



Cyberscope

# Audit Report

## **PoshCoin**

October 2022

Type       BEP20

Network    BSC

Address    0xfcb696088a0f9dAb0715F03AD068aeBDFB6A3286

Audited by © cyberscope

# Table of Contents

<b>Table of Contents</b>	<b>1</b>
<b>Contract Review</b>	<b>3</b>
<b>Audit Updates</b>	<b>3</b>
<b>Source Files</b>	<b>4</b>
<b>Contract Analysis</b>	<b>6</b>
<b>ST - Stops Transactions</b>	<b>7</b>
Description	7
Recommendation	7
<b>BC - Blacklists Addresses</b>	<b>8</b>
Description	8
Recommendation	8
<b>Contract Diagnostics</b>	<b>9</b>
<b>L02 - State Variables could be Declared Constant</b>	<b>10</b>
Description	10
Recommendation	10
<b>L04 - Conformance to Solidity Naming Conventions</b>	<b>11</b>
Description	11
Recommendation	11
<b>L07 - Missing Events Arithmetic</b>	<b>12</b>
Description	12
Recommendation	12
<b>L15 - Local Scope Variable Shadowing</b>	<b>13</b>
Description	13
Recommendation	13
<b>Contract Functions</b>	<b>14</b>
<b>Contract Flow</b>	<b>18</b>

<b>Domain Info</b>	<b>19</b>
<b>Summary</b>	<b>20</b>
<b>Disclaimer</b>	<b>21</b>
<b>About Cyberscope</b>	<b>22</b>

## Contract Review

<b>Contract Name</b>	PoshCoin
<b>Compiler Version</b>	v0.8.17+commit.8df45f5f
<b>Optimization</b>	200 runs
<b>Explorer</b>	<a href="https://bscscan.com/token/0xfcb696088a0f9dAb0715F03AD068aeBDFB6A3286">https://bscscan.com/token/0xfcb696088a0f9dAb0715F03AD068aeBDFB6A3286</a>
<b>Symbol</b>	PSCN
<b>Decimals</b>	18
<b>Total Supply</b>	1,000,000,000
<b>Domain</b>	<a href="https://poshcoin.io">https://poshcoin.io</a>

## Audit Updates

<b>Initial Audit</b>	9th September 2022 <a href="https://github.com/cyberscope-io/audits/blob/main/pscn/v1/audit.pdf">https://github.com/cyberscope-io/audits/blob/main/pscn/v1/audit.pdf</a>
<b>Corrected</b>	20th October 2022

## Source Files

Filename	SHA256
@openzeppelin/contracts/access/AccessControl.sol	0b280a0fe505b5b8bcb700e0b1f6242acf73e0b509372ef3acc46db051512e32
@openzeppelin/contracts/access/IAccessControl.sol	d03c1257f2094da6c86efa7aa09c1c07ebd33dd31046480c5097bc2542140e45
@openzeppelin/contracts/access/Ownable.sol	75e3c97011e75627ffb36f4a2799a4e887e1a3e27ed427490e82d7b6f51cc5c9
@openzeppelin/contracts/security/Pausable.sol	5b6abc290190f46b9941c674594eee083a3fe6b92d1828d0cfefacc94d1cac9a
@openzeppelin/contracts/token/ERC20/ERC20.sol	f7831910f2ed6d32acff6431e5998baf50e4a00121303b27e974aab0ec637d79
@openzeppelin/contracts/token/ERC20/extensions/IERC20Metadata.sol	af5c8a77965cc82c33b7ff844deb9826166689e55dc037a7f2f790d057811990
@openzeppelin/contracts/token/ERC20/IERC20.sol	c2b06bb4572bb4f84bfc5477dad0fcc497cb66c3a1bd53480e68bedc2e154a6
@openzeppelin/contracts/utils/Context.sol	1458c260d010a08e4c20a4a517882259a23a4baa0b5bd9add9fb6d6a1549814a

<b>@openzeppelin/contracts/utils/introspection/ERC165.sol</b>	8806a632d7b656cadb8133ff8f2acae4405b3a64d8709d93b0fa6a216a8a6154
<b>@openzeppelin/contracts/utils/introspection/IERC165.sol</b>	701e025d13ec6be09ae892eb029cd83b3064325801d73654847a5fb11c58b1e5
<b>@openzeppelin/contracts/utils/math/SafeMath.sol</b>	15941f3904992a62ed117e93d9e2d5c4c22bd09a7ff97fd5f49273cf09703ac
<b>@openzeppelin/contracts/utils/Strings.sol</b>	8597c62818dcbc6cf85c21179b90b714fb4f70a4347ca2eed23e88c87b08b8a1
<b>contracts/PoshCoin.sol</b>	44c73875580c1839bd4d1477949da7311e15ad4365ef347b1137e4d88a696357

# Contract Analysis

● Critical ● Medium ● Minor / Informative ● Pass

Severity	Code	Description	Status
●	ST	Stops Transactions	Unresolved
●	OCTD	Transfers Contract's Tokens	Passed
●	OTUT	Transfers User's Tokens	Passed
●	ELFM	Exceeds Fees Limit	Passed
●	ULTW	Transfers Liquidity to Team Wallet	Passed
●	MT	Mints Tokens	Passed
●	BT	Burns Tokens	Passed
●	BC	Blacklists Addresses	Unresolved

## ST - Stops Transactions

<b>Criticality</b>	minor / informative
<b>Location</b>	contract.sol#L128
<b>Status</b>	Unresolved

### Description

The contract owner has the authority to stop the transactions for all users excluding the owner. The owner may take advantage of it by calling the `pause` method.

```
function _transfer(  
    address from,  
    address to,  
    uint256 amount  
) internal override whenNotPaused {
```

### 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 - Blacklists Addresses

Criticality	medium
Location	contract.sol#L51
Status	Unresolved

### Description

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

```
function blacklistAddress(address account, bool value) external onlyOwner {  
    require(account != owner(), "Shouldn't be owner address");  
    _isBlacklisted[account] = value;  
}
```

### 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 / Informative

Severity	Code	Description	Status
●	L02	State Variables could be Declared Constant	Unresolved
●	L04	Conformance to Solidity Naming Conventions	Unresolved
●	L07	Missing Events Arithmetic	Unresolved
●	L15	Local Scope Variable Shadowing	Unresolved

## L02 - State Variables could be Declared Constant

<b>Criticality</b>	minor / informative
<b>Location</b>	PoshCoin.sol#L18
<b>Status</b>	Unresolved

### Description

Constant state variables should be declared constant to save gas.

```
decimal
```

### Recommendation

Add the constant attribute to state variables that never change.

## L04 - Conformance to Solidity Naming Conventions

<b>Criticality</b>	minor / informative
<b>Location</b>	PoshCoin.sol#L28,112,117
<b>Status</b>	Unresolved

### 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.

```
_isBlacklisted  
_taxFee  
_marketingWalletAddress
```

### Recommendation

Follow the Solidity naming convention.

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

## L07 - Missing Events Arithmetic

<b>Criticality</b>	minor / informative
<b>Location</b>	PoshCoin.sol#L63,56,112
<b>Status</b>	Unresolved

### 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.

```
maxAmountHold = newAmount  
maxTxAmount = newAmount  
taxFee = _taxFee
```

### Recommendation

Emit an event for critical parameter changes.

## L15 - Local Scope Variable Shadowing

<b>Criticality</b>	minor / informative
<b>Location</b>	PoshCoin.sol#L41,39,40
<b>Status</b>	Unresolved

### Description

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

```
totalSupply  
name  
symbol
```

### Recommendation

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

# Contract Functions

Contract	Type	Bases		
	Function Name	Visibility	Mutability	Modifiers
<b>AccessControl</b>	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	Internal	✓	
	_revokeRole	Internal	✓	
<b>IAccessControl</b>	Interface			
	hasRole	External		-
	getRoleAdmin	External		-
	grantRole	External	✓	-
	revokeRole	External	✓	-
	renounceRole	External	✓	-
<b>Ownable</b>	Implementation	Context		
	<Constructor>	Public	✓	-
	owner	Public		-
	renounceOwnership	Public	✓	onlyOwner
	transferOwnership	Public	✓	onlyOwner
	_transferOwnership	Internal	✓	

<b>Pausable</b>	Implementation	Context		
	<Constructor>	Public	✓	-
	paused	Public		-
	_pause	Internal	✓	whenNotPaused
	_unpause	Internal	✓	whenPaused
<b>ERC20</b>	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	✓	
	_spendAllowance	Internal	✓	
	_beforeTokenTransfer	Internal	✓	
	_afterTokenTransfer	Internal	✓	
<b>IERC20Metadata</b>	Interface	IERC20		
	name	External		-
	symbol	External		-



	decimals	External		-
<b>IERC20</b>	Interface			
	totalSupply	External		-
	balanceOf	External		-
	transfer	External	✓	-
	allowance	External		-
	approve	External	✓	-
	transferFrom	External	✓	-
<b>Context</b>	Implementation			
	_msgSender	Internal		
	_msgData	Internal		
<b>ERC165</b>	Implementation	IERC165		
	supportsInterface	Public		-
<b>IERC165</b>	Interface			
	supportsInterface	External		-
<b>SafeMath</b>	Library			
	tryAdd	Internal		
	trySub	Internal		
	tryMul	Internal		
	tryDiv	Internal		
	tryMod	Internal		
	add	Internal		
	sub	Internal		
	mul	Internal		
	div	Internal		
	mod	Internal		
	sub	Internal		
	div	Internal		
	mod	Internal		

<b>Strings</b>	Library			
	toString	Internal		
	toHexString	Internal		
	toHexString	Internal		
<b>PoshCoin</b>	Implementation	ERC20, Ownable, AccessCont rol, Pausable		
	<Constructor>	Public	✓	ERC20
	blacklistAddress	External	✓	onlyOwner
	setMaxTxAmount	External	✓	onlyOwner
	setMaxAmountHold	External	✓	onlyOwner
	decimals	Public		-
	excludeFromFees	Public	✓	onlyOwner
	excludeMultipleAccountsFromFees	Public	✓	onlyOwner
	isExcludedFromFees	Public		-
	whitelistWallet	Public	✓	onlyOwner
	isWhiteListedWallet	Public		-
	setTaxFee	External	✓	onlyOwner
	setMarketWalletAddress	External	✓	onlyOwner
	_transfer	Internal	✓	whenNotPaus ed
	pause	Public	✓	onlyOwner
	unpause	Public	✓	onlyOwner
	_beforeTokenTransfer	Internal	✓	whenNotPaus ed

# Contract Flow



## Domain Info

<b>Domain Name</b>	poshcoin.io
<b>Registry Domain ID</b>	03ffff9fe6c54b03b1a0944fb8ac5f59-DONUTS
<b>Creation Date</b>	2022-08-04T15:47:01Z
<b>Updated Date</b>	2022-08-09T15:47:14Z
<b>Registry Expiry Date</b>	2023-08-04T15:47:01Z
<b>Registrar WHOIS Server</b>	whois.godaddy.com/
<b>Registrar URL</b>	<a href="http://www.godaddy.com/domains/search.aspx?ci=8990">http://www.godaddy.com/domains/search.aspx?ci=8990</a>
<b>Registrar</b>	GoDaddy.com, LLC
<b>Registrar IANA ID</b>	146

The domain was created 3 months before the creation of the audit. It will expire in 10 months.

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

## 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. There is also a limit of max 18% fee.

## 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 provide all the essential tools to assist users draw their own conclusions.



The Cyberscope team

<https://www.cyberscope.io>