Cyberscope

Audit Report
CGPT

December 2022

Table of Contents

Contract Review

Contract Name	Token
Compiler Version	v0.8.15+commit.e14f2714
Optimization	200 runs
Licence	None
Explorer	https://bscscan.com/token/0x1012641f794213c75AbbCd9E4321611415549475
Symbol	CGPT
Decimals	9
Total Supply	100,000
Domain	chatgptcoin.top

Source Files

Filename	**SHA256**
contract.sol	ca2245feba676ea08eef7778a9544c1ecd8fa109ecbab81f55ff7efc8b4636c1

Audit Updates

Initial Audit	8th December 2022
Corrected	

Contract Analysis

● Critical   ● Medium   ● Minor / Informative   ● Pass

Severity	Code	Description	Status
●	ST	Stops Transactions	Passed
●	OCTD	Transfers Contract's Tokens	Passed
●	OTUT	Transfers User's Tokens	Passed
●	ELFM	Exceeds Fees Limit	Passed
●	ULTW	Transfers Liquidity to Team Wallet	Passed
●	MT	Mints Tokens	Passed
●	BT	Burns Tokens	Passed
●	BC	Blacklists Addresses	Passed

Contract Diagnostics

● Critical   ● Medium   ● Minor / Informative

Severity	Code	Description	Status
●	PVC	Price Volatility Concern	Unresolved
●	RSML	Redundant SafeMath Library	Unresolved
●	BLC	Business Logic Concern	Unresolved
●	L02	State Variables could be Declared Constant	Unresolved
●	L04	Conformance to Solidity Naming Conventions	Unresolved
●	L07	Missing Events Arithmetic	Unresolved
●	L09	Dead Code Elimination	Unresolved

PVC - Price Volatility Concern

Criticality	minor / informative
Location	contract.sol#L511
Status	Unresolved

Description

The minimumTokensBeforeSwap could produce a dramatically price volatility. If the variable set to a high number, then the contract will sell a huge amount of tokens in a single transaction.

```solidity
function setNumTokensBeforeSwap(uint256 newLimit) external onlyOwner() {
    minimumTokensBeforeSwap = newLimit;
}
```

Recommendation

The contract could ensure that it will not sell more than a reasonable amount of tokens once. A suggested implementation could check that the maximum amount should be less than a fixed percentage of the total supply.

2

RSML - Redundant SafeMath Library

Criticality	minor / informative
Location	contract.sol#L28
Status	Unresolved

Description

The Solidity versions that are greater than or equal to 0.8.0 do not need the use of SafeMath Library. The usage of the SafeMath library produces unnecessary additional gas.

```
library SafeMath {
...
}
```

Recommendation

The team is advised to remove the SafeMath library as it is safe to do math operations without it.

BLC - Business Logic Concern

Criticality	minor / informative
Location	contract.sol#L593,597
Status	Unresolved

Description

The swapAndLiquify method does not swap and liquify. Instead, it just transfers the fee amount to the marketingAddress. Additionally, the takeFee method adds the fee amount to the contract address, and then swapAndLiquify will transfer it to the marketingAddress.

```
function swapAndLiquify(uint256 tAmount) private lockTheSwap {
    _basicTransfer(address(this),marketingWallet,tAmount);
}
...
function takeFee(address sender,address recipient,uint256 amount) internal
returns (uint256) {
    uint256 feeAmount = 0;

    if(isMarketPair[sender]||isMarketPair[recipient]) {
        feeAmount = amount.mul(_totalTax).div(100);
    }

    if(feeAmount > 0) {
        _balances[address(this)] = _balances[address(this)].add(feeAmount);
        emit Transfer(sender, address(this), feeAmount);
    }

    return amount.sub(feeAmount);
}
```

Recommendation

The team is advised to carefully check if the implementation follows the expected business logic. If that is the expected behaviour, then:

- There is no requirement for a swap locker.

- The swap section should be removed and the takeFee method should transfer the fee amount to the marketingAddress directly.

L02 - State Variables could be Declared Constant

Criticality	minor / informative
Location	contract.sol#L378,403,377,376,404,382
Status	Unresolved

Description

Constant state variables should be declared constant to save gas.

```
_decimals
swapAndLiquifyEnabled
_symbol
_name
swapAndLiquifyByLimitOnly
deadAddress
```

Recommendation

Add the constant attribute to state variables that never change.

L04 - Conformance to Solidity Naming Conventions

Criticality	minor / informative
Location	contract.sol#L203,219,525,202,390,238,384,392
Status	Unresolved

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.

```
PERMIT_TYPEHASH
MINIMUM_LIQUIDITY
OpenTrade
DOMAIN_SEPARATOR
_marketingFee
WETH
_balances
_totalTax
```

Recommendation

Follow the Solidity naming convention.
https://docs.soliditylang.org/en/v0.8.17/style-guide.html#naming-conventions.

L07 - Missing Events Arithmetic

Criticality	minor / informative
Location	contract.sol#L511,515
Status	Unresolved

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
_marketingFee = value
```

Recommendation

Emit an event for critical parameter changes.

L09 - Dead Code Elimination

Criticality	minor / informative
Location	contract.sol#L94,110,534,114,119,83,106,102
Status	Unresolved

Description

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

```
sendValue
functionCallWithValue
transferToAddressETH
_functionCallWithValue
isContract
functionCall
```

Recommendation

Remove unused functions.

Contract Functions

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

	_functionCallWithValue	Private	✓	
Ownable	Implementation	Context		
	\<Constructor\>	Public	✓	-
	owner	Public		-
	waiveOwnership	Public	✓	onlyOwner
	transferOwnership	Public	✓	onlyOwner
IUniswapV2Factory	Interface			
	feeTo	External		-
	feeToSetter	External		-
	getPair	External		-
	allPairs	External		-
	allPairsLength	External		-
	createPair	External	✓	-
	setFeeTo	External	✓	-
	setFeeToSetter	External	✓	-
IUniswapV2Pair	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	✓	-
IUniswapV2Router01	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		

	removeLiquidityETHSupportingFeeOn TransferTokens	External	✓	-
	removeLiquidityETHWithPermitSuppo rtingFeeOnTransferTokens	External	✓	-
	swapExactTokensForTokensSupporti ngFeeOnTransferTokens	External	✓	-
	swapExactETHForTokensSupporting FeeOnTransferTokens	External	Payable	-
	swapExactTokensForETHSupporting FeeOnTransferTokens	External	✓	-
Token	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
	setMarketPairStatus	Public	✓	onlyOwner
	setNumTokensBeforeSwap	External	✓	onlyOwner
	setMarketingFee	External	✓	onlyOwner
	setMarketingWallet	External	✓	onlyOwner
	OpenTrade	External	✓	onlyOwner
	getCirculatingSupply	Public		-
	transferToAddressETH	Private	✓	
	<Receive Ether>	External	Payable	-
	transfer	Public	✓	-
	transferFrom	Public	✓	-
	_transfer	Private	✓	

	_basicTransfer	Internal	✓	
	swapAndLiquify	Private	✓	lockTheSwap
	takeFee	Internal	✓	

Contract Flow
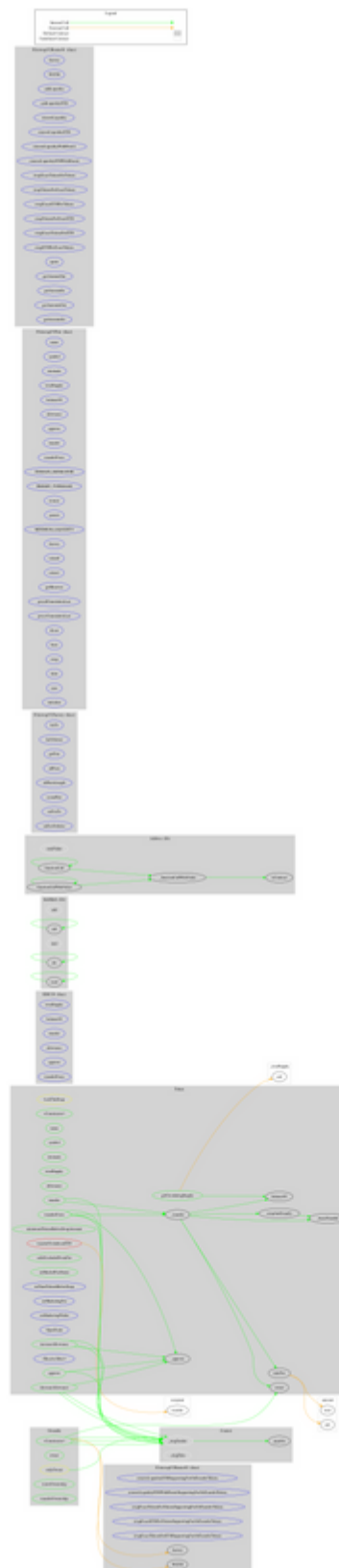
Domain Info

Domain Name	chatgptcoin.top
Registry Domain ID	D20221206G10001G_92481410-top
Creation Date	2022-12-06T14:58:11Z
Updated Date	2022-12-06T14:58:46Z
Registry Expiry Date	2023-12-06T14:58:11Z
Registrar WHOIS Server	whois.dnspod.cn
Registrar URL	https://www.dnspod.cn
Registrar	DNSPod, Inc.
Registrar IANA ID	1697

The domain was created 1 day 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

CGPT 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 10% fees.

Disclaimer

The information provided in this report does not constitute investment, financial or trading advice and you should not treat any of the document's content as such. This report may not be transmitted, disclosed, referred to or relied upon by any person for any purposes nor may copies be delivered to any other person other than the Company without Cyberscope's prior written consent. This report is not nor should be considered an "endorsement" or "disapproval" of any particular project or team. This report is not nor should be regarded as an indication of the economics or value of any "product" or "asset" created by any team or project that contracts Cyberscope to perform a security assessment. This document does not provide any warranty or guarantee regarding the absolute bug-free nature of the technology analyzed, nor do they provide any indication of the technologies proprietors' business, business model or legal compliance. This report should not be used in any way to make decisions around investment or involvement with any particular project. This report represents an extensive assessment process intending to help our customers increase the quality of their code while reducing the high level of risk presented by cryptographic tokens and blockchain technology.

Blockchain technology and cryptographic assets present a high level of ongoing risk Cyberscope's position is that each company and individual are responsible for their own due diligence and continuous security Cyberscope's goal is to help reduce the attack vectors and the high level of variance associated with utilizing new and consistently changing technologies and in no way claims any guarantee of security or functionality of the technology we agree to analyze. The assessment services provided by Cyberscope are subject to dependencies and are under continuing development. You agree that your access and/or use including but not limited to any services reports and materials will be at your sole risk on an as-is where-is and as-available basis Cryptographic tokens are emergent technologies and carry with them high levels of technical risk and uncertainty. The assessment reports could include false positives false negatives and other unpredictable results. The services may access and depend upon multiple layers of third parties.

About Cyberscope

Cyberscope is a blockchain cybersecurity company that was founded with the vision to make web3.0 a safer place for investors and developers. Since its launch, it has worked with thousands of projects and is estimated to have secured tens of millions of investors' funds.

Cyberscope is one of the leading smart contract audit firms in the crypto space and has built a high-profile network of clients and partners.

The Cyberscope team

https://www.cyberscope.io