ANASTASIA LABS

Proof of Achievement - Milestone 1

OpShin Audit

Project Number 1200175
Project Manager Jonathan Rodriguez

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. The project aims to support developers with detailed documentation and best practices, ultimately elevating the quality of smart contracts. The outcomes include a significant reduction in reported vulnerabilities and the establishment of a robust foundation for safe and trustworthy smart contract development on Cardano using OpShin.

Project Deliverables

OpShin Language Analysis

- **Deliverable**: **Detailed Analysis Report**
  - **Description**: The audit team will prepare a comprehensive report that identifies vulnerabilities and areas for improvement within the OpShin language codebase.
  - **Key Activities**: The audit team will conduct high level analysis by evaluating the functionality of the code using the existing unit tests and also perform manual assessments.
  - **Outcome**: This report will be a foundational document for understanding the current state of the OpShin language and guiding future enhancements.

Edge Case Identification

- **Deliverable**: **Edge Case Identification**
  - **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.
  - **Outcome**: This documentation will provide findings from their audit of the opshin project.

Draft Audit Report and Integration of Feedback from Opshin Team

- **Deliverable**: **Comprehensive Audit Report**
  - **Description**: The audit team will prepare 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 get their feedback.
    - OpShin Team will address major issues in the codebase by demonstrating commits, pull requests, or updated documentation.
    - 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 the OpShin team, guiding them in improving the OpShin language.

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**:
    - Publish the final audit report on the official Cardano forum, GitHub, and Medium.
    - OpShin Team will address remaining medium and low-priority findings from the report through pull requests, ensuring all issues are marked.
    - 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, Letting everyone know what's happening into the auditing process and supporting ongoing improvements in the OpShin language.

Audit Objectives

1. **Comprehensive Audit of OpShin Language**: Conduct a thorough audit of the OpShin language used for smart contract development, ensuring meticulous scrutiny of the codebase to identify vulnerabilities and inefficiencies.
2. **Address Edge Cases and Optimize Efficiency**: Identify and address edge cases within the OpShin language to enhance the efficiency and reliability of smart contracts, thereby safeguarding user assets in the Cardano ecosystem.
3. **Engagement of Experienced Professionals**: Collaborate with auditors who have expertise in smart contract development to ensure a robust and informed auditing process.
4. **Facilitate the Auditing Process**: Provide detailed documentation that supports the auditing process, ensuring comprehensive coverage of potential edge cases and vulnerabilities.
5. **Enhance Quality and Security**: Elevate the quality of smart contracts written in OpShin, reinforcing Cardano's reputation as a secure and trustworthy blockchain platform.
6. **Support Openness and Teamwork**: Ensure clear communication and cooperation throughout the audit, taking advantage of OpShin's open-source nature to build trust and get the community involved.

Area of Focus

As part of our auditing process, we will focus on ensuring that the outputs of the smart contract compiler align precisely with the expected behavior defined in the project specifications. The goal is to guarantee that the compiled smart contracts, written in Python, execute exactly as they would in a standard Python environment. This is critical, as the behavior of the compiled contract must match the expectations set by the programmer.

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

- Evaluate the basic syntax and structure of the language.
- Check for consistency with the standard Python environment.
- Identify potential vulnerabilities in the language design.
- Evaluate built-in testing frameworks.
- Analyze the language's runtime performance.
- Evaluate memory management and resource utilization.
- Evaluate the completeness and quality of the standard library.
- Assess the availability and quality of third-party libraries.
- Evaluate the language's ability to handle large-scale projects.
- Review error handling mechanisms.
- Review the quality and completeness of official documentation.

Audit Timeline

Phase 1: Establishing communication channels and identifying time points where both teams can allocate more time will support a healthier audit process and this has taken us extra time, offering multiple timeslots for auditor-developer meetings. The official audit process began at the end of October, instead of the originally estimated September deadline for Milestone 1 submission.

Phase 2: In the weeks 2-3, the audit team will have the Discovery and Planning phase where they will get familiarized with the codebase and project specifications which will cover milestone 2.

Phase 3: Between the weeks 4-10, the auditors will conduct manual review and will perform the following activities which will cover Milestone 3 and Milestone 4

- Perform an in-depth review of the code to identify vulnerabilities.
- Publish the initial findings report.
- Collaborate with the opshin team to gather feedback.
- OpShin team works on described issues and integrates feedback on them into the codebase.
- Integrate the feedback from the OpShin Team and produce a finalized audit report.

Phase 4: The completion of final milestone will take around 1 week wherein the closeout report and final audit report will be published.

Operational Communication Channels

Effective communication is crucial for the smooth progression of the project and ensures that all stakeholders are aligned throughout the audit process.

For this project, we have established **Discord** as the primary operational communication channel with the Opshin team. Discord provides a flexible, real-time platform for ongoing discussions, and quick resolution of queries.

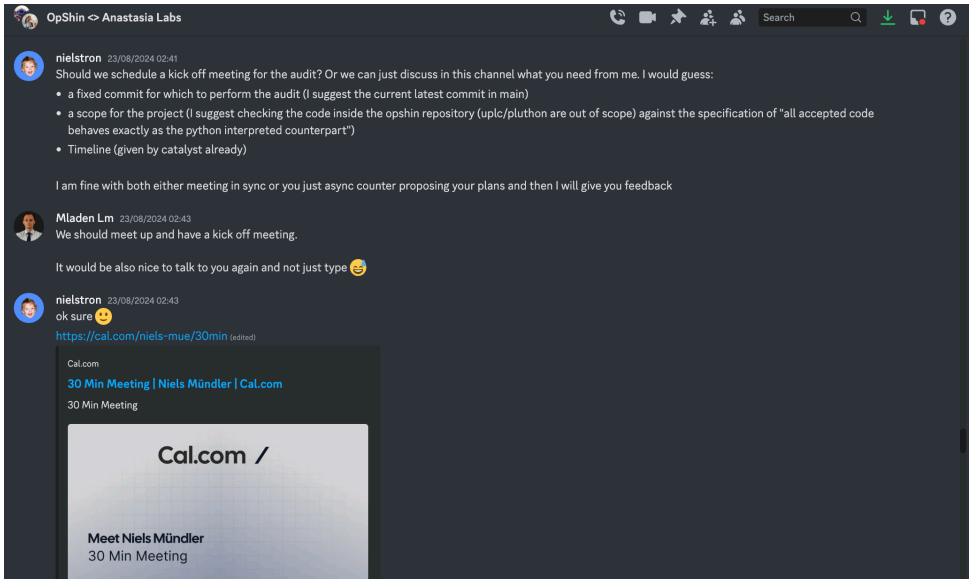
Direct Client Involvement: The OpShin team is part of special channels, so they can get updates, give feedback, and take part in discussions as the project moves forward.

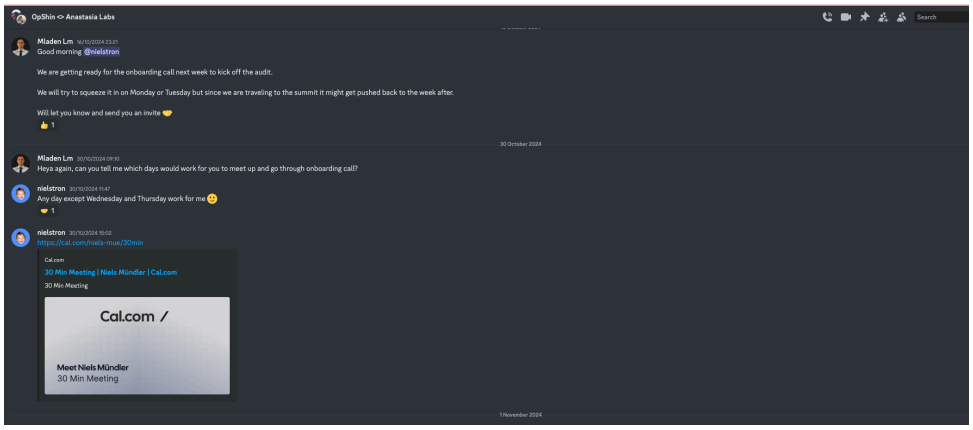
Voice Calls: For more detailed conversations, we use Google Meet for calls, where we can discuss things in real-time and solve problems together.

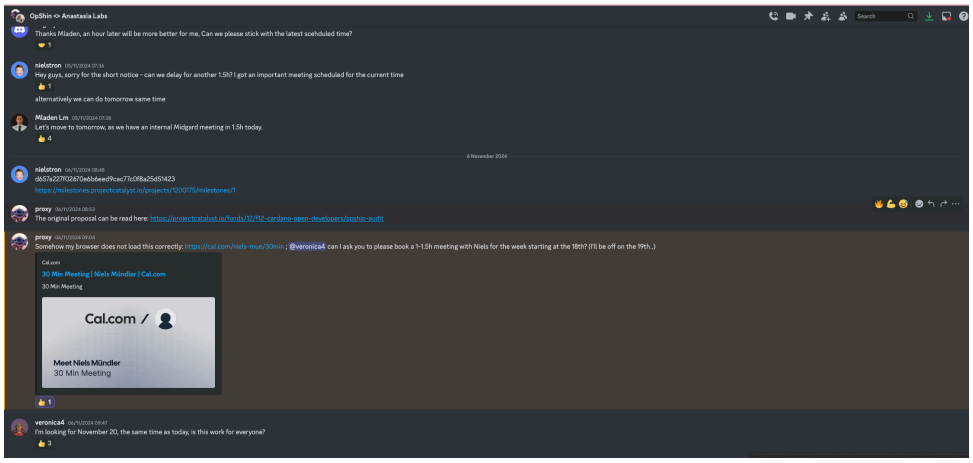
File Sharing: Discord makes it easy to share files, documents, and images, which helps the team exchange important materials and updates without any hassle.

Screenshots of Communication and Active Participation

To provide evidence of active communication, we have included screenshots of Discord conversations that demonstrate active participation from both the OpShin team and the audit team.







Signatures

This Project Scope Document has been reviewed and agreed upon by both parties.

OpShin

Name: Niels Mündler

Signature: 

Anastasia Labs

Name: Mladen Lamesevic

Signature: