COINMERCENARY / SMART CONTRACT AUDIT

ALIVE Token Audit

15 JULY 2018 / TABLE OF CONTENTS

INTRODUCTION 2

AUDIT METHODOLOGY 3

- Design Patterns 3
- Static Analysis 3
- Manual Analysis 3
- Network Behavior 3
- Contracts Reviewed 4
- Remediation Audit 4

AUDIT SUMMARY 5

- Analysis Results 5
- Test Results 5
- Token Allocation Results 5
- Explicit Vulnerability Check Results 5

ISSUES DISCOVERED 6

- Severity Levels 6
- Issues 6

CONCLUSION 7

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 ALIVE token and crowdsale contract.

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

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 July 15th, 2018 using git hash 6acf1f0d2c5232720e028024af3ae22e21cf5a3a the following contract files and their respective SHA256 fingerprints were reviewed:

Filename	SHA256 Fingerprint
Token.sol	40324893861a0e48aa76644f5b45f6b84380c2a9910472762f0485ab293eb5b6
WhiteList.sol	2a691ae4e415847f06562d8ea8e521a6249e512b4b33f89b44a3cb5f7987b8aa
Crowdsale.sol	7f8b0f27072a7e15ae7ee30304658078f289b4674878a968e1cf4bd6a22b2a75

Remediation Audit

Not required.

AUDIT SUMMARY

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

Analysis Results

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

Test Results

- No unit test coverage available.

Token Allocation Results

- Symbol: AL
- 1,000,000,000 AL tokens available.
- Decimals: 4

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

No issues discovered.

CONCLUSION

The reviewed smart contracts are free of security issues and well crafted.

We look forward to seeing the success of the Alive Entertainment team and appreciate the opportunity to be a part of their story.