Cyberscope

Audit Report

Spectre

October 2024

Network	ETH
Address	0xB29E475B69F843046A757747943C00DCe8a3d982
Audited by	© cyberscope

Analysis

Critical Medium Minor / Informative Pass

Severity	Code	Description	Status
●	ST	Stops Transactions	Passed
●	OTUT	Transfers User's Tokens	Passed
●	ELFM	Exceeds Fees Limit	Passed
●	MT	Mints Tokens	Passed
●	BT	Burns Tokens	Passed
●	BC	Blacklists Addresses	Passed

Diagnostics

Critical Medium Minor / Informative

Severity	Code	Description	Status
●	AOI	Arithmetic Operations Inconsistency	Acknowledged
●	MEE	Missing Events Emission	Acknowledged
●	NWES	Nonconformity with ERC-20 Standard	Acknowledged
●	PLPI	Potential Liquidity Provision Inadequacy	Unresolved
●	PTRP	Potential Transfer Revert Propagation	Acknowledged
●	RRA	Redundant Repeated Approvals	Acknowledged
●	RSML	Redundant SafeMath Library	Acknowledged
●	RSRS	Redundant SafeMath Require Statement	Acknowledged
●	UTT	Unverified Token Transfer	Acknowledged
●	L04	Conformance to Solidity Naming Conventions	Acknowledged

Table of Contents

Risk Classification

The criticality of findings in Cyberscope's smart contract audits is determined by evaluating multiple variables. The two primary variables are:

1. **Likelihood of Exploitation**: This considers how easily an attack can be executed, including the economic feasibility for an attacker.
2. **Impact of Exploitation**: This assesses the potential consequences of an attack, particularly in terms of the loss of funds or disruption to the contract's functionality.

Based on these variables, findings are categorized into the following severity levels:

1. **Critical**: Indicates a vulnerability that is both highly likely to be exploited and can result in significant fund loss or severe disruption. Immediate action is required to address these issues.
2. **Medium**: Refers to vulnerabilities that are either less likely to be exploited or would have a moderate impact if exploited. These issues should be addressed in due course to ensure overall contract security.
3. **Minor**: Involves vulnerabilities that are unlikely to be exploited and would have a minor impact. These findings should still be considered for resolution to maintain best practices in security.
4. **Informative**: Points out potential improvements or informational notes that do not pose an immediate risk. Addressing these can enhance the overall quality and robustness of the contract.

Severity	Likelihood / Impact of Exploitation
Critical	Highly Likely / High Impact
Medium	Less Likely / High Impact or Highly Likely/ Lower Impact
Minor / Informative	Unlikely / Low to no Impact

Review

Contract Name	SPECTRE
Compiler Version	v0.8.27+commit.40a35a09
Optimization	200 runs
Explorer	https://etherscan.io/address/0xb29e475b69f843046a757747943c00dce8a3d982
Address	0xb29e475b69f843046a757747943c00dce8a3d982
Network	ETH
Symbol	SPCTR
Decimals	9
Total Supply	100,000,000,000

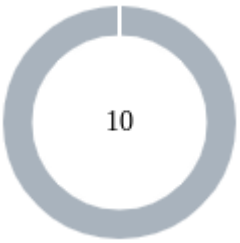
Audit Updates

Initial Audit	16 Sep 2024 https://github.com/cyberscope-io/audits/blob/main/spctr/v1/audit.pdf
Corrected Phase 2	02 Oct 2024

Source Files

Filename	SHA256
SPECTRE.sol	c8460947f96c24ef96b09e352bfff90b07c1b45d311ed531c8f554e442738e04

Findings Breakdown



Critical	0
Medium	0
Minor / Informative	10

Severity	Unresolved	Acknowledged	Resolved	Other
Critical	0	0	0	0
Medium	0	0	0	0
Minor / Informative	1	9	0	0

AOI - Arithmetic Operations Inconsistency

Criticality	Minor / Informative
Location	SPECTRE.sol#L287,328,333,341,352,366,367,395,398,399,400
Status	Acknowledged

Description

The contract uses both the SafeMath library and native arithmetic operations. The SafeMath library is commonly used to mitigate vulnerabilities related to integer overflow and underflow issues. However, it was observed that the contract also employs native arithmetic operators (such as +, -, *, /) in certain sections of the code.

The combination of SafeMath library and native arithmetic operations can introduce inconsistencies and undermine the intended safety measures. This discrepancy creates an inconsistency in the contract's arithmetic operations, increasing the risk of unintended consequences such as inconsistency in error handling, or unexpected behavior.

```
if (taxAmount > 0) {
    _balances[address(this)] =
_balances[address(this)].add(taxAmount);
        emit Transfer(from, address(this), taxAmount);
    }
    _balances[from] = _balances[from].sub(amount);
    _balances[to] = _balances[to].add(amount.sub(taxAmount));
    emit Transfer(from, to, amount.sub(taxAmount));
```

```
if (_buyCount <= (_reduceBuyTaxAt + _reduceSellTaxAt)) {...}
```

Recommendation

To address this finding and ensure consistency in arithmetic operations, it is recommended to standardize the usage of arithmetic operations throughout the contract. The contract should be modified to either exclusively use SafeMath library functions or entirely rely on native arithmetic operations, depending on the specific requirements and design considerations. This consistency will help maintain the contract's integrity and mitigate potential vulnerabilities arising from inconsistent arithmetic operations.

MEE - Missing Events Emission

Criticality	Minor / Informative
Location	SPECTRE.sol#L476
Status	Acknowledged

Description

The contract performs actions and state mutations from external methods that do not result in the emission of events. Emitting events for significant actions is important as it allows external parties, such as wallets or dApps, to track and monitor the activity on the contract. Without these events, it may be difficult for external parties to accurately determine the current state of the contract.

```
function reduceSpectreSellTaxFee(uint256 _newFee) external
onlySpectreWallet {
        require(_newFee <= _finalSellTax, "Invalid fee: New fee
must be lower or equal to current sell tax.");
        _finalSellTax = _newFee;
}
```

Recommendation

It is recommended to include events in the code that are triggered each time a significant action is taking place within the contract. These events should include relevant details such as the user's address and the nature of the action taken. By doing so, the contract will be more transparent and easily auditable by external parties. It will also help prevent potential issues or disputes that may arise in the future.

NWES - Nonconformity with ERC-20 Standard

Criticality	Minor / Informative
Location	SPECTRE.sol#L306
Status	Acknowledged

Description

The contract is not fully conforming to the ERC20 Standard. Specifically, according to the standard, transfers of 0 values must be treated as normal transfers and fire the Transfer event. However the contract implements, a conditional check that prohibits transfers of 0 values.

This discrepancy between the contract's implementation and the ERC20 standard may lead to inconsistencies and incompatibilities with other contracts.

```
function _transfer(address from,address to,int256 amount)
private {
...
require(amount > 0, "Transfer amount must be greater than
zero");
...
}
```

Recommendation

The incorrect implementation of the ERC20 standard could potentially lead to problems when interacting with the contract, as other contracts or applications that expect the ERC20 interface may not behave as expected. The team is advised to review and revise the implementation of the transfer mechanism to ensure full compliance with the ERC20 standard. https://eips.ethereum.org/EIPS/eip-20.

PLPI - Potential Liquidity Provision Inadequacy

Criticality	Minor / Informative
Location	SPECTRE.sol#L407
Status	Unresolved

Description

The contract operates under the assumption that liquidity is consistently provided to the pair between the contract's token and the native currency. However, there is a possibility that liquidity is provided to a different pair. This inadequacy in liquidity provision in the main pair could expose the contract to risks. Specifically, during eligible transactions, where the contract attempts to swap tokens with the main pair, a failure may occur if liquidity has been added to a pair other than the primary one. Consequently, transactions triggering the swap functionality will result in a revert.

```
function swapTokensForEth(uint256 tokenAmount) private
lockTheSwap {
        address[] memory path = new address[](2);
        path[0] = address(this);
        path[1] = uniswapV2Router.WETH();
        _approve(address(this), address(uniswapV2Router),
tokenAmount);

uniswapV2Router.swapExactTokensForETHSupportingFeeOnTransferTok
ens(
            tokenAmount,
            0,
            path,
            address(this),
            block.timestamp
        );
}
```

Recommendation

The team is advised to implement a runtime mechanism to check if the pair has adequate liquidity provisions. This feature allows the contract to omit token swaps if the pair does not have adequate liquidity provisions, significantly minimizing the risk of potential failures.

Furthermore, the team could ensure the contract has the capability to switch its active pair in case liquidity is added to another pair.

Additionally, the contract could be designed to tolerate potential reverts from the swap functionality, especially when it is a part of the main transfer flow. This can be achieved by executing the contract's token swaps in a non-reversible manner, thereby ensuring a more resilient and predictable operation.

PTRP - Potential Transfer Revert Propagation

Criticality	Minor / Informative
Location	SPECTRE.sol#L427
Status	Acknowledged

Description

The contract sends funds to a `_spectreMultiSegWallet` as part of the transfer flow. This address can either be a wallet address or a contract. If the address belongs to a contract then it may revert from incoming payment. As a result, the error will propagate to the token's contract and revert the transfer.

```
function sendETHToMultiSeg(uint256 amount) private {
        (bool success, ) = _spectreMultiSegWallet.call{value:
amount}("");
        if (!success) {
            _spectreWallet.transfer(amount);
        }
}
```

Recommendation

The contract should tolerate the potential revert from the underlying contracts when the interaction is part of the main transfer flow. This could be achieved by not allowing set contract addresses or by sending the funds in a non-revertable way.

RRA - Redundant Repeated Approvals

Criticality	Minor / Informative
Location	SPECTRE.sol#L407
Status	Acknowledged

Description

The contract is designed to `approve` token transfers during the contract's operation by calling the _approve function before specific operations. This approach results in additional gas costs since the approval process is repeated for every operation execution, leading to inefficiencies and increased transaction expenses.

```
function swapTokensForEth(uint256 tokenAmount) private
lockTheSwap {
        address[] memory path = new address[](2);
        path[0] = address(this);
        path[1] = uniswapV2Router.WETH();
        _approve(address(this), address(uniswapV2Router),
tokenAmount);

uniswapV2Router.swapExactTokensForETHSupportingFeeOnTransferTok
ens(
            tokenAmount,
            0,
            path,
            address(this),
            block.timestamp
        );
}
```

Recommendation

Since the approved address is a trusted third-party source, it is recommended to optimize the contract by approving the maximum amount of tokens once in the initial set of the variable, rather than before each operation. This change will reduce the overall gas consumption and improve the efficiency of the contract.

RSML - Redundant SafeMath Library

Criticality	Minor / Informative
Location	SPECTRE.sol
Status	Acknowledged

Description

SafeMath is a popular Solidity library that provides a set of functions for performing common arithmetic operations in a way that is resistant to integer overflows and underflows.

Starting with Solidity versions that are greater than or equal to 0.8.0, the arithmetic operations revert to underflow and overflow. As a result, the native functionality of the Solidity operations replaces the SafeMath library. Hence, the usage of the SafeMath library adds complexity, overhead and increases gas consumption unnecessarily in cases where the explanatory error message is not used.

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

Recommendation

The team is advised to remove the SafeMath library in cases where the revert error message is not used. Since the version of the contract is greater than `0.8.0` then the pure Solidity arithmetic operations produce the same result.

If the previous functionality is required, then the contract could exploit the `unchecked { ... }` statement.

Read more about the breaking change on https://docs.soliditylang.org/en/stable/080-breaking-changes.html#solidity-v0-8-0-breaking-changes.

RSRS - Redundant SafeMath Require Statement

Criticality	Minor / Informative
Location	SPECTRE.sol#L48
Status	Acknowledged

Description

The contract utilizes a `require` statement within the `add` function aiming to prevent overflow errors. This function is designed based on the SafeMath library's principles. In Solidity version 0.8.0 and later, arithmetic operations revert on overflow and underflow, making the overflow check within the function redundant. This redundancy could lead to extra gas costs and increased complexity without providing additional security.

```
function add(uint256 a, uint256 b) internal pure returns
(uint256) {
      uint256 c = a + b;
      require(c >= a, "SafeMath: addition overflow");
      return c;
}
```

Recommendation

It is recommended to remove the `require` statement from the add function since the contract is using a Solidity pragma version equal to or greater than 0.8.0. By doing so, the contract will leverage the built-in overflow and underflow checks provided by the Solidity language itself, simplifying the code and reducing gas consumption. This change will uphold the contract's integrity in handling arithmetic operations while optimizing for efficiency and cost-effectiveness.

UTT - Unverified Token Transfer

Criticality	Minor / Informative
Location	SPECTRE.sol#L487
Status	Acknowledged

Description

The contract transfers tokens implementing the standard transfer method. If the transfer fails due to insufficient funds, contract issues, or other reasons, the transaction does not automatically revert, potentially leading the contract to falsely signal success without confirming the transfer occurred.

```
function sendTokensToSpectreMultiSeg(address tokenAddress)
        external onlySpectreWallet
        returns (bool success)
{
        emit clearTokens(tokenAddress,
IERC20(tokenAddress).balanceOf(address(this)));
        return
IERC20(tokenAddress).transfer(_spectreMultiSegWallet,
IERC20(tokenAddress).balanceOf(address(this)));
}
```

Recommendation

The team is advised to monitor the success of the token transfer and revert the transaction if the transfer fails. By implementing such an approach, it is ensured that the function will not silently succeed in case of an unsuccessful transfer, providing a more secure and reliable token transfer process.

L04 - Conformance to Solidity Naming Conventions

Criticality	Minor / Informative
Location	SPECTRE.sol#L141,168,170,171,173,174,175,176,179,180,181,182,183,184,197,480,524
Status	Acknowledged

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);
address payable public _spectreMultiSegWallet
uint256 private constant _initialBuyTax = 22
uint256 private constant _initialSellTax = 22
uint256 public _finalSellTax = 2
uint256 private constant _reduceBuyTaxAt = 40
uint256 private constant _reduceSellTaxAt = 40
uint256 private constant _preventSwapBefore = 40
uint8 private constant _decimals = 9
uint256 private constant _tTotal = 100000000000 * 10**_decimals
string private constant _name = unicode"Spectre"
string private constant _symbol = unicode"SPCTR"
uint256 public _maxTxAmount = (_tTotal * 1) / 100
uint256 public _maxWalletSize = (_tTotal * 1) / 100

...
```

Recommendation

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

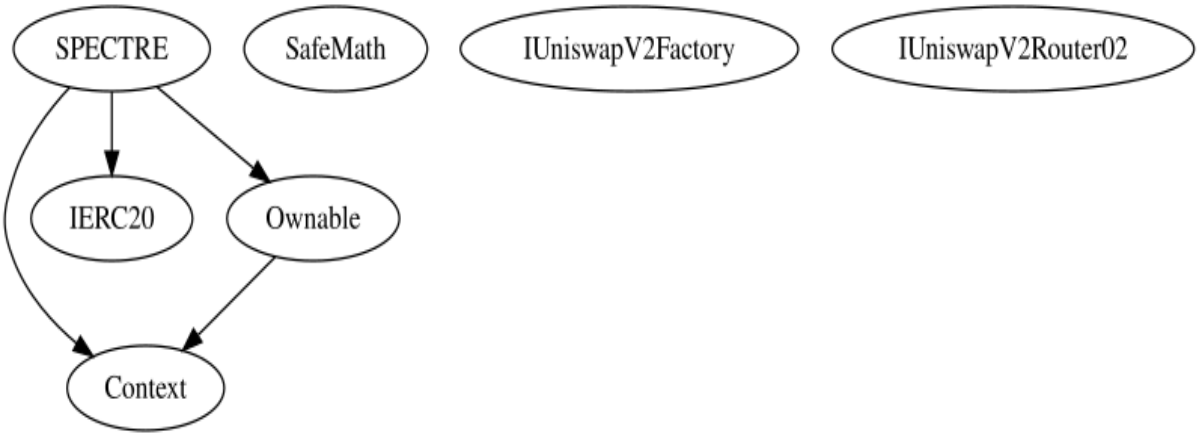
Find more information on the Solidity documentation https://docs.soliditylang.org/en/stable/style-guide.html#naming-conventions.

Functions Analysis

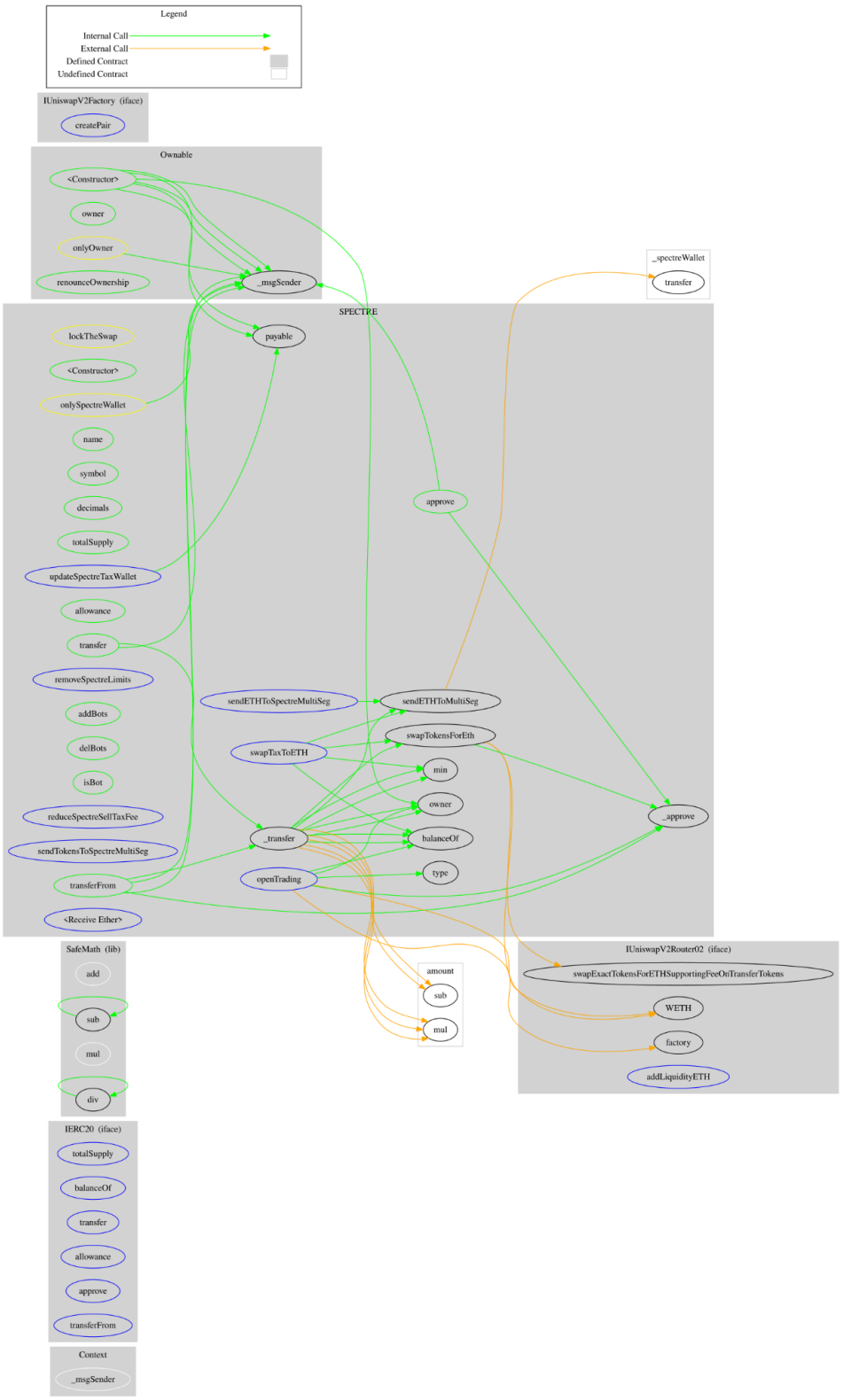
Contract	Type	Bases		
	Function Name	**Visibility**	**Mutability**	**Modifiers**
SPECTRE	Implementation	Context, IERC20, Ownable		
		Public	✓	-
	name	Public		-
	symbol	Public		-
	decimals	Public		-
	totalSupply	Public		-
	balanceOf	Public		-
	transfer	Public	✓	-
	allowance	Public		-
	approve	Public	✓	-
	transferFrom	Public	✓	-
	_approve	Private	✓	
	_transfer	Private	✓	
	min	Private		
	swapTokensForEth	Private	✓	lockTheSwap
	removeSpectreLimits	External	✓	onlyOwner
	sendETHToMultiSeg	Private	✓	
	addBots	Public	✓	onlyOwner
	delBots	Public	✓	onlyOwner

	isBot	Public		-
	openTrading	External	✓	onlyOwner
	reduceSpectreSellTaxFee	External	✓	onlySpectreWallet
	sendTokensToSpectreMultiSeg	External	✓	onlySpectreWallet
	swapTaxToETH	External	✓	onlySpectreWallet
	sendETHToSpectreMultiSeg	External	✓	onlySpectreWallet
	updateSpectreTaxWallet	External	✓	onlyOwner
		External	Payable	-

Inheritance Graph



Flow Graph


Legend
Internal Call
External Call
Defined Contract
Undefined Contract
IUniswapV2Factory (iface)
createPair
Ownable
<Constructor>
owner
onlyOwner
renounceOwnership
_msgSender
_spectreWallet
transfer
SPECTRE
payable
lockTheSwap
<Constructor>
onlySpectreWallet
name
symbol
decimals
totalSupply
updateSpectreTaxWallet
allowance
transfer
removeSpectreLimits
addBots
delBots
isBot
reduceSpectreSellTaxFee
sendTokensToSpectreMultiSeg
transferFrom
<Receive Ether>
approve
sendETHToSpectreMultiSeg
sendETHToMultiSeg
swapTokensForEth
swapTaxToETH
min
owner
_transfer
balanceOf
type
openTrading
_approve
amount
sub
mul
IUniswapV2Router02 (iface)
swapExactTokensForETHSupportingFeeOnTransferTokens
WETH
factory
addLiquidityETH
SafeMath (lib)
add
sub
mul
div
IERC20 (iface)
totalSupply
balanceOf
transfer
allowance
approve
transferFrom
Context
_msgSender

Summary

SPECTRE is an interesting project that has a friendly and growing community. The Smart Contract analysis reported no compiler error and no critical issues. Issues of minor severity were identified to improve the contract's performance and consistency.

This audit investigated security issues, business logic concerns and potential improvements.

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

cyberscope.io