

TechRate
September, 2022



SMART CONTRACTS SECURITY AUDIT REPORT



Techrate_audits



Techrate



Techrate1

Audit Details



Audited project

Metano



Deployer address

0xbaed1a9492b6d3ca8afdfcd48551d23956eebdb6



Client contacts:

<https://twitter.com/Metanotoken>



Blockchain

Ethereum



Project website:

<https://metano.org>

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 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 Metano to perform an audit of smart contracts:

<https://etherscan.io/address/0x9D9e399e5385e2b9A58d4F775A1E16441b571afb#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 24.09.2022

Contract name Metano

Contract address 0x9D9e399e5385e2b9A58d4F775A1E16441b571afb

Total supply 10,000,000,000

Token ticker METANO

Decimals 18

Token holders 130

Transactions count 1,971

Top 100 holders dominance 99.91%

Allow trade at 1662814800

Operator 0xbaed1a9492b6d3ca8afdfcd48551d23956eebdb6

Contract deployer address 0xbaed1a9492b6d3ca8afdfcd48551d23956eebdb6

Owner address 0xbaed1a9492b6d3ca8afdfcd48551d23956eebdb6

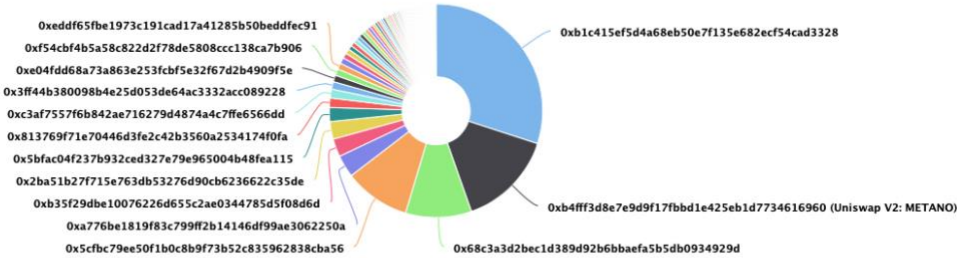
Metano Token Distribution

The top 100 holders collectively own 99.91% (9,991,224,176.33 Tokens) of METANO

Token Total Supply: 10,000,000,000.00 Token | Total Token Holders: 130

METANO Top 100 Token Holders

Source: Etherscan.io



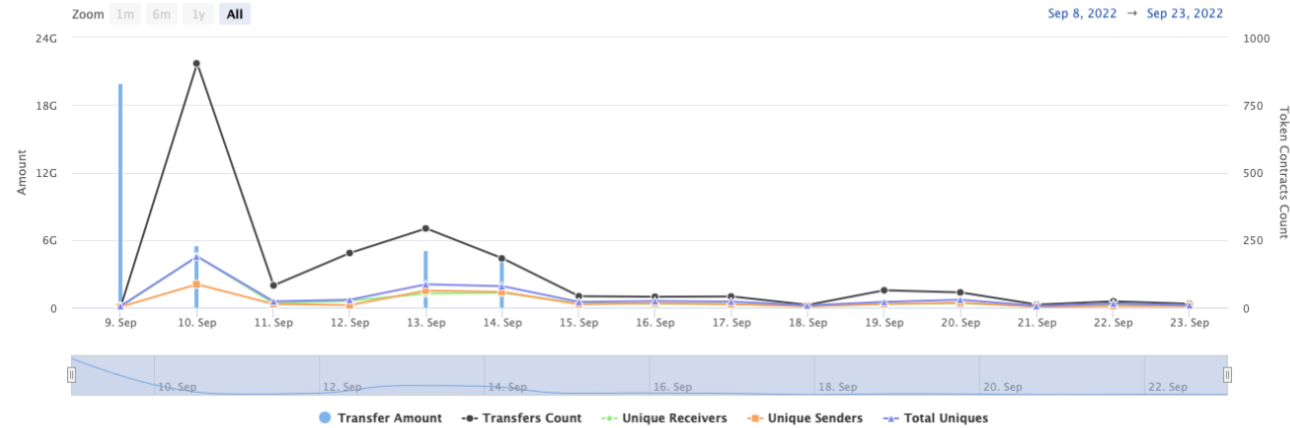
(A total of 9,991,224,176.33 tokens held by the top 100 accounts from the total supply of 10,000,000,000.00 token)

Metano Contract Interaction Details

Time Series: Token Contract Overview

Fri 9, Sept 2022 - Fri 23, Sept 2022

Token Contract 0x9D9e399e5385e2b9A58d4F775A1E16441b571af6 (METANO)
Source: Etherscan.io



Metano Top 10 Token Holders

Rank	Address	Quantity (Token)	Percentage
1	0xb1c415ef5d4a68eb50e7f135e682ecf54cad3328	3,000,000,000	30.0000%
2	Uniswap V2: METANO	1,461,659,230.742423661638515353	14.6166%
3	0x68c3a3d2bec1d389d92b6bbaefa5b5db0934929d	1,000,000,000	10.0000%
4	0x5cfbc79ee50f1b0c8b9f73b52c835962838cba56	1,000,000,000	10.0000%
5	0xa776be1819f83c799ff2b14146df99ae3062250a	337,147,229.24256150930460616	3.3715%
6	0xb35f29dbe10076226d655c2ae0344785d5f08d6d	272,454,887.240433845390556382	2.7245%
7	0x2ba51b27f715e763db53276d90cb6236622c35de	265,586,156.020921955970252674	2.6559%
8	0x5bfac04f237b932ced327e79e965004b48fea115	211,985,581.098504269629232241	2.1199%
9	0x813769f71e70446d3fe2c42b3560a2534174f0fa	143,580,008.423437029388053884	1.4358%
10	0xc3af7557f6b842ae716279d4874a4c7ffe6566dd	132,843,004.369631345217062886	1.3284%

Contract functions details

+ [Lib] Counters

- [Int] current
- [Int] increment #
- [Int] decrement #
- [Int] reset #

+ [Lib] Math

- [Int] max
- [Int] min
- [Int] average
- [Int] ceilDiv
- [Int] mulDiv
- [Int] mulDiv
- [Int] sqrt
- [Int] sqrt

+ [Lib] Arrays

- [Int] findUpperBound

+ [Int] IERC20

- [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
- [Int] _transferOwnership #

+ ERC20 (Context, IERC20)

- [Pub] <Constructor> #
 - [Pub] name
 - [Pub] symbol
 - [Pub] decimals
 - [Pub] totalSupply
 - [Pub] balanceOf
 - [Pub] allowance
 - [Pub] approve #
 - [Pub] transfer #
 - [Pub] transferFrom #
 - [Pub] increaseAllowance #
 - [Pub] decreaseAllowance #
 - [Int] _transfer #
 - [Int] _mint #
 - [Int] _burn #
 - [Int] _approve #
 - [Int] _beforeTokenTransfer #
- + ERC20Snapshot (ERC20)
- [Int] _snapshot #
 - [Int] _getCurrentSnapshotId
 - [Pub] balanceOfAt
 - [Pub] totalSupplyAt
 - [Int] _beforeTokenTransfer #
 - [Prv] _valueAt
 - [Prv] _updateAccountSnapshot #
 - [Prv] _updateTotalSupplySnapshot #
 - [Prv] _updateSnapshot #
 - [Prv] _lastSnapshotId
- + Metano (ERC20Snapshot, Ownable)
- [Pub] <Constructor> #
 - modifiers: ERC20
 - [Pub] transfer #
 - [Ext] updateOperator #
 - [Ext] mint #
 - [Pub] totalSupply
 - [Ext] burn #
 - [Ext] enableFairLaunch #
 - modifiers: onlyOwner
 - [Pub] endFairLaunchEvent #

(\$) = 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.	High 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

1. Abuse of authority

Issue:

- Operator can call burn function and burn users' tokens without any allowance.

Recommendation:

Do not allow anybody to interact with users' balances.

✓ Medium Severity Issues

No medium severity issues found.

✓ Low Severity Issues

No low severity issues found.

Notes:









- swapEnabled is not used.

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



- Owner can enable fair launch.
- Operator can change operator.
- Operator can mint token amounts according to max supply.

Testnet deployment

Contracts Description Table

Contract	Type	Bases	Mutability	Modifiers
L	Function Name	Visibility		
ERC20	Implementation	Context, IERC20		
L	approve	Public !		NO !
L	transferFrom	Public !		NO !
L	increaseAllowance	Public !		NO !
L	decreaseAllowance	Public !		NO !
Metano	Implementation	ERC20Snapshot, Ownable		
L	transfer	Public !		NO !
L	mint	External !		NO !
L	burn	External !		NO !
L	enableFairLaunch	External !		onlyOwner

Legend

Symbol	Meaning
	Function can modify state
	Function is payable

Conclusion

Smart contracts contain high 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 are provided by the team:

https://dx.app/app/v3_3/dxlockview?id=0&add=0xb4fff3D8E7E9d9F17FBbd1E425eb1D7734616960&type=lplock&chain=ETH

Security score: 65.

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.