COINMERCENARY / SMART CONTRACT AUDIT

MessengerBank Metals

15 JANUARY 2019 / TABLE OF CONTENTS

INTRODUCTION

CoinMercenary provides comprehensive, independent smart contract auditing.

We help stakeholders confirm the quality and security of their smart contracts using our comprehensive and standardized audit process. Each audit is unbiased and verified by multiple reputable auditors.

The scope of this audit was to analyze and document the MessengerBank Metals token contract.

This audit provides practical assurance of the logic and implementation of the contract.

AUDIT METHODOLOGY

CoinMercenary audits consist of four categories of analysis.

Design Patterns

We first inspect the overall structure of the smart contract, including both manual and automated analysis.

The design pattern analysis checks appropriate test coverage, utilizes a linter to ensure consistent style and composition, and code comments are reviewed. Overall architecture and safe usage of third party smart contracts are checked to ensure the contract is structured in a way that will not result in future issues.

Static Analysis

The static analysis portion of our audit is performed using a series of automated tools, purposefully designed to test the security of the contract. These tools include:

- **Manticore** - Dynamic binary analysis tool with EVM support.
- **Mythril** - Reversing and bug hunting framework for the Ethereum blockchain.
- **Oyente** - Analyzes Solidity code to find common vulnerabilities.
- **Solgraph** - DOT graph creation for visualizing function control flow of a Solidity contract to highlight potential security vulnerabilities.

Data flow and control flow are also analyzed to identify vulnerabilities.

Manual Analysis

Performing a hands on review of the smart contract to identify common vulnerabilities is the most intensive portion of our audit. Checks for race conditions, transaction-ordering dependence, timestamp dependence, and denial of service attacks are part of our standardized process.

Network Behavior

In addition to our design pattern check, we also specifically look at network behavior. We model how the smart contract will operate once in production,

then determine the answers to questions such as: how much gas will be used, are there any optimizations, how will the contract interact?

Contracts Reviewed

On January 15th, 2019 the following contract files and their respective SHA256 fingerprints were reviewed:

Filename	SHA256 Fingerprint
MBMToken.dist.sol	5d02c746e217db56a530634dc879056f08965912d63bf1e642d14dc219210954

AUDIT SUMMARY

The contracts have been found to be free of security issues.

Analysis Results

	Initial Audit
Design Patterns	Passed
Static Analysis	Passed
Manual Analysis	Passed
Token Allocation	Passed
Network Behavior	Passed

Test Results

- Basic unit test coverage for MBMToken contract.

Token Allocation Results

- Symbol: MBM
- Decimal: 18
- Initial Supply: Specified during deployment

Explicit Vulnerability Check Results

Known Vulnerability	**Results**
Parity Multisig Bug 2	Not vulnerable
Callstack Depth Attack	Not vulnerable
Transaction-Ordering Dependence	Not vulnerable
Timestamp Dependency	Not vulnerable
Re-Entrancy Vulnerability	Not vulnerable
Proxy and Buffer Overflow	Not vulnerable

ISSUES DISCOVERED

Issues below are listed from most critical to least critical. Severity is determined by an assessment of the risk of exploitation or otherwise unsafe behavior.

Severity Levels

- **Informational** - No impact on the contract.
- **Low** - Minimal impact on operational ability.
- **Medium** - Affects the ability of the contract to operate.
- **High** - Affects the ability of the contract to work as designed in a significant way.
- **Critical** - Funds may be allocated incorrectly, lost or otherwise result in a significant loss.

Issues

MBM-1 / Informational: Use latest Solidity compiler version

Present in all contract files

Explanation

Update all contract files to use the latest version of Solidity compiler (0.5.2) in order to ensure the latest performance enhancements, features and bug fixes are available.

Resolution

Resolution not required. This is a recommendation only.

MESSENGERBANK METALS AUDIT CONCLUSION

January 17th, 2019

CoinMercenary provides comprehensive, independent smart contract auditing.

We help stakeholders confirm the quality and security of their smart contracts using our comprehensive and standardized audit process. Each audit is unbiased and verified by multiple reputable auditors.

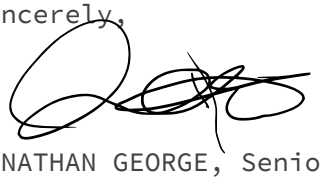
The scope of this audit was to analyze and document the MessengerBank Metals token contract. The audit provides practical assurance of the logic and implementation of the contracts.

CoinMercenary has reviewed the MessengerBank Metals smart contracts and found them to be free of security issues and logic errors.

The audit began on January 15th, 2019, ending on January 17th, 2019. One “informational” level issue was documented, but does not require resolution.

Working with the MessengerBank Metals team has been a pleasure and we look forward to seeing their continued success.

Sincerely,



JONATHAN GEORGE, Senior Auditor