



Smart na Kontrata sa Seguridad Audit

Mga Detalye ng Audit:

Na-audit na proyekto: BODA

Address ng deployer: 0x4acd5d62f01f13a397e5bf5cdf8f4c0a69534ede

Mga kontak ng kliyente: BODA team

Blockchain: Binance Smart Chain

Website ng proyekto: <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.

Background

Ang TechRate ay kinomisyon ng BODA upang magsagawa ng pag-audit sa mga smart na kontrata:

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

Ang layunin ng pag-audit ay upang makamit ang mga sumusunod:

- Tiyaking gumagana ang matalinong kontrata tulad ng nilalayan.
- Kilalanin ang mga potensyal na seguridad sa isyu gamit ang matalinong kontrata.

Ang impormasyon sa ulat na ito ay dapat gamitin upang maunawaan ang peligro na pagkakalantad sa smart na kontrata, at bilang isang gabay upang mapabuti ang seguridad na pustura ng smart na kontrata sa pamamagitan ng pag-aayos ng mga isyu na nakilala.

Mga detalye ng kontrata

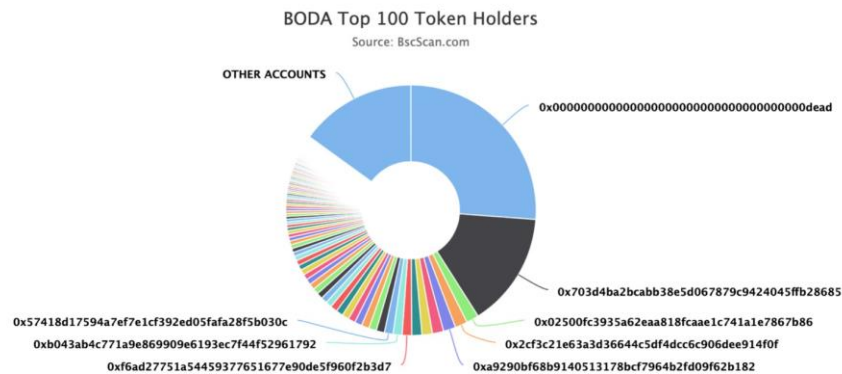
Mga detalye ng kontrata ng token para sa 06.05.2021

Pangalan ng kontrata:	BODA
Address ng kontrata:	0x81cfb5e400eb2caa319130a0dae3b32cfb19392d
Kabuuang supply:	1_000_000_000_000_000_000_000_000
Token ticker:	BODA
Mga Desimal:	9
Mga may hawak ng token:	1161
Bilang ng mga transaksyon	6645
Nangungunang 100 ng nangingibabaw na may-ari:	84.96 %
Bayad sa pagkatubig:	7
Bayad sa buwis:	3
Kabuuang bayarin:	158_388_874_733_266_276_146_654
Pares ng PancakeSwap V2:	0x703d4ba2bcabb38e5d067879c9424045ffb28685
Address ng pag-deploy ng kontrata:	0x4acd5d62f01f13a397e5bf5cdf8f4c0a69534ede
Ang kasalukuyang address ng may-ari ng kontrata:	0x00

Pamamahagi ng token ng 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

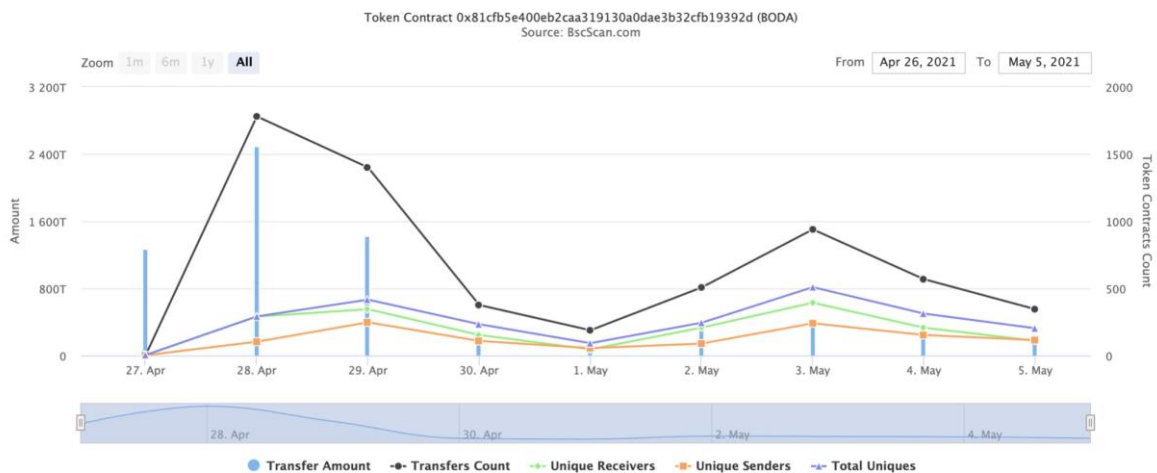


(A total of 849,644,135,423,820.00 tokens held by the top 100 accounts from the total supply of 1,000,000,000,000,000.00 token)


Mga detalye ng pakikipag-ugnay ng BODA

Time Series: Token Contract Overview

Tue 27, Apr 2021 - Wed 5, May 2021



Nangungunang 10 ng mga may hawak ng token ng BODA

Rank	Address	Quantity (Token)	Percentage
1	0x000000000000000000000000000000000000dead	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%

Mga may hawak ng token ng BODA LP

Rank	Address	Quantity	Percentage
1	 0x000000000000000000000000000000000000	2,778.151297143223770026	83.9943%
2	0x000000000000000000000000000000000000dead	503.785866355147604036	15.2314%
3	0x07d80ae6f36a5e08dca74ce884a24d39db9934ed	24.902359302611641429	0.7529%
4	0xe9eff515b9e29c393af69d3c5905458de54fde5a	0.70863107114452575	0.0214%

Mga detalye ng pag-andar ng kontrata

```
+ [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

Mga Katayuan sa Pagsusuri ng Mga Isyu

No	Paglalarawan ng isyu.	Katayuan ng Sinusuri
1	Mga kamalian sa tagatala.	Pasado
2	Mga kondisyon sa lahi at Reentrancy. Mga kondisyon sa lahi ng cross-function.	Pasado
3	Posibleng pagkaantala sa paghahatid ng data.	Pasado
4	Tawag ng Orakulo.	Pasado
5	Front running.	Pasado
6	Timestamp dependence.	Pasado
7	Integer Overflow at Underflow.	Pasado
8	DoS with Revert.	Pasado
9	Ang DoS na may limitasyon sa block gas.	Mababang isyu
10	Mga pahintulot sa pagpapatupad ng mga pamamaraan.	Pasado
11	Modelong pang-ekonomiya ng kontrata.	Pasado
12	Ang epekto sa palitan ng rate sa lohika.	Pasado
13	Mga paglabas ng data ng pribadong gumagamit.	Pasado
14	Nakakahamak na log ng Kaganapan.	Pasado
15	Saklaw at Deklarasyon.	Pasado
16	Hindi naintindihang mga pahiwatig ng imbakan.	Pasado
17	Katumpakan ng Arithmetic.	Pasado
18	Disenyo ng Lohika.	Pasado
19	Mga kondisyon sa lahi ng cross-function.	Pasado
20	Nakakontra ang Safe Open Zeppelin ng pagpapatupad at paggamit.	Pasado
21	Pag-andar ng seguridad ng fallback.	Pasado

Mga Isyu sa Seguridad

Mataas na Isyu sa Kalubhaan

Walang natagpuang mga isyu sa mataas na kalubhaan.

Mga Isyu sa Katamtamang Kalubhaan

Walang nahanap na mga isyu sa katamtamang kalubhaan.

Mababang Mga Isyu sa Kalubhaan

Naubos na gas

Isyu:

- ❑ Ang pagpapaandar ng `includeInReward()` ay gumagamit ng loop upang hanapin at alisin ang mga address mula sa `_excluded` na listahan. Tatanggalin ang pagpapaandar sa `OUT_OF_GAS`

```
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;
        }
    }
}
```

pagbubukod kung magkakaroon ng isang mahabang listahan ng mga address ng mga hindi kasama.

- ❑ Ang pagpapaandar ng `_getCurrentSupply` ay gumagamit din ng loop para sa pagsusuri ng kabuuang supply. Maaari rin itong ma-abort `OUT_OF_GAS` pagbubukod kung magkakaroon ng isang

```
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);
}
```

mahabang listahan ng mga address na hindi kasama.

Recommendation: Use EnumerableSet instead of array or do not use long arrays.

Konklusyon

Walang mataas na mga isyu sa kalubhaan sa mga smart na kontrata!
Ang seguridad ng mga pares ng liquidity ay hindi nasuri dahil wala sila sa saklaw.

Tala ng Techrate:

Mangyaring suriin ang pagtanggì sa itaas at tandaan, ang pag-audit ay walang mga pahayag o garantiya sa modelo ng negosyo, pagiging kaakit-akit ng pamumuhunan o pagpapanatili ng code. Ang ulat ay ibinibigay para sa nag-iisang kontrata na nabanggit sa ulat at hindi kasama ang anumang iba pang mga potensyal na kontrata na ipinakalat ng May-ari.