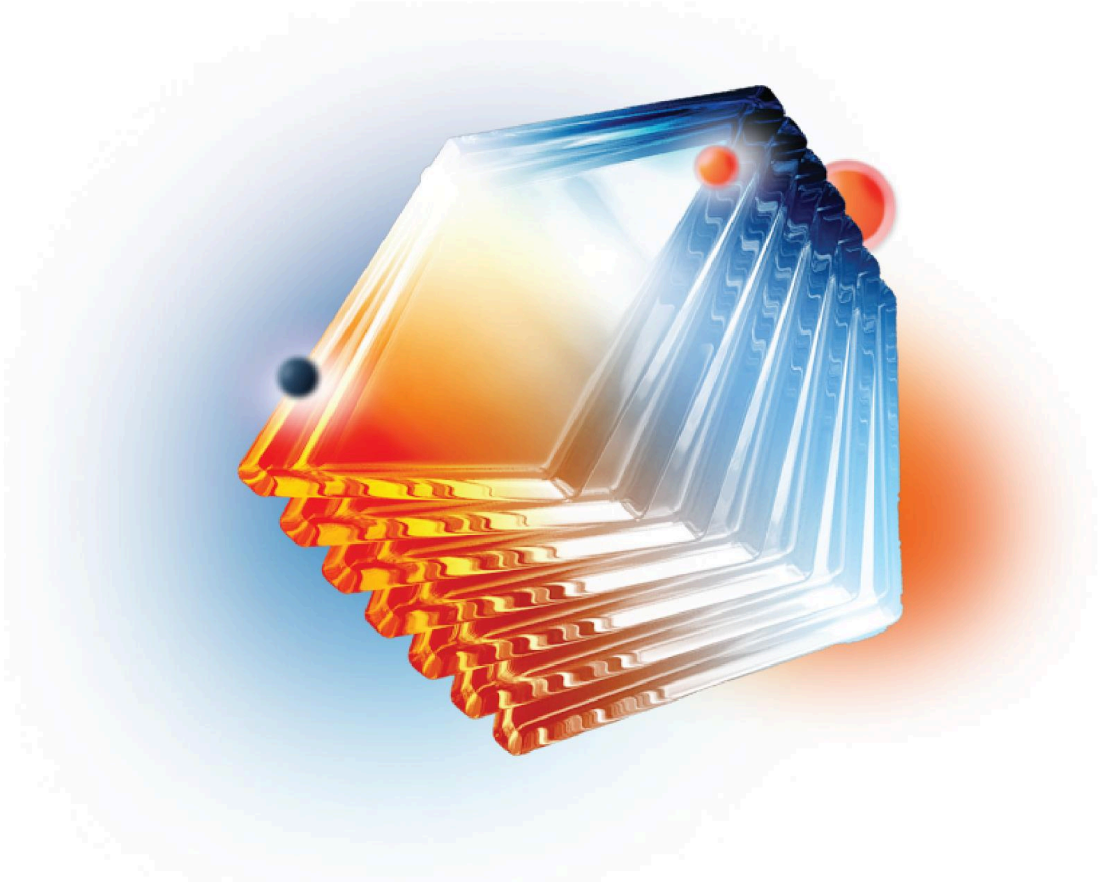

EMURGO Diligence

Profila

Smart Contracts Security Audit Proposal

Table of Contents

Proposal for Audit.....3

Scope of the Audit.....4

Audit Disclaimer.....5

Audit Findings - Severity Classification.....6

Price and Schedule Estimations.....8

Deliverables.....8

Delivery Timelines.....9

Payment Terms.....10

About us.....10

Proposal for Audit

Profila is a decentralized solution that helps its users to share data wisely with brands in exchange for exclusive value in content, products and special offers in a private channel that users control.

This document presents an assessment to be conducted for the Profila smart contracts, aiming to identify potential issues and vulnerabilities within the project's source code, as well as in any associated contract dependencies not originating from officially recognized libraries. The analysis focuses on Manual Review by expert security Auditors.

Key Focus Areas of the Audit:

- Rigorous review of the smart contracts to guard against both typical and atypical attack vectors.
- Evaluation of the codebase to ascertain adherence to the latest best practices and industry benchmarks.
- Verification that the contract logic aligns with the client's specifications and intentions.
- An in-depth, line-by-line manual inspection of the entire codebase by seasoned industry professionals.

Scope of the Audit

Source Git Repository
https://github.com/Profila/cardano-smart-contracts

Git commit to review:
ff661a316eeb34ef2b571a923404c36223d613bc

The detailed breakdown of the file types and contents are outlined below in brief (informational purposes only)

Filetype	# Files	Lines of Code
html	11	4900
ts	26	2895
js	5	1945
ak	10	1440
css	3	1043
json	2	677
yml	1	20
toml	1	14

Note: *We are ignoring whitespace, comments and other inconsequential source lines in the project for the above analysis.*

We perform a thorough analysis of the code line by line by two independent expert auditors to ensure quality and accuracy of the findings. After the independent analysis and review, the findings are categorized and discussed. Then recommendations for each finding are prepared. All the findings are consolidated and compiled into a preliminary report to be submitted to the client.

Audit Disclaimer

In order to conduct a proper audit of the Profila smart contracts, auditors require the following information:

- Contract interactions
- Architecture of the project

Additionally, it will be helpful if Profila can provide the below documents when the audit is undertaken:

- **High-Level Contract Description:** Provide a detailed description of what each contract is designed to achieve, beyond the low-level details. This should include the overall purpose and functionality of the contracts, such as user subscriptions, payment processes, fund management, and access controls.
- **Purpose of Operations:** Explain the purpose behind key operations within the contracts. For example, describe the flow of user subscriptions, fund deposits, regular withdrawals by the service provider, user rights to withdraw or replenish funds, and access restrictions (e.g., only users can withdraw funds, only service providers can perform specific actions).
- **Mapping of Intended to Implemented Functionality:** Detail how the intended functionality aligns with the implemented functionality. This should clarify which contract manages specific functions (e.g., fund management, user authentication) and how elements like NFTs are used to authenticate and authorize users and service providers.
- **Documentation of Intended Functionality:** Ensure that the intended functionality is fully documented, as it is critical for verifying that the implemented functionality meets the intended goals during the audit process.

Note:

The audit process for this project will not include additional test coverage and test cases. It is important to note that these elements can provide valuable insights to auditors into project maturity and assumptions/edge-cases for vulnerability assessments. Additionally, without proper technical specifications, auditors may have to spend extra time inferring specifications from other documentation, which could leave them with less time for vulnerability assessment.

Audit Findings - Severity Classification

When conducting a smart contract audit, we categorize findings in the audit report based on their potential impact on the contract's security and functionality. They can range in severity from critical to informational.

Critical Vulnerabilities: These are severe issues that present existential risks to the protocol, such as potential halting or loss of user funds. Addressing these vulnerabilities is mandatory before deploying the smart contract, as they pose the most severe threats to its security and functionality.

Major Vulnerabilities: These include findings that, while not existential, could cause unexpected behavior or expose the protocol to significant risks if neglected. Examples might include centralization risks or logical errors that could lead to financial losses or reduced control over the contract's operations.

Minor Vulnerabilities: These findings do not pose significant risks to the core functionality of the protocol but may affect its performance or maintainability. Addressing these findings is recommended to ensure the contract operates

efficiently and reliably.

Informational Findings: These are recommendations aimed at improving the semantic and cosmetic quality of the code. While they do not directly impact the protocol's security or functionality, adhering to these recommendations can enhance code readability and maintainability.

Each category requires a different level of attention and action during the audit process, with critical vulnerabilities needing immediate resolution to ensure the security and integrity of the smart contract.

Note: *In certain situations, the impact on the smart contract may not be immediately clear, necessitating further discussion and clarification with the development team. In such cases, we will promptly reach out to Profila to obtain the necessary clarifications from the development team.*

Price and Schedule Estimations

On the basis of our analyses of the code and the examples and partial documentation provided, we recommend the number of hours and costs for the security audit as shown in the below table.

Activity	Time required for Initial Audit Report	Costs in USD
Independent Review by 2 Expert Auditors,	10 working days *	10200
Report comparison and consolidation		
Total Price to be paid in USD *		**10200**

** - Total Costs Excluding any local taxes if applicable*

NOTE: The estimated audit duration of 10 working days is based on the current availability of our auditor, with the goal of completing the audit by the 19th of September. To ensure this timeline, we request that the proposal be signed and payment confirmed by the 10th of September 2024. After this date, the audit may take longer to complete due to other commitments.*

Deliverables

We will provide a PDF report with our findings on the basis of the categories of findings as mentioned under section “Audit Findings - Severity Classification”, and we will also provide recommendations on how these findings can be fixed.

Based upon this report, the Profila team can fix the findings and report back to us

with the new repository. We will then re-check the updated project again to ensure compliance and deliver our final findings.

So this means the following phases are applicable:

- Investigation and producing the security audit report
- Present the results of the security audit report
- Profila makes the changes to their code on the basis of our recommendations
- Profila submits the code with fixes to us (within 2-3 weeks or as reasonable, from the point of receiving the initial audit findings report)
- We will check the changes again and give our final conclusion and audit report.

All steps above are included in our estimations.

Delivery Timelines

We estimate that the initial report can be delivered within 10 working days from the mutually agreed start date, subject to the constraints outlined in the “Price and Schedule Estimations” section. The final report's delivery will depend on how promptly Profila is able to address the identified issues and provide the updated codebase for our verification and confirmation of the resolutions.

Payment Terms

Payment	Stage
Advance Payment - 50% of the total project cost	Before work commences
Balance Payment - 50% of the total project cost	within 2 weeks after final project report is submitted

We are pleased to inform our clients that, in addition to traditional payment methods, **we additionally now accept Ada, the native cryptocurrency of the Cardano platform.** This option is offered to provide greater flexibility and convenience for our clients who prefer digital currency transactions. Our team is prepared to ensure a smooth and secure payment process using this innovative technology.

Statements

- *We will take all reasonable steps to ensure that any information that is provided by the client will be handled confidentially. Information will only be shared with the auditing team members who are assigned with the task to execute the security audit.*
- *We will ensure that measures are in place that the information provided cannot leave its company and associated development teams.*
- *Detailed terms as signed off by the Client and us in the "Master Services Agreement" are binding to this proposal.*

About us

EMURGO Diligence is the specialized audit service division of EMURGO, one of the co-founding entities of the Cardano blockchain protocol. With a deep commitment to fostering trust and security within the blockchain ecosystem, EMURGO Diligence provides comprehensive auditing services tailored to smart contracts, decentralized applications (DApps), and blockchain protocols.

Leveraging our extensive expertise in blockchain technology, particularly within the Cardano ecosystem, we offer rigorous and thorough audits designed to identify vulnerabilities, enhance security, and ensure the robustness of blockchain projects. Our audit process is grounded in industry best practices and informed by our unique position as a foundational partner in the development of Cardano.

At EMURGO Diligence, our mission is to empower blockchain developers and businesses by providing them with the insights and guidance necessary to build secure, reliable, and efficient blockchain solutions. We are dedicated to upholding the highest standards of security and integrity, helping to drive the adoption of blockchain technology by ensuring that projects are ready to meet the demands of the market.

Name:	EMURGO GROUP PTE. LTD (Company No. 201814919W)
HQ Address:	83 Clemenceau Avenue #02-110 UE Square, Singapore 239920
Website:	www.emurgo.io
Contact person:	Bharat Mallapur
Title:	Head - Diligence
Telephone:	+91 - 9916952831
Email:	bharat@emurgo.io