

LIGHT PAPER

**SEALCOIN**

A Revolution in Transactional-IoT

# SEALCOIN WHITEPAPER

## Table of Contents

Light Paper .....	1
<b>EXECUTIVE SUMMARY .....</b>	<b>3</b>
<b>INTRODUCTION .....</b>	<b>4</b>
Historical Background.....	4
Introduction .....	4
Proof-of-Concept .....	5
<b>A COMPREHENSIVE SERVICE PLATFORM.....</b>	<b>7</b>
<b>SEALCOIN TOKEN .....</b>	<b>8</b>
1. Utility .....	8
2. Payment.....	8
Tokenomics .....	9
<b>USE CASES (DEPIN).....</b>	<b>10</b>
EV Charging .....	10
Vehicle Sharing.....	10
Energy Trading .....	10
Fleet Management → opportunities (customer services, cost reduction) and Industrial IoT.....	10
Autonomous Transportation .....	10
Autonomous Delivery.....	10
Autonomous Devices' transactions (Smart Home Automation).....	10
Data Trading .....	10
Sensors Monitoring (Supply Chain Management).....	10
Communication Networks (autonomous routers) .....	10
Health Trackers .....	10
Tracking services.....	10
<b>GOVERNANCE .....</b>	<b>11</b>
<b>PARTNERS .....</b>	<b>12</b>
Web3 .....	12
Traditional .....	12

# EXECUTIVE SUMMARY

**SEALCOIN** introduces a revolutionary services platform designed to empower devices within the Internet of Things (IoT) ecosystem to autonomously transact and coordinate service-for-payment exchanges. At the heart of this ecosystem lies its dedicated utility token, **SEALCOIN**, which serves as the primary medium for facilitating transactions and interactions among devices and participants.

The **SEALCOIN** platform addresses the growing need for seamless and secure transactions within the IoT landscape (Transactional IoT or t-IoT), where devices increasingly rely on interconnected services for their functionality. By leveraging blockchain or Decentralized Ledger Technology and smart contracts, **SEALCOIN** offers the access to a decentralized infrastructure that enables devices to negotiate, execute, and settle transactions independently, without the need for human intervention.

Key features of the SEALCOIN platform include:

- **Autonomous Transaction Facilitation:** **SEALCOIN** empowers IoT devices to initiate and complete transactions autonomously, streamlining the process of service provision and payment settlement.
- **Smart Contract Integration:** Through the utilization of smart contracts, **SEALCOIN** ensures the secure and transparent execution of agreements between parties, enhancing trust and reducing transactional friction.
- **Enhanced Security and Privacy:** **SEALCOIN** leverages blockchain technology to provide robust security measures and safeguard sensitive data in the digital realm, ensuring the integrity and confidentiality of transactions within the ecosystem, secured physically through the Secure Element of a device.
- **Scalability and Interoperability:** With a focus on scalability and interoperability, **SEALCOIN** aims to support a diverse range of IoT devices and services, facilitating seamless integration and interaction across various platforms and protocols.
- **Global Accessibility:** **SEALCOIN's** utility token serves as a universal medium of exchange within the platform, enabling seamless transactions and interactions among IoT devices and participants worldwide.

In summary, **SEALCOIN** represents a groundbreaking solution that harnesses the power of blockchain technology to revolutionize transactions within the IoT ecosystem. By enabling devices to transact autonomously and organize service-for-payment exchanges, **SEALCOIN** paves the way for a more efficient, secure, and interconnected future for t-IoT stakeholders.

# INTRODUCTION

## HISTORICAL BACKGROUND

SEALSQ is one of the very few semiconductor companies in the world that can design and produce certified secure microcontrollers, but also provision them from factory, over the air, or on-premises with a secure and universally trusted digital identity. This identity can be created and managed throughout the device's lifecycle using SEALSQ's own PKI-as-a-Service. Very few players can offer today such a vertically integrated value proposition covering security from root-of-trust to cloud and from birth to end for any connected device.

From Motorola, to Atmel Secure Microcontroller, Inside Secure and now within the WISeKey group, SEALSQ teams have a long history of developing secure hardware, firmware and trust services for a wide variety of customers. Thanks to its robust supply-chain, SEALSQ has produced, provisioned, tested and delivered chips that have been installed into more than 1.6 Billion devices of all kind across the world.

Typical applications include IoT devices for Smart Home, EV charging, Smart Metering, Healthcare, Access Control, IT servers, USB tokens for Data storage and Encryption. Devices equipped with SEALSQ secure chips are often selected and approved to secure military or government security applications, underlining the high standard of trust, reliability and quality of the products. SEALSQ operates under ISO27001 certified environment, and its products are compliant with the most demanding industry certification bodies in the world (NIST and Common Criteria).

With over 120 registered active patents, SEALSQ has long been committed to innovation. Today its dedicated research engineers are designing the next generation of post-quantum secure chips capable to resist to the latest threats brought by quantum technology and deep learning together.

Headquartered in Switzerland SEALSQ is a global organization with offices in the US, EMEA and Asia, serving customers in more than 40 countries. SEALSQ is also a public listed company at the NASDAQ stock exchange under the ticker symbol LAES.

## INTRODUCTION

With this unique historical background, SEALCOIN emerges as a pioneering entity poised to revolutionize decentralized services. Backed by over 25 years of industry-leading experience in developing secure semiconductor chips, embedded firmware, and trusted hardware provisioning services, SEALCOIN is establishing itself as a trusted partner in safeguarding digital assets.

Through the seamless integration of Decentralized Ledger Technology (DLT) components, SEALCOIN bridges the gap between physical secure infrastructure and the digital integrity of DLT. This fusion crystalized around cryptographic structures, not only ensures the highest level of security and reliability but also paves the way for a safer and more connected world.

By prioritizing security, transparency, and trust, SEALCOIN is leading the charge towards a future where decentralized services redefine the boundaries of innovation and connectivity. Together, we embark on a transformative path towards a future where the physical and digital worlds converge seamlessly, ushering in an era of unparalleled connectivity and safety.

## PROOF-OF-CONCEPT

Our Machine-to-Machine (M2M) Proof of Concept (PoC) enables the disintermediation of service providers for interconnected devices.

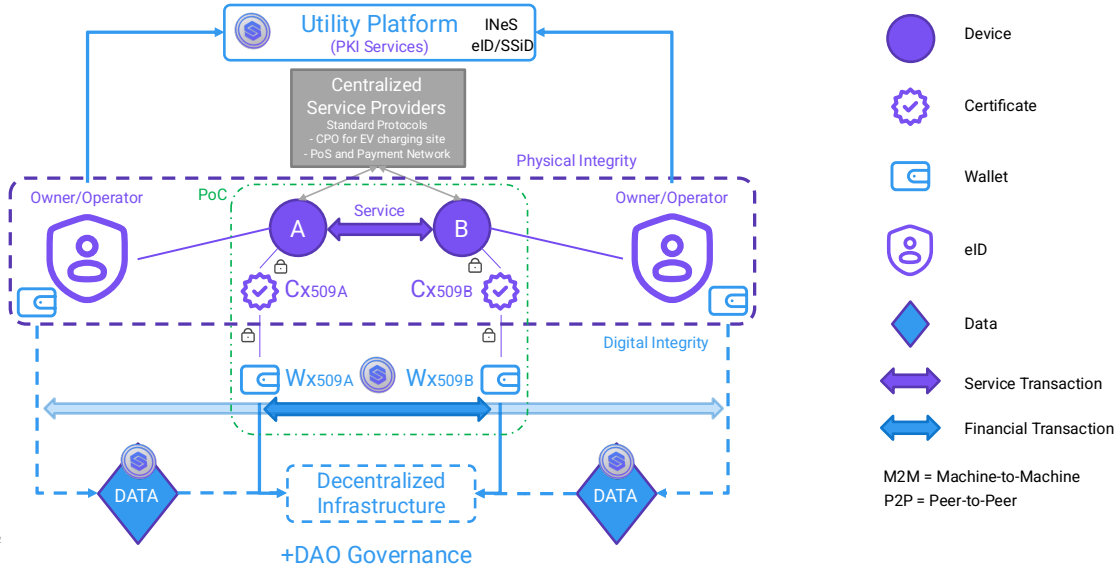
In generic terms, we use the technology inside a semiconductor's device to validate and verify a transaction. The Secure Element embedded in the device protects the private key and the certificate representing the device unique identity. The key is using the same elliptic curve cryptography (ECC) used on a Decentralized Ledger Technology (DLT) and therefore the device can simultaneously authenticate and sign a transaction onchain. The process can be described as follows:

1. **Transaction Validation and Verification:** The semiconductor device is equipped with cryptographic capabilities that enable it to validate and verify transactions. This involves signing the transaction, always keeping the private key in a secure element that is resistant to both physical and logical attacks, thus keeping the funds secured. We are already working on integrating postquantum resistant Secure Element capabilities. **Transaction Signing:** Upon successful validation and verification of the transaction, the semiconductor device generates a digital signature using elliptic curve cryptography. This signature serves as a proof of authorization for the transaction.
2. **Decentralized Ledger Technology Integration:** Simultaneously, the semiconductor device uses a Distributed Ledger Technology (such as a blockchain) to store the transaction in a decentralized manner. It signs and sends the transaction to a DLT network node that will then broadcast it to the rest of the network. The DLT serves as a distributed and immutable ledger where transaction records are stored securely and transparently.
3. **Elliptic Curve Cryptography:** Both the validation and signing processes utilize elliptic curve cryptography, a cryptographic algorithm based on the properties of elliptic curves over finite fields. This allows for efficient and secure generation of digital signatures and ensures the integrity of the transaction data, both physically and digitally.

By leveraging the capabilities of the semiconductor device and elliptic curve cryptography, transactions can be validated, verified, and securely recorded on a Decentralized Ledger Technology in a seamless and efficient manner, offering enhanced security and transparency in digital transactions.

The release of the PoC is scheduled for mid-July 2024, with a comprehensive demo planned shortly thereafter, showcasing the innovative capabilities of SEALCOIN in enabling Service vs Payment transactions between machines.

Picture representing the Ecosystem Mapping for Machine-to-Machine transactions:



# A COMPREHENSIVE SERVICE PLATFORM

	Phase MVP	Phase PoC	Phase Advanced
Account	<ul style="list-style-type: none"> <li><input type="checkbox"/> Onboarding Users:               <ul style="list-style-type: none"> <li>• Sign-up</li> <li>• Log-in</li> </ul> </li> <li><input type="checkbox"/> Create and Associate Hedera Wallet (Private key management: Hot Vs Cold)</li> <li><input type="checkbox"/> Financial Account</li> </ul>		<ul style="list-style-type: none"> <li><input type="checkbox"/> KYC (light, full, on-demand)</li> <li><input type="checkbox"/> Admin Rights</li> <li><input type="checkbox"/> Users Rights</li> <li><input type="checkbox"/> User Reputation</li> </ul>
Device	<ul style="list-style-type: none"> <li><input type="checkbox"/> Register Device               <ul style="list-style-type: none"> <li>• Device ID, MAC, Type, Application Type</li> </ul> </li> <li><input type="checkbox"/> Claim Ownership (Device to Account)</li> <li><input type="checkbox"/> Provisioning (= Tokenization)               <ul style="list-style-type: none"> <li>• Account to device for Hedera's Signature</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li><b>+MVP</b></li> <li><input type="checkbox"/> Device Reputation</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Store Device Data</li> <li><input type="checkbox"/> Device Discovery System</li> <li><input type="checkbox"/> Create Hedera Wallet for each Device</li> </ul>
Certificate	<ul style="list-style-type: none"> <li><input type="checkbox"/> Purchase Certificate               <ul style="list-style-type: none"> <li>• On/Off ramp crypto-fiat</li> <li>• Acquisition of Certificate (INeS)</li> </ul> </li> <li><input type="checkbox"/> Tokenize Certificate               <ul style="list-style-type: none"> <li>• Create a NFT of the certificate</li> </ul> </li> </ul>	N/A	<ul style="list-style-type: none"> <li><input type="checkbox"/> Allocate Certificate to Device (?)</li> <li><input type="checkbox"/> Delegate Device's signature to Certificate's owner</li> </ul>
Services	N/A	<ul style="list-style-type: none"> <li><input type="checkbox"/> OTC Request (Identified Devices AtoB)</li> <li><input type="checkbox"/> Submit Request: Notify Service provider or Device owner</li> <li><input type="checkbox"/> Validation Request: Approve/Reject</li> <li><input type="checkbox"/> Status Update: Receive and display feedback from Execution Request handled by Smart-Contract</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Describe Request (Standardization process)</li> <li><input type="checkbox"/> Network Request:</li> </ul>

# SEALCOIN Token

The M2M PoC can only be achieved through a cryptocurrency, in the form of a token associated to a device that is certified by a secure microcontroller storing its digital certificate, and where the token's software can interact with the SEALCOIN platform to securely organize and execute transactions.

Therefore, SEALCOIN is planning for its dedicated token, that will serve a dual IoT purpose, fulfilling both utility and payment functions.

## 1. UTILITY

- SEALCOIN will provide digital access to applications and services offered on the SEALCOIN platform. Through blockchain-based infrastructure, users can utilize SEALCOIN tokens to access and interact with various IoT applications and services seamlessly.
- Users will be able to leverage SEALCOIN tokens to unlock features, access premium content, or utilize specialized services within the SEALCOIN ecosystem. These tokens act as digital keys, granting users permission to engage with specific functionalities offered by secured devices and services connected to the platform.
- The utility feature of SEALCOIN tokens will ensure that users have convenient and secure access to a wide range of t-IoT applications and services, facilitating seamless integration and interaction within the IoT ecosystem.

## 2. PAYMENT

### 2.1 Payment Features

- SEALCOIN tokens will also serve as a means of payment within the SEALCOIN ecosystem. Users will be able to use SEALCOIN tokens to acquire goods and services offered by IoT devices and service providers on the platform.
- Additionally, SEALCOIN tokens will facilitate the transfer of money or value between users, enabling peer-to-peer transactions within the t-IoT ecosystem. Users can exchange SEALCOIN tokens for goods, services, or other cryptocurrencies securely and efficiently.
- The payment feature of SEALCOIN tokens will enhance the efficiency and liquidity of transactions within the t-IoT ecosystem, providing a seamless and decentralized payment solution for IoT stakeholders.

### 2.2 Volatility Management of Payment Features

The aim at issuing a Token is to be able to capture its intrinsic value within the designed ecosystem, so that the market participants can benefit from it.

The best way to store this value is in designing a Fixed Token supply, which will embed Scarcity and Value Appreciation for using the token. In other words, we are injecting an



inflation mechanism, where, as long as the token usage grows in (volume of participants, volume of transactions, number of use-cases), its intrinsic value will be captured within its face value, having a fixed amount of token for a bigger demand.

To mitigate its inherent volatility that represents a risk for the Participants' treasury management, in the context of purchasing a service at a fixed price (devices, certificates and other services...), we will implement mechanisms to have a transaction price pegged to a local currency (USD, EUR...) and therefore, fix the services' price to regular Fiat volatility.

In summary, the SEALCOIN token will be designed to combine both utility and payment features to provide users with digital access to t-IoT applications and services while also serving as a convenient and secure means of payment within the SEALCOIN ecosystem. By leveraging blockchain technology, SEALCOIN tokens will enable seamless integration, interaction, and transactions within the IoT landscape, fostering innovation and efficiency in t-IoT-related activities.

## TOKENOMICS

Token Supply details will be provided at a later stage.

Details of SEALCOIN token and its distribution for Acquisition and Trading purposes: Information on how to acquire and trade SEALCOIN token will be provided once regulatory process is concluded.

## USE CASES (DePIN)

ENERGY TRADING

EV CHARGING

VEHICLE SHARING

FLEET MANAGEMENT → OPPORTUNITIES (CUSTOMER SERVICES, COST REDUCTION) AND INDUSTRIAL IOT

AUTONOMOUS TRANSPORTATION

AUTONOMOUS DELIVERY

AUTONOMOUS DEVICES' TRANSACTIONS (SMART HOME AUTOMATION)

DATA TRADING

SENSORS MONITORING (SUPPLY CHAIN MANAGEMENT)

COMMUNICATION NETWORKS (AUTONOMOUS ROUTERS)

HEALTH TRACKERS

TRACKING SERVICES

# GOVERNANCE

Decentralized Governance:

Description of the governance model ensuring decentralized decision-making to be provided at a later stage.

# PARTNERS

## WEB3

Hedera / THG

- Consensus Mechanism
- Token Smart Contract
- Governance

## TRADITIONAL

TBD