Audit Report

Equity

March 2022

Type	ERC20
Network	POLYGON
Address	0x91A5a34dA8520B005eD3697b6656b280F1D654D7
Audited by	© coinscope

Table of Contents

Contract Review

Contract Name	Equity
Compiler Version	v0.8.12+commit.f00d7308
Optimization	500 runs
Licence	
Explorer	https://polygonscan.com/token/0x91a5a34da8520b005ed3697b6656b280f1d654d7
Symbol	Equity
Decimals	18
Total Supply	1,000,000
Source	@openzeppelin/contracts/access/Ownable.sol @openzeppelin/contracts/token/ERC20/ERC20.sol @openzeppelin/contracts/token/ERC20/extensions/draft-ERC20Permit.sol @openzeppelin/contracts/token/ERC20/extensions/draft-IERC20Permit.sol @openzeppelin/contracts/token/ERC20/extensions/IERC20Metadata.sol @openzeppelin/contracts/token/ERC20/IERC20.sol @openzeppelin/contracts/utils/Context.sol @openzeppelin/contracts/utils/Counters.sol @openzeppelin/contracts/utils/cryptography/draft-EIP712.sol @openzeppelin/contracts/utils/cryptography/ECDSA.sol @openzeppelin/contracts/utils/Strings.sol @uniswap/v2-core/contracts/interfaces/IUniswapV2Factory.sol @uniswap/v2-periphery/contracts/interfaces/IUniswapV2Router01.sol @uniswap/v2-periphery/contracts/interfaces/IUniswapV2Router02.sol

	contracts/access/SharedOwnable.sol contracts/Equity.sol contracts/interfaces/IFeeable.sol contracts/interfaces/IReflectionTracker.sol contracts/interfaces/IReflective.sol contracts/libraries/IterableMappingUint256Uint256.sol contracts/token/ReflectiveToken.so

Audit Updates

Initial Audit	17th February 2022
Corrected	5th March 2022

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

Severity	Code	Description
●	L12	Using Variables before Declaration
●	L13	Divide before Multiply Operation

L12 - Using Variables before Declaration

Criticality	minor
Location	contracts/token/ReflectiveToken.sol#L455

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.

```
iterations
claims
lastProcessedIndex
gasUsed
```

Recommendation

The variables should be declared before any usage of them.

L13 - Divide before Multiply Operation

Criticality	minor
Location	contracts/token/ReflectiveToken.sol#L421,653

Description

Performing divisions before multiplications may cause loss of prediction.

```
number = (seed - ((seed / 100) * 100))
_swapAndSendReflections((_minimumTokenBalanceForSwapAndSendReflections / 100) *
_getRandomNumber())
```

Recommendation

The multiplications should be prior to the divisions.

Contract Functions

Contract	Type	Bases		
	Function Name	**Visibility**	**Mutability**	**Modifiers**
Ownable	Implementation	Context		
	<Constructor>	Public	✓	-
	owner	Public		-
	renounceOwnership	Public	✓	onlyOwner
	transferOwnership	Public	✓	onlyOwner
	_transferOwnership	Internal	✓	
ERC20	Implementation	Context, IERC20, IERC20Metadata		
	<Constructor>	Public	✓	-
	name	Public		-
	symbol	Public		-
	decimals	Public		-
	totalSupply	Public		-
	balanceOf	Public		-
	transfer	Public	✓	-
	allowance	Public		-
	approve	Public	✓	-
	transferFrom	Public	✓	-
	increaseAllowance	Public	✓	-
	decreaseAllowance	Public	✓	-
	_transfer	Internal	✓	
	_mint	Internal	✓	
	_burn	Internal	✓	
	_approve	Internal	✓	
	_beforeTokenTransfer	Internal	✓	
	_afterTokenTransfer	Internal	✓	

ERC20Permit	Implementation	ERC20, IERC20Permit, EIP712		
	<Constructor>	Public	✓	EIP712
	permit	Public	✓	-
	nonces	Public		-
	DOMAIN_SEPARATOR	External		-
	_useNonce	Internal	✓	
IERC20Permit	Interface			
	permit	External	✓	-
	nonces	External		-
	DOMAIN_SEPARATOR	External		-
IERC20Metadata	Interface	IERC20		
	name	External		-
	symbol	External		-
	decimals	External		-
IERC20	Interface			
	totalSupply	External		-
	balanceOf	External		-
	transfer	External	✓	-
	allowance	External		-
	approve	External	✓	-
	transferFrom	External	✓	-
Context	Implementation			
	_msgSender	Internal		
	_msgData	Internal		
Counters	Library			
	current	Internal		
	increment	Internal	✓	
	decrement	Internal	✓	

	reset	Internal	✓	
EIP712	Implementation			
	<Constructor>	Public	✓	-
	_domainSeparatorV4	Internal		
	_buildDomainSeparator	Private		
	_hashTypedDataV4	Internal		
ECDSA	Library			
	_throwError	Private		
	tryRecover	Internal		
	recover	Internal		
	tryRecover	Internal		
	recover	Internal		
	tryRecover	Internal		
	recover	Internal		
	toEthSignedMessageHash	Internal		
	toEthSignedMessageHash	Internal		
	toTypedDataHash	Internal		
Strings	Library			
	toString	Internal		
	toHexString	Internal		
	toHexString	Internal		
IUniswapV2Factory	Interface			
	feeTo	External		-
	feeToSetter	External		-
	getPair	External		-
	allPairs	External		-
	allPairsLength	External		-
	createPair	External	✓	-
	setFeeTo	External	✓	-
	setFeeToSetter	External	✓	-

IUniswapV2Router01	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		-
IUniswapV2Router02	Interface	IUniswapV2Router01		
	removeLiquidityETHSupportingFeeOnTransferTokens	External	✓	-
	removeLiquidityETHWithPermitSupportingFeeOnTransferTokens	External	✓	-
	swapExactTokensForTokensSupportingFeeOnTransferTokens	External	✓	-
	swapExactETHForTokensSupportingFeeOnTransferTokens	External	Payable	-
	swapExactTokensForETHSupportingFeeOnTransferTokens	External	✓	-
SharedOwnable	Implementation	Ownable		
	<Constructor>	Public	✓	Ownable

	getCreator	External		-
	isSharedOwner	External		-
	setSharedOwner	Internal	✓	onlySharedOwners
	_setSharedOwner	Private	✓	
Equity	Implementation	ReflectiveToken		
	<Constructor>	Public	✓	ReflectiveToken
IFeeable	Interface			
	getMaxFee	External		-
	getBaseFee	External		-
	getCustomFeeOf	External		-
	setCustomFeeOf	External	✓	-
IReflectionTracker	Interface			
	isBoundTo	External		-
	bindTo	External	✓	-
	getBalanceOf	External		-
	refreshBalanceOf	External	✓	-
	refreshBalance	External	✓	-
	getUniswapV2Router02Address	External		-
	setUniswapV2Router02Address	External	✓	-
	getDefaultReflectionTokenAddress	External		-
	setDefaultReflectionTokenAddress	External	✓	-
	getClaimCooldown	External		-
	setClaimCooldown	External	✓	-
	getMinimumTokenBalanceForReflections	External		-
	setMinimumTokenBalanceForReflections	External	✓	-
	getExcludedReflectionStateOfBNB	External		-
	setExcludedReflectionStateOfBNB	External	✓	-
	getExcludedReflectionTokenStateOf	External		-

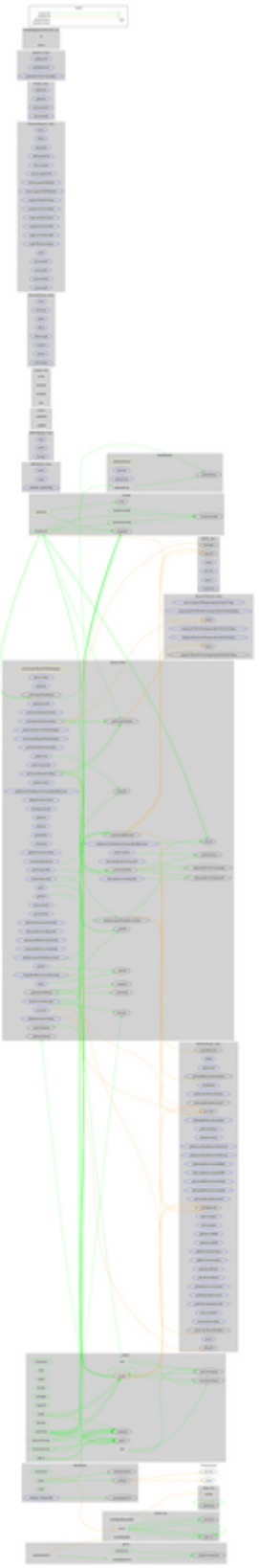
	setExcludedReflectionTokenStateOf	External	✓	-
	getExcludedFromReflectionsOf	External		-
	setExcludedFromReflectionsOf	External	✓	-
	getProcessingGas	External		-
	setProcessingGas	External	✓	-
	getReflectionInBNB	External		-
	setReflectionInBNB	External	✓	-
	getReflectionTokenAddress	External		-
	setReflectionTokenAddress	External	✓	-
	getNumberOfHolders	External		-
	getLastProcessedIndex	External		-
	getTotalReflectionsTransferred	External		-
	getWithdrawnReflectionsOf	External		-
	getWithdrawableReflectionsOf	External		-
	getAccountInfoOf	External		-
	getAccountInfoAtIndex	External		-
	transferReflections	External	Payable	-
	transferReflections	External	✓	-
	process	External	✓	-
	processAll	External	✓	-
	processAll	External	✓	-
	processAll	External	✓	-
IReflective	Interface	IFeeable		
	getBalanceOf	External		-
	getFeeBalancesOf	External		-
	getTokenPairOtherTokenAddress	External		-
IterableMappingUint256Uint256	Library			
	set	Internal	✓	
	remove	Internal	✓	
ReflectiveToken	Implementation	ERC20Permit, IReflective,		

		SharedOwnable		
	<Constructor>	Public	✓	ERC20Permit ERC20
	<Receive Ether>	External	Payable	-
	getMaxFee	External		-
	getBalanceOf	External		-
	getFeeBalancesOf	External		-
	getUniswapV2Router02Address	External		-
	setUniswapV2Router02Address	External	✓	onlySharedOwners
	getUniswapV2Router02WithFeeSupport	External		-
	setUniswapV2Router02WithFeeSupport	External	✓	onlySharedOwners
	getTokenPairOtherTokenAddress	External		-
	setTokenPairOtherTokenAddress	External	✓	onlySharedOwners
	getIsUniswapV2Pair	External		-
	setIsUniswapV2Pair	External	✓	onlySharedOwners
	_setIsUniswapV2Pair	Private	✓	
	getIsFeeCollector	External		-
	setIsFeeCollector	External	✓	onlySharedOwners
	_setIsFeeCollector	Private	✓	
	getMinimumTokenBalanceForSwapAndSendReflections	External		-
	setMinimumTokenBalanceForSwapAndSendReflections	External	✓	onlySharedOwners
	isRegularTransferAllowed	External		-
	allowRegularTransfer	External	✓	onlySharedOwners
	getBaseFee	External		-
	setBaseFee	External	✓	onlySharedOwners
	getDefaultFee	External		-
	setDefaultFee	External	✓	onlySharedOwners
	getReflectionTrackerAddress	External		-

	setReflectionTrackerAddress	External	✓	onlySharedOwners
	getFee	External		-
	getFeeOf	External		-
	setFee	External	✓	-
	setFeeOf	External	✓	onlySharedOwners
	getCustomFeeOf	External		-
	setCustomFeeOf	External	✓	onlyUniswapV2Router02WithFeeSupport
	getExcludedFromFeeCollectionOf	External		-
	setExcludedFromFeeCollectionOf	External	✓	onlySharedOwners
	getExcludedFromFeeBalancesOf	External		-
	setExcludedFromFeeBalancesOf	External	✓	onlySharedOwners
	getAutomatedReflectionTrackerCalls	External		-
	setAutomatedReflectionTrackerCalls	External	✓	onlySharedOwners
	swapAndSendReflections	External	✓	onlySharedOwners
	processAll	External	✓	onlySharedOwners
	swapAndSendReflectionsAndProcessAll	External	✓	onlySharedOwners
	updateDeveloperWalletReflectiveShares	External	✓	onlySharedOwners
	transfer	Public	✓	-
	transferWithExactFee	External	✓	-
	transferFrom	Public	✓	-
	transferFromWithExactFee	External	✓	-
	_transfer	Private	✓	
	_getSuitableFeeBalances	Private		
	_insertionSort	Private		
	_uniqueSort	Private		
	_applyFeeBalances	Private	✓	
	_getOrCreateTokenPair	Private	✓	
	_setDeveloperWalletOptions	Private	✓	

	_updateDeveloperWalletReflectiveShares	Private	✓	
	_getFeeOf	Private		
	_setFeeOf	Private	✓	
	_setExcludedFromFeeCollectionOf	Private	✓	
	_setExcludedFromFeeBalancesOf	Private	✓	
	_swapAndSendReflections	Private	✓	
	_getRandomNumber	Private		

Contract Flow



Summary

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.

The contract contains a built-in tokens lock functionality for the dev wallets. That means that the amount of the dev wallets cannot be transferred.

The contract also contains a reflection distribution mechanism. When the accumulated amount is more than a specific threshold, the contract swaps a pseudo-random percentage of that amount in order to share it as a distribution.

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