MOTECH AUDIT

SMART CONTRACT SECURITY AUDIT

SECURITY ASSESSMENT

2021

SHIBASWAP PROGRESS REPORT

12 OCT 2021

SECURITY ASSESMENT

TABLE OF CONTENTS

SECURITY ASSESMENT

SUMMARY

This report has been prepared for SafeMoon to discover issues and vulnerabilities in the source code ofthe SafeMoon project as well as any contract dependencies that were not part of an officially recognizedlibrary. A comprehensive examination has been performed, utilizing Static Analysis, Manual Review, andTestnet 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 producedby 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 recommendaddressing these findings to ensure a high level of security standards and industry practices. We suggestrecommendations 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;
●Provide more comments per each function for readability, especially contracts that are verified inpublic;
●Provide more transparency on privileged activities once the protocol is live.

SECURITY ASSESMENT

BACKGROUND

MotechAudit was commissioned by SHIBA INU to perform an audit of smart contracts:
https://etherscan.io/address/0x95aD61b0a150d79219dCF64E1E6Cc01f0B64C4cE
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.

SECURITY ASSESMENT

AUDIT DETAILS

AUDITED PROJECT

ShibaSwap

DEPLOYER ADDRESS

0xB8f226dDb7bC672E27dffB67e4adAbFa8c0dFA08

CLIENT CONTACTS:

ShibaSwap team

BLOCKCHAIN

Ethereum Project

WEBSITE:

https://shibatoken.com/

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.

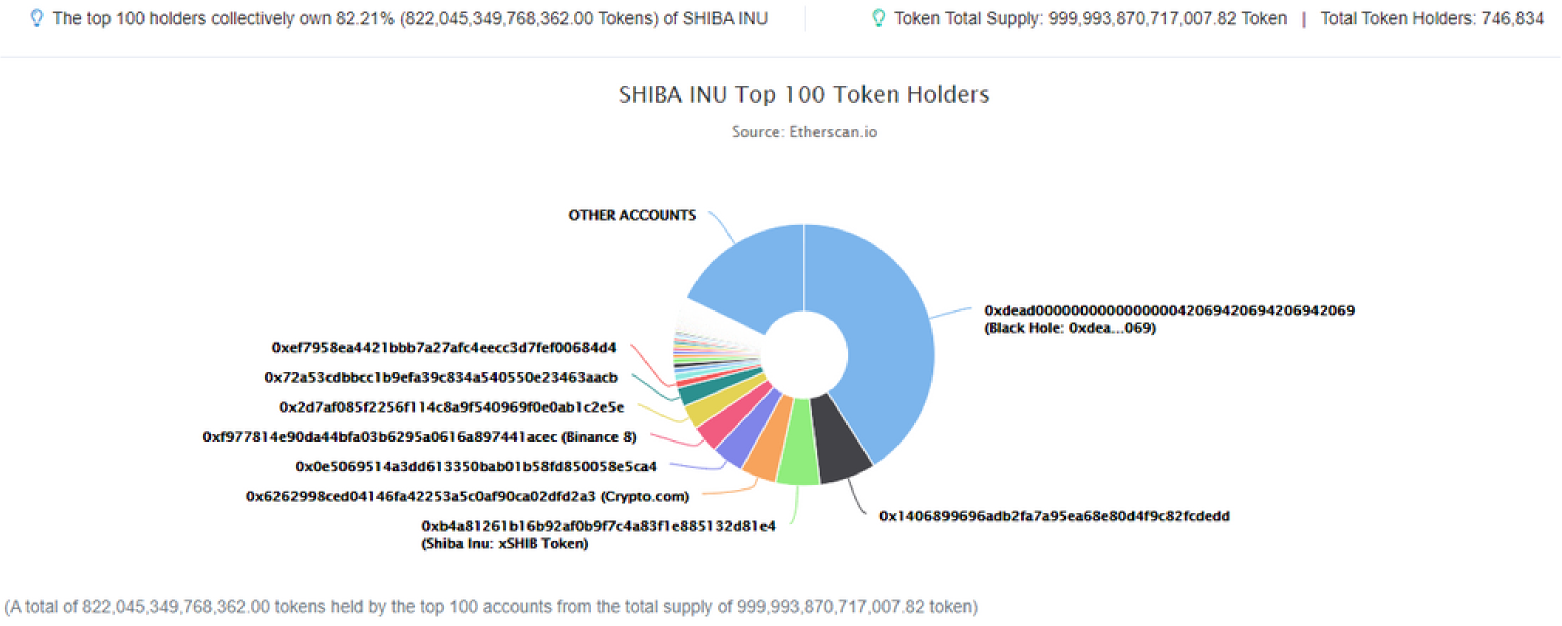
SECURITY ASSESMENT

CONTRACT DETAILS

Token contract details for Feb-18-2018

Contract name	**ShibaSwap**
Contract address	**0x95aD61b0a150d79219dCF64E1E6Cc01f0B64C4cE**
Total supply	**1,000,000,000,000,000**
Token ticker	**SHIBA INU (SHIB)**
Decimals	**18**
Token holders	**746,709**
Transactions count	**4,401,111**
Top 100 holders dominance	**80.5709%**
Contract deployer address	**0xB8f226dDb7bC672E27dffB67e4adAbFa8c0dFA08**
Contract's current owner address	**0x95aD61b0a150d79219dCF64E1E6Cc01f0B64C4cE**

SHIBASWAP TOKEN DISTRIBUTION



The top 100 holders collectively own 82.21% (822,045,349,768,362.00 Tokens) of SHIBA INU | Token Total Supply: 999,993,870,717,007.82 Token | Total Token Holders: 746,834

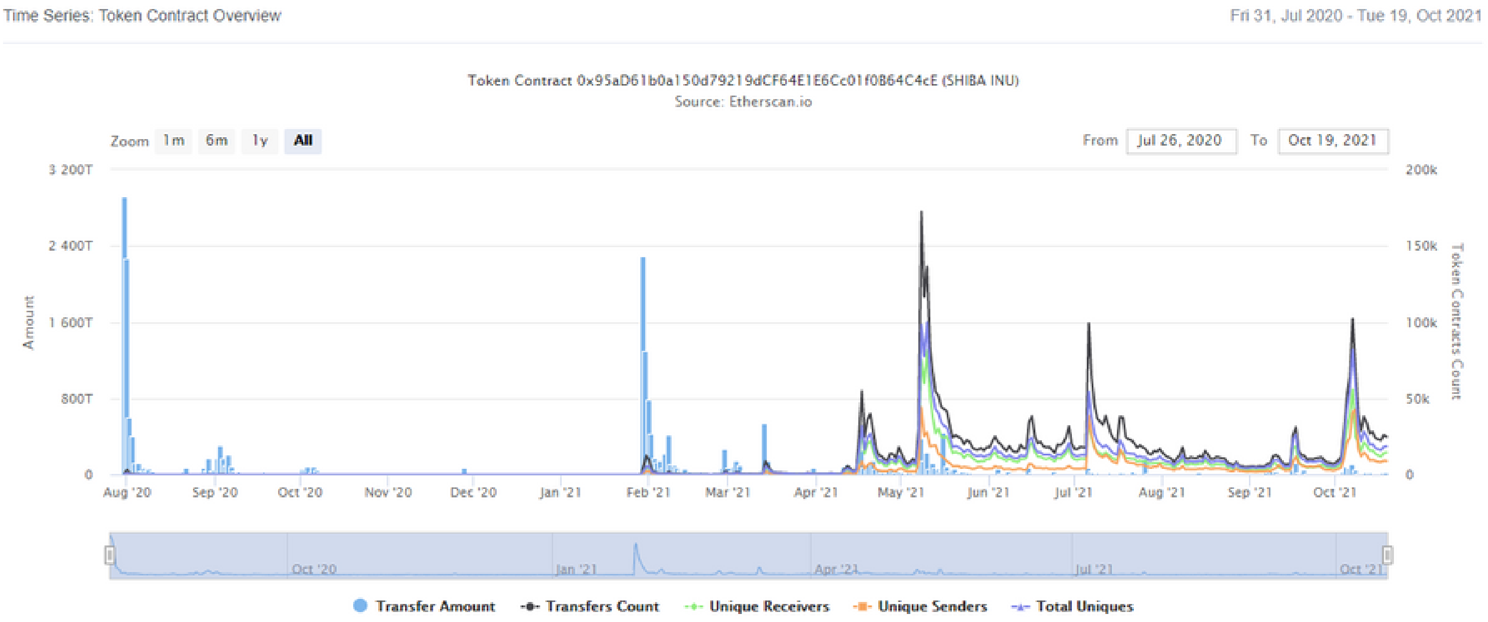
SHIBA INU Top 100 Token Holders

Source: Etherscan.io

OTHER ACCOUNTS
0xdead000000000000000042069420694206942069
(Black Hole: 0xdea...069)
0xef7958ea4421bbb7a27afc4eecc3d7fef00684d4
0x72a53cdbbcc1b9efa39c834a540550e23463aacb
0x2d7af085f2256f114c8a9f540969f0e0ab1c2e5e
0xf977814e90da44bfa03b6295a0616a897441acec (Binance 8)
0x0e5069514a3dd613350bab01b58fd850058e5ca4
0x6262998ced04146fa42253a5c0af90ca02dfd2a3 (Crypto.com)
0xb4a81261b16b92af0b9f7c4a83f1e885132d81e4
(Shiba Inu: xSHIB Token)
0x1406899696adb2fa7a95ea68e80d4f9c82fcdedd

(A total of 822,045,349,768,362.00 tokens held by the top 100 accounts from the total supply of 999,993,870,717,007.82 token)

SHIBASWAP TOKEN CONTRACT INTERACTION DETAILS



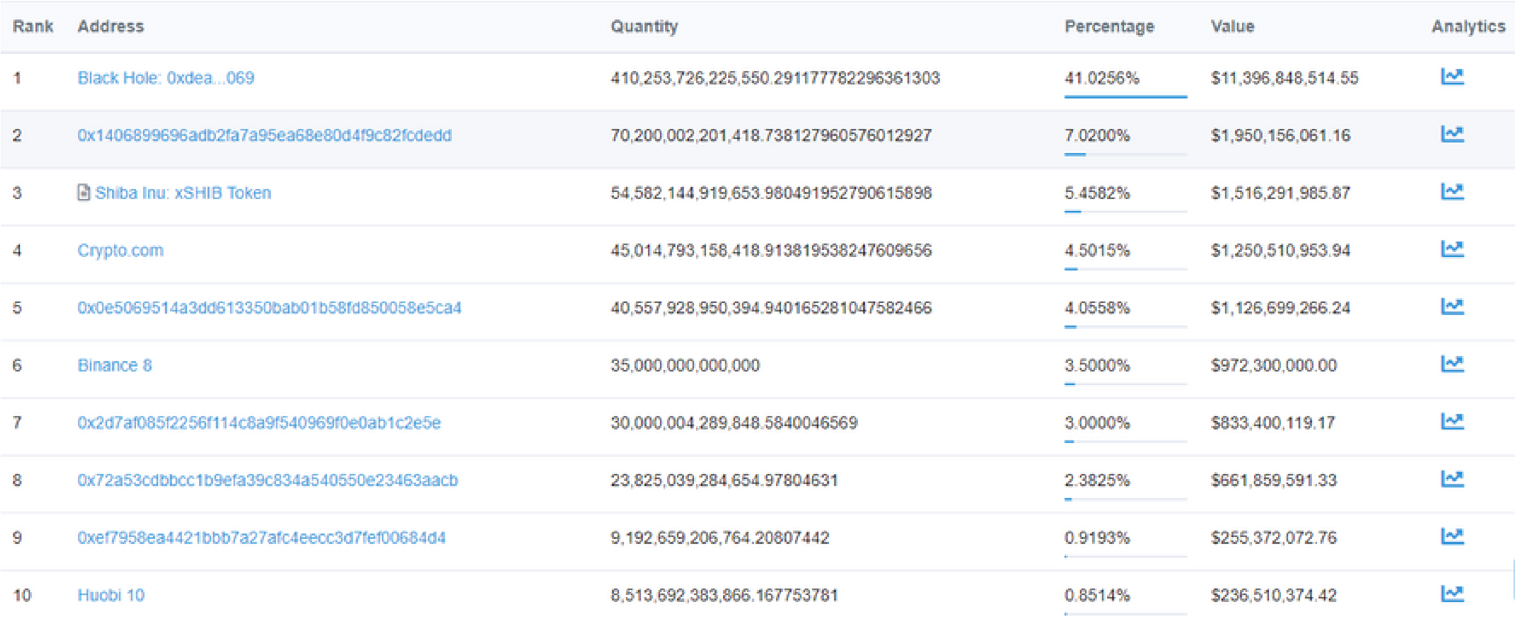
Time Series: Token Contract Overview

Fri 31, Jul 2020 - Tue 19, Oct 2021

Token Contract 0x95aD61b0a150d79219dCF64E1E6Cc01f0B64C4cE (SHIBA INU)

Source: Etherscan.io

TOP 10 TOKEN HOLDERS



Rank	Address	Quantity	Percentage	Value	Analytics
1	Black Hole: 0xdea...069	410,253,726,225,550.291177782296361303	41.0256%	$11,396,848,514.55	📈
2	0x1406899696adb2fa7a95ea68e80d4f9c82fcdedd	70,200,002,201,418.738127960576012927	7.0200%	$1,950,156,061.16	📈
3	Shiba Inu: xSHIB Token	54,582,144,919,653.980491952790615898	5.4582%	$1,516,291,985.87	📈
4	Crypto.com	45,014,793,158,418.913819538247609656	4.5015%	$1,250,510,953.94	📈
5	0x0e5069514a3dd613350bab01b58fd850058e5ca4	40,557,928,950,394.940165281047582466	4.0558%	$1,126,699,266.24	📈
6	Binance 8	35,000,000,000,000	3.5000%	$972,300,000.00	📈
7	0x2d7af085f2256f114c8a9f540969f0e0ab1c2e5e	30,000,004,289,848.5840046569	3.0000%	$833,400,119.17	📈
8	0x72a53cdbbcc1b9efa39c834a540550e23463aacb	23,825,039,284,654.97804631	2.3825%	$661,859,591.33	📈
9	0xef7958ea4421bbb7a27afc4eecc3d7fef00684d4	9,192,659,206,764.20807442	0.9193%	$255,372,072.76	📈
10	Huobi 10	8,513,692,383,866.167753781	0.8514%	$236,510,374.42	📈

source:etherscan.io

SECURITY ASSESMENT

ISSUES CHECKING STATUS

Issue description		Checking status
1.	Compiler errors.	Passed
2.	Race conditions and Reentrancy. Cross-function race conditions.	Passed
3.	Possible delays in data delivery.	Passed
4.	Oracle calls.	Passed
5.	Front running.	Passed
6.	Timestamp dependence.	Passed
7.	Integer Overflow and Underflow.	Passed
8.	DoS with Revert.	Passed
9.	DoS with block gas limit.	Passed
10.	Methods execution permissions.	Passed
11.	Economy model of the contract.	Passed
12.	The impact of the exchange rate on the logic.	Passed
13.	Private user data leaks.	Passed
14.	Malicious Event log.	Passed
15.	Scoping and Declarations.	Passed
16.	Uninitialized storage pointers.	Passed
17.	Arithmetic accuracy.	Passed
18.	Design Logic.	Passed
19.	Cross-function race conditions.	Passed
20.	Safe Open Zeppelin contracts implementation and usage.	Passed
21.	Fallback function security.	Passed

SECURITY ISSUES

✓ High Severity Issues

No high severity issues found.

✓ Medium Severity Issues

No medium severity issues found.

✓ Low Severity Issues

No low severity issues found.

Owner privileges (In the period when the owner is not renounced)

- Issuer can mint any amount of tokens.

- Issuer can burn.

- Owner can edit issuers.

SECURITY ASSESMENT

CONCLUSION

Smart contracts contain owner privileges!

TechRate 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.