Techrate1 Techrate

TechRate

AUDIT COMPANY

Smart Contract Security Audit

TechRate

January, 2022

Audit Details

Audited project

Node Cubed

Deployer address

0xa30ed97694cb86fadc80a8ea7b15124b4fe8246e

Client contacts:

Node Cubed team

Blockchain

Fantom

Project website:

https://cubed.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 Node Cubed to perform an audit of smart contracts:

https://ftmscan.com/address/0xaa9478eb3efe80c18dd99d47be466d760c329181#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

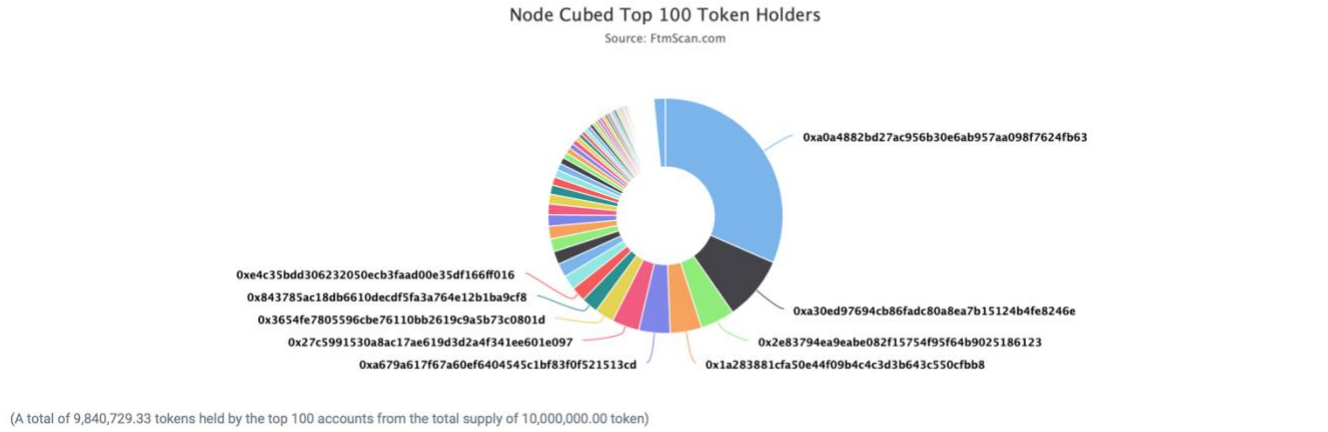
Token contract details for 16.01.2022

Contract name	Node Cubed
Contract address	0xaA9478eb3eFE80C18dd99d47bE466D760c329181
Total supply	10,000,000
Token ticker	N3
Decimals	9
Token holders	264
Transactions count	1,467
Top 100 holders dominance	98.41%
Contract deployer address	0xa30ed97694cb86fadc80a8ea7b15124b4fe8246e
Contract's current owner address	0xa30ed97694cb86fadc80a8ea7b15124b4fe8246e

Node Cubed Token Distribution

The top 100 holders collectively own 98.41% (9,840,729.33 Tokens) of Node Cubed

Token Total Supply: 10,000,000.00 Token | Total Token Holders: 264

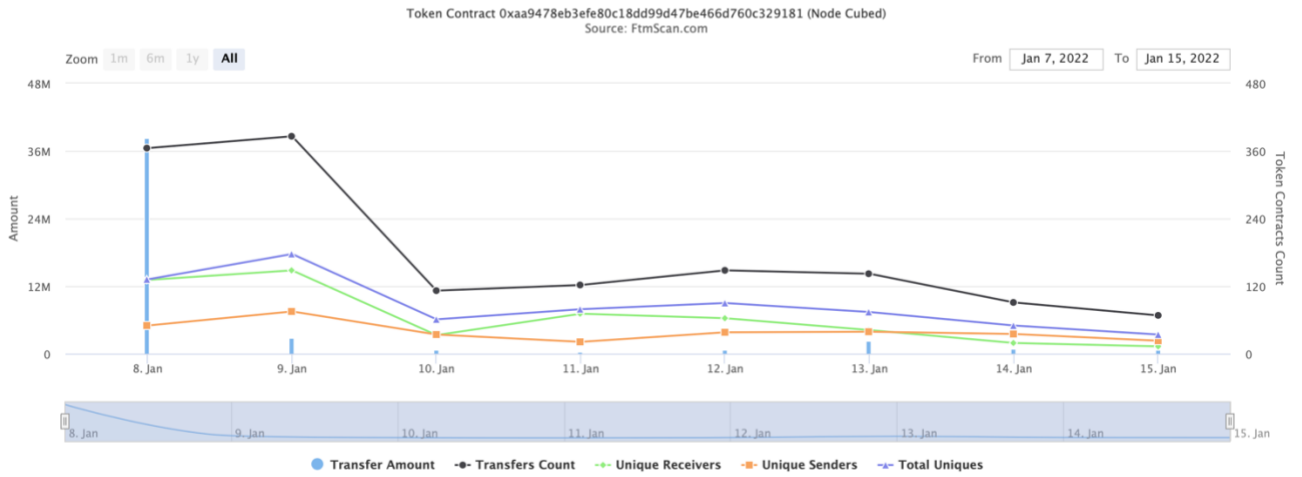


(A total of 9,840,729.33 tokens held by the top 100 accounts from the total supply of 10,000,000.00 token)

Node Cubed Contract Interaction Details

Time Series: Token Contract Overview

Sat 8, Jan 2022 - Sat 15, Jan 2022



Node Cubed Top 10 Token Holders

Rank	Address	Quantity (Token)	Percentage
1	0xa0a4882bd27ac956b30e6ab957aa098f7624fb63	3,151,714.914301247	31.5171%
2	0xa30ed97694cb86fadc80a8ea7b15124b4fe8246e	879,868.751355404	8.7987%
3	0x2e83794ea9eabe082f15754f95f64b9025186123	470,186.266426951	4.7019%
4	0x1a283881cfa50e44f09b4c4c3d3b643c550cfbb8	434,354.542298996	4.3435%
5	0xa679a617f67a60ef6404545c1bf83f0f521513cd	431,484.974254196	4.3148%
6	0x27c5991530a8ac17ae619d3d2a4f341ee601e097	376,512.798999103	3.7651%
7	0x3654fe7805596cbe76110bb2619c9a5b73c0801d	261,662.926119614	2.6166%
8	0x843785ac18db6610decdf5fa3a764e12b1ba9cf8	230,058.271702126	2.3006%
9	0xe4c35bdd306232050ecb3faad00e35df166ff016	202,412.100311337	2.0241%
10	0x03cd46ca8cec228849ad988243dfdb59fb9d5862	198,442.423565894	1.9844%

Contract functions details

+ Context
  - [Int] _msgSender

+ [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

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

+ [Int] IUniswapV2Factory
  - [Ext] createPair #

+ [Int] IUniswapV2Router02
  - [Ext] swapExactTokensForETHSupportingFeeOnTransferTokens #
  - [Ext] factory
  - [Ext] WETH
  - [Ext] addLiquidityETH ($)

+ NodeCubed (Context, IERC20, Ownable)
  - [Pub] <Constructor> #
  - [Pub] name
  - [Pub] symbol
  - [Pub] decimals
  - [Pub] totalSupply
  - [Pub] balanceOf
  - [Pub] transfer #
  - [Pub] allowance
  - [Pub] approve #
  - [Pub] transferFrom #
  - [Ext] setCooldownEnabled #
    - modifiers: onlyOwner
  - [Prv] tokenFromReflection
  - [Prv] _approve #
  - [Prv] _transfer #
  - [Prv] swapTokensForEth #

    - modifiers: lockTheSwap
  - [Prv] sendETHToFee #
  - [Ext] openTrading #
    - modifiers: onlyOwner
  - [Pub] setBots #
    - modifiers: onlyOwner
  - [Pub] removeStrictTxLimit #
    - modifiers: onlyOwner
  - [Pub] delBot #
    - modifiers: onlyOwner
  - [Prv] _tokenTransfer #
  - [Prv] _transferStandard #
  - [Prv] _takeTeam #
  - [Prv] _reflectFee #
  - [Ext] <Fallback> ($)
  - [Ext] manualswap #
  - [Ext] manualsend #
  - [Prv] _getValues
  - [Prv] _getTValues
  - [Prv] _getRValues
  - [Prv] _getRate
  - [Prv] _getCurrentSupply
  - [Pub] excludeFromFee #
    - modifiers: onlyOwner
  - [Pub] includeInFee #
    - modifiers: onlyOwner
  - [Prv] removeAllFee #
  - [Prv] restoreAllFee #
  - [Ext] setFeeAddr1 #
    - modifiers: onlyOwner
  - [Ext] setFeeAddr2 #
    - 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.	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 enable cooldown (user to user trading with time offset).
- Owner can open swap trading.
- Owner can add and remove bots (no transferring between this addresses).
- Owner can exclude/include in fee.
- Owner can change _feeAddr1 and _feeAddr2.
- Owner can change maximum transaction amount.

Conclusion

Smart contracts do not contain high severity issues! Liquidity pair contract's security is not checked due to out of scope.

Liquidity locking details provided by the team:
https://dxsale.app/app/v3/dxlockview?id=0&add=0xA30eD97694CB86fADC80A8ea7B15124b4fE8246e&type=lplock&chain=Fantom

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.