RugFreeCoins Audit

NewBTC Token

Smart Contract Security Audit

June 20, 2021

Contents

Audit details

Audited project

NBTC Token

Contract Address

0xbe878cffb39a347a70809b5d98b65dd85de2e37b

Client contact

NBTC Token Team

Blockchain

Binance smart chain

Project website

https://newbtc.one/

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 Rugfreecoins and its affiliates (including holding companies, shareholders, subsidiaries, employees, directors, officers and other representatives) (Rugfreecoins) owe no duty of care towards you or any other person, nor does Rugfreecoins 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 Rugfreecoins 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, Rugfreecoins hereby excludes all liability and responsibility, and neither you nor any other person shall have any claim against Rugfreecoins, 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

Rugfreecoins was commissioned by NBTC to perform an audit of the smart contract.

https://bscscan.com/token/0xbe878cffb39a347a70809b5d98b65dd85de2e37b

The focus of this audit is to verify that the smart contract is secure, resilient and working according to the specifications.

The information in this report should be used to understand the risk exposure of the smart contract, project feasibility, long term sustainability and as a guide to improve the security posture of the smart contract by remediating the issues that were identified

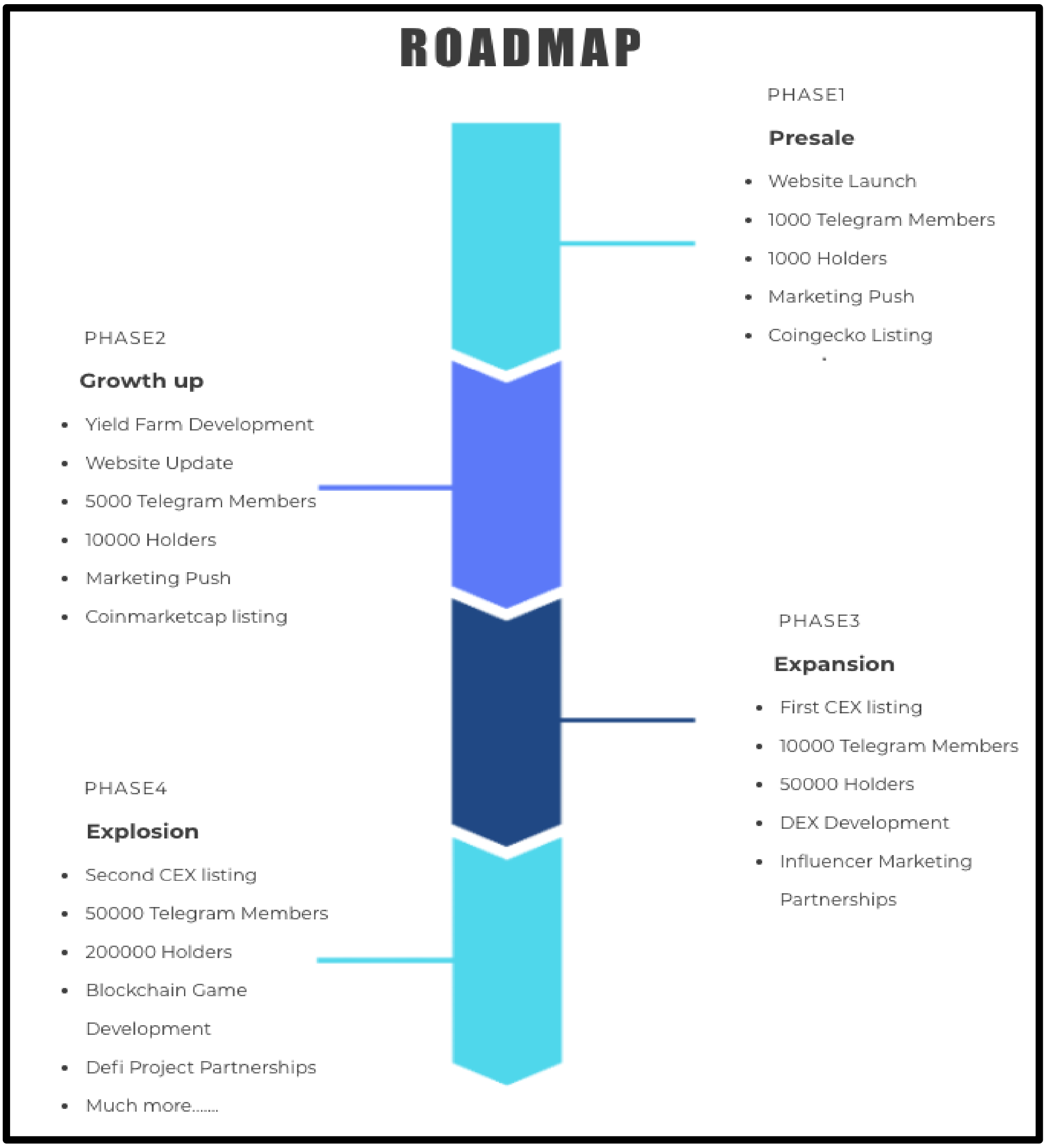
About the project

New BTC has been introduced with the aim of solving the issues such as slow trading speed, high gas fees, and a power-hungry mining process of traditional Bitcoin by adding unique features to it. NBTC is based on Binance Smart Chain technology which is faster, cheaper, and less energy-consuming for transactions which is environment-friendly for daily use.

Tokenomics

- **1%** of every trade goes to holders pockets.
- **1%** of token trades goes to liquidity pool.

Roadmap



ROADMAP

PHASE1

Presale

- Website Launch
- 1000 Telegram Members
- 1000 Holders
- Marketing Push
- Coingecko Listing

PHASE2

Growth up

- Yield Farm Development
- Website Update
- 5000 Telegram Members
- 10000 Holders
- Marketing Push
- Coinmarketcap listing

PHASE3

Expansion

- First CEX listing
- 10000 Telegram Members
- 50000 Holders
- DEX Development
- Influencer Marketing Partnerships

PHASE4

Explosion

- Second CEX listing
- 50000 Telegram Members
- 200000 Holders
- Blockchain Game Development
- Defi Project Partnerships
- Much more.......

Target market and the concept

Target market

- Anyone who’s interested in Crypto space with long term investment plans.
- Anyone who’s interested in making transactions for any sort of financial activity using NBTC since it’s faster and fees are cheaper.
- Anyone who’s ready to earn a passive income by holding tokens.

Core concept

The new BTC concept is to be the new and better version of the current Bitcoin as a substitute by addressing the issues with a few additional features to make it more user-friendly and attractive.

Features

- Fast transaction speed.
- Less transaction fee.
- More eco-friendly since NBTC doesn't require a power-hungry mining process.
- Passive income to all holders since they are getting rewarded from every transaction.

Future Plans

- More extensive marketing to make aware about the new BTC token.
- Development of yield farming.
- Getting listed on coinmarketcap and other similar platforms.
- Development of an airdrop app.
- Making partnerships with other projects.

Potential to grow with score points

1.	Project efficiency	7/10
2.	Project uniqueness	6/10
3	Information quality	8/10
4	Service quality	7/10
5	System quality	7/10
6	Impact on the community	7/10
7	Impact on the business	7/10
8	Preparing for the future	7/10
Total Points		**7/10**

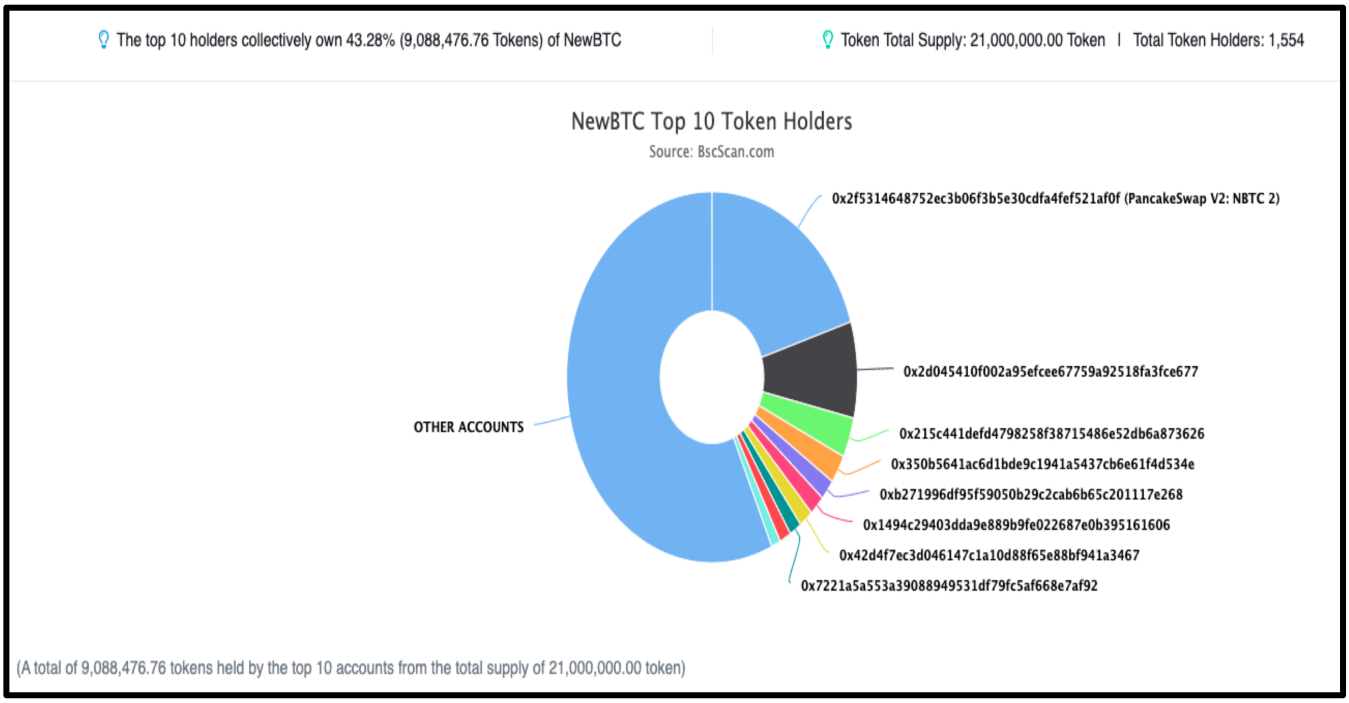
Contract details

Token contract details for 20th June 2021 (Day before launch)

Contract name	NewBTC Token
Contract address	0xbe878cffb39a347a70809b5d98b65dd85de2e37b
Token supply	21,000,000
Token ticker	NBTC
Decimals	9
Token holders	1553
Transaction count	5814
Top 100% holders dominance	81.61%
Contract deployer address	0x44a5ab6b54d456769c4a7a798724a8e097a27df6
Contract's current owner address	0x44a5ab6b54d456769c4a7a798724a8e097a27df6

Top token holders

Top 10 Token Holders



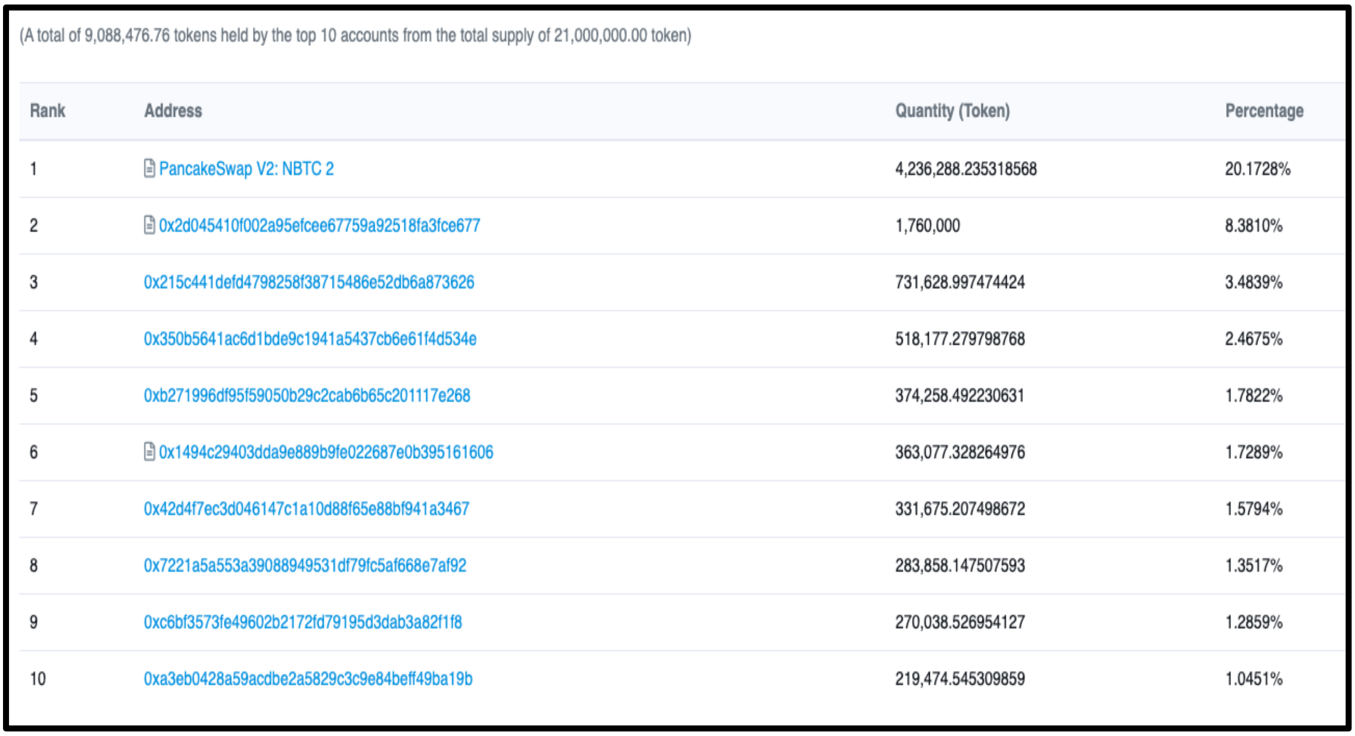
The top 10 holders collectively own 43.28% (9,088,476.76 Tokens) of NewBTC

Token Total Supply: 21,000,000.00 Token | Total Token Holders: 1,554

NewBTC Top 10 Token Holders

Source: BscScan.com

(A total of 9,088,476.76 tokens held by the top 10 accounts from the total supply of 21,000,000.00 token)



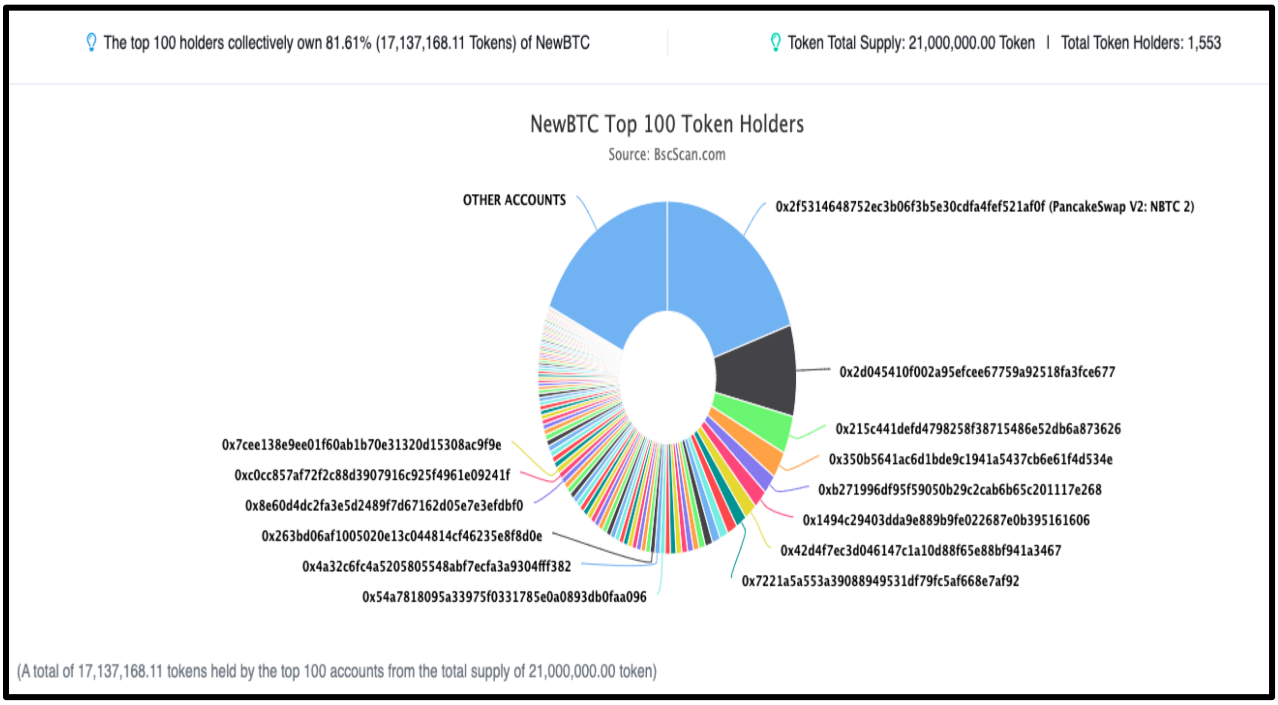
(A total of 9,088,476.76 tokens held by the top 10 accounts from the total supply of 21,000,000.00 token)

Rank	Address	Quantity (Token)	Percentage
1	PancakeSwap V2: NBTC 2	4,236,288.235318568	20.1728%
2	0x2d045410f002a95efcee67759a92518fa3fce677	1,760,000	8.3810%
3	0x215c441defd4798258f38715486e52db6a873626	731,628.997474424	3.4839%
4	0x350b5641ac6d1bde9c1941a5437cb6e61f4d534e	518,177.279798768	2.4675%
5	0xb271996df95f59050b29c2cab6b65c201117e268	374,258.492230631	1.7822%
6	0x1494c29403dda9e889b9fe022687e0b395161606	363,077.328264976	1.7289%
7	0x42d4f7ec3d046147c1a10d88f65e88bf941a3467	331,675.207498672	1.5794%
8	0x7221a5a553a39088949531df79fc5af668e7af92	283,858.147507593	1.3517%
9	0xc6bf3573fe49602b2172fd79195d3dab3a82f1f8	270,038.526954127	1.2859%
10	0xa3eb0428a59acdbe2a5829c3c9e84beff49ba19b	219,474.545309859	1.0451%

Token distribution

Token will be distributed as follows:

Top 100 Token Holders



The top 100 holders collectively own 81.61% (17,137,168.11 Tokens) of NewBTC

Token Total Supply: 21,000,000.00 Token | Total Token Holders: 1,553

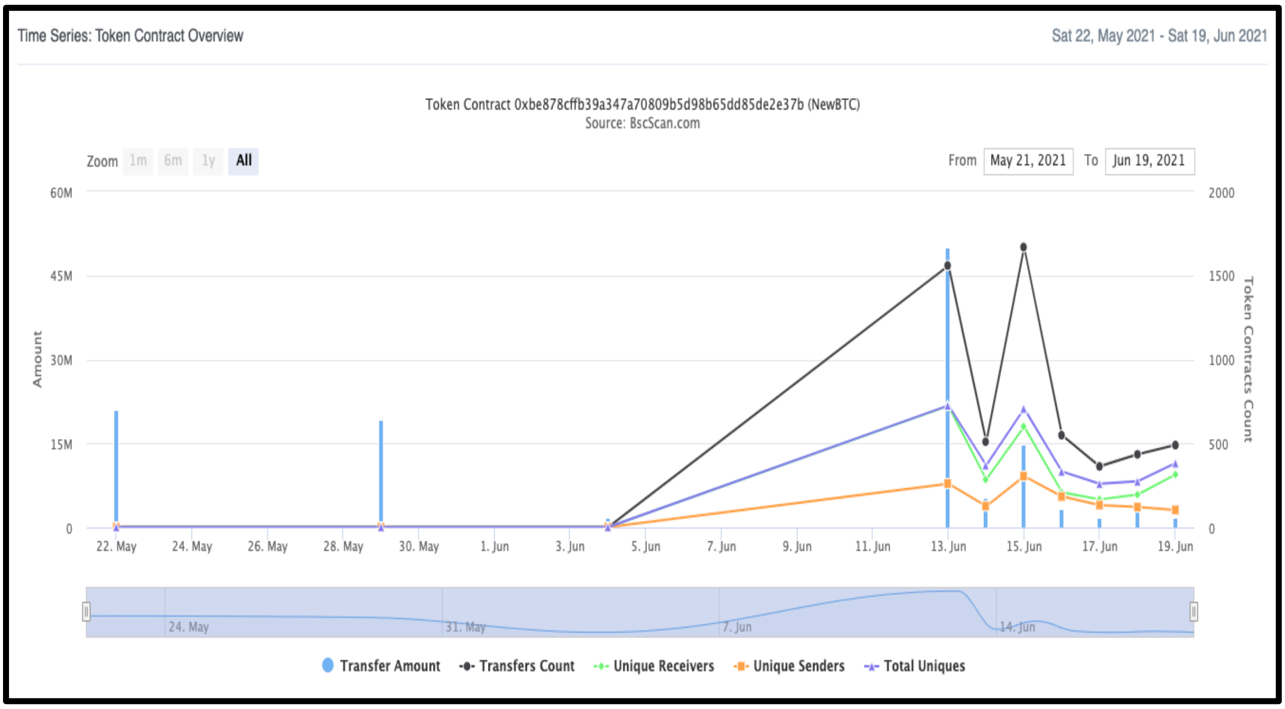
NewBTC Top 100 Token Holders

Source: BscScan.com

OTHER ACCOUNTS
0x2f5314648752ec3b06f3b5e30cdfa4fef521af0f (PancakeSwap V2: NBTC 2)
0x2d045410f002a95efcee67759a92518fa3fce677
0x215c441defd4798258f38715486e52db6a873626
0x350b5641ac6d1bde9c1941a5437cb6e61f4d534e
0xb271996df95f59050b29c2cab6b65c201117e268
0x1494c29403dda9e889b9fe022687e0b395161606
0x42d4f7ec3d046147c1a10d88f65e88bf941a3467
0x7221a5a553a39088949531df79fc5af668e7af92
0x7cee138e9ee01f60ab1b70e31320d15308ac9f9e
0xc0cc857af72f2c88d3907916c925f4961e09241f
0x8e60d4dc2fa3e5d2489f7d67162d05e7e3efdbf0
0x263bd06af1005020e13c044814cf46235e8f8d0e
0x4a32c6fc4a5205805548abf7ecfa3a9304fff382
0x54a7818095a33975f0331785e0a0893db0faa096

(A total of 17,137,168.11 tokens held by the top 100 accounts from the total supply of 21,000,000.00 token)

Contract interaction details



Time Series: Token Contract Overview

Sat 22, May 2021 - Sat 19, Jun 2021

Token Contract 0xbe878cffb39a347a70809b5d98b65dd85de2e37b (NewBTC)

Source: BscScan.com

Zoom: 1m 6m 1y **All**

From: May 21, 2021 To: Jun 19, 2021

Contract code function details

No	Category	Item	Result
1	Coding conventions	BRC20 Token standards	pass
		compile errors	pass
		Compiler version security	pass
		visibility specifiers	pass
		Gas consumption	low issue
		SafeMath features	pass
		Fallback usage	pass
		tx.origin usage	pass
		deprecated items	pass
		Redundant code	pass
		Overriding variables	pass
2	Function call audit	Authorization of function call	pass
		Low level function (call/delegate call) security	pass
		Returned value security	pass
		Selfdestruct function security	pass
3	Business security	Access control of owners	pass
		Business logics	pass
		Business implementations	pass
4	Integer overflow/underflow		pass
5	Reentrancy		pass
6	Exceptional reachable state		pass
7	Transaction ordering dependence		pass
8	Block properties dependence		pass
9	Pseudo random number generator (PRNG)		pass
10	DoS (Denial of Service)		pass
11	Token vesting implementation		pass
12	Fake deposit		pass
13	Event security		pass

Contract description table

Below table represents the summary of the contracts and methods in the token contract. We scanned the whole contract and listed down all the Interfaces, functions and implementations with its visibility and mutability.

Contract	Type	Bases		
└	Function Name	Visibility	Mutability	Modifiers
IERC20	**Interface**			
└	totalSupply	External ❗		NO❗
└	balanceOf	External ❗		NO❗
└	transfer	External ❗	🛑	NO❗
└	allowance	External ❗		NO❗
└	approve	External ❗	🛑	NO❗
└	transferFrom	External ❗	🛑	NO❗
SafeMath	**Library**			
└	add	Internal 🔒		
└	sub	Internal 🔒		
└	sub	Internal 🔒		
└	mul	Internal 🔒		
└	div	Internal 🔒		
└	div	Internal 🔒		
└	mod	Internal 🔒		
└	mod	Internal 🔒		

Context	**Implementation**			
└	_msgSender	Internal 🔒		
└	_msgData	Internal 🔒		
Address	**Library**			
└	isContract	Internal 🔒		
└	sendValue	Internal 🔒	🛑	
└	functionCall	Internal 🔒	🛑	
└	functionCall	Internal 🔒	🛑	
└	functionCallWithValue	Internal 🔒	🛑	
└	functionCallWithValue	Internal 🔒	🛑	
└	_functionCallWithValue	Private 🔐	🛑	
Ownable	**Implementation**	**Context**		
└		Internal 🔒	🛑	
└	owner	Public ❗		NO❗
└	renounceOwnership	Public ❗	🛑	onlyOwner
└	transferOwnership	Public ❗	🛑	onlyOwner
└	geUnlockTime	Public ❗		NO❗
└	lock	Public ❗	🛑	onlyOwner
└	unlock	Public ❗	🛑	NO❗
IUniswapV2Factory	**Interface**			
└	feeTo	External ❗		NO❗
└	feeToSetter	External ❗		NO❗

└	getPair	External ❗		NO❗
└	allPairs	External ❗		NO❗
└	allPairsLength	External ❗		NO❗
└	createPair	External ❗	🛑	NO❗
└	setFeeTo	External ❗	🛑	NO❗
└	setFeeToSetter	External ❗	🛑	NO❗
IUniswapV2Pair	**Interface**			
└	name	External ❗		NO❗
└	symbol	External ❗		NO❗
└	decimals	External ❗		NO❗
└	totalSupply	External ❗		NO❗
└	balanceOf	External ❗		NO❗
└	allowance	External ❗		NO❗
└	approve	External ❗	🛑	NO❗
└	transfer	External ❗	🛑	NO❗
└	transferFrom	External ❗	🛑	NO❗
└	DOMAIN_SEPARATOR	External ❗		NO❗
└	PERMIT_TYPEHASH	External ❗		NO❗
└	nonces	External ❗		NO❗
└	permit	External ❗	🛑	NO❗
└	MINIMUM_LIQUIDITY	External ❗		NO❗
└	factory	External ❗		NO❗
└	token0	External ❗		NO❗
└	token1	External ❗		NO❗

└	getReserves	External ❗		NO❗
└	price0CumulativeLast	External ❗		NO❗
└	price1CumulativeLast	External ❗		NO❗
└	kLast	External ❗		NO❗
└	mint	External ❗	🛑	NO❗
└	burn	External ❗	🛑	NO❗
└	swap	External ❗	🛑	NO❗
└	skim	External ❗	🛑	NO❗
└	sync	External ❗	🛑	NO❗
└	initialize	External ❗	🛑	NO❗
IUniswapV2Router01	**Interface**			
└	factory	External ❗		NO❗
└	WETH	External ❗		NO❗
└	addLiquidity	External ❗	🛑	NO❗
└	addLiquidityETH	External ❗	💵	NO❗
└	removeLiquidity	External ❗	🛑	NO❗
└	removeLiquidityETH	External ❗	🛑	NO❗
└	removeLiquidityWithPermit	External ❗	🛑	NO❗
└	removeLiquidityETHWithPermit	External ❗	🛑	NO❗
└	swapExactTokensForTokens	External ❗	🛑	NO❗
└	swapTokensForExactTokens	External ❗	🛑	NO❗
└	swapExactETHForTokens	External ❗	💵	NO❗
└	swapTokensForExactETH	External ❗	🛑	NO❗

└	swapExactTokensForETH	External ❗	🛑	NO❗
└	swapETHForExactTokens	External ❗	💵	NO❗
└	quote	External ❗		NO❗
└	getAmountOut	External ❗		NO❗
└	getAmountIn	External ❗		NO❗
└	getAmountsOut	External ❗		NO❗
└	getAmountsIn	External ❗		NO❗
IUniswapV2Router02	**Interface**	**IUniswapV2Router01**		
└	removeLiquidityETHSupportingFeeOnTransferTokens	External ❗	🛑	NO❗
└	removeLiquidityETHWithPermitSupportingFeeOnTransferTokens	External ❗	🛑	NO❗
└	swapExactTokensForTokensSupportingFeeOnTransferTokens	External ❗	🛑	NO❗
└	swapExactETHForTokensSupportingFeeOnTransferTokens	External ❗	💵	NO❗
└	swapExactTokensForETHSupportingFeeOnTransferTokens	External ❗	🛑	NO❗
NewBTC	**Implementation**	**Context, IERC20, Ownable**		
└		Public ❗	🛑	NO❗
└	name	Public ❗		NO❗
└	symbol	Public ❗		NO❗
└	decimals	Public ❗		NO❗

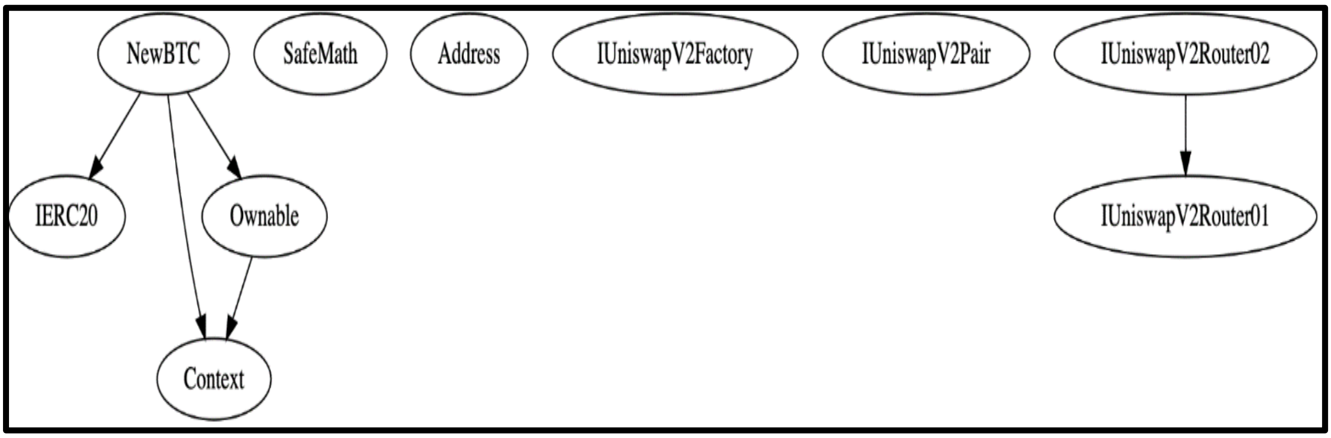
└	totalSupply	Public ❗️		NO❗️
└	balanceOf	Public ❗️		NO❗️
└	transfer	Public ❗️	🛑	NO❗️
└	allowance	Public ❗️		NO❗️
└	approve	Public ❗️	🛑	NO❗️
└	transferFrom	Public ❗️	🛑	NO❗️
└	increaseAllowance	Public ❗️	🛑	NO❗️
└	decreaseAllowance	Public ❗️	🛑	NO❗️
└	isExcludedFromReward	Public ❗️		NO❗️
└	totalFees	Public ❗️		NO❗️
└	deliver	Public ❗️	🛑	NO❗️
└	reflectionFromToken	Public ❗️		NO❗️
└	tokenFromReflection	Public ❗️		NO❗️
└	excludeFromReward	Public ❗️	🛑	onlyOwner
└	includeInReward	External ❗️	🛑	onlyOwner
└	_transferBothExcluded	Private 🔐	🛑	
└	excludeFromFee	Public ❗️	🛑	onlyOwner
└	includeInFee	Public ❗️	🛑	onlyOwner
└	setTaxFeePercent	External ❗️	🛑	onlyOwner
└	setLiquidityFeePercent	External ❗️	🛑	onlyOwner
└	setMaxTxPercent	External ❗️	🛑	onlyOwner
└	setSwapAndLiquifyEnabled	Public ❗️	🛑	onlyOwner
└		External ❗️	💵	NO❗️
└	_reflectFee	Private 🔐	🛑	

└	_getValues	Private 🔐		
└	_getTValues	Private 🔐		
└	_getRValues	Private 🔐		
└	_getRate	Private 🔐		
└	_getCurrentSupply	Private 🔐		
└	_takeLiquidity	Private 🔐	🛑	
└	calculateTaxFee	Private 🔐		
└	calculateLiquidityFee	Private 🔐		
└	removeAllFee	Private 🔐	🛑	
└	restoreAllFee	Private 🔐	🛑	
└	isExcludedFromFee	Public ❗		NO❗
└	_approve	Private 🔐	🛑	
└	_transfer	Private 🔐	🛑	
└	swapAndLiquify	Private 🔐	🛑	lockTheSwap
└	swapTokensForEth	Private 🔐	🛑	
└	addLiquidity	Private 🔐	🛑	
└	_tokenTransfer	Private 🔐	🛑	
└	_transferStandard	Private 🔐	🛑	
└	_transferToExcluded	Private 🔐	🛑	
└	_transferFromExcluded	Private 🔐	🛑	

Legend

Symbol	**Meaning**
🛑	**Function can modify state**
💵	**Function is payable**

Inheritance Hierarchy



Security issue checking status

- ❖ **High severity issues**

  No high severity issues found

- ❖ **Medium severity issues**

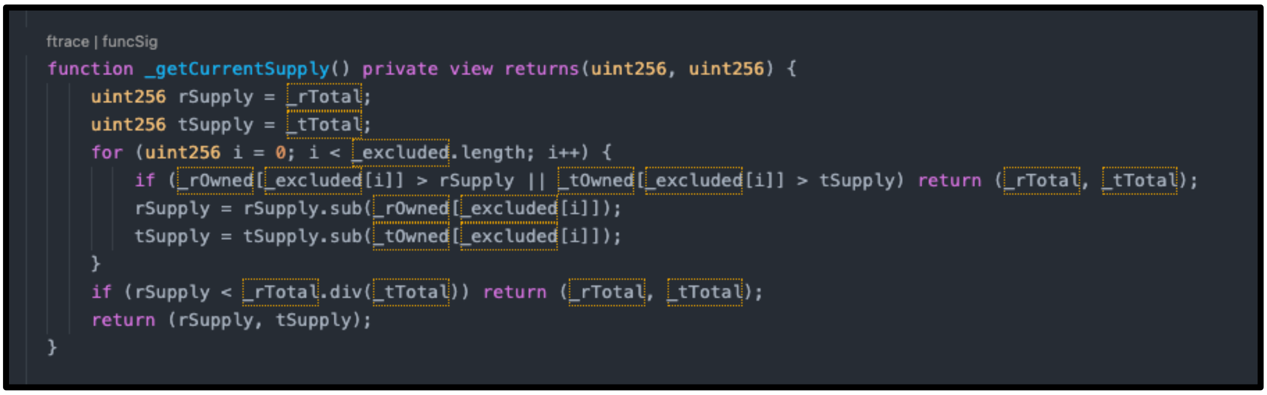
  No medium severity issues found

- ❖ **Low severity issues**

1. Out of gas

Issue:

➢ The function includeInReward() uses the loop to find and remove addresses from the _excluded list. Function will be aborted with OUT_OF_GAS exception if there will be a long excluded addresses list.



```
function _getCurrentSupply() private view returns(uint256, uint256) {
    uint256 rSupply = _rTotal;
    uint256 tSupply = _tTotal;
    for (uint256 i = 0; i < _excluded.length; i++) {
        if (_rOwned[_excluded[i]] > rSupply || _tOwned[_excluded[i]] > tSupply) return (_rTotal, _tTotal);
        rSupply = rSupply.sub(_rOwned[_excluded[i]]);
        tSupply = tSupply.sub(_tOwned[_excluded[i]]);
    }
    if (rSupply < _rTotal.div(_tTotal)) return (_rTotal, _tTotal);
    return (rSupply, tSupply);
}
```

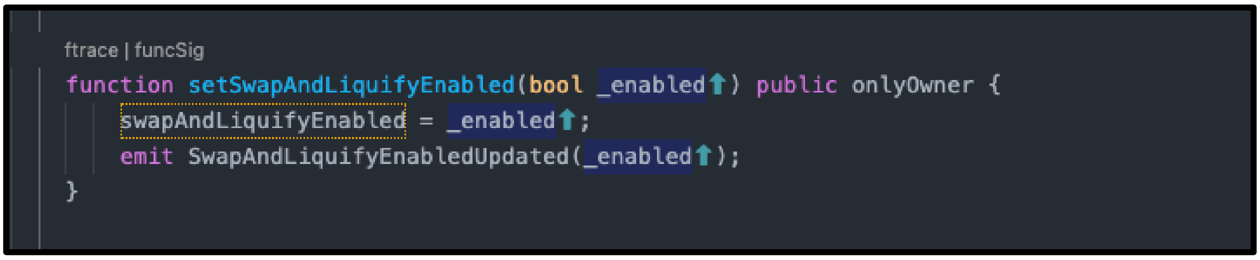
Recommendation:

Check that the excluded array length is not too big.

Owner privileges

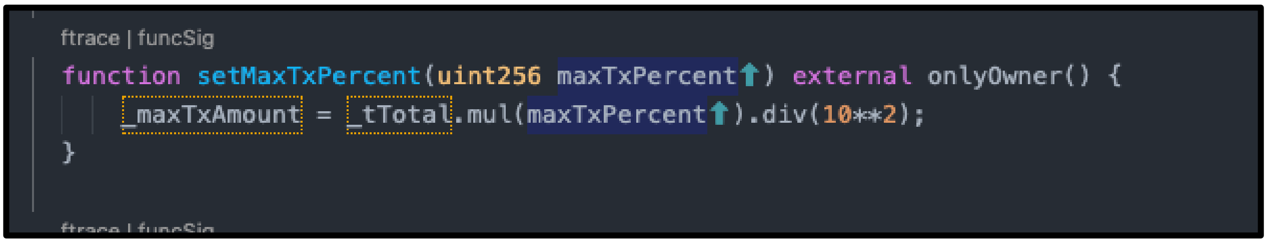
(In the period when the owner is not renounced)

- Owner can enable and disable the swap and liquify function.



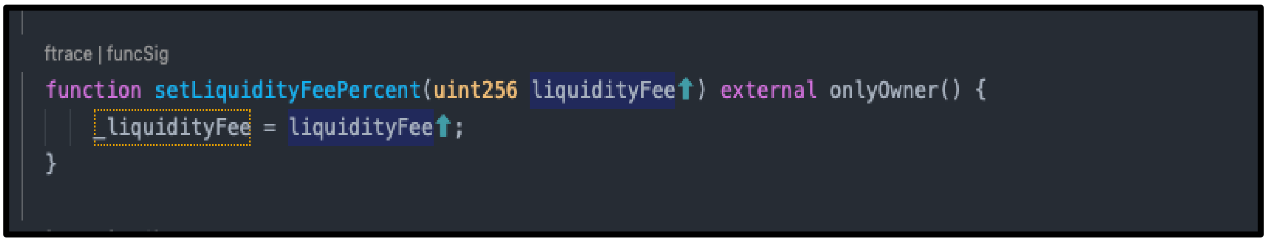
```
ftrace | funcSig
function setSwapAndLiquifyEnabled(bool _enabled) public onlyOwner {
    swapAndLiquifyEnabled = _enabled;
    emit SwapAndLiquifyEnabledUpdated(_enabled);
}
```

- Owner can change maximum transaction amount.



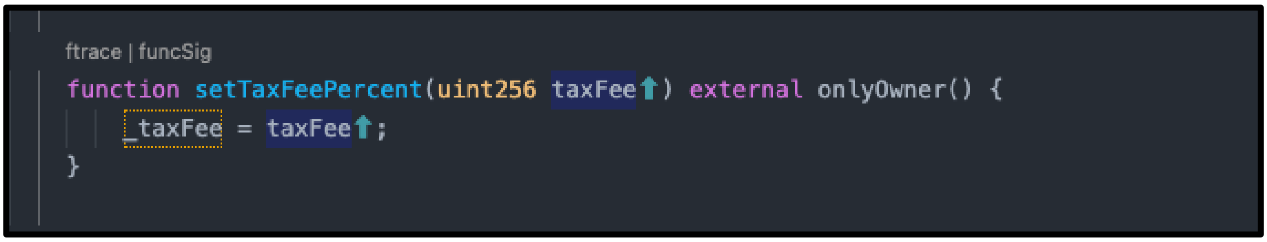
```
ftrace | funcSig
function setMaxTxPercent(uint256 maxTxPercent) external onlyOwner() {
    _maxTxAmount = _tTotal.mul(maxTxPercent).div(10**2);
}

ftrace | funcSig
```

- Owner can change liquidity fee.



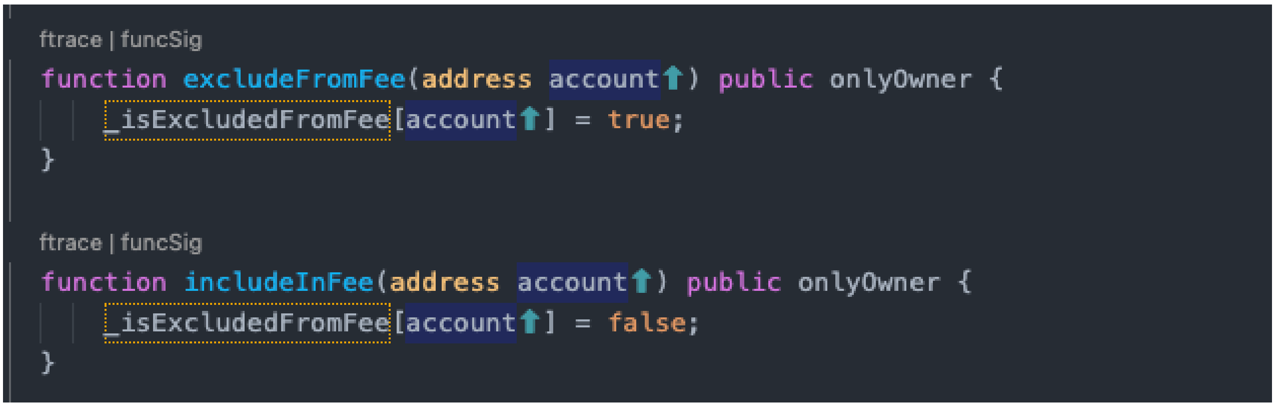
```
ftrace | funcSig
function setLiquidityFeePercent(uint256 liquidityFee) external onlyOwner() {
    _liquidityFee = liquidityFee;
}
```

- Owner can change tax fee.



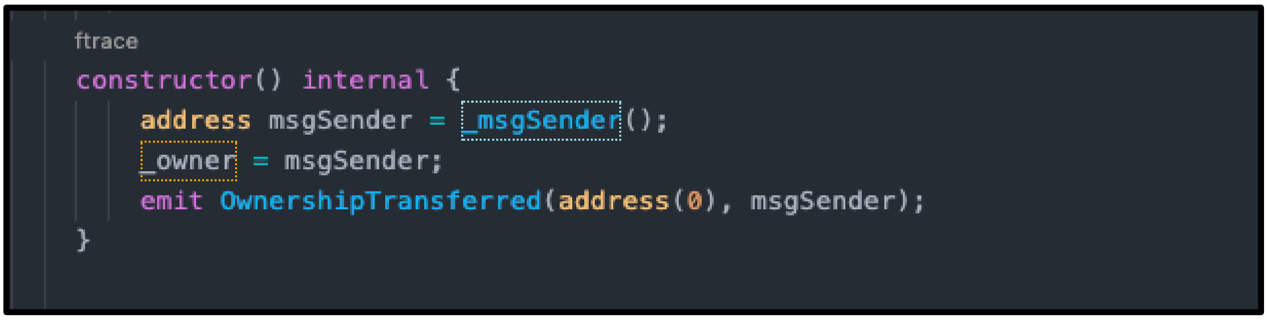
```
ftrace | funcSig
function setTaxFeePercent(uint256 taxFee) external onlyOwner() {
    _taxFee = taxFee;
}
```

❖ Owner can include and exclude accounts from fees.



```
ftrace | funcSig
function excludeFromFee(address account) public onlyOwner {
    _isExcludedFromFee[account] = true;
}

ftrace | funcSig
function includeInFee(address account) public onlyOwner {
    _isExcludedFromFee[account] = false;
}
```

❖ Owner can transfer the ownership.



```
ftrace
constructor() internal {
    address msgSender = _msgSender();
    _owner = msgSender;
    emit OwnershipTransferred(address(0), msgSender);
}
```

Audit conclusion

While conducting the audit of the NBTC smart contract, it was observed that there is nothing alarming with the code and the contract contains only low severity issues.