



# 智能合约安全审计

## 审计细节:

|         |   |
|---------|---|
| 审计项目:   | BODA  |
| 部署人员地址: | 0x4acd5d62f01f13a397e5bf5cdf8f4c0a69534ede                        |
| 客户联系人:  | BODA 团队   |
| 区块链:    | 币安网智能链  |
| 项目网站:   | <a href="https://www.bodatoken.org">https://www.bodatoken.org</a> |

# 免责声明

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.

# 背景

BODA委托TechRate对智能合约进行审计:

- <https://bscscan.com/address/0x81cfb5e400eb2caa319130a0dae3b32cfb19392d#code>

审计是为了达到以下目的:

- 确保智能合约功能符合要求.
- 识别智能合约的潜在安全问题.

本报告中的信息应用于了解智能合约的风险敞口, 并作为通过纠正已确定的问题来改善智能合约安全状况的指南。

# 合约细节

令牌合约细节2021.05. 06

|                      |  |
|----------------------|--|
| 合约名称:                | BODA                                       |
| 合约地址:                | 0x81cfb5e400eb2caa319130a0dae3b32cfb19392d |
| 总供给量:                | 1_000_000_000_000_000_000_000_000          |
| 令牌代码:                | BODA                                       |
| 位数:                  | 9  |
| 令牌持有人数:              | 1161                                       |
| 交易笔数:                | 6645                                       |
| 前100名持股人的优势:         | 84.96 %                                    |
| 流动性费用:               | 7  |
| 税费:                  | 3  |
| 总费用:                 | 158_388_874_733_266_276_146_654            |
| PancakeSwap V2 pair: | 0x703d4ba2bcabb38e5d067879c9424045ffb28685 |
| 合约部署人员地址:            | 0x4acd5d62f01f13a397e5bf5cdf8f4c0a69534ede |
| 合约当前所有者地址:           | 0x00 |

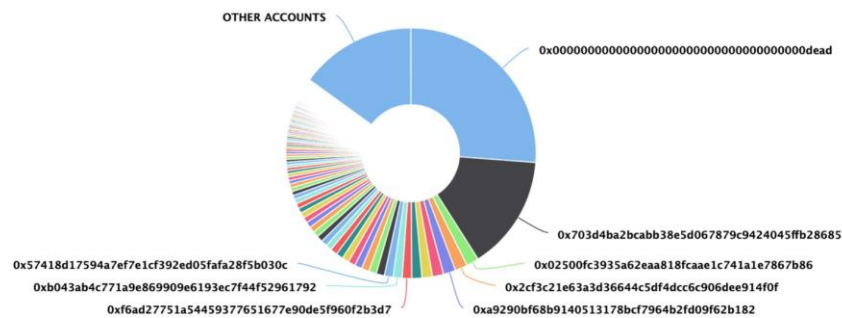
## BODA令牌分布

💡 The top 100 holders collectively own 84.96% (849,644,135,423,820.00 Tokens) of BODA

💡 Token Total Supply: 1,000,000,000,000,000.00 Token | Total Token Holders: 1,161

### BODA Top 100 Token Holders

Source: BscScan.com



(A total of 849,644,135,423,820.00 tokens held by the top 100 accounts from the total supply of 1,000,000,000,000,000.00 token)

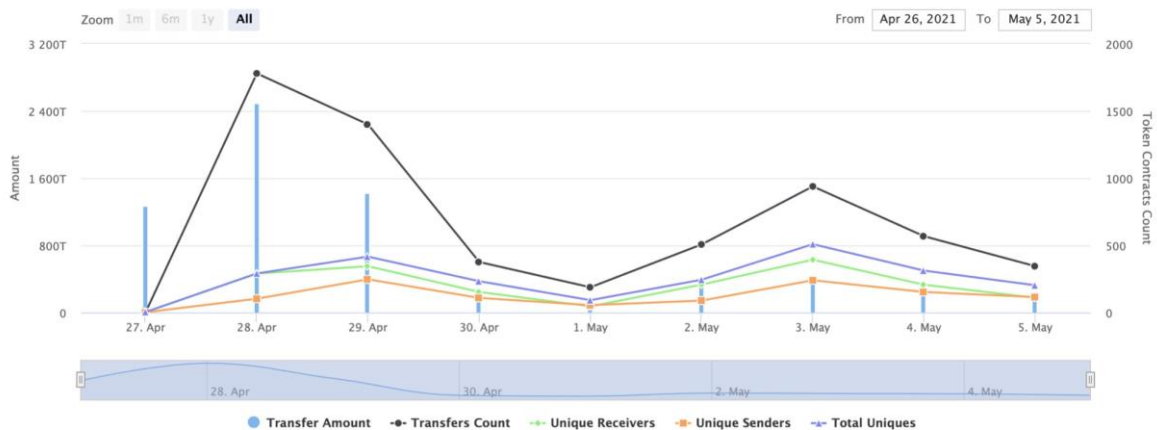
## BODA合约交互细节

### Time Series: Token Contract Overview

Tue 27, Apr 2021 - Wed 5, May 2021

Token Contract 0x81cfb5e400eb2caa319130a0dae3b32cfb19392d (BODA)

Source: BscScan.com



# BODA 十大令牌持有者

| Rank | Address  | Quantity (Token)              | Percentage |
|------|--|-------------------------------|------------|
| 1    | <a href="#">0x0000000000000000000000000000000000dead</a>   | 261,846,632,068,150.734795191 | 26.1847%   |
| 2    | <a href="#">0x703d4ba2bcabb38e5d067879c9424045ffb28685</a> | 148,093,423,272,344.214316344 | 14.8093%   |
| 3    | <a href="#">0x02500fc3935a62eaa818fcaae1c741a1e7867b86</a> | 16,182,538,750,959.627114805  | 1.6183%    |
| 4    | <a href="#">0x2cf3c21e63a3d36644c5df4dcc6c906dee914f0f</a> | 16,003,463,057,035.183010255  | 1.6003%    |
| 5    | <a href="#">0xa9290bf68b9140513178bcf7964b2fd09f62b182</a> | 15,949,136,925,840.478166507  | 1.5949%    |
| 6    | <a href="#">0x8d76fe4578852c3bebd2034564daf3ded4d98406</a> | 14,493,183,093,023.014186082  | 1.4493%    |
| 7    | <a href="#">0xe0d65e3741f1beea47cdf6a5a60cf9ef9fb8411b</a> | 13,508,986,903,972.547580741  | 1.3509%    |
| 8    | <a href="#">0xf4e0e6dee785e8836f09986e1e15b6d9acc14e3d</a> | 13,019,975,334,181.42316904   | 1.3020%    |
| 9    | <a href="#">0xf6ad27751a54459377651677e90de5f960f2b3d7</a> | 12,313,988,838,945.639751371  | 1.2314%    |
| 10   | <a href="#">0xb043ab4c771a9e869909e6193ec7f44f52961792</a> | 11,689,496,228,270.477698551  | 1.1689%    |

# BODA 有限合伙人令牌持有者

| Rank | Address  | Quantity                 | Percentage |
|------|--|--------------------------|------------|
| 1    | <a href="#">0x0000000000000000000000000000000000</a>       | 2,778.151297143223770026 | 83.9943%   |
| 2    | <a href="#">0x0000000000000000000000000000000000dead</a>   | 503.785866355147604036   | 15.2314%   |
| 3    | <a href="#">0x07d80ae6f36a5e08dca74ce884a24d39db9934ed</a> | 24.902359302611641429    | 0.7529%    |
| 4    | <a href="#">0xe9eff515b9e29c393af69d3c5905458de54fde5a</a> | 0.70863107114452575      | 0.0214%    |

# 合约功能细节

```
+ [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

+ 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] IUniswapV2Factory
```

- [Ext] feeTo
- [Ext] feeToSetter
- [Ext] getPair
- [Ext] allPairs
- [Ext] allPairsLength
- [Ext] createPair #
- [Ext] setFeeTo #
- [Ext] setFeeToSetter #

#### + [Int] IUniswapV2Pair

- [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] IUniswapV2Router01

- [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] IUniswapV2Router02 (IUniswapV2Router01)
- [Ext] removeLiquidityETHSupportingFeeOnTransferTokens #
  - [Ext] removeLiquidityETHWithPermitSupportingFeeOnTransferTokens #
  - [Ext] swapExactTokensForTokensSupportingFeeOnTransferTokens #
  - [Ext] swapExactETHForTokensSupportingFeeOnTransferTokens (\$)
  - [Ext] swapExactTokensForETHSupportingFeeOnTransferTokens #
- + BODA (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] 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
- [Ext] setMaxTxPercent#
  - 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] swapAndLiquify #
  - modifiers: lockTheSwap
- [Prv] swapTokensForEth #
- [Prv] addLiquidity #
- [Prv] \_tokenTransfer #
- [Prv] \_transferStandard #
- [Prv] \_transferToExcluded #
- [Prv] \_transferFromExcluded #

(\$ ) = payable function

# = non-constant function

## 问题检查状态

| No | 问题描述。              | 检查状态   |
|----|--------------------|--------|
| 1  | 编译程序错误。            | 通过     |
| 2  | 竞态条件和重入性。依序竞态条件。   | 通过     |
| 3  | 数据传递可能的延迟。         | 通过     |
| 4  | Oracle访问。          | 通过     |
| 5  | 提前交易。              | 通过     |
| 6  | 时间戳依赖。             | 通过     |
| 7  | 整数溢出和下溢出。          | 通过     |
| 8  | DoS与恢复。            | 通过     |
| 9  | 有gas限制的DoS。        | 低严重性问题 |
| 10 | 方法执行权限。            | 通过     |
| 11 | 契约经济模型。            | 通过     |
| 12 | 汇率上逻辑的影响。          | 通过     |
| 13 | 私人用户数据泄露。          | 通过     |
| 14 | 恶意的事件日志。           | 通过     |
| 15 | 范围和声明。             | 通过     |
| 16 | 未初始化的指针存储。         | 通过     |
| 17 | 运算精度。              | 通过     |
| 18 | 设计逻辑。              | 通过     |
| 19 | 依序竞态条件。            | 通过     |
| 20 | 安全开放齐柏林飞船契约的实现和使用。 | 通过     |
| 21 | 回退功能安全。            | 通过     |

# 安全问题

## 高严重程度问题

没有发现高严重程度问题。

## 中等严重程度问题

没有发现中等严重程度问题。

## 低严重程度问题

### 1. Out of gas

问题:

- ❑ includeInReward()函数使用循环从\_excluded列表中查找和删除地址。如果有一个很长的被排除的地址列表，函数将被终止，并出现OUT\_OF\_GAS异常。

```
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;
        }
    }
}
```

- ❑ \_getCurrentSupply函数还使用循环来计算总供给。如果有一个很长的被排除的地址列表，也可以使用OUT\_OF\_GAS异常中止。

```
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);
}
```

建议:使用可数集代替数组或不要使用长数组。

# 结论

智能合约不包含高严重程度问题！流动性配对合同的安全性因超出范围而不会被检查。

**Techrate**备注：

请查阅上述免责声明并注意，本次审计对业务模式、投资吸引力或代码可持续性不作任何声明或保证。该报告仅向报告中提到的合同提供，不包括**Owner**部署的任何其他潜在合同。