Cyberscope

Audit Report

Xocolatl Token

October 2022

Github	https://github.com/La-DAO/xocolatl-contracts
Commit	c367fec4a276bece4e580aca4a26e2147eb09643
Audited by	© cyberscope

Table of Contents

Table of Contents 1
Contract Review 3
Audit Updates 3
Source Files 4
Contract Roles 7
Contract Analysis 8
ST - Stops Transactions 9
Description 9
Recommendation 9
MT - Mints Tokens 10
Description 10
Recommendation 10
BT - Burns Tokens 11
Description 11
Recommendation 11
Contract Diagnostics 12
MC - Missing Check 13
Description 13
Recommendation 13
L04 - Conformance to Solidity Naming Conventions 14
Description 14
Recommendation 14
L05 - Unused State Variable 15
Description 15
Recommendation 15
Contract Functions 16

Contract Flow 24
Domain Info 25
Summary 26
Disclaimer 27
About Cyberscope 28

Contract Review

Contract Name	Xocolatl
Compiler Version	v0.8.13+commit.abaa5c0e
Optimization	0 runs
Github	https://github.com/La-DAO/xocolatl-contracts/blob/main/contracts/Xocolatl.sol
Commit	c367fec4a276bece4e580aca4a26e2147eb09643
Testing Deploy	https://testnet.bscscan.com/token/0xD8E170F8eA29434eE614d850A059c63D81bDb3E3
Decimals	18
Domain	https://xocolatl.club

Audit Updates

Initial Audit	21st October 2022
Corrected	

Source Files

Filename	SHA256
@openzeppelin/contracts-upgradeable/access/AccessControlUpgradeable.sol	86752f503f326b20940831c24fd682d21767235c88dfd5960a43a17c148c93ed
@openzeppelin/contracts-upgradeable/access/IAccessControlUpgradeable.sol	6d3fbd4566bc123db1ee6ba2a1b79544b572df9b9cc9be360ddb3244dd07c86b
@openzeppelin/contracts-upgradeable/interfaces/draft-IERC1822Upgradeable.sol	a94576fd98585c07b2a9725f7c89c910a3a1909a03f49ec2df465327c6a0ffc3
@openzeppelin/contracts-upgradeable/interfaces/IERC3156FlashBorrowerUpgradeable.sol	dad71710c2e3aa6a4e53812789957d113eaf4722369ad307d6d84bb1ef2b1b7f
@openzeppelin/contracts-upgradeable/interfaces/IERC3156FlashLenderUpgradeable.sol	8bf87e7d7c0050f909a2b645db1bd89cc051eb7c4192e1e5fc1047634cf946e7
@openzeppelin/contracts-upgradeable/proxy/beacon/IBeaconUpgradeable.sol	e0ac7115916f0dce0a8e80769694736f3e674bdc5b2e5853964c82004b1e1cc5
@openzeppelin/contracts-upgradeable/proxy/ERC1967/ERC1967UpgradeUpgradeable.sol	f6c1a8b4512e9cc0168278c2a634b184fd86b1e39c7c283bcf34fb154236fc5d
@openzeppelin/contracts-upgradeable/proxy/utils/Initializable.sol	cd823c76cbf5f5b6ef1bda565d58be66c843c37707cd93eb8fb5425deebd6756
@openzeppelin/contracts-upgradeable/proxy/utils/UUPSUpgradeable.sol	f2121091bdea42f19d25a6f043821eba21ccbecc64fa5d44b1574b0541e9a574

@openzeppelin/contracts-upgradeable/security/PausableUpgradeable.sol	c05b019a0b3bee8f3fac2da7c929f7d665b97d6d046aa35126615fff11205119
@openzeppelin/contracts-upgradeable/token/ERC20/ERC20Upgradeable.sol	36a6477c6263d9441dab59861e0ca97a201caf2843598af2a8e04e897a738c2f
@openzeppelin/contracts-upgradeable/token/ERC20/extensions/draft-ERC20PermitUpgradeable.sol	bbd217b34362e113b98b3deb562d5227ffaba52348702278c652b4a5d96d00ca
@openzeppelin/contracts-upgradeable/token/ERC20/extensions/draft-IERC20PermitUpgradeable.sol	b97515a88e75c313eacf0a27c9439ef371d86d4c2730d3b13076640942f813df
@openzeppelin/contracts-upgradeable/token/ERC20/extensions/ERC20BurnableUpgradeable.sol	ca660e828b0c4be205a9f56f3b87b91c1fa67cfd0f6e9dbd431faea7a6280d36
@openzeppelin/contracts-upgradeable/token/ERC20/extensions/ERC20FlashMintUpgradeable.sol	5f31a3580bd620b7cfd4ca8c04f1f5d09a1df68a8253540d50aba8cf798d1a21
@openzeppelin/contracts-upgradeable/token/ERC20/extensions/IERC20MetadataUpgradeable.sol	68bcca423fc72ec9625e219c9e36306c726a347e43f3711467c579bd3f6500c8
@openzeppelin/contracts-upgradeable/token/ERC20/IERC20Upgradeable.sol	4e09a7479aa3e7c313f8fc141c4c8fc04e0abfeb8754615ef7d78ec94c298b07
@openzeppelin/contracts-upgradeable/utils/AddressUpgradeable.sol	35fb271561f3dc72e91b3a42c6e40c2bb2e788cd8ca58014ac43f6198b8d32ca
@openzeppelin/contracts-upgradeable/utils/ContextUpgradeable.sol	5fb301961e45cb482fe4e05646d2f529aa449fe0e90c6671475d6a32356fa2d4
@openzeppelin/contracts-upgradeable/utils/CountersUpgradeable.sol	5c1ac829a429b0c2ca9b4c9ed8b78d412320e9175e45f088c4e9056ef95fbf21

@openzeppelin/contracts-upgradeable/utils/cryptography/draft-EIP712Upgradeable.sol	798dd77cf98881ad27047953b5162f39ae8cc1420f0c0e8570e9342568ab8e9b
@openzeppelin/contracts-upgradeable/utils/cryptography/ECDSAUpgradeable.sol	227bd4d1c0a0eb3428b44e4570bf34d87e30dcfed49e9c7a6079f27b5d2c1b19
@openzeppelin/contracts-upgradeable/utils/introspection/ERC165Upgradeable.sol	fd84e5284eccc479268f0ef36b830019d4f7999ceb7959430d8d8d9e602dd4ef
@openzeppelin/contracts-upgradeable/utils/introspection/IERC165Upgradeable.sol	a39bc026ad6214e9ecd526bd4a1ddf9862d80bd4a9d0d031d9bafa4c3c147c0b
@openzeppelin/contracts-upgradeable/utils/StorageSlotUpgradeable.sol	05b696b46ca1be28e19dfba65ea71c3b3615bd39d19bfd8212864a16c54870fd
@openzeppelin/contracts-upgradeable/utils/StringsUpgradeable.sol	e7b950eee23563e23989a3b51a1456614a1838084eef1fad04eb2be0bc280f48
contracts/Xocolatl.sol	d8de9297d33207bbf0908dbbe977721e804bd02da5f6406ebe5ca2e0c3351e63

Contract Roles

The contract has 4 roles:

- DEFAULT_ADMIN_ROLE
- PAUSER_ROLE
- MINTER_ROLE
- UPGRADER_ROLE

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	Unresolved
●	ULTW	Transfers Liquidity to Team Wallet	Passed
●	MT	Mints Tokens	Unresolved
●	BT	Burns Tokens	Unresolved
●	BC	Blacklists Addresses	Passed

ST - Stops Transactions

Criticality	minor / informative
Location	contract.sol#L152
Status	Unresolved

Description

The contract owner has the authority to stop the transactions for all users excluding the owner. The owner may take advantage of it by calling `pause` function.

```
function _beforeTokenTransfer(
        address from,
        address to,
        uint256 amount
    ) internal override whenNotPaused {
        super._beforeTokenTransfer(from, to, amount);
    }
```

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.

MT - Mints Tokens

Criticality	minor / informative
Location	contract.sol#L79
Status	Unresolved

Description

The contract owner has the authority to mint tokens. The owner may take advantage of it by calling the mint function. As a result, the contract tokens will be highly inflated.

```
function mint(address to, uint256 amount)
        public
        onlyRole(MINTER_ROLE)
        whenNotPaused
    {
        _mint(to, amount);
    }
```

Recommendation

The owner should carefully manage the credentials of the owner’s account. We advised considering an extra-strong security mechanism that the actions may be quarantined by many users instead of one. The owner could also renounce the contract ownership for a period of time or pass the access to the zero address.

BT - Burns Tokens

Criticality	minor / informative
Location	contract.sol#L91
Status	Unresolved

Description

The contract owner has the authority to burn tokens from a specific address. The owner may take advantage of it by calling the burn function. As a result, the targeted contract address will lose the corresponding tokens.

```
function burn(address to, uint256 amount) public onlyRole(MINTER_ROLE) {
        _burn(to, amount);
    }
```

Recommendation

The owner should carefully manage the credentials of the owner’s account. We advised considering an extra-strong security mechanism that the actions may be quarantined by many users instead of one. The owner could also renounce the contract ownership for a period of time or pass the access to the zero address.

Contract Diagnostics

🔴 Critical 🟠 Medium ● Minor / Informative

Severity	Code	Description	Status
●	MC	Missing Check	Unresolved
●	L04	Conformance to Solidity Naming Conventions	Unresolved
●	L05	Unused State Variable	Unresolved

MC - Missing Check

Criticality	minor / informative
Location	contract.sol#L137
Status	Unresolved

Description

The variable flashFeeReceiver can be set to zero address.

```
function setFlashFeeReceiver(address _flashFeeReceiverAddr)
        public
        onlyRole(DEFAULT_ADMIN_ROLE)
    {
        flashFeeReceiver = _flashFeeReceiverAddr;
        emit FlashFeeReceiverChanged(_flashFeeReceiverAddr);
    }
```

Recommendation

The contract should properly check the variables according to the required specifications. The variable flashFeeReceiver should not be zero.

L04 - Conformance to Solidity Naming Conventions

Criticality	minor / informative
Location	contracts/Xocolatl.sol#L137,121,44
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.

```
_flashFeeReceiverAddr
_newFlashFee
_flashFee
```

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 / informative
Location	contracts/Xocolatl.sol#L13
Status	Unresolved

Description

There are segments that contain unused state variables.

```
Xocolatl
```

Recommendation

Remove unused state variables.

Contract Functions

Contract	Type	Bases		
	Function Name	Visibility	Mutability	Modifiers
AccessControlUpgradeable	Implementation	Initializable, ContextUpgradeable, IAccessControlUpgradeable, ERC165Upgradeable		
	__AccessControl_init	Internal	✓	onlyInitializing
	__AccessControl_init_unchained	Internal	✓	onlyInitializing
	supportsInterface	Public		-
	hasRole	Public		-
	_checkRole	Internal		
	_checkRole	Internal		
	getRoleAdmin	Public		-
	grantRole	Public	✓	onlyRole
	revokeRole	Public	✓	onlyRole
	renounceRole	Public	✓	-
	_setupRole	Internal	✓	
	_setRoleAdmin	Internal	✓	
	_grantRole	Internal	✓	
	_revokeRole	Internal	✓	
IAccessControlUpgradeable	Interface			
	hasRole	External		-
	getRoleAdmin	External		-
	grantRole	External	✓	-
	revokeRole	External	✓	-
	renounceRole	External	✓	-

IERC1822ProxiableUpgradeable	Interface			
	proxiableUUID	External		-
IERC3156FlashBorrowerUpgradeable	Interface			
	onFlashLoan	External	✓	-
IERC3156FlashLenderUpgradeable	Interface			
	maxFlashLoan	External		-
	flashFee	External		-
	flashLoan	External	✓	-
IBeaconUpgradeable	Interface			
	implementation	External		-
ERC1967UpgradeUpgradeable	Implementation	Initializable		
	__ERC1967Upgrade_init	Internal	✓	onlyInitializing
	__ERC1967Upgrade_init_unchained	Internal	✓	onlyInitializing
	_getImplementation	Internal		
	_setImplementation	Private	✓	
	_upgradeTo	Internal	✓	
	_upgradeToAndCall	Internal	✓	
	_upgradeToAndCallUUPS	Internal	✓	
	_getAdmin	Internal		
	_setAdmin	Private	✓	
	_changeAdmin	Internal	✓	
	_getBeacon	Internal		
	_setBeacon	Private	✓	
	_upgradeBeaconToAndCall	Internal	✓	
	_functionDelegateCall	Private	✓	

Initializable	Implementation			
	_disableInitializers	Internal	✓	
UUPSUpgradeable	Implementation	Initializable, IERC1822ProxiableUpgradeable, ERC1967UpgradeUpgradeable		
	__UUPSUpgradeable_init	Internal	✓	onlyInitializing
	__UUPSUpgradeable_init_unchained	Internal	✓	onlyInitializing
	proxiableUUID	External		notDelegated
	upgradeTo	External	✓	onlyProxy
	upgradeToAndCall	External	Payable	onlyProxy
	_authorizeUpgrade	Internal	✓	
PausableUpgradeable	Implementation	Initializable, ContextUpgradeable		
	__Pausable_init	Internal	✓	onlyInitializing
	__Pausable_init_unchained	Internal	✓	onlyInitializing
	paused	Public		-
	_requireNotPaused	Internal		
	_requirePaused	Internal		
	_pause	Internal	✓	whenNotPaused
	_unpause	Internal	✓	whenPaused
ERC20Upgradeable	Implementation	Initializable, ContextUpgradeable, IERC20Upgradeable, IERC20MetadataUpgradeable		
	__ERC20_init	Internal	✓	onlyInitializing
	__ERC20_init_unchained	Internal	✓	onlyInitializing

	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	✓	
	_spendAllowance	Internal	✓	
	_beforeTokenTransfer	Internal	✓	
	_afterTokenTransfer	Internal	✓	
ERC20PermitUpgradeable	Implementation	Initializable, ERC20Upgradeable, IERC20PermitUpgradeable, EIP712Upgradeable		
	__ERC20Permit_init	Internal	✓	onlyInitializing
	__ERC20Permit_init_unchained	Internal	✓	onlyInitializing
	permit	Public	✓	-
	nonces	Public		-
	DOMAIN_SEPARATOR	External		-
	_useNonce	Internal	✓	
IERC20PermitUpgradeable	Interface			
	permit	External	✓	-

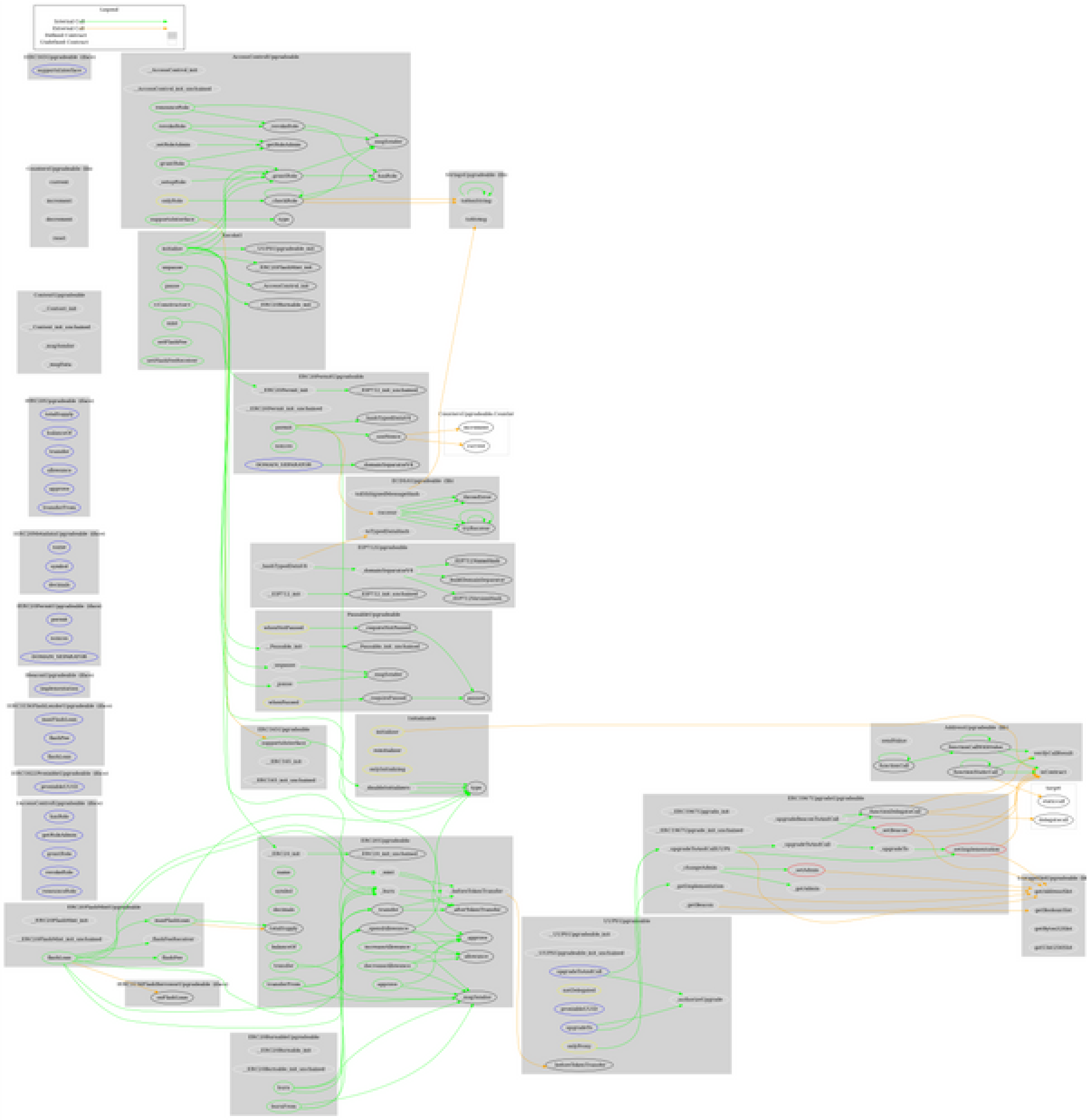
	nonces	External		-
	DOMAIN_SEPARATOR	External		-
ERC20BurnableUpgradeable	Implementation	Initializable, ContextUpgradeable, ERC20Upgradeable		
	__ERC20Burnable_init	Internal	✓	onlyInitializing
	__ERC20Burnable_init_unchained	Internal	✓	onlyInitializing
	burn	Public	✓	-
	burnFrom	Public	✓	-
ERC20FlashMintUpgradeable	Implementation	Initializable, ERC20Upgradeable, IERC3156FlashLenderUpgradeable		
	__ERC20FlashMint_init	Internal	✓	onlyInitializing
	__ERC20FlashMint_init_unchained	Internal	✓	onlyInitializing
	maxFlashLoan	Public		-
	flashFee	Public		-
	_flashFeeReceiver	Internal		
	flashLoan	Public	✓	-
IERC20MetadataUpgradeable	Interface	IERC20Upgradeable		
	name	External		-
	symbol	External		-
	decimals	External		-
IERC20Upgradeable	Interface			
	totalSupply	External		-
	balanceOf	External		-
	transfer	External	✓	-
	allowance	External		-

	approve	External	✓	-
	transferFrom	External	✓	-
AddressUpgradeable	Library			
	isContract	Internal		
	sendValue	Internal	✓	
	functionCall	Internal	✓	
	functionCall	Internal	✓	
	functionCallWithValue	Internal	✓	
	functionCallWithValue	Internal	✓	
	functionStaticCall	Internal		
	functionStaticCall	Internal		
	verifyCallResult	Internal		
ContextUpgradeable	Implementation	Initializable		
	__Context_init	Internal	✓	onlyInitializing
	__Context_init_unchained	Internal	✓	onlyInitializing
	_msgSender	Internal		
	_msgData	Internal		
CountersUpgradeable	Library			
	current	Internal		
	increment	Internal	✓	
	decrement	Internal	✓	
	reset	Internal	✓	
EIP712Upgradeable	Implementation	Initializable		
	__EIP712_init	Internal	✓	onlyInitializing
	__EIP712_init_unchained	Internal	✓	onlyInitializing
	_domainSeparatorV4	Internal		
	_buildDomainSeparator	Private		
	_hashTypedDataV4	Internal		

	_EIP712NameHash	Internal		
	_EIP712VersionHash	Internal		
ECDSAUpgradeable	Library			
	_throwError	Private		
	tryRecover	Internal		
	recover	Internal		
	tryRecover	Internal		
	recover	Internal		
	tryRecover	Internal		
	recover	Internal		
	toEthSignedMessageHash	Internal		
	toEthSignedMessageHash	Internal		
	toTypedDataHash	Internal		
ERC165Upgradeable	Implementation	Initializable, IERC165Upgradeable		
	__ERC165_init	Internal	✓	onlyInitializing
	__ERC165_init_unchained	Internal	✓	onlyInitializing
	supportsInterface	Public		-
IERC165Upgradeable	Interface			
	supportsInterface	External		-
StorageSlotUpgradeable	Library			
	getAddressSlot	Internal		
	getBooleanSlot	Internal		
	getBytes32Slot	Internal		
	getUint256Slot	Internal		
StringsUpgradeable	Library			
	toString	Internal		

	toHexString	Internal		
	toHexString	Internal		
	toHexString	Internal		
Xocolatl	Implementation	Initializable, ERC20Upgradeable, ERC20BurnableUpgradeable, PausableUpgradeable, AccessControlUpgradeable, ERC20PermitUpgradeable, ERC20FlashMintUpgradeable, UUPSUpgradeable		
	<Constructor>	Public	✓	-
	initialize	Public	✓	initializer
	pause	Public	✓	onlyRole
	unpause	Public	✓	onlyRole
	mint	Public	✓	onlyRole whenNotPaused
	burn	Public		-
	burn	Public	✓	onlyRole
	maxFlashLoan	Public		-
	flashFee	Public		-
	setFlashFee	Public	✓	onlyRole
	setFlashFeeReceiver	Public	✓	onlyRole
	_flashFeeReceiver	Internal		
	_beforeTokenTransfer	Internal	✓	whenNotPaused
	_authorizeUpgrade	Internal	✓	onlyRole

Contract Flow



Domain Info

Domain Name	xocolatl.club
Registry Domain ID	D017C2E7D305043B48BB9BAC3CE267A07-GDREG
Creation Date	2022-09-09T07:58:44Z
Updated Date	2022-09-14T07:58:44Z
Registry Expiry Date	2023-09-09T07:58:44Z
Registrar WHOIS Server	whois.opensrs.net
Registrar URL	www.opensrs.com
Registrar	Tucows Domains Inc.
Registrar IANA ID	69

The domain was created about 1 month before the creation of the audit. It will expire in 11 months.

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.

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