Cyberscope

Audit Report

CryptoGotchies

November 2022

Type	BEP20
Network	BSC
Address	0x3902547fD2Ba8f0C74532B08fA7A929a73cEdf0B
Audited by	© cyberscope

Table of Contents

Contract Review

Contract Name	CryptoGotchies
Compiler Version	v0.8.13+commit.abaa5c0e
Optimization	200 runs
Licence	None
Explorer	https://bscscan.com/token/0x3902547fD2Ba8f0C74532B08fA7A929a73cEdf0B
Symbol	GOTCHI
Decimals	9
Total Supply	1,000,000,000
Domain	cryptogotchies.com

Source Files

Filename	**SHA256**
contract.sol	b8586e13551d273d94baa84df9d82ab027021730f8fd41e6b4ed5e1a69552cf8

Audit Updates

Initial Audit	23rd November 2022
Corrected	

Contract Analysis

● Critical ● Medium ● Minor / Informative ● Pass

Severity	Code	Description	Status
●	ST	Stops Transactions	Unresolved
●	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	Unresolved

ST - Stops Transactions

Criticality	critical
Location	contract.sol#L115,117
Status	Unresolved

Description

The contract owner has the authority to stop the sales for all users excluding the owner. The owner may take advantage of it by using an untrusted external contract.

```
require(!antibot.check(_to, _value, true));
...
require(!antibot.check(_from, _value, false));
```

Recommendation

Read more on the untrusted source section.

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.

BC - Blacklists Addresses

Criticality	critical
Location	contract.sol#L112
Status	Unresolved

Description

The contract owner has the authority to stop addresses from transactions. The owner may take advantage of it by calling the setisBlacklisted function.

```
require(!isBlacklisted[_from] && !isBlacklisted[_to], "Blacklisted address");
```

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 / Informative

Severity	Code	Description	Status
●	US	Untrusted Source	Unresolved
●	L02	State Variables could be Declared Constant	Unresolved
●	L04	Conformance to Solidity Naming Conventions	Unresolved

US - Untrusted Source

Criticality	critical
Location	contract.sol#L115,117
Status	Unresolved

Description

The contract uses an external contract in order to determine the transaction's flow. The external contract is untrusted. As a result it may produce security issues and harm the transactions.

```
require(!antibot.check(_to, _value, true));
...
require(!antibot.check(_from, _value, false));
```

Recommendation

The contract should use a trusted external source. A trusted source could be either a commonly recognized or an audited contract. The pointing addresses should not be able to change after the initialization.

L02 - State Variables could be Declared Constant

Criticality	minor / informative
Location	contract.sol#L83,85,84,82
Status	Unresolved

Description

Constant state variables should be declared constant to save gas.

```
symbol
decimals
totalSupply
name
```

Recommendation

Add the constant attribute to state variables that never change.

L04 - Conformance to Solidity Naming Conventions

Criticality	minor / informative
Location	contract.sol#L127,138,53,132
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.

```
_value
_to
WETH
_from
_spender
```

Recommendation

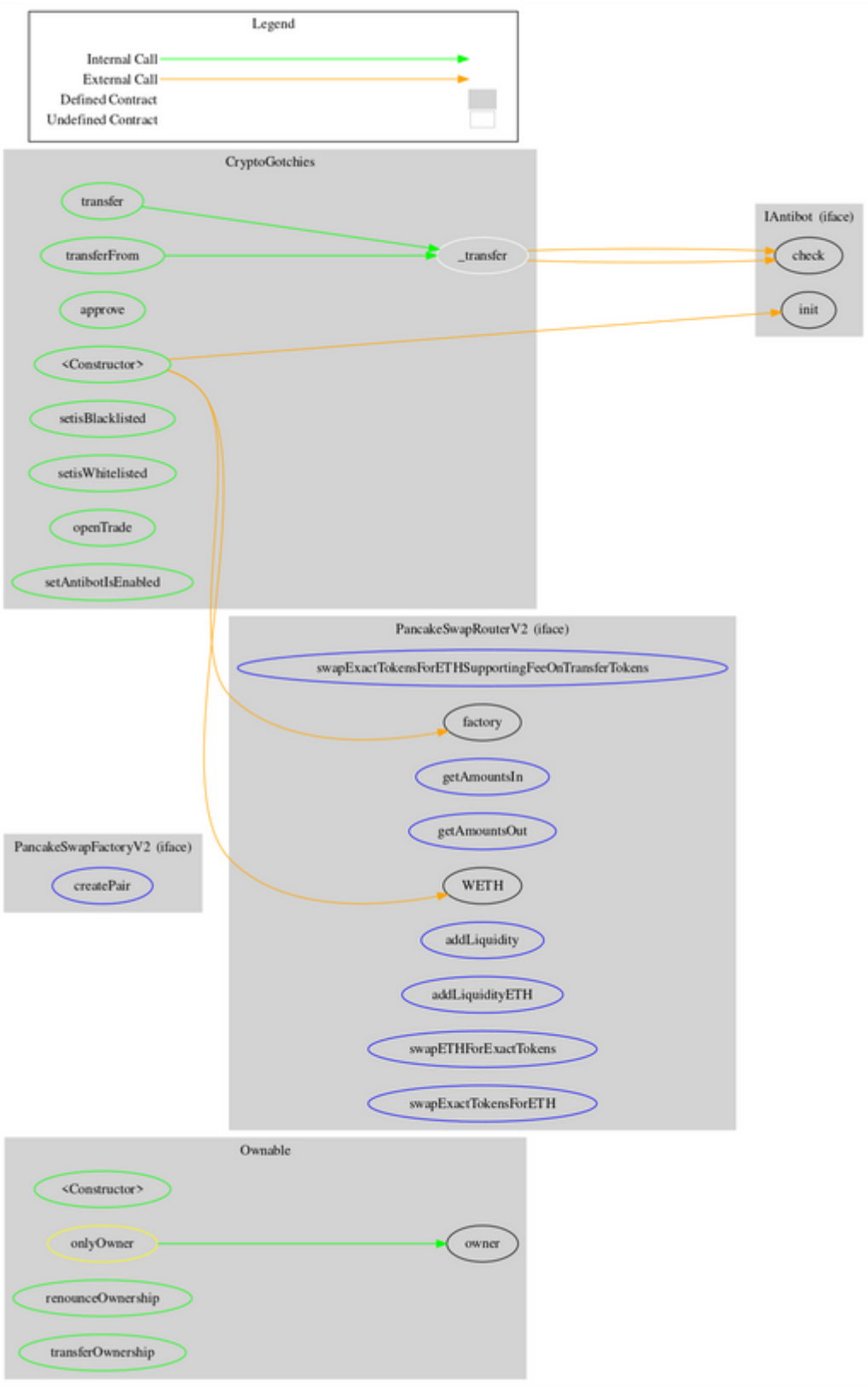
Follow the Solidity naming convention.
https://docs.soliditylang.org/en/v0.8.17/style-guide.html#naming-conventions.

Contract Functions

Contract	Type	Bases		
	Function Name	**Visibility**	**Mutability**	**Modifiers**
Ownable	Implementation			
	<Constructor>	Public	✓	-
	owner	Public		-
	renounceOwnership	Public	✓	onlyOwner
	transferOwnership	Public	✓	onlyOwner
PancakeSwap FactoryV2	Interface			
	createPair	External	✓	-
IAntibot	Interface			
	check	External		-
	init	External	✓	-
PancakeSwap RouterV2	Interface			
	swapExactTokensForETHSupporting FeeOnTransferTokens	External	✓	-
	factory	External		-
	getAmountsIn	External		-
	getAmountsOut	External		-
	WETH	External		-
	addLiquidity	External	✓	-
	addLiquidityETH	External	Payable	-
	swapETHForExactTokens	External	Payable	-
	swapExactTokensForETH	External	✓	-
CryptoGotchies	Implementation	Ownable		
	<Constructor>	Public	✓	-

	_transfer	Internal	✓	
	transfer	Public	✓	-
	approve	Public	✓	-
	transferFrom	Public	✓	-
	setisBlacklisted	Public	✓	onlyOwner
	setisWhitelisted	Public	✓	onlyOwner
	openTrade	Public	✓	onlyOwner
	setAntibotIsEnabled	Public	✓	onlyOwner

Contract Flow



Domain Info

Domain Name	cryptogotchies.com
Registry Domain ID	2731521519_DOMAIN_COM-VRSN
Creation Date	2022-10-12T12:46:10Z
Updated Date	2022-10-12T12:46:12Z
Registry Expiry Date	2025-10-12T12:46:10Z
Registrar WHOIS Server	whois.google.com
Registrar URL	https://domains.google.com
Registrar	Google LLC
Registrar IANA ID	895

The domain was created about 1 month before the creation of the audit. It will expire in almost 3 years.

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

Summary

There are some functions that can be abused by the owner like stopping transactions and massively blacklisting addresses. The contract can be converted into a honeypot and prevent users from selling if the owner abuses the admin functions. A multi-wallet signing pattern will provide security against potential hacks. Temporarily locking the contract or renouncing ownership will eliminate all the contract threats.

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