



Cyberscope

# Audit Report

## Hadouken

April 2022

Type       BEP20

Network    BSC

Address     0xc0D69a6258a2ED8755839a87d51B80548ED878F7

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>L05 - Unused State Variable</b>	<b>9</b>
Description	9
Recommendation	9
<b>L07 - Missing Events Arithmetic</b>	<b>10</b>
Description	10
Recommendation	10
<b>L09 - Dead Code Elimination</b>	<b>11</b>
Description	11
Recommendation	11
<b>L12 - Using Variables before Declaration</b>	<b>12</b>
Description	12

<b>Recommendation</b>	<b>12</b>
<b>L13 - Divide before Multiply Operation</b>	<b>13</b>
<b>Description</b>	<b>13</b>
<b>Recommendation</b>	<b>13</b>
<b>L14 - Uninitialized Variables in Local Scope</b>	<b>14</b>
<b>Description</b>	<b>14</b>
<b>Recommendation</b>	<b>14</b>
<b>L15 - Local Scope Variable Shadowing</b>	<b>15</b>
<b>Description</b>	<b>15</b>
<b>Recommendation</b>	<b>15</b>
<b>Contract Functions</b>	<b>16</b>
<b>Contract Flow</b>	<b>23</b>
<b>Domain Info</b>	<b>24</b>
<b>Summary</b>	<b>25</b>
<b>Disclaimer</b>	<b>26</b>
<b>About Cyberscope</b>	<b>27</b>

## Contract Review

<b>Contract Name</b>	HadoukenCoin
<b>Compiler Version</b>	v0.8.11+commit.d7f03943
<b>Optimization</b>	200 runs
<b>Licence</b>	MIT
<b>Explorer</b>	<a href="https://bscscan.com/token/0xc0d69a6258a2ed8755839a87d51b80548ed878f7">https://bscscan.com/token/0xc0d69a6258a2ed8755839a87d51b80548ed878f7</a>
<b>Symbol</b>	HDKN
<b>Decimals</b>	9
<b>Total Supply</b>	1,000,000,000,000,000
<b>Domain</b>	hadoukencoin.com

## Source Files

<b>Filename</b>	<b>SHA256</b>
<b>contract.sol</b>	ecdfeb8069a9e6e66c9f277cf7d9ad026ee2fe43b24555f580b661d33f2485ba

## Audit Updates

<b>Initial Audit</b>	3rd April 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
●	L05	Unused State Variable
●	L07	Missing Events Arithmetic
●	L09	Dead Code Elimination
●	L12	Using Variables before Declaration
●	L13	Divide before Multiply Operation
●	L14	Uninitialized Variables in Local Scope
●	L15	Local Scope Variable Shadowing

## L01 - Public Function could be Declared External

**Criticality**

minor

**Location**

contract.sol#L65,70,196,204,208,227,232,236,241,252 and 19 more

### Description

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

```
process
getAccountAtIndex
dividendTokenBalanceOf
withdrawableDividendOf
isExcludedFromFees
updateGasForProcessing
setAutomatedMarketMakerPair
excludeMultipleAccountsFromFees
updateUniswapV2Router
...
```

### Recommendation

Use the external attribute for functions never called from the contract

## L02 - State Variables could be Declared Constant

**Criticality**

minor

**Location**

contract.sol#L706,702

### Description

Constant state variables should be declared constant to save gas.

```
deadWallet  
_totalSupply
```

### Recommendation

Add the constant attribute to state variables that never change.



## L04 - Conformance to Solidity Naming Conventions

**Criticality**

minor

**Location**

contract.sol#L391,396,400,404,343,344,510,667,668,675 and 22 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.

```
_account  
_tokens  
_walletMaxHoldingLimit  
_developerWalletAddress  
_marketingWalletAddress  
BUSDRewardsFee  
_maxTxAmount  
_swapTokensAtAmount  
BUSD  
...
```

### Recommendation

Follow the Solidity naming convention.

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

## L05 - Unused State Variable

**Criticality**

minor

**Location**

contract.sol#L135

### Description

There are segments that contain unused state variables.

```
MAX_INT256
```

### Recommendation

Remove unused state variables.

## L07 - Missing Events Arithmetic

**Criticality**

minor

**Location**

contract.sol#L1084,1125,1140

### 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.

```
_swapTokensAtAmount = _value  
_walletMaxHoldingLimit = _amount  
_maxTxAmount = _amount
```

### Recommendation

Emit an event for critical parameter changes.

## L09 - Dead Code Elimination

**Criticality**

minor

**Location**

contract.sol#L409,160

### Description

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

```
abs  
_transfer
```

### Recommendation

Remove unused functions.

## L12 - Using Variables before Declaration

**Criticality**

minor

**Location**

contract.sol#L984

### Description

The contract is using a variable before the declaration. This is usually happening either if it has not been declared yet or the variable has been declared in a different scope.

```
lastProcessedIndex  
iterations  
claims
```

### Recommendation

The variables should be declared before any usage of them.

## L13 - Divide before Multiply Operation

**Criticality**

minor

**Location**

contract.sol#L692

### Description

Performing divisions before multiplications may cause lose of prediction.

```
_walletMaxHoldingLimit = _totalSupply.div(10000).mul(5)
```

### Recommendation

The multiplications should be prior to the divisions.

## L14 - Uninitialized Variables in Local Scope

**Criticality**

minor

**Location**

contract.sol#L984

### Description

There are variables that are defined in the local scope and are not initialized.

```
lastProcessedIndex  
claims  
iterations
```

### Recommendation

All the local scoped variables should be initialized.

## L15 - Local Scope Variable Shadowing

**Criticality**

minor

**Location**

contract.sol#L351,391,396,400,404

### Description

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

```
_owner  
_symbol  
_name
```

### Recommendation

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



# Contract Functions

Contract	Type	Bases		
	Function Name	Visibility	Mutability	Modifiers
<b>IBEP20</b>	Interface			
	totalSupply	External		-
	balanceOf	External		-
	transfer	External	✓	-
	allowance	External		-
	approve	External	✓	-
	transferFrom	External	✓	-
<b>IBEP20Metadata</b>	Interface	IBEP20		
	name	External		-
	symbol	External		-
	decimals	External		-
<b>Context</b>	Implementation			
	_msgSender	Internal		
	_msgData	Internal		
<b>Ownable</b>	Implementation	Context		
	<Constructor>	Public	✓	-
	owner	Public		-
	renounceOwnership	Public	✓	onlyOwner
	transferOwnership	Public	✓	onlyOwner
<b>SafeMath</b>	Library			
	add	Internal		
	sub	Internal		

	sub	Internal		
	mul	Internal		
	div	Internal		
	div	Internal		
	mod	Internal		
	mod	Internal		
<b>SafeMathInt</b>	Library			
	mul	Internal		
	div	Internal		
	sub	Internal		
	add	Internal		
	abs	Internal		
	toUint256Safe	Internal		
<b>SafeMathUint</b>	Library			
	toInt256Safe	Internal		
<b>BEP20</b>	Implementation	Context, IBEP20, IBEP20Meta data		
	<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	✓	
<b>DividendPayingTokenInterface</b>	Interface			
	dividendOf	External		-
	withdrawDividend	External	✓	-
<b>DividendPayingTokenOptionalInterface</b>	Interface			
	withdrawableDividendOf	External		-
	withdrawnDividendOf	External		-
	accumulativeDividendOf	External		-
<b>DividendPayingToken</b>	Implementation	BEP20, Ownable, DividendPayingTokenInterface, DividendPayingTokenOptionalInterface		
	<Constructor>	Public	✓	BEP20
	distributeBUSDDividends	Public	✓	onlyOwner
	withdrawDividend	Public	✓	-
	_withdrawDividendOfUser	Internal	✓	
	dividendOf	Public		-
	withdrawableDividendOf	Public		-
	withdrawnDividendOf	Public		-
	accumulativeDividendOf	Public		-
	_transfer	Internal	✓	
	_mint	Internal	✓	
	_burn	Internal	✓	
	_setBalance	Internal	✓	

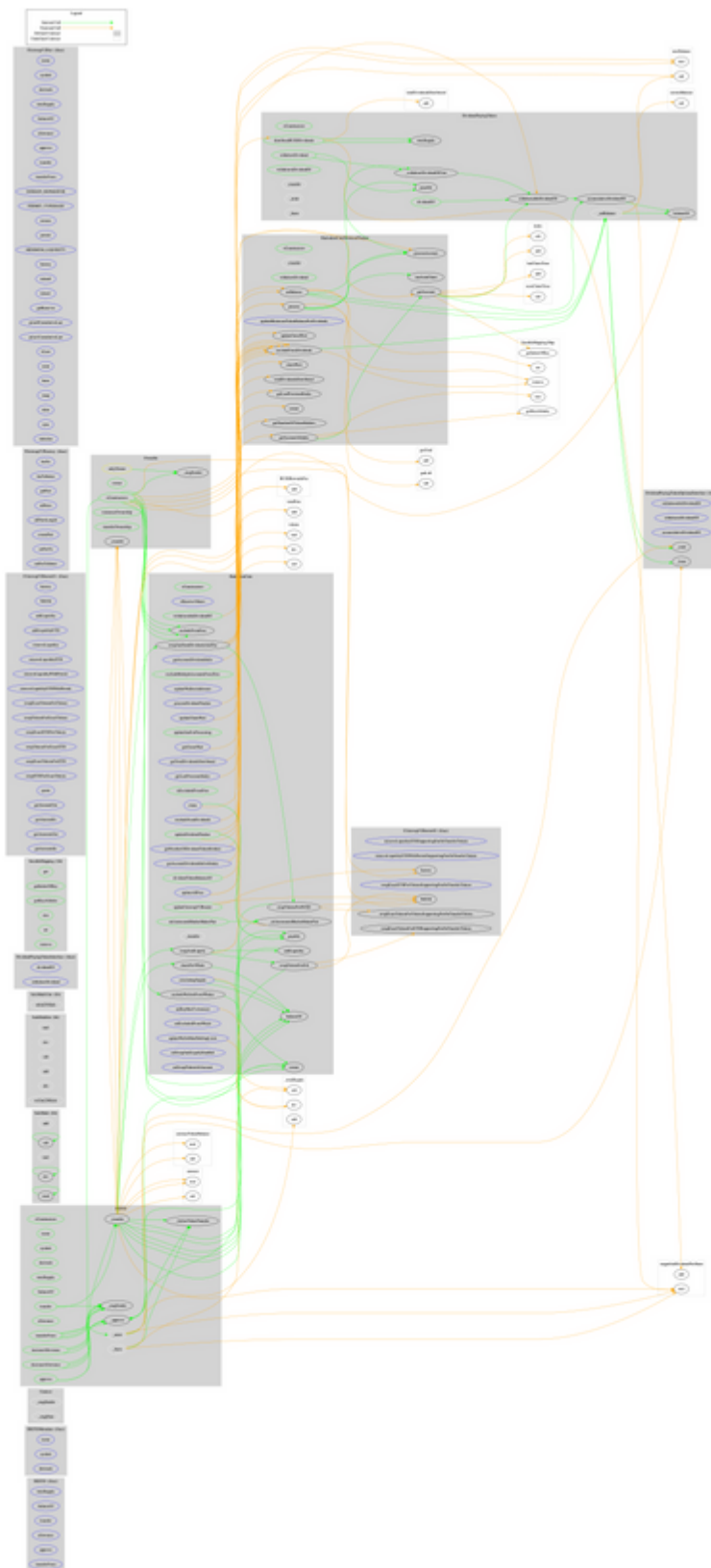
<b>IterableMapping</b>	Library			
	get	Public		-
	getIndexOfKey	Public		-
	getKeyAtIndex	Public		-
	size	Public		-
	set	Public	✓	-
	remove	Public	✓	-
<b>IUniswapV2Router01</b>	Interface			
	factory	External		-
	WETH	External		-
	addLiquidity	External	✓	-
	addLiquidityETH	External	Payable	-
	removeLiquidity	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		-
<b>IUniswapV2Router02</b>	Interface	IUniswapV2Router01		
	removeLiquidityETHSupportingFeeOnTransferTokens	External	✓	-
	removeLiquidityETHWithPermitSupportingFeeOnTransferTokens	External	✓	-

	swapExactTokensForTokensSupportingFeeOnTransferTokens	External	✓	-
	swapExactETHForTokensSupportingFeeOnTransferTokens	External	Payable	-
	swapExactTokensForETHSupportingFeeOnTransferTokens	External	✓	-
<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		-
	mint	External	✓	-
	burn	External	✓	-
	swap	External	✓	-
	skim	External	✓	-
	sync	External	✓	-
	initialize	External	✓	-
<b>HadoukenCoin</b>	Implementation	BEP20, Ownable		
	<Constructor>	Public	✓	BEP20
	<Receive Ether>	External	Payable	-
	circulatingSupply	External		-
	updateDividendTracker	Public	✓	onlyOwner
	updateUniswapV2Router	Public	✓	onlyOwner
	excludeFromFees	Public	✓	onlyOwner
	excludeMultipleAccountsFromFees	Public	✓	onlyOwner
	updateWalletsAddresses	External	✓	onlyOwner
	updateAllFees	External	✓	onlyOwner
	setAutomatedMarketMakerPair	Public	✓	onlyOwner
	_setAutomatedMarketMakerPair	Private	✓	
	updateGasForProcessing	Public	✓	onlyOwner
	updateClaimWait	External	✓	onlyOwner
	getClaimWait	External		-
	getTotalDividendsDistributed	External		-
	isExcludedFromFees	Public		-
	withdrawableDividendOf	Public		-
	dividendTokenBalanceOf	Public		-
	excludeFromDividends	External	✓	onlyOwner
	getAccountDividendsInfo	External		-
	getAccountDividendsInfoAtIndex	External		-
	processDividendTracker	External	✓	-
	claim	External	✓	-

	getLastProcessedIndex	External		-
	getNumberOfDividendTokenHolders	External		-
	_transfer	Internal	✓	
	swapAndLiquify	Private	✓	
	addLiquidity	Private	✓	
	swapTokensForEth	Private	✓	
	swapAndSendDividendsAndFee	Private	✓	
	swapTokensForBUSD	Private	✓	
	setBuyMaxTxAmount	External	✓	onlyOwner
	excludeWalletsFromWhales	Private	✓	
	checkForWhale	Private		
	setExcludedFromWhale	External	✓	onlyOwner
	updateWalletMaxHoldingLimit	External	✓	onlyOwner
	setSwapAndLiquifyEnabled	External	✓	onlyOwner
	setSwapTokensAtAmount	External	✓	onlyOwner
<b>HadoukenCoin DividendTracker</b>	Implementation	Ownable, DividendPay ingToken		
	<Constructor>	Public	✓	DividendPayin gToken
	_transfer	Internal		
	withdrawDividend	Public		-
	excludeFromDividends	External	✓	onlyOwner
	updateClaimWait	External	✓	onlyOwner
	updateMinimumTokenBalanceForDivi dends	External	✓	onlyOwner
	getLastProcessedIndex	External		-
	getNumberOfTokenHolders	External		-
	getAccount	Public		-
	getAccountAtIndex	Public		-
	canAutoClaim	Private		
	setBalance	External	✓	onlyOwner
	process	Public	✓	-
	processAccount	Public	✓	onlyOwner

# Contract Flow





## Domain Info

<b>Domain Name</b>	hadoukencoin.com
<b>Registry Domain ID</b>	2655981470_DOMAIN_COM-VRSN
<b>Creation Date</b>	2021-11-18T17:06:52Z
<b>Updated Date</b>	2021-11-18T17:06:52Z
<b>Registry Expiry Date</b>	2023-11-18T17:06:52Z
<b>Registrar WHOIS Server</b>	whois.godaddy.com
<b>Registrar URL</b>	<a href="https://www.godaddy.com">https://www.godaddy.com</a>
<b>Registrar</b>	GoDaddy.com, LLC
<b>Registrar IANA ID</b>	146

The domain has been created 5 months before the creation of the audit. It will expire in over 1 year.

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

## Summary

Token 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. There is also a limit of max 15% fees.

# 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>