Techrate1 Techrate

TechRate

AUDIT COMPANY

Smart Contract Security Audit

TechRate

October, 2021

Audit Details

Audited project

Nickel Token

Deployer address

0x7df6838dc60b060332170fd72f35be73ce5ec4b7

Client contacts:

Nickel Token team

Blockchain

Binance Smart Chain

Project website:

Not provided

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 Nickel Token to perform an audit of smart contracts:

https://bscscan.com/address/0x8a660e26de13178d7847cf6061a360fdf987e697#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

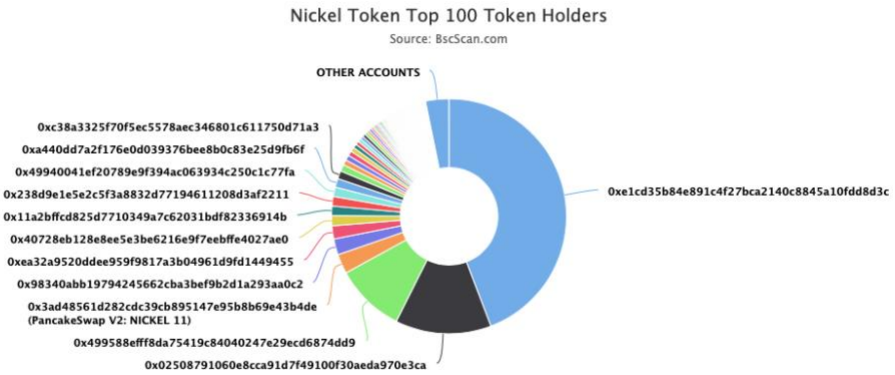
Token contract details for 28.10.2021

Contract name	Nickel Token
Contract address	0x8a660e26dE13178d7847Cf6061a360FDF987e697
Total supply	77,000,000
Token ticker	NICKEL
Decimals	18
Token holders	478
Transactions count	1,410
Top 100 holders dominance	96.80%
Liquidity fee	2
BNB reward fee	2
Marketing fee	5
Total fees	9
Dividend tracker	0xe87846d26348ca13dbb95fbcc668399c0f16efb5
Uniswap V2 pair	0x3ad48561d282cdc39cb895147e95b8b69e43b4de
Contract deployer address	0x7df6838dc60b060332170fd72f35be73ce5ec4b7
Contract’s current owner address	0xe1cd35b84e891c4f27bca2140c8845a10fdd8d3c

Nickel Token Token Distribution

The top 100 holders collectively own 96.80% (74,537,087.20 Tokens) of Nickel Token

Token Total Supply: 77,000,000.00 Token | Total Token Holders: 478

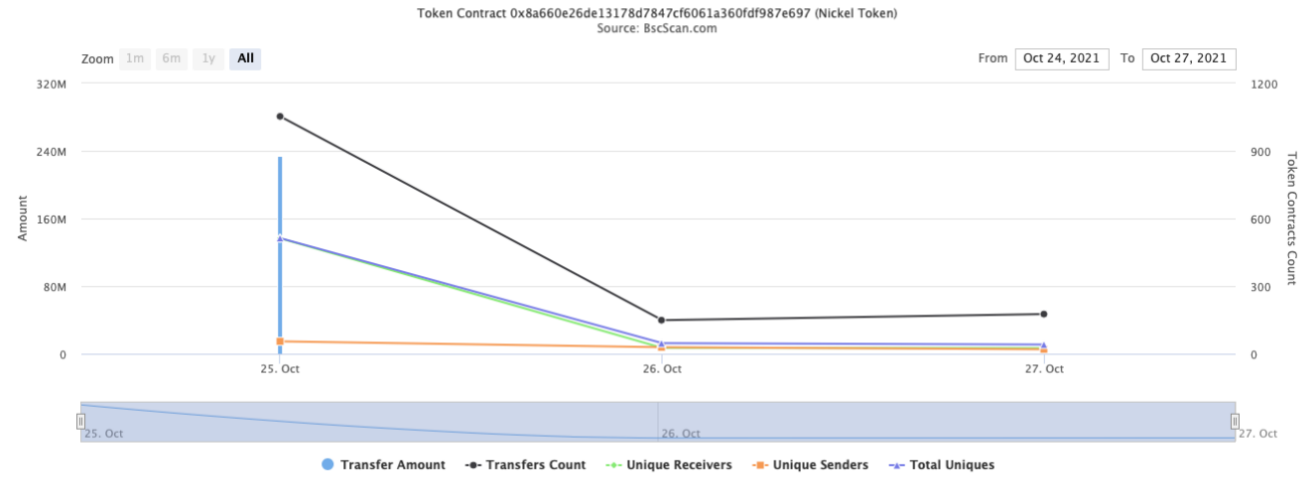


(A total of 74,537,087.20 tokens held by the top 100 accounts from the total supply of 77,000,000.00 token)

Nickel Token Contract Interaction Details

Time Series: Token Contract Overview

Mon 25, Oct 2021 - Wed 27, Oct 2021



Nickel Token Top 10 Token Holders

Rank	Address	Quantity (Token)	Percentage
1	0xe1cd35b84e891c4f27bca2140c8845a10fdd8d3c	34,037,276.9811028347	44.2043%
2	0x02508791060e8cca91d7f49100f30aeda970e3ca	10,170,986.085	13.2091%
3	0x499588efff8da75419c84040247e29ecd6874dd9	7,389,134.068	9.5963%
4	PancakeSwap V2: NICKEL 11	2,078,736.356823285199000092	2.6997%
5	0x98340abb19794245662cba3bef9b2d1a293aa0c2	1,684,358.857159910773647777	2.1875%
6	0xea32a9520ddee959f9817a3b04961d9fd1449455	1,394,442.862	1.8110%
7	0x40728eb128e8ee5e3be6216e9f7eebffe4027ae0	1,068,850.74806	1.3881%
8	0x11a2bffcd825d7710349a7c62031bdf82336914b	1,009,826.48574	1.3115%
9	0x238d9e1e5e2c5f3a8832d77194611208d3af2211	1,000,000	1.2987%
10	0x49940041ef20789e9f394ac063934c250c1c77fa	1,000,000	1.2987%

Contract functions details

+ [Lib] SafeMathUint
  - [Int] toInt256Safe

+ [Lib] SafeMathInt
  - [Int] mul
  - [Int] div
  - [Int] sub
  - [Int] add
  - [Int] abs
  - [Int] toUint256Safe

+ [Lib] SafeMath
  - [Int] add
  - [Int] sub
  - [Int] sub
  - [Int] mul
  - [Int] div
  - [Int] div
  - [Int] mod
  - [Int] mod

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

+ [Lib] IterableMapping
  - [Pub] get
  - [Pub] getIndexOfKey
  - [Pub] getKeyAtIndex
  - [Pub] size
  - [Pub] set #
  - [Pub] remove #

+ [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 #

+ [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] mint #
  - [Ext] burn #
  - [Ext] swap #
  - [Ext] skim #
  - [Ext] sync #
  - [Ext] initialize #

+ [Int] IUniswapV2Factory
  - [Ext] feeTo
  - [Ext] feeToSetter
  - [Ext] getPair
  - [Ext] allPairs
  - [Ext] allPairsLength
  - [Ext] createPair #
  - [Ext] setFeeTo #
  - [Ext] setFeeToSetter #

+ [Int] IERC20Metadata (IERC20)
  - [Ext] name

  - [Ext] symbol
  - [Ext] decimals

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

+ ERC20 (Context, IERC20, IERC20Metadata)
  - [Pub] <Constructor> #
  - [Pub] name
  - [Pub] symbol
  - [Pub] decimals
  - [Pub] totalSupply
  - [Pub] balanceOf
  - [Pub] transfer #
  - [Pub] allowance
  - [Pub] approve #
  - [Pub] transferFrom #
  - [Pub] increaseAllowance #
  - [Pub] decreaseAllowance #
  - [Int] _transfer #
  - [Int] _mint #
  - [Int] _burn #
  - [Int] _approve #
  - [Int] _beforeTokenTransfer #

+ [Int] DividendPayingTokenOptionalInterface
  - [Ext] withdrawableDividendOf
  - [Ext] withdrawnDividendOf
  - [Ext] accumulativeDividendOf

+ [Int] DividendPayingTokenInterface
  - [Ext] dividendOf
  - [Ext] distributeDividends ($)
  - [Ext] withdrawDividend #

+ DividendPayingToken (ERC20, DividendPayingTokenInterface,
DividendPayingTokenOptionalInterface)
  - [Pub] <Constructor> #
    - modifiers: ERC20
  - [Ext] <Fallback> ($)
  - [Pub] distributeDividends ($)
  - [Pub] withdrawDividend #
  - [Int] _withdrawDividendOfUser #
  - [Pub] dividendOf
  - [Pub] withdrawableDividendOf
  - [Pub] withdrawnDividendOf
  - [Pub] accumulativeDividendOf
  - [Int] _transfer #
  - [Int] _mint #
  - [Int] _burn #

- [Int] _setBalance #

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

+ NICKEL (ERC20, Ownable)
  - [Pub] <Constructor> #
    - modifiers: ERC20
  - [Ext] <Fallback> ($)
  - [Pub] updateDividendTracker #
    - modifiers: onlyOwner
  - [Pub] updateUniswapV2Router #
    - modifiers: onlyOwner
  - [Pub] excludeFromFees #
    - modifiers: onlyOwner
  - [Pub] excludeMultipleAccountsFromFees #
    - modifiers: onlyOwner
  - [Pub] setAutomatedMarketMakerPair #
    - modifiers: onlyOwner
  - [Prv] _setAutomatedMarketMakerPair #
  - [Pub] updateLiquidityWallet #
    - modifiers: onlyOwner
  - [Pub] updateMarketingWallet #
    - modifiers: onlyOwner
  - [Pub] updateGasForProcessing #
    - modifiers: onlyOwner
  - [Ext] updateClaimWait #
    - modifiers: onlyOwner
  - [Ext] getClaimWait
  - [Ext] getTotalDividendsDistributed
  - [Pub] isExcludedFromFees
  - [Pub] withdrawableDividendOf
  - [Pub] dividendTokenBalanceOf
  - [Ext] getAccountDividendsInfo
  - [Ext] getAccountDividendsInfoAtIndex
  - [Ext] processDividendTracker #
  - [Ext] claim #
  - [Ext] getLastProcessedIndex
  - [Ext] getNumberOfDividendTokenHolders
  - [Ext] enableTrading #
    - modifiers: onlyOwner
  - [Ext] updateSwapTokenAmount #
    - modifiers: onlyOwner
  - [Ext] updateMaxSellLimiation #
    - modifiers: onlyOwner
  - [Pub] setBotAddress #
    - modifiers: onlyOwner
  - [Pub] transferEnableAddresses #
    - modifiers: onlyOwner
  - [Int] _transfer #
  - [Prv] swapAndLiquify #
  - [Prv] swapTokensForEth #
  - [Prv] addLiquidity #
  - [Prv] swapAndSendMarketing #

  - [Prv] swapAndSendDividends #

+ NICKELDividendTracker (DividendPayingToken, Ownable)
  - [Pub] <Constructor> #
    - modifiers: DividendPayingToken
  - [Int] _transfer #
  - [Pub] withdrawDividend #
  - [Ext] excludeFromDividends #
    - modifiers: onlyOwner
  - [Ext] updateClaimWait #
    - modifiers: onlyOwner
  - [Ext] getLastProcessedIndex
  - [Ext] getNumberOfTokenHolders
  - [Pub] getAccount
  - [Pub] getAccountAtIndex
  - [Prv] canAutoClaim
  - [Ext] setBalance #
    - modifiers: onlyOwner
  - [Pub] process #
  - [Pub] processAccount #
    - 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.	Low issues
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. Out of gas

Issue:

- The function `excludeMultipleAccountsFromFees()` uses the loop to exclude multiple accounts from fees. Function will be aborted with `OUT_OF_GAS` exception if there will be a long addresses list.

Recommendation:
Be careful about accounts array length.

Notes:

- Dividend tracker may be changed. So that logic of setBalance and other functions could be another and not audited.

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

- Owner can change dividend tracker.
- Owner can change Uniswap router address.
- Owner can exclude from the fees.
- Owner can exclude and include addresses in automatedMarketMakerPairs array.
- Owner can change liquidity and marketing wallet.
- Owner can change gas for processing.
- Owner can update claimWait value.
- Owner can enable trading.
- Owner can change swapTokensAtAmount and maxSellTransactionAmount.
- Owner mark addresses as bots.
- Owner can include in canTransferBeforeTradingIsEnable array.

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 are 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.