Auditoría de seguridad de contratos inteligentes

Detalles de la auditoría:

Proyecto auditado:	BODA
Dirección del desplegador:	0x4acd5d62f01f13a397e5bf5cdf8f4c0a69534ede
Contactos del cliente:	BODA team
Blockchain:	Binance Smart Chain
Sitio web del proyecto:	https://www.bodatoken.org

Mayo, 2021
TechRate

Aviso legal
(DO NOT NEED TO TRANSLATE)

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.

Antecedentes

TechRate recibió el encargo de BODA de realizar una auditoría de los contratos inteligentes:

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

El objetivo de la auditoría era conseguir lo siguiente:

- Garantizar que el contrato inteligente funcione según lo previsto.
- Identificar los posibles problemas de seguridad del contrato inteligente.

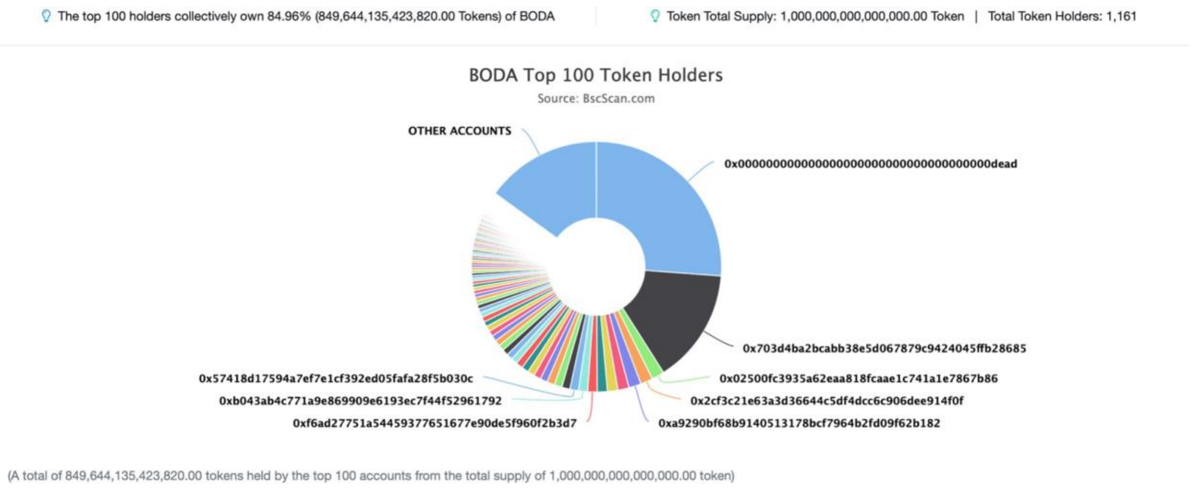
La información de este informe debe utilizarse para comprender la exposición al riesgo del contrato inteligente, y como guía para mejorar la postura de seguridad del contrato inteligente mediante la corrección de los problemas identificados.

Detalles del contrato

Detalles del contrato de token para 06.05.2021.

Nombre del contrato:	BODA
Dirección del contrato:	0x81cfb5e400eb2caa319130a0dae3b32cfb19392d
Suministro total:	1_000_000_000_000_000_000_000_000
Marca de token:	BODA
Decimales:	9
Titulares de tokens:	1161
Recuento de transacciones:	6645
Dominio de los 100 primeros titulares:	84.96 %
Tasa de liquidez:	7
Tasa fiscal:	3
Total de tasas:	158_388_874_733_266_276_146_654
Par de PancakeSwap V2:	0x703d4ba2bcabb38e5d067879c9424045ffb28685
Dirección del desplegador del contrato:	0x4acd5d62f01f13a397e5bf5cdf8f4c0a69534ede
Dirección del propietario actual del contrato:	0x0000000000000000000000000000000000000000

Distribución de tokens BODA
(IMAGES DO NOT NEED TO BE TRANSLATED)



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

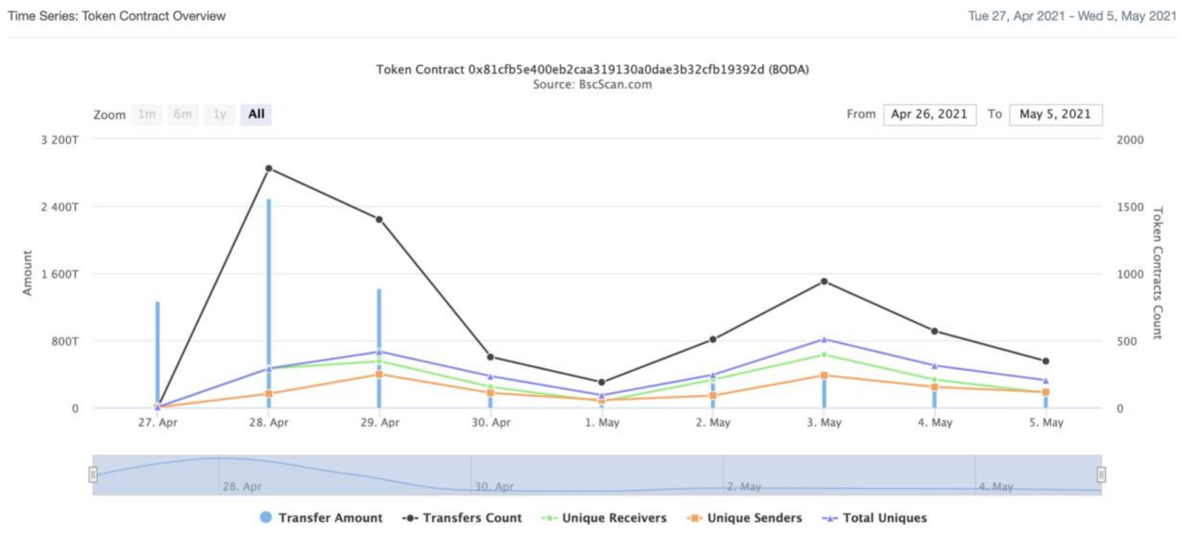
BODA Top 100 Token Holders

Source: BscScan.com

OTHER ACCOUNTS
0x000000000000000000000000000000000000dead
0x703d4ba2bcabb38e5d067879c9424045ffb28685
0x57418d17594a7ef7e1cf392ed05fafa28f5b030c
0x02500fc3935a62eaa818fcaae1c741a1e7867b86
0xb043ab4c771a9e869909e6193ec7f44f52961792
0x2cf3c21e63a3d36644c5df4dcc6c906dee914f0f
0xf6ad27751a54459377651677e90de5f960f2b3d7
0xa9290bf68b9140513178bcf7964b2fd09f62b182

(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)

Detalles de la interacción del contrato BODA



Time Series: Token Contract Overview

Tue 27, Apr 2021 - Wed 5, May 2021

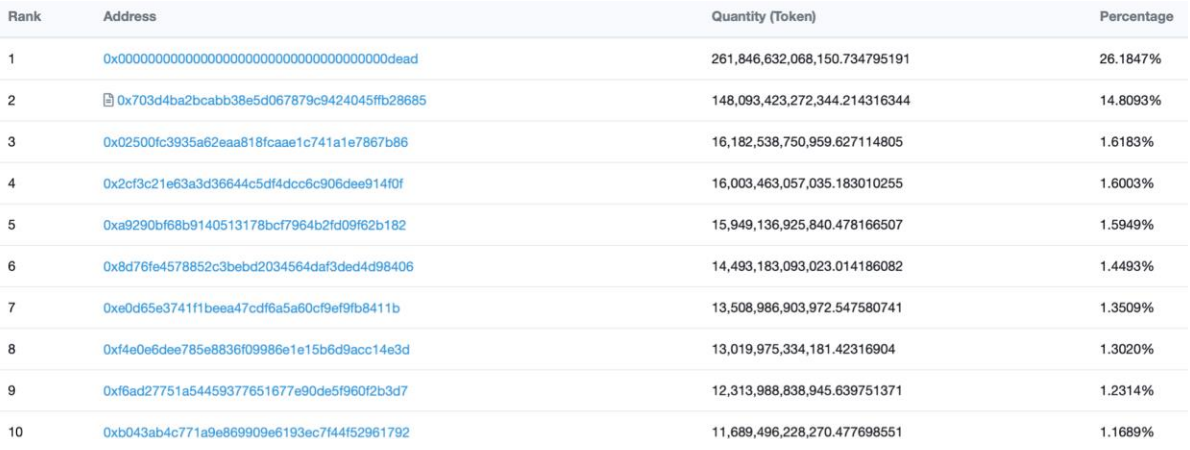
Token Contract 0x81cfb5e400eb2caa319130a0dae3b32cfb19392d (BODA)

Source: BscScan.com

Zoom: All

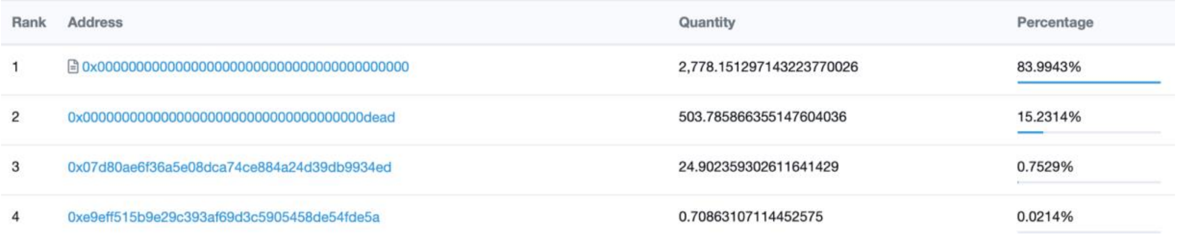
From Apr 26, 2021 To May 5, 2021

Los 10 principales poseedores de tokens de 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%

Titulares de tokens de BODA LP



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%

Detalles de las funciones del contrato
(CODING DOES NOT NEED TO BE TRANSLATED)

```
+ [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

Problemas de comprobación de estado

№	Descripción del problema.	Comprobación de estado
1	Errores del compilador.	Aprobado
2	Condiciones de carrera y reentrada. Condiciones de carrera entre funciones.	Aprobado
3	Posibles retrasos en la entrega de datos.	Aprobado
4	Llamadas a Oracle.	Aprobado
5	Ejecución frontal.	Aprobado
6	Dependencia de la marca de tiempo.	Aprobado
7	Overflow y Underflow de enteros.	Aprobado
8	DoS con Revert.	Aprobado
9	DoS con límite de gas en bloque.	Pocos problemas
10	Permisos de ejecución de métodos.	Aprobado
11	Modelo económico del contrato.	Aprobado
12	Impacto del tipo de cambio en la lógica.	Aprobado
13	Fugas de datos privados de usuarios.	Aprobado
14	Registro de eventos maliciosos.	Aprobado
15	Alcance y declaraciones.	Aprobado
16	Punteros de almacenamiento no inicializados.	Aprobado
17	Precisión aritmética.	Aprobado
18	Lógica de diseño.	Aprobado
19	Condiciones de carrera entre funciones.	Aprobado
20	Implementación y uso seguro de contratos Open Zeppelin.	Aprobado
21	Seguridad de la función Fallback.	Aprobado

Problemas de seguridad

Problemas de alta gravedad

No se han encontrado problemas de alta gravedad.

Problemas de gravedad media

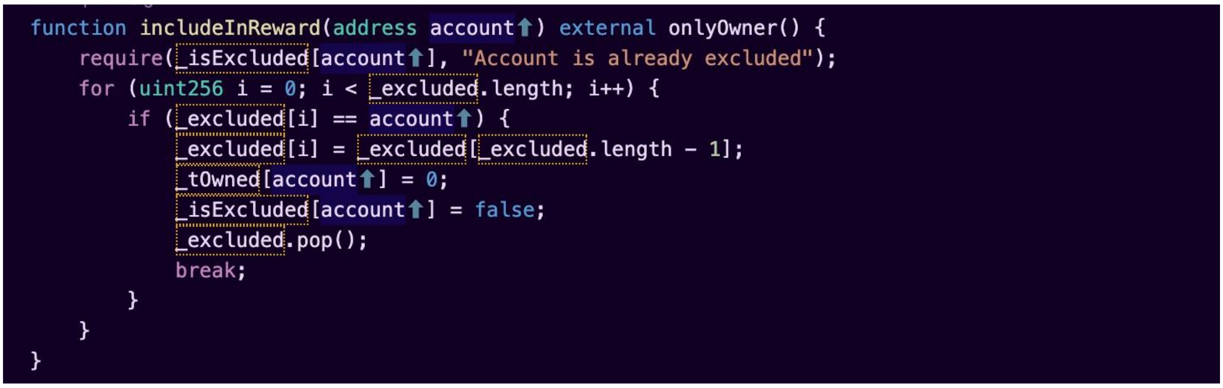
No se han encontrado problemas de gravedad media.

Problemas de baja gravedad

1. Sin gas

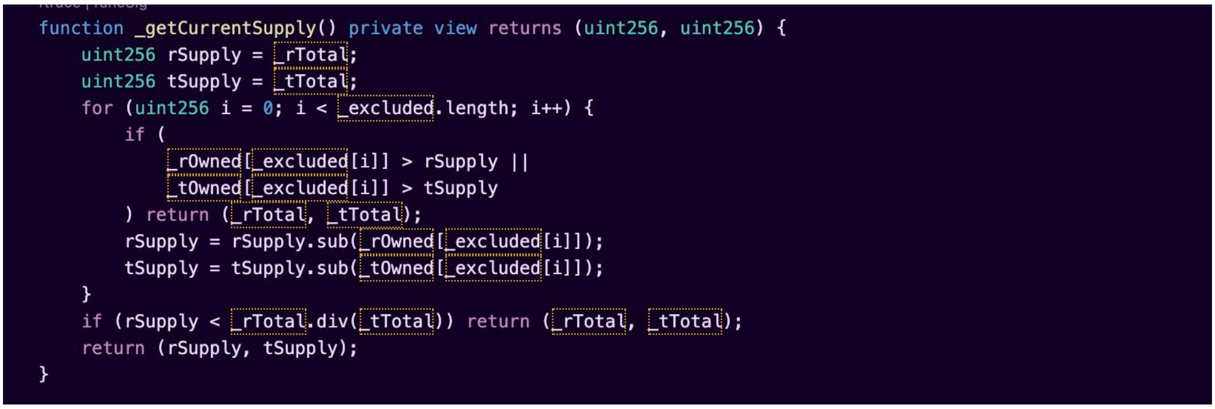
problema:

- La función includeInReward() utiliza el bucle para encontrar y eliminar direcciones de la _excluded list. La función se abortará con la excepción OUT_OF_GAS si hay una lista larga de direcciones excluidas.



```
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;
        }
    }
}
```

- La función _getCurrentSupply también utiliza el bucle para evaluar el suministro total. También puede ser abortada con la excepción OUT_OF_GAS si hay una larga lista de direcciones excluidas.



```
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);
}
```

Recomendación: Utilizar EnumerableSet en lugar de array o no utilizar arrays largos.

Conclusión:

Los contratos inteligentes no contienen problemas de alta gravedad. La seguridad del contrato de par de liquidez no se comprueba debido a que está fuera de alcance.

Nota de Techrate:
Por favor, compruebe la exención de responsabilidad anterior y tenga en cuenta que la auditoría no hace declaraciones ni ofrece garantías sobre el modelo de negocio, el atractivo de la inversión o la sostenibilidad del código. El informe se proporciona para el único contrato mencionado en el informe y no incluye ningún otro contrato potencial desplegado por el propietario.