HackSafe

Smart Contract Security Audit Report

Smart Block Chain City

May **2022**

Security Status

★ ★ ★ ★ ★

www.hacksafe.io

Audit Details

Audited project
Smart Block Chain City

Deployer address
0xE96500f62baBE78B3C2529337dB107Dd0cf13A30

Client contacts
Smart Block Chain City team

Blockchain
Binance Smart Chain

Website
https://www.sbcc.world/

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.

Background

HackSafe was commissioned by Smart Block Chain City to perform an audit of smart contract:

- https://bscscan.com/address/0x6e02Be885FcA1138038420fDdD4B41C59a8Cea6D#code

Contract Details

Token contract details for 16.05.2022

Contract name	: SBCC
Contract address	: 0x6e02Be885FcA1138038420fDdD4B41C59a8Cea6D
Total supply	: 3 billion
Token Ticker	: SBCC
Network	: BSCScan
Decimals	: 18
Token Holders	: 10,082 addresses
Transactions count	: 10,975
Contract deployer address	: 0xE96500f62baBE78B3C2529337dB107Dd0cf13A30

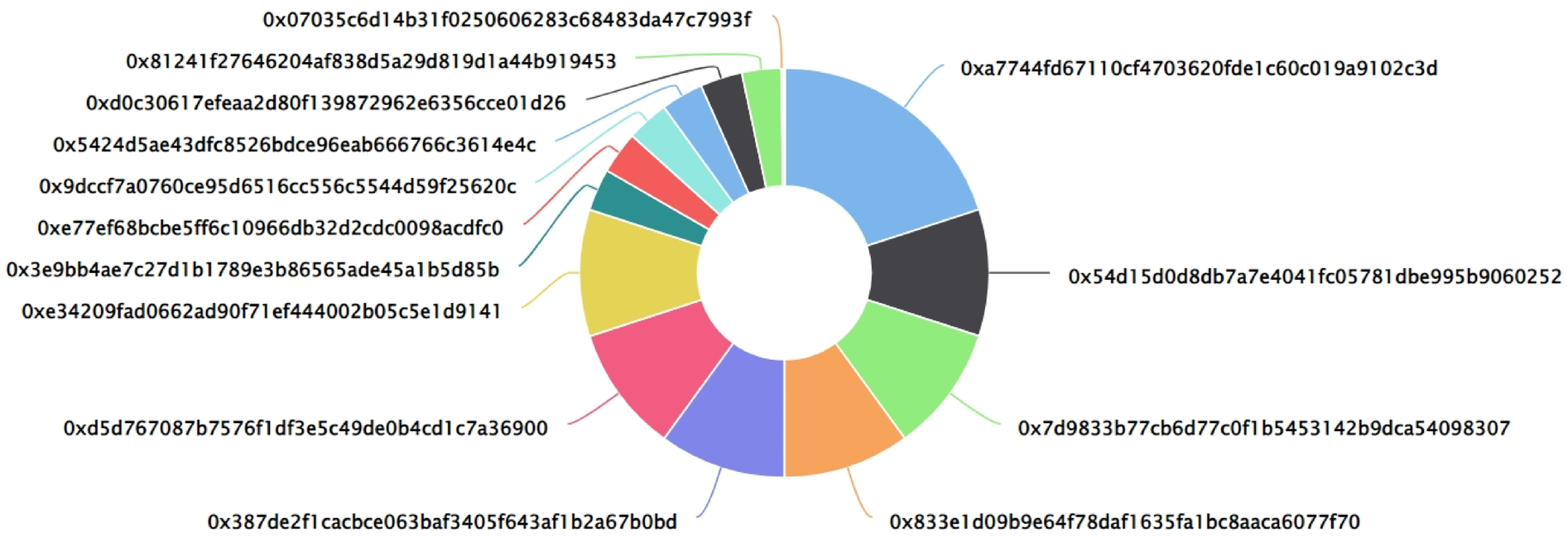
Smart Block Chain City Token Distribution

The top 500 holders collectively own 100.00% (2,999,997,147.21 Tokens) of Smart Block Chain City

Token Total Supply: 3,000,000,000.00 Token | Total Token Holders: 10,082

Smart Block Chain City Top 500 Token Holders

Source: BscScan.com



Smart Block Chain City Top 20 Token Holders

(A total of 2,999,997,147.21 tokens held by the top 500 accounts from the total supply of 3,000,000,000.00 token)

Rank	Address	Quantity (Token)	Percentage
1	0xa7744fd67110cf4703620fde1c60c019a9102c3d	600,000,000	20.0000%
2	0x54d15d0d8db7a7e4041fc05781dbe995b9060252	300,000,000	10.0000%
3	0x7d9833b77cb6d77c0f1b5453142b9dca54098307	300,000,000	10.0000%
4	0x833e1d09b9e64f78daf1635fa1bc8aaca6077f70	300,000,000	10.0000%
5	0x387de2f1cacbce063baf3405f643af1b2a67b0bd	300,000,000	10.0000%
6	0xd5d767087b7576f1df3e5c49de0b4cd1c7a36900	300,000,000	10.0000%
7	0xe34209fad0662ad90f71ef444002b05c5e1d9141	300,000,000	10.0000%
8	0x3e9bb4ae7c27d1b1789e3b86565ade45a1b5d85b	100,000,000	3.3333%
9	0xe77ef68bcbe5ff6c10966db32d2cdc0098acdfc0	100,000,000	3.3333%
10	0x9dccf7a0760ce95d6516cc556c5544d59f25620c	100,000,000	3.3333%
11	0x5424d5ae43dfc8526bdce96eab666766c3614e4c	100,000,000	3.3333%
12	0xd0c30617efeaa2d80f139872962e6356cce01d26	100,000,000	3.3333%
13	0x81241f27646204af838d5a29d819d1a44b919453	92,564,600	3.0855%
14	0x07035c6d14b31f0250606283c68483da47c7993f	2,000,000	0.0667%
15	0x78abbb343694f0f372fbe920638eb6020bff5897	1,000,000	0.0333%
16	0x4c71e0d30b942eccb7aa7f0e63cb40b661217c82	1,000,000	0.0333%
17	0xd85a59d6ebf0a3a9b310fc05f9dc181151fbe81c	1,000,000	0.0333%
18	0x7c563820eee4172d41433a244b61823df566f77b	520,000	0.0173%
19	0xf297585ffa340aa2b3478adb6201b7345f0eeee6	500,000	0.0167%
20	0xfe4d976e574a3199c962c5d0f72d3db11359591e	220,000	0.0073%

Contract functions details

+ Context
    -[Int]_msgsender
    -[Int] _msgdata

+ [Int] IERC20
    -[Ext]totalSupply
    -[Ext]balanceOf
    -[Ext]transfer#
    -[Ext]allowance
    -[Ext]approve#
    -[Ext]transferFrom#

+ [Int] IERC20Metadata (IERC20)
    -[Ext] name
    -[Ext] symbol
    -[Ext] decimals

+ERC20 (Context, IERC20, IERC20Metadata)
    <Constructor>#
    -[Pub] name
    -[Pub] symbol
    -[Pub] decimals
    -[Pub] totalSupply
    -[Pub] balanceOf
    -[Pub] transfer#
    -[Pub] allowance
    -[pub] approve#
    -[Pub] transferFrom#
    -[Pub] increaseAllowance#
    -[Pub] decreaseAllowance#
    -[Int] _transfer#
    -[Int] _mint#
    -[Int] _burn#
    -[Int] _approve#
    -[Int] _spendAllowance#
    -[Int] _beforeTokenTransfer
    -[Int] _afterTokenTransfer

+ SBCC (ERC20)
    <constructor>#

Issues Checking Status

No.	Title	Status
1.	Unlocked Compiler Version	Low issue
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

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 issues found.

1. Unlocked Compiler Version.

- **Description**

  The contract utilizes an unlocked compiler version. An unlocked compiler version in the contract's source code permits the user to compile it at or above a particular version. This, in turn, leads to differences in the generated bytecode between compilations due to differing compiler version numbers. This can lead to ambiguity when debugging as compiler-specific bugs may occur in the codebase that would be difficult to identify over a span of multiple compiler versions rather than a specific one.

- **Recommendation**

  We advise to use only one compiler version instead multi pragma which is alternatively locked at the lowest version possible so that the contract can be compiled. Use following line instead of pragma solidity ^0.8.0;

  pragma solidity 0.8.0;

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.