Techrate1 Techrate

TechRate

AUDIT COMPANY

GoudaToken
Smart Contract Security Audit

TechRate

June, 2021

Audit Details

Audited project

GoudaToken

Deployer address

0x14B06bF2C5B0AFd259c47c4be39cB9368ef0be3f

Client contacts:

GoudaToken team

Blockchain

Binance Smart Chain

Project website:

https://cowswap.app

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

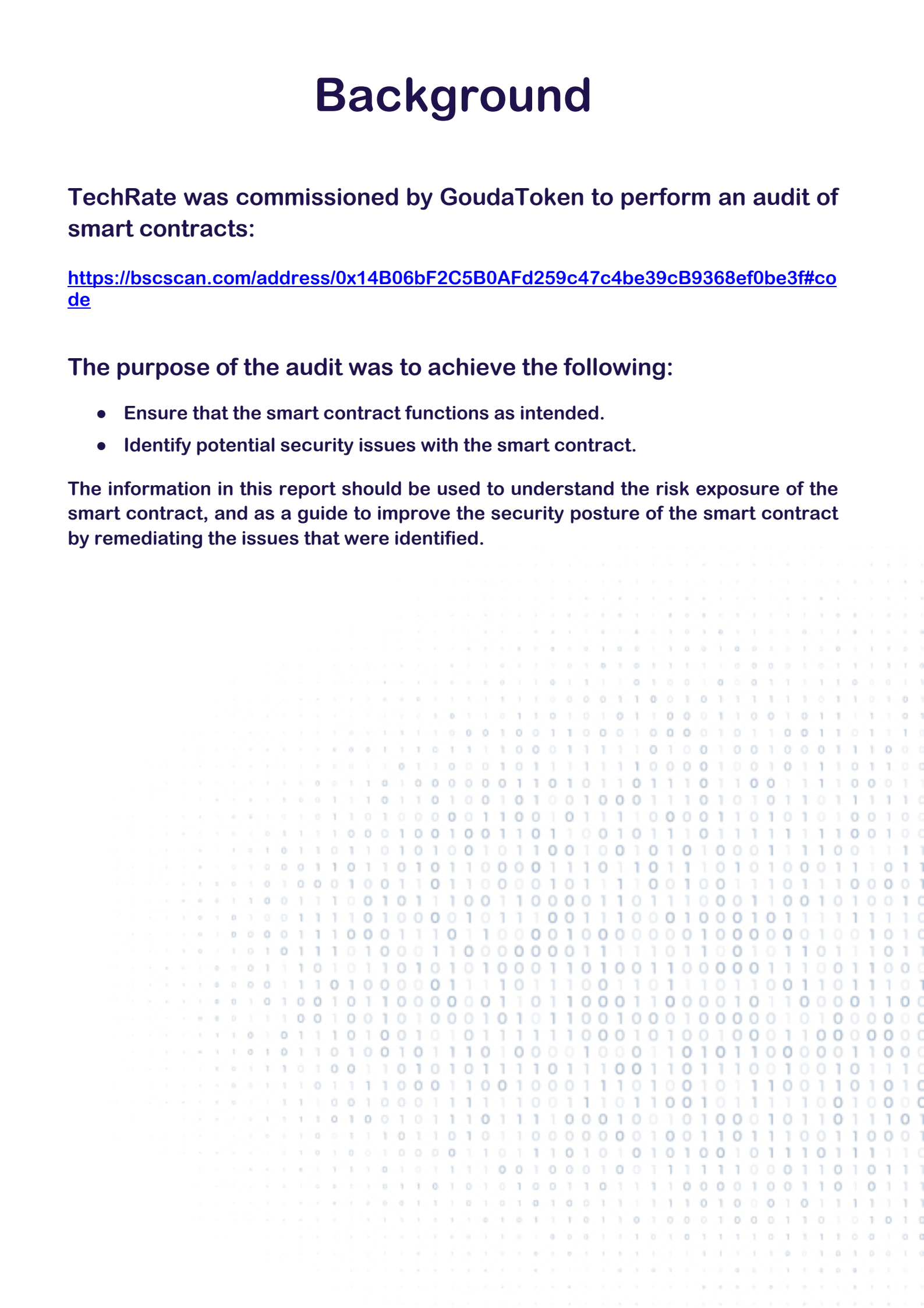
TechRate was commissioned by GoudaToken to perform an audit of smart contracts:

https://bscscan.com/address/0x14B06bF2C5B0AFd259c47c4be39cB9368ef0be3f#code

The purpose of the audit was to achieve the following:

- Ensure that the smart contract functions as intended.
- Identify potential security issues with the smart contract.

The information in this report should be used to understand the risk exposure of the smart contract, and as a guide to improve the security posture of the smart contract by remediating the issues that were identified.



Contract Details

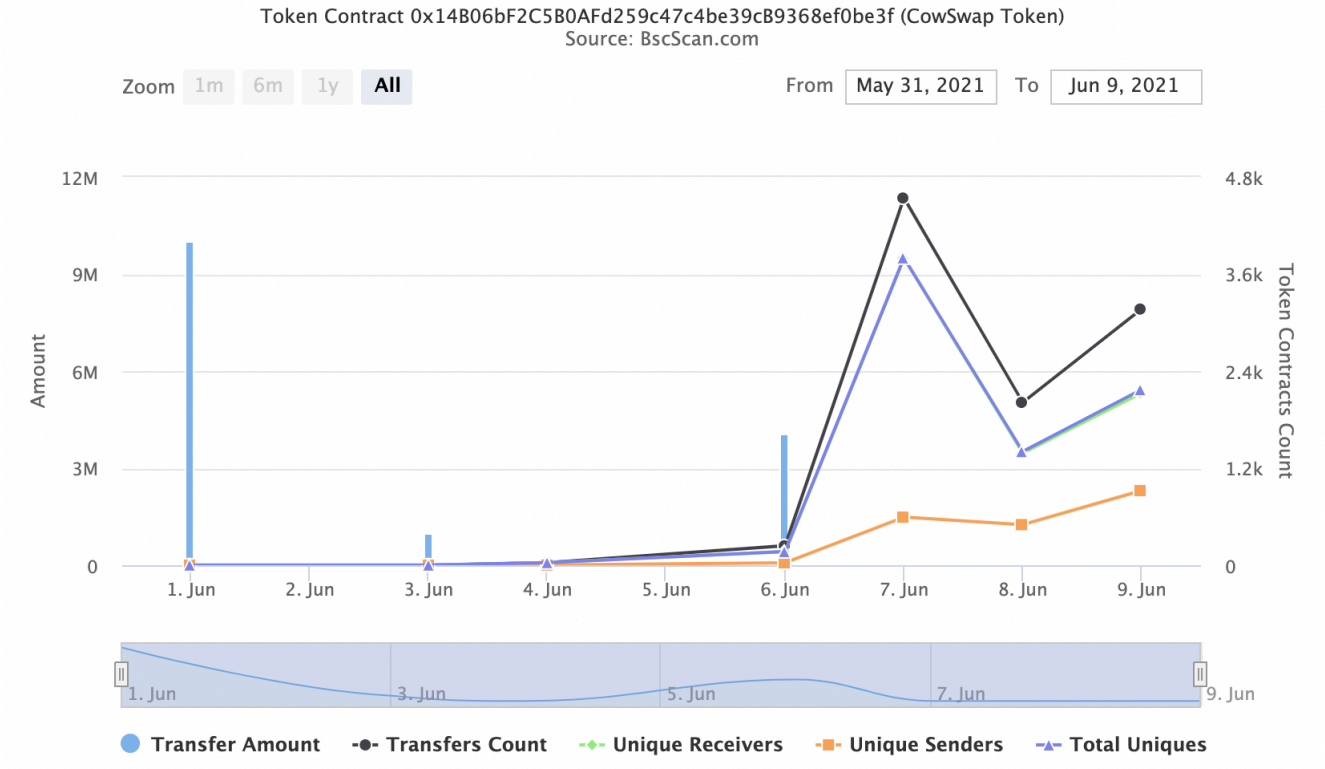
Token contract details for 11.06.2021

Contract name	GoudaToken
Contract address	0x14B06bF2C5B0AFd259c47c4be39cB9368ef0be3f
Total supply	10,000,000
Token ticker	GOUDA
Decimals	18
Token holders	5,730
Transactions count	11,659
Top 100 holders dominance	99.67%
CowSwap V2 Router	0x9f8eff2a51e31c68fad335d4db7e7764ad8f47ee
CowSwap V2 Pair	0xb71584edb3dcdc0f3b325459d7917fca86d35931
Contract deployer address	0xfAa4ce4d49956F6C52ff05b50476Cd08B49708cc
Contract's current owner address	0xfAa4ce4d49956F6C52ff05b50476Cd08B49708cc

GOUDA Token Distribution

(A total of 9,966,977.29 tokens held by the top 100 accounts from the total supply of 10,000,000.00 token)

GoudaToken Contract Interaction Details



GOUDA Top 10 Token Holders

Rank	Address	Quantity	Percentage
1	0x9dc6c547b0a1f29abc1b69a23c7152565991d80e	5,000,000	50.0000%
2	0x2c13bb2bf2d62afe8a9086c4c19c459822c9088d	3,956,845	39.5685%
3	0x0984182c618a302503d44dd0ad70b5962a8bdf9d	974,878.52	9.7488%
4	0xc369d8a741eb652b2c2771d11020f4999ff15b8b	6,807.38	0.0681%
5	0x4398ab800ba35b5dc6ea6d9752e324790eafe516	5,725	0.0573%
6	0xc370a732bb9f9d99c03c52c8672b7650d814bd34	3,654.1	0.0365%
7	0xce649d75a085c53dc80ca485f1177fe409207341	1,815	0.0182%
8	0x08ced7a40aba773d2511a5f68a0f10b2a01fb64c	1,535	0.0154%
9	0x7ee525e78c4e4d122122f99df14a556d970041c2	1,115	0.0112%
10	0x61dd97c60915f5037a5ab7089abb1c2e805c56bb	1,020	0.0102%

Contract functions details

+ Context
  - [Int] <Constructor> #
  - [Int] _msgSender
  - [Int] _msgData

+ Ownable (Context)
  - [Int] <Constructor> #
  - [Pub] owner
  - [Pub] renounceOwnership #
    - modifiers: onlyOwner
  - [Pub] transferOwnership #
    - modifiers: onlyOwner
  - [Int] _transferOwnership #

+ [Int] IBEP20
  - [Ext] totalSupply
  - [Ext] decimals
  - [Ext] symbol
  - [Ext] name
  - [Ext] getOwner
  - [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
  - [Int] min
  - [Int] sqrt

+ [Lib] Address
  - [Int] isContract
  - [Int] sendValue #
  - [Int] functionCall #
  - [Int] functionCall #
  - [Int] functionCallWithValue #
  - [Int] functionCallWithValue #
  - [Prv] _functionCallWithValue #

+ BEP20 (Context, IBEP20, Ownable)
  - [Pub] <Constructor> #
  - [Ext] getOwner
  - [Pub] name
  - [Pub] decimals
  - [Pub] symbol
  - [Pub] totalSupply
  - [Pub] balanceOf
  - [Pub] transfer #

  - [Pub] allowance
  - [Pub] approve #
  - [Pub] transferFrom #
  - [Pub] increaseAllowance #
  - [Pub] decreaseAllowance #
  - [Pub] mint #
    - modifiers: onlyOwner
  - [Int] _transfer #
  - [Int] _mint #
  - [Int] _burn #
  - [Int] _approve #
  - [Int] _burnFrom #

+ [Int] ICowswapRouter01
  - [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] ICowswapRouter02 (ICowswapRouter01)
  - [Ext] removeLiquidityETHSupportingFeeOnTransferTokens #
  - [Ext] removeLiquidityETHWithPermitSupportingFeeOnTransferTokens #
  - [Ext] swapExactTokensForTokensSupportingFeeOnTransferTokens #
  - [Ext] swapExactETHForTokensSupportingFeeOnTransferTokens ($)
  - [Ext] swapExactTokensForETHSupportingFeeOnTransferTokens #

+ [Int] ICowswapV2Factory
  - [Ext] feeTo
  - [Ext] feeToSetter
  - [Ext] getPair
  - [Ext] allPairs
  - [Ext] allPairsLength
  - [Ext] createPair #
  - [Ext] setFeeTo #
  - [Ext] setFeeToSetter #

+ [Int] ICowswapV2Pair
  - [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 #

+ GoudaToken (BEP20)
  - [Pub] <Constructor> #
  - [Ext] <Fallback> ($)
  - [Pub] mint #
    - modifiers: onlyCowMaster
  - [Int] limitCheck #
  - [Pub] transfer #
  - [Ext] removeLimit #
    - modifiers: onlyOwner
  - [Ext] setCowMaster #
    - modifiers: onlyOwner
  - [Ext] delegates
  - [Ext] delegate #
  - [Ext] delegateBySig #
  - [Ext] getCurrentVotes
  - [Ext] getPriorVotes
  - [Int] _delegate #
  - [Int] _moveDelegates #
  - [Int] _writeCheckpoint #
  - [Int] safe32
  - [Int] getChainId

($) = payable function
= non-constant function

Issues Checking Status

	Issue description	Checking status
1.	Compiler errors.	Passed
2.	Race conditions and Reentrancy. Cross-function race conditions.	Passed
3.	Possible delays in data delivery.	Passed
4.	Oracle calls.	Passed
5.	Front running.	Passed
6.	Timestamp dependence.	Passed
7.	Integer Overflow and Underflow.	Passed
8.	DoS with Revert.	Passed
9.	DoS with block gas limit.	Passed
10.	Methods execution permissions.	Passed
11.	Economy model of the contract.	Passed
12.	The impact of the exchange rate on the logic.	Passed
13.	Private user data leaks.	Passed
14.	Malicious Event log.	Passed
15.	Scoping and Declarations.	Passed
16.	Uninitialized storage pointers.	Passed
17.	Arithmetic accuracy.	Passed
18.	Design Logic.	Passed
19.	Cross-function race conditions.	Passed
20.	Safe Open Zeppelin contracts implementation and usage.	Passed
21.	Fallback function security.	Passed

Security Issues

High Severity Issues

No high severity issues found.

Medium Severity Issues

No medium severity issues found.

Low Severity Issues

No low severity issues found.

Information

1. Token address checking

Issue:

- Following the logic of checking `isToken0` in require function should be used `r1` instead of `reserve1`.

```
function limitCheck(address recipient⬆, uint256 amount⬆) internal {
    if (msg.sender == address(cowswapV2Router)) {
        (uint112 reserve0, uint112 reserve1,) = pair.getReserves();
        uint112 r0 = isToken0 ? reserve0 : reserve1;
        uint112 r1 = isToken0 ? reserve1 : reserve0;
        uint256 bnbAmount = cowswapV2Router.getAmountIn(amount⬆, uint256(r1), uint256(r0));

        require(bnbAmount.mul(199) < uint256(reserve1), "Maximum buy limit");
    }
}
```

Owner and CowMaster privileges.

- Owner can enable and disable limit on transfers from CowSwap address.

```
function removeLimit() external onlyOwner {
    limitEnabled = false;
}
```

- Owner can change CowMaster.

```
function setCowMaster(address _cowMaster⬆) external onlyOwner {
    cowMaster = _cowMaster⬆;
}
```

- Owner can mint tokens to himself.

```
function mint(uint256 amount⬆) public onlyOwner returns (bool) {
    _mint(_msgSender(), amount⬆);
    return true;
}
```

- Owner can transfer or renounce ownership.

```
ftrace | funcSig
function renounceOwnership() public onlyOwner {
    emit OwnershipTransferred(_owner, address(0));
    _owner = address(0);
}

ftrace | funcSig
function transferOwnership(address newOwner⬆) public onlyOwner {
    _transferOwnership(newOwner⬆);
}
```

- CowMaster can mint tokens.

```
function mint(address _to⬆, uint256 _amount⬆) public onlyCowMaster {
    _mint(_to⬆, _amount⬆);
    _moveDelegates(address(0), _delegates[_to⬆], _amount⬆);
}
```

Conclusion

Smart contract does not contain any issue!

TechRate note:

Please check the disclaimer above and note, the audit makes no statements or warranties on business model, investment attractiveness or code sustainability. The report is provided for the only contract mentioned in the report and does not include any other potential contracts deployed by Owner.