



Smart Contract Security Audit Report

SiaCashCoin

September 2022

Security Status



www.hacksafe.io



Audit Details



Audited project

SiaCashCoin



Deployer address

0x08ba1E0E80af2F2A4211f5ccD087631228FA5071



Client contacts

SiaCashCoin Team



Blockchain

Binance Smart Chain



Website

<https://www.siacashcoin.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 TechRate and its affiliates (including holding companies, shareholders, subsidiaries, employees, directors, officers and other representatives) (HackSafe) owe no duty of care towards you or any other person, nor does HackSafe 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 HackSafe 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, HackSafe hereby excludes all liability and responsibility, and neither you nor any other person shall have any claim against HackSafe, 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.

Procedure

Step 1 - In-Depth Manual Review

Manual line-by-line code reviews to ensure the logic behind each function is sound and safe from various attack vectors. This is the most important and lengthy portion of the audit process (as automated tools often cannot find the nuances that lead to exploits such as flash loan attacks).

Step 2 - Automated Testing

Simulation of a variety of interactions with your Smart Contract on a test blockchain leveraging a combination of automated test tools and manual testing to determine if any security vulnerabilities exist.

Step 3 – Leadership Review

The engineers assigned to the audit will schedule meetings with our leadership team to review the contracts, any comments or findings, and ask questions to further apply adversarial thinking to discuss less common attack vectors.

Step 4 - Resolution of Issues

Consulting with the team to provide our recommendations to ensure the code's security and optimize its gas efficiency, if possible. We assist project team's in resolving any outstanding issues or implementing our recommendations.

Step 5 - Published Audit Report

Boiling down results and findings into an easy-to-read report tailored to the project. Our audit reports highlight resolved issues and any risks that exist to the project or its users, along with any remaining suggested remediation measures. Diagrams are included at the end of each report to help users understand the interactions which occur within the project.

Background

HackSafe was commissioned by SiaCashCoin to perform an audit of smart contracts:

- <https://bscscan.com/address/0xc26EaFC627624baDf990f8d30116892eD204DB51#code>

The purpose of the audit was to achieve the

- Ensure that the smart contract functions as intended.
- Identify potential security issues with the smart contract.

The information in this report should be understood 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.

Contract Details

Token contract details for 14.09.2022

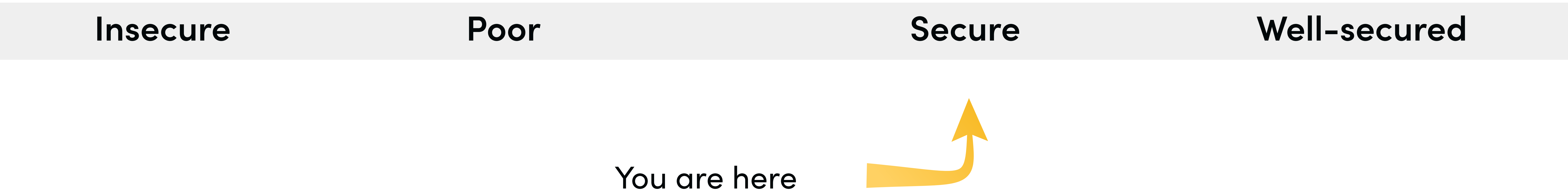
Token Type	: ERC20
Contract name	: CakeToken
Contract address	: 0xc26EaFC627624baDf990f8d30116892eD204DB51
Compiler version	: v0.6.12+commit.27d51765
Total supply	: 25,000,001,721,386,600.188034
Token ticker	: SCC
Decimals	: 18
Token holders	: 16,605
Transactions count	: 23,705
Contract deployer address	: 0x08ba1E0E80af2F2A4211f5ccD087631228FA5071
Owner address	: 0x1080450b1e26df071c613d916055b23e8fcc6fca

Social profiles

Twitter Profile	: https://twitter.com/Siacashcoin
Github profile	: https://github.com/SiaCashCoin
Telegram profile	: https://t.me/SiaCashCoinChat
Coinmarketcap profile	: https://coinmarketcap.com/currencies/siacashcoin/
Coingecko profile	: https://www.coingecko.com/en/coins/siacashcoin/

Audit Summary

According to the standard audit assessment, Customer`s solidity smart contracts are “Secure”. This token contract does contain owner control, which do not make it fully decentralized as owner does have control over smart contract.



We used various tools like Slither, Mythril and Remix IDE. At the same time this finding is based on critical analysis of the manual audit. All issues found during automated analysis were manually reviewed and applicable vulnerabilities are presented in the issues checking status.

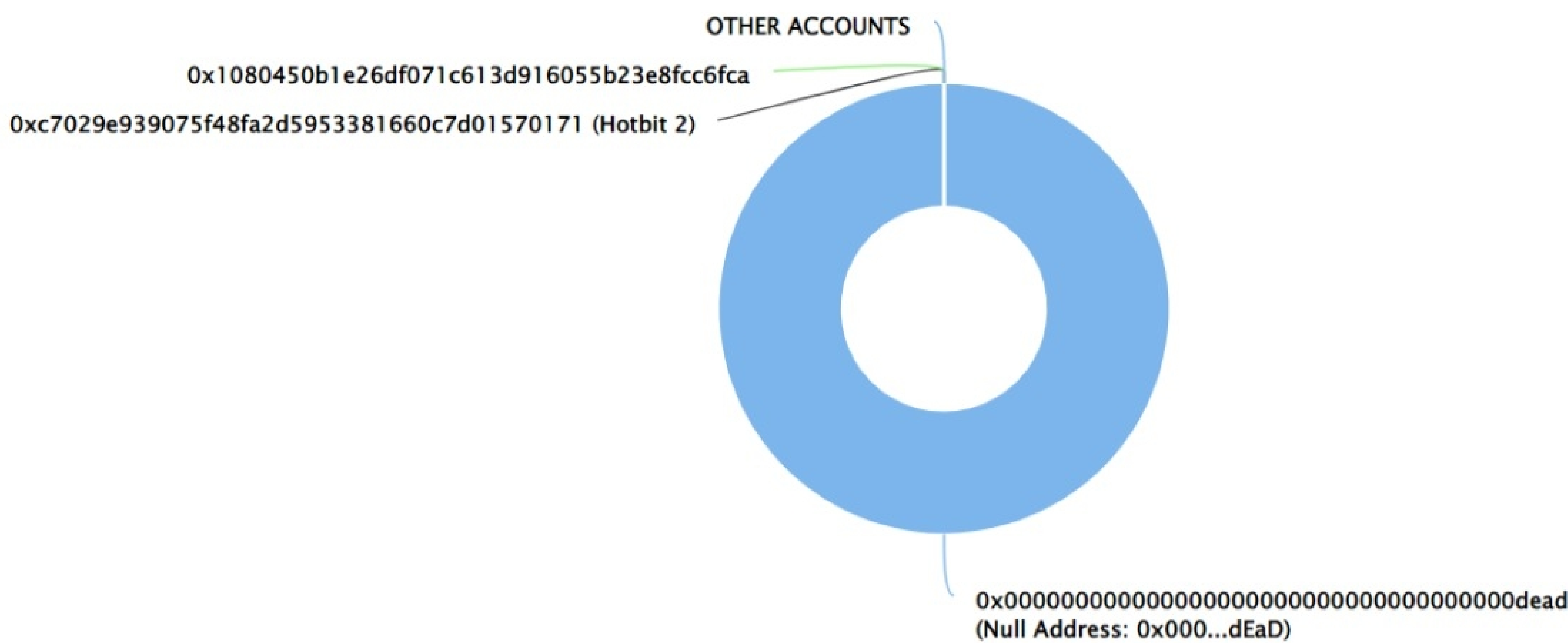
We found 0 critical, 0 high, 0 medium and 1 low and some very low-level issues. These issues are not critical ones.

SiaCashCoin Token Distribution

💡 The top 100 holders collectively own 100.00% (24,999,998,133,377,300.00 Tokens) of SiaCashCoin

💡 Token Total Supply: 25,000,001,721,386,600.19 Token | Total Token Holders: 16,605

SiaCashCoin Top 100 Token Holders
Source: BscScan.com



SiaCashCoin Top 20 Token Holders

(A total of 24,999,998,133,377,300.00 tokens held by the top 100 accounts from the total supply of 25,000,001,721,386,600.19 token)

Rank	Address	Quantity (Token)	Percentage
1	Null Address: 0x000...dEaD	24,999,981,575,390,600.939989686855402587	99.9999%
2	Hotbit 2	5,125,300,257.254210883258408201	0.0000%
3	📄 0x1080450b1e26df071c613d916055b23e8fcc6fca	2,407,011,202.74083588861543546	0.0000%
4	0xf2d2b2ec4a1cd75e26262bebc7c433cb548d040b	1,864,487,249.520335189475536022	0.0000%
5	0xc91795a59f20027848bc785678b53875934792a1	764,351,619	0.0000%
6	📄 0xe63d3fe5e3476f1278e413c2aa5846372ec19df7	742,093,089.139563776185505297	0.0000%
7	0xb8dc7aa9c93ce673230206cd477658641375cf1d	685,873,804.123458805666419717	0.0000%
8	0x0fdd9118cd1b9ddc645f6b466e4de9b36179ed31	400,000,000	0.0000%
9	📄 PancakeSwap V2: Praise-SCC	371,775,086.618294158952713716	0.0000%
10	0x5992e86b4b13c97a112323cf29fb2cc0c2ea1e39	348,890,863.118510496825387124	0.0000%
11	📄 0x35c48cc779337f5be737cd73750137981480ef23	306,927,422.385160594141260981	0.0000%
12	📄 PancakeSwap V2: SCC 54	278,721,172.391909600935029132	0.0000%
13	0xdc1a91a50bb01fda296b4ecb23e5dcb90da46770	218,422,607	0.0000%
14	0x25ba4c7c8746612fb0592b665b568e8aab4de2c2	163,182,926	0.0000%
15	0x5881d32d199e462272bcc3a526d1d978d3d6df2b	141,661,675.95073306	0.0000%
16	0xe7898798b26154365e856d70032d657b304eca49	111,043,536.628770178133881693	0.0000%
17	0xf2e72b89630f0ae57572c08fb2b978c8277541c0	110,451,030.368292301456312019	0.0000%
18	0x008a72b2b0c68cee140ad28001a282e9c62c4824	107,904,261.36911099	0.0000%
19	0xad09074e10964ba7dbc26098c81b35f3c28b2273	100,000,000	0.0000%
20	0x4bbf6ac9a5b37dc6ae32237a737c9b82978cca67	100,000,000	0.0000%

Contract functions details

+ Context

- [Int] _msgSender
- [Int] _msgData

+ Ownable (Context)

- [Int] <constructor>
- [Pub] owner
- [Pub] renounceOwnership #
-modifiers: onlyOwner
- [Pub] transferOwnership #
-modifiers: onlyOwner
- [Int] _transferOwnership

+[Int] IBEP20

- [Ext] totalSupply
- [Ext] decimals
- [Ext] symbol
- [Ext] name
- [Ext] getOwner
- [Ext] balanceOf
- [Ext] transfer
- [Ext] allowance
- [Ext] approve
- [Ext] transferFrom

+[Lib] SafeMath

- [Int] add
- [Int] sub
- [Int] sub
- [Int] mul
- [Int] div
- [Int] div
- [Int] mod
- [Int] mod
- [Int] min
- [Int] sqrt

+[Lib] Address

- [Int] isContract
- [Int] sendValue

Contract functions details

- [Int] functionCall
- [Int] functionCall
- [Int] functionCallWithValue
- [Int] functionCallWithValue
- [Pvt] _functionCallWithValue

+ BEP20 (Context, IBEP20, Ownable)

- [Pub] <constructor>
- [Ext] getOwner
- [Pub] name
- [Pub] decimals
- [Pub] symbol
- [Pub] totalSupply
- [Pub] balanceOf
- [Pub] transfer #
- [Pub] allowance
- [Pub] approve #
- [Pub] transferFrom #
- [Pub] increaseAllowance
- [Pub] decreaseAllowance
- [Pub] mint #
 - modifiers: onlyOwner
- [Int] _transfer #
- [Int] _mint#
- [Int] _burn #
- [Int] _approve #
- [Int] _burnFrom #

+ CakeToken (BEP20)

- [Pub] mint #
 - modifiers: onlyOwner
- [Ext] delegates
- [Ext] delegate
- [Ext] delegateBySig
- [Ext] getCurrentVotes
- [Ext] getPriorVotes
- [Int] _delegate
- [Int] _moveDelegates
- [Int] _writeCheckpoint

Contract functions details

`-[Int]` safe32

`-[Int]` getChainId

`($)` = payable function

`#` = non-constant function

Issues Checking Status

No.	Title	Status
1.	Unlocked Compiler Version	Passed
2.	Missing Input Validation	Passed
3.	Race conditions and Reentrancy. Cross-function race conditions.	Passed
4.	Possible delays in data delivery	Passed
5.	Oracle calls.	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.	Private use data leaks.	Passed
13.	Malicious Event log.	Passed
14.	Scoping and Declarations.	Passed
15.	Uninitialized storage pointers.	Passed
16.	Arithmetic accuracy.	Passed
17.	Design Logic.	Passed
18.	Safe Open Zeppelin contracts implementation and usage.	Passed
19.	Incorrect Naming State Variable	Passed
20.	Too old version	Low issue

Severity Definitions

Risk Level	Description
Critical	Critical vulnerabilities are usually straightforward to exploit and can lead to assets loss or data manipulations.
High	High-level vulnerabilities are difficult to exploit; however, they also have a significant impact on smart contract execution, e.g., public access to crucial functions
Medium	Medium-level vulnerabilities are important to fix; however, they can't lead to assets loss or data manipulations.
Low	Low-level vulnerabilities are mostly related to outdated, unused, etc. code snippets that can't have a significant impact on execution.

Security Issues

✔ Critical Severity Issues

No critical severity issue found.

✔ High Severity Issues

No high severity issue found.

✔ Medium Severity Issues

No medium severity issues found.

✔ Low Severity Issues

One low severity issue found.

1. Too old compiler version.

- **Description**

Contract has been deployed using too old compiler version.

- **Recommendation**

It is advisable that the compiler version of solidity should be among the new compiler versions.

Centralization

Owner Privileges :

- SiaCashCoin Contract:
 - Owner can renounce and transfer ownership.
 - Owner can mint new tokens.

This smart contract has some functions which can be executed by the Admin (Owner) only. If the admin wallet private key would be compromised, then it would create trouble as smart contract ownership has not been renounced. Following are Admin functions functions:

- Transferownership
- Renounceownership
- Mint
- Burn
- Setmanager

Conclusion

Smart contract contains low severity issues! The further transfer and operations with the fund raised are not related to this particular contract.

HackSafe 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.