Techrate1 Techrate

TechRate

AUDIT COMPANY

Smart Contract Security Audit

TechRate

January, 2022

Audit Details

Audited project

TOKE.N

Deployer address

0xcf5fb7da3a6c619293fd1932adb01c653e434029

Client contacts:

TOKE.N team

Blockchain

Binance Smart Chain

Project website:

https://thetokenproject.org/

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 TOKE.N to perform an audit of smart contracts:
https://bscscan.com/address/0xf8d4ccd333f893fc1ad75b626a2c82b4bc7ccbdd#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.

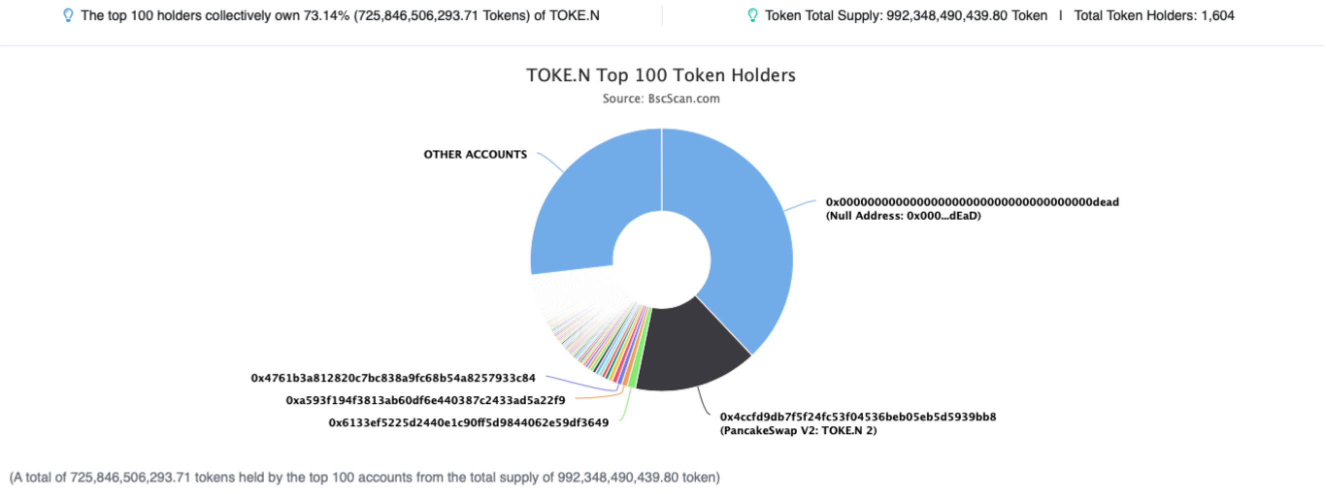
The information in this report should be used to understand the risk exposure of the smart contract, and as a guide to improve the security posture of the smart contract by remediating the issues that were identified.

Contracts Details

Token contract details for 16.01.2022

Contract name	TOKE.N
Contract address	0xF8D4ccd333F893FC1Ad75B626a2C82B4BC7Ccbdd
Total supply	992,348,490,439.801243
Token ticker	TOKE.N
Decimals	9
Token holders	1,604
Transactions count	4,753
Top 100 holders dominance	73.14%
Balance limit divider	50
Sell limit	5000000000000000000
Max buy lock time	9
Team wallet	0x2e0ff83a64373e13179e307523fbe3d08e04a4d8
Contract deployer address	0xcf5fb7da3a6c619293fd1932adb01c653e434029
Contract's current owner address	0xcf5fb7da3a6c619293fd1932adb01c653e434029

TOKE.N Token Distribution



The top 100 holders collectively own 73.14% (725,846,506,293.71 Tokens) of TOKE.N

Token Total Supply: 992,348,490,439.80 Token | Total Token Holders: 1,604

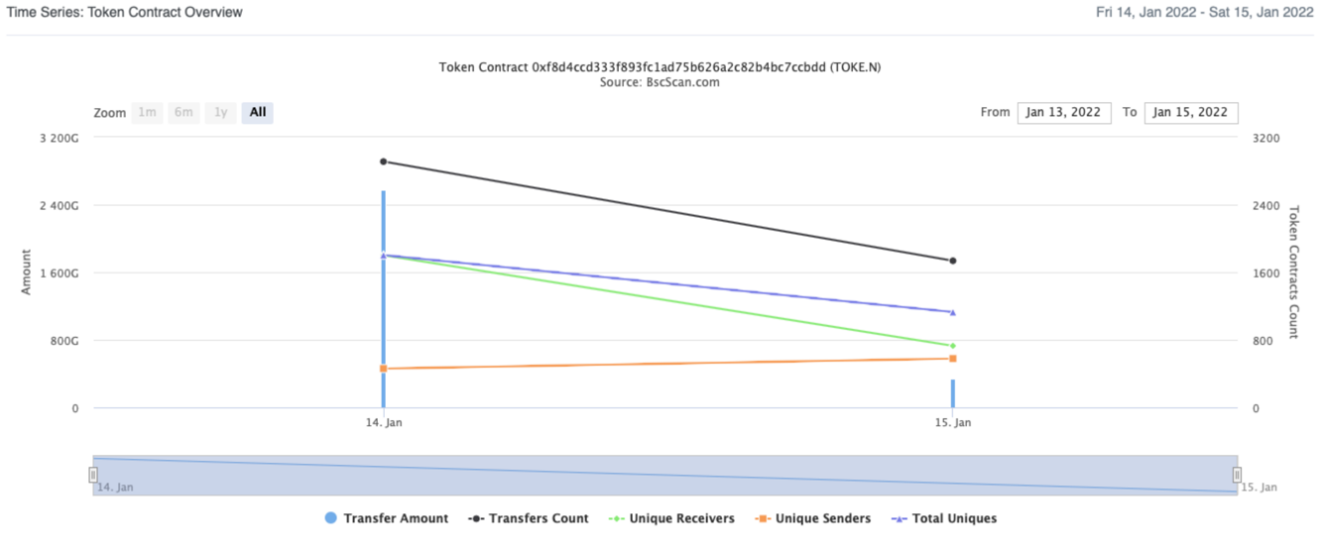
TOKE.N Top 100 Token Holders

Source: BscScan.com

OTHER ACCOUNTS
0x000000000000000000000000000000000000dead
(Null Address: 0x000...dEaD)
0x4761b3a812820c7bc838a9fc68b54a8257933c84
0xa593f194f3813ab60df6e440387c2433ad5a22f9
0x6133ef5225d2440e1c90ff5d9844062e59df3649
0x4ccfd9db7f5f24fc53f04536beb05eb5d5939bb8
(PancakeSwap V2: TOKE.N 2)

(A total of 725,846,506,293.71 tokens held by the top 100 accounts from the total supply of 992,348,490,439.80 token)

TOKE.N Contract Interaction Details



Time Series: Token Contract Overview

Fri 14, Jan 2022 - Sat 15, Jan 2022

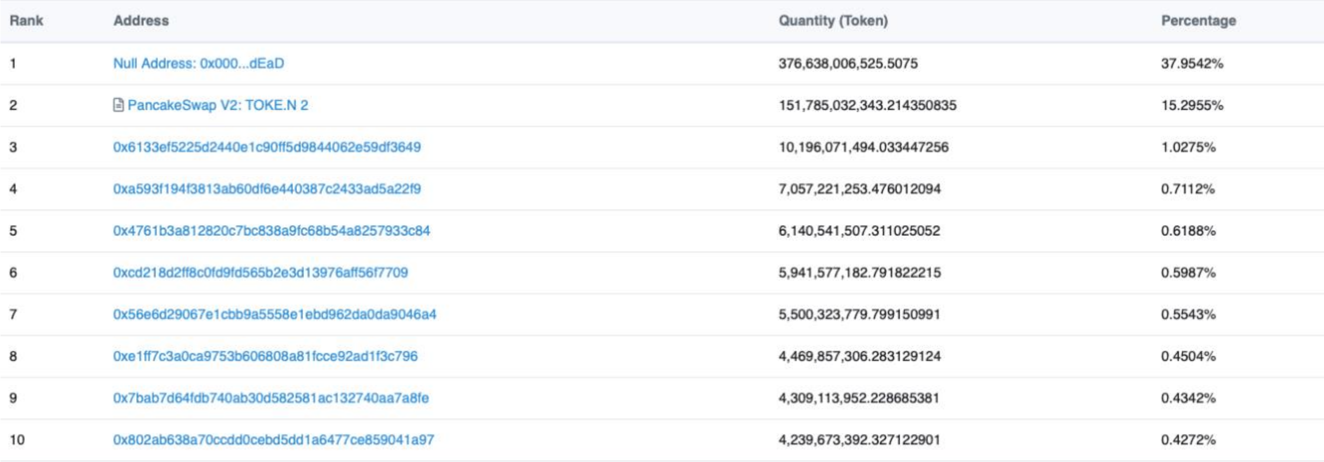
Token Contract 0xf8d4ccd333f893fc1ad75b626a2c82b4bc7ccbdd (TOKE.N)

Source: BscScan.com

Zoom 1m 6m 1y All

From Jan 13, 2022 To Jan 15, 2022

TOKE.N Top 10 Token Holders



Rank	Address	Quantity (Token)	Percentage
1	Null Address: 0x000...dEaD	376,638,006,525.5075	37.9542%
2	🗎 PancakeSwap V2: TOKE.N 2	151,785,032,343.214350835	15.2955%
3	0x6133ef5225d2440e1c90ff5d9844062e59df3649	10,196,071,494.033447256	1.0275%
4	0xa593f194f3813ab60df6e440387c2433ad5a22f9	7,057,221,253.476012094	0.7112%
5	0x4761b3a812820c7bc838a9fc68b54a8257933c84	6,140,541,507.311025052	0.6188%
6	0xcd218d2ff8c0fd9fd565b2e3d13976aff56f7709	5,941,577,182.791822215	0.5987%
7	0x56e6d29067e1cbb9a5558e1ebd962da0da9046a4	5,500,323,779.799150991	0.5543%
8	0xe1ff7c3a0ca9753b606808a81fcce92ad1f3c796	4,469,857,306.283129124	0.4504%
9	0x7bab7d64fdb740ab30d582581ac132740aa7a8fe	4,309,113,952.228685381	0.4342%
10	0x802ab638a70ccdd0cebd5dd1a6477ce859041a97	4,239,673,392.327122901	0.4272%

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 #

 + [Int] IPancakeERC20
  - [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 #

 + [Int] IPancakeFactory
  - [Ext] feeTo
  - [Ext] feeToSetter
  - [Ext] getPair
  - [Ext] allPairs
  - [Ext] allPairsLength
  - [Ext] createPair #
  - [Ext] setFeeTo #
  - [Ext] setFeeToSetter #

 + [Int] IPancakeRouter01
  - [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] factory
  - [Ext] WETH
  - [Ext] quote
  - [Ext] getamountOut
  - [Ext] getamountIn
  - [Ext] getamountsOut
  - [Ext] getamountsIn

+ [Int] IPancakeRouter02 (IPancakeRouter01)
  - [Ext] removeLiquidityETHSupportingFeeOnTransferTokens #
  - [Ext] removeLiquidityETHWithPermitSupportingFeeOnTransferTokens #
  - [Ext] swapExactTokensForTokensSupportingFeeOnTransferTokens #
  - [Ext] swapExactETHForTokensSupportingFeeOnTransferTokens ($)
  - [Ext] swapExactTokensForETHSupportingFeeOnTransferTokens #

+  Ownable
  - [Pub] <Constructor> #
  - [Pub] owner
  - [Ext] renounceOwnership #
    - modifiers: onlyOwner
  - [Ext] transferOwnership #
    - modifiers: onlyOwner

+ [Lib] Address
  - [Int] isContract
  - [Int] sendValue #
  - [Int] functionCall #
  - [Int] functionCall #
  - [Int] functionCallWithValue #
  - [Int] functionCallWithValue #
  - [Int] functionStaticCall
  - [Int] functionStaticCall
  - [Int] functionDelegateCall #
  - [Int] functionDelegateCall #
  - [Prv] _verifyCallResult

+ [Lib] EnumerableSet
  - [Prv] _add #
  - [Prv] _remove #
  - [Prv] _contains
  - [Prv] _length
  - [Prv] _at
  - [Int] add #
  - [Int] remove #
  - [Int] contains
  - [Int] length
  - [Int] at
  - [Int] add #
  - [Int] remove #
  - [Int] contains
  - [Int] length
  - [Int] at
  - [Int] add #
  - [Int] remove #
  - [Int] contains
  - [Int] length
  - [Int] at
```

```
+ TOKEN (IBEP20, Ownable)
  - [Pub] <Constructor> #
  - [Prv] _transfer #
  - [Prv] _taxedTransfer #
  - [Prv] _feelessTransfer #
  - [Prv] _calculateFee
  - [Prv] _addToken #
  - [Prv] _removeToken #
  - [Prv] _swapContractToken #
    - modifiers: lockTheSwap
  - [Prv] _swapTokenForBNB #
  - [Prv] _addLiquidity #
  - [Ext] getLiquidityReleaseTimeInSeconds
  - [Ext] getBurnedTokens
  - [Ext] getLimits
  - [Ext] getTaxes
  - [Ext] getAddressBuyLockTimeInSeconds
  - [Ext] getBuyLockTimeInSeconds
  - [Ext] AddressResetBuyLock #
  - [Ext] TeamWithdrawALLMarketingBNB #
    - modifiers: onlyOwner
  - [Ext] TeamWithdrawXMarketingBNB #
    - modifiers: onlyOwner
  - [Ext] TeamSwitchManualBNBConversion #
    - modifiers: onlyOwner
  - [Ext] TeamChangeAntiWhale #
    - modifiers: onlyOwner
  - [Ext] TeamChangeTeamWallet #
    - modifiers: onlyOwner
  - [Ext] TeamChangeConstructionWallet #
    - modifiers: onlyOwner
  - [Ext] TeamDisableBuyLock #
    - modifiers: onlyOwner
  - [Ext] TeamSetBuyLockTime #
    - modifiers: onlyOwner
  - [Ext] TeamUpdateAmountToSwap #
    - modifiers: onlyOwner
  - [Ext] AddWalletExclusion #
    - modifiers: onlyOwner
  - [Ext] TeamSetTaxes #
    - modifiers: onlyOwner
  - [Ext] TeamCreateLPandBNB #
    - modifiers: onlyOwner
  - [Ext] teamUpdatePancakeRouter #
    - modifiers: onlyOwner
  - [Ext] TeamUpdateLimits #
    - modifiers: onlyOwner
  - [Ext] SetupEnableTrading #
    - modifiers: onlyOwner
  - [Ext] SetupLiquidityTokenAddress #
    - modifiers: onlyOwner
  - [Ext] TeamProlongLiquidityLockInSeconds #
    - modifiers: onlyOwner
  - [Prv] _prolongLiquidityLock #
```

- [Ext] TeamReleaseLiquidity #
  - modifiers: onlyOwner
- [Ext] TeamRemoveLiquidity #
  - modifiers: onlyOwner
- [Ext] TeamRemoveRemainingBNB #
  - modifiers: onlyOwner
- [Ext] <Fallback> ($)
- [Ext] <Fallback> ($)
- [Ext] getOwner
- [Ext] name
- [Ext] symbol
- [Ext] decimals
- [Ext] totalSupply
- [Ext] balanceOf
- [Ext] transfer #
- [Ext] allowance
- [Ext] approve #
- [Prv] _approve #
- [Ext] transferFrom #
- [Ext] increaseAllowance #
- [Ext] decreaseAllowance #

($) = 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.

Notes:

- marketingBalance calculated and withdrawn not in one to one proportion.

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

- Owner can withdraw marketing balance.
- Owner can disable auto call of _swapContractToken function.
- Owner can change antiWhale.
- Owner can change teamWallet and ConstructionWallet addresses.
- Owner can disable buy lock.
- Owner can change currentAmountToSwap.
- Owner can exclude addresses.
- Owner can change buy lock time.
- Owner can change taxes.
- Owner can manually call _swapContractToken function.
- Owner can change PancakeRouter address.
- Owner can change balance and sell limits.
- Owner can enable trading(already called).
- Owner can change liquidity token address.
- Owner can increase _liquidityUnlockTime.
- Owner can withdraw liquidity to team wallet if it is not locked.
- Owner can remove liquidity.
- Owner can withdraw contract balance if it is not locked.

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 are NOT provided by the team.

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.