CyberCrime Shield

cybercrimeshield.org

Smart Contract Audit Report

OIKOS CASH BSC

https://oikos.cash

AUDIT TYPE: **PUBLIC**

digital signature

https://cybercrimeshield.org/secure/oikos-bsc

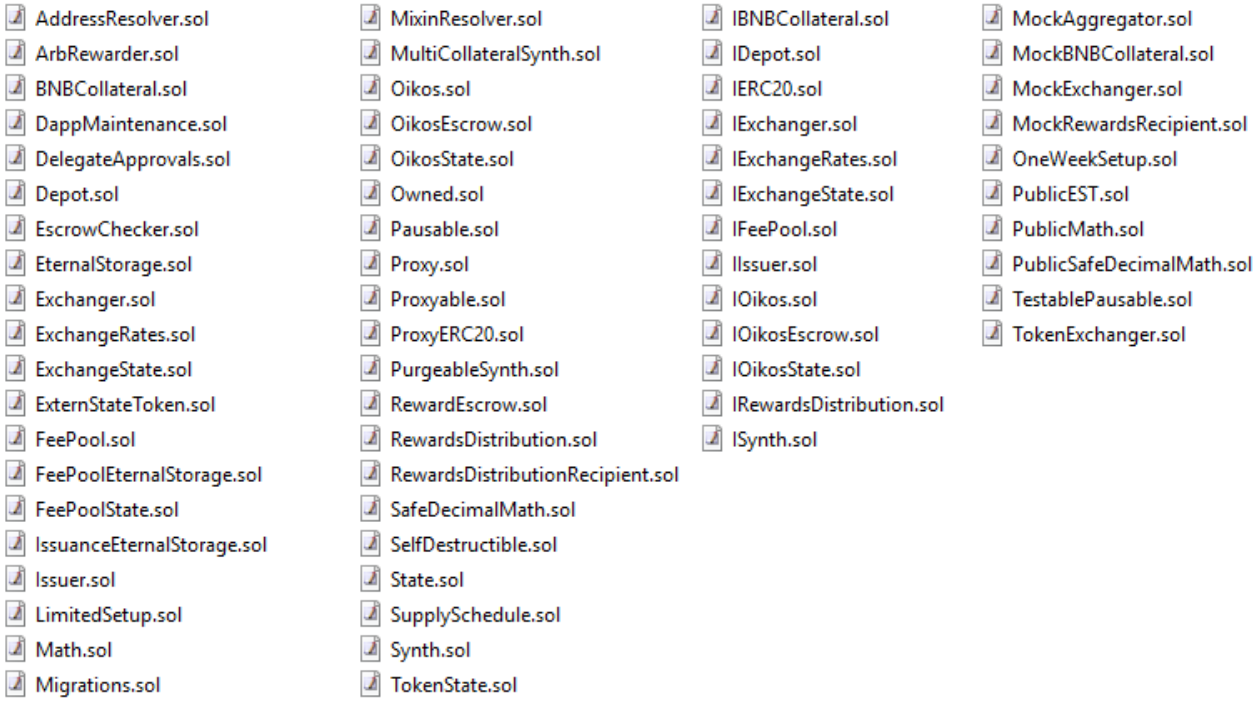
ID:2390319

April 09, 2021

TABLE OF CONTENTS

SMART CONTRACTS

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



Mirror: https://cybercrimeshield.org/secure/uploads/oikos-bsc-master.zip

CRC32: 31DD48E0

MD5: 22D7127F17F4B97B9D0E5DA485047C48

SHA-1: 6394BDC5E9624E201D1C05D6BB1C93EF19B77917

INTRODUCTION

We conducted an independent external audit of smart contracts on the Oikos platform.

In January 2021, we already conducted an audit of this platform on the Tron blockchain.

This revision of smart contacts is adapted for Binance Smart Chain in accordance with the recommendations of the developers of the Binance Smart Chain platform.

Also, the project has implemented solutions for the transition to Binance Smart Chain from the Tron blockchain.

All Oikos project code has good publicly available documentation.

In our research, we analyzed smart contracts according to our internal methodology.

The scope of this audit was to analyze and document the OIKOS CASH BSC contracts.

This document is not financial advice, you perform all financial actions under your own responsibility.

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 energy 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	1

FINDINGS (1)

An outdated compiler version is used.

pragma solidity 0.4.25;

An outdated compiler version is used. The compiler version specified in the pragma directive may have known bugs. It is recommended to use the latest minor release of solc 0.5 or 0.6. For more information on Solidity compiler bug reports and fixes refer to https://github.com/ethereum/solidity/releases

CONCLUSION

- Contracts have high code readability
- Gas usage is optimal
- Contracts are fully BSC completable
- No backdoors or overflows are present in the contracts