Smart Contract Security Audit

Audit details:

Audited project:	BoomCoin
Deployer address:	0x6a6AD7876D99A995e7f74ec5D494E16aB86f3AF9
Client contacts:	BoomCoin team
Blockchain:	Binance Smart Chain
Project website:	Not provided by the BoomCoin team

May, 2021
TechRate

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) (TechRate) owe no duty of care towards you or any other person, nor does TechRate 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 TechRate 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, TechRate hereby excludes all liability and responsibility, and neither you nor any other person shall have any claim against TechRate, 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

TechRate was commissioned by BoomCoin to perform an audit of smart contracts:

- *https://bscscan.com/address/0x761684e229f04ce8985b49e3beb1cd994c776a21#code*

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.

Contracts details

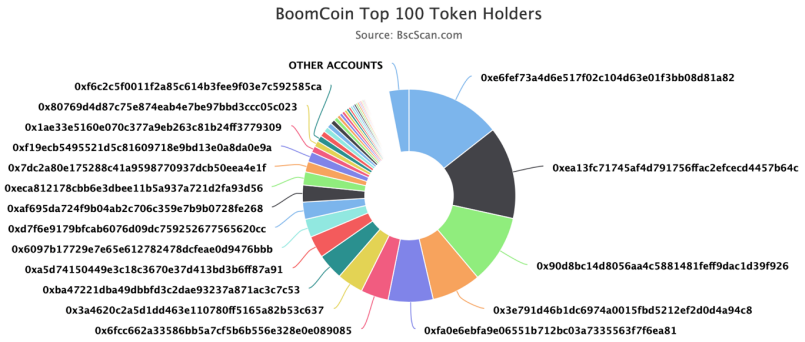
Token contract details for 22.05.2021.

Contract name:	FNX
Contract address:	0x761684e229f04ce8985b49e3BEB1CD994C776A21
Total supply:	250_000_000_000_000_000_000_000_000
Token ticker:	BOOMC
Decimals:	18
Token holders:	569
Transactions count:	2,419
Top 100 holders dominance:	96.95%
Contract deployer address:	0x6a6AD7876D99A995e7f74ec5D494E16aB86f3AF9
Contract's current owner address:	0xa5d74150449e3c18c3670e37d413bd3b6ff87a91

BoomCoin token distribution

The top 100 holders collectively own 96.95% (242,365,242.45 Tokens) of BoomCoin

Token Total Supply: 250,000,000.00 Token | Total Token Holders: 569

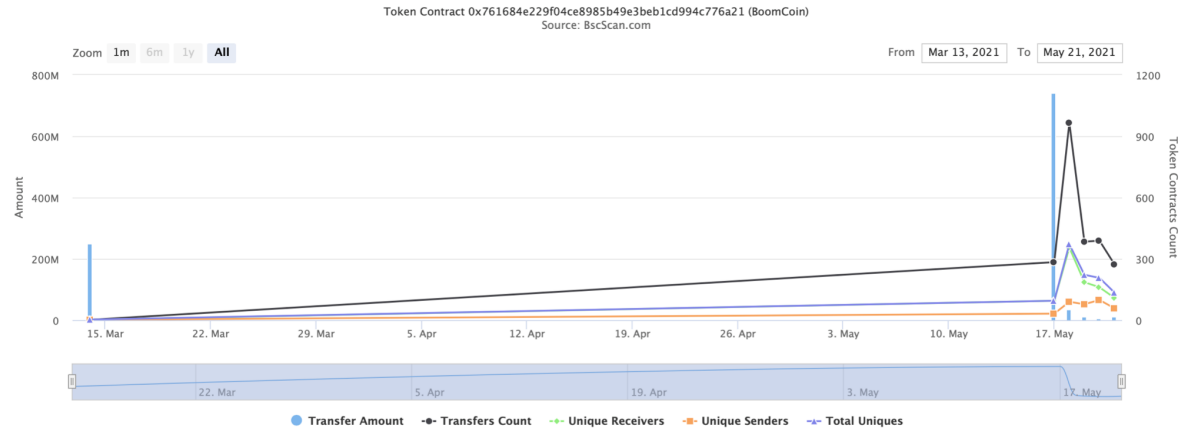


(A total of 242,365,242.45 tokens held by the top 100 accounts from the total supply of 250,000,000.00 token)

BoomCoin contract interaction details

Time Series: Token Contract Overview

Sun 14, Mar 2021 - Fri 21, May 2021



BoomCoin top 10 token holders

Rank	Address	Quantity (Token)	Percentage
1	0xe6fef73a4d6e517f02c104d63e01f3bb08d81a82	36,007,997.389753371532261154	14.4032%
2	0xea13fc71745af4d791756ffac2efcecd4457b64c	35,117,024.189389986775455616	14.0468%
3	0x90d8bc14d8056aa4c5881481feff9dac1d39f926	26,105,628.674447405809144407	10.4423%
4	0x3e791d46b1dc6974a0015fbd5212ef2d0d4a94c8	18,659,822.632970459503631041	7.4639%
5	0xfa0e6ebfa9e06551b712bc03a7335563f7f6ea81	17,044,834.258901401637394885	6.8179%
6	0x6fcc662a33586bb5a7cf5b6b556e328e0e089085	10,506,255.585494912959382266	4.2025%
7	0x3a4620c2a5d1dd463e110780ff5165a82b53c637	9,938,633.300764847125412591	3.9755%
8	0xba47221dba49dbbfd3c2dae93237a871ac3c7c53	9,905,105.525763078999565797	3.9620%
9	0xa5d74150449e3c18c3670e37d413bd3b6ff87a91	8,351,565.66764818666659925	3.3406%
10	0x6097b17729e7e65e612782478dcfeae0d9476bbb	6,936,204.53892750208609434	2.7745%

Contract functions details

+ SafeMath
  - [Pub] safeAdd
  - [Pub] safeSub

- [Pub] safeMul
- [Pub] safeDiv

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

+ ApproveAndCallFallBack
- [Pub] receiveApproval #

+ Owned
- [Pub] <Constructor> #
- [Pub] transferOwnership #
  - modifiers: onlyOwner
- [Pub] acceptOwnership #

+ BoomCoin (IERC20, Owned, SafeMath)
- [Pub] <Constructor> #
- [Pub] totalSupply
- [Pub] balanceOf
- [Pub] transfer #
- [Pub] approve #
- [Pub] transferFrom #
- [Pub] allowance
- [Pub] approveAndCall #
- [Ext] <Fallback> ($)
- [Pub] transferAnyERC20Token #
  - modifiers: onlyOwner

($) = payable function
= non-constant function

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)

- ❏ Owner can transfer tokens from contract to any address

```
// ------------------------------------------------------------------------
// Owner can transfer out any accidentally sent ERC20 tokens
// ------------------------------------------------------------------------
function transferAnyERC20Token(address tokenAddress, uint tokens) public onlyOwner returns (bool success) {
    return IERC20(tokenAddress).transfer(owner, tokens);
}
```

Recommendation

- ❏ In transferFrom(address from,...) and transfer(address to,...) functions check that to address is not contract address

```
require(to != address(this));
```

Conclusion

Smart contracts do not contain high severity issues.

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.