



MOTECH AUDIT

SMART CONTRACT SECURITY AUDIT

SECURITY ASSESSMENT

HEROVERSE TOKEN AUDIT REPORT

2021

2 DEC 2021

SECURITY ASSESMENT

TABLE OF CONTENTS

Summary	3
Disclaimer	4
Background	5
Audit Details	6
Contract Details	7
HeroVerse Token Distribution	8
HeroVerse Token Contract Interaction Details	8
Top 10 Token Holders	9
Security Issue	10 -12
Token Logo	13
Conclusion	14



SECURITY ASSESSMENT SUMMARY

This report has been prepared for HeroVerse to discover issues and vulnerabilities in the source code of the HeroVerse project as well as any contract dependencies that were not part of an officially recognized library. A comprehensive examination has been performed, utilizing Static Analysis, Manual Review, and Test net Deployment techniques.

The auditing process pays special attention to the following considerations:

- Testing the smart contracts against both common and uncommon attack vectors.
- Assessing the codebase to ensure compliance with current best practices and industry standards.
- Ensuring contract logic meets the specifications and intentions of the client.
- Cross referencing contract structure and implementation against similar smart contracts produced by industry leaders.
- Thorough line-by-line manual review of the entire codebase by industry experts.

The security assessment resulted in findings that ranged from critical to informational. We recommend addressing these findings to ensure a high level of security standards and industry practices. We suggest recommendations that could better serve the project from the security perspective:

- Enhance general coding practices for better structures of source codes;
- Add enough unit tests to cover the possible use cases given they are currently missing in the repository;
- Provide more comments per each function for readability, especially contracts are verified in public;
- Provide more transparency on privileged activities once the protocol is live.



MOTECH AUDIT
SMART CONTRACT SECURITY AUDIT

SECURITY ASSESSMENT

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 you 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 you 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 you to conduct your 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.

DISCLAIMER: By reading this report or any part of it, you agree to the terms of this disclaimer. If you do not agree to the terms, then please immediately cease reading this report, and delete and destroy any and all copies of this report downloaded and/or printed by you. This report is provided for information purposes only and on a non-reliance basis, and does not constitute investment advice. No one shall have any right to rely on the report or its contents, and MotechAudit and its affiliates (including holding companies, shareholders, subsidiaries, employees, directors, officers and other representatives) (MotechAudit) owe no duty of care towards you or any other person, nor does MotechAudit make 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 MotechAudit 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 effect in relation to the report. Except and only to the extent that it is prohibited by law, MotechAudit hereby excludes all liability and responsibility, and neither you nor any other person shall have any claim against MotechAudit, for any amount or kind of loss or damage that may result to you 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 smart contracts alone. No applications or operations were reviewed for security. No product code has been reviewed.



MOTECH AUDIT
SMART CONTRACT SECURITY AUDIT

SECURITY ASSESSMENT

BACKGROUND

MotechAudit was commissioned by HeroVerse to perform an audit of smart contracts:

<https://bscscan.com/address/0x6b9f6f911384886b2e622e406327085238f8a3c5>

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.



MOTECH AUDIT
SMART CONTRACT SECURITY AUDIT

SECURITY ASSESSMENT

AUDIT DETAILS



AUDITED PROJECT

HeroVerse



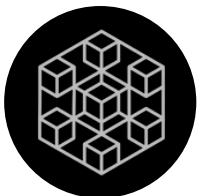
DEPLOYER ADDRESS

0x40ac6fDBEba2128eB4aF048E3199FdB989550e13



CLIENT CONTACTS:

HeroVerse Team



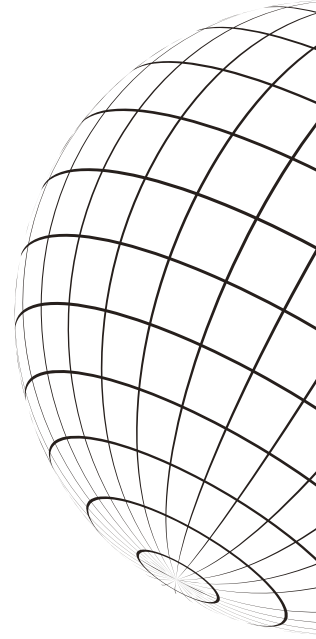
BLOCKCHAIN

BSC Project



WEBSITE:

<https://heroverse.io/>

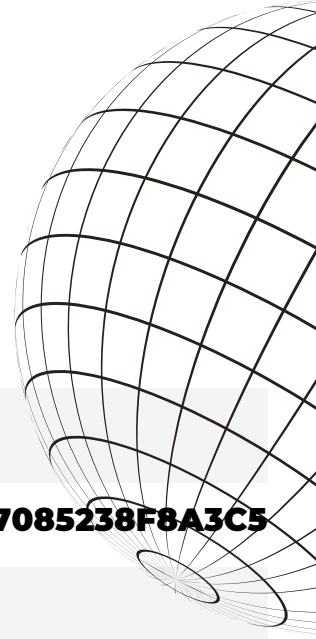


MOTECH AUDIT
SMART CONTRACT SECURITY AUDIT

SECURITY ASSESSMENT

CONTRACT DETAILS

Token contract details for Sep-23-2021



Contract name	HeroVerse
Contract address	0x6B9F6f911384886b2e622e406327085238F8A3C5
Total supply	1,000,000,000 HER
Token ticker	HeroVerse Token (HER)
Decimals	18
Token holders	7,594
Transactions count	155,383
Top 100 holders dominance	98.6910%
Contract deployer address	0x40ac6fDBEba2128eB4aF048E3199FdB989550e13
Contract's current owner address	0x40ac6fDBEba2128eB4aF048E3199FdB989550e13



SECURITY ASSESSMENT

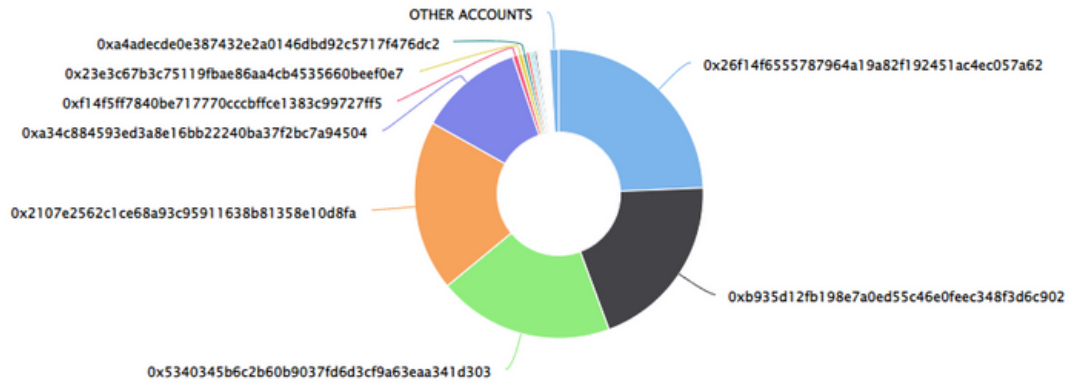
HEROVERSE TOKEN DISTRIBUTION

The top 100 holders collectively own 98.98% (989,828,521.51 Tokens) of HeroVerse Token

Token Total Supply: 1,000,000,000.00 Token | Total Token Holders: 7,595

HeroVerse Token Top 100 Token Holders

Source: BscScan.com



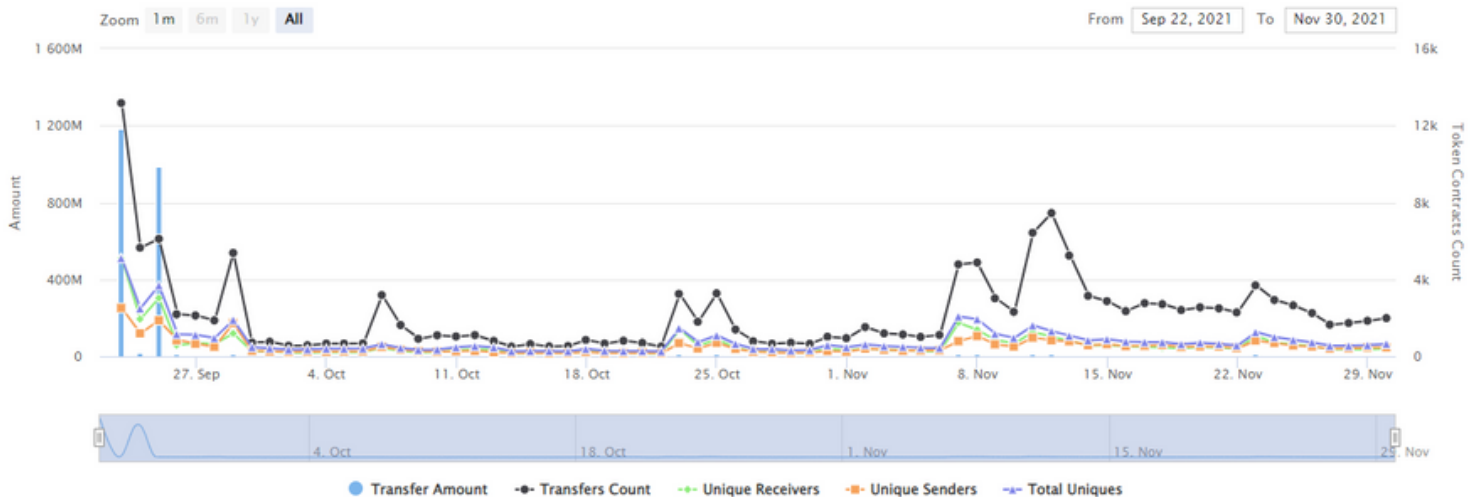
(A total of 989,828,521.51 tokens held by the top 100 accounts from the total supply of 1,000,000,000.00 token)

HEROVERSE TOKEN CONTRACT INTERACTION DETAILS

Time Series: Token Contract Overview

Thu 23, Sept 2021 - Tue 30, Nov 2021



















Token Contract 0x6b9f6f911384886b2e622e406327085238f8a3c5 (HeroVerse Token)
Source: BscScan.com



MOTECH AUDIT
SMART CONTRACT SECURITY AUDIT

SECURITY ASSESSMENT

TOP 10 TOKEN HOLDERS

Rank	Address	Quantity	Percentage	Value	Analytics
1	 0x26f14f6555787964a19a82f192451ac4ec057a62	243,599,900	24.3600%	\$26,314,635.60	
2	 0xb935d12fb198e7a0ed55c46e0feec348f3d6c902	200,000,000	20.0000%	\$21,604,800.00	
3	 0x5340345b6c2b60b9037fd6d3cf9a63eaa341d303	196,666,666	19.6667%	\$21,244,719.93	
4	 0x2107e2562c1ce68a93c95911638b81358e10d8fa	191,000,000	19.1000%	\$20,632,584.00	
5	 0xa34c884593ed3a8e16bb22240ba37f2bc7a94504	117,129,890	11.7130%	\$12,652,839.24	
6	0xf14f5ff7840be717770cccbffce1383c99727ff5	5,851,000	0.5851%	\$632,048.42	
7	 0x23e3c67b3c75119fbae86aa4cb4535660beef0e7	5,560,132.110350405015802683	0.5560%	\$600,627.71	
8	 0xa4adecde0e387432e2a0146dbd92c5717f476dc2	3,775,141.0015661	0.3775%	\$407,805.83	
9	 0x17903b54623c029ec0bbac05265f72586014a47a	3,756,138.418308777	0.3756%	\$405,753.10	
10	0x1f15dd72299445678f287e34e67952e268188361	3,333,333	0.3333%	\$360,079.96	

source:<https://bscscan.com/>



MOTECH AUDIT
SMART CONTRACT SECURITY AUDIT

SECURITY ASSESSMENT

SECURITY ISSUES

✓ High Severity Issues

No high severity issues found.

✓ Medium Severity Issues

No high severity issues found.

⚠ Low Severity Issues

1. Multiplication and power readability.

It's recommended to use scientific notation and ether unit suffix instead of multiplication and power of ten. While the compiler will definitely transform it to the constant in compile-time, scientific notation with ether suffix could be more readable.

Contract: HeroVerseToken.sol

Function: constructor

Recommendation: Please try to use more efficient writing like "1e9 ether" instead.

Status: Fixed

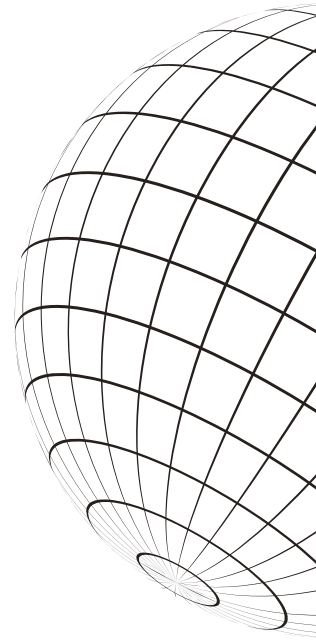
2. Missing zero address validation.

Calling constructor it is possible to set mistaken treasury and heroVerseToken as zero addresses and then there is no possibility to modify those. That could lead to unexpected results.

Contract: HeroNFT.sol

Functions: constructor

Recommendation: Please verify that treasury and heroVerseToken are not zero-address. Status: Fixed



MOTECH AUDIT
SMART CONTRACT SECURITY AUDIT

SECURITY ASSESSMENT

SECURITY ISSUES

3. State variables that could be declared immutable.

State variables that are initialized in the constructor and never change their values should be declared immutable to save gas.

Contract: HeroNFT.sol

Variable: treasury

Recommendation: Add the immutable attributes to state variables that never change and are initialized in the constructor.

Status: Fixed

4. Boolean equality.

Boolean constants can be used directly and do not need to be compared to true or false.

Contract: HeroNFT.sol

Function: _generateHero

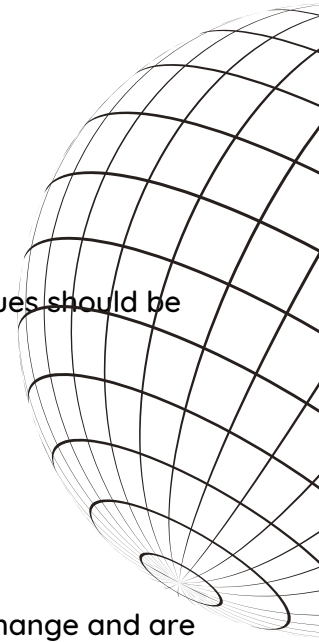
Recommendation: Remove the equality to the boolean constant.

Status: Fixed

5. A public function that could be declared external.

public functions that are never called by the contract should be declared external to save gas.

Contract: ChainlinkRandomNumberGenerator.sol



SECURITY ASSESSMENT

SECURITY ISSUES

Functions: withdrawTokens, requestRandomNumber

Recommendation: Use the external attribute for functions never called from the contract.

Status: Fixed

6. A public function that could be declared external.

public functions that are never called by the contract should be declared external to save gas.

Contract: OraiRandomNumberGenerator.sol

Functions: transferOnlyOwner, requestRandomNumber

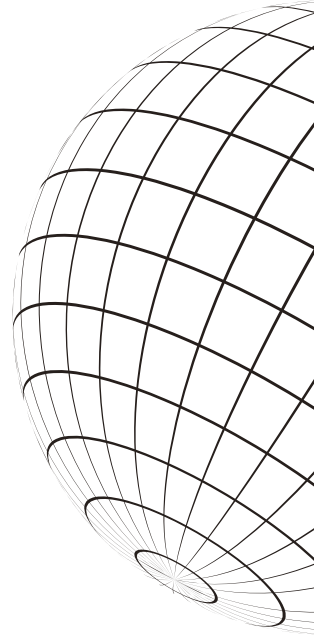
Recommendation: Use the external attribute for functions never called from the contract.

Status: Fixed



MOTECH AUDIT
SMART CONTRACT SECURITY AUDIT

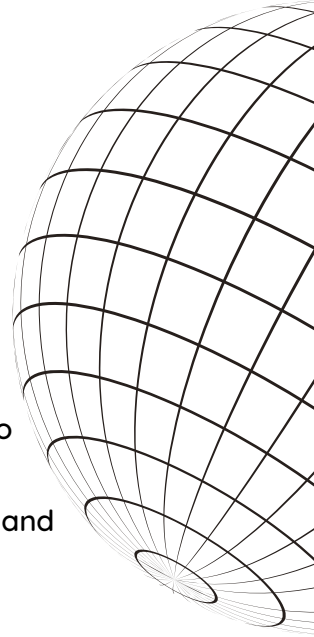
SECURITY ASSESMENT
TOKEN LOGO



SECURITY ASSESMENT CONCLUSION

Smart contracts contain owner privileges!

Motech Audit note: Please check the disclaimer above and note, the audit makes no statements or warranties on business model, investment attractiveness or code sustainability. The report is provided for the only contract mentioned in the report and does not include any other potential contracts deployed by Owner.



MOTECH AUDIT
SMART CONTRACT SECURITY AUDIT