SMART CONTRACTS REVIEW

zokyo

March 22nd 2024 | v. 1.0

Security Audit Score

PASS

Zokyo Security has concluded that these smart contracts passed a security audit.

ZOKYO AUDIT SCORING IOTA

1. Severity of Issues:
    - Critical: Direct, immediate risks to funds or the integrity of the contract. Typically, these would have a very high weight.
    - High: Important issues that can compromise the contract in certain scenarios.
    - Medium: Issues that might not pose immediate threats but represent significant deviations from best practices.
    - Low: Smaller issues that might not pose security risks but are still noteworthy.
    - Informational: Generally, observations or suggestions that don't point to vulnerabilities but can be improvements or best practices.
2. Test Coverage: The percentage of the codebase that's covered by tests. High test coverage often suggests thorough testing practices and can increase the score.
3. Code Quality: This is more subjective, but contracts that follow best practices, are well-commented, and show good organization might receive higher scores.
4. Documentation: Comprehensive and clear documentation might improve the score, as it shows thoroughness.
5. Consistency: Consistency in coding patterns, naming, etc., can also factor into the score.
6. Response to Identified Issues: Some audits might consider how quickly and effectively the team responds to identified issues.

HYPOTHETICAL SCORING CALCULATION:

Let's assume each issue has a weight:
- Critical: -30 points
- High: -20 points
- Medium: -10 points
- Low: -5 points
- Informational: -1 point

Starting with a perfect score of 100:
- 0 Critical issues: 0 points deducted
- 0 High issues: 0 points deducted
- 0 Medium issues: 0 points deducted
- 0 Low issues: 0 points deducted
- 11 Informational issues: 11 resolved = 0 points deducted

Hence, 100

TECHNICAL SUMMARY

This document outlines the overall security of the IOTA smart contract/s evaluated by the Zokyo Security team.

The scope of this audit was to analyze and document the IOTA smart contract/s codebase for quality, security, and correctness.

Contract Status

There were 0 critical issues found during the review. (See Complete Analysis)

It should be noted that this audit is not an endorsement of the reliability or effectiveness of the contract/s but rather limited to an assessment of the logic and implementation. In order to ensure a secure contract that can withstand the Ethereum network's fast-paced and rapidly changing environment, we recommend that the IOTA team put in place a bug bounty program to encourage further active analysis of the smart contract/s.

Table of Contents

AUDITING STRATEGY AND TECHNIQUES APPLIED

The source code of the smart contract was taken from the IOTA repository:
Repo: https://github.com/iotaledger/wasp
Last commit - 01f56f20026012184db418fca68cf7af3e2d7f7e
Fixes - https://github.com/iotaledger/wasp/pull/3349

Within the scope of this audit, the team of auditors reviewed the following contract(s):

- packages/vm

During the audit, Zokyo Security ensured that the contract:

- Implements and adheres to the existing standards appropriately and effectively;
- The documentation and code comments match the logic and behavior;
- Distributes tokens in a manner that matches calculations;
- Follows best practices, efficiently using resources without unnecessary waste;
- Uses methods safe from reentrance attacks;
- Is not affected by the most recent vulnerabilities;
- Meets best practices in code readability, etc.

Zokyo Security has followed best practices and industry-standard techniques to verify the implementation of IOTA smart contract/s. To do so, the code was reviewed line by line by our smart contract developers, who documented even minor issues as they were discovered. In summary, our strategies consist largely of manual collaboration between multiple team members at each stage of the review:

01 Due diligence in assessing the overall code quality of the codebase.

02 Cross-comparison with other, similar smart contract/s by industry leaders.

03 Thorough manual review of the codebase line by line.

Executive Summary

The Zokyo team has performed a security audit of the provided codebase. The contracts submitted for auditing are well-crafted and organized. Detailed findings from the audit process are outlined in the "Complete Analysis" section.

STRUCTURE AND ORGANIZATION OF THE DOCUMENT

For the ease of navigation, the following sections are arranged from the most to the least critical ones. Issues are tagged as “Resolved” or “Unresolved” or “Acknowledged” depending on whether they have been fixed or addressed. Acknowledged means that the issue was sent to the IOTA team and the IOTA team is aware of it, but they have chosen to not solve it. The issues that are tagged as “Verified” contain unclear or suspicious functionality that either needs explanation from the Client or remains disregarded by the Client. 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

FINDINGS SUMMARY

#	Title	Risk	Status
1	Visibility not declared	Informational	Resolved
2	Visibility not declared	Informational	Resolved
3	Visibility not declared	Informational	Resolved
4	Visibility not declared	Informational	Resolved
5	Visibility not declared	Informational	Resolved
6	Visibility not declared	Informational	Resolved
7	Visibility not declared	Informational	Resolved
8	Mixed value and pointer receivers	Informational	Resolved
9	Mixed value and pointer receivers	Informational	Resolved
10	Use of a deprecated function	Informational	Resolved
11	Use of a deprecated function	Informational	Resolved

INFORMATIONAL-1 | RESOLVED

Visibility not declared

File: core/evm/iscmagic/ERC20BaseTokens.sol
Constant: MAX_UINT64
Details:
The constant doesn't have an explicit visibility declared. It will be set as public implicitly. To avoid unintended exposure, declare the visibility explicitly.

Recommendation:
Explicitly define the visibility

INFORMATIONAL-2 | RESOLVED

Visibility not declared

Visibility not declared
File: core/evm/iscmagic/ERC20ExternalNativeTokens.sol
Variable: _nativeTokenID
Details:
The variable doesn't have an explicit visibility declared. It will be set as public implicitly. To avoid unintended exposure, declare the visibility explicitly.

Recommendation:
Explicitly define the visibility

INFORMATIONAL-3 | RESOLVED

Visibility not declared

File: core/evm/iscmagic/ERC20ExternalNativeTokens.sol
Constant: _maximumSupply
Details:
The variable doesn't have an explicit visibility declared. It will be set as public implicitly. To avoid unintended exposure, declare the visibility explicitly.

Recommendation:
Explicitly define the visibility

INFORMATIONAL-4 | RESOLVED

Visibility not declared

File: core/evm/iscmagic/ERC20NativeTokens.sol
Variable: _name
Details:
The variable doesn't have an explicit visibility declared. It will be set as public implicitly. To avoid unintended exposure, declare the visibility explicitly.

Recommendation:
Explicitly define the visibility

INFORMATIONAL-5 | RESOLVED

Visibility not declared

File: core/evm/iscmagic/ERC20NativeTokens.sol
Constant: _tickerSymbol
Details:
The variable doesn't have an explicit visibility declared. It will be set as public implicitly. To avoid unintended exposure, declare the visibility explicitly.

Recommendation:
Explicitly define the visibility

INFORMATIONAL-6 | RESOLVED

Visibility not declared

File: core/evm/iscmagic/ERC20NativeTokens.sol
Constant: _decimals
Details:
The variable doesn't have an explicit visibility declared. It will be set as public implicitly. To avoid unintended exposure, declare the visibility explicitly.

Recommendation:
Explicitly define the visibility

INFORMATIONAL-7 | RESOLVED

Visibility not declared

File: core/evm/iscmagic/ERC721NFTCollection.sol
Constant: _collectionId
Details:
The variable doesn't have an explicit visibility declared. It will be set as public implicitly. To avoid unintended exposure, declare the visibility explicitly.

Recommendation:
Explicitly define the visibility

INFORMATIONAL-8 | RESOLVED

Mixed value and pointer receivers

File: core/blocklog/events.go
Type: EventLookupKey
Details:
Mixing value and pointer receivers for methods on a single type in Go can lead to confusion and potential issues.

Recommendation:
Use either value or pointer receivers for all methods on a type. This improves code clarity and avoids unintended behavior.

INFORMATIONAL-9 | RESOLVED

Mixed value and pointer receivers

File: core/blocklog/receipt.go
Type: RequestLookupKey
Details:
Mixing value and pointer receivers for methods on a single type in Go can lead to confusion and potential issues.

Recommendation:
Use either value or pointer receivers for all methods on a type. This improves code clarity and avoids unintended behavior.

INFORMATIONAL-10 | RESOLVED

Use of a deprecated function

File: core/evm/evmtest/contractInstance.go
Function: types.NewTransaction
Details:
The "buildEthTx" function calls to a "types.NewTransaction" function, which is deprecated, and it is recommended to use the "NewTx" function instead.

Recommendation:
Don't use deprecated functions. Switch to use the NewTx instead of NewTransaction

Use of a deprecated function

File: core/evm/evmimpl/impl.go
Function: types.NewTransaction
Details:
The "newL1Deposit" function calls to a "types.NewTransaction" function, which is deprecated, and it is recommended to use the "NewTx" function instead.

Recommendation:
Don't use deprecated functions. Switch to use the NewTx instead of NewTransaction

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

We are grateful for the opportunity to work with the IOTA team.

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

Zokyo Security recommends the IOTA team put in place a bug bounty program to encourage further analysis of the smart contract by third parties.

zokyo