Soarchain's Verification Framework for Hardware Devices and Data Streams: Overcoming Verification Challenges in Decentralized Physical Infrastructure Networks

Soarchain Team
Release 0.0.2

Abstract

As the Internet of Things (IoT) continues its rapid expansion, it increasingly influences various aspects of daily life and industrial operations. This evolution presents a future where the number of connected devices is expected to surge, reaching staggering figures. However, this growth brings forth critical concerns regarding security and scalability, particularly in Decentralized Physical Infrastructure Networks (DePIN), where verifying real-world data remains a complex challenge (). Traditional verification methods must be improved, leading to conflicts of interest, inactive service providers, and susceptibility to fraudulent activities. Soarchain emerges as a pioneering solution to these pressing challenges. The framework establishes a trust system anchored by a master certificate, ensuring the legitimacy of factory and device certificates. Addressing the pivotal issue of data security, Soarchain incorporates advanced security measures for data originating from vehicles. It encrypts this data for added protection and employs Zero-Knowledge Proofs. This method ensures that information can be verified without revealing the actual data. Additionally, Soarchain adds a layer-2 solution to its system, consisting of specialized nodes responsible for checking these proofs. This dual approach not only enhances the overall security but also improves the system's ability to handle large amounts of data efficiently. This paper explores Soarchain's innovative approach and its potential to offer a comprehensive solution to the verification and security challenges in the DePIN sector. The framework not only promises to enhance trust and reliability within decentralized networks but also addresses future scalability concerns, setting a precedent for secure and efficient IoT integration in various sectors.

1. Introduction

In an era where the Internet of Things (IoT) is rapidly transforming the landscape of technology and communication, the concept of Decentralized Physical Infrastructure Networks (DePIN) has emerged as a pivotal innovation. These networks represent a significant evolution in how we manage and interact with physical infrastructure, leveraging blockchain technology to enhance efficiency, transparency, and security. However, this technological advancement has its challenges. Verifying physical sensor data within these networks presents a unique set of complexities, primarily due to scalability constraints and the inherent difficulties associated with the oracle problem ().

The traditional approaches to verification in DePIN, including hardware-based methods such as embedding public/private key pairs or utilizing custom hardware with secure elements, have shown significant limitations. These methods often introduce unwanted permission layers or are susceptible to security vulnerabilities. Consequently, there is a growing interest in exploring innovative software-based

approaches that can effectively address these verification challenges without compromising the decentralized nature of these networks.

Soarchain's method hinges on a hierarchical chain of trust, integrating both hardware and software elements to establish a robust and scalable verification framework. This approach not only ensures the integrity and authenticity of the devices within the network but also addresses critical incentive challenges such as self-dealing, provider laziness, and susceptibility to malicious actors.

In the following sections, we delve into the intricacies of Soarchain's verification method, examining its layered trust architecture, the role of Zero-Knowledge Proofs in securing data streams, and the innovative use of a secondary layer for proof validation. Our analysis aims to demonstrate how Soarchain's framework not only addresses the current verification challenges in DePIN but also sets the stage for a more secure and scalable future in decentralized physical infrastructure.

1.1 Authentication of hardware devices

Soarchain, an innovative platform within the decentralized ecosystem, employs a hierarchical chain of trust as the backbone of its security infrastructure. Central to this structure are the principles of certificate verification, which provide a dynamic and adaptable system for onboarding new hardware manufacturers through a unique factory certification process.

At the top of this hierarchy sits the Soarchain master certificate, the ultimate authority anchors trust throughout the system. The paramount role of this master certificate is the meticulous verification and authorization of factory certificates, thereby establishing a foundation of security and trust.

Below the master certificate are the factory certificates issued by hardware manufacturers and serving as crucial components of the trust chain. Each factory certificate is a distinct marker of the manufacturer's commitment to quality and security. Integrating new hardware manufacturers into the Soarchain ecosystem involves the issuance of these factory certificates, symbolizing their entry into this prestigious network. This rigorous procedure not only maintains high-security standards but also cultivates an environment conducive to innovation and competitive advancement in the industry.

Delving deeper, we find device certificates at the base of the hierarchy. Issued by the factories, these certificates form the bedrock of trust for individual devices, verifying their authenticity and safeguarding against tampering. The credibility of these device certificates is intrinsically linked to the trust established by the factory certificates, which, in turn, are anchored by the master certificate's unwavering authority.

This layered hierarchy creates a sequence of verification and endorsement, with the master certificate overseeing factory operations and validating the devices produced. It is vital to note that Soarchain functions as a layer-1 network within the Cosmos SDK framework.

A pivotal aspect of Soarchain's approach is the decentralized process of issuing factory certificates. These certificates are pre-configured within the chain, and through a custom governance proposal mechanism,

they can be activated individually. This process allows for a transparent and secure method of onboarding new manufacturers, as the governance body carefully evaluates and approves factory certificate requests. This decentralized Certificate Signing Request (CSR) system ensures that the issuance of factory certificates is governed responsibly and democratically, enhancing the overall integrity of the Soarchain ecosystem.

By employing this comprehensive approach, Soarchain not only ensures system integrity but also fosters engagement from diverse industry players. This method promotes innovation and growth while maintaining the highest levels of security and trust, hinged on a transparent and decentralized governance structure for issuing factory certificates.

1.2 Authentication of live data

In the fast-evolving world of decentralized mobility networks, ensuring the accuracy and privacy of real-time data from a vast network of connected devices is crucial. Soarchain's strategy employs a fusion of cryptographic proofs and a scalable network architecture to address this critical challenge effectively.

At the heart of Soarchain's data verification system are Zero-Knowledge Succinct, Non-Interactive Arguments of Knowledge (zk-SNARKs). This sophisticated cryptographic technique enables vehicles to demonstrate the authenticity of their data without divulging the actual content, thereby preserving privacy. The integration of zk-SNARKs ensures robust data verification while maintaining the confidentiality of sensitive vehicular information.

The process begins when a vehicle joins the Soarchain network, at which point it transmits its Parameter IDs (PIDs) to the blockchain. PIDs are standardized diagnostic codes that convey crucial vehicle information, such as engine speed and temperature. This data is securely signed with the vehicle's certificate, containing public keys derived from the device certificates, thus validating the data's origin and ensuring its integrity.

To address scalability challenges in its decentralized mobility network, Soarchain implements a layer-2 scaling solution using runner nodes. These nodes take on the bulk of data processing tasks, significantly easing the burden on the core blockchain. A key feature in this architecture is the use of specific circuits for Zero-Knowledge Proofs, particularly zk-SNARKs. These circuits are algorithms uniquely crafted to validate data stemming from various Parameter IDs (PIDs) in vehicles' onboard diagnostics systems. Corresponding to diverse data points like fuel pressure or engine temperature, each PID is validated by a dedicated circuit. The deployment of zk-SNARKs, especially through the Groth16 scheme, is pivotal here. It allows vehicles to generate proofs that verify the authenticity, integrity and plausibility of their data, keeping the actual data concealed. This not only ensures the validation of the data in many ways, but also protects its confidentiality, a crucial aspect in the widespread network of vehicles. Opting for Groth16 is strategic, given its proficiency in efficiently managing numerous proofs for similar types of PID data, a common scenario in Soarchain's network. Briefly, with the help of the power of zk-SNARKs, fortifies the network's security, boosts efficiency, and enhances scalability.

In the Soarchain network, the secure transmission of vehicle data is facilitated through MQTT brokers, providing a reliable pathway for communication. When this data reaches the runner nodes, it undergoes a vital verification phase. During this stage, the data's integrity and originality are scrutinized using zk-SNARKs. Vehicles generate these cryptographic proofs, asserting the legitimacy of their data without disclosing its details. The runner nodes then apply specific circuits — predefined computational guidelines — to examine these zk-SNARK proofs. This procedure ascertains that the data adheres to expected standards, remains unmodified, and is sourced from authenticated vehicles. This robust mechanism of data transmission and verification upholds the network's integrity, ensuring that only validated and trustworthy data is exchanged within Soarchain's ecosystem.

Soarchain's layered approach, featuring runner nodes as a layer-2 solution, effectively addresses scalability concerns. This structure significantly alleviates the burden on the primary blockchain, enabling the network to manage an extensive array of data transactions seamlessly. The decentralized configuration of the runner nodes further bolsters the network's resilience and scalability. This configuration is implemented through a system design that employs state machine replication, threshold public key encryption, and staking, which we will explore in the next section.
In essence, Soarchain's method of live data verification in decentralized mobility networks, through the integration of zk-SNARKs and a layer-2 scaling solution, offers a comprehensive and scalable framework. This system not only ensures data integrity and privacy but also guarantees the network's scalability, making it an adaptable and robust solution for the intricate requirements of contemporary decentralized mobility networks.

1.3 Rollup

In blockchain technology, rollups are a scaling solution that processes and stores transaction data off the main chain, while still ensuring its integrity and security. Rollups effectively reduce the load on the main chain, enhancing scalability and efficiency.

In the context of Soarchain, runner nodes adopt a similar approach to sequencers. They play a crucial role in managing the data flow from devices. These nodes are responsible for gathering public keys, signatures of devices and creating a Merkle tree of device messages. This Merkle tree, a structure that summarizes all the data in a compact form, then submitted to the core blockchain of Soarchain. This method not only significantly reduces the data processing burden on the main chain, but also enables infinite scaling of the handling of data as long as a certain percentage of nodes operate as runners. Soarchain's implementation of this rollup-like mechanism enables scalability, security, and efficient data management within its decentralized mobility network.

Runners can be thought of as special types of sequencers, that ingest signed messages from the vehicular nodes within the network, validate them and create proofs from the results. A node can become a runner by staking a certain amount of Soarchain tokens and sending the corresponding special transaction type. One of the key aspects of the runner architecture is that it employs characteristic features to provide trustless and censorship-resistant operation.

The runner pool in the Soarchain framework consists of registered runner nodes capable of managing and sequencing message data. Messages are analogous to special types of transactions that are signed by the private keys of the connectivity devices, whose certification process was mentioned in the previous sections.

A consensus group is dynamically selected from the pool of runners, utilizing the Verifiable Random Function(VRF) that is invoked every epoch within the Soarchain core layer-1 virtual machine. This is to prevent centralization of data validation power and potential collusion between vehicles and runners. The runners within the consensus group at a given epoch are responsible for receiving, ordering and verifying the messages from the vehicles. These runners create Merkle trees from the messages that they receive, using the hashed version of each message as a leaf for the tree. Once the Merkle tree reaches a certain height - which is determined by a network parameter - the consensus group creates a claim that it had in fact received, ordered and verified all the messages and created a complete Merkle tree out of it. The claim contains the root of the Merkle tree and information about the number of unique device addresses and messages. This claim transaction will be later on used to validate whether the runners were in fact acting honestly and correctly. Once the claim transaction has been submitted by one of the runners in the consensus group and processed successfully, the consensus group now works to submit information about a random subset of the messages that they have used to create the Merkle root. The randomness from the VRF is used as an input to determine which random subset of these messages will have to be selected and provided Merkle tree information about. Each runner needs to provide information about the exact Merkle leaves that were picked as a result of the random selection.

At each epoch, a distributed key generation process takes place to create a threshold encryption key, which will later on be used for threshold public key encryption. The generated master public key is written to the blockchain. Using Shamir’s Secret sharing algorithm, each member of the selected runners at that epoch receives a secret key share. Runners are required to encrypt the Merkle tree information that they have been recording and processing throughout this process, and send the encrypted content inside a special type of transaction to the blockchain. Once the threshold number of transactions are reached, each runner’s share is decrypted and the content is compared to each other. The decrypted content must be identical for each runner. If the proofs are verified and identical when compared to each other, the runners are rewarded by the protocol according to the order that they have submitted the results in. The owners of the accounts that correspond to the randomly selected leaves’ are also rewarded for their participation in the proof of availability process.