



SMART CONTRACT AUDIT

ZOKYO.

January 21st, 2022 | v. 1.0

PASS

Zokyo's Security Team has concluded that this smart contract passes security qualifications to be listed on digital asset exchanges.



TECHNICAL SUMMARY

This document outlines the overall security of the Bloktopia smart contracts, evaluated by Zokyo's Blockchain Security team.

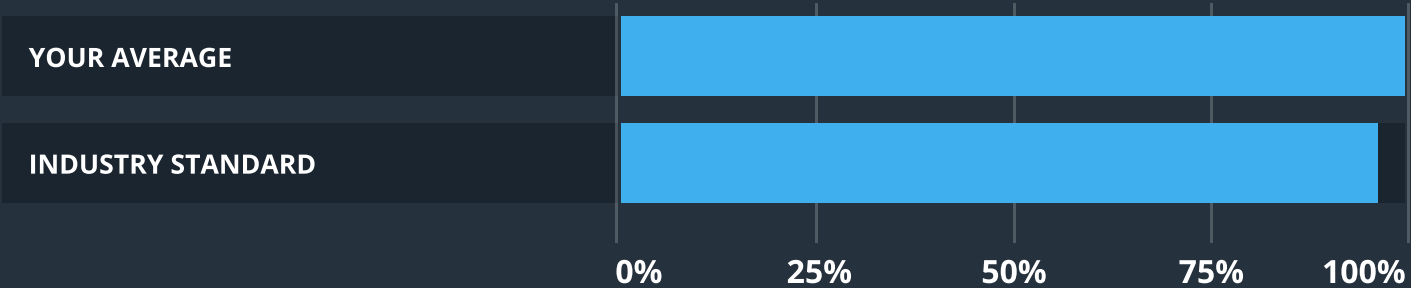
The scope of this audit was to analyze and document Bloktopia smart contract codebase for quality, security, and correctness.

Contract Status



There were no critical, high or medium issues found during the audit.

Testable Code



The testable code is 100%, which is above the industry standard of 95%.

It should be noted that this audit is not an endorsement of the reliability or effectiveness of the contract, rather limited to an assessment of the logic and implementation. In order to ensure a security of the contract we at Zokyo recommend that the Bloktopia team put in place a bug bounty program to encourage further and active analysis of the smart contract.

TABLE OF CONTENTS

- Auditing Strategy and Techniques Applied 3
- Executive Summary. 4
- Structure and Organization of Document 5
- Complete Analysis 6
- Code Coverage and Test Results for all files. 8

AUDITING STRATEGY AND TECHNIQUES APPLIED

The Bloktopia smart contract’s source code was provided as the deployed contract at BSC network by the Bloktopia team

Contract address: <https://bscscan.com/address/0x29132062319aa375e764ef8ef756f2b28c77a9c9#contracts>

Within the scope of this audit Zokyo auditors have reviewed the following contract(s):

- AddrArrayLib.sol.sol
- Blok.sol
- TestAddLib.sol

Throughout the review process, care was taken to ensure that the contract:

- Implements and adheres to existing standards appropriately and effectively;
- Documentation and code comments match logic and behavior;
- Follows best practices in efficient use of resources, without unnecessary waste;
- Uses methods safe from reentrance attacks;
- Is not affected by the latest vulnerabilities;
- Whether the code meets best practices in code readability, etc.

Zokyo’s Security Team has followed best practices and industry-standard techniques to verify the implementation of Bloktopia smart contracts. To do so, the code is reviewed line-by-line by our smart contract developers, documenting any issues as they are discovered. Part of this work includes writing a unit test suite. In summary, our strategies consist largely of manual collaboration between multiple team members at each stage of the review:

1	Due diligence in assessing the overall code quality of the codebase.	3	Testing contract logic against common and uncommon attack vectors.
2	Cross-comparison with other, similar smart contracts by industry leaders.	4	Thorough, manual review of the codebase, line-by-line.

EXECUTIVE SUMMARY

There were no critical, high or medium issues found during the audit. Although certain number of informational issues were discovered, they relate to the following:

- Update solidity version
- Omit SafeMath after Solidity version upgrade.

After recommendations by Zokyo auditors and discussion with the Customer it was decided that all these issues don't influence security and efficiency of the smart contract provided by Bloktopia Team.

STRUCTURE AND ORGANIZATION OF DOCUMENT

For ease of navigation, sections are arranged from most critical to least critical. Issues are tagged “Resolved” or “Unresolved” depending on whether they have been fixed or addressed. Furthermore, the severity of each issue is written as assessed by the risk of exploitation or other unexpected or otherwise unsafe behavior:

Critical

The issue affects the contract in such a way that funds may be lost, allocated incorrectly, or otherwise result in a significant loss.

High

The issue affects the ability of the contract to compile or operate in a significant way.

Medium

The issue affects the ability of the contract to operate in a way that doesn't significantly hinder its behavior.

Low

The issue has minimal impact on the contract's ability to operate.

Informational

The issue has no impact on the contract's ability to operate.

COMPLETE ANALYSIS

INFORMATIONAL | RESOLVED

Update solidity version

Contract utilizes 0.7.6 version, though it is recommended to use the version from the latest release, which is 0.8.11

Recommendation:

update version to 0.8.11

INFORMATIONAL | RESOLVED

Omit SafeMath after Solidity version upgrade

In order to save gas during transactions SafeMath usage can be omitted, because 0.8.11 Solidity has built in support of safe operations.

Recommendation:

after upgrading to 0.8.11 SafeMath may be omitted.

	Blok.sol	AddrArrayLib.sol	TestAddLib.sol
Re-entrancy	Pass	Pass	Pass
Access Management Hierarchy	Pass	Pass	Pass
Arithmetic Over/Under Flows	Pass	Pass	Pass
Delegatecall Unexpected Ether	Pass	Pass	Pass
Default Public Visibility	Pass	Pass	Pass
Hidden Malicious Code	Pass	Pass	Pass
Entropy Illusion (Lack of Randomness)	Pass	Pass	Pass
External Contract Referencing	Pass	Pass	Pass
Short Address/ Parameter Attack	Pass	Pass	Pass
Unchecked CALL Return Values	Pass	Pass	Pass
Race Conditions / Front Running	Pass	Pass	Pass
General Denial Of Service (DOS)	Pass	Pass	Pass
Uninitialized Storage Pointers	Pass	Pass	Pass
Floating Points and Precision	Pass	Pass	Pass
Tx.Origin Authentication	Pass	Pass	Pass
Signatures Replay	Pass	Pass	Pass
Pool Asset Security (backdoors in the underlying ERC-20)	Pass	Pass	Pass

CODE COVERAGE AND TEST RESULTS FOR ALL FILES

Tests written by Zokyo Secured team

As part of our work assisting Bloktopia team in verifying the correctness of their contract code, our team was responsible for writing integration tests using Truffle testing framework.

Tests were based on the functionality of the code, as well as review of the Bloktopia contract requirements for details about issuance amounts and how the system handles these.

Contract: AddrArrayLib

Setup

✓ should deploy (139ms)

On success

✓ should push (735ms)

✓ should remove (476ms)

On reverts

✓ should NOT get address [index out of range] (337ms)

Contract: Block Token

Setup

✓ should deploy (501ms)

On success

✓ should check tax info (47ms)

✓ should update tax info (116ms)

✓ should transfer [with fee] (124ms)

✓ should add to noFeeAddresses (84ms)

✓ should transfer [without fee] (103ms)

✓ should remove from noFeeAddresses (95ms)

On reverts

✓ should NOT deploy (271ms)

✓ should NOT update tax info (120ms)

✓ should NOT remove from noFeeAddrs [address does not exist] (60ms)

✓ should NOT transfer [zero address] (121ms)

15 passing (4s)

FILE	% STMTS	% BRANCH	% FUNCS	% LINES
contracts\	100.00	93.33	100.00	100.00
AddrArrayLib.sol	100.00	100.00	100.00	100.00
Blok.sol	100.00	90.91	100.00	100.00
contracts\test\	100.00	100.00	100.00	100.00
TestAddLib.sol	100.00	100.00	100.00	100.00
All files	100	93.33	100	100

We are grateful to have been given the opportunity to work with the Bloktopia team.

The statements made in this document should not be interpreted as investment or legal advice, nor should its authors be held accountable for decisions made based on them.

Zokyo's Security Team recommends that the Bloktopia team put in place a bug bounty program to encourage further analysis of the smart contract by third parties.

ZOKYO.