



**TechRate**  
AUDIT COMPANY

# Smart Contract Security Audit

# Audit Details



Audited project

**Super Floki**



Deployer address

**0x8BCEe7603f5EE5a87fFB7c4caA39c5aB60415847**



Client contacts:

**Super Floki team**



Blockchain

**Binance Smart Chain**



Project website:

**<https://superfloki.net>**

# 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 Super Floki to perform an audit of smart contracts:

<https://bscscan.com/address/0xf7bf4507336aea836ab5575ec1801d96c3059483#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 13.08.2021

Contract name	Super Floki
Contract address	0xf7BF4507336AeA836ab5575eC1801d96c3059483
Total supply	100,000,000,000,000,000
Token ticker	SLOKI
Decimals	9
Token holders	6,181
Transactions count	23,709
Top 100 holders dominance	78.45%
Liquidity fee	10
Tax fee	2
Total fees	17332832606867467991173221
Uniswap V2 pair	0x67da03b0f19e254bec8d08e666e17a24ee772190
Contract deployer address	0x8BCEe7603f5EE5a87fFB7c4caA39c5aB60415847
Contract's current owner address	0x8bcee7603f5ee5a87ffb7c4caa39c5ab60415847

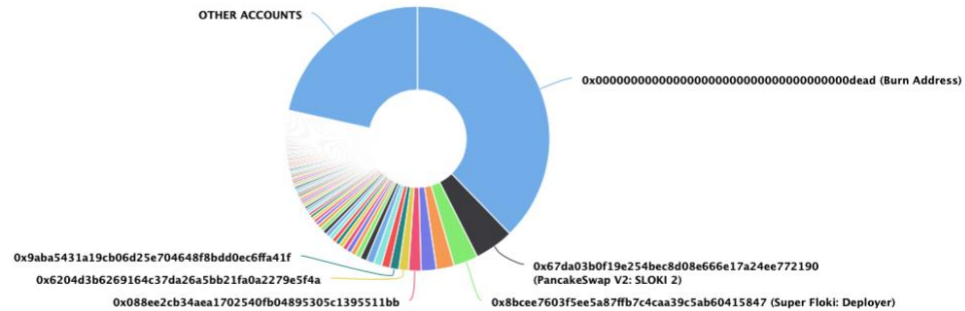
# Super Floki Token Distribution

The top 100 holders collectively own 78.45% (78,454,058,033,357,400.00 Tokens) of Super Floki

Token Total Supply: 100,000,000,000,000.00 Token | Total Token Holders: 6,181

Super Floki Top 100 Token Holders

Source: BscScan.com



(A total of 78,454,058,033,357,400.00 tokens held by the top 100 accounts from the total supply of 100,000,000,000,000.00 token)

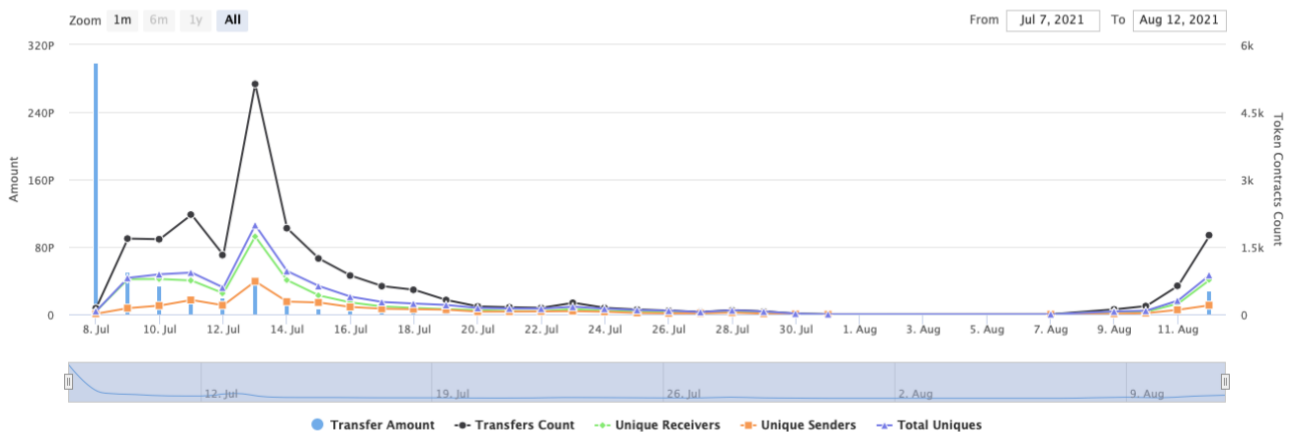
# Super Floki Contract Interaction Details

Time Series: Token Contract Overview

Thu 8, Jul 2021 - Thu 12, Aug 2021


Token Contract 0xf7bf4507336aea836ab5575ec1801d96c3059483 (Super Floki)

Source: BscScan.com





# Super Floki Top 10 Token Holders

Rank	Address	Quantity (Token)	Percentage
1	<a href="#">Burn Address</a>	37,727,671,543,369,400.68090939	37.7277%
2	 <a href="#">PancakeSwap V2: SLOKI 2</a>	4,788,972,114,340,330.490764937	4.7890%
3	<a href="#">Super Floki: Deployer</a>	3,008,712,847,364,100.1640381	3.0087%
4	<a href="#">0x62973d4126a51ce133b7c534304657b4153805fc</a>	2,187,895,214,231,640.203072444	2.1879%
5	<a href="#">0x7cb9295213c67ad1e83e593aa33ff40fea1b33f5</a>	1,852,375,463,503,130.703181793	1.8524%
6	<a href="#">0x088ee2cb34aea1702540fb04895305c1395511bb</a>	1,543,359,741,094,370.171027267	1.5434%
7	<a href="#">0x6204d3b6269164c37da26a5bb21fa0a2279e5f4a</a>	1,168,745,489,314,140.583531919	1.1687%
8	<a href="#">0x9aba5431a19cb06d25e704648f8bdd0ec6ffa41f</a>	1,104,553,523,610,730.282760249	1.1046%
9	<a href="#">0xc110505eaea15cfa0889e3a617a4dfb5010fc12</a>	1,027,413,860,696,580.84093004	1.0274%
10	<a href="#">0xb16e1fe2768966f98074c18734eef03ba19d579e</a>	985,577,472,169,053.723459007	0.9856%



# Contract functions details

- + Context
  - [Int] \_msgSender
  - [Int] \_msgData
- + [Int] IERC20
  - [Ext] totalSupply
  - [Ext] balanceOf
  - [Ext] transfer #
  - [Ext] allowance
  - [Ext] approve #
  - [Ext] transferFrom #
- + [Lib] SafeMath
  - [Int] add
  - [Int] sub
  - [Int] sub
  - [Int] mul
  - [Int] div
  - [Int] div
  - [Int] mod
  - [Int] mod
- + [Lib] Address
  - [Int] isContract
  - [Int] sendValue #
  - [Int] functionCall #
  - [Int] functionCall #
  - [Int] functionCallWithValue #
  - [Int] functionCallWithValue #
  - [Prv] \_functionCallWithValue
- + Ownable (Context)
  - [Pub] <Constructor> #
  - [Pub] owner
  - [Pub] renounceOwnership #
    - modifiers: onlyOwner
  - [Pub] transferOwnership #
    - modifiers: onlyOwner
  - [Pub] getUnlockTime
  - [Pub] getTime
  - [Pub] lock #
    - modifiers: onlyOwner
  - [Pub] unlock #
- + [Int] IUniswapV2Factory
  - [Ext] feeTo
  - [Ext] feeToSetter
  - [Ext] getPair
  - [Ext] allPairs
  - [Ext] allPairsLength
  - [Ext] createPair #
  - [Ext] setFeeTo #
  - [Ext] setFeeToSetter #
- + [Int] IUniswapV2Pair
  - [Ext] name



- [Ext] symbol
- [Ext] decimals
- [Ext] totalSupply
- [Ext] balanceOf
- [Ext] allowance
- [Ext] approve #
- [Ext] transfer #
- [Ext] transferFrom #
- [Ext] DOMAIN\_SEPARATOR
- [Ext] PERMIT\_TYPEHASH
- [Ext] nonces
- [Ext] permit #
- [Ext] MINIMUM\_LIQUIDITY
- [Ext] factory
- [Ext] token0
- [Ext] token1
- [Ext] getReserves
- [Ext] price0CumulativeLast
- [Ext] price1CumulativeLast
- [Ext] kLast
- [Ext] burn #
- [Ext] swap #
- [Ext] skim #
- [Ext] sync #
- [Ext] initialize #
- + [Int] IUniswapV2Router01
  - [Ext] factory
  - [Ext] WETH
  - [Ext] addLiquidity #
  - [Ext] addLiquidityETH (\$)
  - [Ext] removeLiquidity #
  - [Ext] removeLiquidityETH #
  - [Ext] removeLiquidityWithPermit #
  - [Ext] removeLiquidityETHWithPermit #
  - [Ext] swapExactTokensForTokens #
  - [Ext] swapTokensForExactTokens #
  - [Ext] swapExactETHForTokens (\$)
  - [Ext] swapTokensForExactETH #
  - [Ext] swapExactTokensForETH #
  - [Ext] swapETHForExactTokens (\$)
  - [Ext] quote
  - [Ext] getAmountOut
  - [Ext] getAmountIn
  - [Ext] getAmountsOut
  - [Ext] getAmountsIn
- + [Int] IUniswapV2Router02 (IUniswapV2Router01)
  - [Ext] removeLiquidityETHSupportingFeeOnTransferTokens #
  - [Ext] removeLiquidityETHWithPermitSupportingFeeOnTransferTokens #
  - [Ext] swapExactTokensForTokensSupportingFeeOnTransferTokens #
  - [Ext] swapExactETHForTokensSupportingFeeOnTransferTokens (\$)
  - [Ext] swapExactTokensForETHSupportingFeeOnTransferTokens #
- + SuperFloki (Context, IERC20, Ownable)
  - [Pub] <Constructor> #
  - [Pub] name

- [Pub] symbol
- [Pub] decimals
- [Pub] totalSupply
- [Pub] balanceOf
- [Pub] transfer #
- [Pub] allowance
- [Pub] approve #
- [Pub] transferFrom #
- [Pub] increaseAllowance #
- [Pub] decreaseAllowance #
- [Pub] isExcludedFromReward
- [Pub] totalFees
- [Pub] minimumTokensBeforeSwapAmount
- [Pub] buyBackSellLimitAmount
- [Pub] deliver #
- [Pub] reflectionFromToken
- [Pub] tokenFromReflection
- [Pub] excludeFromReward #
  - modifiers: onlyOwner
- [Ext] includeInReward #
  - modifiers: onlyOwner
- [Prv] \_approve #
- [Prv] \_transfer #
- [Prv] swapTokens #
  - modifiers: lockTheSwap
- [Prv] buyBackTokens #
  - modifiers: lockTheSwap
- [Prv] swapTokensForEth #
- [Prv] swapETHForTokens #
- [Prv] addLiquidity #
- [Prv] \_tokenTransfer #
- [Prv] \_transferStandard #
- [Prv] \_transferToExcluded #
- [Prv] \_transferFromExcluded #
- [Prv] \_transferBothExcluded #
- [Prv] \_reflectFee #
- [Prv] \_getValues
- [Prv] \_getTValues
- [Prv] \_getRValues
- [Prv] \_getRate
- [Prv] \_getCurrentSupply
- [Prv] \_takeLiquidity #
- [Prv] calculateTaxFee
- [Prv] calculateLiquidityFee
- [Prv] removeAllFee #
- [Prv] restoreAllFee #
- [Pub] isExcludedFromFee
- [Pub] excludeFromFee #
  - modifiers: onlyOwner
- [Pub] includeInFee #
  - modifiers: onlyOwner
- [Prv] \_getSellBnBAmount
- [Prv] \_removeOldSellHistories #
- [Ext] SetBuyBackMaxTimeForHistories #
  - modifiers: onlyOwner

- [Ext] SetBuyBackDivisor #  
- modifiers: onlyOwner
- [Pub] GetBuyBackTimeInterval
- [Ext] SetBuyBackTimeInterval #  
- modifiers: onlyOwner
- [Ext] SetBuyBackRangeRate #  
- modifiers: onlyOwner
- [Pub] GetSwapMinutes
- [Ext] SetSwapMinutes #  
- modifiers: onlyOwner
- [Ext] setTaxFeePercent #  
- modifiers: onlyOwner
- [Ext] setBuyFee #  
- modifiers: onlyOwner
- [Ext] setSellFee #  
- modifiers: onlyOwner
- [Ext] setLiquidityFeePercent #  
- modifiers: onlyOwner
- [Ext] setBuyBackSellLimit #  
- modifiers: onlyOwner
- [Ext] setMaxTxAmount #  
- modifiers: onlyOwner
- [Ext] setMarketingDivisor #  
- modifiers: onlyOwner
- [Ext] setNumTokensSellToAddToBuyBack #  
- modifiers: onlyOwner
- [Ext] setMarketingAddress #  
- modifiers: onlyOwner
- [Pub] setSwapAndLiquifyEnabled #  
- modifiers: onlyOwner
- [Pub] setBuyBackEnabled #  
- modifiers: onlyOwner
- [Pub] setAutoBuyBackEnabled #  
- modifiers: onlyOwner
- [Ext] prepareForPreSale #  
- modifiers: onlyOwner
- [Ext] afterPreSale #  
- modifiers: onlyOwner
- [Prv] transferToAddressETH #
- [Pub] changeRouterVersion #  
- modifiers: onlyOwner
- [Ext] <Fallback> (\$)
- [Pub] transferForeignToken #  
- modifiers: onlyOwner
- [Ext] Sweep #  
- modifiers: onlyOwner
- [Ext] setAddressFee #  
- modifiers: onlyOwner
- [Ext] setBuyAddressFee #  
- modifiers: onlyOwner
- [Ext] setSellAddressFee #  
- 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.	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

### 1. Out of gas

Issue:

- The function `includeInReward()` uses the loop to find and remove addresses from the `_excluded` list. Function will be aborted with `OUT_OF_GAS` exception if there will be a long excluded addresses list.

```
function includeInReward(address account↑) external onlyOwner() {
    require(!_isExcluded[account↑], "Account is already excluded");
    for (uint256 i = 0; i < _excluded.length; i++) {
        if (_excluded[i] == account↑) {
            _excluded[i] = _excluded[_excluded.length - 1];
            _tOwned[account↑] = 0;
            _isExcluded[account↑] = false;
            _excluded.pop();
            break;
        }
    }
}
```

- The function `_getCurrentSupply` also uses the loop for evaluating total supply. It also could be aborted with `OUT_OF_GAS` exception if there will be a long excluded addresses list.

```
function _getCurrentSupply() private view returns (uint256, uint256) {
    uint256 rSupply = _rTotal;
    uint256 tSupply = _tTotal;
    for (uint256 i = 0; i < _excluded.length; i++) {
        if (
            _rOwned[_excluded[i]] > rSupply ||
            _tOwned[_excluded[i]] > tSupply
        ) return (_rTotal, _tTotal);
        rSupply = rSupply.sub(_rOwned[_excluded[i]]);
        tSupply = tSupply.sub(_tOwned[_excluded[i]]);
    }
    if (rSupply < _rTotal.div(_tTotal)) return (_rTotal, _tTotal);
    return (rSupply, tSupply);
}
```

Recommendation:

Check that the excluded array length is not too big.

## Notes:

- addLiquidity function is unused.

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

- Owner can withdraw tokens.
- Owner can withdraw BNBs.
- Owner can change tax and liquidity fees.
- Owner can change maximum transaction amount.
- Owner can exclude from the fee.
- Owner can change marketingDivisor.
- Owner can change minimum number of tokens to add to liquidity.
- Owner can change marketing address.
- Owner can enable and disable buyBack.
- Owner can enable before and after presale modes.
- Owner can lock and unlock. By the way, using these functions the owner could retake privileges even after the ownership was renounced.
- Owner can set addresses fees.
- Owner can Uniswap router address.
- Owner can disable and enable auto buyback.
- Owner can change buyBackSellLimit.
- Owner can change buy and sell fees.
- Owner can change \_intervalMinutesForSwap.
- Owner can change buyback time interval and range rate.
- Owner can change buyback divisor.
- Owner can change \_buyBackMaxTimeForHistories.

# Conclusion

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

4% of the liquidity goes to the marketing address. The further transfers and operations with the funds raise are not related to this particular contract.

Liquidity locking details provided by the team:

[https://dxsale.app/app/v2\\_9/dxlockview?id=1&add=0x8BCEe7603f5EE5a87fFB7c4caA39c5aB60415847&type=lplock&chain=BSC](https://dxsale.app/app/v2_9/dxlockview?id=1&add=0x8BCEe7603f5EE5a87fFB7c4caA39c5aB60415847&type=lplock&chain=BSC)

[https://dxsale.app/app/v2\\_9/dxlockview?id=0&add=0x8BCEe7603f5EE5a87fFB7c4caA39c5aB60415847&type=lplock&chain=BSC](https://dxsale.app/app/v2_9/dxlockview?id=0&add=0x8BCEe7603f5EE5a87fFB7c4caA39c5aB60415847&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.*