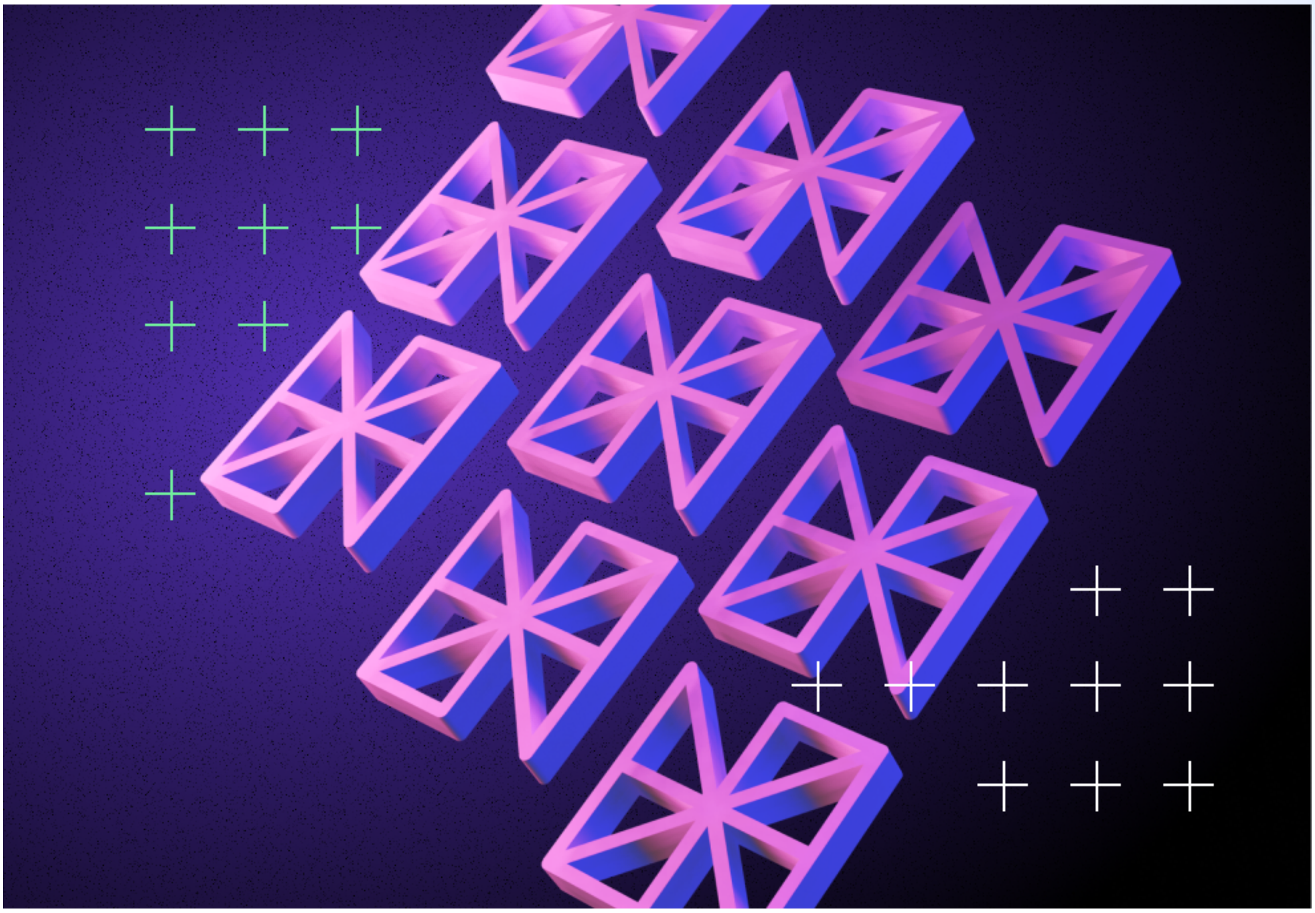
< Back to articles

Neon Labs: SPL Governance Audit Summary

Andrea Nováková // AUDITS, SOLANA JULY 22, 2022



Neon Labs engaged Ackee Blockchain to review and audit their SPL Governance contract between **June 27 and July 22, 2022**. The entire audit process was conducted with a total time commitment of **26 engineering days**. We now publish a summary of our results.

METHODOLOGY

The beginning of the audit was dedicated to understanding the SPL Governance program.

Reviewing the specifications, sources, and instructions provided to us is essential to ensure we understand the project's size, scope, and functionality. This is followed by a detailed manual code review, which is the process of reading the source code line by line to identify potential vulnerabilities.

When the code review is complete, we run client's tests to ensure the system works as expected and potentially write missing unit or fuzzy tests using our testing framework Trdelnik. We also deploy programs locally and try to attack and break the system.

SCOPE

We audited commit *f13d7e7c1507819306797688ce0bb1f6950a5038* of the neonlabsorg/neon-spl-governance repository, specifically programs: *maintanance/program, addin-fixed-weights/program, addin- vesting/program, governance-lib.*

During the security review, we paid particular attention to the following questions:

- Is the correctness of the custom addins ensured (does it correctly implement spl-governance contract specification)?
- Do the program correctly use dependencies or other programs they rely on (e.g., SPL dependencies)?
- Is the code vulnerable to voting manipulation?

FINDINGS

Here we present our findings.

Critical severity

C1: Possibility to manipulate a voting process while using the fixed-weights addin

C2: When using the addin-vesting (for realm), the first user will be able to decide on any proposal after his deposit

High severity

No high severity issues were found.

Medium severity

M1: Possibility to decide on a proposal without a sufficient voting weight

M2: Possibility of a DoS attack that prevents the creation of a valid maintenance record

Low severity

L1: Using find_program_address instead of create_program_address

Warning severity

No warning severity issues were found.

Informational severity

I1: Unused account

I2: Misleading docs

I3: Hanging accounts

CONCLUSION

Our review resulted in **8 findings** ranging from *Informational* to *Critical* severity.

The most severe one (C1) would allow the attacker to increase the weight of their vote to such an extent that they could practically decide on any proposal themselves. It was immediately reported to the client.

We recommended Neon Labs to:

- address all reported issues;
- monitor the SPL governance program and apply major changes in the future, as the program is still in active development.

Update: On **September 5, 2022**, Neon Labs provided an updated codebase that addresses the reported issues. All of the findings were acknowledged and some of them fixed (C1, M2, I1, I2, partially I3). A detailed discussion of the exact status of each issue can be found in Appendix A of the report.

Ackee Blockchain's full *SPL Governance contract* audit report with a more detailed description of all findings and recommendations can be found here.

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

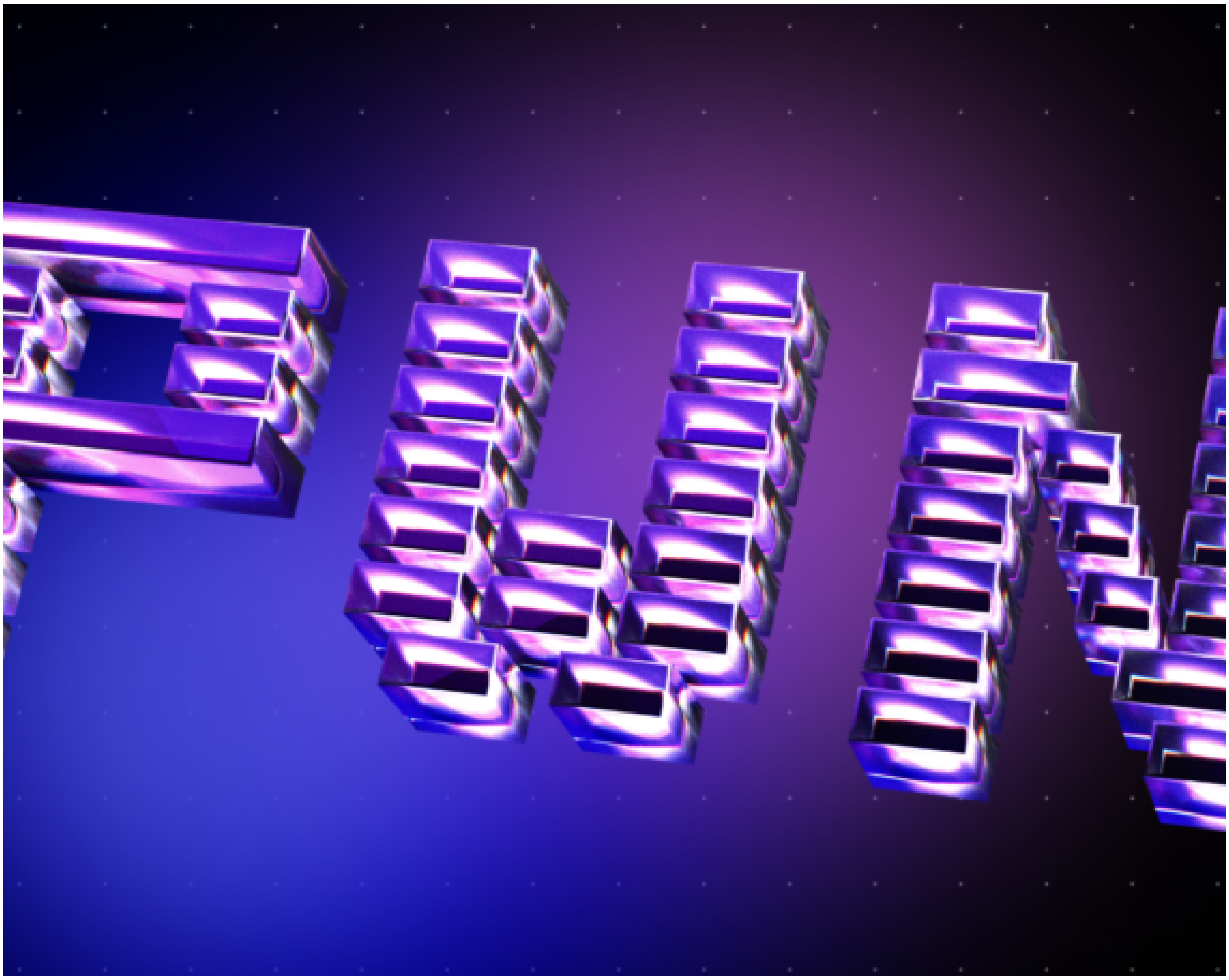
Audit Blockchain Cryptocurrency Findings Security Solana Solana Security

Andrea Nováková

You May Also Like

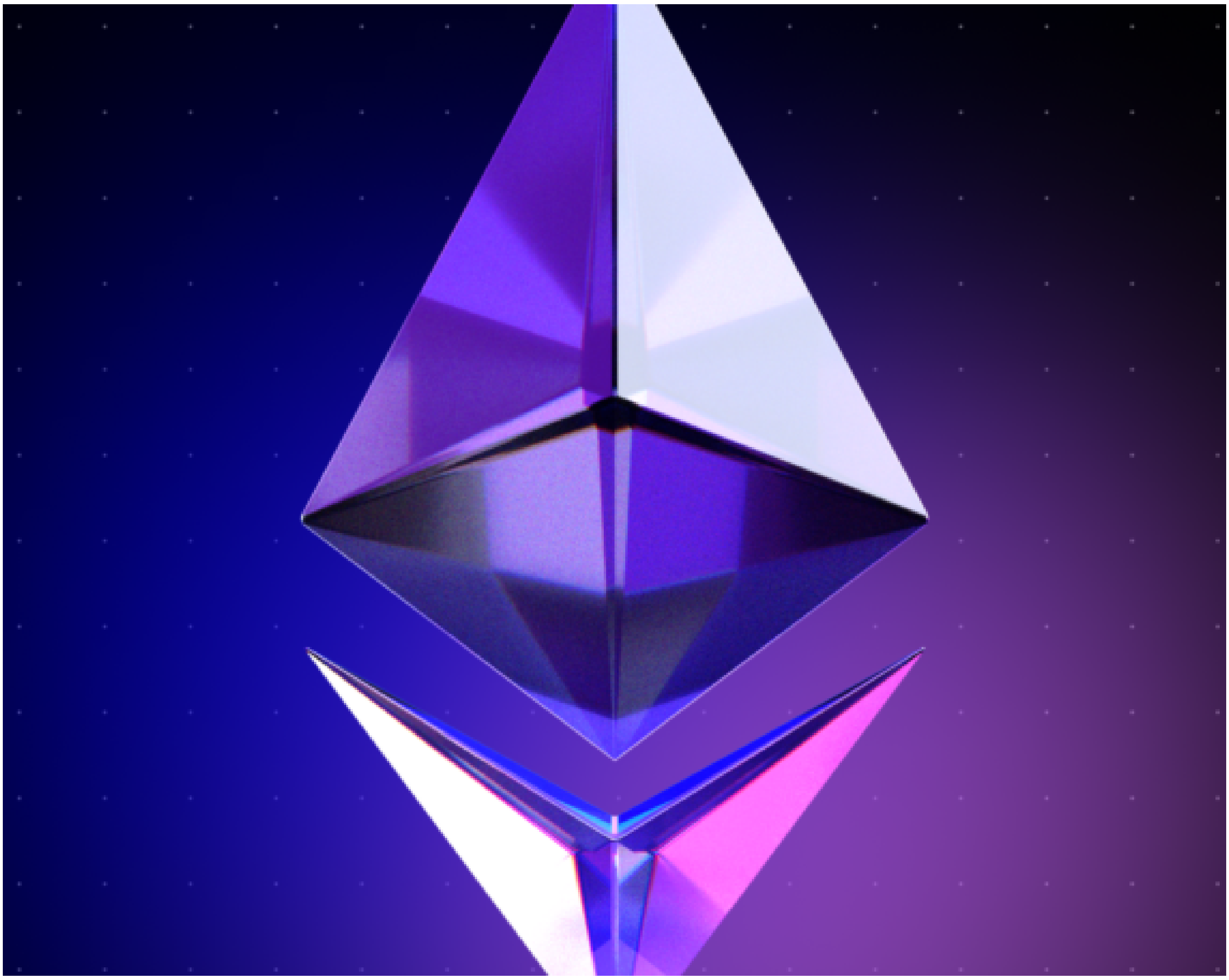
// AUDITS, ETHEREUM, WAKE FEBRUARY 12, 2025

Leech Protocol Audit Summary



// AUDITS, ETHEREUM, WAKE FEBRUARY 6, 2025

PWN Protocol Audit Summary



// EDUCATION NOVEMBER 27, 2024

Ethereum’s Pectra upgrade from the security perspective