스마트 계약 보안 감사

감사 세부사항:

감사 프로젝트:	BODA
배치 책임자 어드레스:	0x4acd5d62f01f13a397e5bf5cdf8f4c0a69534ede
의뢰인 연락:	BODA team
블록체인:	Binance Smart Chain
프로젝트 웹사이트:	https://www.bodatoken.org

2021년 5월

TechRate

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.

배경

Tech Rate는 BODA로부터 스마트 계약서에 대한 감사를 행하도록 위임 받았다.

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

이 감사는 아래와 같은 사항을 위한 목적으로 시행된다:

- 스마트 계약이 의도한 대로 잘 이행되는지 확인.
- 스마트 계약과 관련한 잠재적인 보안 사안들 확인.

이 보고서에 작성된 정보는 스마트 계약의 위험성 인지에 대한 용도와 발견한 문제들을 교정하여 스마트 계약의 안정성을 향상시키기 위한 가이드의 역할로만 사용 되어야 한다.

계약 세부사항

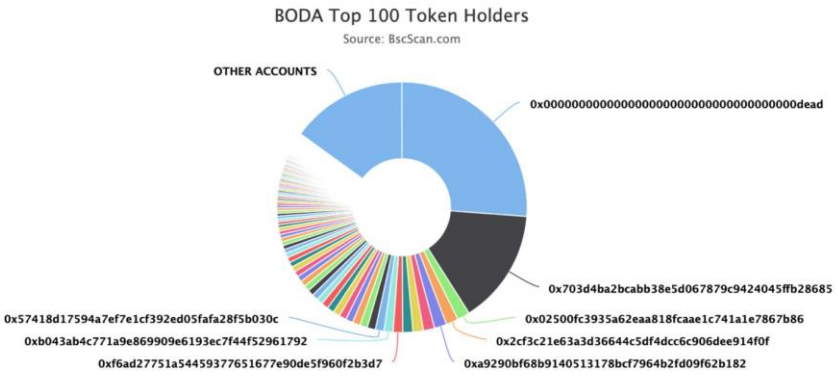
2021.06.05 일자 토큰 계약 세부사항

계약자 성함:	BODA
계약 어드레스:	0x81cfb5e400eb2caa319130a0dae3b32cfb19392d
총 공급:	1_000_000_000_000_000_000_000_000
토큰 티커:	BODA
소수점 허용 범위:	9
토큰 소유자:	1161
거래 수:	6645
상위 100명의 토큰 보유율:	84.96 %
유동성 수수료:	7
세금 :	3
총 수수료:	158_388_874_733_266_276_146_654
PancakeSwap V2 페어:	0x703d4ba2bcabb38e5d067879c9424045ffb28685
계약 배치책임자 어드레스:	0x4acd5d62f01f13a397e5bf5cdf8f4c0a69534ede
계약 현 소유주 어드레스:	0x0000000000000000000000000000000000000000

BODA 토큰 분포

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

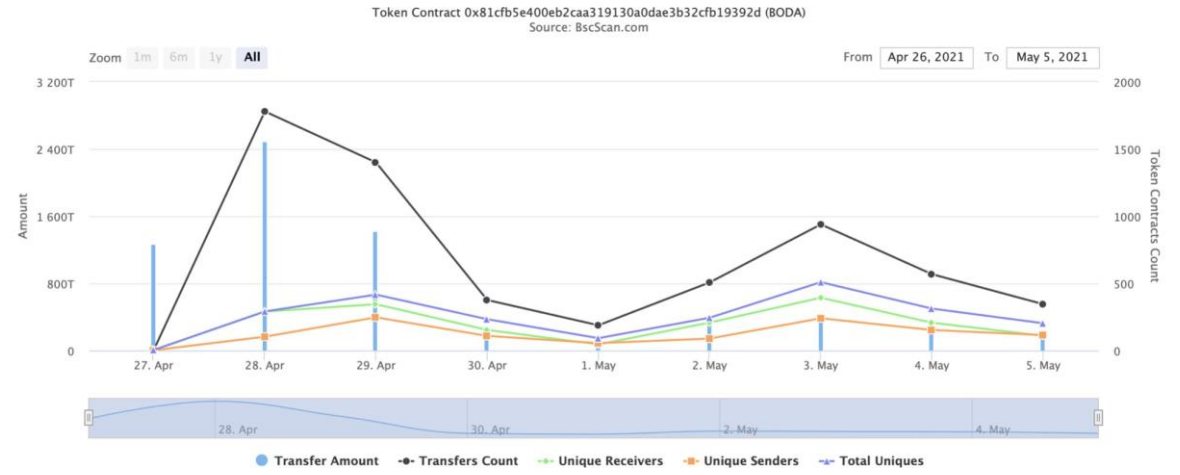


(A total of 849,644,135,423,820.00 tokens held by the top 100 accounts from the total supply of 1,000,000,000,000,000.00 token)

BODA 계약 상호작용 세부사항

Time Series: Token Contract Overview

Tue 27, Apr 2021 - Wed 5, May 2021



BODA 소유자 중 상위 10명

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%

BODA LP 토큰 소유자

Rank	Address	Quantity	Percentage
1	0x0000000000000000000000000000000000000000	2,778.151297143223770026	83.9943%
2	0x000000000000000000000000000000000000dead	503.785866355147604036	15.2314%
3	0x07d80ae6f36a5e08dca74ce884a24d39db9934ed	24.902359302611641429	0.7529%
4	0xe9eff515b9e29c393af69d3c5905458de54fde5a	0.70863107114452575	0.0214%

계약 기능 세부사항

+ [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

사안 확인 현황

№	사안 기술	현황 확인
1	컴파일러 오류.	통과
2	경합 조건과 재진입성. 교차 기능 경합 조건.	통과
3	데이터 전달에 있어 가능한 지연	통과
4	오라클 콜.	통과
5	선행매매.	통과
6	타임스탬프 종속성.	통과
7	정수 오버플로 및 언더플로.	통과
8	복귀 서비스 거부.	통과
9	블록 가스 리밋 서비스 거부.	낮은 심각성의 사안
10	매서드(methods) 실행 권한.	통과
11	계약의 경제모델.	통과
12	논리적 환율의 영향.	통과
13	개인 데이터 유출.	통과
14	악의적 이벤트 로그.	통과
15	범위와 선언.	통과
16	초기화되지 않은 스토리지 포인터.	통과
17	연산 정확도.	통과
18	설계 로직.	통과
19	교차 기능 경합 조건.	통과
20	Safe Open Zeppelin 계약구현 및 사용.	통과
21	대비책 기능 안정성.	통과

안전성 사안

매우 심각한 사안

매우 심각한 사안은 발견되지 않음.

심각한 사안

심각한 사안은 발견되지 않음.

낮은 심각성의 사안

1. 가스 부족(Out of gas)

문제:

- 기능 `includeInReward()`은 `_excluded` 리스트의 어드레스들을 찾고 제거하는 고리를 사용한다. 긴 제외된 어드레스 리스트가 있다면, 이 기능은 `OUT_OF_GAS` 예외로 중단 될 것이다.

```
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;
        }
    }
}
```

- 기능`_getCurrentSupply` 또한 총 보급을 평가하는 고리로 사용된다. 마찬가지로, 긴 제외된 어드레스 리스트가 있다면, 이 기능은 `OUT_OF_GAS` 예외로 중단 될 것이다.

```
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);
}
```

추천사항: 배열을 사용하는 대신 EnumerableSet을 사용하거나 긴 배열을 사용하지 마세요.

결론

스마트 계약은 매우 심각한 사안을 가지고 있지 않습니다! 유동성 페어 계약의 안전성은 영역에서 벗어나는 사안이라 확인하지 않았습니다.

Techrate 참고:

위에 적힌 권리포기각서를 꼭 확인해 주십시오. 그리고 이 감사는 어떤 성명이나 비즈니스 모델, 투자 매력도, 또는 코드 유지가능성에 대한 어떤 증명도 하지 않습니다. 이 보고서는 오직 보고서 속 언급된 계약에만 규정되어 있습니다. 또한, Owner에 의해 배치될 어떤 다른 잠재적인 계약도 포함되어 있지 않습니다.

.