

TechRate
April, 2024



SMART CONTRACTS SECURITY AUDIT REPORT



Techrate_audits



Techrate



Techrate1

Audit Details



Audited project

Spectra Chain



Deployer address

0x0e58aF7E2a5a9471F10f73be146E768b9E2d50dA



Client contacts:

Spectra Chain team



Blockchain

Ethereum



Project website:

<https://spectrachain.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 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 Spectra Chain to perform an audit of smart contracts:

- <https://etherscan.io/address/0x02020595E6a34a03a8E9c1f5624b1b7713810083#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.

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.	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

No low severity issues found.

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

- Owner can activate trading, allowing buys and sells.
- Owner can remove limits on buy/sell.
- Owner can update the maximum allowed buy amount.
- Owner can update the maximum allowed sell amount.
- Owner can update the maximum allowed wallet amount.
- Owner can update the minimum amount of tokens required to trigger a swap.
- Owner can exclude or include an address from the maximum transaction amount restriction.
- Owner can set or unset an address as an automated market maker pair.
- Owner can update the buy fees.
- Owner can update the sell fees.
- Owner can exclude or include an address from fees.
- Owner can change TreasuryAddress and EcosystemAddress.
- TreasuryAddress can withdraw ERC20 tokens and native tokens.
- TreasuryAddress can change swapTokensAtAmount.


















Contract: SpectraChain

- ✓ should deploy the token with the correct name and symbol (1895ms)
- ✓ should assign the initial supply to the deployer (1661ms)
- ✓ should update max buy amount (9409ms)
- ✓ should update max sell amount (9835ms)
- ✓ should remove limits (6240ms)
- ✓ should exclude address from max transaction (6107ms)
- ✓ should update max wallet amount (6787ms)
- ✓ should set treasury address (5746ms)
- ✓ should update swap threshold (5856ms)
- ✓ should transfer foreign token (14848ms)
- ✓ should exclude address from fees (6804ms)
- ✓ should update buy fees (8948ms)
- ✓ should update sell fees (6134ms)
- ✓ should set automated market maker pair (5756ms)
- ✓ should enable trading (12028ms)
- ✓ should set ecosystem address (9370ms)
- ✓ should transfer tokens between accounts (10432ms)
- ✓ should allow approvals and transfers from (21636ms)
- ✓ should increase and decrease allowances (15357ms)



19 passing (3m)

Testnet deployment

Contracts Description Table

Contract	Type	Bases	Mutability	Modifiers
L	Function Name	Visibility		
ERC20	Implementation	Context, IERC20, IERC20Metadata		
L	transfer	Public !		NO !
L	approve	Public !		NO !
L	transferFrom	Public !		NO !
SpectraChain	Implementation	ERC20, Ownable		
L	updateMaxBuyAmount	External !		onlyOwner
L	updateMaxSellAmount	External !		onlyOwner
L	removeLimits	External !		onlyOwner
L	excludeFromMaxTransaction	External !		onlyOwner
L	updateMaxWalletAmount	External !		onlyOwner
L	updateSwapThreshold	Public !		NO !
L	transferForeignToken	Public !		NO !
L	excludeFromFees	Public !		onlyOwner
L	updateBuyFees	External !		onlyOwner
L	updateSellFees	External !		onlyOwner
L	setAutomatedMarketMakerPair	External !		onlyOwner
L	enableTrading	External !		onlyOwner
L	setTreasuryAddress	External !		onlyOwner
L	setEcosystemAddress	External !		onlyOwner

Legend

Symbol	Meaning
	Function can modify state
	Function is payable

Conclusion

Smart contracts do not 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://etherscan.io/tx/0x3446f72c14a2d13163319566179ed7fea37028b5c107e595eaaacc2876d401de>

Security score: 83.

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.