Cyberscope

Audit Report

Tectum Emission Token

March 2023

Network	ETH
Address	0x7e55ccB0bCe9A9094aE5cf75EF71b3275B45658A
Audited by	© cyberscope

Table of Contents

Review

Contract Name	Tettoken
Compiler Version	v0.4.17+commit.bdeb9e52
Optimization	200 runs
Explorer	https://etherscan.io/address/0x7e55ccb0bce9a9094ae5cf75ef71b3275b45658a
Address	0x7e55ccb0bce9a9094ae5cf75ef71b3275b45658a
Network	ETH
Symbol	TET
Decimals	4
Total Supply	10,000,000

Audit Updates

Initial Audit	09 Mar 2023 https://github.com/cyberscope-io/audits/tree/main/2-tet/v1/audit.pdf
Corrected Phase 2	14 Mar 2023 https://github.com/cyberscope-io/audits/tree/main/2-tet/v2/audit.pdf
Corrected Phase 3	17 Mar 2023

Source Files

Filename	SHA256
Token.sol	c577af6627b5f93044b6a233d29830788d023662f7da0242469d769c662611cc

Findings Breakdown

Critical	0
Medium	0
Minor / Informative	2

Severity	Unresolved	Acknowledged	Resolved	Other
Critical	0	0	0	0
Medium	0	0	0	0
Minor / Informative	2	0	0	0

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

Diagnostics

Critical Medium Minor / Informative

Severity	Code	Description	Status
●	RII	Redundant Inheritance Issue	Unresolved
●	L04	Conformance to Solidity Naming Conventions	Unresolved

RII - Redundant Inheritance Issue

Criticality	Minor / Informative
Location	Tettoken.sol#L218
Status	Unresolved

Description

The contract includes the Pausable and BlackList contracts, but it does not make use of their functionalities.

```
contract BlackList is Ownable, BasicToken {
```

Recommendation

The Inheritance of unused contracts in the contract implementation should be avoided. It is recommended to remove unused contracts.

L04 - Conformance to Solidity Naming Conventions

Criticality	Minor / Informative
Location	Token.sol#L20,49,84,122,131,140,149,158,168,169,182,183,195,204,215,216,228,248,249,255,388,399,413,432
Status	Unresolved

Description

The Solidity style guide is a set of guidelines for writing clean and consistent Solidity code. Adhering to a style guide can help improve the readability and maintainability of the Solidity code, making it easier for others to understand and work with.

The followings are a few key points from the Solidity style guide:

1. Use camelCase for function and variable names, with the first letter in lowercase (e.g., myVariable, updateCounter).
2. Use PascalCase for contract, struct, and enum names, with the first letter in uppercase (e.g., MyContract, UserStruct, ErrorEnum).
3. Use uppercase for constant variables and enums (e.g., MAX_VALUE, ERROR_CODE).
4. Use indentation to improve readability and structure.
5. Use spaces between operators and after commas.
6. Use comments to explain the purpose and behavior of the code.
7. Keep lines short (around 120 characters) to improve readability.

```
function WETH() external pure returns (address);
uint256 private constant _totalSupply = 1e7 * 1e18
address public TreasuryWallet = 0x74Adf47aD22a9C95EE58A6D956FA58924D697E0F
address _newTreasury
uint256 _mb
uint256 _ms
uint256 _mt
uint256 _mx
uint256 _lpTax
uint256 _TreasuryTax
uint256 _sc
uint256 _db
uint256 _newAmount
address _wallet

...
```

Recommendation

By following the Solidity naming convention guidelines, the codebase increased the readability, maintainability, and makes it easier to work with.

Find more information on the Solidity documentation

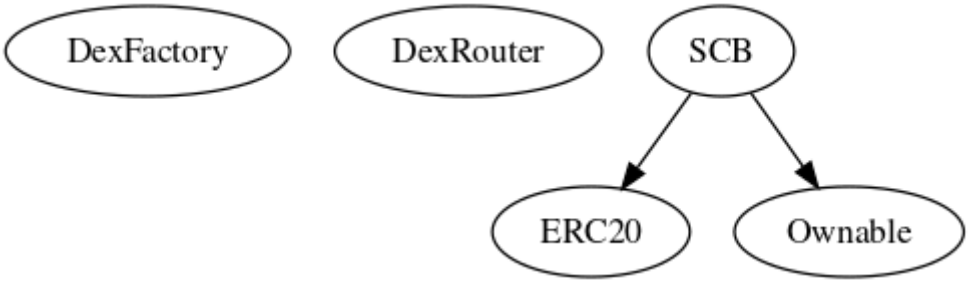
https://docs.soliditylang.org/en/v0.8.17/style-guide.html#naming-convention.

Functions Analysis

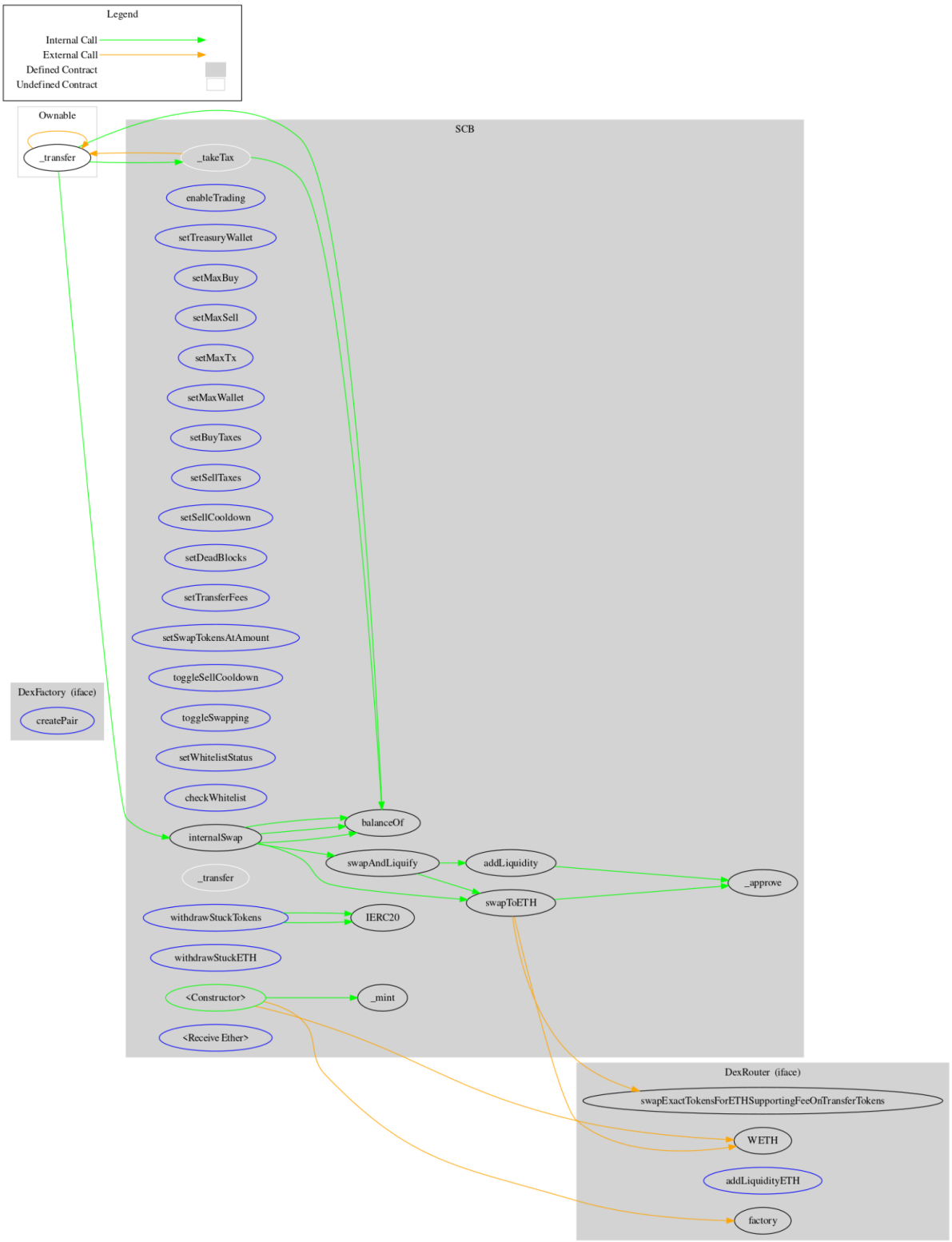
Contract	Type	Bases		
	Function Name	**Visibility**	**Mutability**	**Modifiers**
DexFactory	Interface			
	createPair	External	✓	-
DexRouter	Interface			
	factory	External		-
	WETH	External		-
	addLiquidityETH	External	Payable	-
	swapExactTokensForETHSupportingFeeOnTransferTokens	External	✓	-
SCB	Implementation	ERC20, Ownable		
		Public	✓	ERC20
	enableTrading	External	✓	onlyOwner
	setTreasuryWallet	External	✓	onlyOwner
	setMaxBuy	External	✓	onlyOwner
	setMaxSell	External	✓	onlyOwner
	setMaxTx	External	✓	onlyOwner
	setMaxWallet	External	✓	onlyOwner
	setBuyTaxes	External	✓	onlyOwner

	setSellTaxes	External	✓	onlyOwner
	setSellCooldown	External	✓	onlyOwner
	setDeadBlocks	External	✓	onlyOwner
	setTransferFees	External	✓	onlyOwner
	setSwapTokensAtAmount	External	✓	onlyOwner
	toggleSellCooldown	External	✓	onlyOwner
	toggleSwapping	External	✓	onlyOwner
	setWhitelistStatus	External	✓	onlyOwner
	checkWhitelist	External		-
	_takeTax	Internal	✓	
	_transfer	Internal	✓	
	internalSwap	Internal	✓	
	swapAndLiquify	Internal	✓	
	swapToETH	Internal	✓	
	addLiquidity	Private	✓	
	withdrawStuckETH	External	✓	onlyOwner
	withdrawStuckTokens	External	✓	onlyOwner
		External	Payable	-

Inheritance Graph



Flow Graph


Legend
Internal Call
External Call
Defined Contract
Undefined Contract
Ownable
_transfer
SCB
_takeTax
enableTrading
setTreasuryWallet
setMaxBuy
setMaxSell
setMaxTx
setMaxWallet
setBuyTaxes
setSellTaxes
setSellCooldown
setDeadBlocks
setTransferFees
setSwapTokensAtAmount
toggleSellCooldown
toggleSwapping
setWhitelistStatus
checkWhitelist
internalSwap
_transfer
withdrawStuckTokens
withdrawStuckETH
<Constructor>
<Receive Ether>
balanceOf
swapAndLiquify
addLiquidity
swapToETH
_approve
IERC20
_mint
DexFactory (iface)
createPair
DexRouter (iface)
swapExactTokensForETHSupportingFeeOnTransferTokens
WETH
addLiquidityETH
factory

Summary

Tectum Emission Token contract implements a token mechanism. This audit investigates security issues, business logic concerns, and potential improvements. Tectum Emission Token is an interesting project that has a friendly and growing community. The contract had a mint method that could only be executed once. Since the owner executed this method, then the contract cannot mint tokens anymore. The Smart Contract analysis reported no compiler errors 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

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