Cyberscope

Audit Report

YugiCripto

March 2022

Table of Contents

Contract Review

Contract Name	YugiCriptoContract
Compiler Version	v0.8.7+commit.e28d00a7
Optimization	100 runs
Licence	MIT
Explorer	https://bscscan.com/token/0x81Db8347EEca439fb3a5172b2503BA5fd8c256fc
Symbol	$YCO
Decimals	18
Total Supply	100,000,000
Domain	yugicripto.com

Audit Updates

Initial Audit	24th March 2022
Corrected	

Source Files

Filename	SHA256
Authorized.sol	92fc8a8c2d7c543a452e05a164302f3e357a4d7009fc5030ed6b5ede699fab2b
Context.sol	91bb853b4716bea8540722c7b13af34e2f24b01a3654cadd68246a72e6c759b8
ERC20.sol	adea8d6813eba55020be787c8a9bef8a71f90c96fd5c75544bc4ac1bccbd51ab
IERC20.sol	4ad9e1338842c0a911ed1994774827c17eea117751a56f1111193d0bc4c0006e
IERC20Metadata.sol	aa7bbf621cc23ca80abde64c64ff6f9503aceae5592f8e3ed2d0ab0a345e09e6
IPancake.sol	ce5cedde1004c8768e88974c30f9d386f0e4f56f084d03e1397a5c8a2a274aa9
Ownable.sol	4a0c4ca403220345b36b1a2e02b5fe041c0e93aa5603a964344c4b3f2c3a8a36
Strings.sol	958c2a94731d0ceaaa0830b457842ec11471197f894c2afd6facd7709275f8ac
SwapHelper.sol	82a1d3af307e1561dcfe9844cd83421b3ed372b3dd6fa638810397df4326542d
YugiCripto.sol	1e2ee4483c229ec588bde73c8865bf3a0750fc181aa404360e4ad4905bac106a

Contract Analysis

The contract contains a code optimization section. It uses fixed methodId values in order to proceed with some function calls. We investigated that the actual functions are the expected.

YugiCrypto Function	MathodId	Origin Function	Origin Class
isReversed	0dfe1681	token0()	IUniswapV2Pair
tokenTransfer	a9059cbb	transfer(address,uint256)	IUniswapV2Pair
tokenTransferFrom	23b872dd	transferFrom(address,address,uint256)	IUniswapV2Pair
swapToken	022c0d9f	swap(uint256,uint256,address,bytes)	IUniswapV2Pair
getTokenBalanceOf	70a08231	balanceOf(address)	IUniswapV2Pair
getTokenReserves	0902f1ac	getReserves()	IUniswapV2Pair

● 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

Criticality	minor
Location	contract.sol#L255

Description

The contract owner has the authority to transfer funds to the team wallet. These funds have been accumulated from fees collected from the contract. The owner may take advantage of it by setting a high fee to the `buyBackAndHoldWithDecimals` variable.

```
function buyBackAndHoldWithDecimals(uint256 decimalAmount, address receiver)
public isAuthorized(3) { buyBackWithDecimals(decimalAmount, receiver); }
```

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

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

L01 - Public Function could be Declared External

Criticality	minor
Location	YugiCripto.sol#L88,92,96,97,98,100,101

Description

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

```
setAdministrationWallet
setExemptStaker
setExemptTxLimit
setExemptFeeReceiver
setExemptFee
desactiveTxLimit
activeTxLimit
```

Recommendation

Use the external attribute for functions never called from the contract

L02 - State Variables could be Declared Constant

Criticality	minor
Location	YugiCripto.sol#L76

Description

Constant state variables should be declared constant to save gas.

```
WBNB_BUSD_PAIR
```

Recommendation

Add the constant attribute to state variables that never change.

L04 - Conformance to Solidity Naming Conventions

Criticality	minor
Location	YugiCripto.sol#L396,397,54,55,52,53,56,57,76,78

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.

```
YUGICRIPTO_POOL
WBNB_BUSD_PAIR
_maxTxAmount
_maxSupply
decimalBUSD
decimal
_symbol
_name
getWBNB_BUSD_Pair
...
```

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	YugiCripto.sol#L389

Description

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

```
walletHolder
```

## Recommendation

Remove unused functions.

Contract Functions

Contract	Type	Bases		
	Function Name	Visibility	Mutability	Modifiers
Authorized	Implementation	Ownable		
	<Constructor>	Public	✓	-
	safeApprove	External	✓	isAuthorized
	safeWithdraw	External	✓	isAuthorized
	grantPermission	External	✓	isAuthorized
	revokePermission	External	✓	isAuthorized
	grantAllPermissions	External	✓	isAuthorized
	revokeAllPermissions	External	✓	isAuthorized
Context	Implementation			
	_msgSender	Internal		
	_msgData	Internal		
ERC20	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	✓	
	_beforeTokenTransfer	Internal	✓	
	_afterTokenTransfer	Internal	✓	
IERC20	Interface			
	totalSupply	External		-
	balanceOf	External		-
	transfer	External	✓	-
	allowance	External		-
	approve	External	✓	-
	transferFrom	External	✓	-
IERC20Metadata	Interface	IERC20		
	name	External		-
	symbol	External		-
	decimals	External		-
PancakeFactory	Interface			
	createPair	External	✓	-
PancakeRouter	Interface			
	factory	External		-
Ownable	Implementation	Context		
	<Constructor>	Public	✓	-
	owner	Public		-
	renounceOwnership	Public	✓	onlyOwner
	transferOwnership	Public	✓	onlyOwner
	_setOwner	Private	✓	
Strings	Library			

	toString	Internal		
	toHexString	Internal		
	toHexString	Internal		
SwapHelper	Implementation	Ownable		
	\<Constructor\>	Public	✓	-
	safeApprove	External	✓	onlyOwner
	safeWithdraw	External	✓	onlyOwner
YugiCriptoContract	Implementation	Authorized, ERC20		
	getOwner	External		-
	getFeeTotal	Public		-
	getSwapHelperAddress	External		-
	activeTxLimit	Public	✓	isAuthorized
	desactiveTxLimit	Public	✓	isAuthorized
	setExemptFee	Public	✓	isAuthorized
	setExemptFeeReceiver	Public	✓	isAuthorized
	setExemptTxLimit	Public	✓	isAuthorized
	setExemptStaker	Public	✓	isAuthorized
	setAdministrationWallet	Public	✓	isAuthorized
	\<Receive Ether\>	External	Payable	-
	\<Constructor\>	Public	✓	ERC20
	decimals	Public		-
	_mint	Internal	✓	
	_beforeTokenTransfer	Internal		
	_transfer	Internal	✓	
	exchangeFeeParts	Private	✓	
	buyBackAndHold	External	✓	isAuthorized
	buyBackAndHoldWithDecimals	Public	✓	isAuthorized
	buyBackAndBurn	External	✓	isAuthorized
	buyBackAndBurnWithDecimals	Public	✓	isAuthorized
	buyBackWithDecimals	Private	✓	
	getAmountOut	Internal		
	isReversed	Internal		
	tokenTransfer	Internal	✓	

	tokenTransferFrom	Internal	✓	
	swapToken	Internal	✓	
	getTokenBalanceOf	Internal		
	getTokenReserves	Internal		
	walletHolder	Private		
	safeOtherTokens	External	✓	isAuthorized
	getYUGICRIPTO_POOL	External		-
	getWBNB_BUSD_Pair	External		-

Contract Flow
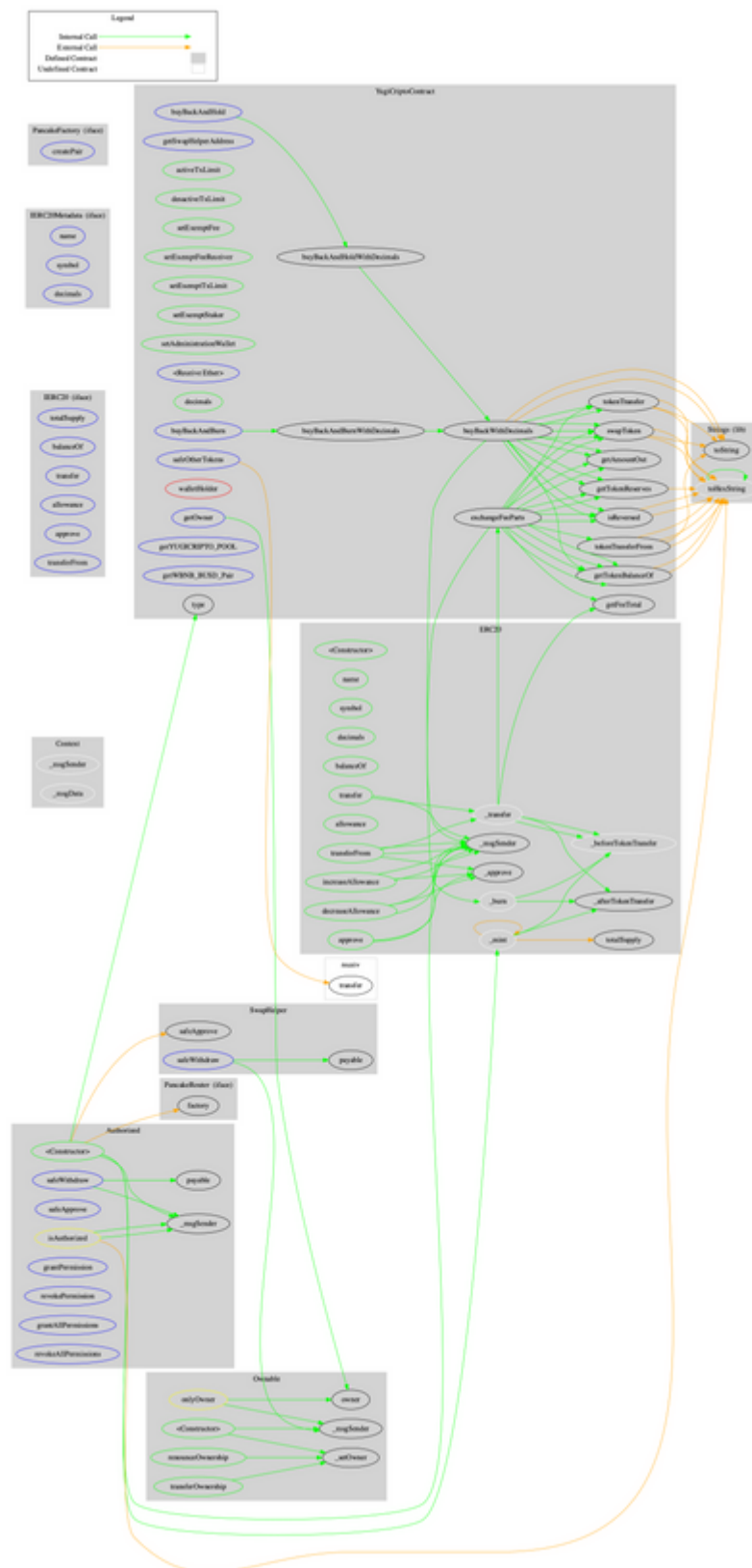
Domain Info

Domain Name	yugicripto.com
Registry Domain ID	2661823636_DOMAIN_COM-VRSN
Creation Date	2021-12-15T18:55:37Z
Updated Date	2022-03-15T22:45:42Z
Registry Expiry Date	2022-12-15T18:55:37Z
Registrar WHOIS Server	whois.godaddy.com
Registrar URL	http://www.godaddy.com
Registrar	GoDaddy.com, LLC
Registrar IANA ID	146

The domain has been created 3 months before the creation of the audit. It will expire in 9 months.

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

Summary

The Smart Contract is using a code optimization pattern with low-level function calls. We are concerned if a compilation with many optimization rounds produces almost the same result as the low-level implementation. The role "operator" has the authority to send funds to the team wallet. The fees are fixed to 10%.

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