



TechRate
AUDIT COMPANY

Smart Contract Security Audit

TechRate

July, 2021

Audit Details



Audited project

Rocket Boys



Deployer address

0x17ab01bCFEc60813F4bba9E2382D554B62D67df2



Client contacts:

Rocket Boys team



Blockchain

Binance Smart Chain



Project website:

<https://rocketboys.io/>

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 Rocket Boys to perform an audit of smart contracts:

<https://bscscan.com/address/0x071fa11f7516cdeb366f7f7d91da5049f7086185#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 17.07.2021

Contract name	Rocket Boys
Contract address	0x071Fa11f7516CDeb366F7f7d91DA5049F7086185
Total supply	1,000,000,000,000,000
Token ticker	RBOYS
Decimals	9
Token holders	6,564
Transactions count	67,500
Top 100 holders dominance	61.26%
Launched at	9157708
Auto liquidity receiver	0xcefdffd1e9a4cd44f07d2d95a30dedd9fbdfdf2
Marketing fee receiver	0xcefdffd1e9a4cd44f07d2d95a30dedd9fbdfdf2
Pair	0x7c03aecf410b24daf4bd90c75af24a08a6cdac07
Contract deployer address	0x17ab01bCFEc60813F4bba9E2382D554B62D67df2
Contract's current owner address	0x17ab01bcfec60813f4bba9e2382d554b62d67df2

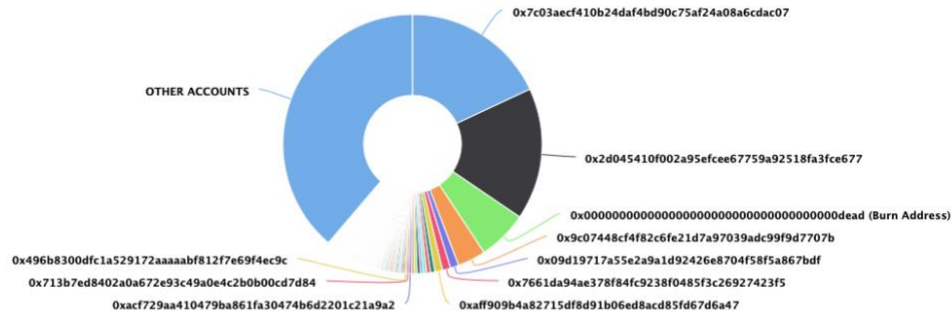
BASE3 Token Distribution

💡 The top 100 holders collectively own 61.26% (612,574,545,696,100.00 Tokens) of Rocket Boys

💡 Token Total Supply: 1,000,000,000,000.00 Token | Total Token Holders: 6,564

Rocket Boys Top 100 Token Holders

Source: BscScan.com



(A total of 612,574,545,696,100.00 tokens held by the top 100 accounts from the total supply of 1,000,000,000,000,000.00 token)

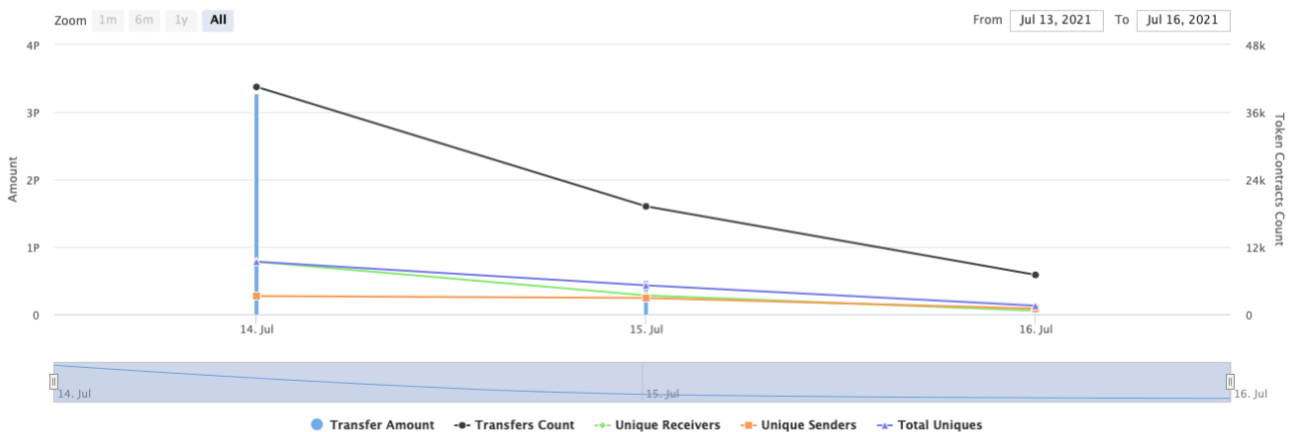
BASE3 Contract Interaction Details

Time Series: Token Contract Overview



Wed 14, Jul 2021 - Fri 16, Jul 2021

Token Contract 0x071fa11f7516cdeb366f7f7d91da5049f7086185 (Rocket Boys)

Source: BscScan.com



BASE3 Top 10 Token Holders

Rank	Address	Quantity (Token)	Percentage
1	 0x7c03aecf410b24daf4bd90c75af24a08a6cdac07	180,490,264,769,340.361793562	18.0490%
2	 0x2d045410f002a95efcee67759a92518fa3fce677	164,500,000,000,000.005	16.4500%
3	Burn Address	62,116,788,245,660.931815727	6.2117%
4	0x9c07448cf4f82c6fe21d7a97039adc99f9d7707b	35,000,000,000,000	3.5000%
5	0x09d19717a55e2a9a1d92426e8704f58f5a867bdf	10,499,999,999,999.995	1.0500%
6	0x7661da94ae378f84fc9238f0485f3c26927423f5	10,262,419,830,614.18613508	1.0262%
7	0xaf909b4a82715df8d91b06ed8acd85fd67d6a47	9,457,110,960,000	0.9457%
8	0x054b905ca86e9a2520b4239f716c9a26db8e545c	5,533,221,702,836.284903893	0.5533%
9	0x6e7d956899ddcd7c2e85a54ebdf02b1cfedc4f	4,631,684,924,406.328458437	0.4632%
10	0x2481a7b31a4ad939d26651bf43dac55bc9c3af82	4,313,514,082,331.015524615	0.4314%



Contract functions details

+ [Lib] SafeMath

- [Int] add
- [Int] sub
- [Int] sub
- [Int] mul
- [Int] div
- [Int] div

+ [Int] IBEP20

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

+ Auth

- [Pub] <Constructor> #
- [Pub] authorize #
 - modifiers: onlyOwner
- [Pub] unauthorize #
 - modifiers: onlyOwner
- [Pub] isOwner
- [Pub] isAuthorized
- [Pub] transferOwnership #
 - modifiers: onlyOwner

+ [Int] IDEXFactory

- [Ext] createPair #

+ [Int] IDEXRouter

- [Ext] factory
- [Ext] WETH
- [Ext] addLiquidity #
- [Ext] addLiquidityETH (\$)
- [Ext] swapExactTokensForTokensSupportingFeeOnTransferTokens #
- [Ext] swapExactETHForTokensSupportingFeeOnTransferTokens (\$)
- [Ext] swapExactTokensForETHSupportingFeeOnTransferTokens #

+ [Int] IDividendDistributor

- [Ext] setDistributionCriteria #
- [Ext] setShare #
- [Ext] deposit (\$)
- [Ext] process #

+ DividendDistributor (IDividendDistributor)

- [Pub] <Constructor> #

- [Ext] getShareholderInfo
 - [Ext] setDistributionCriteria #
 - modifiers: onlyToken
 - [Ext] setShare #
 - modifiers: onlyToken
 - [Ext] deposit (\$)
 - [Ext] process #
 - modifiers: onlyToken
 - [Int] shouldDistribute
 - [Int] distributeDividend #
 - [Ext] claimDividend #
 - [Ext] claimDividendFor #
 - [Pub] getUnpaidEarnings
 - [Int] getCumulativeDividends
 - [Int] addShareholder #
 - [Int] removeShareholder #
- + RocketBoys (IBEP20, Auth)
- [Pub] <Constructor> #
 - modifiers: Auth
 - [Ext] <Fallback> (\$)
 - [Ext] totalSupply
 - [Ext] decimals
 - [Ext] symbol
 - [Ext] name
 - [Ext] getOwner
 - [Pub] balanceOf
 - [Ext] allowance
 - [Pub] approve #
 - [Ext] approveMax #
 - [Ext] transfer #
 - [Ext] transferFrom #
 - [Int] _transferFrom #
 - [Int] _basicTransfer #
 - [Int] checkLaunched
 - [Int] checkTxLimit
 - [Int] shouldTakeFee
 - [Pub] getTotalFee
 - [Int] takeFee #
 - [Int] shouldSwapBack
 - [Int] swapBack #
 - modifiers: swapping
 - [Int] shouldAutoBuyback
 - [Ext] buybackWEI #
 - modifiers: authorized
 - [Ext] buybackBNB #
 - modifiers: authorized
 - [Int] _buyback #
 - [Int] triggerAutoBuyback #
 - [Int] buyTokens #
 - modifiers: swapping
 - [Ext] setAutoBuybackSettings #
 - modifiers: authorized
 - [Int] launched
 - [Int] launch #

- [Ext] setTxLimit #
 - modifiers: authorized
- [Ext] setDividendExempt #
 - modifiers: authorized
- [Ext] setFeeExempt #
 - modifiers: authorized
- [Ext] setTxLimitExempt #
 - modifiers: authorized
- [Ext] setFees #
 - modifiers: authorized
- [Ext] setFeeReceivers #
 - modifiers: authorized
- [Ext] setSwapBackSettings #
 - modifiers: authorized
- [Ext] setAutoLiquifyEnabled #
 - modifiers: authorized
- [Ext] setDistributionCriteria #
 - modifiers: authorized
- [Ext] setDistributorSettings #
 - modifiers: authorized
- [Ext] getAccumulatedFees
- [Ext] getAutoBuybackSettings
- [Ext] getAutoLiquifySettings
- [Ext] getSwapBackSettings
- [Ext] getFees

(\$) = 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 change auto buyback settings.
- Owner can change the maximum transaction amount.
- Owner can include in and exclude from dividends.
- Owner can include in and exclude from fee and transaction amount.
- Owner can change fees.
- Owner can change fee receivers.
- Owner can change swap threshold and disable/enable swap.
- Owner can change autoLiquidity status.
- Owner can change distribution criteria.
- Owner can change distribution GAS.
- Owner can buyback WEI and BNB.

Conclusion

Smart contracts do not contain high severity issues! Liquidity pair contract's security is not checked due to out of scope.

Liquidity locking details provided by the team:

https://dxsale.app/app/v2_9/dxlockview?id=0&add=0x21ca73c28e359a4d57c763715d2f9e7e8446ead4&type=lplock&chain=BSC

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.