Techrate1 Techrate

TechRate

AUDIT COMPANY

Smart Contract Security Audit

TechRate

November, 2021

Audit Details

Audited project

BigNFT

Deployer address

0xf85b3a2f47a93237f6fc00c7a8fbb373933b6675

Client contacts:

BigNFT team

Blockchain

Binance Smart Chain

Project website:

https://www.bignft.io

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 BigNFT to perform an audit of smart contracts:

https://bscscan.com/address/0xace6907e65c9e3445bba25c013c437c7ed124036#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

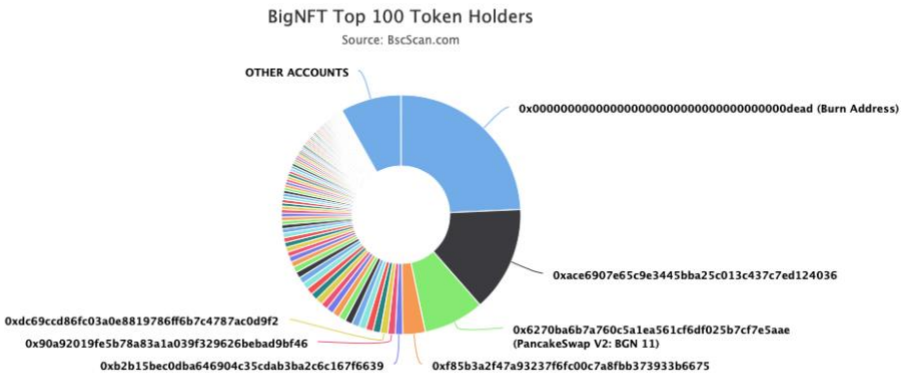
Token contract details for 10.11.2021

Contract name	BigNFT
Contract address	0xaCE6907E65C9E3445bBa25c013C437C7Ed124036
Total supply	24,000,000
Token ticker	BGN
Decimals	9
Token holders	429
Transactions count	5,167
Top 100 holders dominance	91.80%
Marketing fee receiver	0xf85b3a2f47a93237f6fc00c7a8fbb373933b6675
Autoliquidity receiver	0xace6907e65c9e3445bba25c013c437c7ed124036
Total fee	10
Uniswap V2 pair	0x6270ba6b7a760c5a1ea561cf6df025b7cf7e5aae
Contract deployer address	0xf85b3a2f47a93237f6fc00c7a8fbb373933b6675
Contract's current owner address	0xf85b3a2f47a93237f6fc00c7a8fbb373933b6675

BigNFT Token Distribution

The top 100 holders collectively own 91.80% (22,032,249.38 Tokens) of BigNFT

Token Total Supply: 24,000,000.00 Token | Total Token Holders: 429

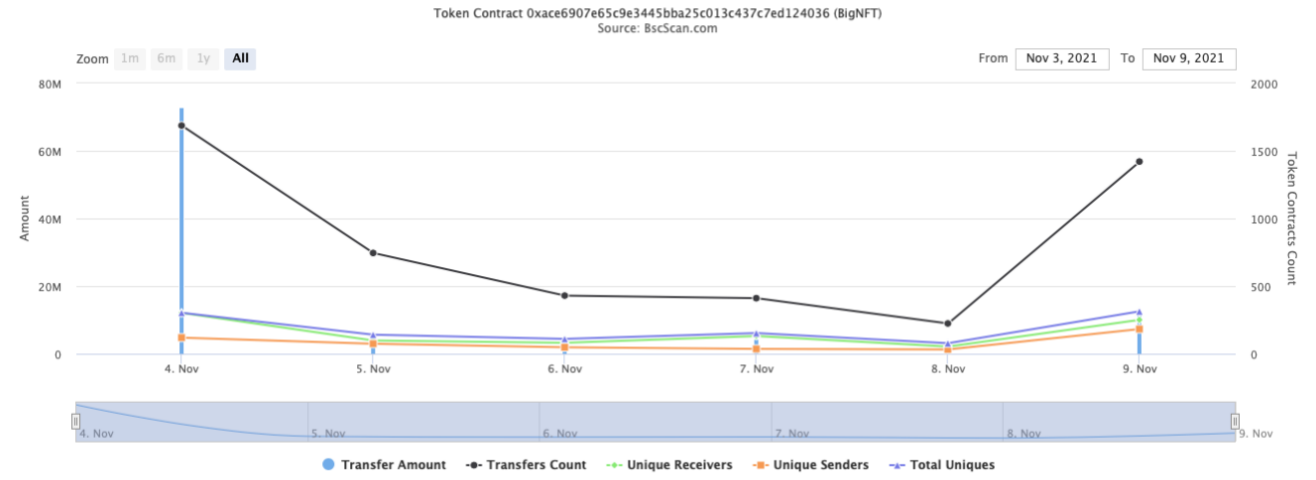


(A total of 22,032,249.38 tokens held by the top 100 accounts from the total supply of 24,000,000.00 token)

BigNFT Contract Interaction Details

Time Series: Token Contract Overview

Thu 4, Nov 2021 - Tue 9, Nov 2021



BigNFT Top 10 Token Holders

Rank	Address	Quantity (Token)	Percentage
1	Burn Address	5,831,017.288439317	24.2959%
2	0xace6907e65c9e3445bba25c013c437c7ed124036	3,418,054.472726615	14.2419%
3	PancakeSwap V2: BGN 11	1,969,615.993291041	8.2067%
4	0xf85b3a2f47a93237f6fc00c7a8fbb373933b6675	730,084	3.0420%
5	0xb2b15bec0dba646904c35cdab3ba2c6c167f6639	240,000	1.0000%
6	0x90a92019fe5b78a83a1a039f329626bebad9bf46	240,000	1.0000%
7	0xdc69ccd86fc03a0e8819786ff6b7c4787ac0d9f2	240,000	1.0000%
8	0xbb8682a5ff1f80f63d19649d928772ce39828ee9	239,999.79	1.0000%
9	0x9a9370ae498c6a1f030a18a4355739f1c0abcc8b	239,995.8	1.0000%
10	0xa4a14da2ff8050d36f596336d013e0a20d2b1091	238,300	0.9929%

Contract functions details

+ [Int] IBEP20
  - [Ext] totalSupply
  - [Ext] decimals
  - [Ext] symbol
  - [Ext] name
  - [Ext] getOwner
  - [Ext] balanceOf
  - [Ext] transfer #
  - [Ext] allowance
  - [Ext] approve #
  - [Ext] transferFrom #

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

+ Auth
  - [Pub] <Constructor> #
  - [Pub] authorize #
    - modifiers: onlyOwner
  - [Pub] unauthorize #
    - modifiers: onlyOwner
  - [Pub] isOwner
  - [Pub] isAuthorized
  - [Pub] transferOwnership #
    - modifiers: onlyOwner
  - [Pub] lockOwner #
    - modifiers: onlyOwner
  - [Pub] seeLockedTime
  - [Pub] unlock #

+ [Int] IDEXFactory
  - [Ext] createPair #

+ [Int] IDEXRouter
  - [Ext] factory
  - [Ext] WETH
  - [Ext] addLiquidity #
  - [Ext] addLiquidityETH ($)
  - [Ext] swapExactTokensForTokensSupportingFeeOnTransferTokens #
  - [Ext] swapExactETHForTokensSupportingFeeOnTransferTokens ($)
  - [Ext] swapExactTokensForETHSupportingFeeOnTransferTokens #

+ BigNFT (IBEP20, Auth)
  - [Pub] <Constructor> #
    - modifiers: Auth
  - [Ext] <Fallback> ($)

- [Ext] totalSupply
- [Ext] decimals
- [Ext] symbol
- [Ext] name
- [Ext] getOwner
- [Pub] balanceOf
- [Ext] allowance
- [Pub] approve #
- [Ext] approveMax #
- [Ext] transfer #
- [Ext] transferFrom #
- [Int] _transferFrom #
- [Int] _basicTransfer #
- [Int] checkTxLimit
- [Int] checkMaxWalletLimit
- [Int] checkBlackList
- [Int] shouldTakeFee
- [Int] takeFee #
- [Int] shouldSwapBack
- [Ext] clearStuckBalance #
  - modifiers: onlyOwner
- [Ext] clearStuckBalance #
  - modifiers: onlyOwner
- [Pub] getCirculatingSupply
- [Pub] getLiquidityBacking
- [Pub] isOverLiquified
- [Int] swapAndLiquify #
  - modifiers: lockTheSwap
- [Ext] setBlacklistSwitch #
  - modifiers: authorized
- [Ext] addToBlackList #
  - modifiers: authorized
- [Ext] setTargetLiquidity #
  - modifiers: authorized
- [Ext] setTranscSettings #
  - modifiers: authorized
- [Ext] setQuickPairSettings #
  - modifiers: authorized
- [Ext] setIsFeeExempt #
  - modifiers: authorized
- [Ext] setIsTxLimitExempt #
  - modifiers: authorized
- [Ext] setIsTimelockExempt #
  - modifiers: authorized
- [Ext] setFees #
  - modifiers: authorized
- [Ext] setFeeReceivers #
  - modifiers: authorized
- [Ext] setSwapBackSettings #
  - modifiers: authorized
- [Pub] setTradingOnDexState #
  - modifiers: onlyOwner
- [Pub] setCooldownEnabledState #
  - modifiers: onlyOwner
- [Ext] vIsExemptedFromFee

    - modifiers: authorized
  - [Ext] vIsExemptedFromMaxHold
    - modifiers: authorized
  - [Ext] vIsExemptedFromMaxTx
    - modifiers: authorized
  - [Ext] viewStuckBNBBalance
    - modifiers: authorized
  - [Ext] vIsBlacklisted
    - modifiers: authorized
  - [Ext] sendOldTokensToBibHolders #
    - 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 `sendOldTokensToBibHolders()` uses the loop to distribute token amount from function argument to addresses list from function argument. Function will be aborted with `OUT_OF_GAS` exception if there will be a long addresses list.

Recommendation:
Check that the arrays' length is not too big.

Owner privileges (In the period when the owner is not renounced)

- Owner can withdraw contract BNBs.
- Owner can enable trading.
- Owner can enable/disable cooldown and change cooldown timer interval.
- Authorized addresses can enable/disable blacklistingSwitch.
- Authorized addresses can blacklist addresses.
- Authorized addresses can change target liquidity.
- Authorized addresses can change the maximum transaction amount and max hold amount.
- Authorized addresses can add addresses in multiple exclusions.
- Authorized addresses can change fees and fee receivers.
- Authorized addresses can enable/disable swap and change swapThreshold.
- Owner can lock and unlock. By the way, using these functions the owner could retake privileges even after the ownership was renounced.

Conclusion

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

Liquidity locking details provided by the team:
https://deeplock.io/lock/0x6270Ba6B7A760c5a1ea561CF6DF025b7cF7e5aAe

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.