TechRate
AUDIT COMPANY

Smart Contract Security Audit

Audit Details

Audited project

Next Token

Deployer address

0x1087151f02855fb080894edc4d359bda75eb75ed

Client contacts:

Next Token team

Blockchain

Binance Smart Chain

Project website:

https://nxt-token.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 Next Token to perform an audit of smart contracts:

https://bscscan.com/address/0x8e428aa75b271ebf905db7e3f2970453e976481e#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

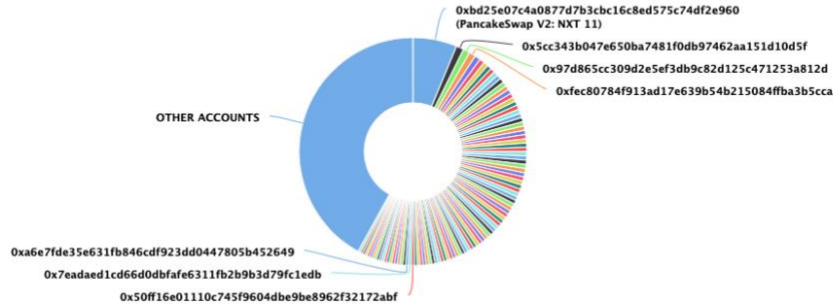|	
Contract name	Next Token
Contract address	0x8e428aA75b271EbF905DB7e3F2970453E976481e
Total supply	100,000,000,000
Token ticker	NXT
Decimals	18
Token holders	4,005
Transactions count	37,555
Top 100 holders dominance	58.02%
Dividend tracker	0xbff77b171b993f896c9839383db43bfbe0b14092
Marketing wallet	0xfb8ce2e7631127974c4fa82c4c0b32553b5e024b
BNB rewards fee	7
Uniswap V2 pair	0xbd25e07c4a0877d7b3cbc16c8ed575c74df2e960
Contract deployer address	0x1087151f02855fb080894edc4d359bda75eb75ed
Contract's current owner address	0xca99649f069cdaec14db8711cb689aa8d8328c9f

Next Token Token Distribution

The top 100 holders collectively own 58.02% (58,017,524,410.68 Tokens) of Next Token

Token Total Supply: 100,000,000,000.00 Token | Total Token Holders: 4,004

Next Token Top 100 Token Holders
Source: BscScan.com

0xbd25e07c4a0877d7b3cbc16c8ed575c74df2e960
(PancakeSwap V2: NXT 11)
0x5cc343b047e650ba7481f0db97462aa151d10d5f
0x97d865cc309d2e5ef3db9c82d125c471253a812d
0xfec80784f913ad17e639b54b215084ffba3b5cca

OTHER ACCOUNTS

0xa6e7fde35e631fb846cdf923dd0447805b452649
0x7eadaed1cd66d0dbfafe6311fb2b9b3d79fc1edb
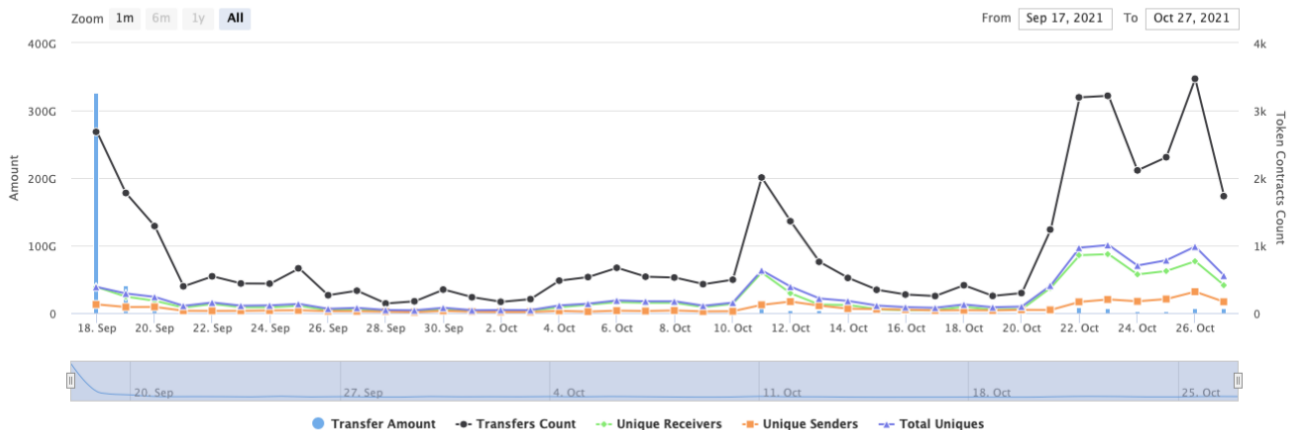0x50ff16e01110c745f9604dbe9be8962f32172abf

(A total of 58,017,524,410.68 tokens held by the top 100 accounts from the total supply of 100,000,000,000.00 token)

Next Token Contract Interaction Details

Time Series: Token Contract Overview   Sat 18, Sept 2021 - Wed 27, Oct 2021

Token Contract 0x8e428aa75b271ebf905db7e3f2970453e976481e (Next Token)
Source: BscScan.com

Zoom 1m 6m 1y All   From Sep 17, 2021 To Oct 27, 2021

● Transfer Amount -●- Transfers Count -●- Unique Receivers -■- Unique Senders -▲- Total Uniques

Next Token Top 10 Token Holders

Rank	Address	Quantity (Token)	Percentage
1	📄 PancakeSwap V2: NXT 11	6,244,794,851.314029183850090181	6.2448%
2	0x5cc343b047e650ba7481f0db97462aa151d10d5f	1,072,977,719.360197250956472483	1.0730%
3	0x97d865cc309d2e5ef3db9c82d125c471253a812d	966,923,546.390605330991066276	0.9669%
4	0xfec80784f913ad17e639b54b215084ffba3b5cca	930,597,535.583343413931447041	0.9306%
5	0xda29dbea0713e46f27ac1dd875010f66505b79d1	806,618,045.9551170323696618244	0.8066%
6	0x4ff5bb21c644125a3aeca43e8ff6f9ad959f4736	711,350,969.706960401781858957	0.7114%
7	0x5099b63755f04db523ea2342812d06063575dc56	655,971,011.1956012669503583	0.6560%
8	0x1837772345454d1d77458e94bd438342fd7eece7	651,523,034.140044679401918757	0.6515%
9	0xad3a499536f7222a83f4523447dd1863a2c602cd	643,396,707.2031692792867714201	0.6434%
10	0xfbdb43bb91eab8b5a85d33b41a17aff4913a1ac6	639,887,431.872952926826668975	0.6399%

Contract functions details

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

+ [Int] IERC20Metadata (IERC20)
- **[Ext] name**
- **[Ext] symbol**
- **[Ext] decimals**

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

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

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

+ 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 #**

+ [Lib] IterableMapping
- **[Pub] get**
- **[Pub] getIndexOfKey**
- **[Pub] getKeyAtIndex**
- **[Pub] size**

- **[Pub]** set **#**
- **[Pub]** remove **#**

+ **[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]** mint **#**
  - **[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 **#**

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

+ **NXTTOKEN** **(ERC20, Ownable)**
  - **[Pub]** **<Constructor>** **#**
    - modifiers: ERC20
  - **[Ext]** **<Fallback>** **($)**
  - **[Pub]** updateDividendTracker **#**
    - modifiers: onlyOwner
  - **[Pub]** updateUniswapV2Router **#**
    - modifiers: onlyOwner
  - **[Pub]** excludeFromFees **#**
    - modifiers: onlyOwner
  - **[Pub]** excludeMultipleAccountsFromFees **#**
    - modifiers: onlyOwner
  - **[Ext]** setMarketingWallet **#**
    - modifiers: onlyOwner
  - **[Ext]** setBNBRewardsFee **#**
    - modifiers: onlyOwner
  - **[Ext]** setLiquiditFee **#**
    - modifiers: onlyOwner
  - **[Ext]** setMarketingFee **#**
    - modifiers: onlyOwner
  - **[Pub]** setAutomatedMarketMakerPair **#**
    - modifiers: onlyOwner
  - **[Ext]** blacklistAddress **#**
    - modifiers: onlyOwner
  - **[Prv]** _setAutomatedMarketMakerPair **#**
  - **[Pub]** updateGasForProcessing **#**
    - modifiers: onlyOwner
  - **[Ext]** updateClaimWait **#**
    - modifiers: onlyOwner
  - **[Ext]** getClaimWait
  - **[Ext]** getTotalDividendsDistributed
  - **[Pub]** isExcludedFromFees

- **[Pub]** withdrawableDividendOf
- **[Pub]** dividendTokenBalanceOf
- **[Ext]** excludeFromDividends **#**
  - modifiers: onlyOwner
- **[Ext]** setmaxTransactionPercentage **#**
  - modifiers: onlyOwner
- **[Ext]** setmaxTokensPerAddressPercentage **#**
  - modifiers: onlyOwner
- **[Ext]** setIsTxLimitExempt **#**
  - modifiers: onlyOwner
- **[Pub]** setIsExcludedFromAntiWhale **#**
  - modifiers: onlyOwner
- **[Pub]** setIsExcludedFromTransactionCooldown **#**
  - modifiers: onlyOwner
- **[Pub]** setTransactionCooldownTime **#**
  - modifiers: onlyOwner
- **[Pub]** setBuyFees **#**
  - modifiers: onlyOwner
- **[Pub]** setSellFees **#**
  - modifiers: onlyOwner
- **[Prv]** setFeeOnBuy **#**
- **[Prv]** setFeeOnSell **#**
- **[Ext]** getAccountDividendsInfo
- **[Ext]** getAccountDividendsInfoAtIndex
- **[Ext]** processDividendTracker **#**
- **[Ext]** claim **#**
- **[Ext]** getLastProcessedIndex
- **[Ext]** getNumberOfDividendTokenHolders
- **[Int]** _transfer **#**
- **[Prv]** swapAndSendToFee **#**
- **[Prv]** swapAndLiquify **#**
- **[Prv]** swapTokensForEth **#**
- **[Prv]** addLiquidity **#**
- **[Prv]** swapAndSendDividends **#**

+ **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 **#**

+ **NXTDividendTracker** (Ownable, DividendPayingToken)
  - **[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

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

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

+ [Lib] SafeMathUint
- **[Int]** toInt256Safe

($) = 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:

- **Owner can change dividend tracker to not audited and some functions may work in different ways.**

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 BNB rewards, marketing, liquidity fee.
- Owner can blacklist addresses.
- Owner can open trading.
- Owner can change gas for processing.
- Owner can update claimWait value.
- Owner can change marketing wallet.
- Owner can exclude from dividends.
- Owner can change maxTxAmount.
- Owner can change maxTokensPerAddress.
- Owner can manage addresses in isTxLimitExempt and isExcludedFromAntiWhale array.
- Owner can change transactionLockTime.
- Owner can change fees.

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 provided by the team:
https://dxsale.app/app/v3/dxlockview?id=0&add=0xCA99649F069cdAEC14DB8711cb689AA8d8328c9f&type=lplock&chain=BSC

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.