



Cyberscope

# Audit Report

## Hope Doge

February 2022

Type      BEP20

Network    BSC

Address    0xCB7C3D1Dd299BE73BC35B03F39e4bda9f0338Ff1

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>Contract Analysis</b>	<b>4</b>
<b>ULTW - Unlimited Liquidity to Team Wallet</b>	<b>5</b>
<b>Description</b>	<b>5</b>
<b>Recommendation</b>	<b>6</b>
<b>Contract Diagnostics</b>	<b>7</b>
<b>FSA - Fixed Swap Address</b>	<b>8</b>
<b>Description</b>	<b>8</b>
<b>Recommendation</b>	<b>8</b>
<b>L01 - Public Function could be Declared External</b>	<b>9</b>
<b>Description</b>	<b>9</b>
<b>Recommendation</b>	<b>9</b>
<b>L02 - State Variables could be Declared Constant</b>	<b>10</b>
<b>Description</b>	<b>10</b>
<b>Recommendation</b>	<b>10</b>
<b>L05 - Unused State Variable</b>	<b>11</b>
<b>Description</b>	<b>11</b>
<b>Recommendation</b>	<b>11</b>
<b>L04 - Conformance to Solidity Naming Conventions</b>	<b>12</b>
<b>Description</b>	<b>12</b>
<b>Recommendation</b>	<b>12</b>
<b>Contract Functions</b>	<b>13</b>
<b>Contract Flow</b>	<b>16</b>
<b>Domain Info</b>	<b>17</b>

<b>Summary</b>	<b>18</b>
<b>Disclaimer</b>	<b>19</b>
<b>About Cyberscope</b>	<b>20</b>

## Contract Review

<b>Contract Name</b>	HopeDoge
<b>Compiler Version</b>	v0.8.4+commit.c7e474f2
<b>Optimization</b>	200 runs
<b>Licence</b>	MIT
<b>Explorer</b>	<a href="https://bscscan.com/token/0xCB7C3D1Dd299BE73BC35B03F39e4bda9f0338Ff1">https://bscscan.com/token/0xCB7C3D1Dd299BE73BC35B03F39e4bda9f0338Ff1</a>
<b>Symbol</b>	Hope Doge
<b>Decimals</b>	9
<b>Total Supply</b>	1,000,000,000,000,000
<b>Source</b>	contract.sol
<b>Domain</b>	hopedoge.live

## Audit Updates

<b>Initial Audit</b>	1st March 2022
<b>Corrected</b>	

# 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

## ULTW - Unlimited Liquidity to Team Wallet

<b>Criticality</b>	medium
<b>Location</b>	contract.sol#L248

### Description

The contract owner has the authority to transfer funds to the team wallet. These funds are accumulated fees (taxFee) collected from the contract.

The taxed tokens can be sold in every sale or transfer transaction.

```
uint256 contractTokenBalance = balanceOf(address(this));
if (!inSwap && from != uniswapV2Pair && swapEnabled && contractTokenBalance > 0)
{
    swapTokensForEth(contractTokenBalance);
    uint256 contractETHBalance = address(this).balance;
    if(contractETHBalance > 0) {
        sendETHToFee(address(this).balance);
    }
}
```

The taxed tokens can also be sold manually by the contract owner.

```
function manualswap() external {
    require(_msgSender() == _developmentAddress || _msgSender() ==
_marketingAddress || _msgSender() == owner());
    uint256 contractBalance = balanceOf(address(this));
    swapTokensForEth(contractBalance);
}

function manualsend() external {
    require(_msgSender() == _developmentAddress || _msgSender() ==
_marketingAddress || _msgSender() == owner());
    uint256 contractETHBalance = address(this).balance;
    sendETHToFee(contractETHBalance);
}
```

## Recommendation

The contract could embody a check for the maximum amount of tokens that can be sold. The contract could also implement a more efficient way to sell and transfer the funds instead of repeating this procedure on every sale or transfer transaction.

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
●	FSA	Fixed Swap Address
●	L01	Public Function could be Declared External
●	L02	State Variables could be Declared Constant
●	L05	Unused State Variable
●	L04	Conformance to Solidity Naming Conventions



## FSA - Fixed Swap Address

<b>Criticality</b>	minor
<b>Location</b>	contract.sol#L166

### Description

The swap address is assigned once in the constructor and it can not be changed. The decentralized swaps sometimes create a new swap version or abandon the current. A contract that cannot change the swap address may not be able to catch-up the upgrade.

```
IUniswapV2Router02 _uniswapV2Router =  
IUniswapV2Router02(0x10ED43C718714eb63d5aA57B78B54704E256024E);  
uniswapV2Router = _uniswapV2Router;  
uniswapV2Pair = IUniswapV2Factory(_uniswapV2Router.factory())  
    .createPair(address(this), _uniswapV2Router.WETH());
```

### Recommendation

It could be better to allow the swap address mutation in case of future swap updates.

## L01 - Public Function could be Declared External

**Criticality**

minor

**Location**

contract.sol#L110,116,184,188,192,196,204,209,213,218 and 6 more

### Description

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

```
excludeMultipleAccountsFromFees  
toggleSwap  
setFee  
setNewMarketingAddress  
setNewDevAddress  
rescueForeignTokens  
transferFrom  
approve  
allowance  
...
```

### Recommendation

Use the external attribute for functions never called from the contract

## L02 - State Variables could be Declared Constant

**Criticality**

minor

**Location**

contract.sol#L93

### Description

Constant state variables should be declared constant to save gas.

```
_previousOwner
```

### Recommendation

Add the constant attribute to state variables that never change.

## L05 - Unused State Variable

<b>Criticality</b>	minor
<b>Location</b>	contract.sol#L93,127

### Description

There are segments that contain unused state variables.

```
_tOwned  
_previousOwner
```

### Recommendation

Remove unused state variables.

## L04 - Conformance to Solidity Naming Conventions

**Criticality**

minor

**Location**

contract.sol#L34,299,305,312,300,398,132,145,146,147 and 2 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.

```
_decimals  
_symbol  
_name  
_tTotal  
_swapEnabled  
_amount  
_to  
_tokenAddr  
marketingAddressUpdated  
...
```

### Recommendation

Follow the Solidity naming convention.

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

## Contract Functions

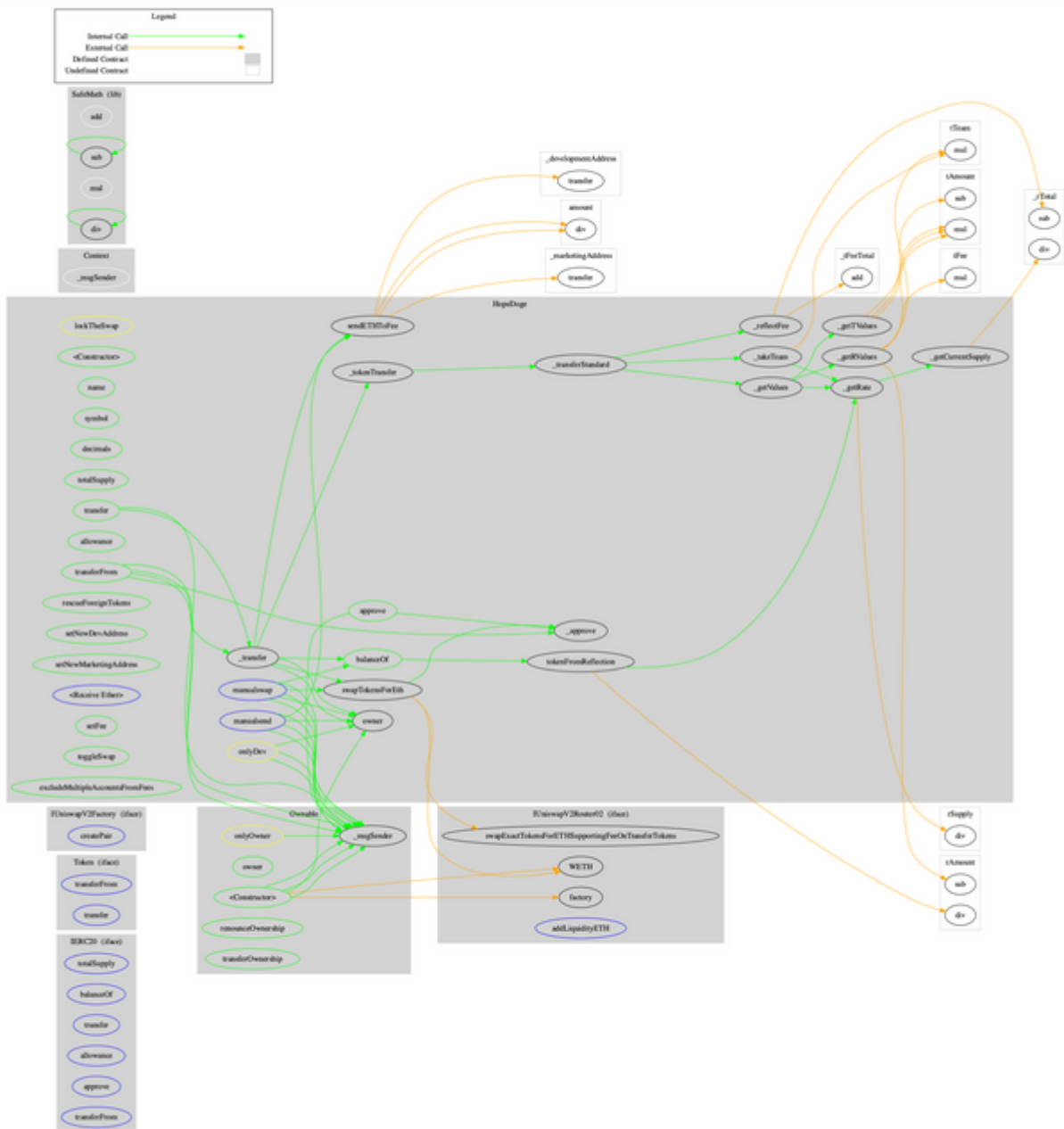
Contract	Type	Bases		
	Function Name	Visibility	Mutability	Modifiers
<b>IERC20</b>	Interface			
	totalSupply	External		-
	balanceOf	External		-
	transfer	External	✓	-
	allowance	External		-
	approve	External	✓	-
	transferFrom	External	✓	-
<b>Token</b>	Interface			
	transferFrom	External	✓	-
	transfer	External	✓	-
<b>IUniswapV2Factory</b>	Interface			
	createPair	External	✓	-
<b>IUniswapV2Router02</b>	Interface			
	swapExactTokensForETHSupportingFeeOnTransferTokens	External	✓	-
	factory	External		-
	WETH	External		-
	addLiquidityETH	External	Payable	-
<b>Context</b>	Implementation			
	_msgSender	Internal		
<b>SafeMath</b>	Library			

	add	Internal		
	sub	Internal		
	sub	Internal		
	mul	Internal		
	div	Internal		
	div	Internal		
<b>Ownable</b>	Implementation	Context		
	<Constructor>	Public	✓	-
	owner	Public		-
	renounceOwnership	Public	✓	onlyOwner
	transferOwnership	Public	✓	onlyOwner
<b>HopeDoge</b>	Implementation	Context, IERC20, Ownable		
	<Constructor>	Public	✓	-
	name	Public		-
	symbol	Public		-
	decimals	Public		-
	totalSupply	Public		-
	balanceOf	Public		-
	transfer	Public	✓	-
	allowance	Public		-
	approve	Public	✓	-
	transferFrom	Public	✓	-
	tokenFromReflection	Private		
	_approve	Private	✓	
	_transfer	Private	✓	
	swapTokensForEth	Private	✓	lockTheSwap
	sendETHToFee	Private	✓	
	_tokenTransfer	Private	✓	
	rescueForeignTokens	Public	✓	onlyDev
	setNewDevAddress	Public	✓	onlyDev
	setNewMarketingAddress	Public	✓	onlyDev
	_transferStandard	Private	✓	

	_takeTeam	Private	✓	
	_reflectFee	Private	✓	
	<Receive Ether>	External	Payable	-
	_getValues	Private		
	_getTValues	Private		
	_getRValues	Private		
	_getRate	Private		
	_getCurrentSupply	Private		
	manualswap	External	✓	-
	manualsend	External	✓	-
	setFee	Public	✓	onlyDev
	toggleSwap	Public	✓	onlyDev
	excludeMultipleAccountsFromFees	Public	✓	onlyOwner



# Contract Flow



## Domain Info

<b>Domain Name</b>	hopedoge.live
<b>Registry Domain ID</b>	6690fc3254f34ac5970a084da8c94ce2-DONUTS
<b>Creation Date</b>	2022-03-01T16:41:54Z
<b>Updated Date</b>	2022-03-01T16:41:55Z
<b>Registry Expiry Date</b>	2023-03-01T16:41:54Z
<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 has been created about 4 hours 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

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 18% fees. The contract could implement a more efficient way of selling and transferring all the accumulated tokens to the dev's wallets.

## 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>