Cyberscope

Audit Report

DRIVEN

July 2022

Type	BEP20
Network	BSC
Address	0x56d3dd84dd3bc1ed37a154c5775481073719988f
Audited by	© cyberscope

Table of Contents

Contract Review

Contract Name	DRIVEN
Compiler Version	v0.8.4+commit.c7e474f2
Optimization	200 runs
Licence	MIT
Explorer	https://bscscan.com/token/0x56D3Dd84dd3bc1Ed37a154C5775481073719988f
Symbol	DRIVEN
Decimals	18
Total Supply	50,000,000
Domain	drivens.org

Source Files

Filename	**SHA256**
contract.sol	07ab826cb1fe4cbff07e66c1f04c4793653c793ee2bb53a8007ba57a3592a391

Audit Updates

Initial Audit	21st July 2022
Corrected	

Contract Analysis

Critical Medium Minor Pass

Severity	Code	Description
	ST	Contract Owner is not able to stop or pause transactions
	OCTD	Contract Owner is not able to transfer tokens from specific address
	OTUT	Owner Transfer User's Tokens
	ELFM	Contract Owner is not able to increase fees more than a reasonable percent (25%)
	ULTW	Contract Owner is not able to increase the amount of liquidity taken by dev wallet more than a reasonable percent
	MT	Contract Owner is not able to mint new tokens
	BT	Contract Owner is not able to burn tokens from specific wallet
	BC	Contract Owner is not able to blacklist wallets from selling

ST - Stop Transactions

Criticality	critical
Location	contract.sol#L2256

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 setting the `killBlockNum` to a high value. As a result, all the buyers will be blacklisted.

```
if (sender == uniswapPair) {
       if(launchBlockNum + killBlockNum >= block.number) {
              _bAddress[recipient] = true;
       }
}
```

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.

OCTD - Owner Contract Tokens Drain

Criticality	minor
Location	contract.sol#L2329

Description

The contract owner has the authority to claim all the balance of the contract. The owner may take advantage of it by calling the `rescueToken` function.

```
function rescueToken(address tokenAddress, address des, uint256 amount) external
onlyOwner returns (bool success){
       return IERC20(tokenAddress).transfer(des, 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.

ELFM - Exceed Limit Fees Manipulation

Criticality	critical
Location	contract.sol#L2187,2190

Description

The contract owner has the authority to increase over the allowed limit of 25%. The owner may take advantage of it by calling the `setMarketFee` function with a high percentage value.

```
function setMarketFee(uint256 marketfee) public onlyOwner {
       marketFee = marketfee;
}
```

Recommendation

The contract could embody a check for the maximum acceptable value.

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 - Blacklisted Contracts

Criticality	critical
Location	contract.sol#L2228

Description

The contract owner has the authority to stop contracts from transactions. The owner may take advantage of it by calling the `setMutilpyBAddress` function.

```
require(!_bAddress[sender] && !_bAddress[recipient], "ERC20: transfer from | to bAddress");
```

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

Severity	Code	Description
	L01	Public Function could be Declared External
	L02	State Variables could be Declared Constant
	L04	Conformance to Solidity Naming Conventions
	L07	Missing Events Arithmetic
	L09	Dead Code Elimination
	L13	Divide before Multiply Operation

L01 - Public Function could be Declared External

Criticality	minor
Location	contract.sol#L1700,1709,1714,1721,1725,1729,1736,2092,2096,2100,2104,2112,2116,2121,2126,2130,2143,2147,2150,2153,2159,2164,2176,2180,2184,2187,2190,2194,2199,2202,2213,2218

Description

Public functions that are never called by the contract should be declared external to save gas.

```
transferFrom
transfer
startSwap
stopSwap
firstLaunch
setMarketFee
setBurnFee
startAddLP
setSwapAndLiquifyByLimitOnly
...
```

Recommendation

Use the external attribute for functions never called from the contract.

L02 - State Variables could be Declared Constant

Criticality	minor
Location	contract.sol#L1996,1995

Description

Constant state variables should be declared constant to save gas.

```
rewardTokenAddress
deadAddress
```

Recommendation

Add the constant attribute to state variables that never change.

L04 - Conformance to Solidity Naming Conventions

Criticality	minor
Location	contract.sol#L6,1693,1786,1788,1805,1835,2176,2000,2008

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.

```
_minimumTokensBeforeSwap
_balances
_enabled
WETH
MINIMUM_LIQUIDITY
PERMIT_TYPEHASH
DOMAIN_SEPARATOR
_owner
console
```

Recommendation

Follow the Solidity naming convention.
https://docs.soliditylang.org/en/v0.4.25/style-guide.html#naming-conventions.

L07 - Missing Events Arithmetic

Criticality	minor
Location	contract.sol#L2159,2168,2187,2190

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.

```
marketFee = marketfee
burnFee = burnfee
_minimumTokensBeforeSwap = newLimit
killBlockNum = num
```

Recommendation

Emit an event for critical parameter changes.

L09 - Dead Code Elimination

Criticality	minor
Location	contract.sol#L1672,1655,1659,1663,1667,1636,1647,2302,2308,9,18,186,250,506,1530,1526,1522,1518,502,1514,1510,1506,1502,498,1498,1494,1490,1486,494,1482,1478,1474,1470,246,490,1466,1462,1458,1454,486,1450,1446,1442,1438,482,1434,1430,1426,1422,478,1418,1414,1410,1406,242,474,1402,1398,1394,1390,470,1386,1382,1378,1374,466,1370,1366,1362,1358,462,1354,1350,1346,1342,238,458,1338,1334,1330,1326,454,1322,1318,1314,1310,450,1306,1302,1298,1294,446,1290,1286,1282,1278,182,234,442,1274,1270,1266,1262,438,1258,1254,1250,1246,434,1242,1238,1234,1230,430,1226,1222,1218,1214,230,426,1210,1206,1202,1198,422,1194,1190,1186,1182,418,1178,1174,1170,1166,414,1162,1158,1154,1150,226,410,1146,1142,1138,1134,406,1130,1126,1122,1118,402,1114,1110,1106,1102,398,1098,1094,1090,1086,222,394,1082,1078,1074,1070,390,1066,1062,1058,1054,386,1050,1046,1042,1038,382,1034,1030,1026,1022,178,218,378,1018,1014,1010,1006,374,1002,998,994,990,370,986,982,978,974,366,970,966,962,958,214,362,954,950,946,942,358,938,934,930,926,354,922,918,914,910,350,906,902,898,894,210,346,890,886,882,878,342,874,870,866,862,338,858,854,850,846,334,842,838,834,830,206,330,826,822,818,814,326,810,806,802,798,322,794,790,786,782,318,778,774,770,766,174,202,314,762,758,754,750,310,746,742,738,734,306,730,726,722,718,302,714,710,706,702,198,298,698,694,690,686,294,682,678,674,670,290,666,662,658,654,286,650,646,642,638,194,282,634,630,626,622,278,618,614,610,606,274,602,598,594,590,270,586,582,578,574,190,266,570,566,562,558,262,554,550,546,542,258,538,534,530,526,254,522,518,514,510,38,34,42,46,82,86,90,94,98,102,106,110,114,118,50,122,126,130,134,138,142,146,150,154,158,54,162,166,170,58,62,66,70,74,78,22,30,26

Description

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

```
logUint
logString
logInt
logBytes9
logBytes8
logBytes7
logBytes6
logBytes5
logBytes4
...
```

Recommendation

Remove unused functions.

L13 - Divide before Multiply Operation

Criticality	minor
Location	contract.sol#L2054

Description

Performing divisions before multiplications may cause lose of prediction.

```
_minimumTokensBeforeSwap = supply.div(1000) * 10 ** _decimals
```

Recommendation

The multiplications should be prior to the divisions.

Contract Functions

Contract	Type	Bases		
	Function Name	Visibility	Mutability	Modifiers
console	Library			
	_sendLogPayload	Private		
	log	Internal		
	logInt	Internal		
	logUint	Internal		
	logString	Internal		
	logBool	Internal		
	logAddress	Internal		
	logBytes	Internal		
	logBytes1	Internal		
	logBytes2	Internal		
	logBytes3	Internal		
	logBytes4	Internal		
	logBytes5	Internal		
	logBytes6	Internal		
	logBytes7	Internal		
	logBytes8	Internal		
	logBytes9	Internal		
	logBytes10	Internal		
	logBytes11	Internal		
	logBytes12	Internal		
	logBytes13	Internal		
	logBytes14	Internal		
	logBytes15	Internal		
	logBytes16	Internal		
	logBytes17	Internal		
	logBytes18	Internal		
	logBytes19	Internal		
	logBytes20	Internal		

	logBytes21	Internal		
	logBytes22	Internal		
	logBytes23	Internal		
	logBytes24	Internal		
	logBytes25	Internal		
	logBytes26	Internal		
	logBytes27	Internal		
	logBytes28	Internal		
	logBytes29	Internal		
	logBytes30	Internal		
	logBytes31	Internal		
	logBytes32	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		

	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		

	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		

	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		

	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		

	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		

	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		

	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		

	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		

	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		
	log	Internal		

	log	Internal		
	log	Internal		
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		

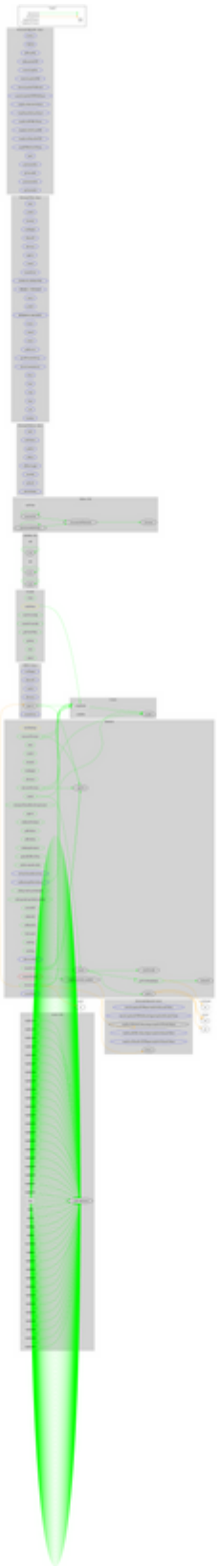
	owner	Public		-
	waiveOwnership	Public	✓	onlyOwner
	transferOwnership	Public	✓	onlyOwner
	getUnlockTime	Public		-
	getTime	Public		-
	lock	Public	✓	onlyOwner
	unlock	Public	✓	-
IUniswapV2Factory	Interface			
	feeTo	External		-
	feeToSetter	External		-
	getPair	External		-
	allPairs	External		-
	allPairsLength	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		-
IUniswapV2Ro	Interface	IUniswapV2		

uter02		Router01		
	removeLiquidityETHSupportingFeeOnTransferTokens	External	✓	-
	removeLiquidityETHWithPermitSupportingFeeOnTransferTokens	External	✓	-
	swapExactTokensForTokensSupportingFeeOnTransferTokens	External	✓	-
	swapExactETHForTokensSupportingFeeOnTransferTokens	External	Payable	-
	swapExactTokensForETHSupportingFeeOnTransferTokens	External	✓	-
DRIVEN	Implementation	Context, IERC20, Ownable		
	<Constructor>	Public	Payable	-
	name	Public		-
	symbol	Public		-
	decimals	Public		-
	totalSupply	Public		-
	balanceOf	Public		-
	allowance	Public		-
	increaseAllowance	Public	✓	-
	decreaseAllowance	Public	✓	-
	minimumTokensBeforeSwapAmount	Public		-
	approve	Public	✓	-
	_approve	Private	✓	
	setMarketPairStatus	Public	✓	onlyOwner
	getBAddress	Public		onlyOwner
	setBAddress	Public	✓	onlyOwner
	setMutilpyBAddress	Public	✓	onlyOwner
	updateKillBlockNum	Public	✓	onlyOwner
	setIsExcludedFromFee	Public	✓	onlyOwner
	setNumTokensBeforeSwap	External	✓	onlyOwner
	setMarketingWalletAddress	External	✓	onlyOwner
	setSwapAndLiquifyEnabled	Public	✓	onlyOwner
	setSwapAndLiquifyByLimitOnly	Public	✓	onlyOwner

	startAddLP	Public	✓	onlyOwner
	setBurnFee	Public	✓	onlyOwner
	setMarketFee	Public	✓	onlyOwner
	firstLaunch	Public	✓	onlyOwner
	stopSwap	Public	✓	onlyOwner
	startSwap	Public	✓	onlyOwner
	getCirculatingSupply	Public		-
	<Receive Ether>	External	Payable	-
	transfer	Public	✓	-
	transferFrom	Public	✓	-
	_transfer	Private	✓	
	takeFee	Internal	✓	
	_basicTransfer	Internal	✓	
	swapAndLiquify	Private	✓	lockTheSwap
	swapTokensForRewardtoken	Private	✓	
	rescueToken	External	✓	onlyOwner

Contract Flow



Domain Info

Domain Name	drivens.org
Registry Domain ID	e43adf043c2d4068a13e479913eb649b-LROR
Creation Date	2022-05-25T15:05:39Z
Updated Date	2022-05-25T15:05:43Z
Registry Expiry Date	2023-05-25T15:05:39Z
Registrar WHOIS Server	whois.dynadot.com
Registrar URL	http://www.dynadot.com
Registrar	Dynadot, LLC
Registrar IANA ID	472

The domain was created 10 months before the creation of the audit.

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, transferring tokens to the team’s wallet, manipulating fees 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

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