



Cyberscope

# Audit Report

## **Simple Stake**

March 2022

Type       BEP20

Network    BSC

Address    0xa70740B48C29E14464B9F40F9793E6c7f6579705

Audited by © cyberscope

# Table of Contents

|                                                         |           |
|---------------------------------------------------------|-----------|
| <b>Table of Contents</b>                                | <b>1</b>  |
| <b>Contract Review</b>                                  | <b>3</b>  |
| <b>Audit Updates</b>                                    | <b>3</b>  |
| <b>Contract Analysis</b>                                | <b>4</b>  |
| <b>ULTW - Unlimited Liquidity to Team Wallet</b>        | <b>5</b>  |
| Description                                             | 5         |
| Recommendation                                          | 5         |
| <b>BC - Blacklisted Contracts</b>                       | <b>6</b>  |
| Description                                             | 6         |
| Recommendation                                          | 6         |
| <b>Contract Diagnostics</b>                             | <b>7</b>  |
| <b>MAL - Misused Algorithmic Logic</b>                  | <b>8</b>  |
| Description                                             | 8         |
| Recommendation                                          | 8         |
| <b>MTS - Manipulate Total Supply</b>                    | <b>9</b>  |
| Description                                             | 9         |
| Recommendation                                          | 9         |
| <b>L01 - Public Function could be Declared External</b> | <b>10</b> |
| Description                                             | 10        |
| Recommendation                                          | 10        |
| <b>L02 - State Variables could be Declared Constant</b> | <b>11</b> |
| Description                                             | 11        |
| Recommendation                                          | 11        |
| <b>L05 - Unused State Variable</b>                      | <b>12</b> |
| Description                                             | 12        |
| Recommendation                                          | 12        |

|                                                         |           |
|---------------------------------------------------------|-----------|
| <b>L04 - Conformance to Solidity Naming Conventions</b> | <b>13</b> |
| Description                                             | 13        |
| Recommendation                                          | 13        |
| <b>L09 - Dead Code Elimination</b>                      | <b>14</b> |
| Description                                             | 14        |
| Recommendation                                          | 14        |
| <b>L14 - Uninitialized Variables in Local Scope</b>     | <b>15</b> |
| Description                                             | 15        |
| Recommendation                                          | 15        |
| <b>L13 - Divide before Multiply Operation</b>           | <b>16</b> |
| Description                                             | 16        |
| Recommendation                                          | 16        |
| <b>Contract Functions</b>                               | <b>17</b> |
| <b>Contract Flow</b>                                    | <b>22</b> |
| <b>Domain Info</b>                                      | <b>23</b> |
| <b>Summary</b>                                          | <b>24</b> |
| <b>Disclaimer</b>                                       | <b>25</b> |
| <b>About Cyberscope</b>                                 | <b>26</b> |

## Contract Review

|                         |                                                                                                                                                         |
|-------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Contract Name</b>    | SimpleStake                                                                                                                                             |
| <b>Compiler Version</b> | v0.7.6+commit.7338295f                                                                                                                                  |
| <b>Optimization</b>     | 200 runs                                                                                                                                                |
| <b>Licence</b>          | Unlicense                                                                                                                                               |
| <b>Explorer</b>         | <a href="https://bscscan.com/token/0xa70740B48C29E14464B9F40F9793E6c7f6579705">https://bscscan.com/token/0xa70740B48C29E14464B9F40F9793E6c7f6579705</a> |
| <b>Symbol</b>           | SStake                                                                                                                                                  |
| <b>Decimals</b>         | 5                                                                                                                                                       |
| <b>Total Supply</b>     | 325,000                                                                                                                                                 |
| <b>Source</b>           | contract.sol                                                                                                                                            |
| <b>Domain</b>           | simplestake.app                                                                                                                                         |

## Audit Updates

|                      |                 |
|----------------------|-----------------|
| <b>Initial Audit</b> | 15th March 2022 |
| <b>Corrected</b>     |                 |

# 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                                                      |

## ULTW - Unlimited Liquidity to Team Wallet

|             |                   |
|-------------|-------------------|
| Criticality | minor             |
| Location    | contract.sol#L732 |

### Description

The contract owner has the authority to transfer funds to the team wallet. These funds have been accumulated from fees collected from the contract. The owner may take advantage of it by calling the `withdrawAllTooperational` function.

```
function withdrawAllTooperational() external swapping onlyOwner {  
  
    uint256 amountToSwap = _gonBalances[address(this)].div(_gonsPerFragment);  
    require( amountToSwap > 0, "There is no SStake token deposited in token  
contract");  
    address[] memory path = new address[](2);  
    path[0] = address(this);  
    path[1] = router.WETH();  
    router.swapExactTokensForETHSupportingFeeOnTransferTokens(  
        amountToSwap,  
        0,  
        path,  
        operationalReceiver,  
        block.timestamp  
    );  
}
```

### Recommendation

The contract could embody a check for the maximum amount of funds that can be swapped. Since a huge amount may violate the token's price.

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 | medium            |
| Location    | contract.sol#L584 |

### Description

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

```
require(!blacklist[sender] && !blacklist[recipient], "in_blacklist");
```

### 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                                |
|----------|------|--------------------------------------------|
| ●        | MAL  | Misused Algorithmic Logic                  |
| ●        | MTS  | Manipulate Total Supply                    |
| ●        | L01  | Public Function could be Declared External |
| ●        | L02  | State Variables could be Declared Constant |
| ●        | L05  | Unused State Variable                      |
| ●        | L04  | Conformance to Solidity Naming Conventions |
| ●        | L09  | Dead Code Elimination                      |
| ●        | L14  | Uninitialized Variables in Local Scope     |
| ●        | L13  | Divide before Multiply Operation           |

## MAL - Misused Algorithmic Logic

|             |                   |
|-------------|-------------------|
| Criticality | minor             |
| Location    | contract.sol#L518 |

### Description

The algorithmic flow does not follow the required business logic.

In the following statement the third and the forth **if** will never be fulfilled since an unsigned integer is either less than or greater/equal to 365 days. Hence, always the first two **if** statements will be fulfilled.

```
if (deltaTimeFromInit < (365 days)) {  
    rebaseRate = 2355;  
} else if (deltaTimeFromInit >= (365 days)) {  
    rebaseRate = 211;  
} else if (deltaTimeFromInit >= ((15 * 365 days) / 10)) {  
    rebaseRate = 14;  
} else if (deltaTimeFromInit >= (7 * 365 days)) {  
    rebaseRate = 2;  
}
```

### Recommendation

The algorithm should be reshaped so it will match to the business logic.

## MTS - Manipulate Total Supply

|                    |                   |
|--------------------|-------------------|
| <b>Criticality</b> | minor             |
| <b>Location</b>    | contract.sol#L529 |

### Description

The contract is manipulating the total supply. This change will have a direct impact on the token price and Market Cap

```
for (uint256 i = 0; i < times; i++) {  
    _totalSupply = _totalSupply  
        .mul((10**RATE_DECIMALS).add(rebaseRate))  
        .div(10**RATE_DECIMALS);  
}
```

### Recommendation

The contract owner should carefully manage the adjustment of the circulating supply (increases or decreases), according to the token's price fluctuations.

## L01 - Public Function could be Declared External

|                    |                                               |
|--------------------|-----------------------------------------------|
| <b>Criticality</b> | minor                                         |
| <b>Location</b>    | contract.sol#L349,362,367,393,397,401,884,903 |

### Description

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

```
setPairAddress  
getLiquidityBacking  
decimals  
symbol  
name  
transferOwnership  
renounceOwnership  
owner
```

### Recommendation

Use the external attribute for functions never called from the contract

## L02 - State Variables could be Declared Constant

**Criticality**

minor

**Location**

contract.sol#L443,444,415,413,414,441,436,432,433,435 and 2 more

### Description

Constant state variables should be declared constant to save gas.

```
swapEnabled
sstakeInsuranceFundFee
sellFee
operationalFee
liquidityFee
incineratorFee
feeDenominator
_symbol
_name
...
```

### Recommendation

Add the constant attribute to state variables that never change.

## L05 - Unused State Variable

**Criticality**

minor

**Location**

contract.sol#L18

### Description

There are segments that contain unused state variables.

```
MAX_INT256
```

### Recommendation

Remove unused state variables.

## L04 - Conformance to Solidity Naming Conventions

**Criticality**

minor

**Location**

contract.sol#L151,152,169,189,781,790,853,873,874,875 and 18 more

### 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.

```
_totalSupply  
_lastAddLiquidityTime  
_lastRebasedTime  
_initRebaseStartTime  
_autoAddLiquidity  
_autoRebase  
ZERO  
DEAD  
_isFeeExempt  
...
```

### Recommendation

Follow the Solidity naming convention.

<https://docs.soliditylang.org/en/v0.4.25/style-guide.html#naming-conventions>

## L09 - Dead Code Elimination

|                    |                  |
|--------------------|------------------|
| <b>Criticality</b> | minor            |
| <b>Location</b>    | contract.sol#L46 |

### Description

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

```
abs
```

### Recommendation

Remove unused functions.

## L14 - Uninitialized Variables in Local Scope

**Criticality**

minor

**Location**

contract.sol#L512

### Description

There are variables that are defined in the local scope and are not initialized.

```
rebaseRate
```

### Recommendation

All the local scoped variables should be initialized.

## L13 - Divide before Multiply Operation

**Criticality**

minor

**Location**

contract.sol#L509,619,884

### Description

Performing divisions before multiplications may cause lose of prediction.

```
liquidityBalance = _gonBalances[pair].div(_gonsPerFragment)
_gonBalances[autoLiquidityReceiver] =
_gonBalances[autoLiquidityReceiver].add(gonAmount.div(feeDenominator).mul(liquidityFee))
_gonBalances[address(this)] =
_gonBalances[address(this)].add(gonAmount.div(feeDenominator).mul(_operationalFee.add(sstakeInsuranceFundFee)))
_gonBalances[incinerator] =
_gonBalances[incinerator].add(gonAmount.div(feeDenominator).mul(incineratorFee))
feeAmount = gonAmount.div(feeDenominator).mul(_totalFee)
times = deltaTime.div(900)
```

### Recommendation

The multiplications should be prior to the divisions.

# Contract Functions

| Contract                     | Type          | Bases      |            |           |
|------------------------------|---------------|------------|------------|-----------|
|                              | Function Name | Visibility | Mutability | Modifiers |
|                              |               |            |            |           |
| <b>SafeMathInt</b>           | Library       |            |            |           |
|                              | mul           | Internal   |            |           |
|                              | div           | Internal   |            |           |
|                              | sub           | Internal   |            |           |
|                              | add           | Internal   |            |           |
|                              | abs           | Internal   |            |           |
|                              |               |            |            |           |
| <b>SafeMath</b>              | Library       |            |            |           |
|                              | add           | Internal   |            |           |
|                              | sub           | Internal   |            |           |
|                              | sub           | Internal   |            |           |
|                              | mul           | Internal   |            |           |
|                              | div           | Internal   |            |           |
|                              | div           | Internal   |            |           |
|                              | mod           | Internal   |            |           |
|                              |               |            |            |           |
| <b>IERC20</b>                | Interface     |            |            |           |
|                              | totalSupply   | External   |            | -         |
|                              | balanceOf     | External   |            | -         |
|                              | allowance     | External   |            | -         |
|                              | transfer      | External   | ✓          | -         |
|                              | approve       | External   | ✓          | -         |
|                              | transferFrom  | External   | ✓          | -         |
|                              |               |            |            |           |
| <b>IPancakeSwap<br/>Pair</b> | Interface     |            |            |           |
|                              | name          | External   |            | -         |
|                              | symbol        | External   |            | -         |
|                              | decimals      | External   |            | -         |

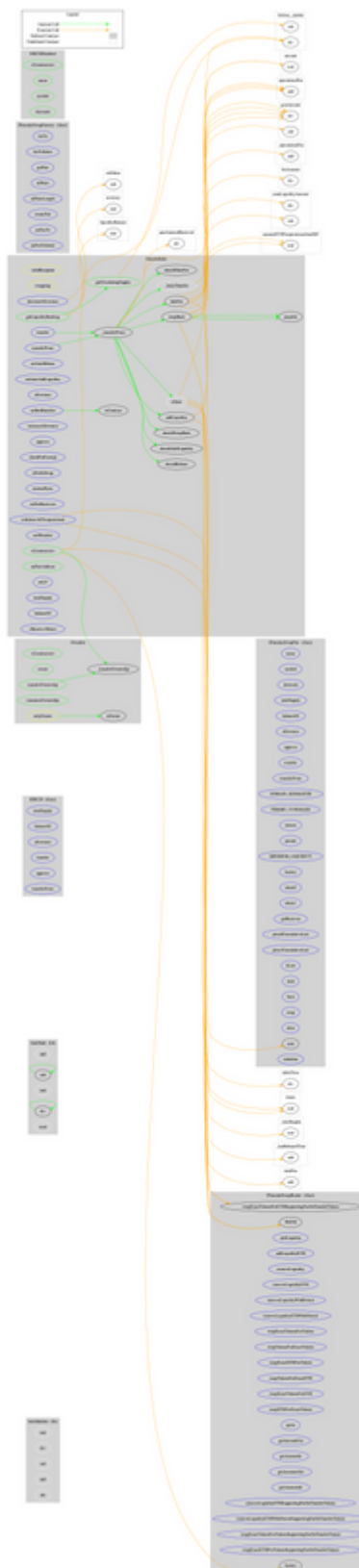
|                            |                              |          |         |   |
|----------------------------|------------------------------|----------|---------|---|
|                            | totalSupply                  | External |         | - |
|                            | balanceOf                    | 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 |         | - |
|                            | mint                         | External | ✓       | - |
|                            | burn                         | External | ✓       | - |
|                            | swap                         | External | ✓       | - |
|                            | skim                         | External | ✓       | - |
|                            | sync                         | External | ✓       | - |
|                            | initialize                   | External | ✓       | - |
|                            |                              |          |         |   |
| <b>IPancakeSwap Router</b> | 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 |         | -         |
|                            | removeLiquidityETHSupportingFeeOnTransferTokens           | External | ✓       | -         |
|                            | removeLiquidityETHWithPermitSupportingFeeOnTransferTokens | External | ✓       | -         |
|                            | swapExactTokensForTokensSupportingFeeOnTransferTokens     | External | ✓       | -         |
|                            | swapExactETHForTokensSupportingFeeOnTransferTokens        | External | Payable | -         |
|                            | swapExactTokensForETHSupportingFeeOnTransferTokens        | External | ✓       | -         |
|                            |                                                           |          |         |           |
| <b>IPancakeSwapFactory</b> | Interface                                                 |          |         |           |
|                            | feeTo                                                     | External |         | -         |
|                            | feeToSetter                                               | External |         | -         |
|                            | getPair                                                   | External |         | -         |
|                            | allPairs                                                  | External |         | -         |
|                            | allPairsLength                                            | External |         | -         |
|                            | createPair                                                | External | ✓       | -         |
|                            | setFeeTo                                                  | External | ✓       | -         |
|                            | setFeeToSetter                                            | External | ✓       | -         |
|                            |                                                           |          |         |           |
| <b>Ownable</b>             | Implementation                                            |          |         |           |
|                            | <Constructor>                                             | Public   | ✓       | -         |
|                            | owner                                                     | Public   |         | -         |
|                            | isOwner                                                   | Public   |         | -         |
|                            | renounceOwnership                                         | Public   | ✓       | onlyOwner |

|                      |                          |                           |   |                          |
|----------------------|--------------------------|---------------------------|---|--------------------------|
|                      | transferOwnership        | Public                    | ✓ | onlyOwner                |
|                      | _transferOwnership       | Internal                  | ✓ |                          |
|                      |                          |                           |   |                          |
| <b>ERC20Detailed</b> | Implementation           | IERC20                    |   |                          |
|                      | <Constructor>            | Public                    | ✓ | -                        |
|                      | name                     | Public                    |   | -                        |
|                      | symbol                   | Public                    |   | -                        |
|                      | decimals                 | Public                    |   | -                        |
|                      |                          |                           |   |                          |
| <b>SimpleStake</b>   | Implementation           | ERC20Detailed,<br>Ownable |   |                          |
|                      | <Constructor>            | Public                    | ✓ | ERC20Detailed<br>Ownable |
|                      | rebase                   | Internal                  | ✓ |                          |
|                      | transfer                 | External                  | ✓ | validRecipient           |
|                      | transferFrom             | External                  | ✓ | validRecipient           |
|                      | _basicTransfer           | Internal                  | ✓ |                          |
|                      | _transferFrom            | Internal                  | ✓ |                          |
|                      | takeFee                  | Internal                  | ✓ |                          |
|                      | addLiquidity             | Internal                  | ✓ | swapping                 |
|                      | swapBack                 | Internal                  | ✓ | swapping                 |
|                      | withdrawAllTooperational | External                  | ✓ | swapping<br>onlyOwner    |
|                      | shouldTakeFee            | Internal                  |   |                          |
|                      | shouldRebase             | Internal                  |   |                          |
|                      | shouldAddLiquidity       | Internal                  |   |                          |
|                      | shouldSwapBack           | Internal                  |   |                          |
|                      | setAutoRebase            | External                  | ✓ | onlyOwner                |
|                      | setAutoAddLiquidity      | External                  | ✓ | onlyOwner                |
|                      | allowance                | External                  |   | -                        |
|                      | decreaseAllowance        | External                  | ✓ | -                        |
|                      | increaseAllowance        | External                  | ✓ | -                        |
|                      | approve                  | External                  | ✓ | -                        |
|                      | checkFeeExempt           | External                  |   | -                        |
|                      | getCirculatingSupply     | Public                    |   | -                        |
|                      | isNotInSwap              | External                  |   | -                        |

|  |                     |          |         |           |
|--|---------------------|----------|---------|-----------|
|  | manualSync          | External | ✓       | -         |
|  | setFeeReceivers     | External | ✓       | onlyOwner |
|  | getLiquidityBacking | Public   |         | -         |
|  | setWhitelist        | External | ✓       | onlyOwner |
|  | setBotBlacklist     | External | ✓       | onlyOwner |
|  | setPairAddress      | Public   | ✓       | onlyOwner |
|  | setLP               | External | ✓       | onlyOwner |
|  | totalSupply         | External |         | -         |
|  | balanceOf           | External |         | -         |
|  | isContract          | Internal |         |           |
|  | <Receive Ether>     | External | Payable | -         |

# Contract Flow



## Domain Info

|                               |                                                                     |
|-------------------------------|---------------------------------------------------------------------|
| <b>Domain Name</b>            | simplestake.app                                                     |
| <b>Registry Domain ID</b>     | 4889504F9-APP                                                       |
| <b>Creation Date</b>          | 2022-03-14T04:12:10Z                                                |
| <b>Updated Date</b>           | 2022-03-14T10:42:15Z                                                |
| <b>Registry Expiry Date</b>   | 2023-03-14T04:12:10Z                                                |
| <b>Registrar WHOIS Server</b> | whois.namecheap.com                                                 |
| <b>Registrar URL</b>          | <a href="https://www.namecheap.com/">https://www.namecheap.com/</a> |
| <b>Registrar</b>              | Namecheap Inc.                                                      |
| <b>Registrar IANA ID</b>      | 1068                                                                |

The domain has been created 1 day before the creation of the audit. It will expire in 12 months.

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 blacklisting contracts and transferring funds to the team's wallet. The maximum fee percentage that can be set is 14% in buys and 16% in sales. The contract is also using a rebase technique that manipulates the total supply. 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 provides all the essential tools to assist users draw their own conclusions.



The Cyberscope team

<https://www.cyberscope.io>