



TechRate
AUDIT COMPANY

Smart Contract Security Audit

Audit Details



Audited project
Flokinomics



Deployer address
0x1eaf9191dd52dcba2637fb1efa84e9552b8daa67



Client contacts:
Flokinomics team



Blockchain
Binance Smart Chain



Project website:
<https://www.flokinomics.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) (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 Flokinomics to perform an audit of smart contracts:

<https://bscscan.com/address/0x97ea5efdcdb5961a99ba5c96123042507c0210ec1#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

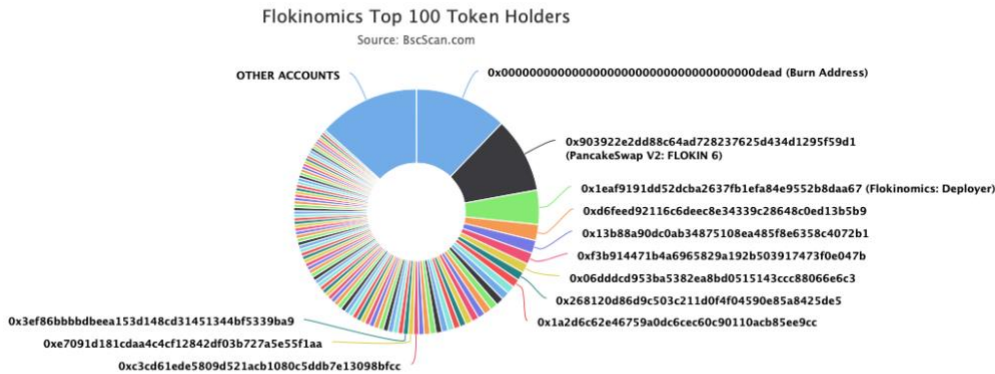
Token contract details for 06.10.2021

Contract name	Flokinomics
Contract address	0x97eA5EfDCb5961A99bA5C96123042507C0210Ec1
Total supply	2,953,539,554,888.72
Token ticker	FLOKIN
Decimals	4
Token holders	5,722
Transactions count	52,803
Top 100 holders dominance	86.62%
Total fee	10
Auto liquidity receiver	0x1eaf9191dd52dcba2637fb1efa84e9552b8daa67
Marketing fee receiver	0x13b88a90dc0ab34875108ea485f8e6358c4072b1
Pair	0x903922e2dd88c64ad728237625d434d1295f59d1
Contract deployer address	0x1eaf9191dd52dcba2637fb1efa84e9552b8daa67
Contract's current owner address	0x1eaf9191dd52dcba2637fb1efa84e9552b8daa67

BASE3 Token Distribution

The top 100 holders collectively own 86.62% (2,558,270,340,440.49 Tokens) of Flokinomics

Token Total Supply: 2,953,539,554,888.72 Token | Total Token Holders: 5,722

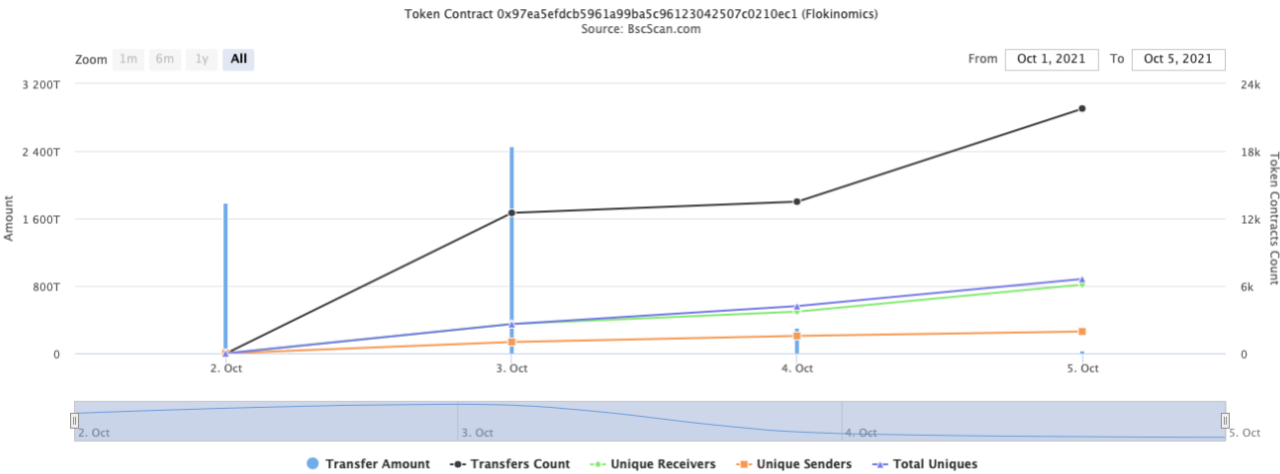


(A total of 2,558,270,340,440.49 tokens held by the top 100 accounts from the total supply of 2,953,539,554,888.72 token)


BASE3 Contract Interaction Details

Time Series: Token Contract Overview

Sat 2, Oct 2021 - Tue 5, Oct 2021



BASE3 Top 10 Token Holders

Rank	Address	Quantity (Token)	Percentage
1	Burn Address	360,667,003,072.2485	12.2113%
2	 PancakeSwap V2: FLOKIN 6	293,059,922,266.359	9.9223%
3	Flokinomics: Deployer	133,621,452,000.3473	4.5241%
4	0xd6feed92116c6deec8e34339c28648c0ed13b5b9	62,536,458,250.7879	2.1173%
5	0x13b88a90dc0ab34875108ea485f8e6358c4072b1	50,221,129,999.9066	1.7004%
6	0xf3b914471b4a6965829a192b503917473f0e047b	44,741,533,281.2002	1.5148%
7	0x06ddcd953ba5382ea8bd0515143ccc88066e6c3	37,011,264,774.4527	1.2531%
8	0x268120d86d9c503c211d0f4f04590e85a8425de5	33,248,613,002.7055	1.1257%
9	0x1a2d6c62e46759a0dc6cec60c90110acb85ee9cc	32,531,860,672.5786	1.1015%
10	0x5d99c515aaeb346ecda5f76229f97f52a834c474	31,577,810,663.7373	1.0692%



Contract functions details

+ [Lib] SafeMath

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

+ [Lib] SafeMathInt

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

+ [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] InterfaceLP

- [Ext] sync #

+ [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] setDistributionCriteria #
 - modifiers: onlyToken
 - [Ext] setShare #
 - modifiers: onlyToken
 - [Ext] deposit (\$)
 - modifiers: onlyToken
 - [Ext] process #
 - modifiers: onlyToken
 - [Int] shouldDistribute
 - [Int] distributeDividend #
 - [Ext] claimDividend #
 - [Pub] getUnpaidEarnings
 - [Int] getCumulativeDividends
 - [Int] addShareholder #
 - [Int] removeShareholder #
- + Flokinomics (IBEP20, Auth)
 - [Pub] rebase_percentage #
 - modifiers: onlyOwner
 - [Pub] rebase #
 - modifiers: onlyMaster
 - [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] checkTxLimit
 - [Int] shouldTakeFee
 - [Int] takeFee #
 - [Int] shouldSwapBack
 - [Ext] clearStuckBalance #
 - modifiers: authorized
 - [Ext] clearStuckBalance_sender #
 - modifiers: authorized

- [Ext] set_sell_multiplier #
 - modifiers: onlyOwner
- [Pub] tradingStatus #
 - modifiers: onlyOwner
- [Pub] launchStatus #
 - modifiers: onlyOwner
- [Pub] enable_hotel_CaliforniaMode #
 - modifiers: onlyOwner
- [Pub] set_max_roomrent #
 - modifiers: onlyOwner
- [Pub] manage_houseguests #
 - modifiers: onlyOwner
- [Pub] cooldownEnabled #
 - modifiers: onlyOwner
- [Int] swapBack #
 - modifiers: swapping
- [Ext] setIsDividendExempt #
 - modifiers: authorized
- [Ext] setIsFeeExempt #
 - modifiers: authorized
- [Ext] setIsTxLimitExempt #
 - modifiers: authorized
- [Ext] setIsTimelockExempt #
 - modifiers: authorized
- [Ext] setFees #
 - modifiers: authorized
- [Ext] setFeeReceivers #
 - modifiers: authorized
- [Ext] setSwapBackSettings #
 - modifiers: authorized
- [Ext] setTargetLiquidity #
 - modifiers: authorized
- [Ext] manualSync #
- [Ext] setLP #
 - modifiers: onlyOwner
- [Ext] setMaster #
 - modifiers: onlyOwner
- [Ext] isNotInSwap
- [Ext] checkSwapThreshold
- [Ext] setDistributionCriteria #
 - modifiers: authorized
- [Ext] setDistributorSettings #
 - modifiers: authorized
- [Pub] rescueToken #
 - modifiers: onlyOwner
- [Pub] getCirculatingSupply
- [Pub] getLiquidityBacking
- [Pub] isOverLiquified
- [Ext] checkMaxWalletToken
- [Ext] checkMaxTxAmount
- [Ext] setMaxWalletPercent_base1000 #
 - modifiers: onlyOwner
- [Ext] setMaxTxPercent_base1000 #
 - modifiers: onlyOwner
- [Ext] multiTransfer #

- modifiers: onlyOwner
- [Ext] multiTransfer_fixed #
 - modifiers: onlyOwner
- [Ext] rebase_updatebalance #
 - 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.	Low issues
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.	Low issues
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

1. Rebase

Issue:

- The function `rebase_updatebalance()` not called automatically after rebase.

Recommendation:

Insert autocall of `rebase_updatebalance()` function in `rebase()` function, not to forget equalize sharings.

2. Out of gas

Issue:

- The function `manage_houseguests()` uses the loop to change status of `isHouseguest` value of addresses. It also could be aborted with `OUT_OF_GAS` exception if there will be a long addresses list.

Recommendation:

Check that the array length is not too big.

Owner privileges (In the period when the owner is not renounced)

- Owner and Master can rebase.
- Owner can change sellMultiplier.
- Owner can change trading and launch status.
- Owner can change hotelCaliforniaMode.
- Owner can change maxRoomRent value.
- Owner can change cooldown settings.
- Owner can change pair address.
- Owner can change master address.
- Owner can withdraw BEP20 tokens.
- Owner can change _maxWalletToken and _maxTxAmount.
- Owner can multiTransfer fixed and listed token amounts.
- Authorized addresses can withdraw contract BNBs.
- Authorized addresses can include in and exclude from dividends.
- Authorized addresses can include in and exclude from fee, timelock and transaction amount.
- Authorized addresses can change fees.
- Authorized addresses can change fee receivers.
- Authorized addresses can change swap threshold and disable/enable swap.
- Authorized addresses can change targetLiquidity.
- Authorized addresses can change distribution criteria.
- Authorized addresses can change distribution GAS.

Conclusion

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

Liquidity locking details provided by the team:

<https://www.pinksale.finance/#/pinklock/record/42?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.