



RugFreeCoins Audit



NewSwap Token Audit

Smart Contract Security Audit

September 4, 2021

Contents

Audit details	1
Disclaimer	2
Background	3
About the project	4
Target market and the concept	6
Potential to grow with score points	9
Total Points	9
Contract details	10
Top token holders	11
Contract interaction details	12
Contract code function details	13
Contract description table	14
Security issue checking status	21
Owner privileges	23
Audit conclusion	26

Audit details

**Audited project**

NewSwap Token

**Contract Address**

0xDA03dEA150A070b8303e60265B740131867e4098

**Client contact**

NewSwap Team

**Blockchain**

Binance smart chain

**Project website**

<https://newswap.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 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 NewSwap to perform an audit of the smart contract.

<https://bscscan.com/token/0xDA03dEA150A070b8303e60265B740131867e4098>

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

NewSwap is a token built on the Binance Smart Chain. Each transaction, purchase and sale incur a 10% fee.

Features

- ❖ The **automatic NEWS tokens rewards of 2% when buying and selling** is what NewSwap attracts for the users: that tokens will be distributed among every holder proportional to how many tokens each individual holds.
- ❖ The **sustainability fee of 2% marketing** is what allows NEWS to hold the aforementioned promise. Tokens will be sent to a marketing wallet per transaction. This way, NewSwap will have enough funds to promote the coin and spend it for future development.
- ❖ The liquidity fee of 3%, which is a redistribution mechanism that ensures the trading pool always has sufficient liquidity. This is a key element for decentralized exchanges like Pancakeswap.
- ❖ **The 3% Charity fee when buying and selling** per transaction will be sent to a private wallet in tokens. This will empower the NewSwap community in the long run, and motivate more people to join in!

Tokenomics

10% fee when buying and selling

- ❖ 2% of trade goes to holders pockets in tokens.
- ❖ 2% of trade goes to the burn wallet.
- ❖ 3% of trade goes to the liquidity pool.
- ❖ 3% of trade goes to the charity wallet.

Roadmap

- ❖ Proper research and planning
- ❖ Testing and deployment of contract
- ❖ Blockchain contract audit
- ❖ Listing on the Pancakeswap
- ❖ White paper
- ❖ Website launch
- ❖ Launch of exchange and farms
- ❖ Marketing
- ❖ Partnerships with charity organizations
- ❖ Launch of NFTs and NFT store
- ❖ Launch of the merchandise store
- ❖ Commence Charity Donations
- ❖ The smooth running of system and development

Target market and the concept

Target market

- ❖ Anyone who's interested in Crypto space with long term investment plans.
- ❖ Anyone who's ready to earn a passive income by holding tokens.
- ❖ Anyone who's interested in trading tokens.
- ❖ Anyone who's interested in stake NewSwap tokens and earn rewards.
- ❖ Anyone who's interested in swap and trade tokens through the NewSwap platform.
- ❖ Anyone who's interested in taking part with the future NFT & merchandise platforms that's going to be built by the NewSwap team.
- ❖ Anyone who's interested in taking part with the good cause of the project by donating kids in Africa for their education and needs.
- ❖ Anyone who's interested in making financial transactions with any other party using NewSwap as the currency.

Core concept

The reward system

2% of each transaction when buying and selling gets sent amongst all holders in tokens. The holders will be eligible to receive tokens, whenever a transaction occurs, and rewards are proportional to how many tokens each individual holds.

Sustainable mechanism

The liquidity fee of 3%, which is a redistribution mechanism that ensures the trading pool always has sufficient liquidity.

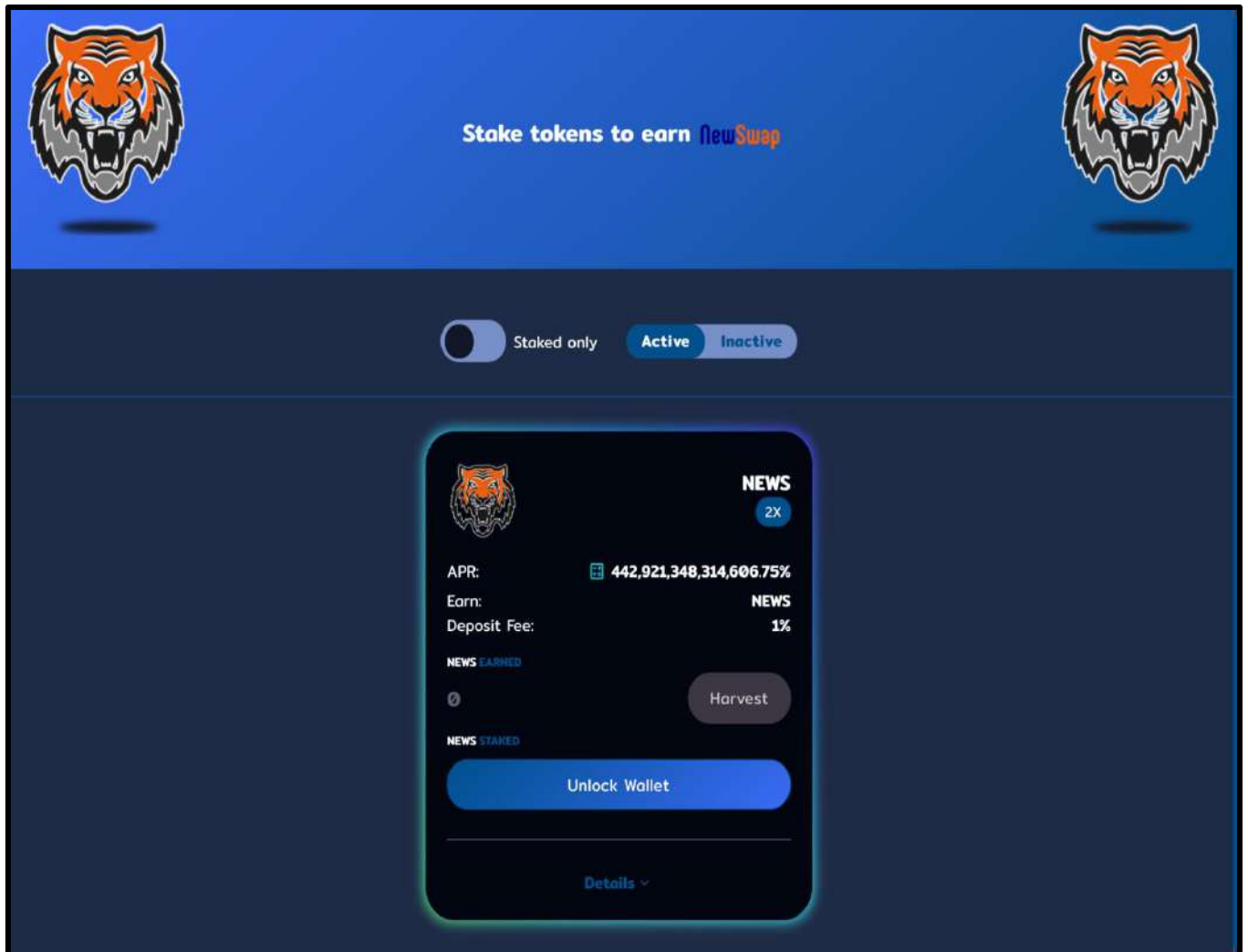
The **fee of 2% marketing** is what allows NewSwap to promote the token and use funds to further development of the platform.

Good cause

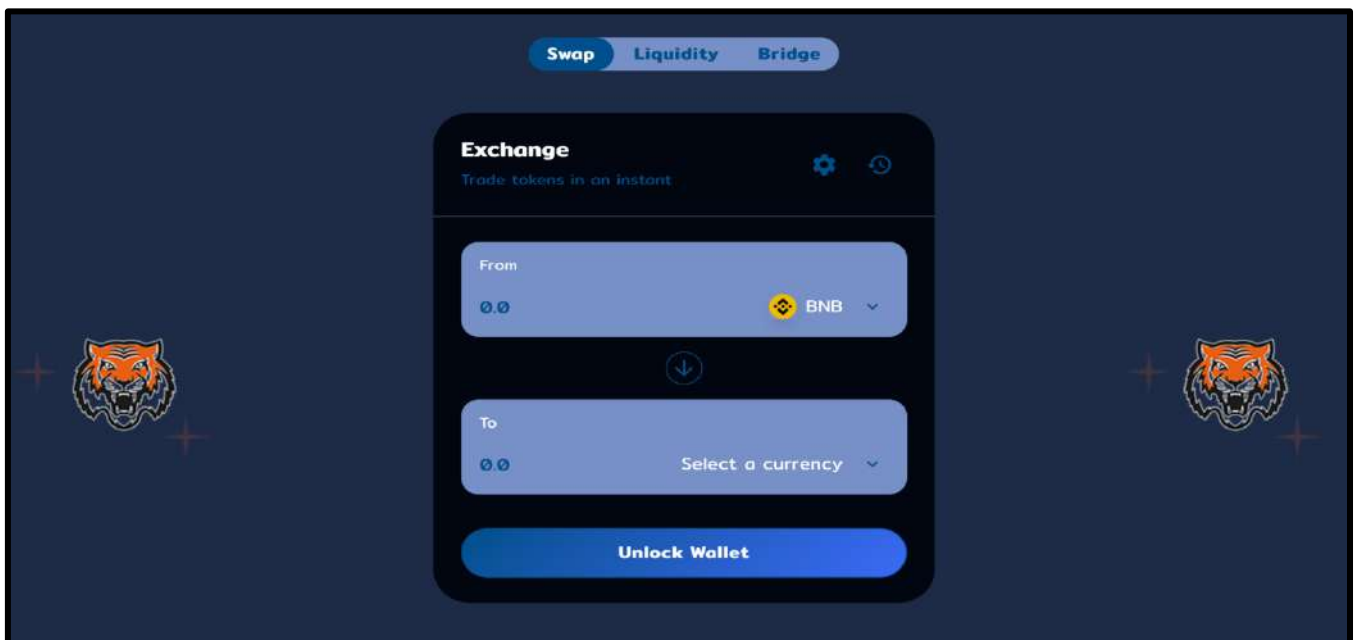
NewSwap, is committed to giving back to the community. A portion (3%) of every transaction will go toward school fees for young boys and girls in Africa. Daily, African families are forced to make a choice between keeping their children in school or putting them to work. One of the drivers of this decision is money. Many, once withdrawn, will never go back to school. Without any meaningful education, they are denied a fair competition in life. These children, their families and the world at-large, would never see the possible impacts that they could have made, had they had a chance at proper education. "The mind is a terrible thing to waste..." This may sound nebulous, but our target is one girl or boy at a time. We must never under-estimate the power of an educated mind to transform itself and it's surrounding.

The future plan

Stake tokens and earn rewards



Stake tokens and earn rewards



Platform for farming



NFT (Coming Soon)

Binance is the largest crypto exchange for digital currencies and tokens. They are also launching a marketplace for the trade of NFTs in the form of digital tokens. These tokens can be exchanged and traded just like other crypto tokens. Hence, this will increase competition among the creators and investors. According to the reports, the total sales of NFTs are more than \$2 billion in the first quarter of 2021.

This amount is more than that of previous sales of the same period which means that market is spreading very rapidly. The standard market allows 1% of the total amount for every sale or auction to the creator or owner. But Binance may allow a high standard market with 10% of the total proceed. Therefore, the competition is going to increase. Binance marketplace is also going to support small digital creators by reducing processing fees and the highest liquidity. In this way, NFTs are going to become a part of digital art in the future.

Potential to grow with score points

1.	Project efficiency	10/10
2.	Project uniqueness	9/10
3	Information quality	9/10
4	Service quality	9/10
5	System quality	10/10
6	Impact on the community	10/10
7	Impact on the business	9/10
8	Preparing for the future	10/10
Total Points		9.5/10

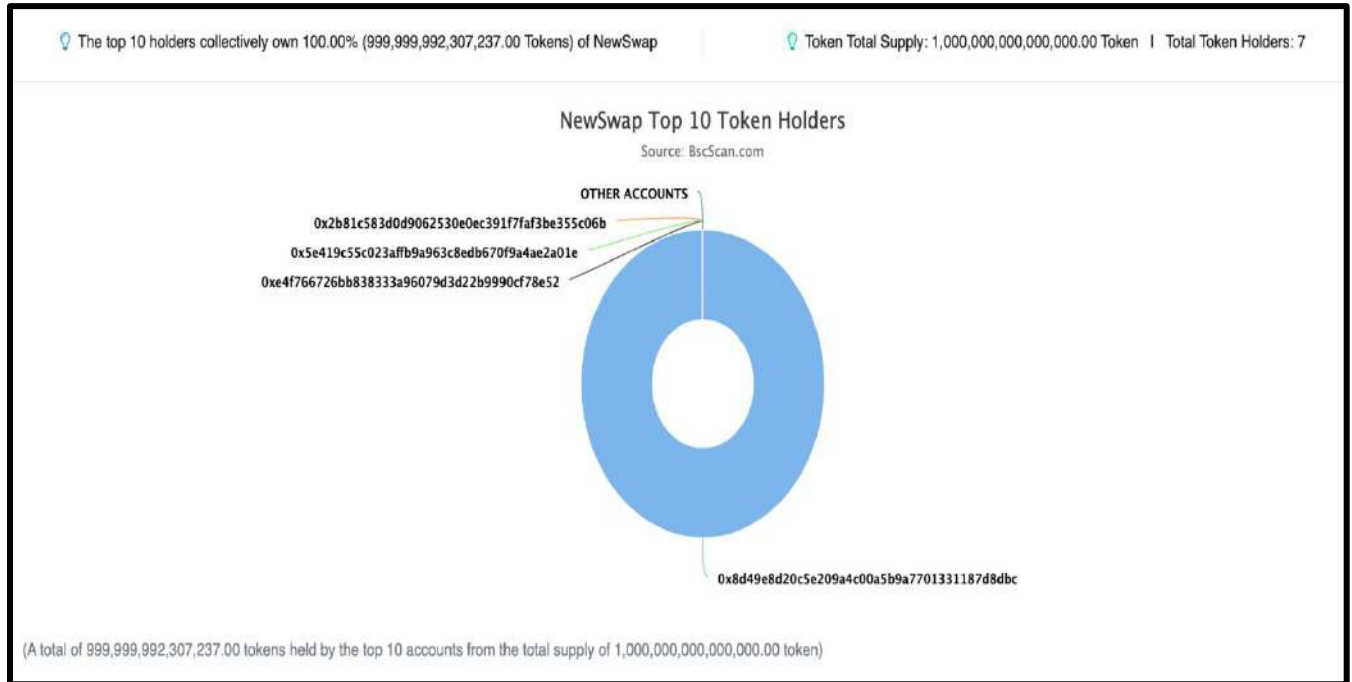
Contract details

Token contract details for 04th September 2021

Contract name	NewSwap
Contract address	0xDa03dEA150A070b8303e60265B740131867e4098
Token supply	1,000,000,000,000,000
Token ticker	NEWS
Decimals	9
Token holders	7
Transaction count	34
charity wallet address	0x2b81c583d0d9062530e0ec391f7faf3be355c06b
Contract deployer address	0x8D49e8d20c5e209A4C00A5B9A7701331187d8dBC
Contract's current owner address	0x8d49e8d20c5e209a4c00a5b9a7701331187d8dbc

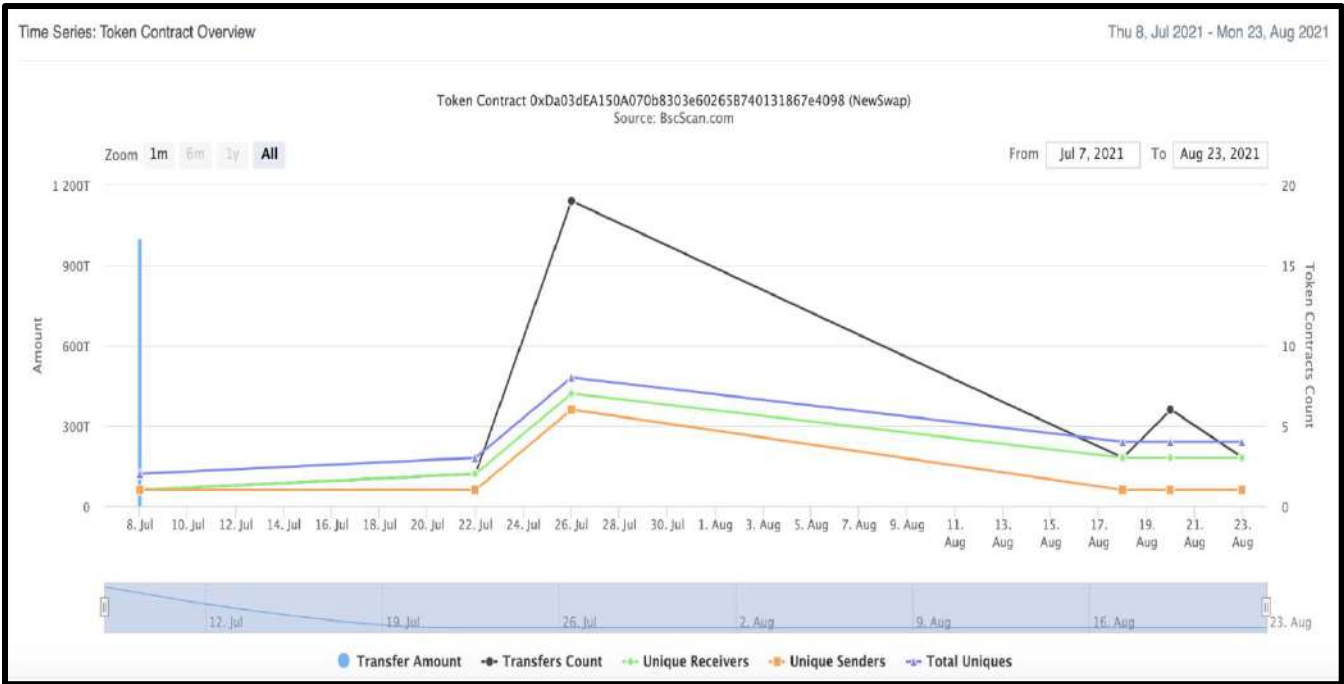
Top token holders

Top 10 Token Holders



Rank	Address	Quantity (Token)	Percentage
1	0x8d49e8d20c5e209a4c00a5b9a7701331187d8dbc	999,998,000,000,000	99.9998%
2	0xe4f766726bb838333a96079d3d22b9990cf78e52	1,099,832,918.805060582	0.0001%
3	0x5e419c55c023affb9a963c8edb670f9a4ae2a01e	884,693,628.43175442	0.0001%
4	0x2b81c583d0d9062530e0ec391f7fa3be355c06b	4,615,661.272015795	0.0000%
5	0x00	3,077,107.514677196	0.0000%
6	0xa089b1c8bdcbb0fbd8e0ab198bd39d61d917633b6	87,921.343814625	0.0000%
7	0x836664ccd7de8dd67bbf92f793a3205a9b86c4bf	0.000000089	0.0000%

Contract interaction details




























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		
L	Function Name	Visibility	Mutability	Modifiers
IERC20	Interface			
L	totalSupply	External 		NO 
L	balanceOf	External 		NO 
L	transfer	External 		NO 
L	allowance	External 		NO 
L	approve	External 		NO 
L	transferFrom	External 		NO 
SafeMath	Library			
L	add	Internal 		
L	sub	Internal 		
L	sub	Internal 		
L	mul	Internal 		
L	div	Internal 		
L	div	Internal 		
L	mod	Internal 		
L	mod	Internal 		
Context	Implementation			
L	_msgSender	Internal 		
L	_msgData	Internal 		

Address	Library			
L	isContract	Internal		
L	sendValue	Internal		
L	functionCall	Internal		
L	functionCall	Internal		
L	functionCallWithValue	Internal		
L	functionCallWithValue	Internal		
L	_functionCallWithValue	Private		
Ownable	Implementation	Context		
L		Internal		
L	owner	Public		NO
L	renounceOwnership	Public		onlyOwner
L	transferOwnership	Public		onlyOwner
L	geUnlockTime	Public		NO
L	lock	Public		onlyOwner
L	unlock	Public		NO
IUniswapV2Factory	Interface			
L	feeTo	External		NO
L	feeToSetter	External		NO
L	getPair	External		NO
L	allPairs	External		NO
L	allPairsLength	External		NO
L	createPair	External		NO
L	setFeeTo	External		NO
L	setFeeToSetter	External		NO



IUniswapV2Pair	Interface			
L	name	External ¶		NO¶
L	symbol	External ¶		NO¶
L	decimals	External ¶		NO¶
L	totalSupply	External ¶		NO¶
L	balanceOf	External ¶		NO¶
L	allowance	External ¶		NO¶
L	approve	External ¶	⦿	NO¶
L	transfer	External ¶	⦿	NO¶
L	transferFrom	External ¶	⦿	NO¶
L	DOMAIN_SEPARATOR	External ¶		NO¶
L	PERMIT_TYPEHASH	External ¶		NO¶
L	nonces	External ¶		NO¶
L	permit	External ¶	⦿	NO¶
L	MINIMUM_LIQUIDITY	External ¶		NO¶
L	factory	External ¶		NO¶
L	token0	External ¶		NO¶
L	token1	External ¶		NO¶
L	getReserves	External ¶		NO¶
L	price0CumulativeLast	External ¶		NO¶
L	price1CumulativeLast	External ¶		NO¶
L	kLast	External ¶		NO¶
L	mint	External ¶	⦿	NO¶
L	burn	External ¶	⦿	NO¶
L	swap	External ¶	⦿	NO¶
L	skim	External ¶	⦿	NO¶
L	sync	External ¶	⦿	NO¶

L	initialize	External ¶		NO¶
IUniswapV2Router01	Interface			
L	factory	External ¶		NO¶
L	WETH	External ¶		NO¶
L	addLiquidity	External ¶		NO¶
L	addLiquidityETH	External ¶		NO¶
L	removeLiquidity	External ¶		NO¶
L	removeLiquidityETH	External ¶		NO¶
L	removeLiquidityWithPermit	External ¶		NO¶
L	removeLiquidityETHWithPermit	External ¶		NO¶
L	swapExactTokensForTokens	External ¶		NO¶
L	swapTokensForExactTokens	External ¶		NO¶
L	swapExactETHForTokens	External ¶		NO¶
L	swapTokensForExactETH	External ¶		NO¶
L	swapExactTokensForETH	External ¶		NO¶
L	swapETHForExactTokens	External ¶		NO¶
L	quote	External ¶		NO¶
L	getAmountOut	External ¶		NO¶
L	getAmountIn	External ¶		NO¶
L	getAmountsOut	External ¶		NO¶
L	getAmountsIn	External ¶		NO¶
IUniswapV2Router02	Interface	IUniswapV2Router01		
L	removeLiquidityETHSupportingFeeOnTransferTokens	External ¶		NO¶
L	removeLiquidityETHWithPermitSupportingFeeOnTransferTokens	External ¶		NO¶
L	swapExactTokensForTokensSupportingFeeOnTransferTokens	External ¶		NO¶

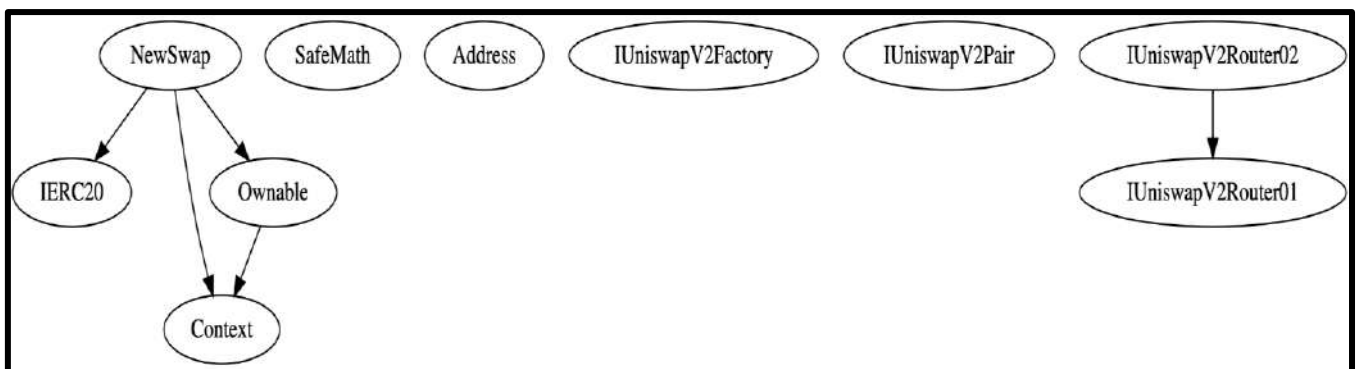
L	swapExactETHForTokensSupportingFeeOnTransferTokens	External ⚡		NO⚡
L	swapExactTokensForETHSupportingFeeOnTransferTokens	External ⚡		NO⚡
NewSwap	Implementation	Context, IERC20, Ownable		
L		Public ⚡		NO⚡
L	name	Public ⚡		NO⚡
L	symbol	Public ⚡		NO⚡
L	decimals	Public ⚡		NO⚡
L	totalSupply	Public ⚡		NO⚡
L	balanceOf	Public ⚡		NO⚡
L	transfer	Public ⚡		NO⚡
L	allowance	Public ⚡		NO⚡
L	approve	Public ⚡		NO⚡
L	transferFrom	Public ⚡		NO⚡
L	increaseAllowance	Public ⚡		NO⚡
L	decreaseAllowance	Public ⚡		NO⚡
L	isExcludedFromReward	Public ⚡		NO⚡
L	totalFees	Public ⚡		NO⚡
L	deliver	Public ⚡		NO⚡
L	reflectionFromToken	Public ⚡		NO⚡
L	tokenFromReflection	Public ⚡		NO⚡
L	excludeFromReward	Public ⚡		onlyOwner
L	includeInReward	External ⚡		onlyOwner
L	_transferBothExcluded	Private 🗑️		
L	excludeFromFee	Public ⚡		onlyOwner
L	includeInFee	Public ⚡		onlyOwner
L	setredistributeTax	External ⚡		onlyOwner

L	setburnAmount	External !		onlyOwner
L	setcharityAmount	External !		onlyOwner
L	setLiquidityFeePercent	External !		onlyOwner
L	setMaxTxPercent	External !		onlyOwner
L	setSwapAndLiquifyEnabled	Public !		onlyOwner
L		External !		NO!
L	_reflectFee	Private 		
L	_takefunds	Private 		
L	_getValues	Private 		
L	_getTValues	Private 		
L	_getRValues	Private 		
L	_getRate	Private 		
L	_getCurrentSupply	Private 		
L	_takeLiquidity	Private 		
L	calculateTaxFee	Private 		
L	calculateLiquidityFee	Private 		
L	removeAllFee	Private 		
L	restoreAllFee	Private 		
L	isExcludedFromFee	Public !		NO!
L	_approve	Private 		
L	_transfer	Private 		
L	swapAndLiquify	Private 		lockTheSwap
L	swapTokensForEth	Private 		
L	addLiquidity	Private 		
L	_tokenTransfer	Private 		
L	_transferStandard	Private 		
L	_transferToExcluded	Private 		
L	_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

- When The addLiquidity function calls the uniswapV2Router.addLiquidityETH function with the address specified as owner () for acquiring the generated LP tokens from the NewSwap-BNB pool. As a result, over time the _owner address will accumulate a significant portion of LP tokens. If the _owner is an EOA(Externally Owned Account), mishandling of its private key can have devastating consequences to the project as a whole.

```
ftrace | funcSig
function addLiquidity(uint256 tokenAmount↑, uint256 ethAmount↑) private {
    // approve token transfer to cover all possible scenarios
    _approve(address(this), address(uniswapV2Router), tokenAmount↑);

    // add the liquidity
    uniswapV2Router.addLiquidityETH{value: ethAmount↑}(
        address(this),
        tokenAmount↑,
        0, // slippage is unavoidable
        0, // slippage is unavoidable
        owner(),
        block.timestamp
    );
}
```


- **Out of gas issue**

In the `includeInReward` function, if they use a long wallet list there can be an `OUT_OF_GAS` issue, better to use a small array list at once.

```
ftrace | funcSig
function includeInReward(address account↑) external onlyOwner {
    require(!_isExcluded[account↑], "Account is already excluded");
    for (uint256 i = 0; i < _excluded.length; i++) {
        if (_excluded[i] == account↑) {
            _excluded[i] = _excluded[_excluded.length - 1];
            _tOwned[account↑] = 0;
            _isExcluded[account↑] = false;
            _excluded.pop();
            break;
        }
    }
}
```

Owner privileges

- ❖ The owner can include/exclude wallets from reward.

```
ftrace | funcSig
function excludeFromReward(address account↑) public onlyOwner {
    // require(account != 0x7a250d5630B4cF539739dF2C5dAcb4c659F2488D, 'We can not exclude Uniswap router. ');
    require(!_isExcluded[account↑], "Account is already excluded");
    if (_rOwned[account↑] > 0) {
        _tOwned[account↑] = tokenFromReflection(_rOwned[account↑]);
    }
    _isExcluded[account↑] = true;
    _excluded.push(account↑);
}

ftrace | funcSig
function includeInReward(address account↑) external onlyOwner {
    require(_isExcluded[account↑], "Account is already excluded");
    for (uint256 i = 0; i < _excluded.length; i++) {
        if (_excluded[i] == account↑) {
            _excluded[i] = _excluded[_excluded.length - 1];
            _tOwned[account↑] = 0;
            _isExcluded[account↑] = false;
            _excluded.pop();
            break;
        }
    }
}
```

- ❖ The owner can include/exclude wallets from fees.

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

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

- ❖ The owner can change all fees.

```
ftrace | funcSig
function setredistributeTax(uint256 taxFee↑) external onlyOwner {
    _taxFee = _taxFee.sub(_redistributeTax);
    _redistributeTax = taxFee↑;
    _taxFee = _taxFee.add(_redistributeTax);
}

ftrace | funcSig
function setburnAmount(uint256 amt↑) external onlyOwner {
    _taxFee = _taxFee.sub(_burn);
    _burn = amt↑;
    _taxFee = _taxFee.add(_burn);
}

ftrace | funcSig
function setcharityAmount(uint256 amt↑) external onlyOwner {
    _taxFee = _taxFee.sub(_charity);
    _charity = amt↑;
    _taxFee = _taxFee.add(_charity);
}

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

- ❖ The owner can change the max transaction amount.

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

- ❖ The owner can enable/disable swap and add liquidity.

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

- ❖ The owner can renounce and transfer ownership.

```
ftrace | funcSig
function renounceOwnership() public virtual onlyOwner {
    emit OwnershipTransferred(_owner, address(0));
    _owner = address(0);
}

/**
 * @dev Transfers ownership of the contract to a new account (`newOwner`).
 * Can only be called by the current owner.
 */
ftrace | funcSig
function transferOwnership(address newOwner) public virtual onlyOwner {
    require(
        newOwner != address(0),
        "Ownable: new owner is the zero address"
    );
    emit OwnershipTransferred(_owner, newOwner);
    _owner = newOwner;
}
```

Audit conclusion

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