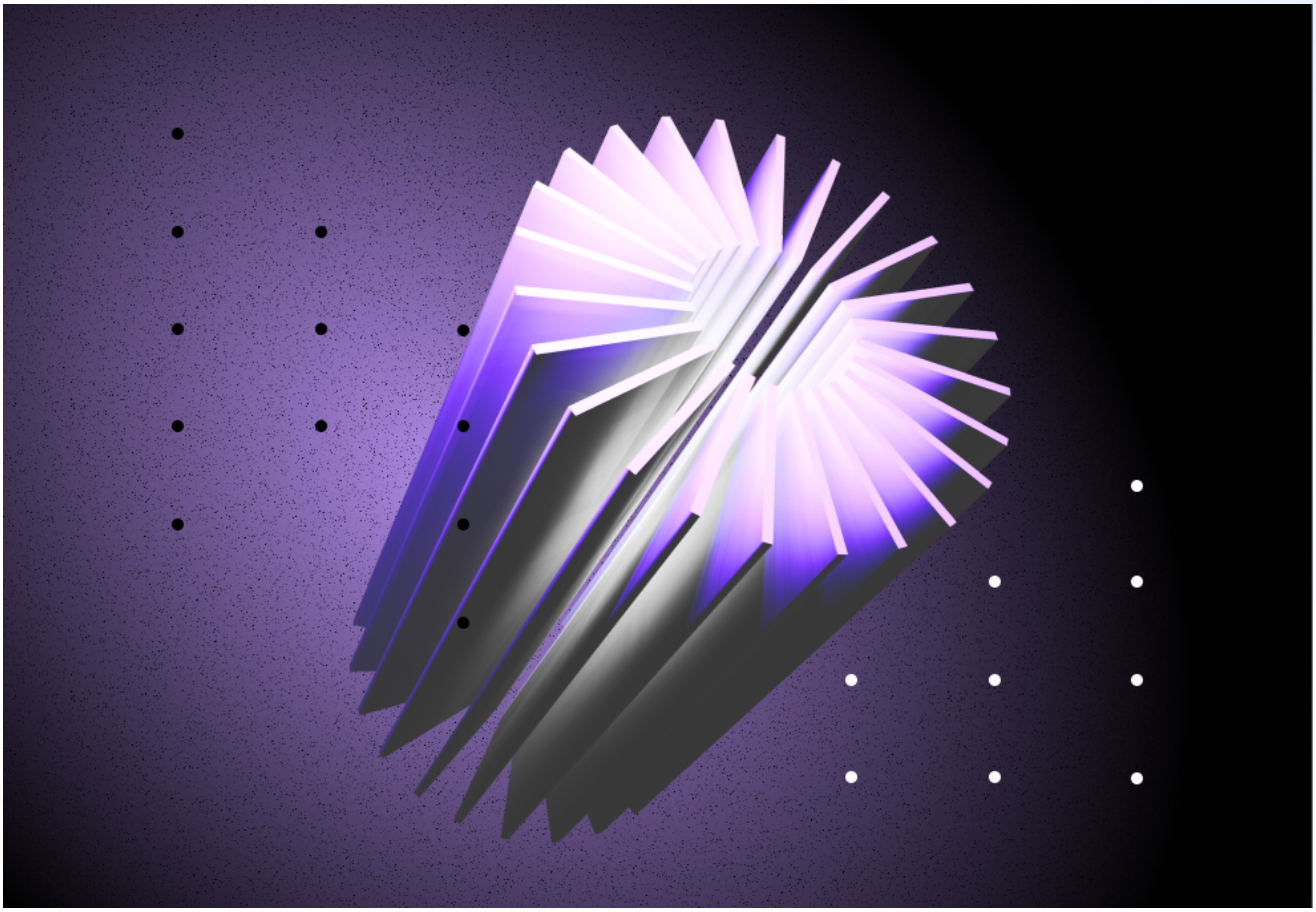
< Back to articles

# LayerZero: Solidity Examples Audit Summary

Andrea Nováková // AUDITS, ETHEREUM AUGUST 8, 2022



LayerZero engaged Ackee Blockchain to review and audit their example contracts. This article is a summary of all audits carried out to date:

- LzApp + Tokens Audit
- Solidity-examples Repository Audit

- NativeProxyOFT20.sol (later renamed to NativeOFT.sol) Audit

We now publish a summary of our results.

### METHODOLOGY

The methodology of all three audits is as follows.

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.

## LzApp + Tokens Audit

The audit was conducted between **April 27 and May 3, 2022** with a total time commitment of **5 engineering days**.

**Scope**

We audited commit *87941ce6160f27a4057372e78c552c780baae524* of the LayerZero-Labs/solidity-examples repository, specifically contracts: *contracts/lzApp, contracts/tokens.*

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

- checking if nobody can exploit the system;
- ensuring access controls are not too weak;
- checking the architecture;
- checking the code quality and Solidity best practices;
- 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:** Burn address issue

### Medium severity

**M1:** Condition bypass

### Low severity

No low severity issues were found.

### Warning severity

**W1:** Low test coverage

**W2:** Code duplication

**W3:** ERC721, ERC1155 reentrancy

**W4:** Unresolved TODO

**W5:** Unintended feature – Renounce ownership

### Informational severity

**I1:** Public functions can be external

**I2:** Missing require message

**I3:** Missing zero length handling

**I4:** Missing documentation

**I5:** Hardcoded types

## CONCLUSION

Our review resulted in **12 findings** ranging from *Informational* to *High* severity.

The code quality is solid. However, we identified a few code duplications, so the inheritance could have been designed better. Also, the unit test coverage is insufficient for some of the contracts reviewed. Although the code is simple, easy to understand, and contains few comments, it is a good practice to cover the code using NatSpec documentation.

**We recommended LayerZero to:**

- avoid code duplications;
- increase unit test coverage;
- use NatSpec documentation.

**Update:** LayerZero provided an updated codebase that addresses the reported issues and we performed the fix review between **May 11 and 13, 2022**. The re-audit was done on the following commit *865a1ab26759b5754e5ca51f11a5f1594c6f11ba*.

All of the findings were acknowledged and some of them fixed (H1, W2, W4, I2, I5, partially W1). A detailed discussion of the exact status of each issue can be found in the full audit report.

**Ackee Blockchain's full *LzApp + Tokens* audit report with a more detailed description of all findings and recommendations can be found here.**

## Solidity-examples Repository Audit

The audit was conducted between **June 15 and June 26, 2022** with a total time commitment of **7 engineering days**.

**Scope**

We audited commit *c7525a549a8db3fb54a89620409bf29c89f23899* of the LayerZero-Labs/solidity-examples repository.

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

- detecting possible reentrancies in the code;
- ensuring the proper handling of the tokens during the cross-chain messages;
- 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

No high severity issues were found.

### Medium severity

**M1:** Renounce ownership

**M2:** Dangerous transfer ownership

### Low severity

No low severity issues were found.

### Warning severity

**W1:** Lack of events in state changing functions

**W2:** Usage of solc optimizer

**W3:** Floating pragma

### Informational severity

No informational severity issues were found.

## CONCLUSION

Our review resulted in **5 findings** ranging from *Warning* to *Medium* severity.

The architecture of the project is well designed and allows easy integration for 3rd parties. The tests are written in JavaScript, and they successfully pass. **Code quality is excellent and well documented**, essential for the example contracts. LayerZero provides high-quality documentation in the white paper and on the gitbook website.

**We recommended LayerZero to:**

- use static analysis tools like Slither;
- ensure that the privileged owner role is well maintained;
- address all the reported issues.

**Ackee Blockchain's full *Solidity-examples repository* audit report with a more detailed description of all findings and recommendations can be found here.**

## Solidity Examples NativeProxy Audit

The audit was conducted between **August 3 and 8, 2022** with a total time commitment of **5 engineering days**.

**Scope**

We audited commit b0bd359e8affb782da83915fe06be8b3a7cc34c7 of the LayerZero-Labs/solidity-examples repository.

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

- detecting possible reentrancies in the code;
- ensuring the proper handling of the tokens during the cross-chain messages;
- 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

No high severity issues were found.

### Medium severity

**M1:** Accepting messages from untrusted remotes

**M2:** Constructor data validation

### Low severity

**L1:** Ownable pattern

**L2:** Missing override for ERC165

### Warning severity

**W1:** Usage of solc optimizer

**W2:** Recent solc version

**W3:** Empty _srcAddress can bypass trusted remote check

**W4:** Unused _lzSend() function

### Informational severity

**I1:** Coding practice

**I2:** Zero token transfer

**I3:** Public functions

**I4:** Unused SafeERC20

## CONCLUSION

Our review resulted in **12 findings** ranging from *Informational* to *Medium* severity.

**We recommended LayerZero to:**

- address all the reported issues.

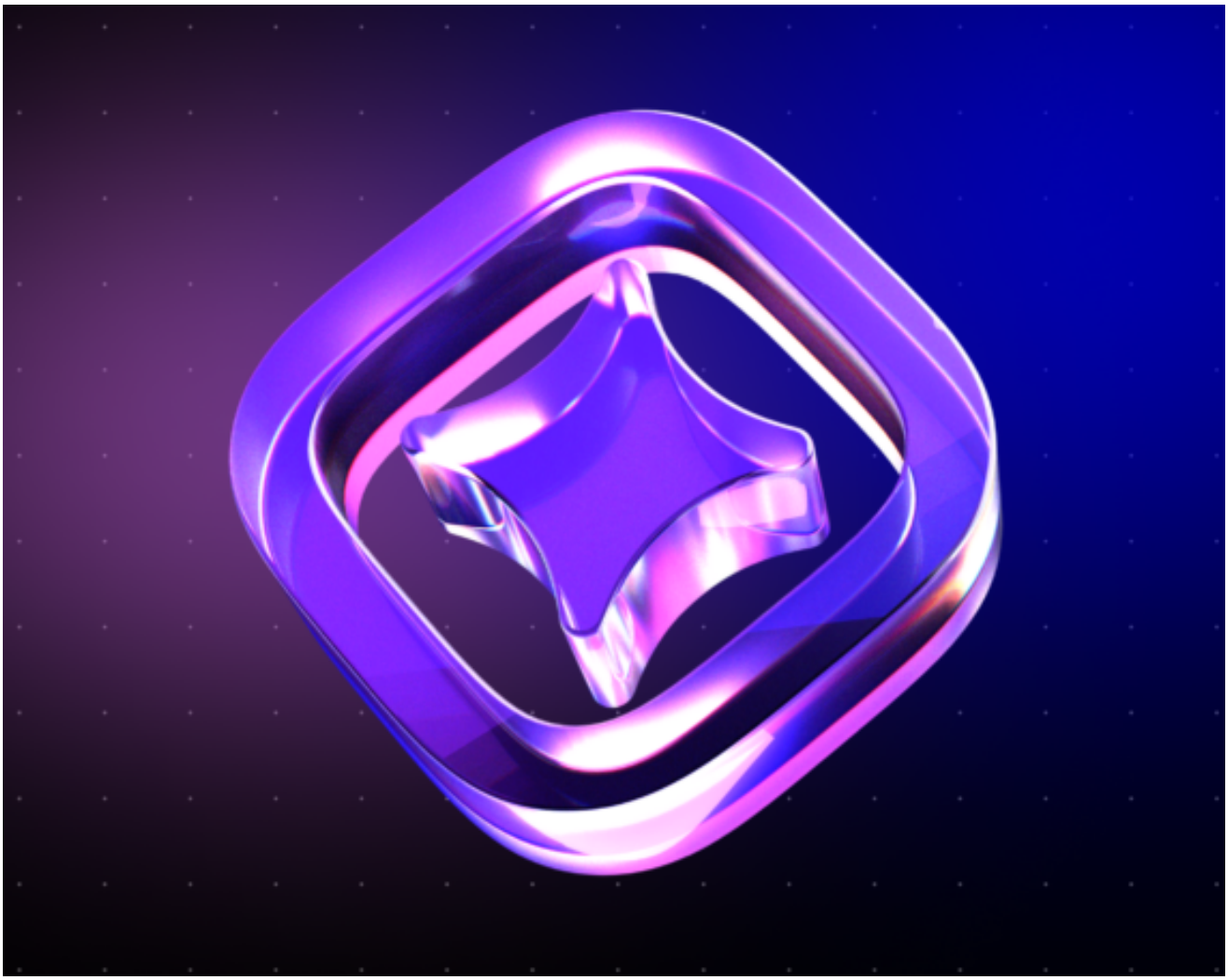
**Ackee Blockchain's full *Solidity Examples NativeProxy* audit report with a more detailed description of all findings and recommendations can be found here.**

We were delighted to audit **LayerZero** and look forward to working with them again.

Audit Blockchain Cryptocurrency Ethereum EVM Layerzero Security Smart Contract

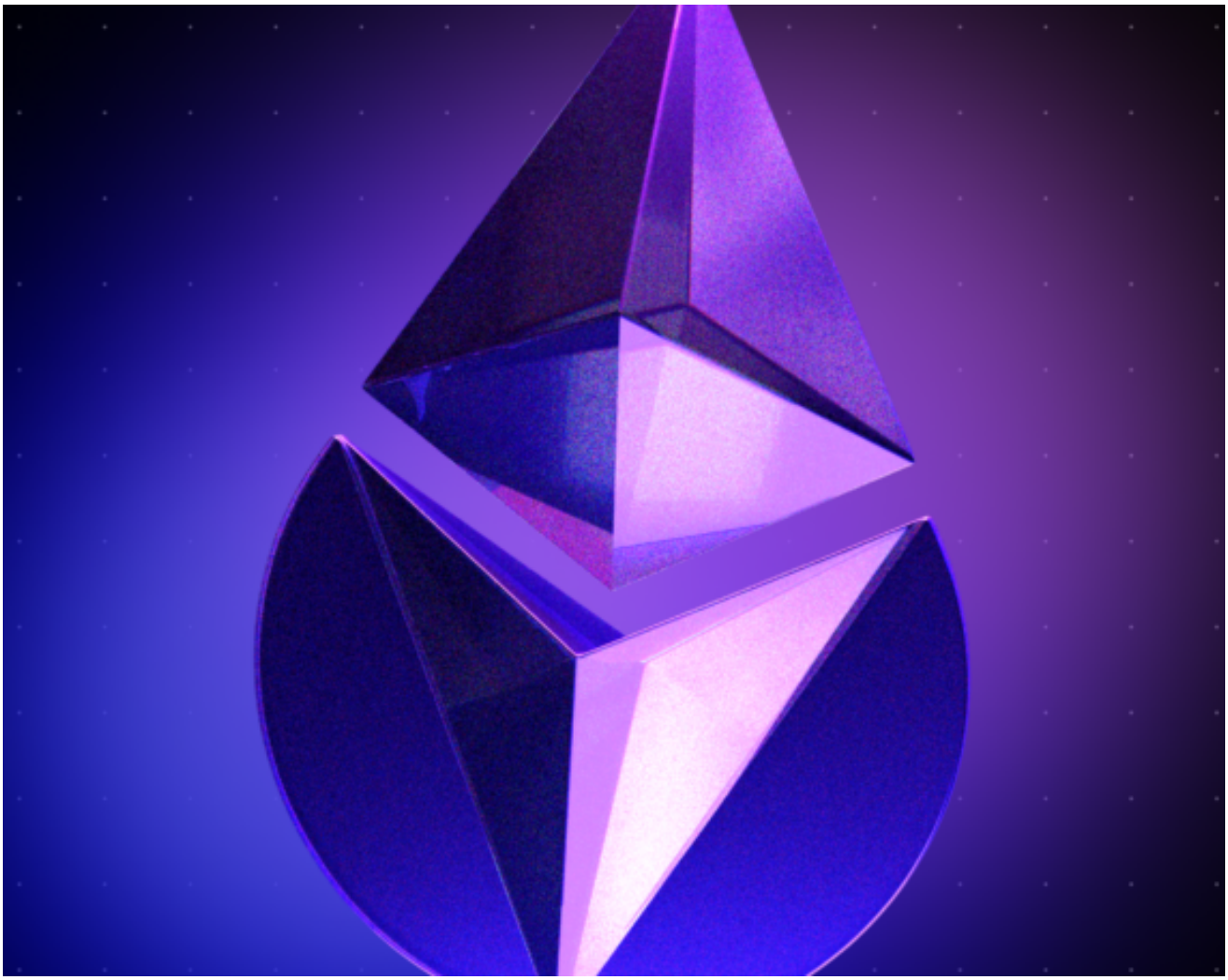
**Andrea Nováková**

# You May Also Like



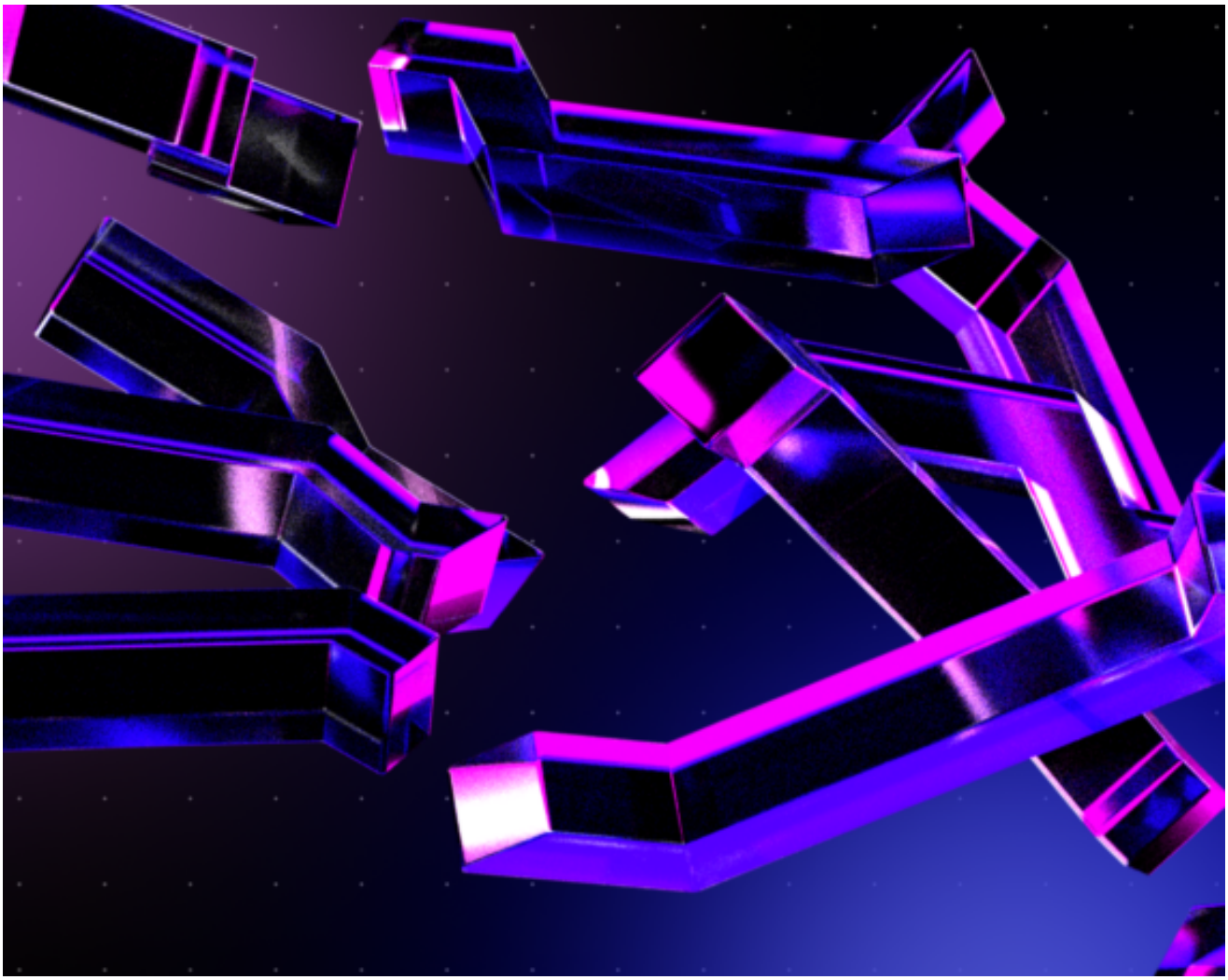
// AUDITS ETHEREUM WAKE AUGUST 2, 2024

# 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