ANASTASIA LABS

Proof of Achievement - Milestone 1

OpShin Audit

Project Number 1200175
Project Manager Jonathan Rodriguez

ANASTASIA LABS

Contents

Project Name: OpShin Audit
URL: Catalyst Proposal

Project Goal

The primary goal of the OpShin audit project is to enhance the reliability and security of smart contracts developed using the OpShin language within the Cardano ecosystem. This is achieved through a comprehensive audit that identifies vulnerabilities, addresses edge cases, and optimizes the language's efficiency. By emphasizing transparency and collaboration, the project aims to support developers with detailed documentation and best practices, ultimately elevating the quality of smart contracts. The anticipated outcomes include a significant reduction in reported vulnerabilities and the establishment of a robust foundation for safe and trustworthy smart contract development on Cardano.

Project Deliverables

OpShin Language Analysis

- **Deliverable**: **Detailed Analysis Report**
  - **Description**: The audit team will produce a comprehensive report that identifies vulnerabilities and areas for improvement within the OpShin language codebase.
  - **Key Activities**:
    - Utilize automated analysis tools to support findings.
    - Conduct unit tests to evaluate the functionality of the code.
    - Perform manual assessments to complement automated analyses.
  - **Outcome**: This report will serve as a foundational document for understanding the current state of the OpShin language and guiding future enhancements.

Edge Case Identification

- **Deliverable**: **Documented List of Edge Cases**
  - **Description**: The audit team will compile a thorough list of edge cases relevant to the development of smart contracts using OpShin.
  - **Key Activities**:
    - Identify and document edge cases through extensive manual analysis.
    - Propose strategies for addressing these edge cases that can be applied in future iterations of the language.
    - Utilize tailored analysis tools to support the identification process.
  - **Outcome**: This documentation will provide valuable insights into potential pitfalls in smart contract development, helping developers avoid common errors.

Draft Audit Report Preparation and Feedback Integration

- **Deliverable**: **Comprehensive Audit Report**
  - **Description**: The audit team will compile a detailed audit report that outlines identified vulnerabilities, recommended fixes, and best practices for the development of OpShin.
  - **Key Activities**:
    - Document vulnerabilities and provide actionable recommendations.
    - Collaborate with the OpShin team to integrate feedback and address reported issues in the codebase.
    - Ensure that the audit report reflects the most current state of the code following these integrations.
  - **Outcome**: This report will serve as a crucial resource for developers, guiding them in improving the reliability and security of smart contracts written in OpShin.

Public Dissemination and Resolution of Remaining Issues

- **Deliverable**: **Finalized Audit Report and Presentation**
  - **Description**: The finalized audit report will be publicly shared, and the findings will be presented to the Cardano community.
  - **Key Activities**:
    - Disseminate the audit report through appropriate channels to ensure community access.
    - Present findings and recommendations in a format that encourages discussion and further inquiry.
    - Address remaining medium and low-priority findings from the report, ensuring all issues are resolved.
    - Produce a final close-out report summarizing the project outcomes and lessons learned.
    - Create a final close-out video to visually represent the project's achievements and key takeaways.

- **Outcome**: This will enhance community trust and engagement, providing transparency into the auditing process and supporting ongoing improvements in the OpShin language.

Project Timelines

Signatures

Approved Audit Objectives

Purpose of Audit

Audit Objectives

Manual Revision

Our manual code auditing is focused on a wide range of attack vectors, including but not limited to:

- UTXO Value Size Spam (Token Dust Attack)
- Large Datum or Unbounded Protocol Datum
- EUTXO Concurrency DoS
- Unauthorized Data Modification
- Multisig PK Attack
- Infinite Mint
- Incorrect Parameterized Scripts
- Other Redeemer
- Other Token Name
- Arbitrary UTXO Datum
- Unbounded Protocol Value
- Foreign UTXO Tokens
- Double or Multiple Satisfaction
- Locked Ada
- Locked Non-Ada Values
- Missing UTXO Authentication
- UTXO Contention

Approvals

Audit Timeline

Approvals

ANASTASIA LABS

Operational Communication Channels

Communication Channels

Participation Evidence