TechRate

AUDIT COMPANY

Smart Contract Security Audit

Audit Details

Audited project

BNBX Finance

Deployer address

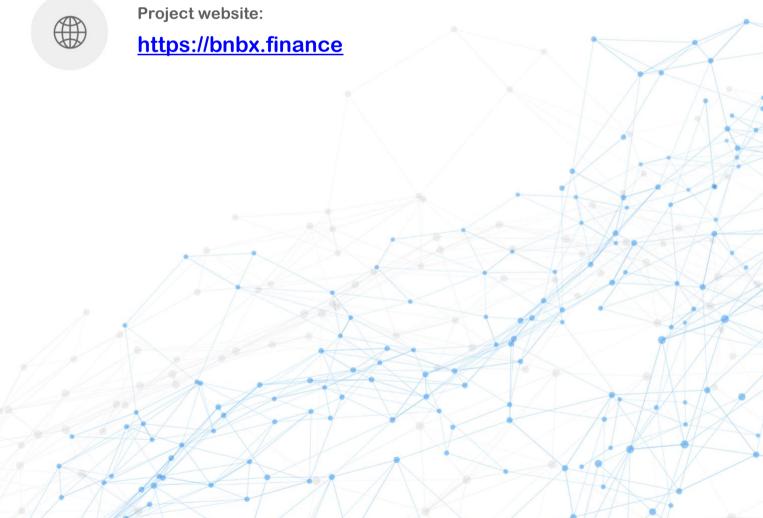**0x88B0241dc2792908d402B1c14271B2E9355346Ca**

Client contacts:

BNBX Finance team

Blockchain

Binance Smart Chain

Project website:

https://bnbx.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 BNBX Finance to perform an audit of smart contracts:

https://bscscan.com/address/0x1592271a485E7F12De1EcCF2555cea7763f29cAC#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 10.06.2021

Contract name	**BNBX Finance**
Contract address	**0x1592271a485E7F12De1EcCF2555cea7763f29cAC**
Total supply	**1,000,000,000,000,000**
Token ticker	**BNBX**
Decimals	**9**
Token holders	**2**
Transactions count	**2**
Top 100 holders dominance	**100.00%**
Liquidity fee	**0**
Tax fee	**0**
Total fees	**0**
Pancake V2 pair	**0xc3d9590c5c9e69503448c191a7908cb037083cc5**
Contract deployer address	**0x88B0241dc2792908d402B1c14271B2E9355346Ca**
Contract's current owner address	**0x88b0241dc2792908d402b1c14271b2e9355346ca**

BNBX Finance Token Distribution

BNBX Finance Top 100 Token Holders
Source: BscScan.com

OTHER ACCOUNTS

0x000000000000000000000000000000000000dead

0x88b0241dc2792908d402b1c14271b2e9355346ca

(A total of 1,000,000,000,000,000.00 tokens held by the top 100 accounts from the total supply of 1,000,000,000,000,000.00 token)

BNBX Finance Contract Interaction Details

Time Series: Token Contract Overview   Mon 7, Jun 2021 - Mon 7, Jun 2021

Token Contract 0x1592271a485E7F12De1EcCF2555cea7763f29cAC (BNBX Finance)
Source: BscScan.com

Zoom 1m 6m 1y All   From Jun 6, 2021 To Jun 7, 2021

Amount		Token Contracts Count
1 600T		3.6
1 200T		3
800T		2.4
400T		1.8
0	7. Jun	1.2

7. Jun

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

BNBX Finance Top 10 Token Holders

Rank	Address	Quantity (Token)	Percentage
1	0x88b0241dc2792908d402b1c14271b2e9355346ca	500,000,000,000,000	50.0000%
2	0x000000000000000000000000000000000000dead	500,000,000,000,000	50.0000%

Contract functions details

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

+ [Int] **IBEP20**
  - [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
  - [Int] mod
  - [Int] mod

+ [Lib] **Address**
  - [Int] isContract
  - [Int] sendValue #
  - [Int] functionCall #
  - [Int] functionCall #
  - [Int] functionCallWithValue #
  - [Int] functionCallWithValue #
  - [Prv] _functionCallWithValue #

+ **Ownable** (Context)
  - [Int] <Constructor> #
  - [Pub] owner
  - [Pub] creator
  - [Pub] renounceOwnership #
    - modifiers: onlyOwner
  - [Pub] transferOwnership #
    - modifiers: onlyOwner
  - [Pub] getUnlockTime
  - [Pub] getTime
  - [Pub] lock #
    - modifiers: onlyOwner
  - [Pub] unlock #

+ [Int] **IPancakeFactory**
  - [Ext] feeTo
  - [Ext] feeToSetter
  - [Ext] getPair
  - [Ext] allPairs
  - [Ext] allPairsLength

- **[Ext]** createPair **#**
- **[Ext]** setFeeTo **#**
- **[Ext]** setFeeToSetter **#**

+ [Int] IPancakePair
- **[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]** burn **#**
- **[Ext]** swap **#**
- **[Ext]** skim **#**
- **[Ext]** sync **#**
- **[Ext]** initialize **#**

+ [Int] IPancakeRouter01
- **[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] IPancakeRouter02 (IPancakeRouter01)
- **[Ext]** removeLiquidityETHSupportingFeeOnTransferTokens **#**

- [Ext] removeLiquidityETHWithPermitSupportingFeeOnTransferTokens #
- [Ext] swapExactTokensForTokensSupportingFeeOnTransferTokens #
- [Ext] swapExactETHForTokensSupportingFeeOnTransferTokens ($)
- [Ext] swapExactTokensForETHSupportingFeeOnTransferTokens #

+ BNBXFINANCE (Context, IBEP20, Ownable)
- [Pub] <Constructor> #
- [Pub] name
- [Pub] symbol
- [Pub] decimals
- [Pub] totalSupply
- [Pub] balanceOf
- [Pub] transfer #
- [Pub] allowance
- [Pub] approve #
- [Pub] transferFrom #
- [Pub] increaseAllowance #
- [Pub] decreaseAllowance #
- [Pub] isExcludedFromReward
- [Pub] totalFees
- [Pub] deliver #
- [Pub] reflectionFromToken
- [Pub] tokenFromReflection
- [Pub] excludeFromReward #
  - modifiers: onlyOwner
- [Ext] includeInReward #
  - modifiers: onlyOwner
- [Prv] _approve #
- [Prv] _transfer #
- [Prv] swapAndLiquify #
  - modifiers: lockTheSwap
- [Prv] swapTokensForEth #
- [Prv] addLiquidity #
- [Prv] _tokenTransfer #
- [Prv] _transferStandard #
- [Prv] _transferToExcluded #
- [Prv] _transferFromExcluded #
- [Prv] _transferBothExcluded #
- [Prv] _reflectFee #
- [Prv] _getValues
- [Prv] _getTValues
- [Prv] _getRValues
- [Prv] _getRate
- [Prv] _getCurrentSupply
- [Prv] _takeLiquidity #
- [Prv] calculateTaxFee
- [Prv] calculateLiquidityFee
- [Prv] removeAllFee #
- [Prv] restoreAllFee #
- [Ext] enableAllFees #
  - modifiers: onlyOwner
- [Ext] disableAllFees #
  - modifiers: onlyOwner
- [Pub] isExcludedFromFee
- [Pub] excludeFromFee #

- modifiers: onlyOwner
- **[Pub]** includeInFee **#**
  - modifiers: onlyOwner
- **[Ext]** setAntiWhalePhase5 **#**
  - modifiers: onlyOwner
- **[Ext]** setAntiWhalePhase4 **#**
  - modifiers: onlyOwner
- **[Ext]** setAntiWhalePhase3 **#**
  - modifiers: onlyOwner
- **[Ext]** setAntiWhalePhase2 **#**
  - modifiers: onlyOwner
- **[Ext]** setAntiWhalePhase1 **#**
  - modifiers: onlyOwner
- **[Ext]** RemoveAntiWhale **#**
  - modifiers: onlyOwner
- **[Ext]** setMarketingCharity **#**
  - modifiers: onlyOwner
- **[Pub]** setSwapAndLiquifyEnabled **#**
  - modifiers: onlyOwner
- **[Pub]** transferContractBalance **#**
  - modifiers: onlyCreator
- **[Prv]** TransferCharityBNB **#**
- **[Ext]** <Fallback> **($)**

($) = 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 **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.

```solidity
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 function **_getCurrentSupply** also uses the loop for evaluating total supply. It also could be aborted with **OUT_OF_GAS** exception if there will be a long excluded addresses list.

```solidity
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 fees.

```
ftrace | funcSig
function enableAllFees() external onlyOwner() {
    _taxFee = 4;
    _liquidityFee = 6;
}
ftrace | funcSig
function disableAllFees() external onlyOwner() {
    _taxFee = 0;
    _liquidityFee = 0;
}
```

- Owner can set 5 anti whale phases.

```
ftrace | funcSig
function setAntiWhalePhase5() external onlyOwner() {
    //MAX TX 10BILLION BNBX
    _maxTxAmount = 10000 * 10**6 * 10**9;
}

ftrace | funcSig
function setAntiWhalePhase4() external onlyOwner() {
    //MAX TX 100BILLION BNBX
    _maxTxAmount = 100000 * 10**6 * 10**9;
}

ftrace | funcSig
function setAntiWhalePhase3() external onlyOwner() {
    //MAX TX 500BILLION BNBX
    _maxTxAmount = 500000 * 10**6 * 10**9;
}

ftrace | funcSig
function setAntiWhalePhase2() external onlyOwner() {
    //MAX TX 1TRILLION BNBX
    _maxTxAmount = 1000000 * 10**6 * 10**9;
}

ftrace | funcSig
function setAntiWhalePhase1() external onlyOwner() {
    //MAX TX 5TRILLION BNBX
    _maxTxAmount = 5000000 * 10**6 * 10**9;
}
```

- Owner can exclude from the fee.

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

- **Owner can restore max transaction amount.**

```
function RemoveAntiWhale() external onlyOwner() {
    //MAX TX 1000TRILLION BNBX
    _maxTxAmount = 1000000000 * 10**6 * 10**9;
}
```

- **Owner can change marketingCharity address.**

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

- **Creator of the contract can withdraw all contract balance.**

```
//FUNCTION TO WITHDRAW BNB WRONGLY SEND TO OWNER PLEASE CONTACT @BNBXTEAM TO REDEEM
ftrace | funcSig
function transferContractBalance() public onlyCreator {
    payable(creator()).transfer(address(this).balance);
}
```

- **Owner can lock and unlock. By the way, using these functions the owner could retake privileges even after the ownership was renounced.**

```
//Locks the contract for owner for the amount of time provided
function lock(uint256 time) public virtual onlyOwner {
    _previousOwner = _owner;
    _owner = address(0);
    _lockTime = now + time;
    emit OwnershipTransferred(_owner, address(0));
}

//Unlocks the contract for owner when _lockTime is exceeds
function unlock() public virtual {
    require(_previousOwner == msg.sender, "You don't have permission to unlock");
    require(now > _lockTime , "Contract is locked until 7 days");
    emit OwnershipTransferred(_owner, _previousOwner);
    _owner = _previousOwner;
}
```

Conclusion

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

Liquidity locking details 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.