< Back to articles

Ackee Blockchain audited LayerZero

Andrea Nováková // AUDITS, ETHEREUM MARCH 15, 2022

ABOUT LAYERZERO

LayerZero is **an omnichain interoperability protocol** designed for lightweight message passing across chains. LayerZero provides authentic and guaranteed message delivery with configurable trustlessness. The protocol is implemented as **a set of gas-efficient, non-upgradable smart contracts**.

Currently, LayeZero supports Ethereum and EVM-compatible chains like: Avalanche, Polygon, BNB Chain, Fantom, Arbitrum, and Optimism.

To learn more about LayerZero, read **the official documentation here**.

LayerZero engaged Ackee Blockchain to conduct security reviews of LayerZero and Stargate Finance protocols on a regular basis. The Ackee Blockchain security team has **so far conducted 5 audits**, several features of the LayerZero protocol are still under review and more are about to come. Here we publish the first results of our work.

In this blog post, we'll mention information about the following LayerZero audits:

- **LayerZero proof-lib audit**
- **LayerZero Stargate DAO/Voting Escrow audit**
- **LayerZero protocol audit** (the only one publicly accessible)

LayerZero proof-lib audit was completed on **March 11, 2022** with a total time donation of 4 engineering days. Our security team found **3 low** severity and **1 medium** severity issues. All findings were acknowledged or fixed by LayerZero development team.

LayerZero Stargate DAO/Voting Escrow audit was completed on **March 29, 2022** with a total time donation of 6 engineering days. Our security team found **5 low** severity issues, all of them were general recommendations rather than security issues. All findings were acknowledged or fixed by LayerZero development team.

ABOUT THE LAYERZERO PROTOCOL AUDIT

LayerZero protocol audit was completed by two auditors of Ackee Blockchain on **March 15, 2022**. The total time donation of this audit was **12 engineering days**.

During the review, **special attention was paid to**:

- checking if nobody can exploit the protocol;
- ensuring access controls are not too weak;
- checking the protocol architecture;
- checking the code quality and Solidity best practices;
- and looking for common issues such as data validation.

We strive for a gradual and thorough approach to auditing the LayerZero protocol, which is why **our audit methodology consists of**:

1. **Technical specification/documentation** – a brief overview of the system is requested from the client, and the audit scope is defined.
2. **Tool-based analysis** – deep check with automated Solidity analysis tools and Slither is performed.
3. **Manual code review** – the code is checked line by line for common vulnerabilities, code duplication, best practices, and the code architecture is reviewed.
4. **Local deployment + hacking** – contracts are deployed locally, and we try to attack the system and break it.
5. **Unit testing** – run unit tests to ensure that the system works as expected. Potentially we write our unit tests for specific suspicious scenarios.

FINDINGS

We began our review by using static analysis tools and then took a deep dive into the logic of the contract, this led to the following findings:

8 low severity and **1 medium** severity issue were identified.

CONCLUSION

The overall code quality is very good and the architecture is well designed. The protocol is well documented in the whitepaper, Gitbook documentation, and in the code.

We identified only a few hypothetical issues that were not directly exploitable, but we still had to point them out. Most of these were general recommendations rather than security issues.

We **recommended LayerZero** to:

- design some Oracle & Relayer control mechanism for independence;
- use compiler >0.8 with native SafeMath instead of library;
- use compiler no more than six months old;
- use the same compiler version across the whole project;
- do not use floating pragma;
- use 3rd party libraries wisely;
- use assembly code wisely;
- remove unused code.

All findings were **acknowledged and fixed** by LayerZero development team except 3 low severity issues that have been descoped and they will be reviewed in different audits.

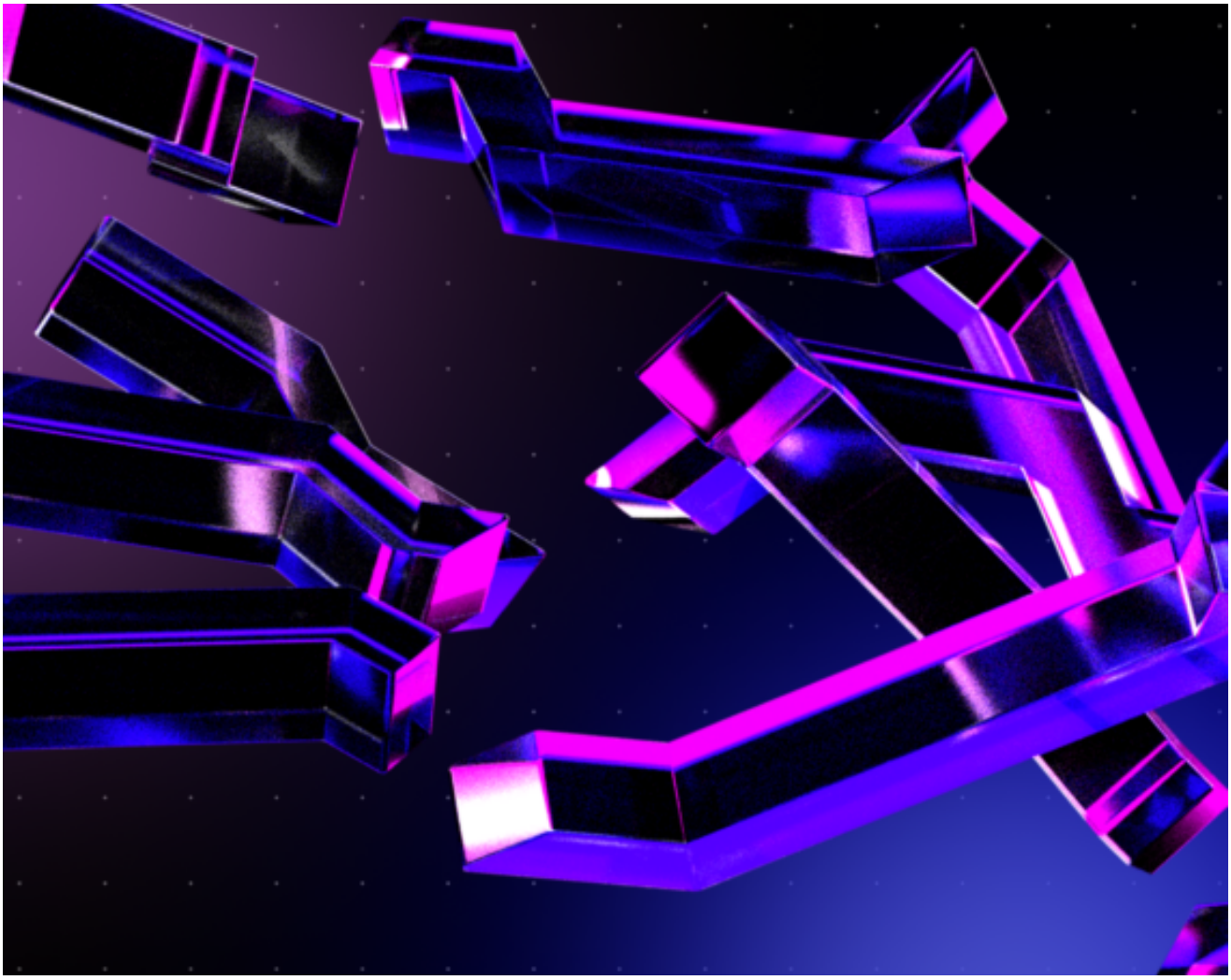
We were delighted to audit **LayerZero – an omnichain interoperability protocol** and we look forward to further cooperation.

The full Ackee Blockchain audit report of LayerZero protocol with a more detailed description of all findings and recommendations can be found here.

Audit Bridge Ethereum EVM Interoperability Layerzero Omnichain

Andrea Nováková

You May Also Like

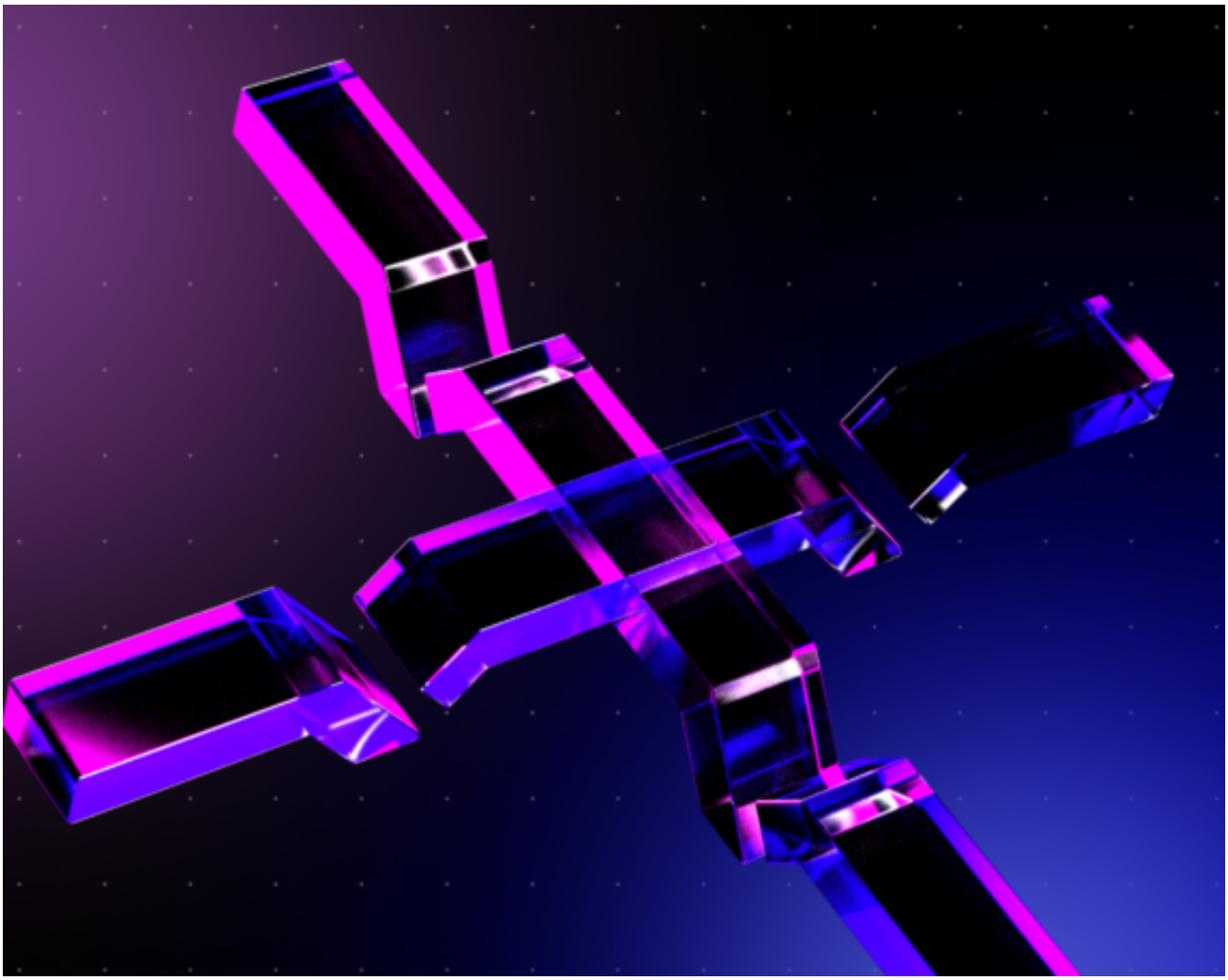


// EDUCATION, ETHEREUM, HACKS, TUTORIAL, WAKE JULY 11, 2024

Cross Contract Reentrancy Attack

// AUDITS ETHEREUM JULY 9, 2024

Catalyst's Incentivized Message Escrow Revision 2.0 Audit Summary



// EDUCATION, ETHEREUM, HACKS, TUTORIAL, WAKE JULY 4, 2024

Cross Function Reentrancy Attack