Attestation

Overview

Attestation, in the context of hardware and computer security, is a process that allows a device to prove its identity and integrity to another device. This process is a critical component of modern computer security, providing a robust and tamper-resistant method for verifying the identity and integrity of devices.

What we aim to do is to enable these devices to publish and verify their attestations on the blockchain, and to link every step in the entire chain, such as code submission, binary file construction, service deployment, and the hardware environment in which the service operates. In this way, we can establish a chain of trust throughout the entire process.

Definition

Attestor : Attestor is an entity, often a trusted third party, that validates or verifies the authenticity and integrity of a device or system, typically through the process of attestation.

Attestation : The report provided by attestor, which validates or verifies the integrity and identity of a device or system.

Attestation Types

Single-step Optimistic Attestation

Single-step optimistic attestation is a process that contrasts with optimistic attestation, requiring immediate on-chain verification of an attestation report once it has been submitted by the attestor.

In this approach, the attestation report is not simply accepted on an optimistic basis; instead, it must undergo a verification process on the blockchain. Only reports that pass this verification are allowed to be submitted to the chain.

This method emphasizes the importance of immediate validation and ensures a higher level of trust and security. By mandating that each attestation report be verified before being accepted, verifiable attestation minimizes the risk of incorrect or fraudulent reports being added to the chain, providing a more robust and reliable mechanism for establishing trust within the system.

Multi-step Optimistic Attestation

Multi-step optimistic attestation is a concept where an attestor can stake to gain the qualification to submit an attestation report, and once submitted, the report is accepted without immediate verification. The system operates on the optimistic assumption that the attestor's report is correct.

In this framework, there is also a role known as a challenger, who can initiate a challenge if they discover an issue with the attestor's report. The challenge process can be categorized into different types, such as interactive, akin to optimistic rollup's fraud proof, or non-interactive, such as direct on-chain verification of the attestation report. If the challenger successfully proves that the attestor's report is incorrect, the attestor may be slashed, or penalized.

This approach to attestation combines trust with mechanisms for accountability and verification, providing a balance between efficiency and security in the attestation process.

Consensus-based Attestation

Consensus-based attestation is a method designed to address situations where not all attestation reports can be verified on-chain, possibly due to high costs or current technological limitations.

In this approach, the verification is conducted off-chain, and multiple attestors work together to reach a consensus. Once a predetermined number of attestors agree that the report is correct, it is then submitted to the chain.

This method leverages the collective agreement of a group of attestors, rather than relying on a single entity or an immediate on-chain verification. By utilizing a consensus mechanism, consensus-based attestation ensures that the attestation report is accepted only when there is sufficient agreement among the participating attestors.

This approach provides a flexible and collaborative way to validate attestation reports, maintaining trust and integrity within the system while accommodating scenarios where on-chain verification may not be feasible.

Contract

```

Copy / *@noticeThe status of an attestation* @paramSubmitted The attestation is submitted *@paramChallenging The attestation is being challenged* @paramRevoked The attestation is revoked *@paramAttested The attestation is verified on-chain or off-chain* @paramSlashed The attestation is slashed, used for optimistic attestation */ enumAttestationStatus{
```

Submitted, Challenging, Revoked, Attested, Slashed }

/ *@noticeThe dependency of an attestation*@paramregistry The address of the attestation registry contract*@paramhash The hash of the attestation* / structAttestationDependency{ addressregistry; bytes32hash; }

/ *@paramhash The hash of the attestation*@paramattester The address of the attester*@paramrevokable Whether the attestation is revokable* @paramstatus The status of the attestation*@paramdepCount The number of dependencies* @paramcreatedAt The timestamp when the attestation was created*@paramexpiry The timestamp when the attestation expires* @paramrevokedAt The timestamp when the attestation was revoked*@paramdata The data of the attestation*/ structAttestation{ bytes32hash; addressattester; boolrevokable; AttestationStatus status; uint80depCount; uint256createdAt; uint256expiry; uint256revokedAt; bytesdata; }

```

The Attestation struct is a core data structure within the system, representing the report submitted by the attestor along with its status. Each attestation report submitted to the chain corresponds to a non-transferable NFT (Non-Fungible Token), serving as a credential for the submission of the report. The image of the NFT is rendered based on the actual status of the attestation.

Attestation Dependency

Attestation dependency refers to the relationship or linkage between different attestations within a system or process. It highlights how one attestation might rely on or be influenced by another, creating a chain or network of dependencies that must be considered in the overall attestation process.

Attestation Rollup

Attestation Rollup is a concept that pertains to the aggregation of attestations performed on Layer 2 (L2), with the final state being rolled up to Layer 1 (L1), such as Ethereum. This process allows for the efficient handling of multiple attestations, consolidating them into a single state root that can be committed to the main chain.

Here's a more detailed explanation:

1. Layer 2 Attestations
2. : All the attestations are initially conducted on L2, allowing for scalability and efficiency. This includes the submission of attestation reports, verification, and the handling of corresponding NFTs.
3. State Root Rollup
4. : The final state of these attestations, along with other L2 transactions, is consolidated into a state root. This state root is then rolled up to L1, providing a summarized representation of all the L2 activities.
5. Verification on L1
6. : If there are any trust concerns regarding the L2 attestations, it is possible to resubmit the attestation report on L1 and perform verification there. This adds an extra layer of security and trust, ensuring that the attestation process can be independently validated if needed.
7. Integration with Main Chain
8. : By rolling up the attestations to L1, they become part of the main blockchain, benefiting from its security and decentralization while maintaining the efficiency gained from handling the attestations on L2.
9.

Attestation Rollup thus provides a bridge between the scalability and efficiency of L2 attestations and the security and trust of the main blockchain. It enables the system to handle a large volume of attestations without overloading the main chain, while still providing the option for direct L1 verification if required. It represents a flexible and robust approach to managing attestations within a layered blockchain architecture.

Previous Specification Next Attestor Last updated6 months ago On this page *

Was this helpful?
```