COINMERCENARY / SMART CONTRACT AUDIT

XCOYNZ Audit

30 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 XCOYNZ Token smart contracts.

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 31st, 2019 the following contract files and their respective SHA256 fingerprints were reviewed:

Filename	SHA256 Fingerprint
XCOYNZ Test SC.sol	6b05d26879e64579765e1771a049e8fb2fad32e6e65c0420924155d15f762bb2

The above referenced smart contract is also available on Rinkeby, located at: 0x59e423a58748109140978920e6a0d305704afd7f

Contract Review #2

On February 5th, 2019 the following contract files and their respective SHA256 fingerprints were reviewed:

Filename	SHA256 Fingerprint
XCOYNZ_Test_SC_v2.sol	e2f0a8df7c59a63f65946805f6026a6b87d190f69fca96effc1ace28eb7ccb50

The above referenced smart contract is also available on Rinkeby, located at: 0x307a97930f8791677ef7c69e21d676b55db905dc

AUDIT SUMMARY

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

Analysis Results

	Initial Audit	Audit #2
Design Patterns	Passed	Passed
Static Analysis	Passed	Passed
Manual Analysis	Passed	Passed
Token Allocation	Update Required	Passed
Network Behavior	Passed	Passed
Business Logic	Update Required	Passed

Test Results

- No unit test coverage available.

Token Allocation Results

- Symbol: XCOYNZ
- Decimal: 18
- Initial Supply: 1,250,000,000

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

XC-1 / Critical: Locking dates for tokens does not match required business logic

Present in XCOYNZ Test SC.sol

Explanation

The smart contract lock a set amount of tokens based on four vesting dates. The vesting dates in the contracts do not match the dates as required by the business logic. All current dates are set to 2019-01-23 with four one hour increments, rather than the required 2020-01-02, 2020-01-08, 2021-01-08, 2022-01-08.

Resolution

Resolved in commit 4f272c4f301c7005e8a58f7bf144b1b8c3324274.

XC-2 / Informational: Hardcoded Values

Present in XCOYNZ Test SC.sol

Explanation

CoinMercenary recommends that external addresses be set using constructor argument when initializing the contracts. This allows for a smoother transition between testnet and production contracts, among other benefits

The referenced address, 0xc6cFC081c9e728f6bBBC1101640f29BC57a7E76f, has been confirmed to belong to the XCOYNZ team.

Resolution

Resolution not required.

XCOYNZ AUDIT CONCLUSION

February 5th, 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 XCOYNZ token contract. The audit provides practical assurance of the logic and implementation of the contracts.

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

The audit began on January 30th, 2019, ending on February 5th, 2019. One critical and one informational level issue were documented.

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

Sincerely,

JONATHAN GEORGE, Senior Auditor