COINMERCENARY / SMART CONTRACT AUDIT

XYO Network (XYO)

18 MARCH 2018 / 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 XYO Network (XYO) token generation 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 March 18, 2018 using git hash 14ad4a3b8b3d6e1fb1f84bd943afed9ed6ac43ac, the following contract files and their respective SHA256 fingerprints were reviewed:

Filename	SHA256 Fingerprint
XYOfficialTokenSale.sol	c2f5a40e961f71bc5052da9e6d80a380f68eca1ea53ce37817def1ed93be78ac
XYEligibleTokenSale.sol	84000c3d774e7daccf0b2bf62c4a45ac0030083eb6df4c8f00a0365aabb59170
XYProofOfEligibility.sol	df34fecb63b2b4ff2e9a2c649df3a7ea9129253e7f4dc2c38fc4c08b27f36a07
XYPendingTokenSale.sol	98300dd2c20127a100dca569bf6e26cb118819dfdacf6c6de23f8559d5901daf
XYVariablePrice.sol	951e4f331132ce0cd6c53f26e8df56c99032e20ad59e4d8ff5c92144d9526a2c
XYApprovable.sol	25fbeff7373bcc772e5062f2fccc0e8798303b007ae22211d22be092ba62143a
XYBlockable.sol	8457365dae015a0638c645eaf340fff999ea6d657e9b0a323400262194b432d2
XYTimedTokenSale.sol	c9c7c72b6cf624ae8453f698eb87224185ec3baa46ce2371f8cfcbaa8334214a
XYTokenSale.sol	f7cb2f0870d91b513f075a0fb0774c28b3a4f905c0446e9c00cf331e5443c974
XYKillable.sol	e627ca813b9bb92f86412cb0079713f6b0ccf5dfbbca204163582e1adeebd2b6

Remediation Audit

No issues discovered during initial audit.

AUDIT SUMMARY

The contracts have been found to be free of security issues. The XYO token generation contract is well written, follows Solidity best practices and overall is the cleanest Solidity code base we have audited.

Analysis Results

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

Test Results

Basic test coverage available for contracts.

Token Allocation Results

Not available.

Explicit Vulnerability Check Results

Known Vulnerability	Results
Parity Multisig Bug 2	Not vulnerable
Callstack Depth Attacks	Not vulnerable
Transaction Ordering Dependence	Not vulnerable
Timestamp Dependency	Not vulnerable
Re-Entrancy Vulnerabilities	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

No issues were discovered.

CONCLUSION

No critical problems have been found. The reviewed smart contracts are well crafted and follow common security practices.

The care and attention to detail by the XYO Network team is incredible. The contracts are the cleanest we have ever audited. Being able to review the work of the XYO team has been a rare opportunity to see craftsmen at work.