



Cyberscope

# Audit Report

## **Apefund V2**

January 2023

Type           BEP20

Network       BSC

Address       0x7BE236a96e53dc7B1069f0212CB77d33aD8CBacF

Audited by   © cyberscope

# Table of Contents

|                                                         |           |
|---------------------------------------------------------|-----------|
| <b>Table of Contents</b>                                | <b>1</b>  |
| <b>Review</b>                                           | <b>3</b>  |
| <b>Audit Updates</b>                                    | <b>3</b>  |
| <b>Source Files</b>                                     | <b>3</b>  |
| <b>Analysis</b>                                         | <b>4</b>  |
| <b>Diagnostics</b>                                      | <b>5</b>  |
| <b>PTRP - Potential Transfer Revert Propagation</b>     | <b>6</b>  |
| Description                                             | 6         |
| Recommendation                                          | 6         |
| <b>L02 - State Variables could be Declared Constant</b> | <b>7</b>  |
| Description                                             | 7         |
| Recommendation                                          | 7         |
| <b>L04 - Conformance to Solidity Naming Conventions</b> | <b>8</b>  |
| Description                                             | 8         |
| Recommendation                                          | 9         |
| <b>L07 - Missing Events Arithmetic</b>                  | <b>10</b> |
| Description                                             | 10        |
| Recommendation                                          | 10        |
| <b>L12 - Using Variables before Declaration</b>         | <b>11</b> |
| Description                                             | 11        |
| Recommendation                                          | 11        |
| <b>L13 - Divide before Multiply Operation</b>           | <b>12</b> |
| Description                                             | 12        |
| Recommendation                                          | 12        |
| <b>L14 - Uninitialized Variables in Local Scope</b>     | <b>13</b> |
| Description                                             | 13        |
| Recommendation                                          | 13        |
| <b>L20 - Succeeded Transfer Check</b>                   | <b>14</b> |
| Description                                             | 14        |
| Recommendation                                          | 14        |
| <b>Contract Functions</b>                               | <b>15</b> |

|                          |           |
|--------------------------|-----------|
| <b>Inheritance Graph</b> | <b>19</b> |
| <b>Flow Graph</b>        | <b>20</b> |
| <b>Summary</b>           | <b>21</b> |
| <b>Disclaimer</b>        | <b>22</b> |
| <b>About Cyberscope</b>  | <b>23</b> |

## Review

|                         |                                                                                                                                                             |
|-------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Contract Name</b>    | ApefundV2                                                                                                                                                   |
| <b>Compiler Version</b> | v0.8.17+commit.8df45f5f                                                                                                                                     |
| <b>Optimization</b>     | 500 runs                                                                                                                                                    |
| <b>Explorer</b>         | <a href="https://bscscan.com/address/0x7be236a96e53dc7b1069f0212cb77d33ad8cbacf">https://bscscan.com/address/0x7be236a96e53dc7b1069f0212cb77d33ad8cbacf</a> |
| <b>Address</b>          | 0x7be236a96e53dc7b1069f0212cb77d33ad8cbacf                                                                                                                  |
| <b>Network</b>          | BSC                                                                                                                                                         |
| <b>Symbol</b>           | AFND                                                                                                                                                        |
| <b>Decimals</b>         | 18                                                                                                                                                          |
| <b>Total Supply</b>     | 100,000,000                                                                                                                                                 |

## Audit Updates

|                      |             |
|----------------------|-------------|
| <b>Initial Audit</b> | 09 Jan 2023 |
|----------------------|-------------|

## Source Files

|                      |                                                                  |
|----------------------|------------------------------------------------------------------|
| <b>Filename</b>      | SHA256                                                           |
| <b>ApefundV2.sol</b> | 834b876d7f28877f9ef360dd5261354455762bc301b798e83b9453b4e75f1eaa |

# 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     |
|----------|------|--------------------------------------------|------------|
| ●        | L02  | State Variables could be Declared Constant | Unresolved |
| ●        | L04  | Conformance to Solidity Naming Conventions | Unresolved |
| ●        | L07  | Missing Events Arithmetic                  | Unresolved |
| ●        | L12  | Using Variables before Declaration         | Unresolved |
| ●        | L13  | Divide before Multiply Operation           | Unresolved |
| ●        | L14  | Uninitialized Variables in Local Scope     | Unresolved |
| ●        | L20  | Succeeded Transfer Check                   | Unresolved |

## L02 - State Variables could be Declared Constant

|                    |                     |
|--------------------|---------------------|
| <b>Criticality</b> | Minor / Informative |
| <b>Location</b>    | ApefundV2.sol#L158  |
| <b>Status</b>      | Unresolved          |

### Description

State variables can be declared as constant using the constant keyword. This means that the value of the state variable cannot be changed after it has been set. Additionally, the constant variables decrease gas consumption of the corresponding transaction.

```
address payable public marketingWallet =  
payable(0x60808eaaED5AfA68DC2d7B1b8B3effF84c846754d)
```

### Recommendation

Constant state variables can be useful when the contract wants to ensure that the value of a state variable cannot be changed by any function in the contract. This can be useful for storing values that are important to the contract's behavior, such as the contract's address or the maximum number of times a certain function can be called. The team is advised to add the constant keyword to state variables that never change.

## L04 - Conformance to Solidity Naming Conventions

|                    |                                                                                   |
|--------------------|-----------------------------------------------------------------------------------|
| <b>Criticality</b> | Minor / Informative                                                               |
| <b>Location</b>    | ApefundV2.sol#L33,111,112,113,114,115,132,138,147,148,149,150,151,157,168,187,388 |
| <b>Status</b>      | 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 constant private startingSupply = 100_000_000
string constant private _name = "Apefund V2"
string constant private _symbol = "AFND"
uint8 constant private _decimals = 18
uint256 constant private _tTotal = startingSupply * 10**_decimals

Fees public _taxRates = Fees({
    buyFee: 500,
    sellFee: 1500,
    transferFee: 0
})

...
```

## 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>.

## L07 - Missing Events Arithmetic

|                    |                                |
|--------------------|--------------------------------|
| <b>Criticality</b> | Minor / Informative            |
| <b>Location</b>    | ApefundV2.sol#L431,436,452,462 |
| <b>Status</b>      | Unresolved                     |

### Description

Events are a way to record and log information about changes or actions that occur within a contract. They are often used to notify external parties or clients about events that have occurred within the contract, such as the transfer of tokens or the completion of a task.

It's important to carefully design and implement the events in a contract, and to ensure that all required events are included. It's also a good idea to test the contract to ensure that all events are being properly triggered and logged.

```
_maxTxAmount = (_tTotal * percent) / divisor  
_maxWalletSize = (_tTotal * percent) / divisor  
swapThreshold = (_tTotal * thresholdPercent) / thresholdDivisor  
piSwapPercent = priceImpactSwapPercent
```

### Recommendation

By including all required events in the contract and thoroughly testing the contract's functionality, the contract ensures that it performs as intended and does not have any missing events that could cause issues with its arithmetic.

## L12 - Using Variables before Declaration

|                    |                     |
|--------------------|---------------------|
| <b>Criticality</b> | Minor / Informative |
| <b>Location</b>    | ApefundV2.sol#L682  |
| <b>Status</b>      | Unresolved          |

### Description

The contract is using a variable before the declaration. This is usually happening either if it has not been declared yet or if the variable has been declared in a different scope. It is not a good practice to use a local variable before it has been declared.

```
bool check
```

### Recommendation

By declaring local variables before using them, contract ensures that it operates correctly. It's important to be aware of this rule when working with local variables, as using a variable before it has been declared can lead to unexpected behavior and can be difficult to debug.

## L13 - Divide before Multiply Operation

|                    |                                |
|--------------------|--------------------------------|
| <b>Criticality</b> | Minor / Informative            |
| <b>Location</b>    | ApefundV2.sol#L567,585,718,719 |
| <b>Status</b>      | Unresolved                     |

### Description

It is important to be aware of the order of operations when performing arithmetic calculations. This is especially important when working with large numbers, as the order of operations can affect the final result of the calculation. Performing divisions before multiplications may cause loss of precision.

```
uint256 toLiquify = ((contractTokenBalance * ratios.liquidity) / ratios.totalSwap) /  
2  
uint256 liquidityBalance = (amtBalance * toLiquify) / swapAmt
```

### Recommendation

To avoid this issue, it is recommended to carefully consider the order of operations when performing arithmetic calculations in Solidity. It's generally a good idea to use parentheses to specify the order of operations. The basic rule is that the multiplications should be prior to the divisions.

## L14 - Uninitialized Variables in Local Scope

|                    |                        |
|--------------------|------------------------|
| <b>Criticality</b> | Minor / Informative    |
| <b>Location</b>    | ApefundV2.sol#L681,682 |
| <b>Status</b>      | Unresolved             |

### Description

Using an uninitialized local variable can lead to unpredictable behavior and potentially cause errors in the contract. It's important to always initialize local variables with appropriate values before using them.

```
bool checked  
bool check
```

### Recommendation

By initializing local variables before using them, the contract ensures that the functions behave as expected and avoid potential issues.

## L20 - Succeeded Transfer Check

|                    |                                |
|--------------------|--------------------------------|
| <b>Criticality</b> | Minor / Informative            |
| <b>Location</b>    | ApefundV2.sol#L623,626,629,669 |
| <b>Status</b>      | Unresolved                     |

### Description

According to the ERC20 specification, the transfer methods should be checked if the result is successful. Otherwise, the contract may wrongly assume that the transfer has been established.

```
IERC20_BUSD.transfer(_taxWallets.opex, opexBalance)
IERC20_BUSD.transfer(_taxWallets.investment, investmentBalance)
IERC20_BUSD.transfer(_taxWallets.futureTax, futureTaxBalance)
TOKEN.transfer(_owner, TOKEN.balanceOf(address(this)))
```

### Recommendation

The contract should check if the result of the transfer methods is successful. The team is advised to check the SafeERC20 library from the [Openzeppelin library](#).

# Contract Functions

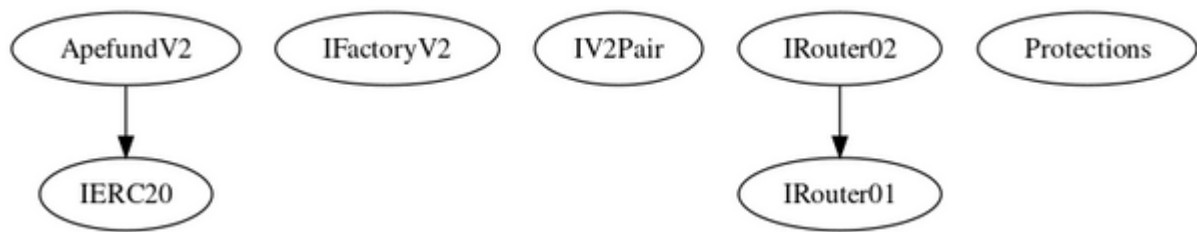
| Contract          | Type          | Bases      |            |           |
|-------------------|---------------|------------|------------|-----------|
|                   | Function Name | Visibility | Mutability | Modifiers |
|                   |               |            |            |           |
| <b>IERC20</b>     | Interface     |            |            |           |
|                   | totalSupply   | External   |            | -         |
|                   | decimals      | External   |            | -         |
|                   | symbol        | External   |            | -         |
|                   | name          | External   |            | -         |
|                   | getOwner      | External   |            | -         |
|                   | balanceOf     | External   |            | -         |
|                   | transfer      | External   | ✓          | -         |
|                   | allowance     | External   |            | -         |
|                   | approve       | External   | ✓          | -         |
|                   | transferFrom  | External   | ✓          | -         |
|                   |               |            |            |           |
| <b>IFactoryV2</b> | Interface     |            |            |           |
|                   | getPair       | External   |            | -         |
|                   | createPair    | External   | ✓          | -         |
|                   |               |            |            |           |
| <b>IV2Pair</b>    | Interface     |            |            |           |
|                   | factory       | External   |            | -         |
|                   | getReserves   | External   |            | -         |
|                   | sync          | External   | ✓          | -         |
|                   |               |            |            |           |
| <b>IRouter01</b>  | Interface     |            |            |           |
|                   | factory       | External   |            | -         |
|                   | WETH          | External   |            | -         |

|                    |                                                           |           |         |           |
|--------------------|-----------------------------------------------------------|-----------|---------|-----------|
|                    | addLiquidityETH                                           | External  | Payable | -         |
|                    | addLiquidity                                              | External  | ✓       | -         |
|                    | swapExactETHForTokens                                     | External  | Payable | -         |
|                    | getAmountsOut                                             | External  |         | -         |
|                    | getAmountsIn                                              | External  |         | -         |
|                    |                                                           |           |         |           |
| <b>IRouter02</b>   | Interface                                                 | IRouter01 |         |           |
|                    | swapExactTokensForETHSupporting<br>FeeOnTransferTokens    | External  | ✓       | -         |
|                    | swapExactETHForTokensSupporting<br>FeeOnTransferTokens    | External  | Payable | -         |
|                    | swapExactTokensForTokensSupporti<br>ngFeeOnTransferTokens | External  | ✓       | -         |
|                    | swapExactTokensForTokens                                  | External  | ✓       | -         |
|                    |                                                           |           |         |           |
| <b>Protections</b> | Interface                                                 |           |         |           |
|                    | checkUser                                                 | External  | ✓       | -         |
|                    | setLaunch                                                 | External  | ✓       | -         |
|                    | setLpPair                                                 | External  | ✓       | -         |
|                    | setProtections                                            | External  | ✓       | -         |
|                    | removeSniper                                              | External  | ✓       | -         |
|                    |                                                           |           |         |           |
| <b>ApefundV2</b>   | Implementation                                            | IERC20    |         |           |
|                    |                                                           | Public    | Payable | -         |
|                    | transferOwner                                             | External  | ✓       | onlyOwner |
|                    | renounceOwnership                                         | External  | ✓       | onlyOwner |
|                    |                                                           | External  | Payable | -         |
|                    | totalSupply                                               | External  |         | -         |
|                    | decimals                                                  | External  |         | -         |
|                    | symbol                                                    | External  |         | -         |
|                    | name                                                      | External  |         | -         |

|  |                             |          |   |           |
|--|-----------------------------|----------|---|-----------|
|  | getOwner                    | External |   | -         |
|  | allowance                   | External |   | -         |
|  | balanceOf                   | Public   |   | -         |
|  | transfer                    | Public   | ✓ | -         |
|  | approve                     | External | ✓ | -         |
|  | _approve                    | Internal | ✓ |           |
|  | approveContractContingency  | External | ✓ | onlyOwner |
|  | transferFrom                | External | ✓ | -         |
|  | setNewRouter                | External | ✓ | onlyOwner |
|  | setLpPair                   | External | ✓ | onlyOwner |
|  | setInitializer              | External | ✓ | onlyOwner |
|  | isExcludedFromLimits        | External |   | -         |
|  | setExcludedFromLimits       | External | ✓ | onlyOwner |
|  | isExcludedFromFees          | External |   | -         |
|  | setExcludedFromFees         | Public   | ✓ | onlyOwner |
|  | isExcludedFromProtection    | External |   | -         |
|  | setExcludedFromProtection   | External | ✓ | onlyOwner |
|  | getCirculatingSupply        | Public   |   | -         |
|  | removeSniper                | External | ✓ | onlyOwner |
|  | setProtectionSettings       | External | ✓ | onlyOwner |
|  | lockTaxes                   | External | ✓ | onlyOwner |
|  | setTaxes                    | External | ✓ | onlyOwner |
|  | setRatios                   | External | ✓ | onlyOwner |
|  | setWallets                  | External | ✓ | onlyOwner |
|  | setMaxTxPercent             | External | ✓ | onlyOwner |
|  | setMaxWalletSize            | External | ✓ | onlyOwner |
|  | getMaxTX                    | External |   | -         |
|  | getMaxWallet                | External |   | -         |
|  | getTokenAmountAtPriceImpact | External |   | -         |

|  |                          |          |   |            |
|--|--------------------------|----------|---|------------|
|  | setSwapSettings          | External | ✓ | onlyOwner  |
|  | setPriceImpactSwapAmount | External | ✓ | onlyOwner  |
|  | setContractSwapEnabled   | External | ✓ | onlyOwner  |
|  | excludePresaleAddresses  | External | ✓ | onlyOwner  |
|  | _hasLimits               | Internal |   |            |
|  | _transfer                | Internal | ✓ |            |
|  | contractSwap             | Internal | ✓ | inSwapFlag |
|  | _checkLiquidityAdd       | Internal | ✓ |            |
|  | enableTrading            | Public   | ✓ | onlyOwner  |
|  | sweepContingency         | External | ✓ | onlyOwner  |
|  | sweepExternalTokens      | External | ✓ | onlyOwner  |
|  | multiSendTokens          | External | ✓ | onlyOwner  |
|  | finalizeTransfer         | Internal | ✓ |            |
|  | takeTaxes                | Internal | ✓ |            |

## Inheritance Graph



# Flow Graph

## Summary

Apefund V2 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. There is also a limit of max 20% buy, sell and transfer fees.

## 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>