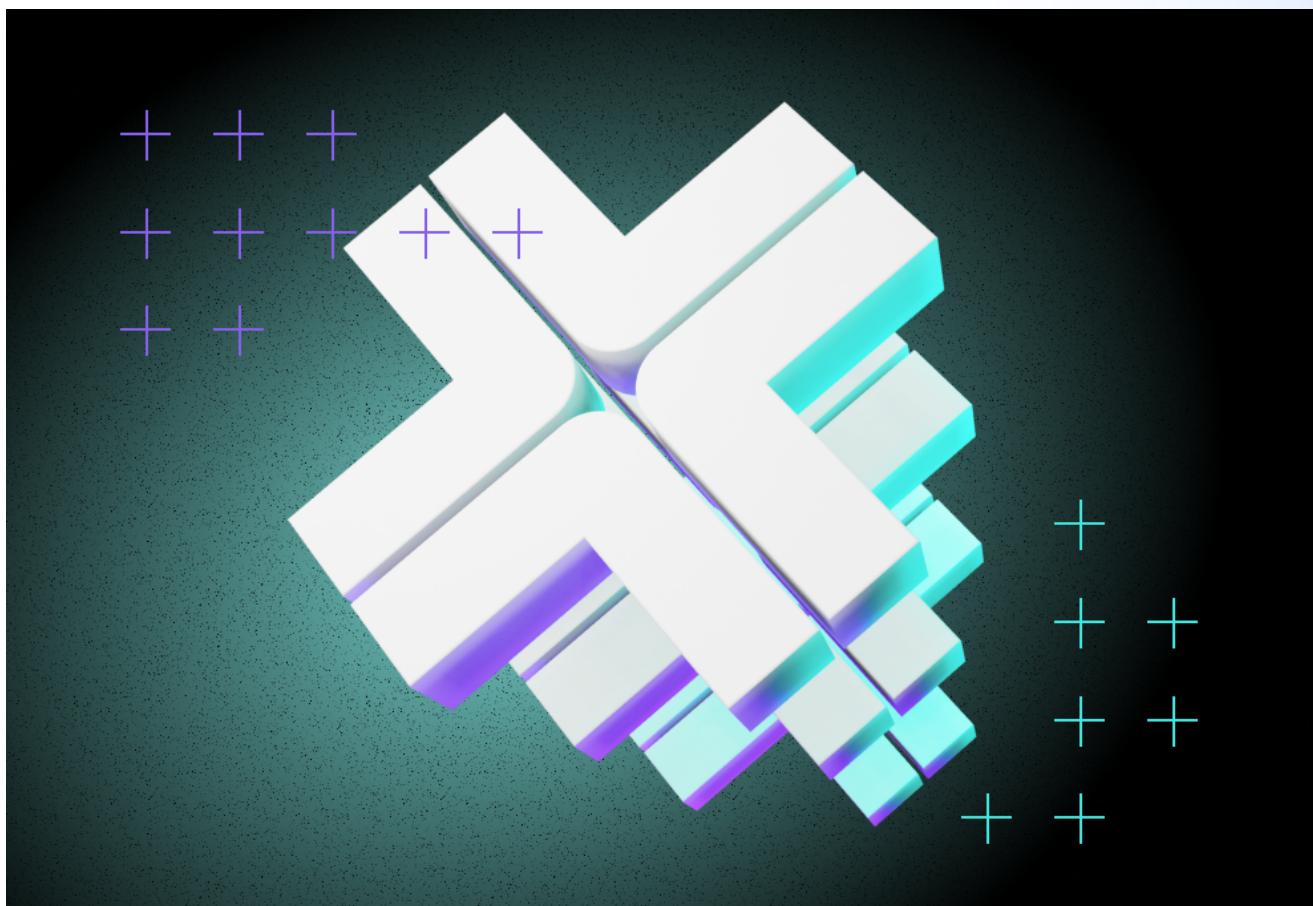


[< Back to articles](#)

Axelar: Token Linker & Forecall Service Audit Summary



Andrea Nováková // AUDITS, ETHEREUM AUGUST 12, 2022



[Axelar](#) engaged [Ackee Blockchain](#) to review and [audit](#) the **Token Linker** and the **Forecall Service**. Token Linker is a set of contracts used to link any tokens across two or more different EVM-compatible chains on a one-to-one basis using only Axelar's general message passing. The **Forecall Service** allows an application that receives messages from Axelar to accept messages before they are approved on Gateway.

The audit was conducted between **August 1 and August 5, 2022**, with a total time commitment of **5 engineering days**. We now publish a summary of our results.

METHODOLOGY

We start by reviewing the specifications, sources, and instructions provided to us, which is essential to ensure we understand the project's size, scope, and functionality. This is followed by due diligence using the automated [Solidity](#) analysis tools and [Slither](#).

In addition to tool-based analysis, we continue with a detailed manual code review, which is the process of reading the source code line by line to identify potential vulnerabilities or code duplications. When the code review is complete, we run unit tests to ensure the system works as expected and potentially write missing unit or fuzzy tests. We also deploy the [contracts](#) locally and try to attack and break the system.

SCOPE

The audit was performed on two repositories: we audited commit *5e1d4bb* of the [axelarnetwork/token-linker](#) repository and commit *db238d7* of the [axelarnetwork/axelar-utils-solidity](#) repository.

During the security review, **we paid particular attention to:**

- execution logic in Forecall Service is matching requirements;
- token linking is not leading to unauthorized access to funds;
- detecting possible reentrancies in the code;
- ensuring access controls are not too relaxed or too strict;
- looking for common issues such as data validation.

FINDINGS

Here we present our [findings](#).

Critical severity

No critical severity issues were found.

High severity

H1: The `forecall` and `forecallWithToken` can be called repeatedly with a same payload

Medium severity

M1: The `tokenAddress` is missing zero-address check

M2: TokenLinker has insufficient data validation

Low severity

No low severity issues were found.

Warning severity

W1: Usage of `solc` optimizer

W2: Floating dependency on AxelarGateway

W3: Multiple ways to receive ether can lead to loss of funds

W4: The `forecall` function is missing any checks by default

Informational severity

I1: Typo in the error name

CONCLUSION

Our review resulted in **8 findings** ranging from *Informational* to *High* severity. The most severe one is a violation of an intended behavior in Forecall Service (see H1 in the full audit report).

After the audit, **we recommended Axelar to:**

- add documentation including Natspec comments;
- write a more extensive test suite;
- address all other reported issues.

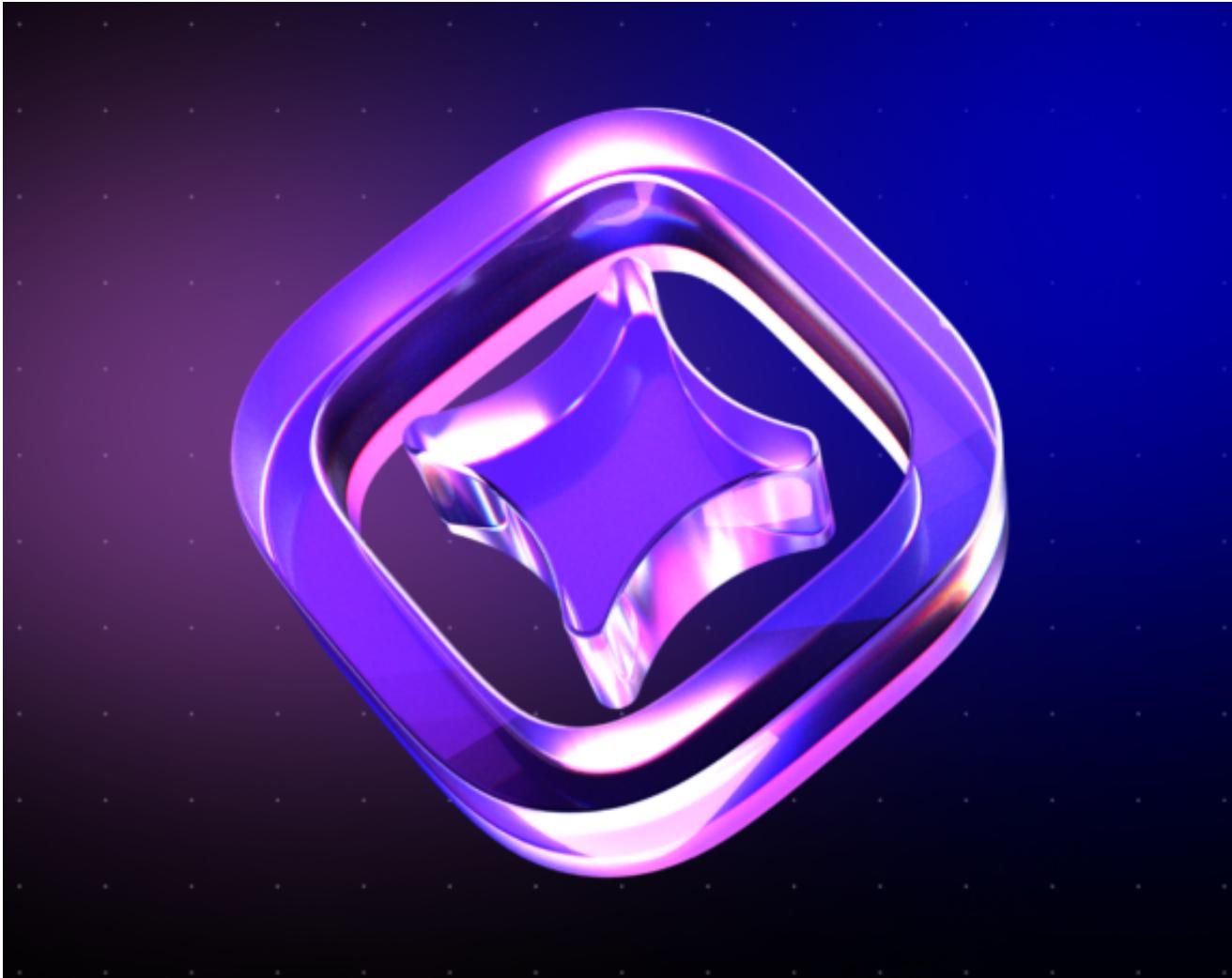
Ackee Blockchain's full *Token Linker & Forecall Service* audit report with a more detailed description of all findings and recommendations can be found [here](#).



Andrea Nováková

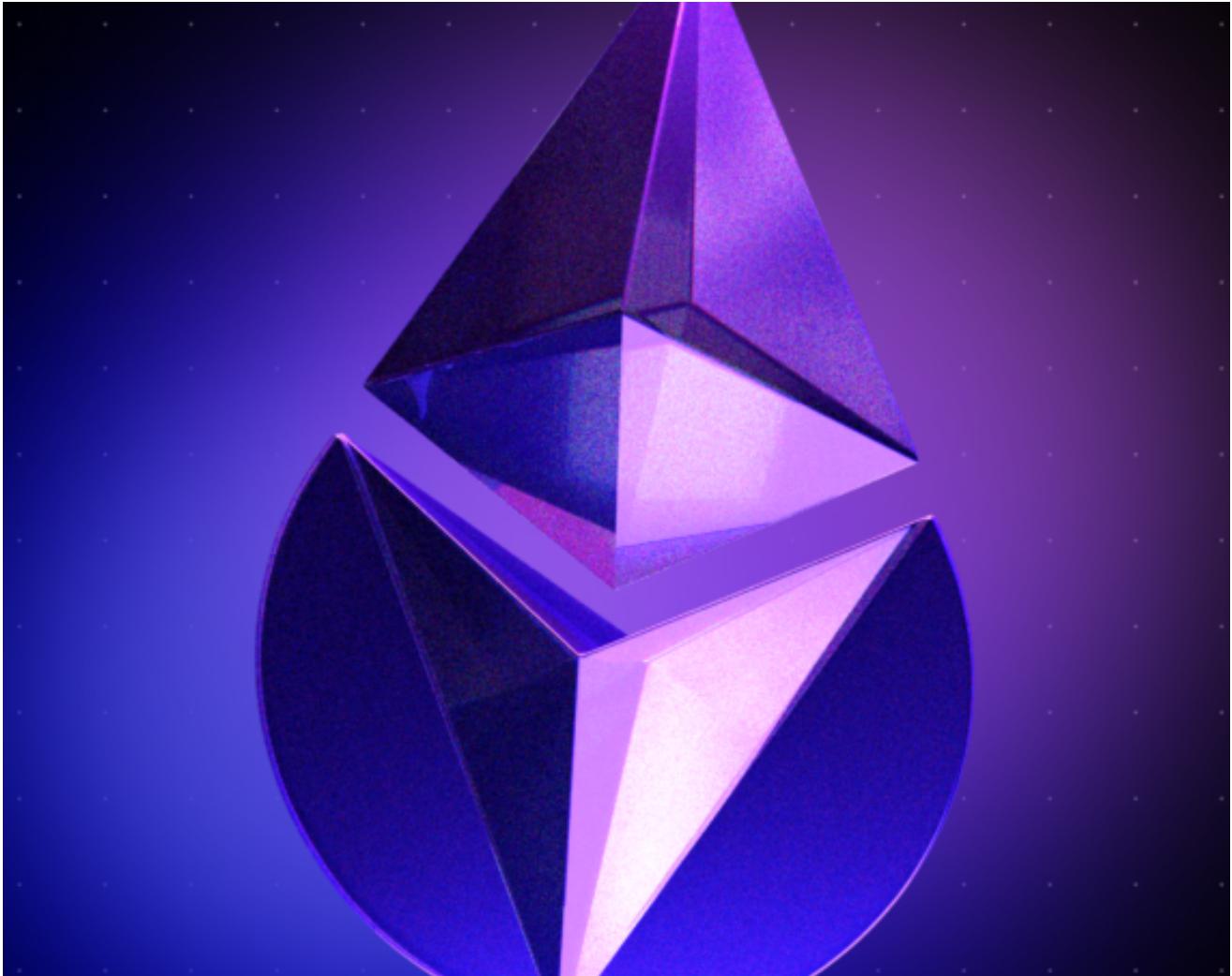


You May Also Like



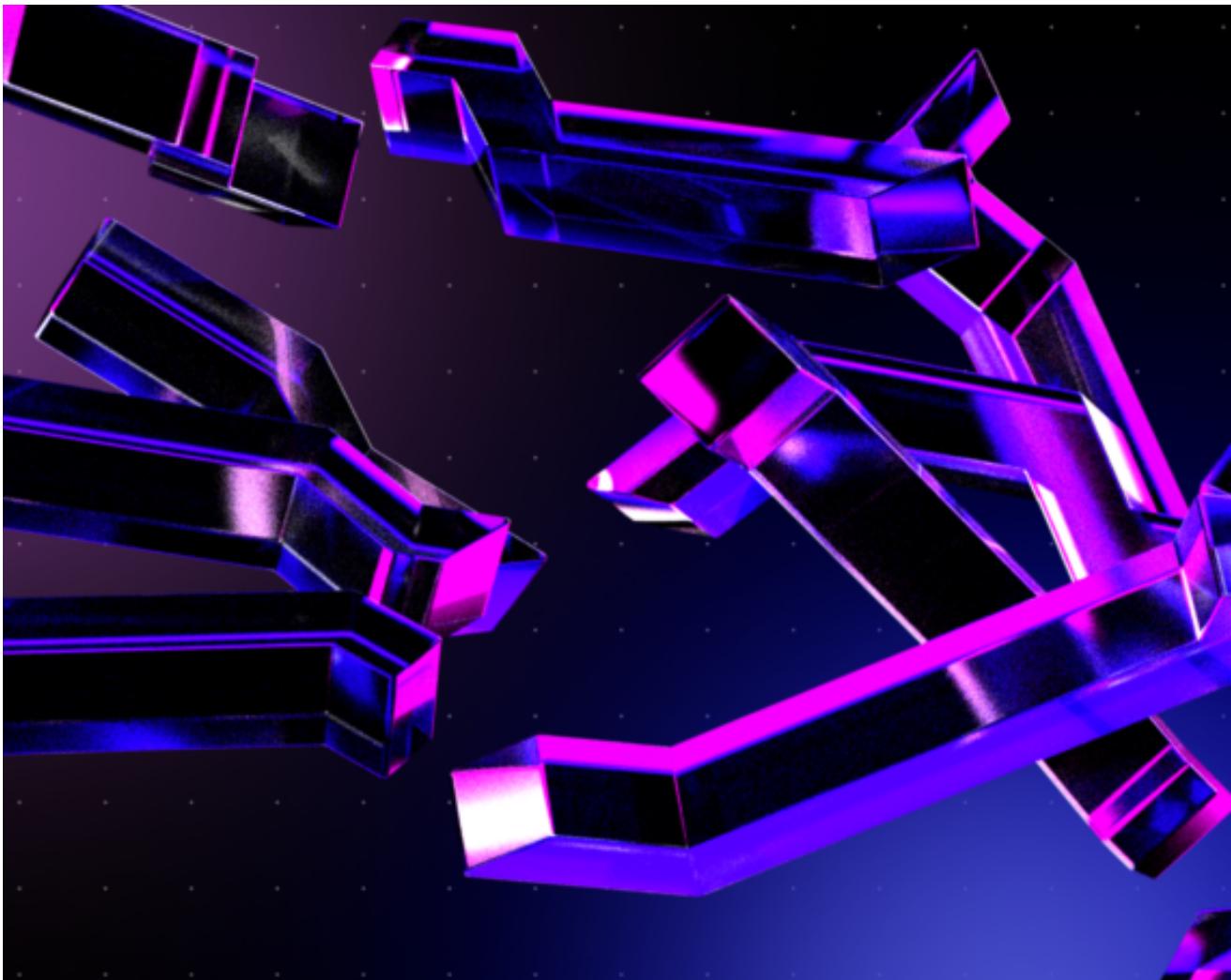
// AUDITS ETHEREUM WAKE AUGUST 2, 2024

Rhinestone Module Registry Audit Summary



// AUDITS ETHEREUM WAKE JULY 29, 2024

Lido stETH on Optimism Audit Summary



// EDUCATION ETHEREUM HACKS TUTORIAL WAKE JULY 11, 2024

Cross Contract Reentrancy Attack