HackSafe

Smart Contract Security Audit Report

BrickToken

August 2022

Security Status

★ ★ ★ ★ ★

www.hacksafe.io

Audit Details

Audited project
BrickToken

Deployer address
0x99aC326f0678FD915A484b964b07368E7a215c53

Client contacts
Brick team

Blockchain
Binance Smart Chain

Website
https://bricksestate.co/

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 Brick to perform an audit of smart contracts:

- https://bscscan.com/address/0x4e5ab517719a2bdbafefc22c712d7b5bc5f5544e#code

The purpose of the audit was to achieve the

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

The information in this report should be understand the risk exposure of the smart contract, and as a guide to improve the security posture of the smart contract by remediating the

Contract Details

Token contract details for 01.08.2022

Token Type	: BEP-20
Contract name	: BRICKToken
Contract address	: 0x4e5aB517719a2BDbafEFC22C712d7b5BC5F5544E
Compiler version	: v0.7.6+commit.7338295f
Total supply	: 1,000,000
Token Ticker	: BRICK
Decimals	: 18
Token Holders	: 392
Top 100 token holder's	: 99.92 %
Transactions count	: 6,582
Contract deployer address	: 0x99aC326f0678FD915A484b964b07368E7a215c53
Owner address	: 0x99aC326f0678FD915A484b964b07368E7a215c53

Social profiles

Twitter Profile	: https://twitter.com/bricks_estate
Telegram Profile	: https://t.me/bricksestate
LinkedIN Profile	: https://www.linkedin.com/company/bricks-estate/
Coinmarketcap profile	: https://coinmarketcap.com/currencies/brick-token/
Coingecko profile	: https://www.coingecko.com/en/coins/brick-token/

Audit Summary

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

Insecure	Poor	Secure	Well-secured

You are here 

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

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

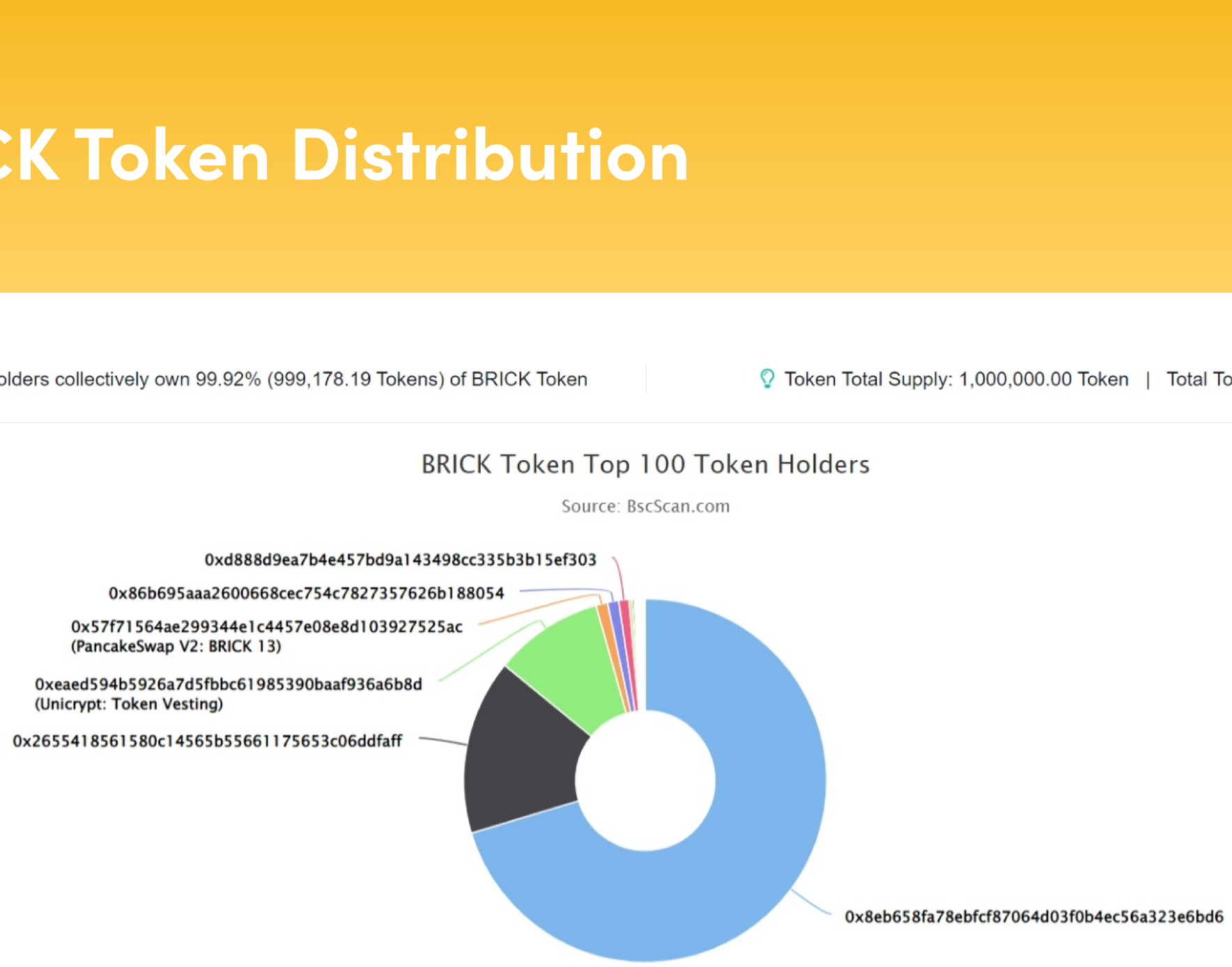
BRICK Token Distribution

The top 100 holders collectively own 99.92% (999,178.19 Tokens) of BRICK Token

Token Total Supply: 1,000,000.00 Token | Total Token Holders: 392

BRICK Token Top 100 Token Holders

Source: BscScan.com



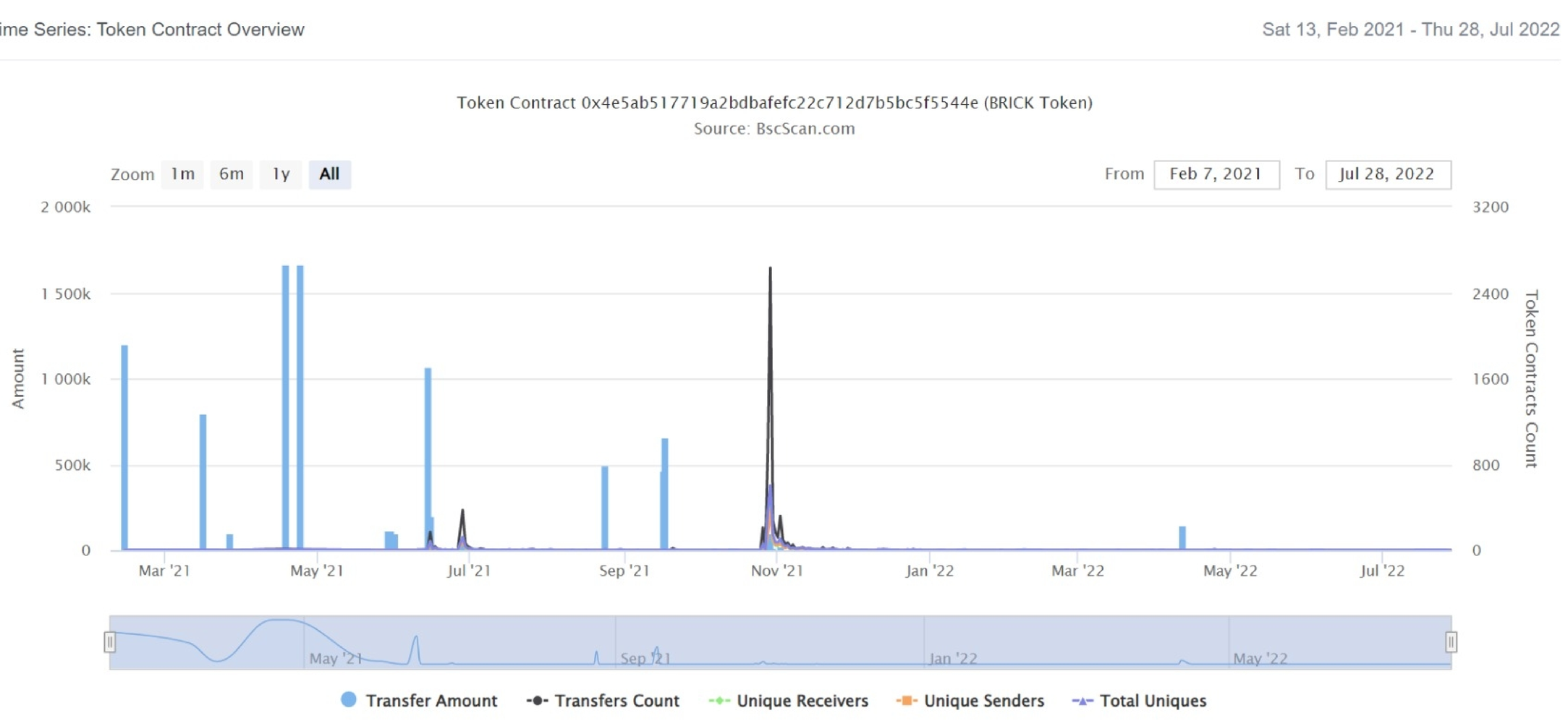
BRICK Top 20 Token Holders

(A total of 999,178.19 tokens held by the top 100 accounts from the total supply of 1,000,000.00 token)

Rank	Address	Quantity (Token)	Percentage
1	0x8eb658fa78ebfcf87064d03f0b4ec56a323e6bd6	703,376.457177840359903521	70.3376%
2	0x2655418561580c14565b55661175653c06ddfaff	155,811.908651168501357709	15.5812%
3	Unicrypt: Token Vesting	97,150	9.7150%
4	PancakeSwap V2: BRICK 13	10,287.058506890579310731	1.0287%
5	0x86b695aaa2600668cec754c7827357626b188054	10,000	1.0000%
6	0xd888d9ea7b4e457bd9a143498cc335b3b15ef303	9,000	0.9000%
7	0xf676565f7102a73c5e6c5058ad93b2330359321d	2,617.545011712538941956	0.2618%
8	0x51f150d83c65e56f34b399e38123e19d28e1153c	2,000	0.2000%
9	0xaa3d85ad9d128dfecb55424085754f6dfa643eb1	1,400	0.1400%
10	0xbaffd1164525ef9df529bc59a052e645a0645f6b	990	0.0990%
11	0xcd5060874116d9169ebf790ff207a11888de126a	505.3755	0.0505%
12	0x7ce7b99448308608e128fc61137962836d26b568	499.665505740328807528	0.0500%
13	0xb2a263943c31693ae5ad6a1409a66e78fc2ad68a	338.818093438530388201	0.0339%
14	0xa89992e24a345fd2b8aef8c93159fb25217a911a	315.640876863661468155	0.0316%
15	0x6798b3fad0b9e2e9539edad47f34f52e8e615af4	279.324191701879281631	0.0279%
16	0xd3eb88b203e1a952ad59b90fd35fcdd85b53ce0c	224.33009063081228192	0.0224%
17	0x45ab19a4b453524b3e32b7c4308fbed034de3b0a	219.876986266540188335	0.0220%
18	0xc582707c0799cea4f5122ab8ddc9d8e80d24d0e8	200	0.0200%
19	0x37d36c3a296afa824abe8133ffa1b972e19e7f44	174.153150713916670981	0.0174%
20	0xac150e9fc993d757a3bd48a81a8be95ee245347c	172.175191885922291192	0.0172%

BRICK Token Distribution

BRICK Contract Overview



Contract functions details

+ [Int] IBEP20
    -[Ext] totalSupply
    -[Ext] decimals
    -[Ext] symbol
    -[Ext] name
    -[Ext] getOwner
    -[Ext] balanceOf
    -[Ext] transfer
    -[Ext] allowance
    -[Ext] approve
    -[Ext] transferFrom

+ Context
    -[Int] _msgSender
    -[Int] _msgData

+ [Lib] SafeMath
    -[Int] add
    -[Int] sub
    -[Int] sub
    -[Int] mul
    -[Int] div
    -[Int] div
    -[Int] mod
    -[Int] mod

+ Ownable (Context)
    -<constructor>
    -[Pub] owner
    -[Int] _checkOwner
    -[Pub] renounceOwnership #
      -modifiers: onlyOwner
    -[Pub] transferOwnership
      -modifiers: onlyOwner
    -[Int] _transferOwnership #

+ BRICKToken (Context, IBEP20, Ownable)
    -<constructor> #
    -[Ext] getOwner
    -[Ext] decimals

Contract functions details

-[Ext] symbol
-[Ext] name
-[Ext] totalSupply
-[Ext] balanceOf
-[Ext] transfer #
-[Ext] allowance
-[Ext] approve #
-[Ext] transferFrom #
-[Pub] increaseAllowance
-[Pub] decreaseAllowance
-[Int] _transfer #
-[Int] _approve #

($) = 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	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

No low severity issue found.

Centralization

Owner privileges:

- BRICK Contract:
    - Owner can remove and transfer ownership.

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:

- Transferownership
- Renounceownership

Conclusion

Smart contract contains no 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.