Techrate1 Techrate

TechRate

AUDIT COMPANY

Smart Contract Security Audit

TechRate

October, 2021

Audit Details

Audited project

BlueSparrow

Deployer address

0x957ce2122f56b329cbbdbf939f2446ae9d09d3bd

Client contacts:

BlueSparrow team

Blockchain

Ethereum

Project website:

https://bluesparrowtoken.com/

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 BlueSparrow to perform an audit of smart contracts:
https://etherscan.io/address/0x4D67EDef87a5fF910954899f4e5a0AaF107afd42#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

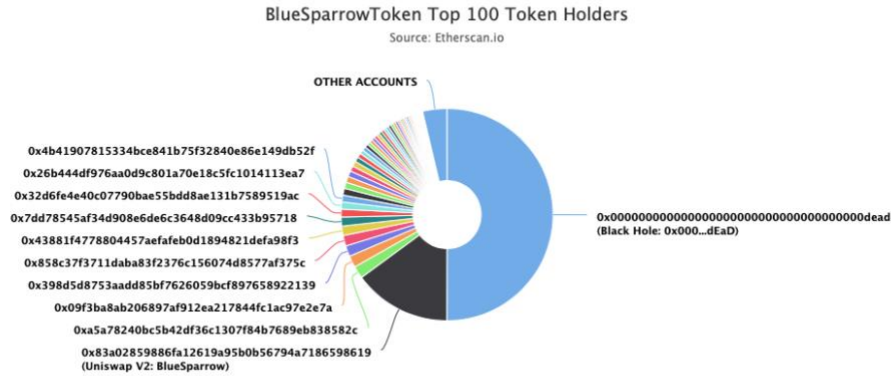
Token contract details for 31.10.2021

Contract name	BlueSparrow
Contract address	0x4D67EDef87a5fF910954899f4e5a0AaF107afd42
Total supply	100,000,000,000,000,000
Token ticker	BlueSparrow
Decimals	9
Token holders	70
Transactions count	194
Top 100 holders dominance	96.30%
Dev wallet	0x1f054a5e9ac34abd49a3c02078dff1eb9ccb83cf
Charity wallet	0xf14b674507390bef4435386a81f7bc4d55386f21
Total fees	3000111825473502078642501
Marketing wallet	0xa6f368fc6f4f3f7bbe224b392c50abc1d585f083
Contract deployer address	0x957ce2122f56b329cbbdbf939f2446ae9d09d3bd
Contract's current owner address	0x957ce2122f56b329cbbdbf939f2446ae9d09d3bd

BlueSparrow Token Distribution

The top 100 holders collectively own 96.30% (96,303,072,038,188,300.00 Tokens) of BlueSparrowToken

Token Total Supply: 100,000,000,000,000,000.00 Token | Total Token Holders: 70

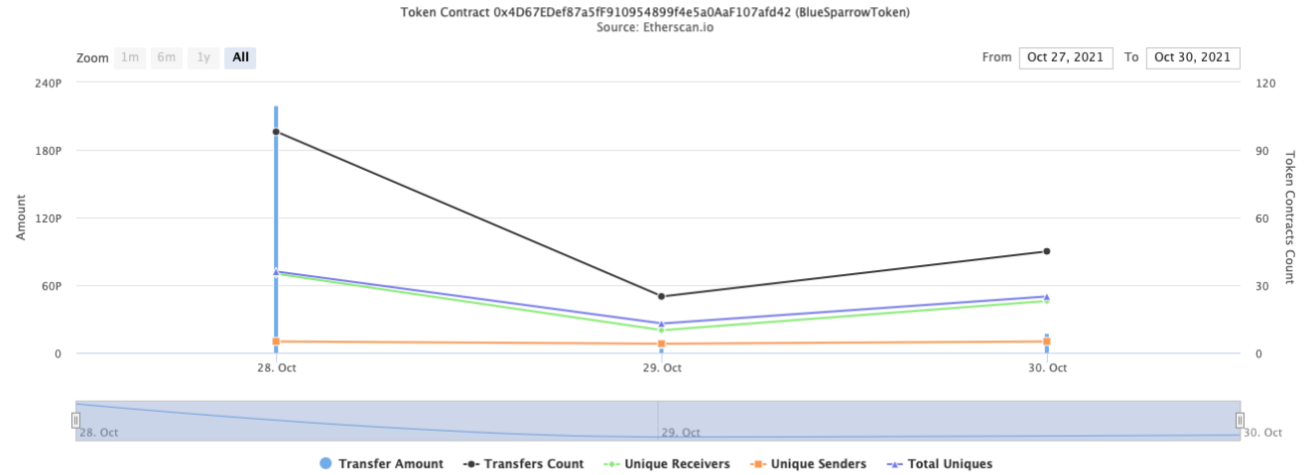


(A total of 96,303,072,038,188,300.00 tokens held by the top 100 accounts from the total supply of 100,000,000,000,000,000.00 token)

BlueSparrow Contract Interaction Details

Time Series: Token Contract Overview

Thu 28, Oct 2021 - Sat 30, Oct 2021



BlueSparrow Top 10 Token Holders

Rank	Address	Quantity (Token)	Percentage
1	Black Hole: 0x000...dEaD	50,040,903,081,164,800.866360475	50.0409%
2	Uniswap V2: BlueSparrow	14,888,697,893,312,500.83396893	14.8887%
3	0xa5a78240bc5b42df36c1307f84b7689eb838582c	1,874,329,653,696,520.042280124	1.8743%
4	0x09f3ba8ab206897af912ea217844fc1ac97e2e7a	1,782,808,081,793,770.281121315	1.7828%
5	0x398d5d8753aadd85bf7626059bcf897658922139	1,642,714,843,946,160.211543159	1.6427%
6	0x858c37f3711daba83f2376c156074d8577af375c	1,615,549,286,757,500.549166716	1.6155%
7	0x43881f4778804457aefafeb0d1894821defa98f3	1,425,427,628,288,490.545963789	1.4254%
8	0x7dd78545af34d908e6de6c3648d09cc433b95718	1,377,899,590,881,360.593122005	1.3779%
9	0x32d6fe4e40c07790bae55bdd8ae131b7589519ac	1,187,796,949,237,310.327331832	1.1878%
10	0x26b444df976aa0d9c801a70e18c5fc1014113ea7	1,092,573,194,698,420.746851057	1.0926%

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

+ [Int] RNG
  - [Ext] getRandomNumber #
  - [Ext] randomResult

+ BlueSparrow (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
- [Ext] setMinCoAmount #
  - modifiers: onlyOwner
- [Ext] setMaxTxPercent #
  - modifiers: onlyOwner
- [Pub] changeAddresses #
  - modifiers: onlyOwner
- [Pub] reflect #
- [Pub] reflectionFromToken
- [Pub] tokenFromReflection
- [Ext] excludeAccount #
  - modifiers: onlyOwner
- [Ext] includeAccount #
  - modifiers: onlyOwner
- [Prv] _approve #
- [Prv] takeTransactionFee #
- [Prv] calculateFee
- [Prv] takeDrawFee #
- [Pub] getRandomNumber #
  - modifiers: onlyOwner
- [Pub] getResult #
  - modifiers: onlyOwner
- [Pub] pickIndexOfWinners #
  - modifiers: onlyOwner
- [Pub] pickWinners #
  - modifiers: onlyOwner
- [Pub] _enterDaWinReward #
  - modifiers: onlyOwner
- [Pub] _enterWeWinReward #
  - modifiers: onlyOwner
- [Prv] _transfer #
- [Prv] ExcludeFEA #
- [Prv] checkState #
- [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 `includeInAccount()` 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.

- 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.

Recommendation:
Check that the excluded array length is not too big.

- The function `ExcludeFEA()` uses the loop to remove addresses from _DrawHolders list. It also could be aborted with `OUT_OF_GAS` exception if there will be a long _DrawHolders addresses list.

Recommendation:
Check that the _DrawHolders array length is not too big.

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

- Owner can change _minCoAmount.

```
function setMinCoAmount(uint256 minCoAmount) external onlyOwner {
    _minCoAmount = minCoAmount.mul(10**9);
}
```

- Owner can change the maximum transaction amount.

```
function setMaxTxPercent(uint256 maxTxPercent) external onlyOwner {
    _maxTxAmount = _tTotal.mul(maxTxPercent).div(10**4);
}
```

- Owner can change fee addresses.

```
function changeAddresses(
    address _marketingWallet,
    address _charityWallet,
    address _mounthlyDrawWallet,
    address _devWallet
) public onlyOwner {
    marketingWallet = _marketingWallet;
    charityWallet = _charityWallet;
    mounthlyDrawWallet = _mounthlyDrawWallet;
    devWallet = _devWallet;
}
```

- Owner can get RNG random number and random result.

```
function getResult() public onlyOwner returns (uint256) {
    return randomResult = _RNG.randomResult();
}
```

```
function getRandomNumber() public onlyOwner {
    _RNG.getRandomNumber();
}
```

- Owner can get winners and charge rewards.

```
ftrace | funcSig
function pickIndexOfWinners() public onlyOwner {
    uint256[] memory indexOfWinners = new uint256[](7);

    for (uint256 i = 0; i < 7; i++) {
        indexOfWinners[i] = (uint256(
            keccak256(abi.encode(randomResult, i))
        ) % _DrawHolders.length);
    }

    _indexOfWinners = indexOfWinners;
}

ftrace | funcSig
function pickWinners() public onlyOwner {
    address[] memory Winners = new address[](7);

    for (uint256 i = 0; i < 7; i++) {
        Winners[i] = _DrawHolders[_indexOfWinners[i]];
    }

    _Winners = Winners;
    delete _indexOfWinners;
}

//Transfer Reward to Daily Winners

ftrace | funcSig
function _enterDaWinReward() public onlyOwner {
    uint256 currentRate = _getRate();

    for (uint256 i = 0; i < 7; i++) {
        _rOwned[_Winners[i]] = _rOwned[_Winners[i]].add(
            _accumulatedDailyReward.div(7).mul(currentRate)
        );
    }

    delete _Winners;
    _accumulatedDailyReward = 0;
}
```

Conclusion

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

Liquidity locking details are provided by the team: https://www.team.finance/view-coin/0x4D67EDef87a5fF910954899f4e5a0AaF107afd42?name=BlueSparrowToken&symbol=BlueSparrow

---

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.