion, and community engagement.

The TGE establishes the initial circulating supply of QAIT while the remaining tokens are released progressively according to structured distribution schedules. These mechanisms are designed to align long-term incentives between ecosystem participants and ensure that token availability evolves in parallel with the growth of the SEALCOIN network.

The QAIT token is defined with the following parameters:
Maximum Supply: **10,000,000,000 QAIT**
Token Symbol: **QAIT**
Initial Reference Price: **1 QAIT = 0.002 USD**

The maximum supply of QAIT tokens is fixed and no additional tokens will be created beyond this cap.

Archived copy · cryp2nova.com

12.2 Token Allocation

The total QAIT supply is distributed across several allocation categories that support the development, operation, and expansion of the SEALCOIN ecosystem.

The allocation model ensures that a significant portion of tokens is dedicated to ecosystem development and marketplace participation while maintaining long-term alignment between contributors, investors, and community participants.

The token allocation is defined as follows:

	QAIT in %
Founders & Team	18.00%
Investors	10.00%
Ecosystem & Community	29.50%
Protocol Development	20.00%
Treasury	18.50%
Advisors	2.00%
Liquidity	2.00%

Table: Representation of QAIT distribution

CRYP2NOVA

Archived copy · cryp2nova.com

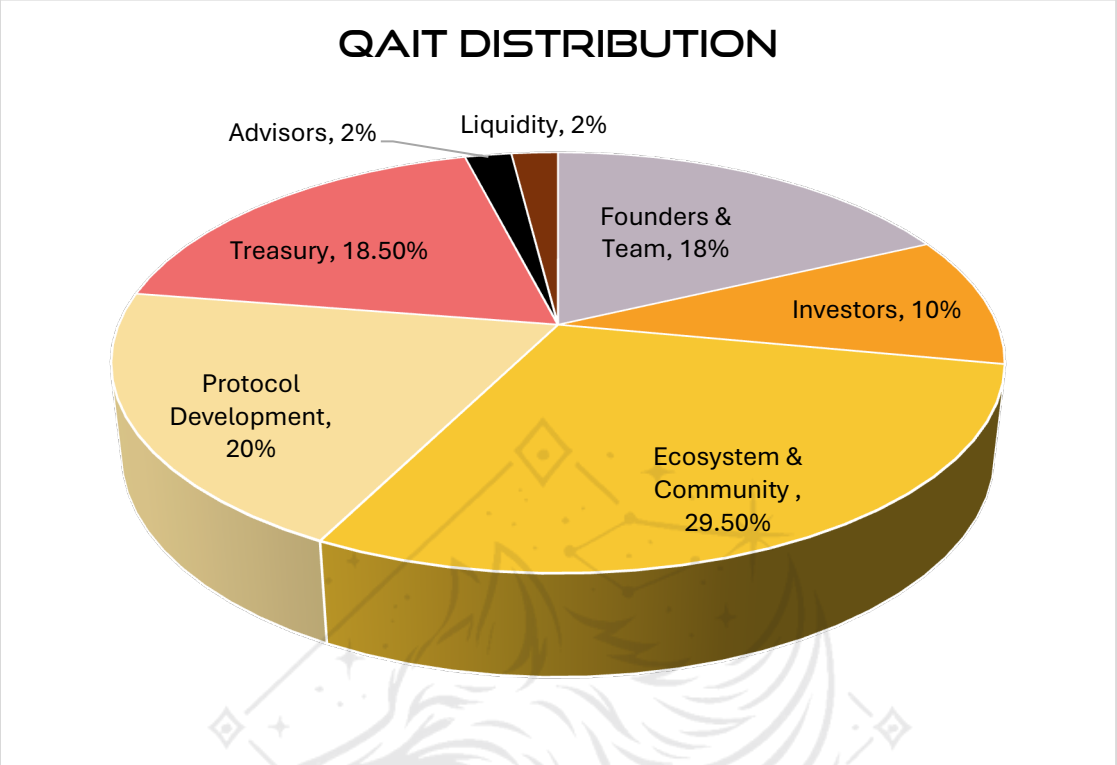


Figure 12: Pie chart representation of QAIT distribution

This distribution structure allocates a majority of tokens to ecosystem growth, marketplace expansion, and community participation while maintaining appropriate allocations for development teams and early contributors to the project.

CRYP2NOVA

12.3 Allocation Breakdown

Founders and Team (18%)

Tokens allocated to founders and the core development team recognize their role in designing and building the SEALCOIN protocol and its associated infrastructure.

These tokens are subject to a **12-month cliff from the Token Generation Event**, followed by a **24-month vesting period**. This structure aligns the incentives of the development team with the long-term evolution of the ecosystem.

Archived copy · cryp2nova.com

Investors (10%)

This allocation recognizes early participants who supported the development of the SEALCOIN ecosystem during its early phases.

Investor allocations are subject to a **12-month cliff**, followed by a **24-month vesting schedule**. This mechanism ensures that early investors participate in the long-term growth of the ecosystem while avoiding excessive early token circulation.

Ecosystem & Community (29.50%)

Tokens allocated to the Ecosystem and Community provide broad access to the SEALCOIN ecosystem.

A gradual portion of these tokens become **fully liquid at the Token Generation Event**, enabling participants to engage directly with the network through marketplace activity, PoSy participation, and other ecosystem interactions.

Protocol Development (20%)

This allocation supports the continued expansion of the SEALCOIN ecosystem.

Tokens in this category may be used to support partnerships, infrastructure integrations, protocol development initiatives, and the deployment of services across the Vertical Marketplaces.

These tokens are **available from the Token Generation Event**, enabling the ecosystem to scale as new integrations and infrastructure deployments occur.

Treasury (18.50%)

The treasury allocation supports operational and strategic activities required for the long-term development of the ecosystem.

Treasury funds may be used to support operational infrastructure, liquidity management, ecosystem expansion initiatives, and other strategic activities necessary for maintaining the SEALCOIN platform and marketplace infrastructure.

These tokens are **available at the Token Generation Event** and are managed according to governance frameworks defined by the ecosystem.

Archived copy · cryp2nova.com

Advisors (2%)

Advisor allocations recognize the contributions of individuals providing strategic guidance and domain expertise to the development of the SEALCOIN ecosystem.

Advisor tokens are subject to a **12-month cliff**, followed by a **24-month vesting period**, ensuring long-term alignment between advisors and the ecosystem's development.

Liquidity (2%)

The Liquidity allocation is dedicated to supporting the orderly launch, trading, and ongoing market development of QAIT across centralized and decentralized trading venues.

These tokens may be used to provide initial liquidity at the Token Generation Event (TGE), support exchange listings, facilitate market-making activities, improve trading efficiency, and maintain adequate liquidity conditions as the QAIT ecosystem expands.

This allocation is intended to promote healthy price discovery, reduce market friction, and support continued access to QAIT for ecosystem participants, partners, and investors throughout the token's lifecycle.

This allocation becomes available **immediately following the Token Generation Event**.

12.4 Emission and Vesting Structure

To maintain economic stability and prevent excessive early token circulation, certain allocation categories are subject to vesting schedules that release tokens progressively over time.

These schedules combine a **cliff period**, during which no tokens are released, with a **vesting period**, during which tokens unlock gradually according to predefined timelines.

The vesting structure for the principal allocation categories is summarized below:

Archived copy · cryp2nova.com

	Cliff from TGE in months	**Vesting from Cliff end** in months
Founders & Team	12	24
Investors	12	24
Ecosystem & Community	N/A	N/A
Protocol Development	N/A	N/A
Treasury	N/A	N/A
Advisors	12	24
Liquidity	N/A	N/A

Table 2: Representation of Cliff and Vesting Periods

A cliff represents the minimum period after the Token Generation Event during which no tokens are distributed. Once the cliff period ends, tokens are gradually released throughout the vesting period until the full allocation becomes available.

This distribution model ensures that the circulating supply of QAIT tokens grows progressively alongside the expansion of the SEALCOIN ecosystem, reducing the risk of supply shocks while maintaining long-term alignment between ecosystem stakeholders.

CRYP2NOVA

Archived copy · cryp2nova.com

13. Ecosystem Partnerships

The development and deployment of the SEALCOIN ecosystem relies on collaboration with technology providers, infrastructure operators, device manufacturers, and industry partners that contribute complementary capabilities to the machine economy architecture.

These partnerships enable the integration of secure device identity, trusted data generation, decentralized infrastructure, and real-world service deployment across the Vertical Marketplaces described in this whitepaper. Through these collaborations, the SEALCOIN protocol connects to operational environments in which machines and AI agents can execute autonomous economic transactions.

Partners contribute expertise in areas such as hardware security, satellite communications, distributed ledger infrastructure, IoT device manufacturing, and digital trust services. Together they form a growing ecosystem supporting the deployment of authenticated devices, decentralized marketplaces, and machine-to-machine economic activity.

13.1 WISeKey

WISeKey International Holding Ltd. is a cybersecurity and digital identity company specializing in trusted digital infrastructure, cryptographic identity management, and secure hardware technologies.

Within the SEALCOIN ecosystem, WISeKey contributes expertise in digital identity frameworks and trust infrastructure. Its technologies support the creation and management of secure digital identities that allow devices and services to authenticate themselves within distributed environments.

These capabilities are directly aligned with the identity architecture underpinning the SEALCOIN protocol. By enabling secure device authentication and identity verification mechanisms, WISeKey contributes to the development of trusted machine identities required for secure autonomous transactions.

13.2 WISeSat.Space

WISeSat.Space operates satellite infrastructure designed to support secure communications, IoT connectivity, and space-based data services.

Archived copy · cryp2nova.com

Within the SEALCOIN ecosystem, WISeSat.Space contributes to orbital infrastructure that can participate in decentralized machine marketplaces. Satellites equipped with secure device identity frameworks and compatible agent software can operate as autonomous service providers capable of delivering communication services and transmitting authenticated data streams.

This infrastructure supports the development of the **Space Communication Marketplace**, where communication capacity and satellite services can be dynamically allocated and transacted between connected devices and network participants.

Through this integration, space-based infrastructure becomes part of the broader machine economy enabled by the SEALCOIN protocol.

13.3 SEALSQ

SEALSQ is a semiconductor and cybersecurity technology company specializing in secure microcontrollers, cryptographic hardware, and post-quantum security technologies.

The company develops secure semiconductor platforms designed to protect cryptographic keys and digital identities within connected devices. These platforms incorporate advanced hardware-level security mechanisms intended to resist tampering and cyber-attacks while ensuring the integrity of device identities.

Within the SEALCOIN ecosystem, SEALSQ contributes with hardware-rooted security technologies that enable devices to generate and protect cryptographic identities. These identities form the basis for device authentication and secure participation within the SEALCOIN protocol.

SEALSQ also provides scalable public key infrastructure services capable of issuing and managing digital certificates for large populations of connected devices. These capabilities support device onboarding and identity lifecycle management across the SEALCOIN network.

By combining secure semiconductors with scalable identity infrastructure, SEALSQ strengthens the hardware trust layer required for autonomous machine transactions.

Archived copy · cryp2nova.com

13.4 Hedera Hashgraph LLC

Hedera Hashgraph LLC operates a distributed ledger technology platform built on the Hashgraph consensus algorithm.

The Hedera network is governed by the Hedera Governing Council, a decentralized group of global organizations responsible for overseeing the stability and development of the network. This governance structure ensures distributed oversight of the platform while maintaining enterprise-grade reliability.

Within the SEALCOIN ecosystem, Hedera provides the distributed ledger infrastructure used to record transactions, manage digital assets, and provide consensus services.

The SEALCOIN protocol leverages Hedera's network to ensure that machine-to-machine transactions are securely recorded and verifiable. Hedera's Token Service supports the creation and management of the QAIT token used for settlement within the ecosystem, while the Consensus Service provides trusted timestamping and ordering of transaction events.

These capabilities enable scalable, low-latency transaction processing while maintaining the transparency and immutability required for decentralized machine economies.

13.5 The Hashgraph Group

The Hashgraph Group AG (THG), headquartered in Zug, Switzerland, focuses on accelerating enterprise adoption of Hedera Hashgraph distributed ledger technologies.

The organization works with enterprises, startups, and public institutions to support the development and deployment of decentralized applications built on the Hedera network. Its activities include technical advisory services, ecosystem development initiatives, and strategic support for projects integrating distributed ledger technologies.

Within the SEALCOIN ecosystem, The Hashgraph Group contributes technical and strategic support to the development of the platform. This includes guidance on distributed architecture design, smart contract integration, and alignment with the Hedera technology stack.

The Hashgraph Group also facilitates integration with the broader Hedera ecosystem by connecting SEALCOIN with developers, partners, and enterprises building on the network. These activities support the expansion of decentralized infrastructure initiatives and the adoption of machine-to-machine transactional systems enabled by the SEALCOIN protocol.

Archived copy · cryp2nova.com

14. Conclusion

The rapid expansion of connected devices, artificial intelligence systems, and distributed digital infrastructure is transforming the nature of economic activity. Machines are no longer passive tools within digital systems; they are increasingly capable of operating autonomously, generating data, consuming resources, and executing services without continuous human intervention.

The emergence of this new machine-driven environment requires infrastructure capable of supporting trusted interactions between autonomous systems. Identity, authentication, secure communication, and reliable transaction settlement must be embedded directly into the technological fabric that connects devices and services.

The SEALCOIN protocol addresses this challenge by establishing a secure and programmable infrastructure designed specifically for machine-to-machine economic activity. Through the integration of cryptographic device identity, hardware-rooted trust models, decentralized transaction settlement, and marketplace-based service discovery, the protocol enables authenticated machines and AI agents to participate as autonomous economic actors.

By structuring economic activity through Vertical Marketplaces, SEALCOIN provides a framework in which sector-specific machine economies can develop while operating on a shared technological backbone. Space communication infrastructure, distributed energy systems, authenticated data markets, and decentralized compute networks represent early examples of how machines can exchange services and resources within such environments.

The QAIT token complements this architecture by providing a programmable settlement mechanism that enables automated transactions across the ecosystem. By combining fiat-denominated service pricing with token-based settlement, the protocol preserves economic clarity for enterprises while enabling efficient decentralized transactions.

Governance of the ecosystem is structured to support long-term sustainability. The SEALCOIN platform provides the technological infrastructure enabling device interaction and marketplace functionality, while the QAIT Association oversees the economic layer and the responsible evolution of the token economy. This institutional structure enables technological innovation to progress alongside transparent and accountable economic governance.

As the number of connected devices continues to expand globally, the need for secure, autonomous machine interaction will become increasingly critical. Infrastructure capable

Archived copy · cryp2nova.com

of supporting trusted machine identities, verifiable data generation, and decentralized service transactions will form a foundational layer of the next generation of digital economies.

The SEALCOIN ecosystem is designed to contribute to this transformation by providing the infrastructure through which machines, devices, and AI agents can securely discover services, negotiate value, and settle transactions across decentralized networks.

In doing so, SEALCOIN aims to support the emergence of a new economic paradigm in which autonomous systems participate directly in global digital markets.

CRYP2NOVA

Archived copy · cryp2nova.com

15. Appendices

15.1 Glossary

Agent (SEALCOIN Agent)

A software component installed on a device or system that enables it to participate autonomously in the SEALCOIN ecosystem. The Agent manages the device's cryptographic identity, wallet, and secure communications, allowing it to discover services, negotiate transaction parameters, and execute machine-to-machine transactions.

Anti-Money Laundering (AML)

Regulatory frameworks designed to prevent financial crimes such as money laundering and illicit financing. The SEALCOIN ecosystem supports AML compliance through identity verification and transaction monitoring procedures where required.

Autonomous Economic Agent

A connected device or AI system capable of independently discovering services, negotiating transaction terms, and executing payments within the SEALCOIN ecosystem.

Certificate (Operational Certificate)

A digital certificate used to authenticate the identity of a device or agent participating in the SEALCOIN ecosystem. Certificates are issued through Public Key Infrastructure (PKI) mechanisms and enable secure communication and transaction verification.

Cliff

In the context of token distribution or vesting schedules, a cliff is the minimum period during which allocated tokens cannot be accessed or released.

Connectivity Standards Alliance (CSA)

Archived copy · cryp2nova.com

An industry organization that develops interoperability standards for connected devices, including the Matter protocol, enabling secure and reliable communication across IoT systems.

Decentralized Autonomous Organization (DAO)

An organizational structure governed by smart contracts and decentralized voting mechanisms where participants collectively manage decisions through distributed governance processes.

Decentralized Identity (DID)

A digital identity model that allows individuals, organizations, or devices to manage their identity credentials independently from centralized authorities.

Decentralized Marketplace

A marketplace infrastructure where services, data, or resources can be exchanged directly between participants without centralized intermediaries.

Decentralized Physical Infrastructure Networks (DePIN)

A model where physical infrastructure systems such as sensors, connectivity nodes, or compute resources are coordinated through decentralized technologies.

Device Identity Layer

The architectural layer responsible for managing cryptographic identities of devices participating in the SEALCOIN ecosystem using certificates and cryptographic keys.

Device Onboarding

The process through which a device securely registers on the SEALCOIN platform, receives authentication credentials, and becomes authorized to interact with other devices and services.

Archived copy · cryp2nova.com

Device Trust Layer

The foundational security layer that establishes trust in participating devices through hardware security components, trusted execution environments, and certificate-based authentication.

Distributed Compute Marketplace

A SEALCOIN Vertical Marketplace where computing resources such as CPUs, GPUs, and edge computing devices can be shared and monetized by participating devices.

Distributed Ledger Technology (DLT)

A decentralized database architecture in which transaction records are maintained across multiple nodes, ensuring transparency, immutability, and security.

Elliptic Curve Cryptography (ECC)

A public-key cryptographic method commonly used to secure digital communications and distributed ledger transactions.

Energy and Electric Mobility Marketplace

A SEALCOIN Vertical Marketplace where devices such as solar panels, smart meters, batteries, electric vehicles, and charging stations can exchange energy services and settle transactions autonomously.

Fiat-Denominated Pricing

A pricing model used within the SEALCOIN ecosystem where services and data are priced in fiat currencies while settlement occurs using QAIT tokens.

Global System for Mobile Communications Association (GSMA)

Archived copy · cryp2nova.com

An industry organization representing mobile network operators and developing standards for mobile connectivity, identity, and security.

Hardware Root of Trust (RoT)

A hardware-based security mechanism that securely stores cryptographic keys and provides the trusted foundation for device authentication.

Hedera

A public distributed ledger network based on the Hashgraph consensus algorithm, providing high-throughput infrastructure for decentralized applications and tokenized assets.

Know Your Customer (KYC)

A regulatory process used to verify the identity of participants in order to prevent fraud and financial crime.

Machine Economy

An economic framework in which connected devices and AI agents autonomously exchange services, data, and resources through digital transactions.

Machine-to-Machine Transactions (M2M Transactions)

Automated transactions executed directly between devices or AI agents without human intervention.

Marketplace Architecture Model

The layered framework used by SEALCOIN to structure Vertical Marketplaces, including device trust, certified devices, business logic, token economics, and service discovery layers.

Archived copy · cryp2nova.com

Multi-Party Computation (MPC)

A cryptographic method allowing multiple parties to jointly compute functions while keeping their individual inputs private.

Premium Data Marketplace

A SEALCOIN Vertical Marketplace where authenticated machine-generated data can be securely exchanged as a digital asset.

Proof-of-Security (PoSy)

A security framework within the SEALCOIN ecosystem enabling large-scale onboarding of trusted devices and AI agents through prevalidated security pools. Participants lock QAIT tokens to obtain onboarding capacity and contribute to network security.

Public Key Infrastructure (PKI)

A cryptographic system that manages digital keys and certificates used to authenticate devices and secure communications.

QAIT Token

The native settlement token of the SEALCOIN ecosystem used for machine-to-machine transactions, PoSy participation, and economic coordination across vertical marketplaces.

Root of Trust (RoT)

The foundational security component in a device or system that securely manages cryptographic keys and enables trusted authentication.

Secure Element (SE)

A tamper-resistant hardware component designed to securely store cryptographic keys and execute security-sensitive operations.

Archived copy · cryp2nova.com

SEALCOIN Messaging Protocol

A standardized off-chain communication protocol enabling SEALCOIN Agents to discover services, negotiate transaction parameters, and coordinate machine-to-machine transactions.

SEALCOIN Platform

The operational environment through which users onboard devices, manage certificates, access vertical marketplaces, and monitor ecosystem activity.

SEALCOIN Protocol

The overarching framework enabling secure identity management, messaging, and economic transactions between devices and AI agents.

Service Discovery Layer

The system enabling devices to locate and identify available services offered by other devices within the SEALCOIN ecosystem.

Smart Contracts

Self-executing programs deployed on distributed ledger networks that automatically enforce predefined conditions of a transaction or agreement.

Space Communication Marketplace

A SEALCOIN Vertical Marketplace dedicated to satellite communication services where satellites and ground stations exchange communication bandwidth, relay services, and data.

Token Generation Event (TGE)

Archived copy · cryp2nova.com

The event marking the initial issuance and distribution of the QAIT token.

Tokenomics

The economic design governing the supply, distribution, incentives, and role of a token within a digital ecosystem.

Transport Layer Security (TLS)

A cryptographic protocol used to secure communications between systems through encrypted data exchange.

Trusted Execution Environment (TEE)

A secure area within a processor that isolates sensitive computations from the main operating system.

Utility Payment

The use of a digital token to pay for services within a platform or ecosystem.

Vertical Marketplace

A sector-specific marketplace within the SEALCOIN ecosystem where devices exchange services related to a particular industry such as space communications, energy and mobility, premium data, or distributed computing.

Vesting Period

The time period during which allocated tokens are gradually released according to a predefined schedule.

WebSocket Secure (WSS)

Archived copy · cryp2nova.com

A secure protocol enabling real-time, encrypted communication between systems over persistent network connections.

15.2 Legal Disclaimer

This whitepaper has been prepared for informational purposes only and describes the vision, architecture, and proposed economic framework of the SEALCOIN ecosystem. The document is provided solely to assist readers in understanding the technology and the intended development of the SEALCOIN protocol and associated infrastructure.

This whitepaper does not constitute a prospectus, an offer to sell, or a solicitation to purchase any securities, financial instruments, or regulated investment products in any jurisdiction. Nothing contained in this document should be interpreted as legal, financial, tax, or investment advice.

The QAIT token is intended to function as a utility and settlement token within the SEALCOIN ecosystem. Ownership of QAIT tokens does not grant any ownership rights, equity participation, dividend rights, or governance rights in SEALCOIN AG, the QAIT Association, or any affiliated entity unless explicitly stated in applicable governance documentation.

The information contained in this document reflects the current design intentions of the project and may be subject to modification, updates, or revisions as the technology and ecosystem evolve. No representation or warranty is made as to the accuracy, completeness, or future performance of the concepts described.

This whitepaper may contain forward-looking statements relating to future developments of the SEALCOIN ecosystem, including anticipated technological capabilities, marketplace adoption, and ecosystem growth. Such statements are based on current expectations and assumptions and involve known and unknown risks and uncertainties that may cause actual outcomes to differ materially.

Participation in token-based ecosystems and decentralized networks involves inherent technological, operational, and regulatory risks. Prospective participants should carefully evaluate these risks and consult independent professional advisors before making any decisions relating to digital assets or decentralized technologies.

Nothing in this document should be interpreted as regulatory approval or endorsement by any authority. Regulatory treatment of digital assets varies across jurisdictions and participants are responsible for ensuring compliance with applicable laws

Archived copy · cryp2nova.com