TechRate
AUDIT COMPANY

Smart Contract Security Audit

TechRate

August, 2021

Audit Details

Audited project

Maka

Deployer address

0x4078b2228f80ca39116454de2e60103324e9434b

Client contacts:

Maka team

Blockchain

Binance Smart Chain

Project website:

https://maka.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 Maka to perform an audit of smart contracts:

https://bscscan.com/address/0x75b429A3D699e6E711BDBC8C0d00cca6a6da4CfE#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.
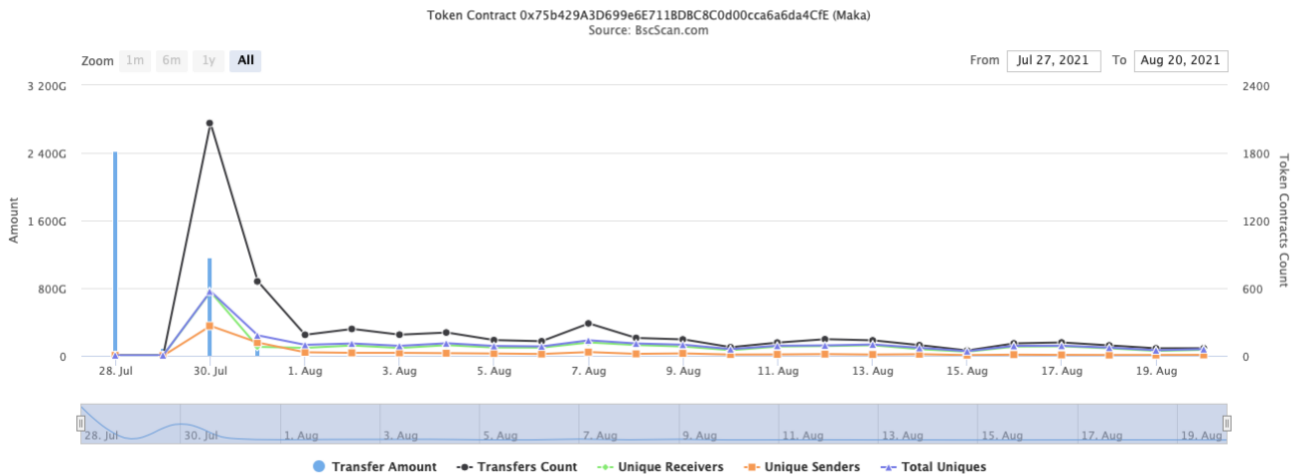
Contracts Details

Token contract details for 21.08.2021

Contract name	Maka
Contract address	0x75b429A3D699e6E711BDBC8C0d00cca6a6da4CfE
Total supply	1,000,000,000,000
Token ticker	MAKA
Decimals	9
Token holders	312
Transactions count	5,493
Top 100 holders dominance	98.28%
Reward cycle period	86400
Global reward dampening %	6
Auto liquidity wallet	0x4078b2228f80ca39116454de2e60103324e9434b
Pancake V2 pair	0x7953d870e3d85704a089b8bac8cbdd2b944d17c6
Contract deployer address	0x4078b2228f80ca39116454de2e60103324e9434b
Contract's current owner address	0x4078b2228f80ca39116454de2e60103324e9434b

Maka Token Distribution

Maka Top 100 Token Holders
Source: BscScan.com

OTHER ACCOUNTS

0x0000000000000000000000000000000000000dead (Burn Address)

0xcb88f9fa672311fe95a5a8b5965ca725b4f78707
0x2b526834d3294520d838fdd0e3af56cc6b90bfb7
0x4a4f289196cdc54aaba35c864b961d44f503693d
0x65dc60b5872d066144e451c4a1988874e62f40d4
0x1e2d3969fb5f19fd3eec493eaf58dabd76ecddc8
0x72556b09a73d22067502f125110b168a16190b97
0xbb75ae519f5d5d4389be505b40f32d1d25ae729e
0x75b429a3d699e6e711bdbc8c0d00cca6a6da4cfe
(Maka Finance: MAKA Token)
0x3f4d6bf08cb7a003488ef082102c2e6418a4551e

0x7953d870e3d85704a089b8bac8cbdd2b944d17c6
(PancakeSwap V2: MAKA 8)
0x78a5cae394b1707ce55b0c67788a0cf2427deb30

(A total of 982,794,226,921.69 tokens held by the top 100 accounts from the total supply of 1,000,000,000,000.00 token)

Maka Contract Interaction Details

Time Series: Token Contract Overview   Wed 28, Jul 2021 - Fri 20, Aug 2021

Token Contract 0x75b429A3D699e6E711BDBC8C0d00cca6a6da4CfE (Maka)
Source: BscScan.com

Zoom 1m 6m 1y All   From Jul 27, 2021 To Aug 20, 2021

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

Maka Top 10 Token Holders

Rank	Address	Quantity (Token)	Percentage
1	Burn Address	300,005,513,792.777761381	30.0006%
2	PancakeSwap V2: MAKA 8	143,009,950,240.148032878	14.3010%
3	0x78a5cae394b1707ce55b0c67788a0cf2427deb30	66,035,986,478.399612776	6.6036%
4	0x3f4d6bf08cb7a003488ef082102c2e6418a4551e	62,755,999,999	6.2756%
5	Maka Finance: MAKA Token	40,770,758,507.125103171	4.0771%
6	0xbb75ae519f5d5d4389be505b40f32d1d25ae729e	32,315,470,725.999999714	3.2315%
7	0x72556b09a73d22067502f125110b168a16190b97	28,000,000,000	2.8000%
8	0x1e2d3969fb5f19fd3eec493eaf58dabd76ecddc8	21,538,227,479.368062236	2.1538%
9	0x65dc60b5872d066144e451c4a1988874e62f40d4	18,555,275,292.600630047	1.8555%
10	0x4a4f289196cdc54aaba35c864b961d44f503693d	18,210,074,025.000000013	1.8210%

Contract functions details

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

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

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

+ [Int] IERC20Metadata (IERC20)
  - **[Ext]** name
  - **[Ext]** symbol
  - **[Ext]** decimals

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

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

+ ReentrancyGuard
- **[Pub]** <Constructor> #

+ MakaBase (Context, IERC20Metadata, Ownable, ReentrancyGuard)
- **[Pub]** <Constructor> #
- **[Pub]** presale #
  - modifiers: onlyOwner
- **[Pub]** activate #
  - modifiers: onlyOwner
- [Int] onActivated #
- **[Pub]** balanceOf
- **[Pub]** transfer #
- **[Pub]** transferFrom #
- **[Pub]** approve #
- [Int] doTransfer #
- [Int] onBeforeTransfer #
- [Int] onTransfer #
- **[Prv]** updateBalances #
- **[Prv]** doApprove #
- **[Prv]** calculateFeeRate
- **[Prv]** executeSwapIfNeeded #
- **[Prv]** executeSwap #
- [Int] swapTokensForBNB #
- [Int] swapBNBForTokens #
- [Int] swapBNBForBusd #
- **[Prv]** isTransferLimited
- **[Prv]** isSwapTransfer
- [Int] isMarketTransfer
- **[Pub]** amountUntilSwap
- **[Pub]** increaseAllowance #
- **[Pub]** decreaseAllowance #
- **[Pub]** setPancakeSwapRouter #
  - modifiers: onlyOwner
- [Int] onPancakeSwapRouterUpdated #
- [Int] isPancakeSwapPair
- **[Pub]** setFees #
  - modifiers: onlyOwner
- **[Pub]** setTransactionLimit #
  - modifiers: onlyOwner
- **[Pub]** transactionLimit
- **[Pub]** setTokenSwapThreshold #
  - modifiers: onlyOwner
- **[Pub]** tokenSwapThreshold
- **[Pub]** name
- **[Pub]** symbol

- [Pub] totalSupply
- [Pub] decimals
- [Pub] allowance
- [Pub] pancakeSwapRouterAddress
- [Pub] pancakeSwapPairAddress
- [Pub] autoLiquidityWallet
- [Pub] setAutoLiquidityWallet #
  - modifiers: onlyOwner
- [Pub] totalFeesPooled
- [Pub] totalBNBLiquidityAddedFromFees
- [Pub] isSwapEnabled
- [Pub] setSwapEnabled #
  - modifiers: onlyOwner
- [Pub] isFeeEnabled
- [Pub] setFeeEnabled #
  - modifiers: onlyOwner
- [Pub] isExcludedFromFees
- [Pub] setExcludedFromFees #
  - modifiers: onlyOwner
- [Pub] activateBuying #
  - modifiers: onlyOwner
- [Ext] <Fallback> ($)

+ Maka (MakaBase)
  - [Pub] <Constructor> #
    - modifiers: MakaBase
  - [Int] onActivated #
  - [Int] onBeforeTransfer #
  - [Int] onTransfer #
  - [Prv] processGradualBurn #
  - [Prv] updateAutoClaimQueue #
  - [Ext] claimReward #
    - modifiers: isHuman,nonReentrant
  - [Pub] claimReward #
  - [Prv] doClaimReward #
  - [Prv] claimBNB #
  - [Prv] claimMaka #
  - [Prv] claimBusd #
  - [Pub] processRewardClaimQueue #
  - [Ext] processRewardClaimQueueAndRefundGas #
  - [Pub] isRewardReady
  - [Pub] isIncludedInRewards
  - [Pub] calculateRewardCycleExtension
  - [Pub] calculateClaimRewards
  - [Pub] calculateBNBReward
  - [Int] onPancakeSwapRouterUpdated #
  - [Int] isMarketTransfer
  - [Prv] isBurnTransfer
  - [Pub] shouldBurn
  - [Ext] buyAndBurn #
    - modifiers: onlyOwner
  - [Prv] doBuyAndBurn #
  - [Pub] isContract
  - [Pub] totalAmountOfTokensHeld
  - [Pub] bnbRewardClaimed

- **[Pub]** bnbRewardClaimedAsBusd
- **[Pub]** bnbRewardClaimedAsMaka
- **[Pub]** totalBNBClaimed
- **[Pub]** totalBNBClaimedAsMaka
- **[Pub]** totalBNBClaimedAsBusd
- **[Pub]** rewardCyclePeriod
- **[Pub]** setRewardCyclePeriod **#**
  - modifiers: onlyOwner
- **[Pub]** setRewardCycleExtensionThreshold **#**
  - modifiers: onlyOwner
- **[Pub]** nextAvailableClaimDate
- **[Pub]** maxClaimAllowed
- **[Pub]** setMaxClaimAllowed **#**
  - modifiers: onlyOwner
- **[Pub]** minRewardBalance
- **[Pub]** setMinRewardBalance **#**
  - modifiers: onlyOwner
- **[Pub]** maxGasForAutoClaim
- **[Pub]** setMaxGasForAutoClaim **#**
  - modifiers: onlyOwner
- **[Pub]** isAutoClaimEnabled
- **[Pub]** setAutoClaimEnabled **#**
  - modifiers: onlyOwner
- **[Pub]** isExcludedFromRewards
- **[Pub]** setExcludedFromRewards **#**
  - modifiers: onlyOwner
- **[Pub]** globalRewardDampeningPercentage
- **[Pub]** setGlobalRewardDampeningPercentage **#**
  - modifiers: onlyOwner
- **[Pub]** approveClaim **#**
- **[Pub]** isClaimApproved
- **[Pub]** isRewardAsTokensEnabled
- **[Pub]** setRewardAsTokensEnabled **#**
  - modifiers: onlyOwner
- **[Pub]** gradualBurnMagnitude
- **[Pub]** setGradualBurnMagnitude **#**
  - modifiers: onlyOwner
- **[Pub]** gradualBurnTimespan
- **[Pub]** setGradualBurnTimespan **#**
  - modifiers: onlyOwner
- **[Pub]** minBnbPoolSizeBeforeBurn
- **[Pub]** setMinBnbPoolSizeBeforeBurn **#**
  - modifiers: onlyOwner
- **[Pub]** claimRewardAsBnbPercentage
- **[Pub]** claimRewardAsBusdPercentage
- **[Pub]** claimRewardAsMakaPercentage
- **[Pub]** setClaimRewardPercentage **#**
- **[Pub]** mainBnbPoolSize
- **[Pub]** setMainBnbPoolSize **#**
  - modifiers: onlyOwner
- **[Pub]** isInRewardClaimQueue
- **[Pub]** reimburseAfterMakaClaimFailure
- **[Pub]** setReimburseAfterMakaClaimFailure **#**
  - modifiers: onlyOwner
- **[Pub]** lastBurnDate

- **[Pub]** rewardClaimQueueLength
- **[Pub]** rewardClaimQueueIndex
- **[Pub]** isWhitelistedExternalProcessor
- **[Pub]** setWhitelistedExternalProcessor **#**
  - modifiers: onlyOwner
- **[Pub]** setSendWeiGasLimit **#**
  - modifiers: onlyOwner
- **[Pub]** setExcludeNonHumansFromRewards **#**
  - 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.	Low issues
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

1. Reentrancy

Issue:

- The function claimReward() marked nonReentrant but function claimReward(address user) is also accessible but not nonReentrant.

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

- Owner can run presale and activate presets.
- Owner can change Pancake router.
- Owner can change fees.
- Owner can change _transactionLimit and _tokenSwapThreshold.
- Owner can change auto liquidity wallet address.
- Owner can disable/enable swap and fees.
- Owner can activate buying.
- Owner can manually buy&burn.
- Owner can change _rewardCyclePeriod and _rewardCycleExtensionThreshold.
- Owner can change max claim allowed
- Owner can change min reward balance.
- Owner can exclude from the fees.
- Owner can change max gas for autoclaim.
- Owner can enable/disable autoclaim.
- Owner can exclude from rewards.
- Owner can change _globalRewardDampeningPercentage.
- Owner can change _rewardAsTokensEnabled.
- Owner can change _gradualBurnMagnitude and _gradualBurnTimespan.
- Owner can change min BNB pool before burn.
- Owner can change main BNB pool size.
- Owner can change _reimburseAfterMakaClaimFailure.
- Owner can add _whitelistedExternalProcessors addresses.
- Owner can change _sendWeiGasLimit value.
- Owner can change _excludeNonHumansFromRewards restriction.

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 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.