AUDIT METHODOLOGY

DISTRIBUTED LAB

What is an Audit?

An audit is an extensive review of the system that embraces the analysis of the **system's solvency**, **hack-proofness**, and **coincidence** with the expected business logic. The review is done manually by the senior solidity developer(s) with bug-bounty-hunting experience and an inclination towards the code-perfectionism.

The audit results are presented in the form of a technical PDF with the descriptive findings, their severity, and suggestions for their mitigation.

The system reviewed will be labeled as **secure** if there were no vulnerabilities found during the audit. In case of bugs discovery, the client will be inquired to resolve the findings and asked if they wished to proceed with the reaudit. Several reaudit sessions might occur with the security acceptance criteria of bugs' mitigation mutual agreement.

What is included in the Audit?

The **Solidity** audit includes the in-depth review of the smart contract in-scope together with the shallow review of the out-of-scope contracts that might influence the in-scope behaviour.

The audit is not limited to the solidity, it might also cover the integration with 3’rd party protocols like **The Graph**.

How is the Audit conducted?

01

Acquaintance with the system. The auditor will negotiate the system details and caveats with the client to minimize the context-switch friction.

02

Static analysis. The auditor will hover through the code to spot obvious mistakes, typos, code smell, misinitialization, and ways of optimization. The auditor will also run static-analysis tools such as Slither to cover the less obvious errors such as code unreachability.

03

Business logic/code flow due diligence. The auditor will accurately follow the code flow and try to catch any unhandled edge cases. They will also meticulously compare the business logic realization with the concept and try to find any imperfections and contradictions (such as upgradeability). The auditor will also verify the correctness of the integration with the external protocols.

How is the Audit conducted?

04 **Hack-proofness examination**. The auditor will intentionally try to break the system as if they were bounty-hunting. Precisely, the auditor will implement exploiter contracts, apply several common attacks, and check the system's ability to resist.

05 **Known bugs**. The auditor will check the system’s stack against the known and resolved bugs list to estimate the potential side effects. This includes compiler bugs, bugs in obsolete libraries, etc.

06 **Optional report design**. The designer will polish the assembled report to uniquely match the aesthetics of the project being audited. They will add summarizing infographics and refresh the look of the document.

Audit cost & estimations

Each audit is evaluated individually in a transparent-to-client way and the estimate mostly depends on the system’s complexity, size, and the auditing scope. The client is free to pay 50% upfront and the rest upon the audit completion.

Distributed Lab public Audits

- Tornado Cash
- Pollen DEFI
- NFTxCards