Cyberscope

Audit Report

RBX Token

May 2022

0xace3574b8b054e074473a9bd002e5dc6dd3dff1b (BSC)
0x8254e26e453eb5abd29b3c37ac9e8da32e5d3299 (ETH)
0x94960952876e3ED6A7760B198354fCc5319A406a (AVAX)

Audited by © cyberscope

Table of Contents

Contract Review

AVAX

Contract Name	RBX
Compiler Version	v0.8.12+commit.f00d7308
Optimization	200 runs
Licence	
Explorer	https://snowtrace.io/token/0x94960952876e3ED6A7760B198354fCc5319A406a
Symbol	RBX
Decimals	18
Total Supply	100,000,000

BSC

Contract Name	RBX
Compiler Version	v0.8.7+commit.e28d00a7
Optimization	200 runs
Licence	
Explorer	https://bscscan.com/token/0xace3574b8b054e074473a9bd002e5dc6dd3dff1b
Symbol	RBX

Decimals	18
Total Supply	100,000,000

ETH

Contract Name	RBX
Compiler Version	v0.8.7+commit.e28d00a7
Optimization	200 runs
Licence	
Explorer	https://etherscan.io/token/0x8254e26e453eb5abd29b3c37ac9e8da32e5d3299
Symbol	RBX
Decimals	18
Total Supply	100,000,000

Audit Updates

Initial Audit	20th May 2022
Corrected	

Source Files

Filename	SHA256
@openzeppelin/contracts/access/AccessControl.sol	6815a22e5b2ef7e0e813961ad06afac5c9d6e7cdced9165f2cedbf11032044bd
@openzeppelin/contracts/access/IAccessControl.sol	81a867af9f5344a0efffcfb2970db5354c8684d4d50139db1524321fbd60979b
@openzeppelin/contracts/token/ERC20/ERC20.sol	80e33e340442acecc4bd995b4ead9b51adc4231c8213357fca18996b945f850b
@openzeppelin/contracts/token/ERC20/extensions/draft-ERC20Permit.sol	4caeef3716ac6c9bed65567dbc61169bc9740824e8791bfced2775dfd5a4f06b
@openzeppelin/contracts/token/ERC20/extensions/draft-IERC20Permit.sol	0d1854245c9e46c351d403ccc3e5979582e8451a3c729dee7d0c0cddf3166cd8
@openzeppelin/contracts/token/ERC20/extensions/ERC20Burnable.sol	600052c7df2ee2e969592df597ae5f78aad5822c8bee181e58b2713321efb888
@openzeppelin/contracts/token/ERC20/extensions/ERC20Snapshot.sol	cd072ee3d83f3758b507c3ea7c39b83311043247807a78a2832099a6c38440c4
@openzeppelin/contracts/token/ERC20/extensions/ERC20Votes.sol	09852784cfc3ed955e4d9129231fedd23c0eaad720092821bf622f41b5376ae7

@openzeppelin/contracts/token/ERC20/extensions/IERC20Metadata.sol	4e2ce556a0419415ec3b01a0fa0322c20d6d53de5a05728c068e90d5684486c1
@openzeppelin/contracts/token/ERC20/IERC20.sol	b2565dec975f684ef0edfa505e212d0d0b602e1311afab782ea06ea8d3f49bb6
@openzeppelin/contracts/token/ERC20/utils/SafeERC20.sol	729097c056b8bf1dd93ac16831380ce4ff54703d75983f57354240cc8be2edec
@openzeppelin/contracts/utils/Address.sol	1370d859f5c6d11025afb409d1b724279f663c4cf4bc4d2ba057290bdcf45a66
@openzeppelin/contracts/utils/Arrays.sol	28c1c0c9e6f645643973e00fab4473d098e0d0038002deaeb67c98ea8e72e660
@openzeppelin/contracts/utils/Context.sol	5828bf38f9376b659a8edbbe2df0d06b29a09e37ecd470465dda2bbcb612c85d
@openzeppelin/contracts/utils/Counters.sol	e664dd2b610b11a9a060e109027a2acdc8c8555de0b99b6071fddf719a27c8ac
@openzeppelin/contracts/utils/cryptography/draft-EIP712.sol	60c2fd58640750c2f47472c5221cd99308260214ef1f2926ba3bc9daf0d3a2b9
@openzeppelin/contracts/utils/cryptography/ECDSA.sol	bff8e3c973e5c6eb0fc6f5205531328bb173fffd7b2e9920977abea924363bb2
@openzeppelin/contracts/utils/introspection/ERC165.sol	381b0589da0e1a32242d7314905d2cc6edd8dce8193ddb6bfacc5b685e311422

@openzeppelin/contracts/utils/introspection/IERC165.sol	072805b211a653c333b232a3199b9e65fa7b82fc7a40ee5a3bc8a2dadd1cba01
@openzeppelin/contracts/utils/math/Math.sol	b1417f64b6fba54e2b715f2228c4dde4065e742245e6bf7c68f39c5f42af043b
@openzeppelin/contracts/utils/math/SafeCast.sol	8dec6dd63908459be4b909861eb3a00b31431575f8169c1f0cbb6519af754bfe
@openzeppelin/contracts/utils/Strings.sol	3b2b0d75c7e5688950d3b6e63e46473054395dad6e390431f73febb2199913c5
contracts/libs/uni.sol	483aa544ef8a5afe8e0f5a253d894022c96d1b846be067e4b04f7a3be123198f
contracts/RBX.sol	2cfa0f7505225ebb13e4e16a2c5cd5b726df411e5dea3c4d690e4fa4c325029b

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

ST - Stop Transactions

Criticality	medium
Location	contract.sol#L185

Description

The contract owner has the authority to stop transactions for all users excluding the owner. The owner may take advantage of it by enabling the `swapInProgress` boolean.

```
if(swapInProgress)
    require(_whiteListed[sender], "Token swap still in progress!");
```

Recommendation

The team should carefully manage the private keys of the owner's account. We strongly recommend a powerful security mechanism that will prevent a single user from accessing the contract admin functions. That risk can be prevented by temporarily locking the contract or renouncing ownership.

BC - Blacklisted Contracts

Criticality	medium
Location	contract.sol#L188

Description

The contract owner has the authority to stop contracts from transactions. The owner may take advantage of it by calling the `blacklistAddress` function.

```
require(!_blacklisted[sender] && !_blacklisted[recipient], "Blacklisted address given");
```

Recommendation

The team should carefully manage the private keys of the owner’s account. We strongly recommend a powerful security mechanism that will prevent a single user from accessing the contract admin functions. That risk can be prevented by temporarily locking the contract or renouncing ownership.

Contract Diagnostics

Critical Medium Minor

Severity	Code	Description
	L02	State Variables could be Declared Constant
	L04	Conformance to Solidity Naming Conventions
	L07	Missing Events Arithmetic

L02 - State Variables could be Declared Constant

Criticality	minor
Location	contracts/RBX.sol#L131

Description

Constant state variables should be declared constant to save gas.

```
fundingFee
```

Recommendation

Add the constant attribute to state variables that never change.

L04 - Conformance to Solidity Naming Conventions

Criticality	minor
Location	contracts/RBX.sol#L258,272,282,292,306,129

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.

```
_routerPairs
_swapInProgress
_wallet
_setting
_tokenThreshold
_addPair
```

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	contracts/RBX.sol#L272

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.

```
tokenThreshold = _tokenThreshold
```

Recommendation

Emit an event for critical parameter changes.

Contract Functions

Contract	Type	Bases		
	Function Name	**Visibility**	**Mutability**	**Modifiers**
AccessControl	Implementation	Context, IAccessControl, ERC165		
	supportsInterface	Public		-
	hasRole	Public		-
	_checkRole	Internal		
	getRoleAdmin	Public		-
	grantRole	Public	✓	onlyRole
	revokeRole	Public	✓	onlyRole
	renounceRole	Public	✓	-
	_setupRole	Internal	✓	
	_setRoleAdmin	Internal	✓	
	_grantRole	Private	✓	
	_revokeRole	Private	✓	
IAccessControl	Interface			
	hasRole	External		-
	getRoleAdmin	External		-
	grantRole	External	✓	-
	revokeRole	External	✓	-
	renounceRole	External	✓	-
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		-
ERC20Burnable	Implementation	Context, ERC20		
	burn	Public	✓	-
	burnFrom	Public	✓	-
ERC20Snapshot	Implementation	ERC20		

	_snapshot	Internal	✓	
	_getCurrentSnapshotId	Internal		
	balanceOfAt	Public		-
	totalSupplyAt	Public		-
	_beforeTokenTransfer	Internal	✓	
	_valueAt	Private		
	_updateAccountSnapshot	Private	✓	
	_updateTotalSupplySnapshot	Private	✓	
	_updateSnapshot	Private	✓	
	_lastSnapshotId	Private		
ERC20Votes	Implementation	ERC20Permit		
	checkpoints	Public		-
	numCheckpoints	Public		-
	delegates	Public		-
	getVotes	Public		-
	getPastVotes	Public		-
	getPastTotalSupply	Public		-
	_checkpointsLookup	Private		
	delegate	Public	✓	-
	delegateBySig	Public	✓	-
	_maxSupply	Internal		
	_mint	Internal	✓	
	_burn	Internal	✓	
	_afterTokenTransfer	Internal	✓	
	_delegate	Internal	✓	
	_moveVotingPower	Private	✓	
	_writeCheckpoint	Private	✓	
	_add	Private		
	_subtract	Private		
IERC20Metadata	Interface	IERC20		
	name	External		-
	symbol	External		-

	decimals	External		-
IERC20	Interface			
	totalSupply	External		-
	balanceOf	External		-
	transfer	External	✓	-
	allowance	External		-
	approve	External	✓	-
	transferFrom	External	✓	-
SafeERC20	Library			
	safeTransfer	Internal	✓	
	safeTransferFrom	Internal	✓	
	safeApprove	Internal	✓	
	safeIncreaseAllowance	Internal	✓	
	safeDecreaseAllowance	Internal	✓	
	_callOptionalReturn	Private	✓	
Address	Library			
	isContract	Internal		
	sendValue	Internal	✓	
	functionCall	Internal	✓	
	functionCall	Internal	✓	
	functionCallWithValue	Internal	✓	
	functionCallWithValue	Internal	✓	
	functionStaticCall	Internal		
	functionStaticCall	Internal		
	functionDelegateCall	Internal	✓	
	functionDelegateCall	Internal	✓	
	verifyCallResult	Internal		
Arrays	Library			
	findUpperBound	Internal		
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		
	toTypedDataHash	Internal		
ERC165	Implementation	IERC165		
	supportsInterface	Public		-
IERC165	Interface			
	supportsInterface	External		-
Math	Library			
	max	Internal		
	min	Internal		

	average	Internal		
	ceilDiv	Internal		
SafeCast	Library			
	toUint224	Internal		
	toUint128	Internal		
	toUint96	Internal		
	toUint64	Internal		
	toUint32	Internal		
	toUint16	Internal		
	toUint8	Internal		
	toUint256	Internal		
	toInt128	Internal		
	toInt64	Internal		
	toInt32	Internal		
	toInt16	Internal		
	toInt8	Internal		
	toInt256	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	✓	-
IUniswapV2Pai	Interface			

r				
	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	✓	-
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	✓	-
RBX	Implementation	ERC20, ERC20Burnable, ERC20Snapshot, AccessControl, ERC20Permit, ERC20Votes		
	<Constructor>	Public	✓	ERC20 ERC20Permit
	snapshot	Public	✓	-

	_beforeTokenTransfer	Internal	✓	
	whitelistAddress	Public	✓	-
	_transfer	Internal	✓	
	swapTokensByPair	Private	✓	
	_addPair	Public	✓	-
	setTokenThreshold	External	✓	onlyRole
	setFundingSells	External	✓	onlyRole
	setFundingWallet	External	✓	onlyRole
	blacklistAddress	External	✓	onlyRole
	setSwapInProgress	External	✓	onlyRole
	_afterTokenTransfer	Internal	✓	
	_burn	Internal	✓	
	_mint	Internal	✓	
	rescueTokens	Public	✓	-
	rescueTokensSafe	Public	✓	-
	rescueEth	Public	✓	-

Contract Flow

Summary

There are some functions that can be abused by the owner like stopping transactions and blacklisting addresses. A multi-wallet signing pattern will provide security against potential hacks. Temporarily locking the contract or renouncing ownership will eliminate all the contract threats.

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