TechRate

AUDIT COMPANY

Smart Contract Security Audit

Audit Details

Audited project

NFTBlackMarket

Deployer address

0xCABAFa6736aFc9bd9cF68c573eBf9569A55AFdda

Client contacts:

NFTBlackMarket team

Blockchain

Binance Smart Chain

Project website:

http://NFTBlackMarket.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.

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 NFTBlackMarket to perform an audit of smart contracts:
https://bscscan.com/address/0x12da2f2761038486271c99da7e0fb4413e2b5e38#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 23.06.2021

Contract name	NFTBlackMarket
Contract address	0x12Da2f2761038486271C99DA7e0FB4413e2B5E38
Total supply	1,000,000,000,000,000
Token ticker	NBM
Decimals	9
Token holders	168
Transactions count	601
Top 100 holders dominance	96.44%
Tax fee	5
Total fees	9112019293894418063730 5
Contract deployer address	0xCABAFa6736aFc9bd9cF68c573eBf9569A55AFdda
Contract's current owner address	0xcabafa6736afc9bd9cf68c573ebf9569a55afdda

NFTBlackMarket Token Distribution

NFTBlackMarket Top 100 Token Holders
Source: BscScan.com

OTHER ACCOUNTS

0x0000000000000000000000000000000000000dead (Burn Address)

0x0757089cbac4b1714fffc53ddaff47e28495961d

0x78c14b3bf0573376fa33c497e70dc22d570f8e17

0xaefc9a06c7be0ffd0cfb25e12b7b05ca1a54b9d6

0xcabafa6736afc9bd9cf68c573ebf9569a55afdda

0xe569262f97e02aa7408633df65bb303626d744fe
(PancakeSwap V2: NBM 3)
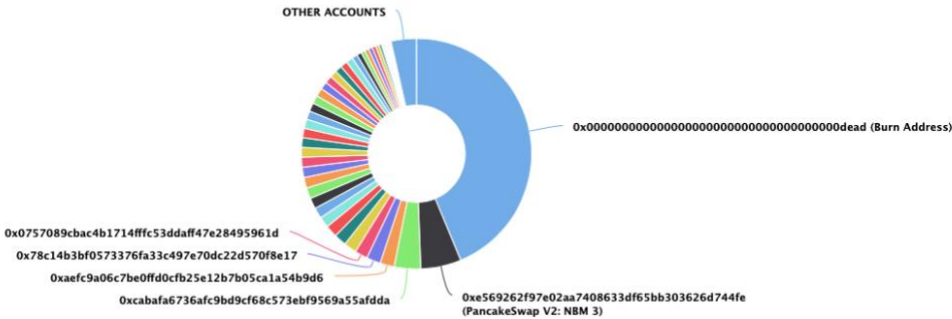
(A total of 964,423,646,474,857.00 tokens held by the top 100 accounts from the total supply of 1,000,000,000,000,000.00 token)

NFTBlackMarket Contract Interaction Details

Time Series: Token Contract Overview   Sat 12, Jun 2021 - Tue 22, Jun 2021

Token Contract 0x12da2f2761038486271c99da7e0fb4413e2b5e38 (NFTBlackMarket)
Source: BscScan.com

Zoom 1m 6m 1y All   From Jun 11, 2021 To Jun 22, 2021

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

NFTBlackMarket Top 10 Token Holders

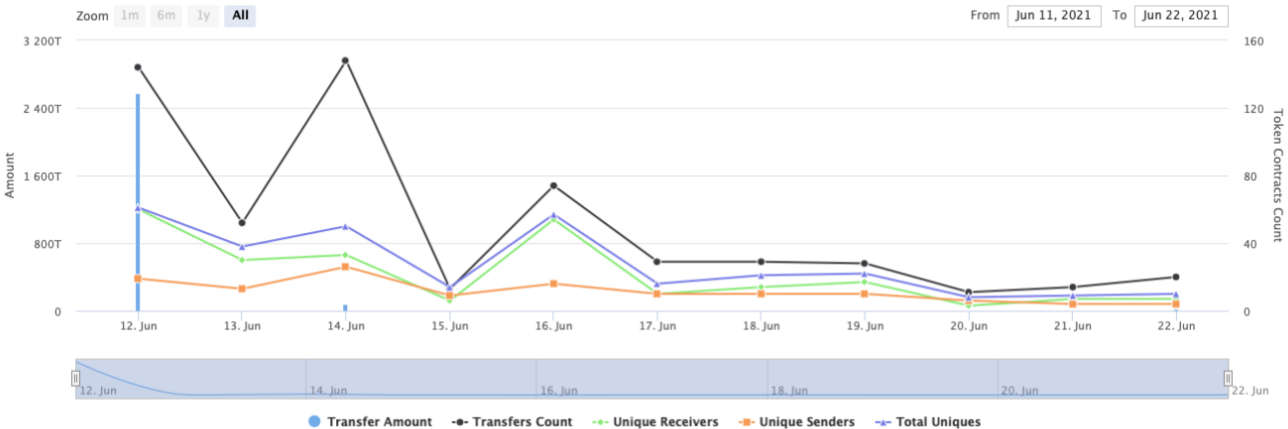| Rank	Address	Quantity (Token)	Percentage
1	Burn Address	437,340,153,452,685.421994884	43.7340%
2	📄 PancakeSwap V2: NBM 3	56,834,711,573,261.164085704	5.6835%
3	0xcabafa6736afc9bd9cf68c573ebf9569a55afdda	37,013,552,445,695.334815176	3.7014%
4	0xaefc9a06c7be0ffd0cfb25e12b7b05ca1a54b9d6	20,021,902,831,531.734466702	2.0022%
5	0x78c14b3bf0573376fa33c497e70dc22d570f8e17	19,770,447,201,738.657947299	1.9770%
6	0x0757089cbac4b1714fffc53ddaff47e28495961d	18,015,892,467,466.928370524	1.8016%
7	0xccc44d512b6538429dd4db813c68ee2325a7314c	17,979,693,091,747.404405761	1.7980%
8	0x13b9f430262ceb956cc164805fd33348fb29d2d0	17,401,098,094,908.277817661	1.7401%
9	0xeec2aff85c0377f247a555ec634de00501065df6	16,775,374,135,364.62034805	1.6775%
10	0x3f2e212b29fcaba88803fca9e6c5c5ffd58d5c87	15,345,107,728,998.360536392	1.5345%

Contract functions details

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

+ [Int] IERC20
 - [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)
 - [Pub] <Constructor> #
 - [Pub] owner
 - [Pub] renounceOwnership #
   - modifiers: onlyOwner
 - [Pub] transferOwnership #
   - modifiers: onlyOwner

+ NFTBLACKMARKET (Context, IERC20, 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]** isExcluded
- **[Pub]** totalFees
- **[Pub]** reflect **#**
- **[Pub]** reflectionFromToken
- **[Pub]** tokenFromReflection
- **[Ext]** excludeAccount **#**
  - modifiers: onlyOwner
- **[Ext]** includeAccount **#**
  - modifiers: onlyOwner
- **[Prv]** _approve **#**
- **[Prv]** _transfer **#**
- **[Prv]** _transferStandard **#**
- **[Prv]** _transferToExcluded **#**
- **[Prv]** _transferFromExcluded **#**
- **[Prv]** _transferBothExcluded **#**
- **[Prv]** _reflectFee **#**
- **[Prv]** _getValues
- **[Prv]** _getTValues
- **[Prv]** _getRValues
- **[Prv]** _getRate
- **[Prv]** _getCurrentSupply

($) = 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 includeAccount() 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 includeAccount(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

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:
https://bscscan.com/tx/0x1515139794eb9cf7dd8bb5ee04234ccfbf4c19b6016805e5be62547e5d7b5840

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.