



SHIBA INU



Ethereum

Public audit report



trustedbytes.org



contact@trustedbytes.org

2023



Contents

| | |
|---|----------|
| 1. Project description..... | 3 |
| 2. Introduction..... | 4 |
| 3. Technical audit..... | 5 |
| 3.1 Automatic check results..... | 5 |
| 3.2 Issues..... | 6 |
| 4. Project Overview..... | 7 |
| 5. Disclaimer..... | 8 |



Project description

| | |
|--------------|---|
| Token name | SHIBA |
| URL | https://shibatoken.com/ |
| Blockchain | Ethereum |
| Project name | SHIBA INU |
| Logo |  |
| Ticker | \$SHIB |
| Address | 0x95aD61b0a150d79219dCF64E1E6Cc01f0B64C4cE |
| Date | 2023-02-04 |



Introduction

The report was prepared for SHIBA INU team. The audit was requested by a community member.

The token supports the ERC-20 interface and realizes a custom tokens redistribution concept. Commissions are taken on transfers and redistributed between other users.

.....

🛡 Procedure

We perform our audit according to the following procedure:

- Automated analysis;
- Scanning the project's smart contracts with automated Solidity analysis tools of our own development;
- Manual verification all the issues found by the tools.

Manual audit

- 🛡 Manually analyse smart contracts for well known or trended security vulnerabilities
- 🛡 Smart contracts' logic check



Automatic check results

| Title | Check result |
|--|--------------|
| Unencrypted Private Data On-Chain | passed |
| Code With No Effects | passed |
| Message call with hardcoded gas amount | passed |
| Typographical Error | passed |
| DoS With Block Gas Limit | passed |
| Presence of unused variables | passed |
| Incorrect Inheritance Order | passed |
| Requirement Violation | passed |
| Weak Sources of Randomness from Chain | passed |
| Attributes | passed |
| Shadowing State Variables | passed |
| Incorrect Constructor Name | passed |
| Block values as a proxy for time | passed |
| Authorization through tx.origin | passed |
| DoS with Failed Call | passed |
| Delegatecall to Untrusted Callee | passed |
| Use of Deprecated Solidity Functions | passed |
| Assert Violation | passed |
| State Variable Default Visibility | passed |
| Reentrancy | passed |
| Unprotected SELFDESTRUCT Instruction | passed |



Issues

| | |
|-------------|-----------|
| High risk | Not found |
| Medium risk | Not found |
| Low risk | Not found |

Security Score: A

Issues description:

Issues not found

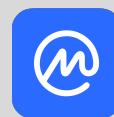


Project overview



Twitter

**3,6m
subscribers**



Coinmarketcap

rating: #13
- 46,23% (1Y) price



Token Holders

1,287,019



Telegram

**78k
members**



Disclaimer

This audit report is based on the existing knowledge and skills of our auditors, as well as specialized tools of our own development. Verification is always carried out for already known main types of vulnerabilities and threats, both from the user (investor) and from the developers. An audit of a smart contract doesn't provide a full guarantee that a particular project is completely safe. An audit is just one of the tools to check the honesty of the founders (developers) and their professional skills in developing, along with such methods as liquidity pool locking , KYC and others. Only in the aggregate, you can decide whether to invest in a project or not to do it. First of all DYOR and nothing else.



Trustedbytes.org



Contact@trustedbytes.org



/Trustedbytesorg



@trustedbytes



@trustedbytesorg