OFFSIDE LABS

Mind Token

Smart Contract Security Assessment

March 2025

Prepared for:

Mind Network

Prepared by:

Offside Labs

Yao Li

Siji Feng

Contents

1 About Offside Labs **2**

2 Executive Summary **3**

3 Summary of Findings **4**

4 Key Findings and Recommendations **5**

4.1 Redundant withdrawNative Function 5

5 Disclaimer **6**

1 About Offside Labs

Offside Labs stands as a pre-eminent security research team, comprising highly skilled hackers with top - tier talent from both academia and industry.

The team demonstrates extensive and diverse expertise in modern software systems, which encompasses yet are not restricted to *browsers*, *operating systems*, *IoT devices*, and *hypervisors*. Offside Labs is at the forefront of innovative domains such as *cryptocurrencies* and *blockchain technologies*. The team achieved notable accomplishments including the successful execution of remote jailbreaks on devices like the **iPhone** and **PlayStation 4**, as well as the identification and resolution of critical vulnerabilities within the **Tron Network**.

Offside Labs actively involves in and keeps contributing to the security community. The team was the winner and co-organizer for the *DEFCON CTF*, the most renowned CTF competition in Web2. The team also triumphed in the **Paradigm CTF 2023** in Web3. Meanwhile, the team has been conducting responsible disclosure of numerous vulnerabilities to leading technology companies, including *Apple*, *Google*, and *Microsoft*, safeguarding digital assets with an estimated value exceeding **$300 million**.

During the transition to Web3, Offside Labs has attained remarkable success. The team has earned over **$9 million** in bug bounties, and **three** of its innovative techniques were acknowledged as being among the **top 10 blockchain hacking techniques of 2022** by the Web3 security community.

2 Executive Summary

Introduction

Offside Labs completed a security audit of *Mind Token* smart contracts, starting on March 10, 2025, and concluding on March 11, 2025.

Project Overview

Mind Network is pioneering FHE (Fully Homomorphic Encryption) Infra for a Fully Encrypted Web by enabling quantum-resistant, fully encrypted internet data and AI computation through FHE.

The MindNetwork FHE Token is a cross-chain token seamlessly integrated with Chainlink CCIP and the Arbitrum native bridge. Initially minted on the Ethereum mainnet, the token will be airdropped on the Mind mainnet, ensuring broad accessibility and interoperability.

Audit Scope

The assessment scope contains mainly the smart contracts of the Mind Token program for the *Mind Network* project.

The audit is based on the following specific branches and commit hashes of the codebase repositories:

- Mind Token
  - Codebase: `https://github.com/mind-network/mind-token-contracts`
  - Commit Hash: 2cd8c73a3f59c698caed83656ede6cf00b75ccd7

We listed the files we have audited below:

- Mind Token
  - contracts/**/*.sol

Findings

The security audit revealed:

- 0 critical issue
- 0 high issue
- 0 medium issue
- 0 low issue
- 1 informational issues

Further details, including the nature of these issues and recommendations for their remediation, are detailed in the subsequent sections of this report.

3 Summary of Findings

ID	Title	Severity	Status
01	`Redundant withdrawNative Function`	Informational	Fixed

4 Key Findings and Recommendations

4.1 Redundant withdrawNative Function

Severity: Informational	Status: Fixed
Target: Smart Contract	Category: Optimization

In the `Airdrop` contract, the `withdrawNative` function is designed to withdraw the native tokens held by the contract. However, the contract does not include `receive`, `fallback`, or `payable` functions to accept native tokens. As a result, the native token balance of the contract can only increase through forced transfers, such as via the self-destruct mechanism of other contracts. This scenario is highly unlikely, making the presence of the `withdrawNative` function redundant.

5 Disclaimer

This report reflects the security status of the project as of the date of the audit. It is intended solely for informational purposes and should not be used as investment advice. Despite carrying out a comprehensive review and analysis of the relevant smart contracts, it is important to note that Offside Labs' services do not encompass an exhaustive security assessment. The primary objective of the audit is to identify potential security vulnerabilities to the best of the team's ability; however, this audit does not guarantee that the project is entirely immune to future risks.

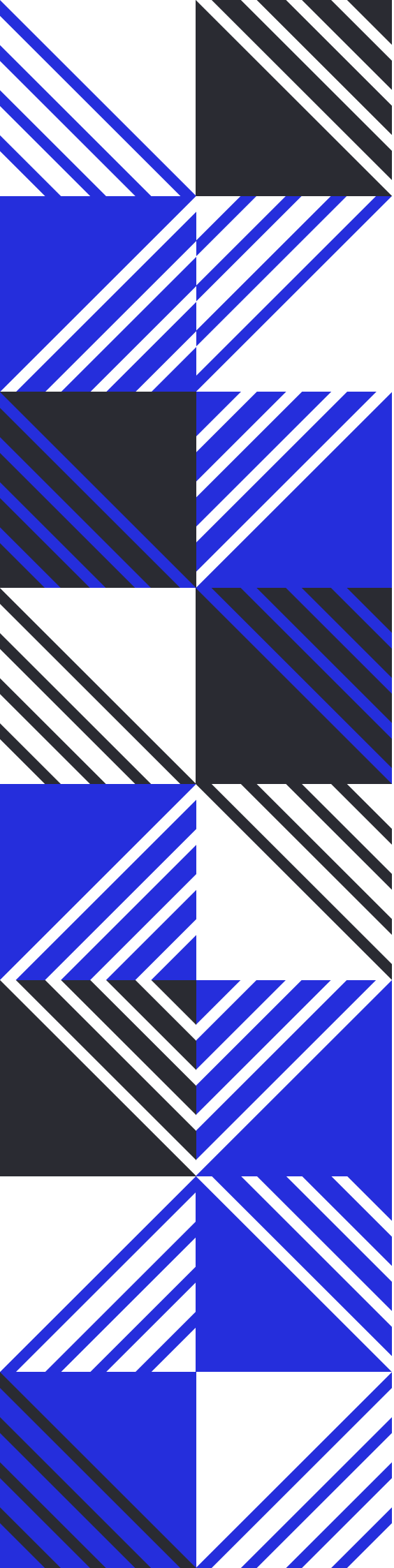
Offside Labs disclaims any liability for losses or damages resulting from the use of this report or from any future security breaches. The team strongly recommends that clients undertake multiple independent audits and implement a public bug bounty program to enhance the security of their smart contracts.

The audit is limited to the specific areas defined in Offside Labs' engagement and does not cover all potential risks or vulnerabilities. Security is an ongoing process, regular audits and monitoring are advised.

Please note: Offside Labs is not responsible for security issues stemming from developer errors or misconfigurations during contract deployment and does not assume liability for centralized governance risks within the project. The team is not accountable for any impact on the project's security or availability due to significant damage to the underlying blockchain infrastructure.

By utilizing this report, the client acknowledges the inherent limitations of the audit process and agrees that the firm shall not be held liable for any incidents that may occur after the completion of this audit.

This report should be considered null and void in case of any alteration.



OFFSIDE LABS

https://offside.io/

https://github.com/offsidelabs

https://twitter.com/offside_labs