TechRate
March, 2022

TECH
RATE

SMART CONTRACTS SECURITY AUDIT REPORT

Techrate_audits Techrate Techrate1

Audit Details

Audited project

BackstabDoge

Deployer address

0xbb180e1f5969e763c44255953599c46e70fac6f3

Client contacts:

BackstabDoge team

Blockchain

Binance Smart Chain

Project website:

https://backstabdoge.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 BackstabDoge to perform an audit of smart contracts:

https://bscscan.com/address/0x0cdda5de813af159d1e831f785de0110a414a3fb#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.

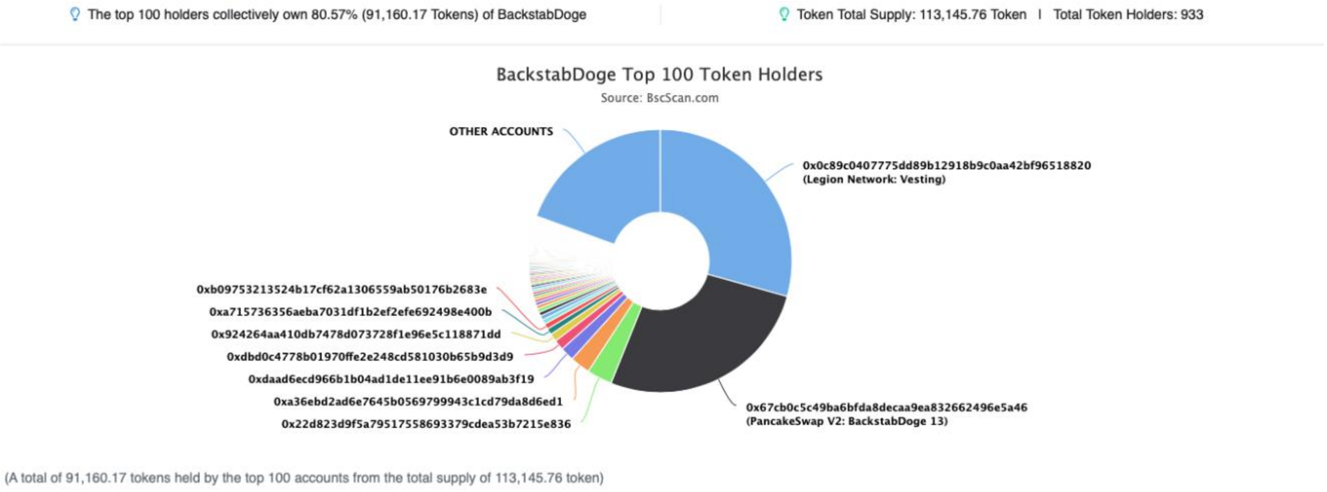
The information in this report should be used to understand the risk exposure of the smart contract, and as a guide to improve the security posture of the smart contract by remediating the issues that were identified.

Contracts Details

Token contract details for 26.03.2022

Contract name	BackstabDoge
Contract address	0x0CddA5dE813Af159D1E831F785de0110A414A3Fb
Total supply	113,145.76231
Token ticker	BackstabDoge
Decimals	5
Token holders	933
Transactions count	8,846
Top 100 holders dominance	80.57%
Autoliquidity receiver	0xbb180e1f5969e763c44255953599c46e70fac6f3
Liquidity fee	40
Total fee	140
pair	0x67cb0c5c49ba6bfda8decaa9ea832662496e5a46
Contract deployer address	0xbb180e1f5969e763c44255953599c46e70fac6f3
Owner address	0xbb180e1f5969e763c44255953599c46e70fac6f3

BackstabDoge Token Distribution



The top 100 holders collectively own 80.57% (91,160.17 Tokens) of BackstabDoge

Token Total Supply: 113,145.76 Token | Total Token Holders: 933

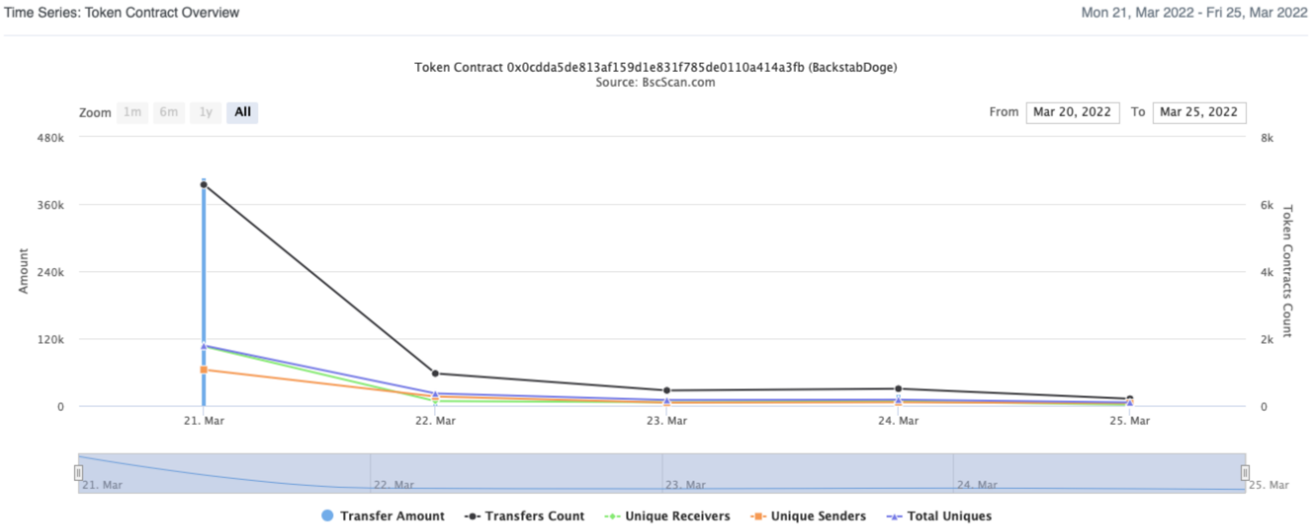
BackstabDoge Top 100 Token Holders

Source: BscScan.com

OTHER ACCOUNTS
0x0c89c0407775dd89b12918b9c0aa42bf96518820
(Legion Network: Vesting)
0xb09753213524b17cf62a1306559ab50176b2683e
0xa715736356aeba7031df1b2ef2efe692498e400b
0x924264aa410db7478d073728f1e96e5c118871dd
0xdbd0c4778b01970ffe2e248cd581030b65b9d3d9
0xdaad6ecd966b1b04ad1de11ee91b6e0089ab3f19
0xa36ebd2ad6e7645b0569799943c1cd79da8d6ed1
0x22d823d9f5a79517558693379cdea53b7215e836
0x67cb0c5c49ba6bfda8decaa9ea832662496e5a46
(PancakeSwap V2: BackstabDoge 13)

(A total of 91,160.17 tokens held by the top 100 accounts from the total supply of 113,145.76 token)

BackstabDoge Contract Interaction Details



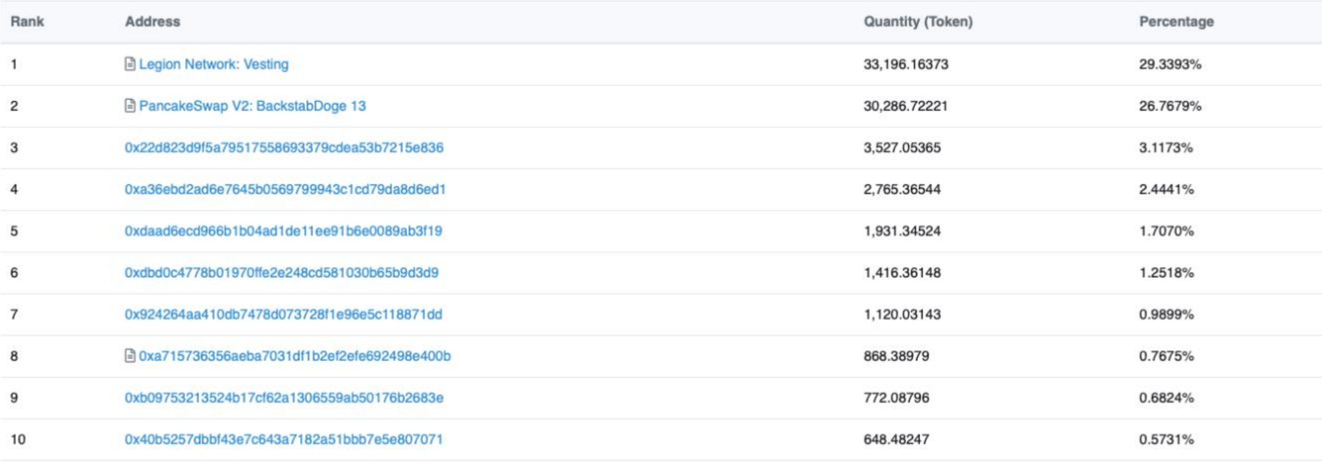
Time Series: Token Contract Overview

Mon 21, Mar 2022 - Fri 25, Mar 2022

Token Contract 0x0cdda5de813af159d1e831f785de0110a414a3fb (BackstabDoge)

Source: BscScan.com

BackstabDoge Top 10 Token Holders



Rank	Address	Quantity (Token)	Percentage
1	Legion Network: Vesting	33,196.16373	29.3393%
2	PancakeSwap V2: BackstabDoge 13	30,286.72221	26.7679%
3	0x22d823d9f5a79517558693379cdea53b7215e836	3,527.05365	3.1173%
4	0xa36ebd2ad6e7645b0569799943c1cd79da8d6ed1	2,765.36544	2.4441%
5	0xdaad6ecd966b1b04ad1de11ee91b6e0089ab3f19	1,931.34524	1.7070%
6	0xdbd0c4778b01970ffe2e248cd581030b65b9d3d9	1,416.36148	1.2518%
7	0x924264aa410db7478d073728f1e96e5c118871dd	1,120.03143	0.9899%
8	0xa715736356aeba7031df1b2ef2efe692498e400b	868.38979	0.7675%
9	0xb09753213524b17cf62a1306559ab50176b2683e	772.08796	0.6824%
10	0x40b5257dbbf43e7c643a7182a51bbb7e5e807071	648.48247	0.5731%

Contract functions details

```
+ [Lib] SafeMathInt
  - [Int] mul
  - [Int] div
  - [Int] sub
  - [Int] add
  - [Int] abs

 + [Lib] SafeMath
  - [Int] add
  - [Int] sub
  - [Int] sub
  - [Int] mul
  - [Int] div
  - [Int] div
  - [Int] mod

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

 + [Int] IPancakeSwapPair
  - [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] mint #
  - [Ext] burn #
  - [Ext] swap #
  - [Ext] skim #
  - [Ext] sync #
  - [Ext] initialize #

+ [Int] IPancakeSwapRouter
  - [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 ($)
  - [Ext] quote
  - [Ext] getAmountOut
  - [Ext] getAmountIn
  - [Ext] getAmountsOut
  - [Ext] getAmountsIn
  - [Ext] removeLiquidityETHSupportingFeeOnTransferTokens #
  - [Ext] removeLiquidityETHWithPermitSupportingFeeOnTransferTokens #
  - [Ext] swapExactTokensForTokensSupportingFeeOnTransferTokens #
  - [Ext] swapExactETHForTokensSupportingFeeOnTransferTokens ($)
  - [Ext] swapExactTokensForETHSupportingFeeOnTransferTokens #

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

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

+  ERC20Detailed (IERC20)
  - [Pub] <Constructor> #
  - [Pub] name
  - [Pub] symbol
  - [Pub] decimals

+  BackstabDoge (ERC20Detailed, Ownable)
  - [Pub] <Constructor> #
    - modifiers: ERC20Detailed,Ownable
  - [Pub] rebase #
  - [Ext] transfer #
    - modifiers: validRecipient
  - [Ext] transferFrom #
    - modifiers: validRecipient
  - [Int] _basicTransfer #
  - [Int] _transferFrom #
  - [Int] takeFee #
  - [Int] addLiquidity #
    - modifiers: swapping
  - [Int] swapBack #
    - modifiers: swapping
  - [Ext] withdrawAllToTreasury #
    - modifiers: swapping,onlyOwner
  - [Ext] withdrawBNB #
    - modifiers: onlyOwner
  - [Int] shouldTakeFee
  - [Int] shouldRebase
  - [Int] shouldAddLiquidity
  - [Int] shouldSwapBack
  - [Ext] setAutoRebase #
    - modifiers: onlyOwner
  - [Ext] setAutoAddLiquidity #
```

  - modifiers: onlyOwner
- [Ext] allowance
- [Ext] decreaseAllowance #
- [Ext] increaseAllowance #
- [Ext] approve #
- [Ext] checkFeeExempt
- [Pub] getCirculatingSupply
- [Ext] isNotInSwap
- [Ext] manualSync #
- [Pub] getLiquidityBacking
- [Ext] setWhitelist #
  - modifiers: onlyOwner
- [Ext] setBotBlacklist #
  - modifiers: onlyOwner
- [Pub] setPairAddress #
  - modifiers: onlyOwner
- [Ext] setLP #
  - modifiers: onlyOwner
- [Ext] totalSupply
- [Ext] balanceOf
- [Ext] <Fallback> ($)

($) = 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.**	Low issues
15.	**Scoping and Declarations.**	Passed
16.	**Uninitialized storage pointers.**	Passed
17.	**Arithmetic accuracy.**	Low issues
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 rebase() uses the loop to rebase the contract by the time. Function will be aborted with OUT_OF_GAS exception if there will be a long time without rebase.

Recommendation:

Check that the rebase is not turned off for too long.

2. Rounding errors

Issue:

- At some calculation with division, it goes first. In Solidity we don’t have floating points, but instead we get rounding errors.

Recommendation:

Do division after multiplication.

3. No event on basic transfer

Issue:

- The function _basicTransfer() do not emit transferring event.

Recommendation:

Add event emitting.

Notes:

- MAX_SUPPLY could be exceeded, because there is no checking of future _totalSupply to be less than MAX_SUPPLY.

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

- Owner can swap all contract balance to treasury address.
- Owner can change autorebase settings.
- Owner can change autoliquidity settings.
- Owner can exclude addresses from fees.
- Owner can blacklist addresses.
- Owner can change pair address and pair contract.
- Owner can withdraw contract BNBs.

Conclusion

Smart contracts contain low severity issues! Liquidity pair contract's security is not checked due to out of scope. The further transfers and operations with the funds raise are not related to this particular contract.

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.