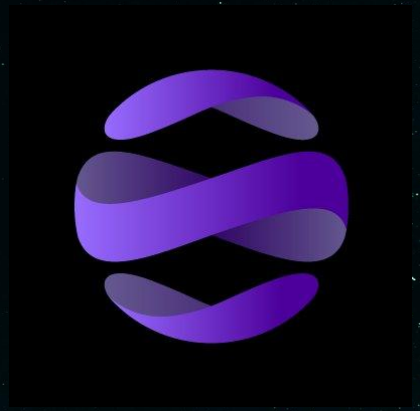
Audit By ICSA

International Crypto Services Agency



Inter World Metaverse: IWT Token

February 15th, 2024

https://icsa.website/

Disclaimer

ICSA audits and reports should not be considered as a form of project's "advertisement" and does not cover any interaction and assessment from "project's contract" to "external contracts" such as Pancakeswap or similar.

ICSA does not provide any warranty on its released reports. We should not be used as a decision to invest into an audited project please do your own research. ICSA provides transparent reports to all its "clients" and to its "clients participants" and will not claim any guarantee of bug-free code within its Smart Contract.

Each company or project shall be liable for its own security flaws and functionalities.
ICSA presence is to analyze, audit and assess the client's smart contract's code.

Scope of Work

The main focus of this report/audit, is to document an accurate assessment of the condition of the smart contract and whether it has any security flaws in the implementation of the contract.

Inter World team agreed and provided us with the files that needed to be tested (Through Github, AbeyScan, files, etc.).

ICSA will be focusing on contract issues and functionalities along with the projects claims from smart contract to their website, white paper and repository where available, which has been provided by the project.

Code is reviewed manually and with the use of software using industry best practices.

Background

ICSA was commissioned by Inter World to perform an audit of smart contract:

Contract Address

0x64F7e4B5B48654c45476ADbc7800a78D3f577C8d

Blockchain

Abey Chain

The purpose of the audit was to achieve the following:

- Ensure that the smart contract functions as intended.
- Identify potential security issues with the smart contract.

The information in this report should be used to understand the risk exposure of the smart contract, and as a guide to improve the security posture of the smart contract by remediating the issues that were identified.

Audit Details

Inter World is a virtual world that allows users to build their own tools, games, content, markets, and businesses. Assets in InterWorld may be purchased by individual community members, giving them full control over their creations.

Inter World Twitter

Inter World Website

Inter World Discord

Contract Details

Token Name - IWT Token

Token Ticker - ITW

Token Description - Mining Token

Decimals - 18

Compiler Version - LIM

LP Lock - No LP Lock

Current Holders - 6 Addresses

KYCd by - ICSA

Current Transaction Count - 30

Buy Fee - 0%

Max Supply - 100,000,000

Sell Fee - 0%

Total Current Supply - 3,681,541.1

Launch Type - GemPad Presale

Decimals - 18

Owner can not set buy/sell fees.
Owner can mint tokens up to the maximum supply. LIM is Limitation due to no info available.

Tokenomics

Contract Address

0x64F7e4B5B48654c45476ADbc7800a78D3f577C8d

Contract Deployer

0x2829f082751b36c59ceaec5ca50ee6aa9feed134

Contract Owner

0x2829f082751b36c59ceaec5ca50ee6aa9feed134

Owner Privileges

Privileges

Ownership HAS NOT BEEN renounced. The owner has some privileges or authority to make SOME changes. Owner can add minter and mint new tokens.

Adjustable Functions

1. addMinter
2. approve
3. elegate
4. mint
5. removeMinter
6. renounceOwnership
7. transfer
8. transferFrom
9. transferOwnership

Vulnerabilities

Passed = No Issues detected. Code is in good working order

Low Issue = Low-level weakness/vulnerabilities are mostly related to outdated, unused etc. code snippets, that can't have significant impact on execution.

High Issue = High-level weakness/vulnerabilities

SWC-100 –> Function Default Visibility = PASSED

SWC-101 –> Integer Overflow and Underflow = PASSED

SWC=102 –> Outdated Compiler Version = PASSED

SWC-103 –> Floating Pragma = LOW ISSUE

SWC-104 –> Unlocked Call Return Value = PASSED

Vulnerabilities

SCAN RESULTS

SWC-105 –> Unprotected Ether Withdrawal = PASSED

SWC=106 –> Unprotected SELF DESTRUCT Instruction = PASSED

SWC-107 –> Reentrancy = PASSED

SWC-108 –> State Variable Default Visibility = LOW ISSUE

SWC-109 –> Uninitialized Storage Pointer = PASSED

SWC-110 –> Assert Violation = PASSED

SWC-111 –> Use of Deprecated Solidity Functions = PASSED

SWC-112 –> Delegatecall to Untrusted Callee = PASSED

Vulnerabilities

SCAN RESULTS

SWC-113 –> DoS with Failed Call = PASSED

SWC-114 –> Transaction Order Dependence = PASSED

SWC-115 –> Authorization Through Tx. Origin = PASSED

SWC-116 –> Block Values as a Value for Time = PASSED

SWC-117 –> Signature Malleability = PASSED

SWC-118 –> Incorrect Constructor Name = PASSED

SWC-119 –> Shadowing State Variables = PASSED

SWC-120 –> Weak Source of Randomness From Chain Attributes = LOW ISSUE

Vulnerabilities

SCAN RESULTS

SWC-121 –> Missing Protection Against Signature Replay Attacks = PASSED

SWC-122 –> Lack of Proper Signature Verification = PASSED

SWC-123 –> Requirement Violation = PASSED

SWC-124 –> Write to Arbitrary Storage Location = PASSED

SWC-125 –> Incorrect Inheritance Order = PASSED

SWC-126 –> Insufficient Gas Griefing = PASSED

SWC-127 –> Arbitrary Jump with Function Type Variable = PASSED

SWC=128 –> DoS with Block Gas Limit = PASSED

Vulnerabilities

SCAN RESULTS

SWC-129 –> Typographical Error = PASSED

SWC-130 –> Right-to-Left Override Control Character = PASSED

SWC-131 –> Presence of Unused Variables = PASSED

SWC-132 –> Unexpected Ether Balance = PASSED

SWC-133 –> Hash Collisions with Multiple Variable Length Arguments = PASSED

SWC-134 –> Message Call with Hardcoded Gas Amount = PASSED

SWC-135 –> Code with no effects = PASSED

SWC-136 –> Unencrypted Private Data On-Chain = PASSED

Low Issues Found

* Please Note:

SWC-103- L. 2 C. 1

Floating Pragma

“A Floating Pragma is set”

Contracts should be deployed with the same compiler version and flags that they have been tested with thoroughly. Locking the pragma helps to ensure that contracts do not accidentally get deployed using, for example, an outdated compiler version that might introduce bugs that affect the contract system negatively.

Low Issues Found

Please Note:

SWC-120 - L. 29 C. 3469 & L. 29 C. 6856

Weak sources of Randomness from Chain Attributes

“Potential use of “block.number” as a source of randomness”

Ability to generate random numbers is very helpful in all kinds of applications. One obvious example is gambling DApps, where pseudo-random number generator is used to pick the winner. However, creating a strong enough source of randomness in Ethereum is very challenging. For example, use of block.timestamp is insecure, as a miner can choose to provide any timestamp within a few seconds and still get his block accepted by others. Use of blockhash, block.difficulty and other fields is also insecure, as they're controlled by the miner. If the stakes are high, the miner can mine lots of blocks in a short time by renting hardware, pick the block that has required block hash for him to win, and drop all others.

.

Overall Assessment

Satisfactory!

Inter World ITW Token has
successfully passed the ICSA Audit!

February 15th, 2024

Closing Notes

Enhance the security of your crypto smart contracts with ICSA - the company you can trust with your digital assets. Contact us today to schedule an audit and benefit from our cutting-edge expertise in securing your blockchain projects. ICSA: Your gateway to safer, more secure smart contracts.

Whilst there are limitless ownable callable functions that have the potential to be dangerous, they are not overtly so. Trust in the team would mitigate many of these risks. Please make sure you do your own research. If in doubt please contact the project team.

Always make sure to inspect all values and variables.

This includes, but is not limited to: · Ownership · Proper Ownership Renouncement (if any) · Taxes · Transaction/Wallet Limits · Token Distributions · Timelocks · Liquidity Locks · Any other owner-adjustable settings or variables.

Thank you for choosing ICSA

https://icsa.website/