Audit Report

Oracula

December 2021

Type	BEP20
Address	0x85f3ec4EC49aB6a5901278176235957ef521970d
Audited by	© coinscope

Table of Contents

Contract Review

Contract Name	Oracula
Compiler Version	v0.8.11+commit.d7f03943
Optimization	200 runs
Licence	MIT
Explorer	https://bscscan.com/token/0x85f3ec4EC49aB6a5901278176235957ef521970d
Symbol	ORACULA
Decimals	18
Total Supply	50,000,000
Source	contract.sol
Domain	oracula.io

Audit Updates

Initial Audit	30th December 2021
Corrected	

Contract Analysis

● Critical ● Medium ● Minor ● Pass

Severity	Code	Description
●	ST	Contract Owner is not able to stop or pause transactions
●	OCTD	Contract Owner is not able to transfer tokens from specific address
●	ELFM	Contract Owner is not able to increase fees more than a reasonable percent (25%)
●	ULTW	Contract Owner is not able to increase the amount of liquidity taken by dev wallet more than a reasonable percent
●	MT	Contract Owner is not able to mint new tokens
●	BT	Contract Owner is not able to burn tokens from specific wallet
●	BC	Contract Owner is not able to blacklist wallets from selling

Contract Diagnostics

Critical Medium Minor

Severity	Code	Description
	L09	Dead Code Elimination
	L04	Conformance to Solidity Naming Conventions
	L03	Redundant Statements
	L02	State Variables could be Declared Constant
	L01	Public Function could be Declared External

L09 - Dead Code Elimination

Criticality	minor
Location	contract.sol#L69,L29,L33 and 9 more

Description

Functions that are not used in the contract, and make the code's size bigger.

```
_verifyCallResult
functionCall
functionCall
...
```

Recommendation

Remove unused functions.

L04 - Conformance to Solidity Naming Conventions

Criticality	minor
Location	contract.sol#L242,L243,L260 and 9 more

Description

Solidity defines a naming convention that should be followed. Rule exceptions:

- Allow constant variable name/symbol/decimals to be lowercase.
- Allow _ at the beginning of the mixed_case match for private variables and unused parameters.

```
DOMAIN_SEPARATOR
PERMIT_TYPEHASH
MINIMUM_LIQUIDITY
...
```

Recommendation

Follow the Solidity naming convention.
https://docs.soliditylang.org/en/v0.4.25/style-guide.html#naming-conventions

L03 - Redundant Statements

Criticality	minor
Location	contract.sol#L10

Description

Detect the usage of redundant statements that have no effect.

Context

Recommendation

Remove redundant statements if they congest code but offer no value.

L02 - State Variables could be Declared Constant

Criticality	minor
Location	contract.sol#L418,L416,L417 and 1 more

Description

Constant state variables should be declared constant to save gas.

```
_decimals
_name
_symbol
...
```

Recommendation

Add the constant attribute to state variables that never change.

L01 - Public Function could be Declared External

Criticality	minor
Location	contract.sol#L103,L109,L503 and 5 more

Description

Public functions that are never called by the contract should be declared external to save gas.

```
renounceOwnership
transferOwnership
transfer
...
```

Recommendation

Use the external attribute for functions never called from the contract

Contract Functions

Contract	Type	Bases		
	Function Name	**Visibility**	**Mutability**	**Modifiers**
Context	Implementation			
	_msgSender	Internal		
	_msgData	Internal		
Address	Library			
	isContract	Internal		
	sendValue	Internal	✓	
	functionCall	Internal	✓	
	functionCall	Internal	✓	
	functionCallWithValue	Internal	✓	
	functionCallWithValue	Internal	✓	
	functionStaticCall	Internal		
	functionStaticCall	Internal		
	functionDelegateCall	Internal	✓	
	functionDelegateCall	Internal	✓	
	_verifyCallResult	Private		
Ownable	Implementation	Context		
	<Constructor>	Public	✓	-
	owner	Public		-
	renounceOwnership	Public	✓	onlyOwner
	transferOwnership	Public	✓	onlyOwner
IBEP20	Interface			
	totalSupply	External		-
	decimals	External		-
	symbol	External		-
	name	External		-
	getOwner	External		-

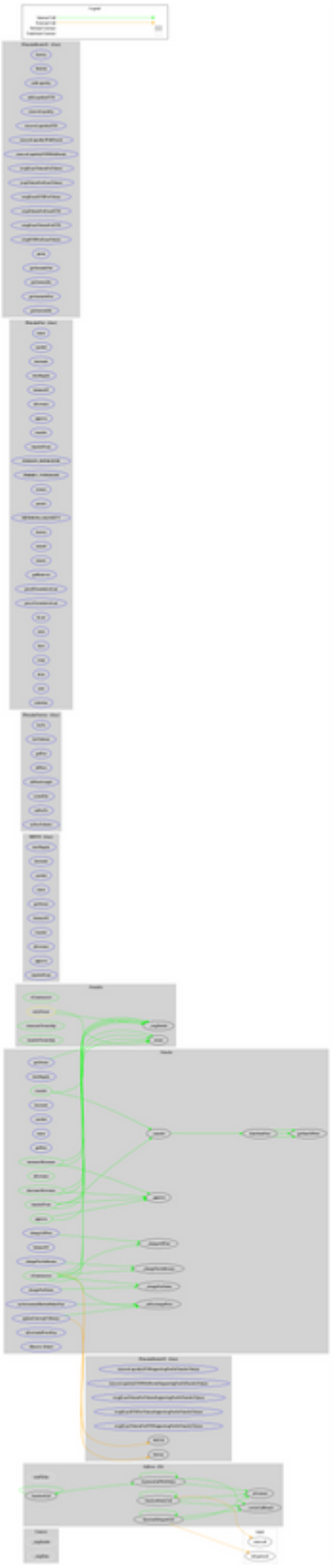
	balanceOf	External		-
	transfer	External	✓	-
	allowance	External		-
	approve	External	✓	-
	transferFrom	External	✓	-
IPancakeFactory	Interface			
	feeTo	External		-
	feeToSetter	External		-
	getPair	External		-
	allPairs	External		-
	allPairsLength	External		-
	createPair	External	✓	-
	setFeeTo	External	✓	-
	setFeeToSetter	External	✓	-
IPancakePair	Interface			
	name	External		-
	symbol	External		-
	decimals	External		-
	totalSupply	External		-
	balanceOf	External		-
	allowance	External		-
	approve	External	✓	-
	transfer	External	✓	-
	transferFrom	External	✓	-
	DOMAIN_SEPARATOR	External		-
	PERMIT_TYPEHASH	External		-
	nonces	External		-
	permit	External	✓	-
	MINIMUM_LIQUIDITY	External		-
	factory	External		-
	token0	External		-
	token1	External		-
	getReserves	External		-

	price0CumulativeLast	External		-
	price1CumulativeLast	External		-
	kLast	External		-
	mint	External	✓	-
	burn	External	✓	-
	swap	External	✓	-
	skim	External	✓	-
	sync	External	✓	-
	initialize	External	✓	-
IPancakeRouter01	Interface			
	factory	External		-
	WETH	External		-
	addLiquidity	External	✓	-
	addLiquidityETH	External	Payable	-
	removeLiquidity	External	✓	-
	removeLiquidityETH	External	✓	-
	removeLiquidityWithPermit	External	✓	-
	removeLiquidityETHWithPermit	External	✓	-
	swapExactTokensForTokens	External	✓	-
	swapTokensForExactTokens	External	✓	-
	swapExactETHForTokens	External	Payable	-
	swapTokensForExactETH	External	✓	-
	swapExactTokensForETH	External	✓	-
	swapETHForExactTokens	External	Payable	-
	quote	External		-
	getAmountOut	External		-
	getAmountIn	External		-
	getAmountsOut	External		-
	getAmountsIn	External		-
IPancakeRouter02	Interface	IPancakeRouter01		
	removeLiquidityETHSupportingFeeOnTransferTokens	External	✓	-

	removeLiquidityETHWithPermitSupportingFeeOnTransferTokens	External	✓	-
	swapExactTokensForTokensSupportingFeeOnTransferTokens	External	✓	-
	swapExactETHForTokensSupportingFeeOnTransferTokens	External	Payable	-
	swapExactTokensForETHSupportingFeeOnTransferTokens	External	✓	-
Oracula	Implementation	Context, IBEP20, Ownable		
	<Constructor>	Public	✓	-
	totalSupply	External		-
	getOwner	External		-
	decimals	External		-
	symbol	External		-
	name	External		-
	getFees	External		-
	getSumOfFees	Public		-
	transfer	Public	✓	-
	allowance	Public		-
	approve	Public	✓	-
	transferFrom	Public	✓	-
	increaseAllowance	Public	✓	-
	decreaseAllowance	Public	✓	-
	_transfer	Internal	✓	
	_approve	Internal	✓	
	balanceOf	External		-
	distributeFees	Internal	✓	
	updateUniswapV2Router	External	✓	onlyOwner
	changeAllFees	External	✓	onlyOwner
	_changeAllFees	Internal	✓	
	changeFeeAddresses	External	✓	onlyOwner
	_changeFeeAddresses	Internal	✓	
	changeFeeStatus	External	✓	onlyOwner
	_changeFeeStatus	Internal	✓	

	setAutomatedMarketMakerPair	External	✓	onlyOwner
	_setExchangePairs	Internal	✓	
	isExcludedFromFees	External		-
	<Receive Ether>	External	Payable	-

Contract Flow



Domain Info

Domain Name	oracula.io
Registry Domain ID	86b16db1b1d647ec9c0c021c8e067bcc-DONUTS
Creation Date	2021-03-23T14:48:24Z
Updated Date	2021-05-22T20:34:58Z
Registry Expiry Date	2022-03-23T14:48:24Z
Registrar WHOIS Server	whois.tucows.com
Registrar URL	http://www.tucows.com
Registrar	Tucows Domains Inc.
Registrar IANA ID	69

The domain has been created 9 months before the creation of the audit. It will expire in 3 months.

There is no public billing information, the creator is protected by the privacy settings.

Summary

Oracula is aiming to create a DeFi Prediction markets platform. The token has a friendly and growing community. No compiler errors or major issues were found on the contract. The owner can change fees, but there are limitations to how high he can set them. There are some minor comments and improvements that do not affect the contract security.

Disclaimer

All the content provided in this document is for general information only and should not be used as financial advice or a reason to buy any investment.

Coinscope team provides no guarantees against the sale of team tokens or the removal of liquidity by the project audited in this document. Always Do your own research and protect yourselves from being scammed.

The Coinscope team has audited this project for general information and only expresses their opinion based on similar projects and checks from popular diagnostic tools. Under no circumstances did Coinscope receive a payment to manipulate those results or change the awarding badge that we will be adding in our website.

Always Do your own research and protect yourselves from scams. This document should not be presented as a reason to buy or not buy any particular token.

The Coinscope team disclaims any liability for the resulting losses.

About Coinscope

Coinscope is the leading early coin listing, voting and auditing authority firm. The audit process is analyzing and monitoring many aspects of the project. That way, it gives the community a good sense of security using an informative report and a generic score.

Coinscope is aiming to make crypto discoverable and efficient globally. It provides all the essential tools to assist users draw their own conclusions.

The Coinscope.co team

https://www.coinscope.co