



TechRate
AUDIT COMPANY

Smart Contract Security Audit

TechRate

July, 2021

Audit Details



Audited project

Mini Doge Pro



Deployer address

0xB2836a011a3F883eA65A19d72756B04A0CF8cA38



Client contacts:

Mini Doge Pro team



Blockchain

Binance Smart Chain



Project website:

<https://dogeback.finance/>

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 Mini Doge Pro to perform an audit of smart contracts:

<https://bscscan.com/address/0x305DdF199398E308A59fb9EBC623c0AA2058ee91#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 19.07.2021

Contract name	Mini Doge Pro
Contract address	0x305DdF199398E308A59fb9EBC623c0AA2058ee91
Total supply	1,100,000,000,000,000
Token ticker	MINIDOGEPRO
Decimals	9
Token holders	6
Transactions count	11
Top 100 holders dominance	100.00%
Liquidity fee	6
Total sell fees	18
Total buy fees	12
Uniswap V2 pair	0x4ccc7649c77b1361c0a82d31a4ec33fc45a81c08
Contract deployer address	0xB2836a011a3F883eA65A19d72756B04A0CF8cA38
Contract's current owner address	0xef7d5bb1b3b9e8b822b8781cbe34d92ffcc58067

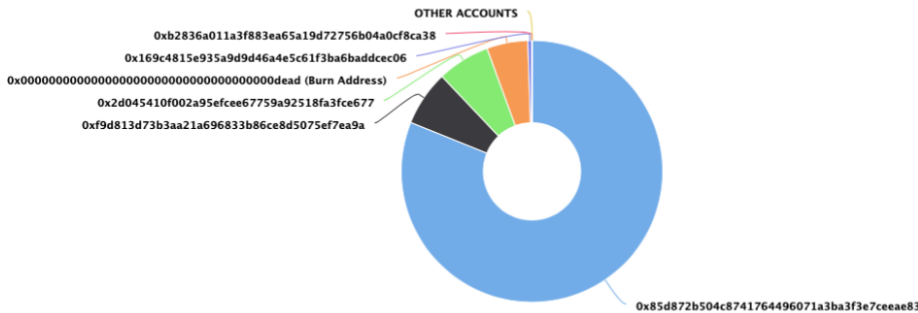
Mini Doge Pro Token Distribution

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

Token Total Supply: 1,100,000,000,000,000.00 Token | Total Token Holders: 6

Mini Doge Pro Top 100 Token Holders

Source: BscScan.com



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

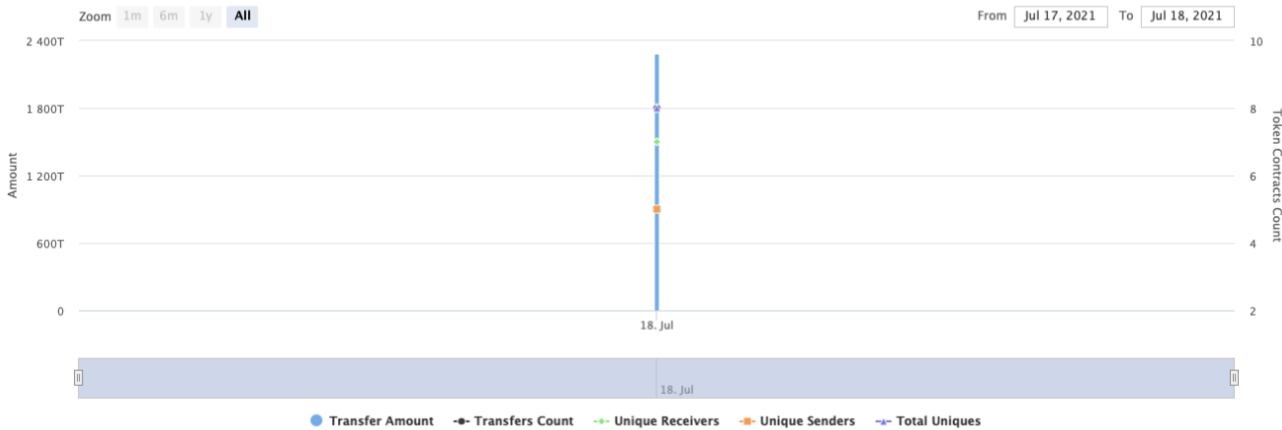
Mini Doge Pro Contract Interaction Details

Time Series: Token Contract Overview



Sun 18, Jul 2021 - Sun 18, Jul 2021

Token Contract 0x305DdF199398E308A59fb9EBC623c0AA2058ee91 (Mini Doge Pro)

Source: BscScan.com



Mini Doge Pro Top 10 Token Holders

Rank	Address	Quantity (Token)	Percentage
1	 0x85d872b504c8741764496071a3ba3f3e7ceae83	892,080,000,000,001	81.0982%
2	0xf9d813d73b3aa21a696833b86ce8d5075ef7ea9a	75,000,000,000,000	6.8182%
3	 0x2d045410f002a95efcee67759a92518fa3fce677	71,500,000,000,000	6.5000%
4	Burn Address	55,919,999,999,998	5.0836%
5	0x169c4815e935a9d9d46a4e5c61f3ba6baddcec06	5,500,000,000,000	0.5000%
6	0xb2836a011a3f883ea65a19d72756b04a0cf8ca38	1	0.0000%



Contract functions details

+ Context

- [Int] _msgSender
- [Int] _msgData

+ Ownable (Context)

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

+ [Int] IERC20

- [Ext] totalSupply
- [Ext] balanceOf
- [Ext] transfer #
- [Ext] allowance
- [Ext] approve #
- [Ext] transferFrom #

+ ERC20 (Context, IERC20)

- [Pub] <Constructor> #
- [Pub] name
- [Pub] symbol
- [Pub] decimals
- [Pub] totalSupply
- [Pub] balanceOf
- [Pub] transfer #
- [Pub] allowance
- [Pub] approve #
- [Pub] transferFrom #
- [Pub] increaseAllowance #
- [Pub] decreaseAllowance #
- [Int] _transfer #
- [Int] _mint #
- [Int] _burn #
- [Int] _approve #
- [Int] _setupDecimals #
- [Int] _beforeTokenTransfer #

+ [Int] IDividendPayingToken

- [Ext] dividendOf
- [Ext] distributeDividends (\$)
- [Ext] withdrawDividend #

+ [Int] IDividendPayingTokenOptional

- [Ext] withdrawableDividendOf
- [Ext] withdrawnDividendOf
- [Ext] accumulativeDividendOf

+ DividendPayingToken (ERC20, IDividendPayingToken, IDividendPayingTokenOptional)

- [Pub] <Constructor> #
 - modifiers: ERC20
- [Ext] <Fallback> (\$)
- [Pub] distributeDividends (\$)
- [Int] _distributeDividends #
- [Pub] withdrawDividend #
- [Int] _setDividendTokenAddress #
- [Int] _resetDividendsOfUser #
- [Int] _withdrawDividendOfUser #
- [Pub] dividendOf
- [Pub] withdrawableDividendOf
- [Pub] withdrawnDividendOf
- [Pub] accumulativeDividendOf
- [Int] _transfer #
- [Int] _mint #
- [Int] _burn #
- [Int] _setBalance #

+ [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 #
- + [Lib] IterableMapping
 - [Pub] get
 - [Pub] getIndexOfKey
 - [Pub] getKeyAtIndex
 - [Pub] size
 - [Pub] set #
 - [Pub] remove #
- + [Lib] SafeMath
 - [Int] tryAdd
 - [Int] trySub
 - [Int] tryMul
 - [Int] tryDiv
 - [Int] tryMod
 - [Int] add
 - [Int] sub
 - [Int] mul
 - [Int] div
 - [Int] mod
 - [Int] sub
 - [Int] div
 - [Int] mod
- + [Lib] SafeMathInt
 - [Int] mul

- [Int] div
 - [Int] sub
 - [Int] add
 - [Int] toUint256Safe
- + [Lib] SafeMathUint
- [Int] toInt256Safe
- + MiniDogePro (ERC20, Ownable)
- [Pub] <Constructor> #
 - modifiers: ERC20
 - [Ext] <Fallback> (\$)
 - [Pub] whitelistDxSale #
 - modifiers: onlyOwner
 - [Ext] setMaxBuyTransaction #
 - modifiers: onlyOwner
 - [Ext] setMaxSellTransaction #
 - modifiers: onlyOwner
 - [Ext] setMaxWalletToken #
 - modifiers: onlyOwner
 - [Ext] setSwapTokensAmount #
 - modifiers: onlyOwner
 - [Ext] setMarketingDivisor #
 - modifiers: onlyOwner
 - [Ext] prepareForPreSale #
 - modifiers: onlyOwner
 - [Ext] afterPreSale #
 - modifiers: onlyOwner
 - [Pub] setTradingIsEnabled #
 - modifiers: onlyOwner
 - [Pub] setBuyBackEnabled #
 - modifiers: onlyOwner
 - [Pub] setBuyBackRandomEnabled #
 - modifiers: onlyOwner
 - [Pub] triggerBuyBack #
 - modifiers: onlyOwner
 - [Pub] updateDividendTracker #
 - modifiers: onlyOwner
 - [Pub] updateLiquidityFee #
 - modifiers: onlyOwner
 - [Pub] updateBuybackFee #
 - modifiers: onlyOwner
 - [Pub] updateUniswapV2Router #
 - modifiers: onlyOwner
 - [Pub] excludeFromFees #
 - modifiers: onlyOwner
 - [Pub] setDividendToken #
 - modifiers: onlyOwner
 - [Pub] excludeMultipleAccountsFromFees #
 - modifiers: onlyOwner
 - [Pub] setAutomatedMarketMakerPair #
 - modifiers: onlyOwner
 - [Priv] _setAutomatedMarketMakerPair #
 - [Pub] updateBuyBackWallet #
 - modifiers: onlyOwner

- [Pub] updateGasForProcessing #
 - modifiers: onlyOwner
- [Ext] updateClaimWait #
 - modifiers: onlyOwner
- [Ext] getClaimWait
- [Ext] getTotalDividendsDistributed
- [Pub] isExcludedFromFees
- [Pub] withdrawableDividendOf
- [Pub] dividendTokenBalanceOf
- [Ext] getAccountDividendsInfo
- [Ext] getAccountDividendsInfoAtIndex
- [Ext] processDividendTracker #
- [Ext] claim #
- [Ext] getLastProcessedIndex
- [Ext] getNumberOfDividendTokenHolders
- [Int] _transfer #
- [Prv] swapTokensForBNB #
- [Prv] swapBNBForTokens #
- [Prv] swapTokensForDividendToken #
- [Prv] swapAndSendDividends #
- [Prv] swapAndSendDividendsInBNB #
- [Prv] transferToBuyBackWallet #
- [Ext] transferToMarketWallet #
 - modifiers: onlyOwner
- [Prv] removeAllFee #
- [Prv] restoreAllFee #
- [Ext] setTaxFeePercent #
 - modifiers: onlyOwner
- [Ext] setBuyFee #
 - modifiers: onlyOwner
- [Ext] setSellFee #
 - modifiers: onlyOwner
- [Ext] setLiquidityFeePercent #
 - modifiers: onlyOwner
- [Ext] excludeFromDividends #
 - modifiers: onlyOwner

+ MiniDogeProDividendTracker (DividendPayingToken, Ownable)

- [Pub] <Constructor> #
 - modifiers: DividendPayingToken
- [Int] _transfer
- [Pub] withdrawDividend
- [Ext] excludeFromDividends #
 - modifiers: onlyOwner
- [Ext] updateClaimWait #
 - modifiers: onlyOwner
- [Ext] getLastProcessedIndex
- [Ext] getNumberOfTokenHolders
- [Pub] getAccount
- [Pub] getAccountAtIndex
- [Prv] canAutoClaim
- [Ext] setBalance #
 - modifiers: onlyOwner
- [Pub] process #
- [Pub] processAccount #

- modifiers: onlyOwner
- **[Pub]** setDividendToken #
 - modifiers: onlyOwner
- **[Pub]** distributeDividends #
 - 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:

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

Recommendation:

Do division after multiplication.

Notes:

- Owner can change dividend tracker that could be not audited and some functions may work in different ways.
- In swap part of the transaction, 40% of contract balance goes to `buyBackAddress`.
- Function `distributeDividends()` may increase `magnifiedDividendPerShare` not in `dividentTracker` proportion(In case when `dividentTracker` not equal to BNB).

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

- Owner can change max buy and sell transaction amounts and fees.
- Owner can change max wallet token number.
- Owner can enable and disable trading.
- Owner can enable and disable random buyback(not used).
- Owner can manually do buyback.
- Owner can change dividendTracker.
- Owner can change buyBack and liquidity fees.
- Owner can change Uniswap router.
- Owner can change dividend token(resets all dividends).
- Owner can exclude and include addresses in automatedMarketMakerPairs array.
- Owner can change buyback wallet address.
- Owner can change gas for processing.
- Owner can update claimWait value.
- Owner can withdraw all BNBs from the contract.
- Owner can exclude from the fee.
- Owner can change marketingDivisor.
- Owner can enable and disable buyBack.
- Owner can enable before and after presale modes.
- Owner can exclude from dividends.
- Owner can change swapTokensAtAmount value.

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 provided by the team:

https://dxsale.app/app/v2_9/defipresale?saleID=1341&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.