



Cyberscope

Audit Report

Rebase Aggregator Capital

April 2022

Type ERC20

Network AVAX

Address 0xd33df97747dD6bEcAD26B2e61F818c94B7588E69

Audited by © cyberscope

Table of Contents

Table of Contents	1
Contract Review	3
Source Files	3
Audit Updates	3
Contract Analysis	4
Contract Diagnostics	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
L07 - Missing Events Arithmetic	10
Description	10
Recommendation	10
L11 - Unnecessary Boolean equality	11
Description	11
Recommendation	11
L12 - Using Variables before Declaration	12
Description	12
Recommendation	12
L13 - Divide before Multiply Operation	13
Description	13

Recommendation	13
L14 - Uninitialized Variables in Local Scope	14
Description	14
Recommendation	14
Contract Functions	15
Contract Flow	21
Domain Info	22
Summary	23
Caution is advised	23
Disclaimer	24
About Cyberscope	25

Contract Review

Contract Name	RebaseAggregatorCapital
Compiler Version	v0.8.13+commit.abaa5c0e
Optimization	100 runs
Licence	MIT
Explorer	https://snowtrace.io/address/0xd33df97747dD6bEcAD26B2e61F818c94B7588E69
Symbol	\$REACT
Decimals	18
Total Supply	100,000,000
Domain	react.ac

Source Files

Filename	SHA256
contract.sol	02aae206510a01bb3c522fe630194b078a52811d560e373e12bfb8553f6c7485

Audit Updates

Initial Audit	11th April 2022
Corrected	

Contract Analysis



Unverified libraries are imported and can't be audited. The scope of the audit will be limited only to the verified contracts.

● 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
●	L01	Public Function could be Declared External
●	L02	State Variables could be Declared Constant
●	L04	Conformance to Solidity Naming Conventions
●	L07	Missing Events Arithmetic
●	L11	Unnecessary Boolean equality
●	L12	Using Variables before Declaration
●	L13	Divide before Multiply Operation
●	L14	Uninitialized Variables in Local Scope

L01 - Public Function could be Declared External

Criticality	minor
Location	contract.sol#L293,313,327,344,368,445,472,476,480,488,498,512,516,763,787,799,803

Description

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

```
addMultipleTokens
addTokenToList
getCurrentTokenLength
multiSendTokens
getMaxWallet
getMaxTX
setExcludedFromFees
setDividendExcluded
isExcludedFromLimits
...
```

Recommendation

Use the external attribute for functions never called from the contract.

L02 - State Variables could be Declared Constant

Criticality	minor
Location	contract.sol#L133

Description

Constant state variables should be declared constant to save gas.

```
_tTotal
```

Recommendation

Add the constant attribute to state variables that never change.

L04 - Conformance to Solidity Naming Conventions

Criticality

minor

Location

contract.sol#L32,72,73,364,424,435,848,120,123,129,130,131,132,151,158,167,168,169,170,171,186,208,215

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.

```
initialLockTime
_hasLiqBeenAdded
_taxWallets
masterTaxDivisor
maxSniperFee
maxTransferTaxes
maxSellTaxes
maxBuyTaxes
_ratios
...
```

Recommendation

Follow the Solidity naming convention.

<https://docs.soliditylang.org/en/v0.4.25/style-guide.html#naming-conventions>

L07 - Missing Events Arithmetic

Criticality	minor
Location	contract.sol#L429,440,502,507,520

Description

Detected missing events for critical arithmetic parameters. There are functions that have no event emitted, so it is difficult to track off-chain changes.

```
boostTime = time
_maxWalletSize = (_tTotal * percent) / divisor
_maxTxAmount = (_tTotal * percent) / divisor
reflectorGas = gas
swapThreshold = (_tTotal * thresholdPercent) / thresholdDivisor
```

Recommendation

Emit an event for critical parameter changes.

L11 - Unnecessary Boolean equality

Criticality

minor

Location

contract.sol#L458,831

Description

The comparison to boolean constants is redundant. Boolean constants can be used directly and do not need to be compared to true or false.

```
_isExcludedFromFees[msg.sender] == false  
enabled == false
```

Recommendation

Remove the equality to the boolean constant.

L12 - Using Variables before Declaration

Criticality	minor
Location	contract.sol#L612

Description

The contract is using a variable before the declaration. This is usually happening either if it has not been declared yet or the variable has been declared in a different scope.

check

Recommendation

The variables should be declared before any usage of them.

L13 - Divide before Multiply Operation

Criticality	minor
Location	contract.sol#L683

Description

Performing divisions before multiplications may cause lose of prediction.

```
toLiquify = ((contractTokenBalance * ratios.liquidity) / (ratios.total)) / 2
```

Recommendation

The multiplications should be prior to the divisions.

L14 - Uninitialized Variables in Local Scope

Criticality

minor

Location

contract.sol#L612,611

Description

These are variables that are defined in the local scope and are not initialized.

checked
check

Recommendation

All the local scoped variables should be initialized.

Contract Functions

Contract	Type	Bases		
	Function Name	Visibility	Mutability	Modifiers
IERC20	Interface			
	totalSupply	External		-
	decimals	External		-
	symbol	External		-
	name	External		-
	getOwner	External		-
	balanceOf	External		-
	transfer	External	✓	-
	allowance	External		-
	approve	External	✓	-
	transferFrom	External	✓	-
IFactoryV2	Interface			
	getPair	External		-
	createPair	External	✓	-
IV2Pair	Interface			
	factory	External		-
	getReserves	External		-
IRouter01	Interface			
	factory	External		-
	WAVAX	External		-
	addLiquidityAVAX	External	Payable	-
	quote	External		-
	getAmountOut	External		-
	getAmountIn	External		-
	getAmountsOut	External		-
	getAmountsIn	External		-

IRouter02	Interface	IRouter01		
	swapExactTokensForAVAXSupportingFeeOnTransferTokens	External	✓	-
AntiSnipe	Interface			
	checkUser	External	✓	-
	setLaunch	External	✓	-
	setLpPair	External	✓	-
	setProtections	External	✓	-
	removeSniper	External	✓	-
	removeBlacklisted	External	✓	-
	isBlacklisted	External		-
	transfer	External	✓	-
	isSniper	External		-
Cashier	Interface			
	whomst	External		-
	whomst_router	External		-
	whomst_token	External		-
	setToken	External	✓	-
	setReflectionCriteria	External	✓	-
	tally	External	✓	-
	load	External	Payable	-
	cashout	External	✓	-
	giveMeWelfarePlease	External	✓	-
	giveMeSpecificWelfarePlease	External	✓	-
	getTotalDistributed	External		-
	getShareholderInfo	External		-
	getShareholderRealized	External		-
	getPendingRewards	External		-
	initialize	External	✓	-
	setUserReflectingToken	External	✓	-
	compoundDividends	External	✓	-
	addTokenToList	External	✓	-
	addMultipleTokens	External	✓	-

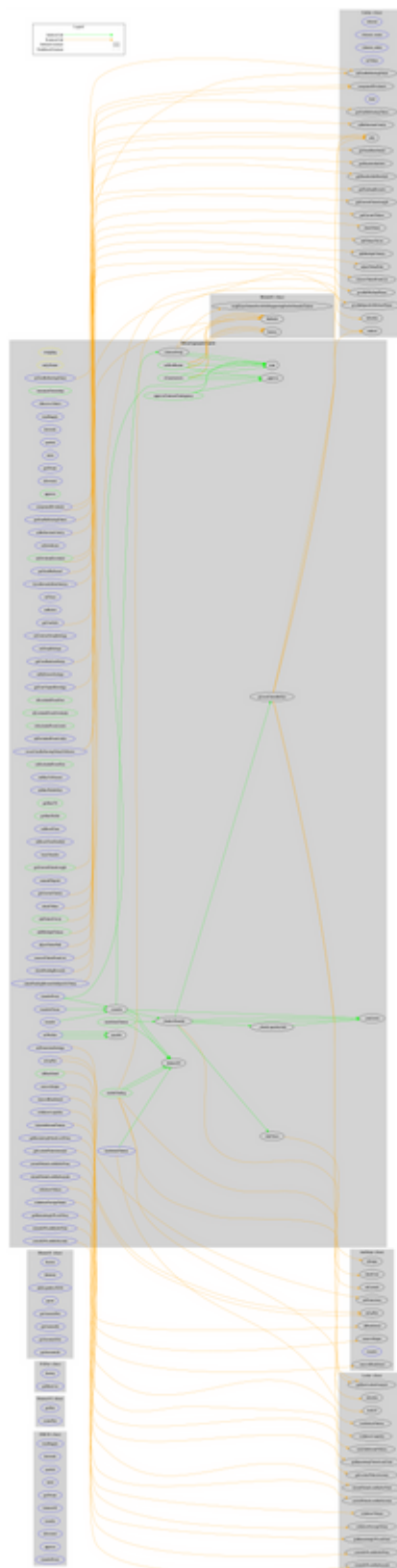
	adjustTokenPath	External	✓	-
	removeTokenFromList	External	✓	-
	getCurrentTokenLength	External		-
	getCurrentTokens	External		-
	checkToken	External		-
	getUserReflectingToken	External		-
Locker	Interface			
	initialize	External	✓	-
	withdrawForeignToken	External	✓	-
	lockLP	External	✓	-
	getRemainingLPLockTime	External		-
	extendLPLOCKBySetTime	External	✓	-
	extendLPLOCKBySeconds	External	✓	-
	withdrawLiquidity	External	✓	-
	lockInitialTokens	External	✓	-
	lockAdditionalTokens	External	✓	-
	getRemainingTokenLockTime	External		-
	getLockedTokenAmount	External		-
	getRawLockedAmount	External		-
	extendTokenLockBySetTime	External	✓	-
	extendTokenLockBySeconds	External	✓	-
	withdrawTokens	External	✓	-
RebaseAggregatorCapital	Implementation	IERC20		
	<Constructor>	Public	Payable	-
	transferOwner	External	✓	onlyOwner
	renounceOwnership	Public	✓	onlyOwner
	<Receive Ether>	External	Payable	-
	totalSupply	External		-
	decimals	External		-
	symbol	External		-
	name	External		-
	getOwner	External		-
	balanceOf	Public		-

	allowance	External		-
	approve	Public	✓	-
	_approve	Private	✓	
	approveContractContingency	Public	✓	onlyOwner
	transfer	External	✓	-
	transferFrom	External	✓	-
	isBlacklisted	Public		-
	setInitializers	External	✓	onlyOwner
	removeSniper	External	✓	onlyOwner
	removeBlacklisted	External	✓	onlyOwner
	setProtectionSettings	External	✓	onlyOwner
	enableTrading	Public	✓	onlyOwner
	setTaxes	External	✓	onlyOwner
	setRatios	External	✓	-
	setWallets	External	✓	onlyOwner
	setContractSwapSettings	External	✓	onlyOwner
	setSwapSettings	External	✓	onlyOwner
	setReflectionCriteria	External	✓	onlyOwner
	setReflectorSettings	External	✓	onlyOwner
	setNewRouter	Public	✓	onlyOwner
	setLpPair	External	✓	onlyOwner
	isExcludedFromFees	Public		-
	isExcludedFromDividends	Public		-
	isExcludedFromLimits	Public		-
	setExcludedFromLimits	External	✓	onlyOwner
	setDividendExcluded	Public	✓	onlyOwner
	setExcludedFromFees	Public	✓	onlyOwner
	setMaxTxPercent	External	✓	onlyOwner
	setMaxWalletSize	External	✓	onlyOwner
	getMaxTX	Public		-
	getMaxWallet	Public		-
	setBoostTime	External	✓	onlyOwner
	setBoostTimeEnabled	External	✓	onlyOwner
	basicTransfer	External	✓	-
	_hasLimits	Private		

	_transfer	Internal	✓	
	_finalizeTransfer	Internal	✓	
	processTokenReflect	Internal	✓	
	forceRewardsDistribution	External	✓	-
	takeTaxes	Internal	✓	
	contractSwap	Internal	✓	swapping
	_checkLiquidityAdd	Private	✓	
	manualDeposit	External	✓	onlyOwner
	multiSendTokens	Public	✓	onlyOwner
	getTotalReflected	External		-
	getUserInfo	External		-
	getUserRealizedGains	External		-
	getUserUnpaidEarnings	External		-
	getCurrentTokenLength	Public		-
	getCurrentTokens	External		-
	checkToken	External		-
	addTokenToList	Public	✓	onlyOwner
	addMultipleTokens	Public	✓	onlyOwner
	adjustTokenPath	External	✓	onlyOwner
	removeTokenFromList	External	✓	onlyOwner
	claimPendingRewards	External	✓	-
	claimPendingRewardsInSpecificToken	External	✓	-
	setUserReflectingToken	External	✓	-
	revertUserReflectingTokenToNative	External	✓	-
	compoundDividends	External	✓	-
	getUserReflectingToken	External		-
	withdrawForeignToken	External	✓	onlyOwner
	getRemainingLPLOCKTime	External		-
	extendLPLOCKBySetTime	External	✓	onlyOwner
	extendLPLOCKBySeconds	External	✓	onlyOwner
	withdrawLiquidity	External	✓	onlyOwner
	lockInitialTokens	External	✓	-
	lockAdditionalTokens	External	✓	-
	getRemainingTokenLockTime	External		-
	getLockedTokenAmount	External		-

	extendTokenLockBySetTime	External	✓	-
	extendTokenLockBySeconds	External	✓	-
	withdrawTokens	External	✓	-

Contract Flow



Domain Info

Domain Name	react.ac
Registry Domain ID	fb81ee8d4b134a9bbaf029b296fac71f-DONUTS
Creation Date	2022-03-27T02:31:23Z
Updated Date	2022-04-04T06:11:22Z
Registry Expiry Date	2023-03-27T02:31:23Z
Registrar WHOIS Server	whois.namecheap.com
Registrar URL	https://www.namecheap.com/
Registrar	NameCheap, Inc.
Registrar IANA ID	1068

The domain has been created 15 days before the creation of the audit. It will expire in 12 months.

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

Summary

React Token is an interesting project that has a friendly and growing community. The Smart Contract analysis reported no compiler error or critical issues. There is also a limit of max 25% fees to buys, sells and direct transfers and 30% max fee limit to snipe fee.

Caution is advised

A great amount of code lines are not audited as they extend an unverified library and therefore are not visible or included in the scope of the audit.

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>