BlockSAFU

# ADVANCE MANUAL
# SMART CONTRACT AUDIT

**Project:** CUstodiy

**Website:** custodiy.com


**BlockSAFU Score: 85**

**Contract Address:**

0x188173379AC8963048Afe01C5d3D5998FEe67254

# DISCLAMER

BlockSAFU has completed this report to provide a summary of the Smart Contract functions, and any security, dependency, or cybersecurity vulnerabilities. This is often a constrained report on our discoveries based on our investigation and understanding of the current programming versions as of this report's date. To understand the full scope of our analysis, it is vital for you to at the date of this report. To understand the full scope of our analysis, you need to review the complete report. Although we have done our best in conducting our investigation and creating this report, it is vital to note that you should not depend on this report and cannot make any claim against BlockSAFU or its Subsidiaries and Team members on the premise of what has or has not been included in the report. Please remember to conduct your independent examinations before making any investment choices. We do not provide investment advice or in any way claim to determine if the project will be successful or not.

By perusing this report or any portion of it, you concur to the terms of this disclaimer. In the unlikely situation where you do not concur to the terms, you should immediately terminate reading this report, and erase and discard any duplicates of this report downloaded and/or printed by you. This report is given for data purposes as it were and on a non-reliance premise and does not constitute speculation counsel. No one should have any right to depend on the report or its substance, and BlockSAFU and its members (including holding companies, shareholders, backups, representatives, chiefs, officers, and other agents) BlockSAFU and its subsidiaries owe no obligation of care towards you or any other person, nor does BlockSAFU make any guarantee or representation to any individual on the precision or completeness of the report.

ABOUT THE AUDITOR:

BlockSAFU (BSAFU) is an Anti-Scam Token Utility that reviews Smart Contracts and Token information to Identify Rug Pull and Honey Pot scamming activity. BlockSAFUs Development Team consists of several Smart Contract creators, Auditors Developers, and Blockchain experts. BlockSAFU provides solutions, prevents, and hunts down scammers. BSAFU is a utility token with features Audit, KYC, Token Generators, and Bounty Scammers. It will enrich the crypto ecosystem.

# OVERVIEW

**BlockSAFU was commissioned by CUstodiy Finance Token to complete a Smart Contract audit. The objective of the Audit is to achieve the following:**

- Review the Project and experience and Development team
- Ensure that the Smart Contract functions are necessary and operate as intended.
- Identify any vulnerabilities in the Smart Contract code.

DISCLAIMER: This Audit is intended to inform about token Contract Risks, the result does not imply an endorsement or provide financial advice in any way, all investments are made at your own risk. (https://blocksafu.com/)

# SMART CONTRACT REVIEW

| | |
|---|---|
| Token Name | CUSTODIY |
| Token Symbol | CTY |
| Token Decimal | 18 |
| Total Supply | 1,000,000 **CTY** |
| Contract Address | 0x188173379AC8963048Afe01C5d3D5998FEe67254 |
| Deployer Address | 0xb235928d3830fFC69B23A996f6548dB303D430dd |
| Owner Address | 0xb235928d3830fFC69B23A996f6548dB303D430dd |
| Tax Fees Buy | 10% |
| Tax Fees Sell | 10% |
| Gas Used for Buy | 256,639 |
| Gas Used for Sell | 431,169 |
| Contract Created | Mar-07-2022 05:21:51 PM +UTC |
| Initial Liquidity | *will be updated after the DEX listing* |
| Liquidity Status | Locked |
| Unlocked Date | *will be updated after the DEX listing* |
| Verified CA | Yes |
| Compiler | v0.8.11+commit.d7f03943 |
| Optimization | Enable with 200 runs |
| Sol License | MIT License |
| Top 5 Holders | *will be updated after the DEX listing* |
| Other | default evmVersion |

# TAX

| **BUY & SELL** | |
|---|---|
| Dividend | 3% |
| Marketing | 3% |
| LP Liquidity | 4% |

# TOP HOLDER

| Rank | Address | Quantity | Percentage | Analytics |
|---|---|---|---|---|
| 1 | 0xb235928d3830ffc69b23a996f6548db303d430dd | 984,265 | 98.4265% | |
| 2 | 0x1f9b130ddc3ccc961b206580660d999afc63e46c | 11,853.5 | 1.1854% | |
| 3 | 0xe73ff8f93c151fcd2ab7c7d1a6ea9c70f0949f81 | 826 | 0.0826% | |
| 4 | 0xa2396705eb916d6d643150d27cffbace4a4ccaa5 | 360 | 0.0360% | |
| 5 | 0xf8c2994778c6a441529b3797b2fa08e3fbf0997b | 330 | 0.0330% | |
| 6 | 0xfc499bba2f15514f620979a6222fdf3ce11f2b9f | 250 | 0.0250% | |
| 7 | 0x82bbc69dd7e9607dcc501cb514d1a71a7eb88b38 | 132.75 | 0.0133% | |
| 8 | 0xff4f08d4ac87b671e30857805c6d52ac03c0db9f | 130 | 0.0130% | |
| 9 | 0x93f7015055574345e995419d9ef51ebe01240789 | 130 | 0.0130% | |
| 10 | 0xb150095c06ed999484515461442ece28380a4149 | 119 | 0.0119% | |
| 11 | 0xea4648a925cd42c99b9313ac052196cb55c865cb | 100 | 0.0100% | |
| 12 | 0x080aab7edcac6d4c765da67889c5afcb91e72b3e | 100 | 0.0100% | |
| 13 | 0xa14ad5fa0e9f2bb52fe9e33916b9bafc2cf8f352 | 100 | 0.0100% | |
| 14 | 0xabdaa3f562abdb0a349b85d119e979a1bfad3acc | 84 | 0.0084% | |

## Team Review

The CUstodiy team has a nice website, their website is professionally built and the Smart contract is well developed, their social media is growing with over 852 people in their telegram group (count in audit date).

## OFFICIAL WEBSITE AND SOCIAL MEDIA

Website: https://www.custodiy.com/

Telegram Group: https://t.me/custodiy_international

Telegram Group China: https://t.me/custodiy_cn

Twitter: https://twitter.com/Custodiy1

Facebook: https://www.facebook.com/custodiyofficial/

Discord: https://discord.com/invite/dJmaqdWj2r

Instagram: https://www.instagram.com/custodiyapp/

# MANUAL CODE REVIEW

## Minor-risk

## 3 minor-risk code issues found

## Could be fixed, and will not bring problems.

1. Weak PRNG (***Pseudo-random number generator***), do not use blocktimestamp as source randomness as this can be manipulated by miners.
   Recommendation: Avoid relying on block.timestamp

```
emit updateBuyFee(totalFee, block.timestamp);
...
emit updateSellFee(totalFee, block.timestamp);
```

2. The return value of an external transfer/transfer from the return value is checked.
   Recommendation: use SafeERC20, or ensure that the transfer/transfers from return value are checked

```
function transferFrom(address sender, address recipient, uint256 amount) public override
returns (bool) {
      _transfer(sender, recipient, amount);
      _approve(sender, _msgSender(), _allowances[sender][_msgSender()].sub(amount,
"ERC20: transfer amount exceeds allowance"));
      return true;
   }
```

3. Calls to a function sending bnb to an arbitrary address.

```
if(marketingTokens>0) {  _transferStandard(sender, marketingAddress,
marketingTokens); }

if(developerTokens>0) {  _transferStandard(sender, developerAddress, developerTokens);
}
```

## Medium-risk

0 medium-risk code issues found

Should be fixed, could bring problems.

## High-Risk

0 high-risk code issues found

Must be fixed, and will bring problem.

## Critical-Risk

0 critical-risk code issues found

Must be fixed, and will bring problem.

# EXTRA NOTES SMART CONTRACT

## 1. IBEP20

```
interface IBEP20 {
    function totalSupply() external view returns (uint256);
    function balanceOf(address account) external view returns (uint256);
    function transfer(address recipient, uint256 amount) external returns (bool);
    function allowance(address owner, address spender) external view returns (uint256);
    function approve(address spender, uint256 amount) external returns (bool);
    function transferFrom(address sender, address recipient, uint256 amount) external
returns (bool);
    event Transfer(address indexed from, address indexed to, uint256 value);
    event Approval(address indexed owner, address indexed spender, uint256 value);
}
```

IBEP20 Normal Base Template

## 2. SafeMath Library

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

    function sub(uint256 a, uint256 b) internal pure returns (uint256) {
        return sub(a, b, "SafeMath: subtraction overflow");
    }
    ...

    function div(uint256 a, uint256 b, string memory errorMessage) internal pure returns
(uint256) {
        require(b > 0, errorMessage);
        uint256 c = a / b;
        // assert(a == b * c + a % b); // There is no case in which this doesn't hold

        return c;
    }

    function mod(uint256 a, uint256 b) internal pure returns (uint256) {
        return mod(a, b, "SafeMath: modulo by zero");
    }

    function mod(uint256 a, uint256 b, string memory errorMessage) internal pure returns
(uint256) {
        require(b != 0, errorMessage);
        return a % b;
    }
}
```

Normal SafeMath Library

### 3. Contract CUSTODIYCIT

```
....
string private _name = "CUSTODIY $CTY";
string private _symbol = "CTY";
uint8 private _decimals = 18;

uint256 public _liquidityFee = 1; (now 4)
uint256 private _previousLiquidityFee = _liquidityFee;

uint256 public _marketingFee = 2; (now 3)
uint256 private _previousMarketingFee = _marketingFee;

uint256 public _developerFee = 0; (now 3)
uint256 private _previousDeveloperFee = _developerFee;

uint256 _saleLiquidityFee = 1;
uint256 _saleMarketingFee = 1;
uint256 _saleDeveloperFee = 1;

uint256 public _maxTxAmount = _tTotal.div(100).mul(1); //1%
uint256 private _minimumTokensBeforeSwap = 1_00 * 10**18;

uint256 public _walletHoldingMaxLimit =  _tTotal.div(100).mul(2); // 2%
...

event updateBuyFee(uint256 totalFee, uint256 timestamp);
   function setAllBuyFeePercentages(uint256 liquidityFee, uint256 marketingFee, uint256
developerFee)
   external onlyOwner()
   {
      _liquidityFee = liquidityFee;
      _previousLiquidityFee = liquidityFee;

      _marketingFee = marketingFee;
      _previousMarketingFee = marketingFee;

      _developerFee = developerFee;
      _previousDeveloperFee = developerFee;

      uint256 totalFee = liquidityFee.add(marketingFee).add(developerFee);
      require(totalFee<=12, "Too High Fee");
      emit updateBuyFee(totalFee, block.timestamp);
   }


   event updateSellFee(uint256 totalFee, uint256 timestamp);
   function setAllSaleFeePercentages(uint256 liquidityFee, uint256 marketingFee, uint256
```

```
developerFee)
    external onlyOwner()
    {
        _saleLiquidityFee = liquidityFee;
        _saleMarketingFee = marketingFee;
        _saleDeveloperFee = developerFee;

        uint256 totalFee = liquidityFee.add(marketingFee).add(developerFee);
        require(totalFee<=15, "Too High Fee");
        emit updateSellFee(totalFee, block.timestamp);
    }
```

The owner can set a buy and sell fee, less than or equal to 12% for buy, less than or equal to 15% for sell

```
uint256 private _tTotal = 1_000_000 * 10**18;
...
uint256 public _maxTxAmount = _tTotal.div(100).mul(1); //1%
...
function setMaxTxAmount(uint256 _mount) external onlyOwner()
{
    require(_mount>_tTotal.div(1000), "Too low Txn limit"); // Min 0.1%
    _maxTxAmount = _mount;
}
```

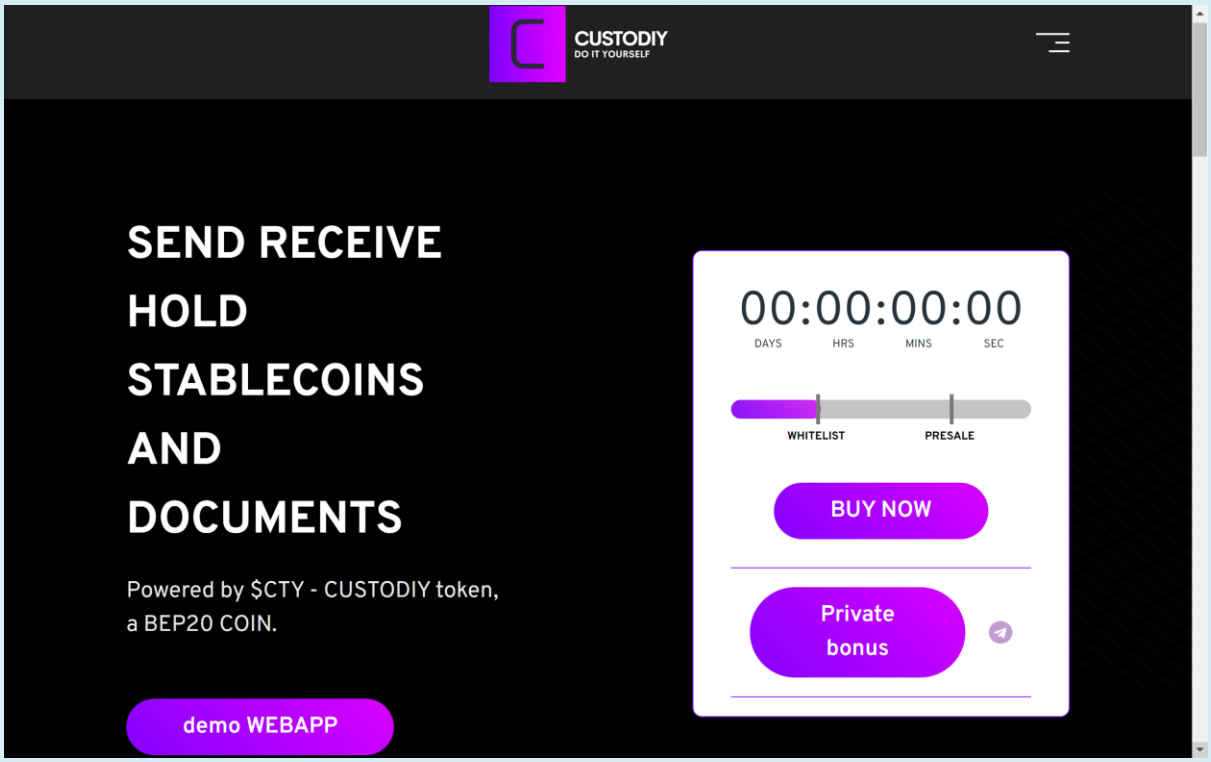
Informational: The owner cannot set the maximum transaction amount below 0.1% of the total supply **(Informational)**

```
uint256 public _walletHoldingMaxLimit =  _tTotal.div(100).mul(2); // 2%

function setWalletMaxHoldingLimit(uint256 _amount) public onlyOwner
{
    require(_amount>_tTotal.div(1000), "Too less limit");
    _walletHoldingMaxLimit = _amount;
}
```

Informational: The owner cannot set Wallet Max Holding with less than 0.1% of total inventory **(Informational)**

## WEBSITE REVIEW




- **Mobile Friendly**
- **Contains no code error**
- **SSL Secured (By Let's Encrypt SSL)**

**Web-Tec stack:** jQuery, apache, Cloudflare, chart js

Domain .com - (register.it) - Tracked by whois

| | |
|---|---|
| First Contentful Paint: | 1.0s |
| Fully Loaded Time | 5.6s |
| Performance | 86% |
| Accessibility | 71% |
| Best Practices | 83% |
| SEO | 100% |

## RUG-PULL REVIEW

Based on the available information analyzed by us, we come to the following conclusions:

- Locked Liquidity (*not presale yet*)

  (*Will be updated after DEX listing*)

- TOP 5 Holder

  (*Will be updated after DEX listing*)

- The team is not yet KYC

  (*Will be updated after DEX listing*)

## HONEYPOT REVIEW

- Ability to sell
- The owner is not able to pause the contract
- The owner cannot set buy fees over 12% and sell fees over 15%
- The owner cannot set the maximum transaction amount below 0.1% of the total supply

Note: Please check the disclaimer above and note, that the audit makes no statements or warranties on the business model, investment attractiveness, or code sustainability. The report is provided for the only contract mentioned in the report and does not include any other potential contracts deployed by the project owner.