Techrate1 Techrate

TechRate

AUDIT COMPANY

Smart Contract Security Audit

TechRate

August, 2021

Audit Details

Audited project

DogeAxie

Deployer address

0x7adaf2d7fa4c58d3d05b171eb23ae6d44e63d5c4

Client contacts:

DogeAxie team

Blockchain

Binance Smart Chain

Project website:

dogeaxie.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 DogeAxie to perform an audit of smart contracts:
https://bscscan.com/address/0xac5c2b692176efd1bc46914b122736a75e6e7ae4#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

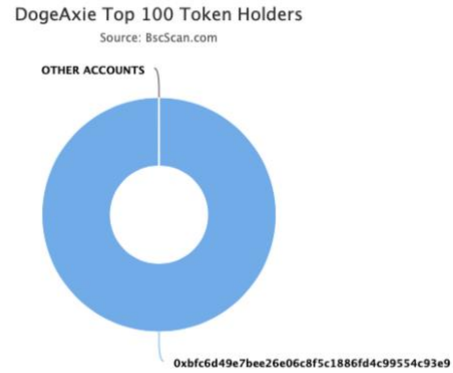
Token contract details for 19.08.2021

Contract name	DogeAxie
Contract address	0xac5C2b692176EfD1bC46914B122736a75e6E7aE4
Total supply	1,000,000,000,000,000
Token ticker	DogeAxie
Decimals	9
Token holders	1
Transactions count	2
Top 100 holders dominance	100.00%
Swap threshold	100000000000000000000
Auto liquidity receiver	0x1b2c2be5ef078b62ab9babc8c984bf0672c1ad52
Marketing fee receiver	0x2dacd42560df508965f82fd71ff140d5b879ce92
Pair	0x1b2c2be5ef078b62ab9babc8c984bf0672c1ad52
Contract deployer address	0x7adaf2d7fa4c58d3d05b171eb23ae6d44e63d5c4
Contract's current owner address	0xbfc6d49e7bee26e06c8f5c1886fd4c99554c93e9

BASE3 Token Distribution

The top 100 holders collectively own 100.00% (1,000,000,000,000,000.00 Tokens) of DogeAxie

Token Total Supply: 1,000,000,000,000,000.00 Token | Total Token Holders: 1

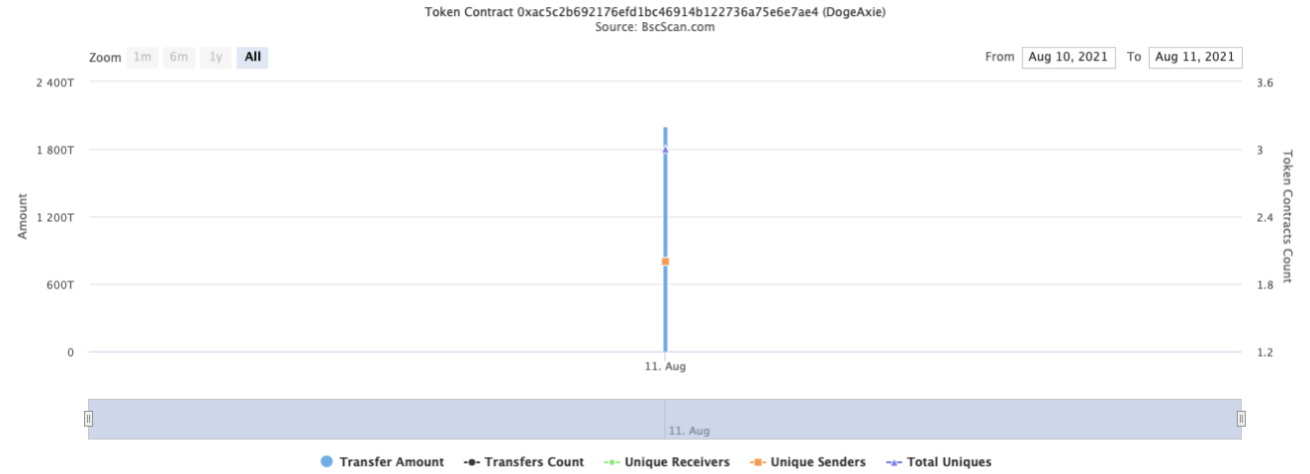


(A total of 1,000,000,000,000,000.00 tokens held by the top 100 accounts from the total supply of 1,000,000,000,000,000.00 token)

BASE3 Contract Interaction Details

Time Series: Token Contract Overview

Wed 11, Aug 2021 - Wed 11, Aug 2021



BASE3 Top 10 Token Holders

Rank	Address	Quantity (Token)	Percentage
1	0xbfc6d49e7bee26e06c8f5c1886fd4c99554c93e9	1,000,000,000,000,000	100.0000%

Contract functions details

+ [Int] IDividendDistributor
  - [Ext] setDistributionCriteria #
  - [Ext] setShare #
  - [Ext] deposit #
  - [Ext] process #
  - [Ext] processManually #

+ [Lib] Address
  - [Int] isContract
  - [Int] sendValue #
  - [Int] functionCall #
  - [Int] functionCall #
  - [Int] functionCallWithValue #
  - [Int] functionCallWithValue #
  - [Prv] _functionCallWithValue #

+ [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

+ Context
  - [Int] _msgSender
  - [Int] _msgData

+ Ownable (Context)
  - [Pub] <Constructor> #
  - [Pub] owner
  - [Pub] renounceOwnership #
    - modifiers: onlyOwner
  - [Pub] transferOwnership #
    - modifiers: onlyOwner
  - [Pub] geUnlockTime
  - [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] mint #
- [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 #

+ DividendDistributor (IDividendDistributor)
- [Pub] <Constructor> #
- [Ext] setDistributionCriteria #
  - modifiers: onlyToken
- [Ext] setShare #
  - modifiers: onlyToken
- [Ext] deposit #
  - modifiers: onlyToken
- [Ext] process #
  - modifiers: onlyToken
- [Ext] processManually #
  - modifiers: onlyToken
- [Int] shouldDistribute
- [Int] distributeDividend #
- [Ext] claimDividend #
- [Pub] getUnpaidEarnings
- [Int] getCumulativeDividends
- [Int] addShareholder #
- [Int] removeShareholder #
- [Ext] setAxieinfinityAddress #
  - modifiers: onlyToken
- [Ext] <Fallback> ($)

+ DogeAxie (IERC20, Context, Ownable)
- [Pub] <Constructor> #
- [Ext] <Fallback> ($)
- [Ext] totalSupply
- [Pub] balanceOf
- [Ext] allowance
- [Pub] name
- [Pub] symbol
- [Pub] decimals
- [Pub] approve #
- [Ext] approveMax #
- [Ext] transfer #
- [Ext] transferFrom #
- [Int] _transferFrom #
- [Int] handleTransferBody #
- [Int] _basicTransfer #
- [Int] shouldTakeFee
- [Int] takeFee #
- [Int] shouldSwapBack
- [Int] swapBack #
  - modifiers: swapping

- [Int] transferToDistributorAndMarketing #
- [Int] shouldAutoBuyback
- [Int] triggerAutoBuyback #
- [Int] buyTokens #
  - modifiers: swapping
- [Pub] manuallyProcessDividends #
- [Ext] setFees #
  - modifiers: onlyOwner
- [Ext] setIsFeeExempt #
  - modifiers: onlyOwner
- [Ext] setIsTxLimitExempt #
  - modifiers: onlyOwner
- [Ext] getIsFeeExempt
- [Ext] getIsDividendExempt
- [Ext] getIsTxLimitExempt
- [Ext] setFeeReceivers #
  - modifiers: onlyOwner
- [Ext] setAutoBuybackSettings #
  - modifiers: onlyOwner
- [Ext] setSwapBackSettings #
  - modifiers: onlyOwner
- [Ext] setTargetLiquidity #
  - modifiers: onlyOwner
- [Ext] setDistributionCriteria #
  - modifiers: onlyOwner
- [Ext] setDistributorGas #
  - modifiers: onlyOwner
- [Ext] setTxLimit #
  - modifiers: onlyOwner
- [Ext] setIsDividendExempt #
  - modifiers: onlyOwner
- [Pub] triggerVaultBuyback #
  - modifiers: onlyOwner
- [Pub] setAllowTransferToMarketing #
  - modifiers: onlyOwner
- [Pub] setBuyingFee #
  - modifiers: onlyOwner
- [Pub] setDexRouter #
  - modifiers: onlyOwner
- [Pub] setAutoBuyBack #
  - modifiers: onlyOwner
- [Pub] setSafemoonContractAddress #
  - modifiers: onlyOwner
- [Pub] getBNBQuantityInContract
- [Pub] getTotalFee
- [Pub] getCirculatingSupply
- [Pub] isOverLiquified
- [Ext] getDistributorAddress

($) = 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.	Medium 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

1. Manual processing

Issue:

- The function `processManually()` that could be called only by the owner resets currentIndex value to 0.

Recommendation:
Do not reset currentIndex even if process distribution manually.

Low Severity Issues

2. Wrong value addition

Issue:

- The function `transferToDistributorAndMarketing()` adds marketingBNB instead of distributorBNB to totalBNBAxieinfinityReflections if deposit is succes.

Recommendation:
Add distributorBNB.

3. Manual processing

Issue:

- The function `processManually()` uses loop to distribute dividends. Function will be aborted with `OUT_OF_GAS` exception if there will be a long shareholders list.

Notes:

- In _transferFrom function there is only swapBack or autoBuyBack or auto dividend distribution available, not all of them at once. So, if owner will not switch active mode some part of the contract won't work.

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

- Owner can change fees.
- Owner can include in and exclude from fee and transaction amount.
- Owner can change fee receivers.
- Owner can change auto buyback settings.
- Owner can change swap back settings.
- Owner can change target liquidity values.
- Owner can change distribution criteria.
- Owner can change distribution GAS.
- Owner can change the maximum transaction amount.
- Owner can include in and exclude from dividends.
- Owner can manually buyback tokens.
- Owner can allow transferring to marketing.
- Owner can change total buy fee.
- Owner can change Dex router.
- Owner can enable/disable buyback.
- Owner can change Axieinfinity address.

Conclusion

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

Liquidity locking details 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.