Techrate1 Techrate

TechRate

AUDIT COMPANY

Smart Contract Security Audit

TechRate

February, 2022

Audit Details

Audited project

Meta Club

Deployer address

0x54496512484413 6aada4d67e841b4eb4742fe7f2

Client contacts:

Meta Club team

Blockchain

Binance Smart Chain

Project website:

https://metaclubtoken.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 Meta Club to perform an audit of smart contracts:
https://bscscan.com/address/0xae01ac36deb43ec2593855e35f5e62dc992d7c95#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

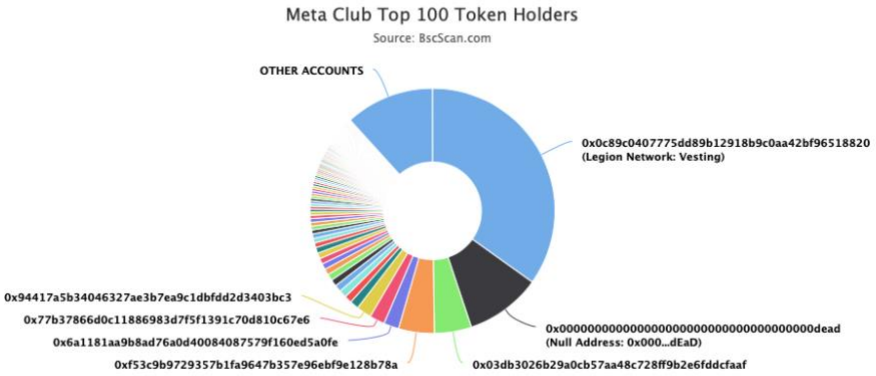
Token contract details for 16.02.2022

Contract name	Meta Club
Contract address	0xAE01Ac36DEb43eC2593855e35f5E62Dc992d7c95
Total supply	1,000,000,000
Token ticker	CLUB
Decimals	9
Token holders	1,384
Transactions count	15,880
Top 100 holders dominance	88.26%
Total tax selling	12
Total tax buying	12
Marketing wallet address	0x03db3026b29a0cb57aa48c728ff9b2e6fddcfaaf
Uniswap V2 pair	0xf53c9b9729357b1fa9647b357e96ebf9e128b78a
Contract deployer address	0x544965124844136aada4d67e841b4eb4742fe7f2
Contract's current owner address	0x544965124844136aada4d67e841b4eb4742fe7f2

Meta Club Token Distribution

The top 100 holders collectively own 88.26% (882,635,640.59 Tokens) of Meta Club

Token Total Supply: 1,000,000,000.00 Token | Total Token Holders: 1,384

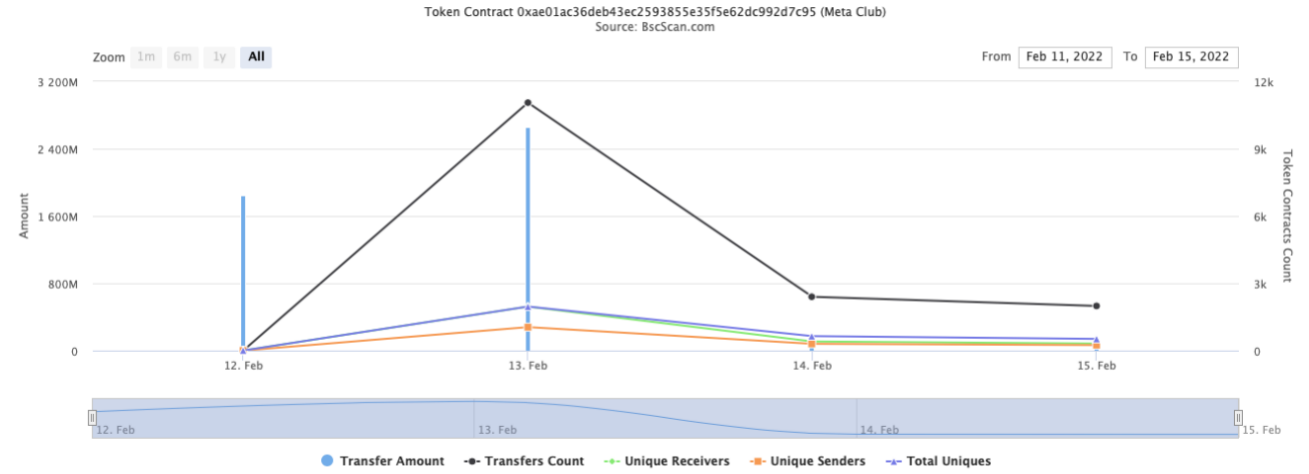


(A total of 882,635,640.59 tokens held by the top 100 accounts from the total supply of 1,000,000,000.00 token)

Meta Club Contract Interaction Details

Time Series: Token Contract Overview

Sat 12, Feb 2022 - Tue 15, Feb 2022



Meta Club Top 10 Token Holders

Rank	Address	Quantity (Token)	Percentage
1	Legion Network: Vesting	348,632,812.176367188	34.8633%
2	Null Address: 0x000...dEaD	100,000,000	10.0000%
3	0x03db3026b29a0cb57aa48c728ff9b2e6fddcfaaf	49,000,000	4.9000%
4	0xf53c9b9729357b1fa9647b357e96ebf9e128b78a	47,350,623.896500701	4.7351%
5	0x6a1181aa9b8ad76a0d40084087579f160ed5a0fe	20,000,000	2.0000%
6	0x77b37866d0c11886983d7f5f1391c70d810c67e6	20,000,000	2.0000%
7	0x94417a5b34046327ae3b7ea9c1dbfdd2d3403bc3	20,000,000	2.0000%
8	0x00c1d0fcce7220580afc70c033deb8a593818d30	11,492,800	1.1493%
9	0xfc91a524a2ba437382118eed4d4021ab5aa2e8ee	10,000,000	1.0000%
10	0x14c01b079b4afaba8b229e8f567d19ac793b4ac2	10,000,000	1.0000%

Contract functions details

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

+ [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
+ [Lib] Address
  - [Int] isContract
  - [Int] sendValue #
  - [Int] functionCall #
  - [Int] functionCall #
  - [Int] functionCallWithValue #
  - [Int] functionCallWithValue #
  - [Prv] _functionCallWithValue #
+ Ownable (Context)
  - [Pub] <Constructor> #
  - [Pub] owner
  - [Pub] waiveOwnership #
    - modifiers: onlyOwner
  - [Pub] transferOwnership #
    - modifiers: onlyOwner
  - [Pub] getTime

+ [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] 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 #

+ MetaClub (Context, IERC20, Ownable)
  - [Pub] <Constructor> #
  - [Pub] name
  - [Pub] symbol
  - [Pub] decimals
  - [Pub] totalSupply

- [Pub] balanceOf
- [Pub] allowance
- [Pub] increaseAllowance #
- [Pub] decreaseAllowance #
- [Pub] minimumTokensBeforeSwapAmount
- [Pub] approve #
- [Prv] _approve #
- [Pub] setMarketPairStatus #
  - modifiers: onlyOwner
- [Ext] setIsTxLimitExempt #
  - modifiers: onlyOwner
- [Pub] setIsExcludedFromFee #
  - modifiers: onlyOwner
- [Ext] setBuyTaxes #
  - modifiers: onlyOwner
- [Ext] setSelTaxes #
  - modifiers: onlyOwner
- [Ext] setDistributionSettings #
  - modifiers: onlyOwner
- [Ext] setMaxTxAmount #
  - modifiers: onlyOwner
- [Ext] enableDisableWalletLimit #
  - modifiers: onlyOwner
- [Ext] setIsWalletLimitExempt #
  - modifiers: onlyOwner
- [Ext] setWalletLimit #
  - modifiers: onlyOwner
- [Ext] setNumTokensBeforeSwap #
  - modifiers: onlyOwner
- [Ext] setMarketingWalletAddress #
  - modifiers: onlyOwner
- [Ext] setTeamWalletAddress #
  - modifiers: onlyOwner
- [Pub] setSwapAndLiquifyEnabled #
  - modifiers: onlyOwner
- [Pub] setSwapAndLiquifyByLimitOnly #
  - modifiers: onlyOwner
- [Pub] getCirculatingSupply
- [Prv] transferToAddressETH #
- [Pub] changeRouterVersion #
  - modifiers: onlyOwner
- [Ext] <Fallback> ($)
- [Pub] transfer #
- [Pub] transferFrom #
- [Prv] _transfer #
- [Int] _basicTransfer #
- [Prv] swapAndLiquify #
  - modifiers: lockTheSwap
- [Prv] swapTokensForEth #
- [Prv] addLiquidity #
- [Int] takeFee #

($) = 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.	Low issues
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. Wrong event emitting

Issue:

- The function waiveOwnership() emits event of transferring ownership to zero address, but actually transfers owner to 0x544965124844136AaDA4d67e841b4eB4742FE7F2 address.

Recommendation:
Emit the right event.

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

- Owner can change the marketing, team and liquidity fees.
- Owner can change the maximum transaction amount.
- Owner can exclude from the fee and maxTX.
- Owner can change marketing and team wallets.
- Owner can change minimum number of tokens before swap.
- Owner can change Uniswap router address.
- Owner can change swap and liquify settings.
- Owner can include in isMarketPair array.
- Owner can enable/disable wallet limit, exclude from it and change this limit value.

Conclusion

Smart contracts contain low severity issues! Liquidity pair contract's security is not checked due to out of scope. Function setSelTaxes() has spelling mistake.

Liquidity locking details are provided by the team:
https://mudra.website/?certificate=yes&type=0&lp=0xf53c9b9729357b1fa9647b357e96ebf9e128b78a

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.