CYBER AUDIT

CYBER audit

Audit Report

META LEDGER

METALEDGER TOKEN

WWW.CYBERAUDIT.SITE

Audit Summary

This report has been prepared for METALEDGER TOKEN on the Binance Chain network. Cyber Audit provides both client-centered and user-centered examination of the smart contracts and their current status when applicable. This report represents the security assessment made to find issues and vulnerabilities on the source code along with the current liquidity and token holder statistics of the protocol. A comprehensive examination has been performed, utilizing Cross Referencing, Static Analysis, In-House Security Tools, and line-by-line Manual Review. The auditing process pays special attention to the following considerations: Ensuring contract logic meets the specifications and intentions of the client without exposing the user's funds to risk. Testing the smart contracts against both common and uncommon attack vectors. Inspecting liquidity and holders statistics to inform the current status to both users and client when applicable. Assessing the codebase to ensure compliance with current best practices and industry standards. Verifying contract functions that allow trusted and/or untrusted actors to mint, lock, pause, and transfer assets. Thorough line-by-line manual review of the entire codebase by industry experts.

Cyber Audit

Details and results
of this smart contract security audit

Token Name

Meta Ledger

Website

Meta-Ledger.com

Contract address

0x93C19572DDCF8A9B835ca24a3cE46100FC92C965

Link Address

https://bscscan.com/address/0x93C19572DDCF8A9B835ca24a3cE46100FC92C965

The audit items and results:

Other unknown security vulnerabilities are not included in the audit responsibility scope

Audit Result

Passed

KYC Verification

Verified

CYBER AUDIT X META LEDGER

Table of Content

Introduction

This Audit Report mainly focuses on the overall security of MetaLedger Smart Contract With this report, we have tried to ensure the reliability and correctness of the smart contract by complete and rigorous assessment of their system's architecture and the smart contract codebase

Auditing Approach and Methodologies applied

The Cyber Audit team has performed rigorous testing of the project starting with analyzing the code design patterns in which we reviewed the smart contract architecture to ensure it is

structured and safe use of third-party smart contracts and libraries

Our team then performed a formal ine by line inspection of the Smart Contract to find any potential issue like race conditions, transaction ordering dependence, timestamp dependence.

and denial of service attacks.

In the Unit testing Phase, we coded/conducted custom unit tests written for each function in the

contract to venty that each function works as expected.

In Automated Testing we tested the Smart Contract with our in-house developed tools to

idently vulnerabebes and security flaws.

The code was tested in collaboration of our multiple team members and the included

- Testing the functionality of the Smart Contract to determine proper logic has been followed

throughout the whole process Analyzing the complexity of the code in depth and detailed, manual review of the code, line

by-line

Deploying the code on testnet using multiple clients to run live tests

- Analyzing fare preparations to check how the Smart Contract performs in case of any bugs and vunerabilities

Checking whether all the libraries used in the code are on the latest version

- Analyzing the security of the on-chan data

Audit Details

Project Name: MetaLedger [redacted]

Languages: Solidity (Smart contract) Platforms and Tools Remix IDE, Truffle, Truffle Team Ganache, Solhint, VScode, Myth Contract Library

Audit Goals

The focus of the audit was to verify that the Smart Contract System is secure, resilient and working according to the specifications. The audit activities can be grouped in the following three categories:

Security

Identifying security related issues within each contract and the system of contract.

Sound Architecture

Evaluation of the architecture of this system through the lens of established smart contract best practices and general software best practices.

Code Correctness and Quality

A full review of the contract source code. The primary areas of focus include:

- Accuracy
- Readability
- Sections of code with high complexity
- Quantity and quality of test coverage

Issue Categories

Every issue in this report was assigned a severity level from the following:

High level severity issues

Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.

Medium level severity issues

Issues on this level could potentially bring problems and should eventually be fixed.

Low level severity issues

Issues on this level are minor details and warnings that can remain unfixed but would be better fixed at some point in the future.

Issues Checking Status

№	Issue description.	Checking status
1	Compiler warnings.	Passed
2	Race conditions and Reentrancy. Cross-function race	Passed
3	conditions. Possible delays in data delivery.	Passed
4	Oracle calls.	Passed
5	Front running.	Passed
6	Timestamp dependence.	Passed
7	Integer Overflow and Underflow.	Passed
8	DoS with Revert.	Passed
9	DoS with block gas limit.	Passed
10	Methods execution permissions.	Passed
11	Economy model.	Passed
12	The impact of the exchange rate on the logic.	Passed
13	Private user data leaks.	Passed
14	Malicious Event log.	Passed
15	Scoping and Declarations.	Passed
16	Uninitialized storage pointers.	Passed
17	Arithmetic accuracy.	Passed
18	Design Logic.	Passed
19	Cross-function race conditions.	Passed
20	Safe Zeppelin module.	Passed
21	Fallback function security.	Passed

Number of issues per severity

Critical	High	Medium	Low	Note
0	0	0	0	0

Manual Audit

For this section the code was tested/read line by line by our developers.
We also used Remix IDE's JavaScript VM and Kovan networks to test the contract functionality.

Critical Severity Issues

No critical severity issues found.

High Severity Issues

No high severity issues found.

Medium Severity Issues

No medium severity issues found.

Low Severity Issues

No medium severity issues found.

Automated Audit

Remix Compiler Warnings

It throws warnings by Solidity's compiler. If it encounters any errors the contract cannot be compiled and deployed. No issues found.

Summary

Smart contracts do not contain any high severity issues.

Disclaimer

Cyber Audit has conducted an independent audit to verify the integrity of and highlight any vulnerabilities or errors, intentional or unintentional, that may be present in the codes that were provided for the scope of this audit. This audit report does not constitute agreement, acceptance or advocation for the Project that was audited, and users relying on this audit report should not consider this as having any merit for financial advice in any shape, form or nature. The contracts audited do not account for any economic developments that may be pursued by the Project in question, and that the veracity of the findings thus presented in this report relate solely to the proficiency, competence, aptitude and discretion of our independent auditors, who make no guarantees nor assurance that the contracts are completely free of exploits, bugs, vulnerabilities or deprecation of technologies. All information provided in this report does not constitute financial or investment advice, nor should it be used to signal that any persons reading this report should invest their funds without sufficient individual due diligence regardless of the findings presented in this report. Information is provided 'as is', and Cyber Audit is under no covenant to the completeness, accuracy or solidity of the contracts audited. In no event will Cyber Auditor its partners, employees, agents or parties related to the provision of this audit report be liable to any parties for, or lack thereof, decisions and/or actions with regards to the information provided in this audit report. The assessment services provided by Cyber Audit is subject to dependencies and under continuing development. You agree that your access and/or use, including but not limited to any services, reports, and materials, will be at your sole risk on an as-is, whereis, and as-available basis. Cryptographic tokens are emergent technologies and carry with them high levels of technical risk and uncertainty. The assessment reports could include false positives, false negatives, and other unpredictable results. The services may access, and depend upon, multiple layers of third parties

CYBER audit

WWW.CYBERAUDIT.SITE