



Аудит безопасности смарт-контракта

Информация об аудите:

Название проекта:	BODA
Адрес проекта:	0x4acd5d62f01f13a397e5bf5cdf8f4c0a69534ede
Контактное лицо:	Команда проекта BODA
Блокчейн:	Binance Smart Chain
Сайт проекта:	https://www.bodatoken.org

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.

Общая информация

Команда проекта BODA привлекла компанию TechRate для проведения всестороннего аудита следующих смарт-контрактов:

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

В рамках аудита были поставлены следующие цели:

- Убедиться в том, что смарт-контракт функционирует должным образом.
- Определить потенциальные проблемы безопасности смарт-контракта.

Обратите внимание, что информация, представленная в настоящем отчете, может использоваться для оценки рисков, которые несет в себе смарт-контракт, а также в качестве документа, направленного на повышение уровня безопасности смарт-контракта путем устранения выявленных проблем.

Информация о контракте

Информация о токенах, связанных с контрактом на 06.05.2021 г.

Наименование контракта:	BODA
Адрес контракта:	0x81cfb5e400eb2caa319130a0dae3b32cfb19392d
Общее количество токенов:	1_000_000_000_000_000_000_000_000
Тикер токена:	BODA
Количество десятичных разрядов:	9
Держатели токенов:	1161
Количество транзакций:	6645
Доля 100 крупнейших держателей токена:	84.96 %
Абсорбирование ликвидности:	7
Налоговый сбор:	3
Общая сумма сборов:	158_388_874_733_266_276_146_654
Пара в PancakeSwap V2:	0x703d4ba2bcabb38e5d067879c9424045ffb28685
Адрес развертывания контракта:	0x4acd5d62f01f13a397e5bf5cdf8f4c0a69534ede
Текущий адрес владельца контракта:	0x0000000000000000000000000000000000000000

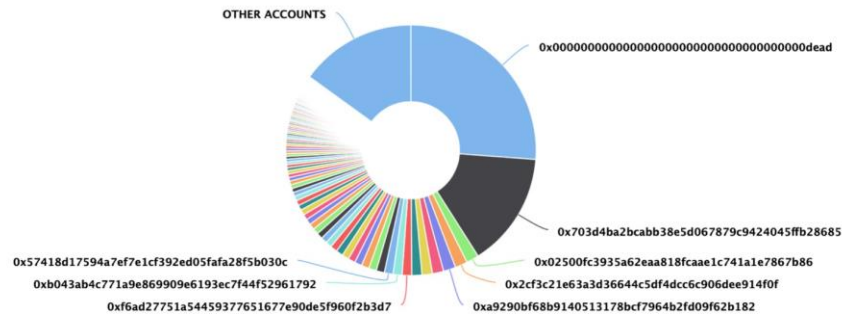
Распределение токенов BODA

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

💡 Token Total Supply: 1,000,000,000,000.00 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)

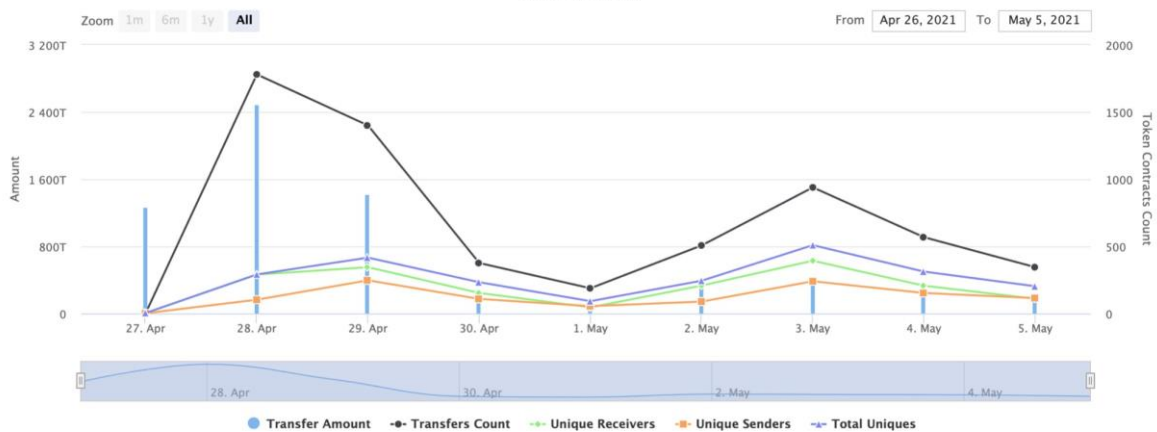
Информация об активности по контракту BODA

Time Series: Token Contract Overview


Tue 27, Apr 2021 - Wed 5, May 2021

Token Contract 0x81cfb5e400eb2caa319130a0dae3b32cfb19392d (BODA)

Source: BscScan.com



Топ-10 держателей токенов BODA

Rank	Address	Quantity (Token)	Percentage
1	0x00000000000000000000000000000000dead	261,846,632,068,150.734795191	26.1847%
2	 0x703d4ba2bcabb38e5d067879c9424045ffb28685	148,093,423,272,344.214316344	14.8093%
3	0x02500fc3935a62eaa818fcaae1c741a1e7867b86	16,182,538,750,959.627114805	1.6183%
4	0x2cf3c21e63a3d36644c5df4dcc6c906dee914f0f	16,003,463,057,035.183010255	1.6003%
5	0xa9290bf68b9140513178bcf7964b2fd09f62b182	15,949,136,925,840.478166507	1.5949%
6	0x8d76fe4578852c3bebd2034564daf3ded4d98406	14,493,183,093,023.014186082	1.4493%
7	0xe0d65e3741f1beea47cdf6a5a60cf9ef9fb8411b	13,508,986,903,972.547580741	1.3509%
8	0xf4e0e6dee785e8836f09986e1e15b6d9acc14e3d	13,019,975,334,181.42316904	1.3020%
9	0xf6ad27751a54459377651677e90de5f960f2b3d7	12,313,988,838,945.639751371	1.2314%
10	0xb043ab4c771a9e869909e6193ec7f44f52961792	11,689,496,228,270.477698551	1.1689%

Держатели токенов BODA LP

Rank	Address	Quantity	Percentage
1	 0x0000000000000000000000000000000000000000	2,778.151297143223770026	83.9943%
2	0x00000000000000000000000000000000dead	503.785866355147604036	15.2314%
3	0x07d80ae6f36a5e08dca74ce884a24d39db9934ed	24.902359302611641429	0.7529%
4	0xe9eff515b9e29c393af69d3c5905458de54fde5a	0.70863107114452575	0.0214%

Информация о функциях контракта

- + [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 #
 - [Priv] _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

Результат проверки наличия текущих проблем и уязвимостей

№	Описание проблемы	Результат проверки
1	Ошибки в работе компилятора	Не обнаружено
2	Состязательная ситуация и реентерабельность, а также в кросс-режиме	Не обнаружено
3	Возможные задержки в доставке данных	Не обнаружено
4	Работа с запросами Oracle	Не обнаружено
5	Опережающая сделка	Не обнаружено
6	Зависимость от временных отметок	Не обнаружено
7	Переполнение целочисленного значения и отрицательное переполнение	Не обнаружено
8	Обратная DoS-атака	Не обнаружено
9	DoS-атака через ограничение объема газа в блоке.	Незначительные проблемы
10	Разрешения на выполнение методов	Не обнаружено
11	Экономическая модель контракта	Не обнаружено
12	Влияние обменного курса на логику	Не обнаружено
13	Утечки личных пользовательских данных	Не обнаружено
14	Журнал вредоносных и опасных событий	Не обнаружено
15	Определение контекста и описание	Не обнаружено
16	Неинициализированные указатели места хранения	Не обнаружено
17	Арифметическая точность	Не обнаружено
18	Логика построения и структуры	Не обнаружено
19	Состязательная ситуация в кросс-режиме	Не обнаружено
20	Безопасная реализация и использование контрактов OpenZeppelin.	Не обнаружено
21	Безопасность резервной функции	Не обнаружено

Вопросы безопасности

Проблемы особой важности

Проблем особой важности не обнаружено.

Проблемы средней важности

Проблем средней важности не обнаружено.

Проблемы малой важности

1. Нехватка газа

Обнаруженная проблема:

- ❑ Функция `includeInReward()` использует цикл для поиска и удаления адресов из списка `_excluded`. Функция прекращает работу с ошибкой `OUT_OF_GAS` при использовании длинного списка исключенных адресов.

```
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;
        }
    }
}
```

- ❑ Функция `_getCurrentSupply` также использует цикл для оценки общего количества токенов. Функция также прекращает работу с ошибкой `OUT_OF_GAS` при использовании длинного списка исключенных адресов.

```
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);
}
```

Рекомендация: необходимо использовать `EnumerableSet` вместо текущего массива или отказаться от длинных массивов.

Общий вывод

Исследованные смарт-контракты не содержат проблем высокой важности, которые могли бы вызвать опасения! Безопасность контракта пары, выбранной для создания ликвидности, не проверяется, так как не входит в задачи аудита.

Комментарий Techrate:

Мы убедительно просим вас ознакомиться с отказом от ответственности и обратить особое внимание на то, что результаты аудита не могут служить гарантией или основой для принятия решения об устойчивости бизнес-модели, инвестиционной привлекательности или надежности кода. Данный отчет содержит результаты аудита единственного контракта, упомянутого в отчете, и не включает других контрактов, которые могли или могут быть созданы владельцем текущего контракта.