Smart Contract Security Audit

Audit details:

Audited project:	XBN Community Token
Deployer address:	0xd6da6e2c0432e8ebfd8a2258339d04f01b5da528
Client contacts:	XBN Community Token team
Blockchain:	Binance Smart Chain
Project website:	https://www.xbn.finance/xbc/

May, 2021
TechRate

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 XBN Community Token to perform an audit of smart contracts:

- *https://bscscan.com/address/0x0321394309cad7e0e424650844c3ab3b659315d3#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 08.05.2021.

Contract name:	XBN Community Token
Contract address:	0x0321394309cad7e0e424650844c3ab3b659315d3
Total supply:	100000000000000000000000000
Token ticker:	XBC
Decimals:	9
Token holders:	40493
Transactions count:	107849
Top 100 holders dominance:	69.44 %
Liquidity fee:	8
Tax fee:	2
Total fees:	73769382741270392109909
Pancake pair:	0x2e8da1ec183c2854fe4973fd5edf3dc0e78b873d
Contract deployer address:	0xd6da6e2c0432e8ebfd8a2258339d04f01b5da528
Contract’s current owner address:	0xd6da6e2c0432e8ebfd8a2258339d04f01b5da528

XBN Community Token distribution

The top 100 holders collectively own 69.44%
(694,431,387,355,050.00 Tokens) of XBN Community Token

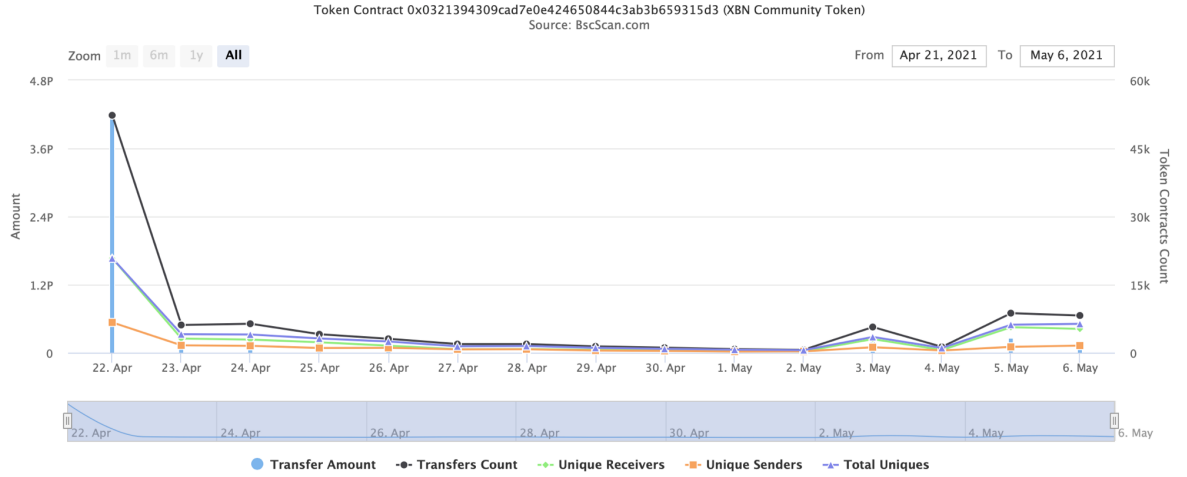
Token Total Supply: 1,000,000,000,000,000.00 Token | Total Token Holders: 40,493

(A total of 694,431,387,355,050.00 tokens held by the top 100 accounts from the total supply of 1,000,000,000,000,000.00 token)

XBN Community Token contract interaction details

Time Series: Token Contract Overview

Thu 22, Apr 2021 - Thu 6, May 2021



XBN Community Token top 10 token holders

Rank	Address	Quantity (Token)	Percentage
1	PancakeSwap: XBC 2	77,556,281,157,614.231402606	7.7556%
2	0x256e637b98968785662d57d7ded3de018142585e	59,075,812,989,658.388501655	5.9076%
3	0x020b0c6d05fdf1713ce9b5672c8c3da7bcb8119c	49,791,177,165,576.440559637	4.9791%
4	0x7bf6a5a556546654bd59bf98f8442c4cae661f43	37,472,070,799,465.113510801	3.7472%
5	0x9f77b0bb12221cc05969e608e2ea1615ec42907e	34,825,555,528,617.750896388	3.4826%
6	0xd182de2a5019592c7afeb8426533d9ce94fed765	33,687,584,397,036.233988151	3.3688%
7	0x76b59b86102d04b972298a6a3ea14daa9667e59b	30,800,159,930,405.23300272	3.0800%
8	0xe0ffd928f2eda22795f860b8c396179e47799e39	27,108,754,310,093.973372351	2.7109%
9	0xb1c86a62eca7f389fb763a4e1fd692143e4e28ad	25,265,996,143,406.830397986	2.5266%
10	0x000000000000000000000000000000000000dead	23,720,038,861,218.481432568	2.3720%

XBN Community Token LP top 10 token holders

Rank	Address	Quantity	Percentage
1	0x000000000000000000000000000000000000dead	6,539.843169966348414184	97.1488%
2	0xd6da6e2c0432e8ebfd8a2258339d04f01b5da528	105.878240700931555995	1.5728%
3	0x9e2c4933d6228a69149e3011cb1302f3e46a4263	85.568160511877210685	1.2711%
4	0x994640e1c699c07405a85b4d4302bebfe5873b75	0.476800242543320783	0.0071%
5	0x9b0f6bc4f7fc6f2e610d0a91dfde50e44b05559d	0.008537532056756911	0.0001%
6	0xadbeaeb20e6c9a8b9eb528e1b87b8cd1cd26f0cf	0.006917931437518482	0.0001%
7	0x0000000000000000000000000000000000000000	0.000000000000001	0.0000%

Contract functions details

+ [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

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

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

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

+ [Lib] Utils
  - [Prv] random
  - [Prv] isLotteryWon
  - [Pub] calculateBNBReward
  - [Pub] calculateTopUpClaim #
  - [Pub] swapTokensForEth #
  - [Pub] swapETHForTokens #
  - [Pub] addLiquidity #

+ ReentrancyGuard
  - [Pub] <Constructor> #

+ XBCToken (Context, IBEP20, Ownable, ReentrancyGuard)
  - [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] _transferBothExcluded #
- [Pub] excludeFromFee #
  - modifiers: onlyOwner
- [Pub] includeInFee #
  - modifiers: onlyOwner
- [Ext] setTaxFeePercent #
  - modifiers: onlyOwner
- [Ext] setLiquidityFeePercent #
  - modifiers: onlyOwner
- [Pub] setSwapAndLiquifyEnabled #
  - modifiers: onlyOwner
- [Ext] <Fallback> ($)
- [Prv] _reflectFee #
- [Prv] _getValues
- [Prv] _getTValues
- [Prv] _getRValues
- [Prv] _getRate
- [Prv] _getCurrentSupply
- [Prv] _takeLiquidity #
- [Prv] calculateTaxFee
- [Prv] calculateLiquidityFee
- [Prv] removeAllFee #
- [Prv] restoreAllFee #
- [Pub] isExcludedFromFee
- [Prv] _approve #
- [Prv] _transfer #
- [Prv] _tokenTransfer #
- [Prv] _transferStandard #
- [Prv] _transferToExcluded #
- [Prv] _transferFromExcluded #
- [Pub] setMaxTxPercent #
  - modifiers: onlyOwner
- [Pub] calculateBNBReward
- [Pub] getRewardCycleBlock
- [Pub] claimBNBReward #
  - modifiers: nonReentrant
- [Prv] topUpClaimCycleAfterTransfer #
- [Prv] ensureMaxTxAmount #
- [Pub] disruptiveTransfer ($)
- [Prv] swapAndLiquify #
- [Pub] activateContract #

    - modifiers: onlyOwner
  - [Pub] activateTestnet #
    - 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 `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 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.

```
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:

Use EnumerableSet instead of array or do not use long arrays.

Owner privileges

- ❏ Owner can change the tax and liquidity fee.
- ❏ Owner can change the maximum transaction amount.
- ❏ Owner can exclude from the fee.
- ❏ Owner can activate the contract a few times using functions activateContract and activateTestnet.

Recommendations

- ❏ activateTestnet function should be removed!

Conclusion

Smart contracts contain low severity issues, recommendations and owner privileges! Liquidity pair contract is not checked due to out of scope. No liquidity locking info 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.