CyberCrime Shield

cybercrimeshield.org

Smart Contract Audit Report

Oikos Cash

AUDIT TYPE: **PUBLIC**

ID:2390137

February 5, 2021

TABLE OF CONTENTS

SMART CONTRACTS

https://github.com/oikos-cash/oikos

Mirror: cybercrimeshield.org/files/oikos-master.zip

CRC32: 2A76738E

MD5: A8565686DE3E617B84296B73CC078BA5

SHA-1: C08DABF57606D9717DFB1689FD33715C17FE46FF

INTRODUCTION

Blockchain platforms, such as Nakamoto's Bitcoin, enable the trade of crypto-currencies between mutually mistrusting parties.

To eliminate the need for trust, Nakomoto designed a peer-to-peer network that enables its peers to agree on the trading transactions.

Vitalik Buterin identified the applicability of decentralized computation beyond trading, and designed the Ethereum blockchain which supports the execution of programs, called smart contracts, written in Turing-complete languages.

Smart contracts have shown to be applicable in many domains including financial industry, public sector and cross-industry.

The increased adoption of smart contracts demands strong security guarantees. Unfortunately, it is challenging to create smart contracts that are free of security bugs.

As a consequence, critical vulnerabilities in smart contracts are discovered and exploited every few months.

In turn, these exploits have led to losses reaching billions worth of USD in the past few years.

It is apparent that effective security checks for smart contracts are strictly needed.

Our company provides comprehensive, independent smart contract auditing.

We help stakeholders confirm the quality and security of their smart contracts using our standardized audit process.

The scope of this audit was to analyze and document the Oikos contract.

AUDIT METHODOLOGY

1. Design Patterns

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

2. Static Analysis

The static analysis is performed using a series of automated tools, purposefully designed to test the security of the contract.
All the issues found by tools were manually checked (rejected or confirmed).

3. Manual Analysis

Contract reviewing to identify common vulnerabilities. Comparing of requirements and implementation. Reviewing of a smart contract for compliance with specified customer requirements. Checking for a gas optimization and self-documentation. Running tests of the properties of the smart contract in test net.

ISSUES DISCOVERED

Issues 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

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

AUDIT SUMMARY

The summary result of the audit performed is presented in the table below
Findings list:

LEVEL	AMOUNT
Critical	0
Medium	0
Low	0
Informational	3

Suitable for deploying on mainnet.

FINDINGS

Informational

(Line 23,33,41, DapMaintenace.sol) – These functions can be merged together to a single function with multiple parameters

CONCLUSION

- Contract has well-formed structure
- High code readability
- User input validation is performed
- No backdoors or overflows are present in the contract

Suitable for deploying on mainnet.