



Cyberscope

# Audit Report

## YanHuangDao

June 2022

Type	BEP20
Network	BSC
Address	0xa5ae7b441d96ec1b5b05493d483c900f9f24e03d
Audited by	© cyberscope

# Table of Contents

<b>Table of Contents</b>	<b>1</b>
<b>Contract Review</b>	<b>3</b>
<b>Source Files</b>	<b>3</b>
<b>Audit Updates</b>	<b>3</b>
<b>Contract Analysis</b>	<b>4</b>
<b>Contract Diagnostics</b>	<b>5</b>
<b>L01 - Public Function could be Declared External</b>	<b>6</b>
Description	6
Recommendation	6
<b>L02 - State Variables could be Declared Constant</b>	<b>7</b>
Description	7
Recommendation	7
<b>L04 - Conformance to Solidity Naming Conventions</b>	<b>8</b>
Description	8
Recommendation	8
<b>L07 - Missing Events Arithmetic</b>	<b>9</b>
Description	9
Recommendation	9
<b>L09 - Dead Code Elimination</b>	<b>10</b>
Description	10
Recommendation	10
<b>Contract Functions</b>	<b>11</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>

**About Cyberscope****20**

## Contract Review

<b>Contract Name</b>	YHD
<b>Compiler Version</b>	v0.8.12+commit.f00d7308
<b>Optimization</b>	200 runs
<b>Licence</b>	None
<b>Explorer</b>	<a href="https://bscscan.com/token/0xA5AE7b441D96ec1b5B05493D483C900F9f24e03D">https://bscscan.com/token/0xA5AE7b441D96ec1b5B05493D483C900F9f24e03D</a>
<b>Symbol</b>	YHD
<b>Decimals</b>	9
<b>Total Supply</b>	2,000,000
<b>Domain</b>	yhddao.xyz

## Source Files

<b>Filename</b>	<b>SHA256</b>
<b>contract.sol</b>	1bc61b3cd8c030e52da35fc854ed0bd84ab9f9914305ebf6463f3f18815698dc

## Audit Updates

<b>Initial Audit</b>	6th June 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

# 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
●	L07	Missing Events Arithmetic
●	L09	Dead Code Elimination

## L01 - Public Function could be Declared External

<b>Criticality</b>	minor
<b>Location</b>	contract.sol#L163,168,469,473,477,481,489,493,498,503,507,521,529,540,545

### Description

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

```
transferFrom
transfer
getCirculatingSupply
setIsExcludedFromFee
approve
minimumTokensBeforeSwapAmount
decreaseAllowance
increaseAllowance
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#L397,399,382,400,398,380,381,387,385,389,386,384,411,418,417

### Description

Constant state variables should be declared constant to save gas.

```
swapAndLiquifyEnabled
swapAndLiquifyByLimitOnly
snipeBlocks
marketingWalletAddress
lpWallet
deadAddress
buyBackWallet
antibotWallet
_symbol
...
```

### Recommendation

Add the constant attribute to state variables that never change.



## L04 - Conformance to Solidity Naming Conventions

**Criticality**

minor

**Location**

contract.sol#L206,207,223,242,391,397,398,399,400,402

### 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.

```
_totalTax  
_lpFee  
_buybackFee  
_marketingFee  
_burnFee  
_balances  
WETH  
MINIMUM_LIQUIDITY  
PERMIT_TYPEHASH  
...
```

### 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**

contract.sol#L525

### 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.

```
minimumTokensBeforeSwap = newLimit
```

### Recommendation

Emit an event for critical parameter changes.

## L09 - Dead Code Elimination

<b>Criticality</b>	minor
<b>Location</b>	contract.sol#L123,106,110,114,118,87,98,657

### Description

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

```
swapEthForCustomToken  
sendValue  
isContract  
functionCallWithValue  
functionCall  
_functionCallWithValue
```

### Recommendation

Remove unused functions.

# Contract Functions

Contract	Type	Bases		
	Function Name	Visibility	Mutability	Modifiers
<b>Context</b>	Implementation			
	_msgSender	Internal		
	_msgData	Internal		
<b>IERC20</b>	Interface			
	totalSupply	External		-
	balanceOf	External		-
	transfer	External	✓	-
	allowance	External		-
	approve	External	✓	-
	transferFrom	External	✓	-
<b>SafeMath</b>	Library			
	add	Internal		
	sub	Internal		
	sub	Internal		
	mul	Internal		
	div	Internal		
	div	Internal		
	mod	Internal		
	mod	Internal		
<b>Address</b>	Library			
	isContract	Internal		
	sendValue	Internal	✓	
	functionCall	Internal	✓	
	functionCall	Internal	✓	
	functionCallWithValue	Internal	✓	

	functionCallWithValue	Internal	✓	
	_functionCallWithValue	Private	✓	
<b>Ownable</b>	Implementation	Context		
	<Constructor>	Public	✓	-
	owner	Public		-
	waiveOwnership	Public	✓	onlyOwner
	transferOwnership	Public	✓	onlyOwner
<b>IUniswapV2Factory</b>	Interface			
	feeTo	External		-
	feeToSetter	External		-
	getPair	External		-
	allPairs	External		-
	allPairsLength	External		-
	createPair	External	✓	-
	setFeeTo	External	✓	-
	setFeeToSetter	External	✓	-
<b>IUniswapV2Pair</b>	Interface			
	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		-
	burn	External	✓	-
	swap	External	✓	-
	skim	External	✓	-
	sync	External	✓	-
	initialize	External	✓	-
<b>IUniswapV2Router01</b>	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	✓	-
YHD	Implementation	Context, IERC20, Ownable		
	<Constructor>	Public	✓	-
	name	Public		-
	symbol	Public		-
	decimals	Public		-
	totalSupply	Public		-
	balanceOf	Public		-
	allowance	Public		-
	increaseAllowance	Public	✓	-
	decreaseAllowance	Public	✓	-
	minimumTokensBeforeSwapAmount	Public		-
	approve	Public	✓	-
	_approve	Private	✓	
	setIsExcludedFromFee	Public	✓	onlyOwner
	setNumTokensBeforeSwap	External	✓	onlyOwner
	getCirculatingSupply	Public		-
	transferToAddressETH	Private	✓	
	<Receive Ether>	External	Payable	-
	transfer	Public	✓	-
	transferFrom	Public	✓	-
	_transfer	Private	✓	
	_basicTransfer	Internal	✓	
	swapAndLiquify	Private	✓	lockTheSwap

	swapTokensForEth	Private	✓	
	swapEthForCustomToken	Private	✓	
	addLiquidity	Private	✓	
	takeFee	Internal	✓	



# Contract Flow



## Domain Info

<b>Domain Name</b>	yhddao.xyz
<b>Registry Domain ID</b>	D301112266-CNIC
<b>Creation Date</b>	2022-06-03T15:01:13.0Z
<b>Updated Date</b>	2022-06-03T15:02:07.0Z
<b>Registry Expiry Date</b>	2023-06-03T23:59:59.0Z
<b>Registrar WHOIS Server</b>	whois.gname.com
<b>Registrar URL</b>	<a href="https://www.gname.com/">https://www.gname.com/</a>
<b>Registrar</b>	Gname.com Pte. Ltd.
<b>Registrar IANA ID</b>	1923

The domain has been created 3 days 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

YanHuangDao is an interesting project that has a friendly and growing community. 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. The fees are fixed to 9%.

# 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>