Smart Contract Security Audit

TechRate

August, 2021

Audit Details

Audited project

Mother of Memes

Deployer address

0x47dF0bC77958005c955d884563B8672914DB2f37

Client contacts:

Mother of Memes team

Blockchain

Binance Smart Chain

Project website:

https://momtoken.io/

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 Mother of Memes to perform an audit of smart contracts:

https://bscscan.com/address/0x211fa9e7e390c29b0ab1a9248949a0ab716c4154#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 03.08.2021

|	
Contract name	Mother of Memes
Contract address	0x211Fa9E7E390c29B0AB1a9248949A0aB716c4154
Total supply	100,000,000,000,000,000
Token ticker	MOM
Decimals	9
Token holders	1
Transactions count	2
Top 100 holders dominance	100.00%
Liquidity fee	2
Tax holder fee	1
Total fees	0
Fee beneficiary	0x2f86c4cbd561ba58ce8e093c6de0f64f7e8b5162
Contract deployer address	0x47dF0bC77958005c955d884563B8672914DB2f37
Contract's current owner address	0x6d5243b940d4e9143acd9021b878f599879e42bb

Mother of Memes Token Distribution

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

Mother of Memes Top 100 Token Holders
Source: BscScan.com

OTHER ACCOUNTS

0x6d5243b940d4e9143acd9021b878f599879e42bb
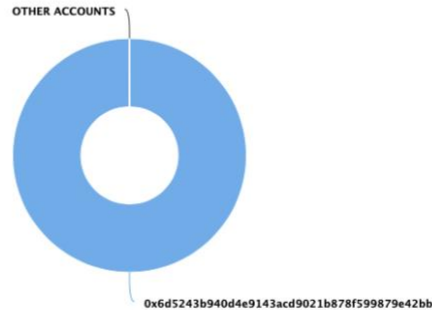
(A total of 100,000,000,000,000,000.00 tokens held by the top 100 accounts from the total supply of 100,000,000,000,000,000.00 token)

Mother of Memes Contract Interaction Details

Time Series: Token Contract Overview   Thu 8, Jul 2021 - Thu 8, Jul 2021

Token Contract 0x211fa9e7e390c29b0ab1a9248949a0ab716c4154 (Mother of Memes)
Source: BscScan.com

Zoom 1m 6m 1y All   From Jul 7, 2021   To   Jul 8, 2021

● Transfer Amount   -●- Transfers Count   -●- Unique Receivers   -●- Unique Senders   -▲- Total Uniques

Mother of Memes Top 10 Token Holders

Rank	Address	Quantity (Token)	Percent
1.	0x6d5243b940d4e9143acd9021b878f599879e42bb	100,000,000,000,000,000	100.0000%

Contract functions details

+ [Int] IBEP20
- **[Ext]** totalSupply
- **[Ext]** balanceOf
- **[Ext]** transfer **#**
- **[Ext]** allowance
- **[Ext]** approve **#**
- **[Ext]** transferFrom **#**

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

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

+ [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

+ [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 **#**

+ [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 **#**

+ AbstractDeflationaryToken (Context, IBEP20, Ownable)
- **[Pub]** <Constructor> **#**
- **[Ext]** name
- **[Ext]** symbol

- **[Ext]** decimals
- **[Ext]** totalSupply
- **[Ext]** transfer **#**
- **[Ext]** allowance
- **[Ext]** approve **#**
- **[Ext]** transferFrom **#**
- **[Ext]** increaseAllowance **#**
- **[Ext]** decreaseAllowance **#**
- **[Ext]** isExcludedFromReward
- **[Ext]** isExcludedFromFee
- **[Ext]** totalFees
- **[Ext]** deliver **#**
- **[Ext]** excludeFromFee **#**
  - modifiers: onlyOwner
- **[Ext]** includeInFee **#**
  - modifiers: onlyOwner
- **[Ext]** setTaxHolderFeePercent **#**
  - modifiers: onlyOwner
- **[Ext]** setMaxTxPercent **#**
  - modifiers: onlyOwner
- **[Pub]** excludeFromReward **#**
  - modifiers: onlyOwner
- **[Pub]** includeInReward **#**
  - modifiers: onlyOwner
- **[Pub]** balanceOf
- **[Pub]** reflectionFromToken
- **[Pub]** tokenFromReflection
- **[Int]** _reflectHolderFee **#**
- **[Int]** _getRate
- **[Int]** _approve **#**
- **[Int]** _getFeesArray
- **[Int]** _getTransferAmount
- **[Int]** _recalculateRewardPool **#**
- **[Int]** _transfer **#**
- **[Int]** _tokenTransfer **#**

+ AbstractBurnableDeflToken (AbstractDeflationaryToken)
- **[Ext]** burn **#**

+ AbstractDeflationaryAutoLPToken (AbstractDeflationaryToken)
- **[Pub]** <Constructor> **#**
  - modifiers: AbstractDeflationaryToken
- **[Ext]** <Fallback> **($)**
- **[Ext]** setLiquidityFeePercent **#**
  - modifiers: onlyOwner
- **[Ext]** setNumTokensSellToAddToLiquidity **#**
  - modifiers: onlyOwner
- **[Ext]** setSwapAndLiquifyEnabled **#**
  - modifiers: onlyOwner
- **[Ext]** setLiquidityOwner **#**
  - modifiers: onlyOwner
- **[Int]** _takeLiquidity **#**
- **[Int]** _getTransferAmount
- **[Int]** _recalculateRewardPool **#**
- **[Int]** _transfer **#**

- [Int] _swapAndLiquify #
- [Int] _swapTokensForEth #
- [Int] _addLiquidity #
- [Int] _getFeesArray
- [Int] _tokenTransfer #

+ **DeflationaryAutoLPToken** (AbstractDeflationaryAutoLPToken)
  - **[Pub]** \<Constructor\> #
    - modifiers: AbstractDeflationaryAutoLPToken
  - **[Ext]** withdrawStuckFunds #
    - modifiers: onlyOwner
  - [Int] _swapAndLiquify #
    - modifiers: lockTheSwap
  - [Int] _swapTokensForEth #
  - [Int] _addLiquidity #

+ **FeeToAddress** (Ownable)
  - **[Ext]** setToAddressFee #
    - modifiers: onlyOwner
  - **[Ext]** setFeeBeneficiary #
    - modifiers: onlyOwner

+ **FeeToAddrDeflAutoLPToken** (DeflationaryAutoLPToken, FeeToAddress)
  - **[Pub]** \<Constructor\> #
    - modifiers: DeflationaryAutoLPToken
  - [Int] _getFeesArray
  - [Int] _tokenTransfer #

+ **MOM** (FeeToAddrDeflAutoLPToken, AbstractBurnableDeflToken)
  - **[Pub]** \<Constructor\> #
    - modifiers: FeeToAddrDeflAutoLPToken
  - **[Ext]** totalSupply

($) = 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.	Low 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

No medium severity issues found.

✓ Low Severity Issues

1. Fee taking

Issue:

- Due to the commits, if any of account is excluded from fee, fee won't be taken. But takeFee expression has logical AND instead of logical OR.

Recommendation:
Check logic of fee taking in transfer function and correct issue if needed.

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

- Owner can change the tax and liquidity fee.
- Owner can exclude from fee.
- Owner can change _taxHolderFee value.
- Owner can change max transaction amount.
- Owner can change liquidity fee.
- Owner can change number of tokens to add to liquidity.
- Owner can change liquidity owner.
- Owner can withdraw contract BNBs.
- Owner can change feeToAddress percent.
- Owner can change feeBeneficiary.

Conclusion

Smart contracts contain low 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.

Techrate1   Techrate   Techrate_audits