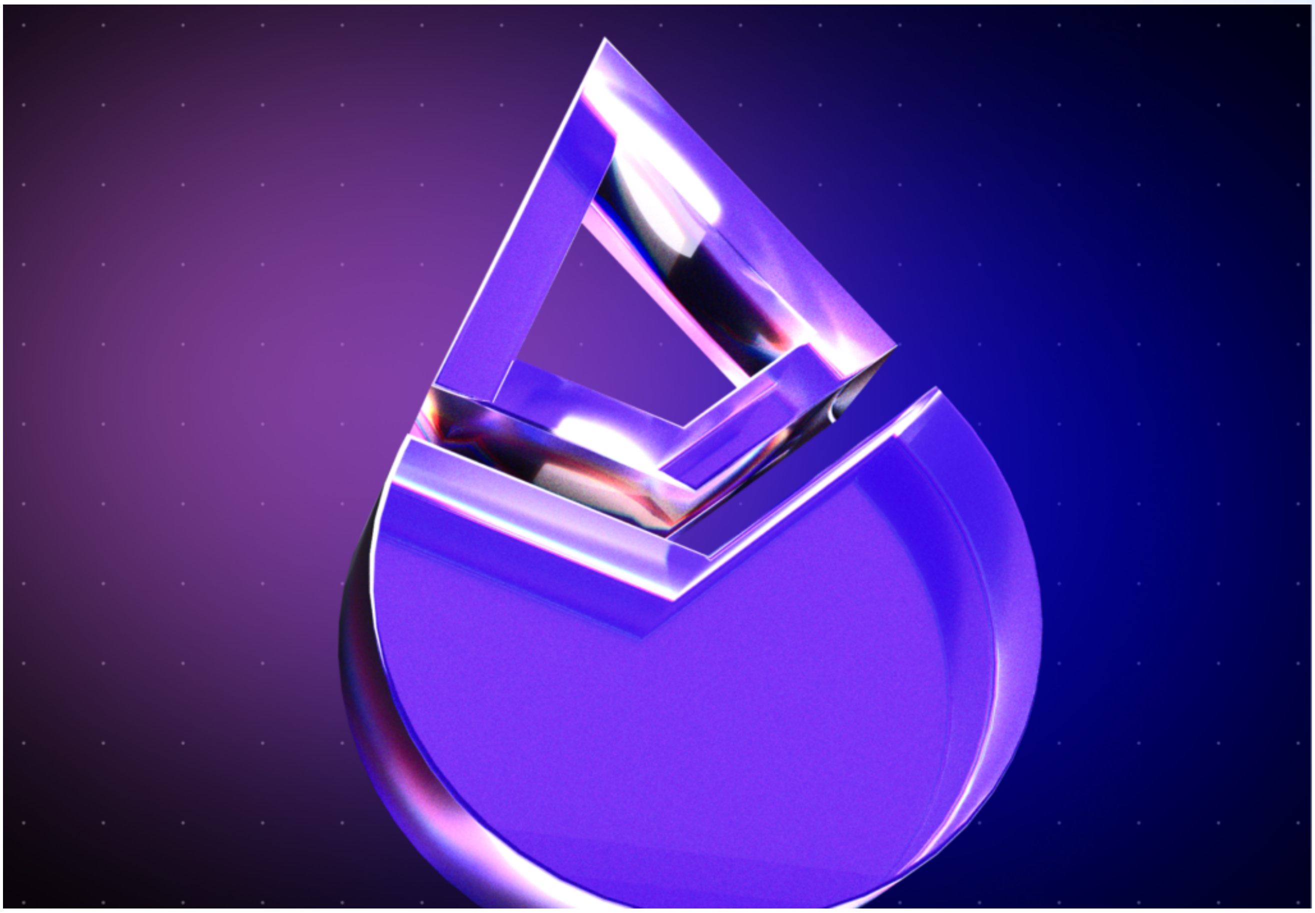
< Back to articles

Lido Simple Delegation Audit Summary

Andrey Babushkin // AUDITS, ETHEREUM, WAKE AUGUST 9, 2024



Lido Finance Simple Delegation allows LDO token holders to delegate their voting power to other addresses and delegates to participate in on-chain voting on behalf of their delegated voters.

Lido Finance engaged Ackee Blockchain to perform a security review of the Lido Finance Simple Delegation for a total of 10 engineering days in a period between Mar 18 and Mar 28, 2024.

Lido Finance also engaged Ackee Blockchain to perform a fix review of findings in Revision 1.0 on commit `e3cef8c`. Three out of ten findings were fixed, the remaining seven findings were acknowledged by the team with explanations. Lido Finance added several new tests and improved the documentation of private functions.

Revision 2.0

Lido Finance engaged Ackee Blockchain to perform an incremental review of the Simple Delegation project with a total time donation of 2 engineering days in a period between Jun 27 and Jul 1, 2024.

Lido Finance engaged Ackee Blockchain to perform a fix review of the findings discovered in the previous revision on commit `50d9802`. Three out of four findings were fixed, and one informational finding was acknowledged. Except for the fixed findings, two minor changes were made to the codebase to improve readability and gas usage. The new changes were reviewed as well. See Revision 2.1 for the details of the updated codebase.

METHODOLOGY

We began our review using static analysis tools, including Wake. We then took a deep dive into the logic of the contracts. For testing and fuzzing, we have involved the Wake testing framework.

A complex, fully differential fuzz test was prepared to ensure the system's correctness. The fuzzing was performed with the bytecode generated by the Solidity compiler in version 0.4.24 with the optimizer enabled.

During the review, we paid special attention to:

- ensuring the code is not subject to bugs of the outdated compiler version,
- the voting logic is correct and is not affected by the additional delegation logic,
- ensuring the arithmetic of the system is correct, and there are no overflows or underflows in the arithmetic operations,

- the upgradeability is implemented and used correctly,
- detecting possible reentrancies in the code,
- ensuring access controls are not too relaxed or too strict,
- looking for common issues such as data validation.

Revision 2.0

The review began with the migration to Solidity 0.6.2 needed to run Wake static analysis detectors. We then continued updating the fuzz test prepared in the previous revision and performed an incremental manual review in parallel with the fuzzing.

During the review, we specifically checked:

- the refactoring did not introduce new ways to exploit the system,
- the code style and readability remained at a high level.

SCOPE

The scope includes the implementation of voting for Lido DAO with the simple delegation of votes. The audit was performed on commit `08d43e3`, and the scope was the following:

- Voting.sol

Revision 2.0

The audit was performed on the commit `079dd88` with the file Voting.sol as the scope.

FINDINGS

Here we present our findings.

Critical severity

No critical-severity issues were found.

High severity

No high-severity issues were found.

Medium severity

No medium-severity issues were found.

Low severity

No low-severity issues were found.

Warning severity

W1: Usage of `solc` optimizer

W2: Delegation does not expire

W3: The initializer can be front-run

W4: The initializer does not have validations for the correctness of `_token`

W5: Declaration shadowing

W6: Unused function parameters

W7: Outdated Solidity version

W8: Division rounding error

W9: Set delegate with zero voting power

W10: Inconsistent `attemptVoteForMultiple` checks

Information severity

I1: Unused function

I2: Reserved keyword

I3: Cache array length

I4: Incorrect NatSpec format

CONCLUSION

Our review resulted in 10 warnings. In addition, we have concerns about the very concept of vote delegation. Vote delegation is a powerful tool that can increase voter turnout, but it can also centralize power in the hands of a few. Moreover, this mechanism can be potentially misused (see the original report, issue W2: Delegation does not expire). Since Lido has a strong influence on the Ethereum ecosystem, we encourage the team to consider a different approach to address voter apathy that would be more conducive to decentralization.

Revision 2.0

The static analysis yielded the I1 finding, and our review resulted in 4 informational findings. The vote delegation concept remained unchanged.

Ackee Blockchain recommends Lido Finance to:

- consider using the latest Solidity version to take advantage of the latest optimizations and bug fixes,
- consider a different approach to address voter apathy that would be more conducive to decentralization,
- address all other reported issues.

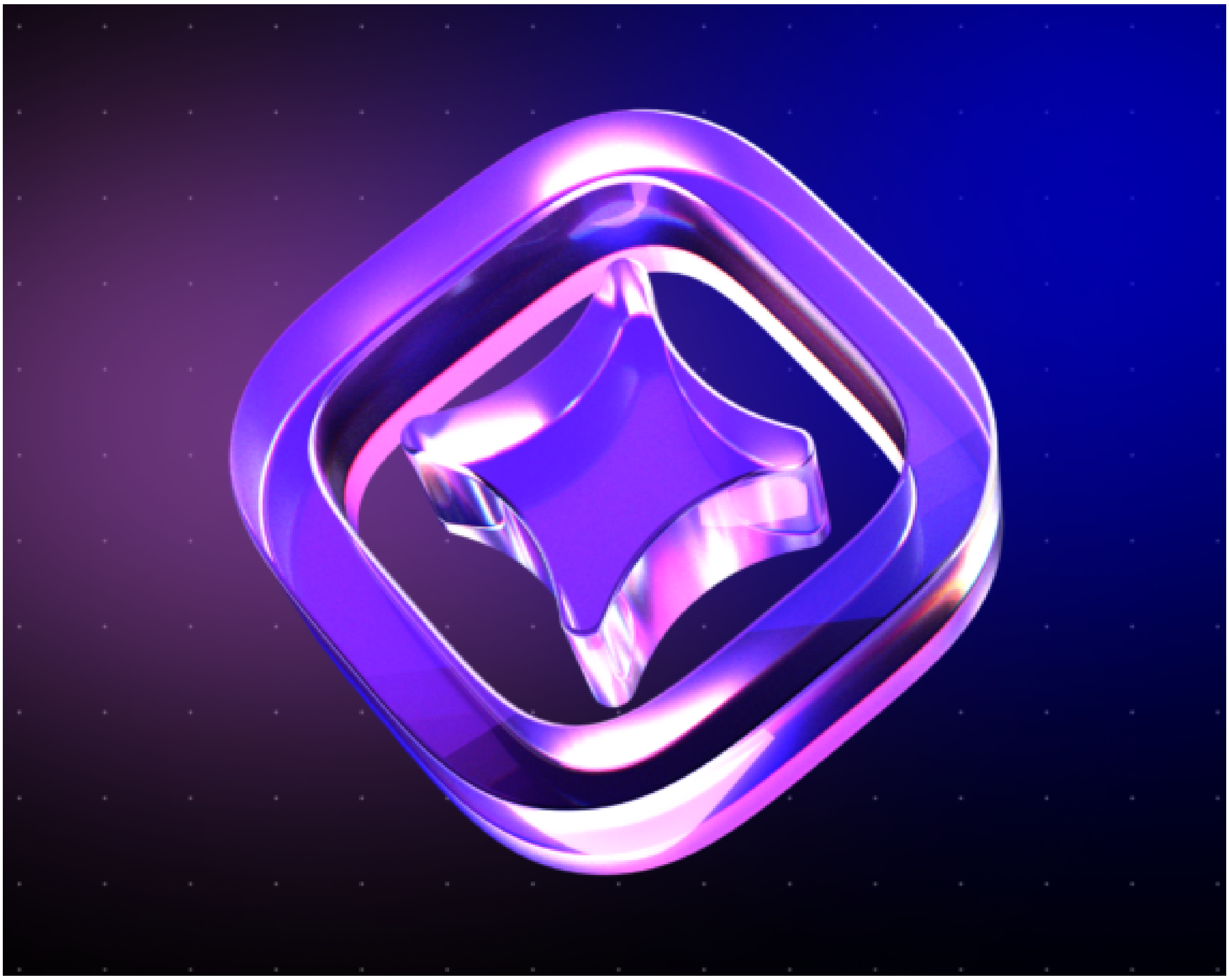
Ackee Blockchain's full Lido Finance audit report, which includes a more detailed description of all findings and recommendations, can be found here.

We were delighted to audit Lido Finance and look forward to working with them again.

Audit Summary Lido Wake

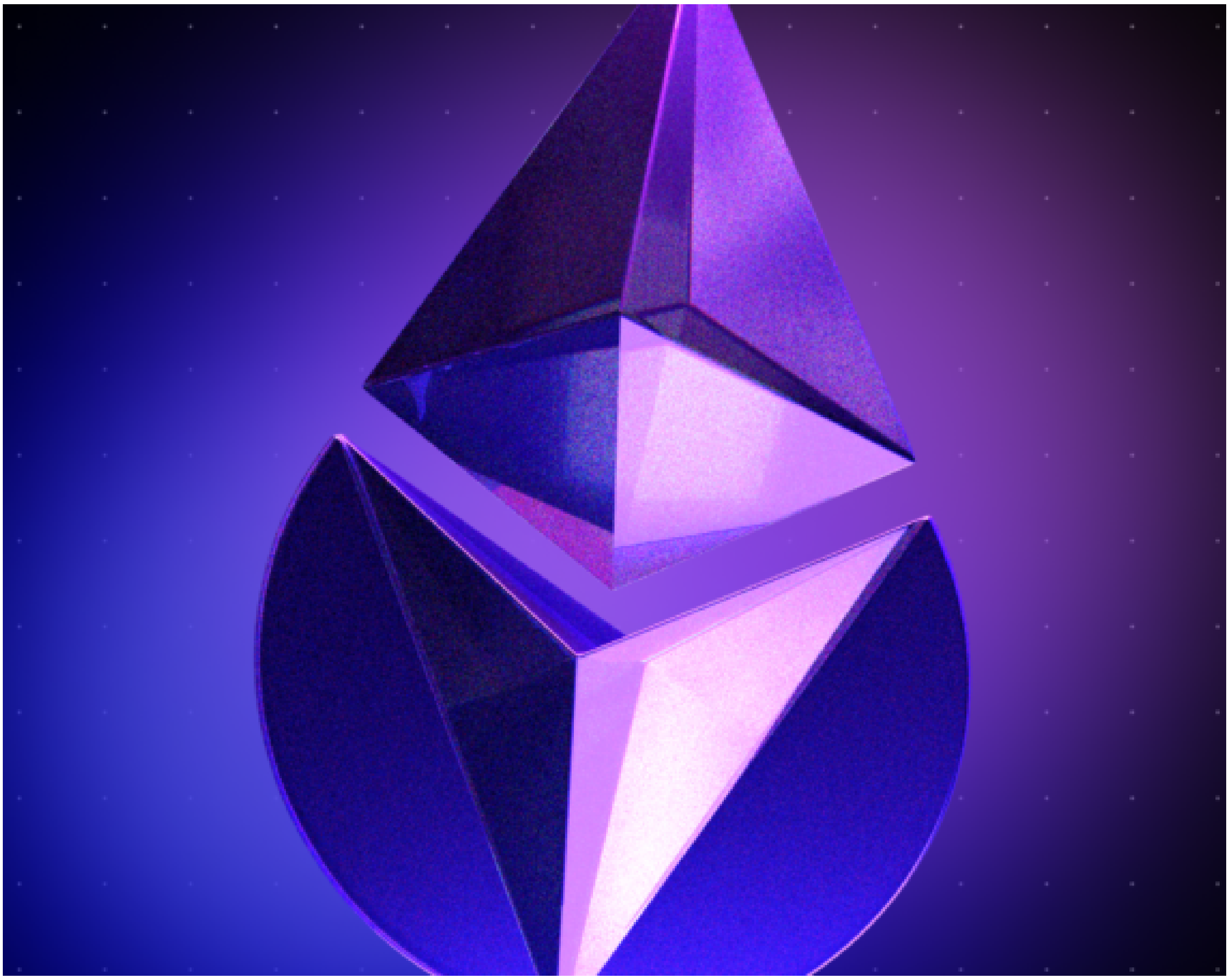
Andrey Babushkin

You May Also Like



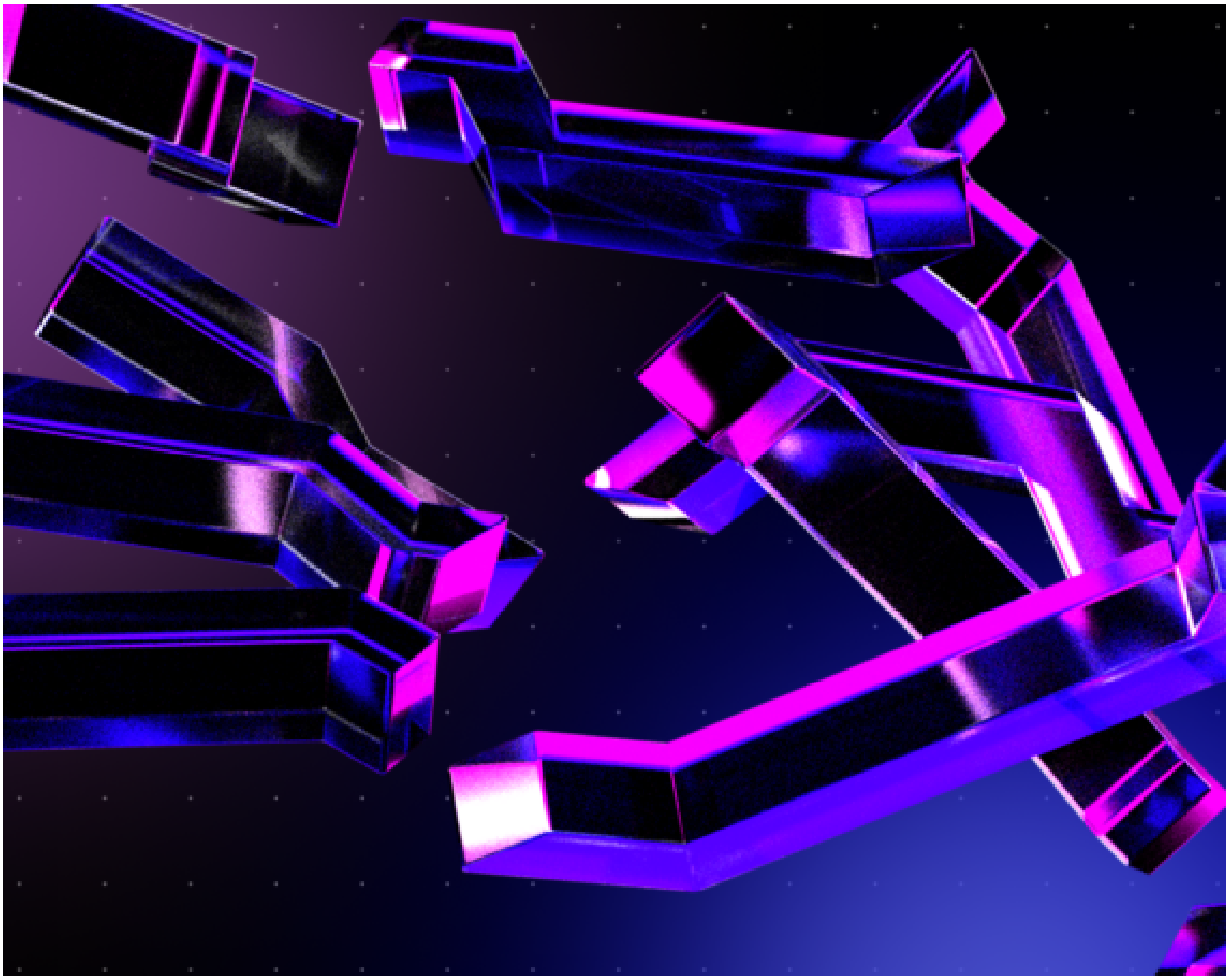
// AUDITS, ETHEREUM, WAKE AUGUST 2, 2024

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