Audit Report

Pope Inu

January 2022

Type   BEP20

Network   BSC

Address   0xac9cc719532aab9d6c16a7c8739cb4e4b2ca45f9

Audited by   © coinscope

Table of Contents

Contract Review

Contract Name	PopeInuCoin
Compiler Version	v0.7.6+commit.7338295f
Optimization	200 runs
Licence	MIT
Explorer	https://bscscan.com/token/0xac9cc719532aab9d6c16a7c8739cb4e4b2ca45f9
Symbol	POPE
Decimals	18
Total Supply	10,000,000,000,000
Source	contract.sol
Domain	popeinu.com

Audit Updates

Initial Audit	5th January 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

OCTD - Owner Contract Tokens Drain

Criticality	medium
Location	contract.sol#L757,L784

Description

The contract owner has the authority to claim tokens from the contract. The owner may take advantage of it by calling the `endCrowdsale` and `endAirDrop` function. There is no check for performing these events only once, so the contract owner may call these functions multiple times.

```
function endCrowdsale() public onlyOwner {
    crowdSaleEnabled = false;
    _burn(address(this), (PRESALE_TOKEN.sub(PRESALE_TOKEN_SOLD)).div(2));
    _transfer(address(this), owner,
(PRESALE_TOKEN.sub(PRESALE_TOKEN_SOLD)).div(2));

    emit CrowdSaleEnd(PRESALE_TOKEN, RATE);
}
```

```
function endAirDrop() public onlyOwner {
    airdropEnabled = false;
    _transfer(address(this), owner, AIRDROP_TOKEN.sub(totalAirdrop));
}
```

Recommendation

There should be a logic in the contract that allows these events to be accomplished once, in a specific timespan. Similar logic is applied to the open trading period.

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
●	L01	Public Function could be Declared External
●	L02	State Variables could be Declared Constant
●	L04	Conformance to Solidity Naming Conventions
●	L09	Dead Code Elimination
●	L11	Unnecessary Boolean equality

L01 - Public Function could be Declared External

Criticality	minor
Location	contract.sol#L784,L779,L774 and 18 more

Description

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

```
endCrowdsale
pauseCrowdsale
startCrowdsale
...
```

Recommendation

Use the external attribute for functions never called from the contract

L02 - State Variables could be Declared Constant

Criticality	minor
Location	contract.sol#L765,L678,L766 and 2 more

Description

Constant state variables should be declared constant to save gas.

```
RATE
PRESALE_TOKEN
MAX_PURCHASE
...
```

Recommendation

Add the constant attribute to state variables that never change.

L04 - Conformance to Solidity Naming Conventions

Criticality	minor
Location	contract.sol#L766,L765,L764 and 5 more

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.

```
MAX_PURCHASE
RATE
PRESALE_TOKEN_SOLD
...
```

Recommendation

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

L09 - Dead Code Elimination

Criticality	minor
Location	contract.sol#L57,L67,L92 and 7 more

Description

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

```
trySub
tryMul
tryMod
...
```

Recommendation

Remove unused functions.

L11 - Unnecessary Boolean equality

Criticality	minor
Location	contract.sol#L736,L697

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.

```
require(bool,string)(airdropReceivedList[msg.sender] == false,You already
received airdrop)
require(bool,string)(ableToTransferBeforeLaunch[from] == true,You are not
allowed to transfer before launching)
```

Recommendation

Remove the equality to the boolean constant.

Contract Functions

Contract	Type	Bases			
	Function Name	Visibility	Mutability	Modifiers	
Context	Implementation				
	_msgSender	Internal			
	_msgData	Internal			
SafeMath	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			
IERC20	Interface				
	totalSupply	External		-	
	balanceOf	External		-	
	transfer	External	✓	-	
	allowance	External		-	
	approve	External	✓	-	
	transferFrom	External	✓	-	

ERC20	Implementation	Context, IERC20		
	<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	✓	
	_setupDecimals	Internal	✓	
	_beforeTokenTransfer	Internal	✓	
ERC20Burnable	Implementation	Context, ERC20		
	burn	Public	✓	-
	burnFrom	Public	✓	-
Ownable	Implementation			
	<Constructor>	Public	✓	-
	transferOwnership	Public	✓	onlyOwner
PopeInuCoin	Implementation	ERC20Burnable, Ownable		
	<Constructor>	Public	✓	ERC20
	setAbleToTransferBeforeLaunch	Public	✓	onlyOwner
	launch	Public	✓	onlyOwner
	_transfer	Internal	✓	

	<Receive Ether>	External	Payable	-
	enablePurchaseCounter	Public	✓	onlyOwner
	disablePurchaseCounter	Public	✓	onlyOwner
	airdrop	Public	Payable	-
	startAirDrop	Public	✓	onlyOwner
	stopAirDrop	Public	✓	onlyOwner
	endAirDrop	Public	✓	onlyOwner
	startCrowdsale	Public	✓	onlyOwner
	pauseCrowdsale	Public	✓	onlyOwner
	endCrowdsale	Public	✓	onlyOwner
	buyToken	Public	Payable	-

Contract Flow

Domain Info

Domain Name	popeinu.com
Registry Domain ID	2664266424_DOMAIN_COM-VRSN
Creation Date	2021-12-27T15:01:28.00Z
Updated Date	0001-01-01T00:00:00.00Z
Registry Expiry Date	
Registrar WHOIS Server	whois.namecheap.com
Registrar URL	http://www.namecheap.com
Registrar	NAMECHEAP INC
Registrar IANA ID	1068

The domain has been created 9 days before the creation of the audit.

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

Summary

Pope Inu is aiming to use the proceeds from the sale to back sustainable NFT projects that will in turn support charities around the world. The token has a friendly and growing community. The contract analysis reported no compiler errors and only one medium threat issue. The contract owner could accidentally call some methods that are moving tokens from the contract to the owner's balance. 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.

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