Introduction

The development of the Layer 2 ecosystem has flourished, which has reduced the barriers to entry for users to a certain extent. However, there is a significant issue in that it could lead to a substantial division of the user base and funds within the Ethereum ecosystem, turning the UX of utilizing the Ethereum ecosystem into a considerable challenge.

Ideally, across the entire Layer 2 landscape, users would only need one EVM-compatible account to become roamers within the Ethereum ecosystem.

Supported Features

- End-to-end forwarding of arbitrary messages across Layer 2 Networks.
- A flexible balance between timeliness and security: Users can choose the transmission speed of cross-chain messages, allowing them to make a reasonable choice between the security of funds and the timeliness of the transaction.

We have designed a set of architectural solutions that satisfy the characteristics of decentralization, security, and high efficiency.

The Orbital Station Network

, abbreviated as OSN

is constructed in a manner similar to ZKRollup. It is primarily used for decentralized aggregation of messages pertaining to cross-chain intentions of users within the Ethereum ecosystem and for realizing the capability of secure and efficient message transmission.

[

image

1026×780 60.2 KB

](https://ethresear.ch/uploads/default/original/2X/4/47167bf247cba87c9fd7bb32989722e5288bd13e.png)

Next, we will outline our technical architecture based on the above discussion.

Decentralized Model

RVS (Relayer Validator Separation) :Users choose the target Relayer and include the Relayer’s address information when sending messages to the Launch Pad on the Source Chain.

Relayers are responsible for transmitting users’ cross-chain intent messages to the OSN

network, where validators will perform decentralized election verification of the message’s correctness on the Source Chain, followed by block consensus packaging.

Security Model

- Security is inherited from Ethereum Layer 1: All user transactions will ultimately be recorded on Ethereum L1, and the DA from Layer 2s can be effectively verified on L1.
- A rigorous arbitration process ensures the security of cross-chain messages.
- Margin pledge, relayer and validator will pledge a large amount of margin to compensate for the loss caused by the malicious process.
- Severe punishment mechanism, once there is an evil behavior, the relayer and validator involved will forfeit all the pledge money, which will be used to compensate the loss to the user.

Margin Mechanism

- Each Realyer node has to pledge a certain margin to participate in the message delivery.
- Each decentralized node in the OSN network must pledge a certain margin to participate in the security maintenance

of the node

Efficiency Model

- Speed

: Optimistically

transmit messages to minimize performance loss during the message transfer process, while reserving a portion of time blocks to ensure the security of message delivery.

- Cost

: Reduce the cost of arbitration through zero-knowledge proofs

.

In the following section, we will introduce the architecture of this system, including some details.