Lido on Polygon V2

Contract Audit Report

VER 1.1

10 May 2022

No. 2022051017001

Project Summary

1. Project Introduction

Lido on Polygon V2 is an updated version of the Lido proxy stake protocol on matic network. Based on the original proxy stake management, the logic of Delegation and Rebalance, Request Withdrawal, and Node Operator Registry has been updated, removing unnecessary management logic and making the rewards received by the validator fairer.

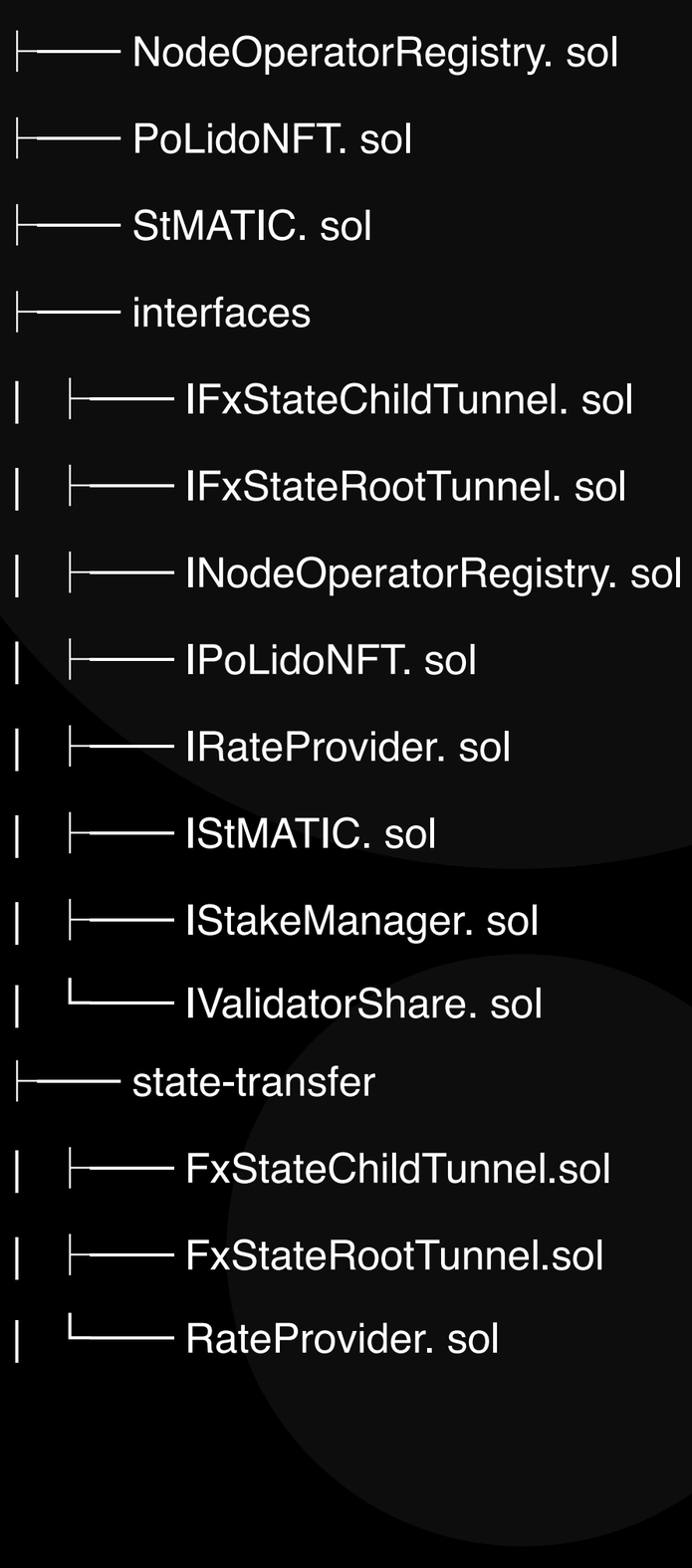
2. Audit Summary

Project Name	Lido on Polygon V2	**Platform**	N/A
Token	N/A	**Token symbol**	N/A
Start date	11 Apr 2022	**Language**	Solidity
End date	29 Apr 2022	**Website**	https://polygon.lido.fi/
Github	https://github.com/Shard-Labs/PoLido-V2/tree/6b18e23ae258ff0aa84aecb82d8498f3c52f29e4	**Whitepaper**	https://almanac.io/docs/polido-v2-a2zsdB3XWDaUDgE6DYymLGIF62o9UGGx

3. Audit Scope

ID	File	SHA-256 checksum
contracts	NodeOperatorRegistry.sol	0c96605c1b6cb376be9f009fd96cee09dcb5af5fb1d7c1803833cc7be3bfe1ef
contracts	StMATIC.sol	7be08dcbc6e6837135fede03337e7a8a6891def3b57917111abde067dbae1e70
contracts	PoLidoNFT.sol	350260f7a850c061623b170915abf05cf73ccb8e33d9823869e10e8c8651e03b
contracts/state-transfer	FxStateChildTunnel.sol	24b3220e6c2895f7956d7bb55c37faeeff28bb1add78194b73332bea0bc8d67a
contracts/state-transfer	FxStateRootTunnel.sol	8de8ba41153f7d4e0eeb032c88c4c51d3778a9deb9aa6f764260848689fe81df
contracts/state-transfer	RateProvider.sol	0b94737894bb28f11d933cae2123b15d33f03fb1e55bd6cbe0fb1b030961324f

4. Code Structure



Audit Report Summary

1. Audit Methods

The audit was conducted to gain a clear understanding of how the project was implemented and how it works. The audit team conducted in-depth research, analysis, and testing of the project code and collected detailed data. In this report, the audit team will list in detail each issue identified, where it is located, the root cause of the issue, and a description of the issue, and will recommend changes to the issue accordingly.

Audit methods	Static analysis, Manual Review

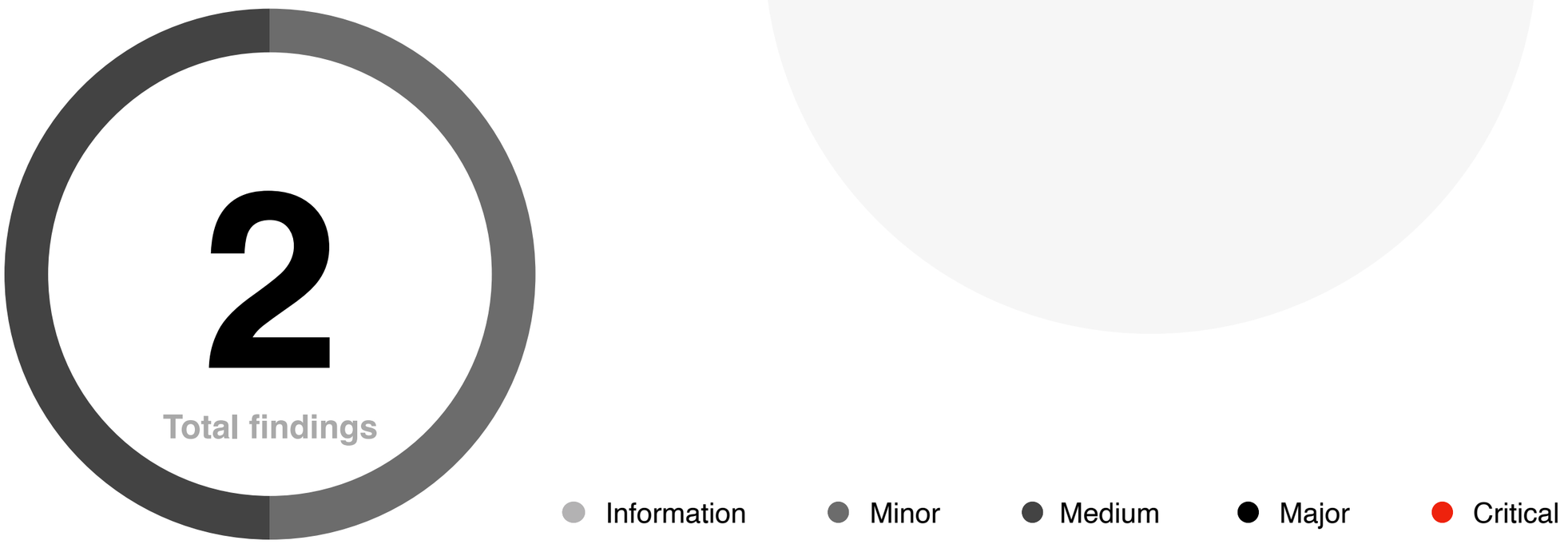
2. Audit Process

Steps	Operation	Description
1	Background	Read project descriptions, white papers, contract source code, and other relevant information the project team provides to ensure a proper understanding of project functions.
2	Automated testing	Scanning source code mainly with automated tools to find common potential vulnerabilities.
3	Manual review	Engineers read the code line by line to find potential vulnerabilities.
4	Logical proofread	The engineer will compare the understanding of the code with the information provided by the project and check whether the code implementation is in line with the project white paper information.
5	Test case	Including test case design, test scope analysis, symbolic execution, etc.
6	Optimization items	Review of projects in terms of maintainability, safety, and operability based on application scenarios, deployment methods, and latest research results.

3. Risk Levels

Risk level	Issue description
Critical	Fatal risks and hazards that need to fix immediately
Major	Some high risks and hazards will lead to related problems that must be solved
Medium	Some moderate risks and pitfalls may lead to potential risks that will eventually need to be addressed
Minor	There are low risks and hazards, mainly details of various types of mishandling or warning messages, which can be set aside for the time being
Information	Some parts can be optimized, such problems can be shelved, but it is recommended that the final solution

4. Audit Results



ID	Audit project	Risk level	Status
1	Reentrancy	None	
2	Injection	None	
3	Authentication bypass	None	
4	MEV Possibility	None	
5	Revert	None	
6	Race condition	None	
7	Insufficient Gas Griefing	Medium	Acknowledged
8	The major impact of flash loans	None	
9	Unreasonable economic model	None	
10	Predictable random numbers	None	
11	Voting rights management confusion	None	

ID	Audit project	Risk level	Status
12	Privacy leak	None	
13	Improper use of time on chain	None	
14	Improper codes in fallback function	None	
15	Improper identification	None	
16	Inappropriate opcode	None	
17	Inappropriate assembly	None	
18	Constructor irregularities	None	
19	Return value irregularity	None	
20	Event irregularity	None	
21	Keywords irregularity	None	
22	Not following ERC standards	None	
23	Irregularity of condition judgment	Minor	Acknowledged
24	Risk of liquidity drain	None	
25	Centralization Risk	None	
26	Logic change risk	None	
27	Integer overflow	None	
28	Improper function visiblity	None	
29	Improper initialization of variables	None	
30	Improper contract calls	None	
31	Variable irregularities	None	
32	Replay	None	
33	Write to Arbitrary Storage Location	None	
34	Honeypot logic	None	
35	Hash collision	None	
36	Improper logic in receiving awards	None	
37	Use the not recommended method	None	
38	Basic coding principles were not followed	None	

*In the above table, if the status column is **Acknowledged**, the audit team has informed the project owner of the vulnerability. Still, the project owner has not made any changes to the vulnerability or has not announced to the audit team the progress of the changes to the vulnerability. If the status column is **Resolved**, the project owner has changed the exposure, and the audit team has confirmed the changes.

5. Risk and Modification Program

The following section provides detailed information about the risk items learned after the audit, including the type of risk, risk level, location of the issue, description of the problem, recommendations for changes, and feedback from the project owner.

Risk type	Insufficient Gas Griefing	**Risk level**	**Medium**
Location	Line 297, Line 319, Line 563	Contract file	StMATIC.sol
Description	There is a loop of unknown size, and there are external calls in the loop.		
Recommendation	Limit the number of loops, or do not make external calls in the loop.		
Update	-		

Risk type	Irregularity of condition judgment	**Risk level**	**Minor**
Location	Line 38, Line 176	Contract file	PoLidoNFT.sol、FxStateRootTunnel.sol
Description	Partial address pass-through to determine whether the address is 0 and what the address type is.		
Recommendation	Add to determine if the parameter address is 0 or if the address is a StMatic contract (using EIP165)		
Update	-		

6. Recommendation

N/A

Disclaimer

i. This audit report focuses only on the types of audits identified in the final report issued. Other unknown security vulnerabilities are not part of this audit, and we do not accept responsibility for them.

ii. We shall only issue an audit report based on an attack or vulnerability that existed or occurred before the issuance of the audit report. We cannot determine the likely impact on the security posture of our projects for new attacks or vulnerabilities that may exist or occur in the future, and we are not responsible for them.

iii. The security audit analysis and other elements of our published audit report shall be based solely on documents and materials (including, but not limited to, contract codes) provided to us by the Project Party before the release of the audit report. Such documents and materials shall not be untrue, inaccurate, uninformative, altered, deleted, or concealed, and if the documents and materials provided by the Project Party are false, inaccurate, uninformative, changed, deleted or hidden, or if the documents and materials provided by the Project Party are untrue, inaccurate, uninformative, altered, deleted or concealed, or if the documents and materials provided by the Project Party are uninformative, uninformative, altered, deleted or hidden. If the records and information provided by the Project Party are untrue, inaccurate, uninformative, altered, deleted, or concealed, or if changes to such documents and information are made after the issuance of the audit report, we shall not be liable for any loss or adverse effect arising from any inconsistency between the reflected and actual conditions.

iv. The Project Parties are aware that our audit report is based on documents and information provided by the Project Parties and relies on the technology currently available. However, due to the technical limitations of any organization, there is a possibility that our audit report may not fully detect all risks. Our audit team encourages the project development team and any interested parties to conduct subsequent testing and audits of the project.

v. The project owner warrants that the project for which we are engaged to provide audit or testing services is legal, compliant, and does not violate applicable laws. The audit report is for the project owner's reference only, and the contents, manner of obtaining, use of, and any services or resources involved in the audit report shall not be relied upon for investment, tax, legal, regulatory, or advisory purposes of any kind, and we shall not be liable therefor. The Project Party shall not refer to, quote, display, or send the Audit Report in whole or in part to any third party without our prior written consent. The Project Party shall bear any loss or liability arising from that place. We assume no responsibility for any reliance on or use of the audit report for any purpose.

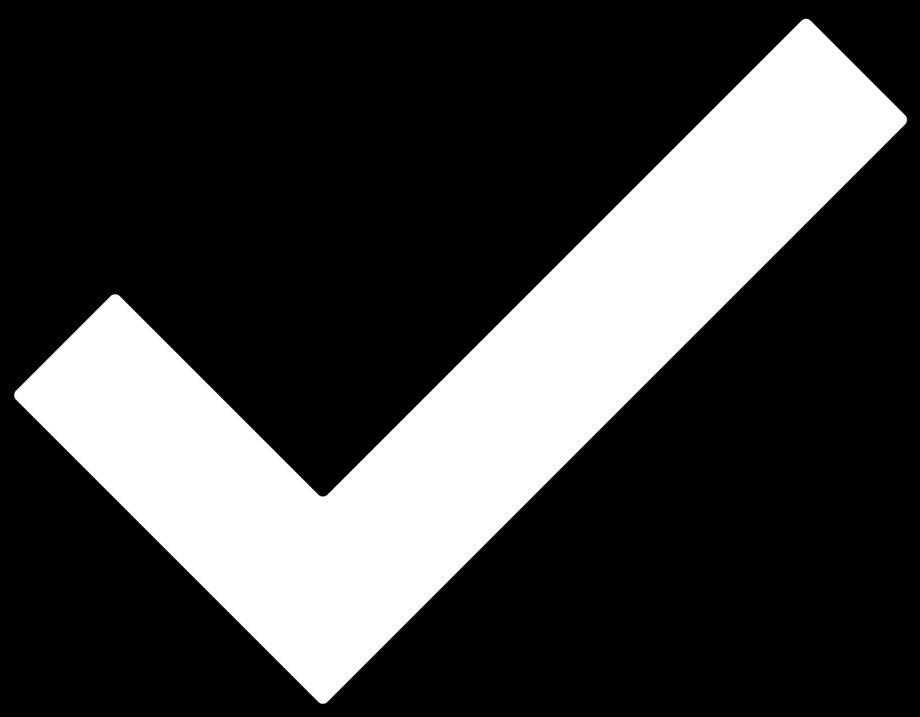
vi. This audit report does not cover the compiler of the contract or any areas beyond the programming language of the Smart Contract. The risk and liability of the audited Smart Contract arising from references to off-chain information or resources is the sole responsibility of the project party.

vii. Force Majeure. Force majeure means an unforeseen event whose occurrence and consequences cannot be avoided and cannot be overcome by the parties at the time of entering into the contract, including but not limited to natural disasters such as war, typhoon, flood, fire, earthquake, tidal wave, lightning, natural disaster, strike, nuclear explosion, epidemic and other unforeseen events such as changes in laws, regulations and policies and governmental acts, whose occurrence and consequences cannot be prevented or avoided, and which contains, affects or delays the performance by either party of all or part of its obligations under the contract.

viii. Suppose either party believes that the occurrence of force majeure affects the performance of its obligations under this Agreement. In that case, it shall promptly notify the other party and, depending on the extent of the effect of the event on the performance of the Agreement; the parties shall consult to determine whether to terminate the Agreement or partially relieve itself of its obligations to perform the Agreement, or to extend the performance of the Agreement.

ix. In force majeure, neither party shall be deemed in breach or non-performance of its obligations under this Agreement. Any financial commitments existing before the event shall not be affected, and the project party shall make payment for work performed by us.

10 May 2022



Passed.

Date	10 May 2022
Audit Team	歐科雲鏈

The purpose of this audit is to review the matic node stake agent, validator management, ERC20 stake credentials, NFT withdrawal credentials, and other protocols written in Solidity language for the PoLido project, to study their design and architecture, to discover potential security risks and to try to find possible vulnerabilities.