



BLOCK AUDIT REPORT

Smart Contract Security Audit Report



UShark



BLOCK AUDIT REPORT

Block Audit Report Team received the Token.sol file for smart contract security audit of the on October 12, 2022. The following are the details and results of this smart contract security audit:

Project Name: [Ushark](#)

Link Address:

<https://bscscan.com/address/0xc6893701753bd185f6ed3ff204fd3d76f19a50ea#code>

The audit items and results:

(Other undiscovered security vulnerabilities are not included in the audit responsibility scope)

Audit Result: Passed

Audit Number: BAR0027121072022

Audit Date: October 14, 2022

Audit Team: Block Audit Report Team



Table of Content

Introduction	4-5
Auditing Approach and Methodologies applied	4
Audit Details.....	5
Audit Goals	6-7
Security	6
Sound Architecture.....	6
Code Correctness and Quality	6
Audit Results	6
High level severity issues	6
Medium level severity issues	6
Low level severity issues.....	6
Issues Checking Status	7
Manual Audit:	8-9
Critical level severity issues	9
High level severity issues	9
Medium level severity issues	9
Low level severity issues.....	9
Owner Privileges	9
Automated Audit	10
Remix Compiler Warnings	10
Disclaimer	11
Summary	12



Introduction

This Audit Report mainly focuses on the extensive security of Mezmerize Game Smart Contracts. With this report, we attempt to ensure the reliability and correctness of the smart contract by complete and rigorous assessment of the system's architecture and the smart contract codebase.

Auditing Approach and Methodologies applied

The Block Audit Report team has performed rigorous testing of the project including the analysis of the code design patterns where we reviewed the smart contract architecture to ensure it is structured along with the safe use of standard inherited contracts and libraries. Our team also conducted a formal line by line inspection of the Smart Contract i.e., a manual review, to find potential issues including but not limited to;

- ✓ Race conditions
- ✓ Zero race conditions approval attacks
- ✓ Re-entrancy
- ✓ Transaction-ordering dependence
- ✓ Timestamp dependence
- ✓ Check-effects-interaction pattern (optimistic accounting)
- ✓ Decentralized denial-of-service attacks
- ✓ Secure ether transfer pattern
- ✓ Guard check pattern
- ✓ Fail-safe mode
- ✓ Gas-limits and infinite loops
- ✓ Call Stack depth

In the Unit testing Phase, we coded/conducted custom unit tests written against each function in the contract to verify the claimed functionality from our client.

In Automated Testing, we tested the Smart Contract with our standard set of multifunctional tools to identify vulnerabilities and security flaws.

The code was tested in collaboration of our multiple team members and this included but not limited to;

- Testing the functionality of the Smart Contract to determine proper logic has been followed throughout the whole process.
- Analyzing the complexity of the code in depth and detailed, manual review of the code,



line-by-line.

- Deploying the code on testnet using multiple clients to run live tests.
- Analyzing failure preparations to check how the Smart Contract performs in case of any bugs and vulnerabilities.
- Checking whether all the libraries used in the code are on the latest version.
- Analyzing the security of the on-chain data.

Audit Details

Project Name: Mezmerize Game

Website: <https://ushark.io/>

Twitter: <https://twitter.com/usharktoken>

LinkedIn: <https://www.linkedin.com/in/utility-shark-token-117616224/>

Facebook: <https://web.facebook.com/profile.php?id=100074181520893>

Discord: <https://ushark.io/#utilitysharktoken#0078>

Instagram: https://instagram.com/usharktoken?utm_medium=copy_link

Telegram: <https://t.me/usharkGlobal>

Languages: Solidity (Smart contract)

Platforms and Tools: Remix IDE, Truffle, Ganache, Mythril, Contract Library, Slither, DappTools, Echidna, Etheno



Audit Goals

The focus of the audit was to verify that the Smart Contract System is secure, resilient and working according to the specifications. The audit activities can be grouped in the following three categories:

Sound Architecture

Evaluation of the architecture of this system through the lens of established smart contract best practices and general software best practices, standard software design principle, design patterns and practices.

Code Correctness and Quality

A full review of the contract source code. The primary areas of focus include:

- Accuracy
- Readability
- Usability vs Security
- Sections of code with high complexity
- Quantity and quality of test coverage

Issue Categories

Every issue in this report was assigned a severity level from the following:

Critical Severity Issues

Issues of this level are critical to the smart contract's performance/functionality and should be fixed before moving to a production environment.

High level severity issues

Issues on this level are strongly suggested by the team to be fixed before moving to the production environment.

Medium level severity issues

Issues on this level could potentially bring problems and should eventually be fixed.

Low level severity issues

Issues on this level are minor details and warnings that can remain unfixed but would be better fixed at some point in the future.



Issues Checking Status

S.No.	Issue description	Checking status
1	Compiler warnings.	Passed
2	Race conditions and Reentrancy. Cross-function race conditions.	Passed
3	Oracle calls.	Passed
4	Timestamp dependence.	Passed
5	DoS with Revert.	Passed
6	DoS with block gas limit.	Passed
7	Methods execution permissions.	Passed
8	Economy model.	Passed
9	The impact of the exchange rate on the logic.	Passed
10	Malicious Event log.	Passed
11	Scoping and Declarations.	Passed
12	Uninitialized storage pointers.	Passed
13	Arithmetic Operations accuracy.	Passed
14	Design Logic.	Passed
15	Cross-function race conditions.	Passed
16	Safe usage for Open Zeppelin module.	Passed
17	Fallback function security.	Passed
18	Send & receive ether.	Passed
19	Zero race condition approval attacks.	Passed
20	Short address attack.	Passed
21	Owner's authority to freeze.	Passed
22	Attempt to block ether flows.	Passed
23	Redundant inheritance check.	Passed
24	Silent overrides of mapping structs.	Passed
25	Function state mutability.	Passed
26	Unnecessary conversion of type.	Passed



Manual Audit:

For this section the code was tested/read line by line by our auditors. We used Remix IDE's JavaScript VM, Truffle and testnet Kovan to test the contract functionality in a simulated environment.

Files in scope

<https://github.com/MezmerizeGame/SmartContract/blob/main/MZEGAME.sol>

File 1 of 1 : Token.sol	Passed
-------------------------	--------



Audit Results

Critical Severity Issues

No critical severity issues found.

High Severity Issues

No high severity issues found.

Medium Severity Issues

No medium severity issues found

Low Severity Issues

Issue	File	Type	Line	Description
#1	Main	Contract doesn't import npm packages from source (like OpenZeppelin etc.)	-	We recommend importing all packages from npm directly without flattening the contract. Functions could be modified or can be susceptible to vulnerabilities
#2	Main	Floating Pragma	-	The current pragma Solidity directive is "^0.5.0". Contracts should be deployed with the same compiler version and flags that they have been tested thoroughly. Locking the pragma helps to ensure that contracts do not accidentally get deployed using other versions.
#3	Main	Old Compiler Version	-	The contract uses an old compiler version which is not recommended because old versions are prone to known attacks and vulnerabilities.



BLOCK AUDIT REPORT

#4	Main	Missing Zero check	138,170	There is no zero address validation in the transfer functions which may lead to loss of user funds if the users send the funds to the zero address by accident.
#5	Main	Owner can drain tokens	212	Owner can pass the native token address in the function and drain/withdraw the complete balance of the smart contract.

Ownership privileges

The contract is highly centralized and if the owner's keys are somehow compromised then it can bring down the whole project. We advise to keep the private keys secure and use a multi-sig wallet. Moreover, if the ownership is renounced without proper research and information, the changes in the contract will be irreversible.

Owner's Address: 0x5a4F1BAC9Ea8272d34296a1736740877C6C5C9Fe

Issue	File	Description
#1	Main	<ul style="list-style-type: none">The owner can withdraw stuck tokens and also the native tokens

Automated Audit

No major issues were found. Some false positive errors were reported by the tools. All the other issues have been characterized above conferring to their level of severity.



Disclaimer

This is a limited report on our findings based on our analysis, in accordance with good industry practice as at the date of this report, in relation to cybersecurity vulnerabilities and issues in the framework and algorithms based on smart contracts, the details of which are set out in this report. In order to get a full view of our analysis, it is crucial for the client to read the full report. While we have done our best in conducting our analysis and producing this report, it is important to note that the client should not rely on this report and cannot claim against us on the basis of what it says or doesn't say, or how we produced it, and it is important for the client to conduct the client's own independent investigations before making any decisions. We go into more detail on this in the below disclaimer below – please make sure to read it in full.

By reading this report or any part of it, the client agrees to the terms of this disclaimer. If the client does not agree to the terms, then please immediately cease reading this report, and delete and destroy any/all copies of this report downloaded and/or printed by the client. This report is provided for information purposes only and stays on a non-reliance basis, and does not constitute investment advice. No one/ NONE shall have any rights to rely on the report or its contents, and BlockAudit and its affiliates (including holding companies, shareholders, subsidiaries, employees, directors, officers and other representatives).

(BlockAudit) owes no duty of care towards the client or any other person, nor does BlockAudit claim any warranty or representation to any person on the accuracy or completeness of the report. The report is provided "as is", without any conditions, warranties or other terms of any kind except as set out in this disclaimer, and BlockAudit hereby excludes all representations, warranties, conditions and other terms (including, without limitation, the warranties implied by law of satisfactory quality, fitness for purpose and the use of reasonable care and skill) which, but for this clause, might have effects in relation to the report. Except and only to the extent that it is prohibited by law, BlockAudit hereby excludes all liability and responsibility, and neither the client nor any other person shall have any claim against BlockAudit, for any amount or kind of loss or damage that may result to the client or any other person (including without limitation, any direct, indirect, special, punitive, consequential or pure economic loss or damages, or any loss of income, profits, goodwill, data, contracts, use of money, or business interruption, and whether in delict, tort (including without limitation negligence), contract, breach of statutory duty, misrepresentation (whether innocent or negligent) or otherwise under any claim of any nature whatsoever in any jurisdiction) in any way arising from or connected with this report and the use, inability to use or the results of use of this



report, and any reliance on this report.

The analysis of the security is purely based on the received smart contracts alone. No related/third-party smart contracts, applications or operations were reviewed for security. No product code has been reviewed.

Note: 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. Securing smart contracts is a multistep process. One audit cannot be considered enough. We recommend that the USHark team put a bug bounty program in place to encourage further analysis of the smart contracts by other third parties.



BLOCK AUDIT REPORT



Summary

Smart contracts received in file named: "Token.sol" does not contain any high severity issues!

Note:

Please read the disclaimer above and note, the audit claims NO statements or warranties on business model, investment advice/ attractiveness or code sustainability. This report is provided for the only set of contracts mentioned in the report and does not claim responsibility to include security audits for any other contracts deployed by Owner.



BLOCK AUDIT REPORT



BLOCK AUDIT REPORT



BLOCK AUDIT REPORT

Official Website

www.blockaudit.report



E-Mail

team@blockaudit.report



Twitter

<https://twitter.com/BlockAudit>



Github

<https://github.com/blockauditreport>