

MARCH 2023

Citrix Audit



SHIBONSU INU
AUDIT

Shibonsu Inu Audit Report

Analysis Smart Contract



PREPARED BY
Jonas Eddie

APPROVED BY
Mike Den

Audit Summary

Project Name - DogaCEO

DATE : 7 MARCH, 2023

Audit Status:

PASSED.

Scope of Audit

In the world of blockchain technology, the importance of security cannot be overstated, and that's why it's so critical to have a team like Audit on your side. Their smart contract audit services are second to none, and they're dedicated to providing the highest level of security and quality to their clients.

03/03/2023



ISSUE REPORT

Issues Found

| Status | Critical | High | Medium | Low | Suggestion |
|--------------|----------|------|--------|-----|------------|
| Open | 0 | 0 | 0 | 0 | 2 |
| Acknowledged | 0 | 0 | 0 | 0 | 0 |
| Resolved | 0 | 0 | 0 | 0 | 0 |

Date Release:

07/03/2023



SHIBONSU INU

TOKEN INFORMATION

Token name : DogaCEO

Token Symbol : Shibonsu

Decimals : 9

Total Supply : 100,000,000,000,000,000

Address:

0x5a99e99b50bb16d2e5b795e9509f0774ee4e
c4f5

Owner :

0xc9393B875be8Eb8a3aBd862256765bADB3100d
0F



Doga CEO

Token Overview

Fees:

Buy Fee : 10%

Sell Fee : 10%

Ownership :

Owned

Minting

No mint function

Max Tx Amount/ Max Wallet Amount:

No

Blacklist:

No

Other Privileges:

None

VULNERABILITY CHECKLIST



Return values of low-level calls



Private modifier



Multiple Sends



Using Suicide



Gas Limitand Loops



Address hardcoded



Exception Disorder



Using inline assembly



Divide before multiply



Missing Zero Address Validation



Compiler version not fixed



Gasless Send



Using block.timestamp



Re-entrancy



Tautology or contradiction



Timestamp Dependence



Revert/require functions



Use of tx.origin



Integer overflow/underflow



Dangerous strict equalities



Using SHA3



Using throw

CLASSIFICATION OF RISK

| Severity | Description |
|--------------------------------|--|
| ◆ Critical | These vulnerabilities could be exploited easily and can lead to asset loss, data loss, asset, or data manipulation. They should be fixed right away. |
| ◆ High-Risk | A vulnerability that affects the desired outcome when using a contract, or provides the opportunity to use a contract in an unintended way. |
| ◆ Medium-Risk | A vulnerability that could affect the desired outcome of executing the contract in a specific scenario. |
| ◆ Low-Risk | A vulnerability that does not have a significant impact on possible scenarios for the use of the contract and is probably subjective. |
| ◆ Gas Optimization /Suggestion | A vulnerability that has an informational character but is not affecting any of the code. |

Findings

| Severity | Found |
|-------------------------------------|-------|
| ◆ Critical | 0 |
| ◆ High-Risk | 0 |
| ◆ Medium-Risk | 0 |
| ◆ Low-Risk | 0 |
| ◆ Gas Optimization / Suggestions | 2 |

DISCLAIMER

All the content provided in this document is for general information only and should not be used as financial advice or a reason to buy any investment. Team provides no guarantees against the sale of team tokens or the removal of liquidity by the project audited in this document. Always Do your own research and protect yourselves from being scammed. The Auditace team has audited this project for general information and only expresses their opinion based on similar projects and checks from popular diagnostic tools. Under no circumstances did Auditace receive a payment to manipulate those results or change the awarding badge that we will be adding in our website. Always Do your own research and protect yourselves from scams. This document should not be presented as a reason to buy or not buy any particular token. The Auditace team disclaims any liability for the resulting losses.
