Cyberscope

Audit Report

Justice Token

April 2022

Table of Contents

Table of Contents   1

Contract Review   3

Source Files   3

Audit Updates   3

Contract Analysis   4

Contract Diagnostics   5

    CO - Code Optimization   6

        Description   6

        Recommendation   6

    L01 - Public Function could be Declared External 7

        Description   7

        Recommendation   7

    L02 - State Variables could be Declared Constant 8

        Description   8

        Recommendation   8

    L04 - Conformance to Solidity Naming Conventions 9

        Description   9

        Recommendation   9

    L08 - Tautology or Contradiction   10

        Description   10

        Recommendation   10

    L09 - Dead Code Elimination   11

        Description   11

        Recommendation   11

    L13 - Divide before Multiply Operation   12

        Description   12

Contract Review

Contract Name	Justice
Compiler Version	v0.8.7+commit.e28d00a7
Optimization	200 runs
Licence	MIT
Explorer	https://bscscan.com/token/0xFFDCCACB0aD5f9FEFdc99870EB6Ac73A4c714842
Symbol	JUSTICE
Decimals	9
Total Supply	100,000,000
Domain	justiceproject.io

Source Files

Filename	SHA256
Justice Token AntiBot.sol	db91dd3cfe1b019585c75d24032913b07c8703ccd7962c5769215ade086cda26
justicetoken-importsV2.sol	eceeba5278ba8cdaae256e51e86a259014e9271b669670fdba6fc779ca22e1e2

Audit Updates

Initial Audit	12th April 2022
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
●	OTUT	Owner Transfer User's Tokens
●	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
●	CO	Code Optimization
●	L01	Public Function could be Declared External
●	L02	State Variables could be Declared Constant
●	L04	Conformance to Solidity Naming Conventions
●	L08	Tautology or Contradiction
●	L09	Dead Code Elimination
●	L13	Divide before Multiply Operation
●	L15	Local Scope Variable Shadowing

CO - Code Optimization

Criticality	minor
Location	contract.sol#L61, 475

Description

There are code segments that could be optimized. A segment may be optimized so that it becomes a smaller size, consumes less memory, executes more rapidly, or performs fewer operations.

```
uint256 internal constant maxWalletBalance = 0;
```

```
if ( maxWalletBalance > 0 && !_isUnlimitedSender(sender) &&
!_isUnlimitedRecipient(recipient) && !_isV2Pair(recipient) ){
            uint256 recipientBalance = balanceOf(recipient);
            require(recipientBalance + amount <= maxWalletBalance, "New
balance would exceed the maxWalletBalance");
        }
```

Also, the contract is calling _takeFee through _takeFeeToEth.

```
function _takeFeeToETH(uint256 amount, uint256 currentRate, uint256 fee,
address recipient, uint256 index) private {
      _takeFee(amount, currentRate, fee, recipient, index);
    }
```

Recommendation

Rewrite some code segments so the runtime will be more performant.

L01 - Public Function could be Declared External

Criticality	minor
Location	Justice Token AntiBot.sol#L344,349,409
	justicetoken-importsV2.sol#L104,108,113,116,122

Description

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

```
unlock
lock
getUnlockTime
transferOwnership
renounceOwnership
isExcludedFromFee
decreaseAllowance
increaseAllowance
```

Recommendation

Use the external attribute for functions never called from the contract

L02 - State Variables could be Declared Constant

Criticality	minor
Location	Justice Token AntiBot.sol#L615,617,619,121,119,120,116

Description

Constant state variables should be declared constant to save gas.

```
burnAddress
Staking
Gameplay
Development
_testnetRouterAddress
_mainnetRouterV2Address
_mainnetRouterV1Address
```

Recommendation

Add the constant attribute to state variables that never change.

L04 - Conformance to Solidity Naming Conventions

Criticality	minor
Location	Justice Token AntiBot.sol#L37,61,75,119,120,121,332,421,201,202 and 5 more
	justicetoken-importsV2.sol#L153

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.

```
WETH
_pair
_router
_isExcludedFromRewards
_isExcludedFromFee
_allowances
_balances
_reflectedBalances
_enable
...
```

Recommendation

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

L08 - Tautology or Contradiction

Criticality	minor
Location	Justice Token AntiBot.sol#L169

Description

Detects expressions that are tautologies or contradictions. For instance, an uint variable will always be greater than or equal to zero.

```
require(bool,string)(index >= 0 && index < fees.length,FeesSettings._getFeeStruct: Fee index out of bounds)
```

Recommendation

Fix the incorrect comparison by changing the value type or the comparison.

L09 - Dead Code Elimination

Criticality	minor
Location	justicetoken-importsV2.sol#L76,51,52,53,54,68,71,60,63,46 and 1 more Justice Token AntiBot.sol#L565,575,580,602,808,142,147,183

Description

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

```
getCollectedFeeTotal
_addFees
_addFee
_approveDelegate
_takeTransactionFees
_isV2Pair
_getSumOfFees
_beforeTokenTransfer
sendValue
...
```

Recommendation

Remove unused functions.

L13 - Divide before Multiply Operation

Criticality	minor
Location	Justice Token AntiBot.sol#L527,591,905,913

Description

Performing divisions before multiplications may cause lose of prediction.

```
tAmount = amount.mul(fee).div(FEES_DIVISOR)
tBurn = amount.mul(fee).div(FEES_DIVISOR)
tFee = amount.mul(fee).div(FEES_DIVISOR)
tTotalFees = tAmount.mul(feesSum).div(FEES_DIVISOR)
```

Recommendation

The multiplications should be prior to the divisions.

L15 - Local Scope Variable Shadowing

Criticality	minor
Location	Justice Token AntiBot.sol#L499,521,839,883

Description

The are variables that are defined in the local scope containing the same name from an upper scope.

```
name
_env
sumOfFees
```

Recommendation

The local variables should have different names from the upper scoped variables.

Contract Functions

Contract	Type	Bases		
	Function Name	Visibility	Mutability	Modifiers
Tokenomics	Implementation			
	<Constructor>	Public	✓	-
	_addFee	Private	✓	
	_addFees	Private	✓	
	_getFeesCount	Internal		
	_getFeeStruct	Private		
	_getFee	Internal		
	_addFeeCollectedAmount	Internal	✓	
	getCollectedFeeTotal	Internal		
Presaleable	Implementation	Manageable		
	setPreseableEnabled	External	✓	onlyManager
BaseRfiToken	Implementation	IERC20, IERC20Met adata, Ownable, Presaleable, Tokenomics		
	<Constructor>	Public	✓	-
	name	External		-
	symbol	External		-
	decimals	External		-
	totalSupply	External		-
	balanceOf	Public		-
	transfer	External	✓	-
	allowance	External		-
	approve	External	✓	-
	transferFrom	External	✓	-
	burn	External	✓	-

	_burnTokens	Internal	✓	
	setMaxTransactionAmount	External	✓	onlyOwner
	increaseAllowance	Public	✓	-
	decreaseAllowance	Public	✓	-
	isExcludedFromReward	External		-
	reflectionFromToken	External		-
	tokenFromReflection	Internal		
	excludeFromReward	External	✓	onlyManager
	_exclude	Internal	✓	
	includeInReward	External	✓	onlyManager
	setExcludedFromFee	External	✓	onlyManager
	isExcludedFromFee	Public		-
	_approve	Internal	✓	
	setEnableAntiBot	External	✓	onlyOwner
	_isUnlimitedSender	Internal		
	_isUnlimitedRecipient	Internal		
	_transfer	Private	✓	
	_transferTokens	Private	✓	
	_takeFees	Private	✓	
	_getValues	Internal		
	_getCurrentRate	Internal		
	_getCurrentSupply	Internal		
	_beforeTokenTransfer	Internal	✓	
	_getSumOfFees	Internal		
	_isV2Pair	Internal		
	_redistribute	Internal	✓	
	_takeTransactionFees	Internal	✓	
Liquifier	Implementation	Ownable, Manageable		
	\<Receive Ether\>	External	Payable	-
	initializeLiquiditySwapper	Internal	✓	
	liquify	Internal	✓	
	_setRouterAddress	Private	✓	
	_swapAndLiquify	Private	✓	lockTheSwap
	_swapTokensForEth	Private	✓	

	_addLiquidity	Private	✓	
	setRouterAddress	External	✓	onlyManager
	setSwapAndLiquifyEnabled	External	✓	onlyManager
	withdrawLockedEth	External	✓	onlyManager
	_approveDelegate	Internal	✓	
Antiwhale	Implementation	Tokenomics		
	_getAntiwhaleFees	Internal		
JusticeToken	Implementation	BaseRfiToken, Liquifier, Antiwhale		
	<Constructor>	Public	✓	-
	_isV2Pair	Internal		
	_getSumOfFees	Internal		
	_beforeTokenTransfer	Internal	✓	
	_takeTransactionFees	Internal	✓	
	_burn	Private	✓	
	_takeFee	Private	✓	
	_takeFeeToETH	Private	✓	
	_approveDelegate	Internal	✓	
Justice	Implementation	JusticeToken		
	<Constructor>	Public	✓	JusticeToken
IPinkAntiBot	Interface			
	setTokenOwner	External	✓	-
	onPreTransferCheck	External	✓	-
IERC20	Interface			
	totalSupply	External		-
	balanceOf	External		-
	transfer	External	✓	-
	allowance	External		-
	approve	External	✓	-

	transferFrom	External	✓	-
IERC20Metad ata	Interface	IERC20		
	name	External		-
	symbol	External		-
	decimals	External		-
Context	Implementation			
	_msgSender	Internal		
	_msgData	Internal		
JusticeLib	Library			
	add	Internal		
	sub	Internal		
	mul	Internal		
	div	Internal		
	mod	Internal		
	sub	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
	getUnlockTime	Public		-
	lock	Public	✓	onlyOwner
	unlock	Public	✓	-
Manageable	Implementation	Context		
	<Constructor>	Public	✓	-
	manager	Public		-
	transferManagement	External	✓	onlyManager
IPancakeV2Factory	Interface			
	createPair	External	✓	-
IPancakeV2Router	Interface			
	factory	External		-
	WETH	External		-
	addLiquidityETH	External	Payable	-
	swapExactTokensForETHSupporting FeeOnTransferTokens	External	✓	-

Contract Flow
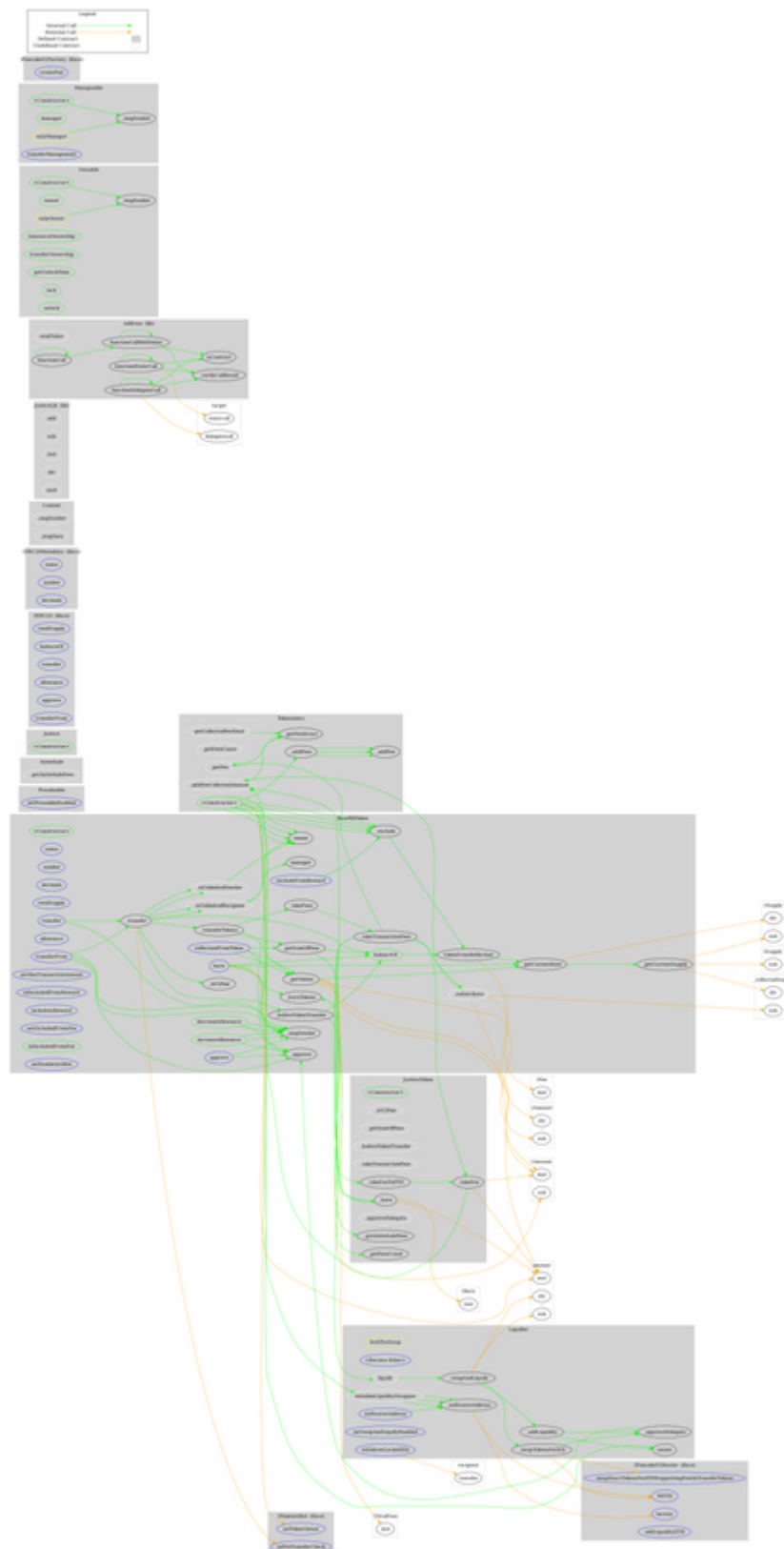
Domain Info

Domain Name	justiceproject.io
Registry Domain ID	af27f681165240b2b932d6afb4205e3b-DONUTS
Creation Date	2022-01-12T05:43:53Z
Updated Date	2022-02-23T13:35:08Z
Registry Expiry Date	2023-01-12T05:43:53Z
Registrar WHOIS Server	whois.godaddy.com/
Registrar URL	http://www.godaddy.com/domains/search.aspx?ci=8990
Registrar	GoDaddy.com, LLC
Registrar IANA ID	146

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

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

Summary

Justice is an interesting project that has a friendly and growing community. The Smart Contract analysis reported no compiler error or critical issues. The contract Owner can access some admin functions that can not be used in a malicious way to disturb the users' transactions. There is also a limit of max 25% fees.

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.

Cyberscope 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 Cyberscope 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 Cyberscope 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 Cyberscope team disclaims any liability for the resulting losses.

About Cyberscope

Coinscope audit and K.Y.C. service has been rebranded to Cyberscope.

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.

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

The Cyberscope team

https://www.cyberscope.io