



## स्मार्ट अनुबंध सिक्यूरिटी ऑडिट

ऑडिट विवरण:

ऑडिट की गई परियोजना : BODA

नियोक्ता का पता : 0x4acd5d62f01f13a397e5bf5cdf8f4c0a69534ede

ग्राहक संपर्क : BODA टीम

ब्लॉकचैन: बिनांस स्मार्ट चैन

परियोजना वेबसाइट : <https://www.bodatoken.org>

मई, 2021

टेकरेट

# 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.

# पृष्ठभूमि

टेकरेट को स्मार्ट अनुबंधों का ऑडिट करने के लिए बोडा द्वारा कमीशन किया गया था:

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

इस रिपोर्ट में दी गई जानकारी का उपयोग स्मार्ट अनुबंध के जोखिम को समझने के लिए किया जाना चाहिए, और पहचान की गई समस्याओं को दूर करके स्मार्ट अनुबंध की सुरक्षा स्थिति में सुधार करने के लिए एक गाइड के रूप में उपयोग किया जाना चाहिए।

ऑडिट का उद्देश्य निम्नलिखित प्राप्त करना था:

- सुनिश्चित करें कि स्मार्ट अनुबंध उद्देश्य के अनुसार कार्य करता है।
- स्मार्ट अनुबंध के साथ संभावित सुरक्षा मुद्दों की पहचान करें।

## संपर्क विवरण

06.05.2021 के लिए टोकन अनुबंध विवरण

अनुबंध नाम:	बोडा
अनुबंध पता:	0x81cfb5e400eb2caa319130a0dae3b32cfb19392d
कुल आपूर्ति:	1_000_000_000_000_000_000_000_000
टोकन टिकर:	BODA
दशमलव:	9
टोकन होल्डर्स:	1161
ट्रांसजेक्शन गणना:	6645
शीर्ष 100 होल्डर्स का हिस्सा:	84.96 %
लिक्विडिटी शुल्क:	7
टैक्स शुल्क:	3
कुल शुल्क:	158_388_874_733_266_276_146_654
पेनकेकस्वैप वी2 जोड़ी:	0x703d4ba2bcabb38e5d067879c9424045ffb28685
अनुबंध नियोक्ता का पता:	0x4acd5d62f01f13a397e5bf5cdf8f4c0a69534ede
अनुबंध के वर्तमान मालिक का पता:	0x00

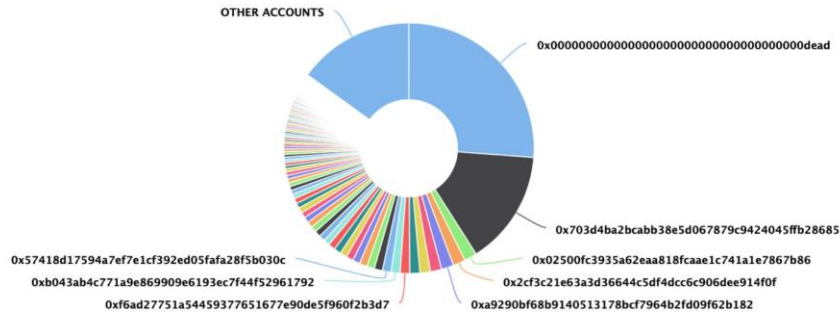
## बोडा टोकन वितरण

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

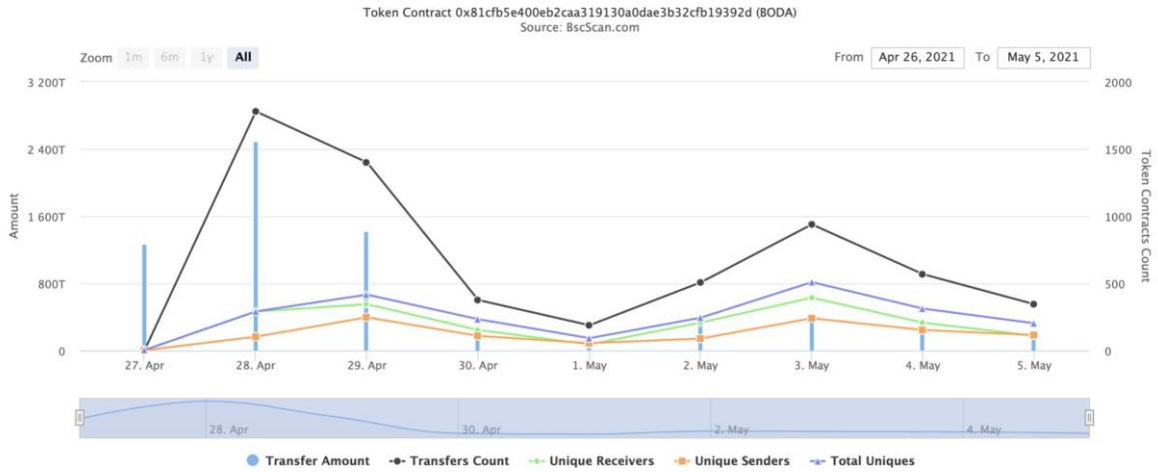


(A total of 849,644,135,423,820.00 tokens held by the top 100 accounts from the total supply of 1,000,000,000,000.00 token)


## बोडा अनुबंध इंटरैक्शन विवरण

Time Series: Token Contract Overview

Tue 27, Apr 2021 - Wed 5, May 2021



## बोडा शीर्ष 10 टोकन धारक

Rank	Address	Quantity (Token)	Percentage
1	0x000000000000000000000000000000dead	261,846,632,068,150.734795191	26.1847%
2	 0x703d4ba2bcabb38e5d067879c9424045ffb28685	148,093,423,272,344.214316344	14.8093%
3	0x02500fc3935a62eaa818fcae1c741a1e7867b86	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	0x8d76fe4578852c3bebd2034564daf3ded498406	14,493,183,093,023.014186082	1.4493%
7	0xe0d65e3741f1beea7cdf6a5a60cf9ef9fb8411b	13,508,986,903,972.547580741	1.3509%
8	0xf4e0e6dee785e8836f09986e1e15b6d9acc14e3d	13,019,975,334,181.42316904	1.3020%
9	0xf6ad27751a5445937651677e90de5f960f2b3d7	12,313,988,838,945.639751371	1.2314%
10	0xb043ab4c771a9e869909e6193ec7f44f52961792	11,689,496,228,270.477698551	1.1689%

## बोडा एलपी टोकन धारक

Rank	Address	Quantity	Percentage
1	 0x00	2,778.151297143223770026	83.9943%
2	0x00dead	503.785866355147604036	15.2314%
3	0x07d80ae6f36a5e08dca74ce884a24d39db9934ed	24.902359302611641429	0.7529%
4	0xe9eff515b9e29c393af69d3c5905458de54fde5a	0.70863107114452575	0.0214%

## अनुबंध कार्यों का विवरण

- + [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

## विभिन्न मुद्दों की जांच की स्थितियां

संख्या	मुद्दे का विवरण.	जाँच की स्थिति
1	कम्पाइलर (संकलक) त्रुटि.	उत्तीर्ण
2	रेस की स्थिति और पुनर्विक्रय। क्रॉस-फ़ंक्शन रेस की स्थिति।	उत्तीर्ण
3	डेटा वितरण में संभावित देरी।	उत्तीर्ण
4	ओरेकल कॉल्स	उत्तीर्ण
5	फ्रंट रनिंग	उत्तीर्ण
6	टाइमस्टैम्प निर्भरता	उत्तीर्ण
7	इंटीजर ओवरफ्लो और अंडरफ्लो।	उत्तीर्ण
8	रिवर्ट के साथ DoS	उत्तीर्ण
9	ब्लाक गैस सीमा के साथ DoS	कम मुद्दे
10	निष्पादन अनुमतियाँ के तरीके	उत्तीर्ण
11	अनुबंध का आर्थिक मॉडल	उत्तीर्ण
12	लॉजिक पर विनिमय दर का प्रभाव।	उत्तीर्ण
13	निजी उपयोगकर्ता डेटा लीक	उत्तीर्ण
14	मेलेसियस इवेंट (दुर्भावनापूर्ण घटना) लॉग	उत्तीर्ण
15	दायरा और घोषणाएं	उत्तीर्ण
16	शुरू न हुए भंडारण संकेत	उत्तीर्ण
17	अंकगणित सटीकता	उत्तीर्ण
18	डिजाइन लॉजिक	उत्तीर्ण
19	क्रॉस-फ़ंक्शन रेस की स्थिति।	उत्तीर्ण
20	सेफ ओपन ज़ेपेलिन अनुबंध कार्यान्वयन और उपयोग	उत्तीर्ण
21	फॉलबैक फ़ंक्शन सुरक्षा	उत्तीर्ण

# सुरक्षा समस्याएं

## उच्च गंभीरता के मुद्दे

कोई उच्च गंभीरता के मुद्दे नहीं

## मध्यम गंभीरता के मुद्दे

कोई मध्यम गंभीरता के मुद्दे नहीं

## निम्न गंभीरता के मुद्दे

### 1. गैस खत्म

मुद्दा:

- ❑ फंक्शन `includeInReward()` `_excluded` सूची से पते खोजने और निकालने के लिए लूप का उपयोग करता है। यदि लंबी बहिष्कृत पतों की सूची होगी तो `OUT_OF_GAS` अपवाद के साथ फंक्शन निरस्त कर दिया जाएगा।

```
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;
        }
    }
}
```

- ❑ फंक्शन `_getCurrentSupply` भी कुल आपूर्ति का मूल्यांकन करने के लिए लूप का उपयोग करता है। यदि लंबी बहिष्कृत पतों की सूची होगी तो इसे भी `OUT_OF_GAS` अपवाद के साथ निरस्त किया जा सकता है।

```
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);
}
```

अनुशंसा: सरणी (array) के बजाय `EnumerableSet` का उपयोग करें या लंबी सरणी का उपयोग न करें।

स्मार्ट अनुबंधों में उच्च गंभीरता के मुद्दे नहीं होते हैं! दायरे से बाहर होने के कारण लिक्विडिटी जोड़ी अनुबंध की सुरक्षा की जाँच नहीं की जाती है।

टेकरेट नोट:

कृपया ऊपर दिए गए अस्वीकरण की जांच करें और ध्यान दें, ऑडिट व्यवसाय मॉडल, निवेश आकर्षण या कोड स्थिरता पर कोई बयान या वारंटी नहीं देता है। रिपोर्ट में उल्लिखित एकमात्र अनुबंध के लिए रिपोर्ट प्रदान की गई है और इसमें इसके मालिक द्वारा तैनात कोई अन्य संभावित अनुबंध शामिल नहीं है।