Audit By ICSA

International Crypto Services Agency

Blocjerk Token

February 28th, 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.

Blocjerk team agreed and provided us with the files that needed to be tested (Through Github, EtherScan, 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 Blocjerk to perform an audit of their smart contract:

Contract Address

0x9cAAe40DCF950aFEA443119e51E821D6FE2437ca

Blockchain

Ethereum

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

Blocjerk is the first ever layer 2 protocol for adult markets leveraging AI and Blockchain. They offer cutting edge data analytic toolkits that are integrated with tokenized fan services, free tube streaming and their very own Wank2Earn.

Blocjerk Telegram

Blocjerk Website

Blocjerk Discord

Blocjerk Twitter

Contract Details

Token Name - Blocjerk Token

Token Description - DAO Token

Compiler Version - v0.8.9

Current Holders - 3 Addresses

Current Transaction Count - 3

Max Supply - 10,000,000

Token Ticker - BJ

Decimals - 18

LP Lock - No LP Lock

KYCd by - ICSA

Buy Fee - 0%

Sell Fee - 0%

Launch Type - Private/Presale

Owner can set buy/sell fees to up to 100%. Owner can mint tokens up to the maximum supply.. Contract is Proxy to

Tokenomics

Contract Address

0x9cAAe40DCF950aFEA443119e51E821D6FE2437ca

Contract Deployer

0x394ee51b4a2415e89c1bb2de46d3eB3dE8dc96dC

Contract Owner

0x9f29801ac82befe279786e5691b0399b637c560c

Contract proxy to

0x9123e113BD21C50f436Ab41d25f16674b9Fea64D

Owner Privileges

Privileges and notes

Ownership HAS NOT BEEN renounced. The owner has some privileges or authority to make SOME changes. Owner can add mint new tokens and set tax's yo 100%, project is KYC and Ltd Co.

Adjustable Functions

1. addPoolToTax
2. approve
3. authorizeSnapshotter
4. burn
5. burnBulk
6. deauthorizeSnapshotter
7. increaseAllowance
8. decreaseAllowance
9. initialize
10. initializeImplementation
11. mint
12. pause
13. renounceOwnership
14. setBuySellTaxRate
15. setTaxTo
16. snapshot
17. transfer
18. transferBulk
19. transferFrom
20. transferFromBulk
21. transferOwnership
22. unpause

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 = PASSED

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:

Several Low issues found within the code but none that can affect the security of the contract.

Overall Assessment

Satisfactory!

Blocjerk Token has successfully passed the ICSA Audit!

February 28th, 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,. 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/