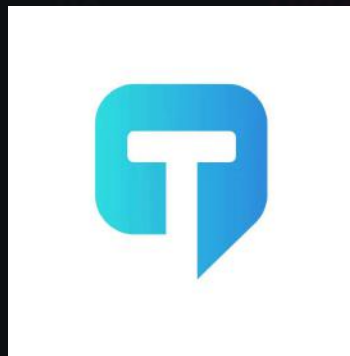




Coinsult

Advanced Manual Smart Contract Audit



Project: TCoin

Website: <https://tcoins.vip>

Low-Risk

2 low-risk code
issues found

Medium-Risk

0 medium-risk code
issues found

High-Risk

0 high-risk code
issues found

Contract Address

0xc8dfa3379a00C00CF033CE566AD13b93f9ACB636

Disclaimer: Coinsult is not responsible for any financial losses. Nothing in this contract audit is financial advice, please do your own research.

Disclaimer

Coinsult is not responsible if a project turns out to be a scam, rug-pull or honeypot. We only provide a detailed analysis for your own research.

Coinsult is not responsible for any financial losses. Nothing in this contract audit is financial advice, please do your own research.

The information provided in this audit is for informational purposes only and should not be considered investment advice. Coinsult does not endorse, recommend, support or suggest to invest in any project.

Coinsult can not be held responsible for when a project turns out to be a rug-pull, honeypot or scam.

Tokenomics

Rank	Address	Quantity (Token)	Percentage
1	0xafb1306976ca6a4cf55253ee217b50a05394d0f2	157,990,000	75.2333%
2	0x3f7f27d3d2a7f97be73623f5afb3e20c5c333ed	42,000,000	20.0000%
3	0x76d780b445ee3383c0ae979080a7b30bd0dfe1f	10,000,000	4.7619%
4	0xb9c33cbf2f99e7361c80e694abd460aeb6761b8e	9,997	0.0048%
5	0x7dd0c073cb4f4d3fc6d6843eeb31437d79a7df61	1.7	0.0000%

Source Code

Coinsult was commissioned by TCoin to perform an audit based on the following smart contract:

<https://bscscan.com/address/0xc8dfa3379a00C00CF033CE566AD13b93f9ACB636#code>

Manual Code Review

In this audit report we will highlight all these issues:

Low-Risk

2 low-risk code
issues found

Medium-Risk

0 medium-risk code
issues found

High-Risk

0 high-risk code
issues found

The detailed report continues on the next page...

● **Low-Risk:** Could be fixed, will not bring problems.

Too many digits

Literals with many digits are difficult to read and review.

```
_mint(msg.sender, 210000000 * 10 ** decimals());
```

Recommendation

Use: Ether suffix, Time suffix, or The scientific notation

Exploit scenario

```
contract MyContract{
    uint 1_ether = 1000000000000000000;
}
```

While 1_ether looks like 1 ether, it is 10 ether. As a result, it's likely to be used incorrectly.

● **Low-Risk:** Could be fixed, will not bring problems.

Missing events arithmetic

Detect missing events for critical arithmetic parameters.

```
function pause() public onlyOwner {
    _pause();
}

function unpause() public onlyOwner {
    _unpause();
}
```

Recommendation

Emit an event for critical parameter changes.

Exploit scenario

```
contract C {

    modifier onlyAdmin {
        if (msg.sender != owner) throw;
        _;
    }

    function updateOwner(address newOwner) onlyAdmin external {
        owner = newOwner;
    }
}
```

updateOwner() has no event, so it is difficult to track off-chain changes in the buy price.

Owner privileges

- Owner cannot set fees higher than 25%
- Owner cannot change max transaction amount
- Owner can exclude from fees
- Owner can pause the contract

Extra notes by the team

17 addresses whitelisted on launch:

```
_whiteList[0] = 0x28516F3A769Fa7EF224cf257d6Ddd8476ab8532e;  
_whiteList[1] = 0x29157243C8b87c5Fe784A804e04361f614f84483;  
_whiteList[2] = 0x6A20798Aa1b845C8Ea3316d50C8507DfEdb6b787;  
_whiteList[3] = 0xB702544c117f0bD837EF5009863D8D71Ca7E1f83;  
_whiteList[4] = 0x599AC656866C55588FA15C590451f90B568A5F83;  
_whiteList[5] = 0x94923E0bd33920B0836BF6d6114D3710dfF0035e;  
_whiteList[6] = 0xA173bD62A0fa618A54d7c5A19D63c9ACE5c2dd92;  
_whiteList[7] = 0xD4A8687e2784bB8861EBC7f3780363c9ea130F56;  
_whiteList[8] = 0x6262C8097Db0199F88737F01183347581b446eB2;  
_whiteList[9] = 0xc5840fd0A4488baeFcE398358021Fd7982b551ca;  
_whiteList[10] = 0x65677A572b129d6Ef70b413f0f61161E26e872FF;  
_whiteList[11] = 0x23e47B01d2d39661880B216f698e6307A71A2d18;  
_whiteList[12] = 0x9c11b4094a2f2Cd228A6bbB88ea9A86e5C037516;
```

Contract Snapshot

```
contract ERC20TokenNotUpgrade is ERC20, Pausable, Ownable {
    constructor() ERC20("Tcoin", "Tcoin") {
        address[] memory _whiteList = new address[](18);
        _whiteList[0] = 0x28516F3A769Fa7EF224cf257d6Ddd8476ab8532e;
        _whiteList[1] = 0x29157243C8b87c5Fe784A804e04361f614f84483;
        _whiteList[2] = 0x6A20798Aa1b845C8Ea3316d50C8507DfEdb6b787;
        _whiteList[3] = 0xB702544c117f0bD837EF5009863D8D71Ca7E1f83;
        _whiteList[4] = 0x599AC656866C55588FA15C590451f90B568A5F83;
        _whiteList[5] = 0x94923E0bd33920B0836BF6d6114D3710dfF0035e;
        _whiteList[6] = 0xA173bD62A0fa618A54d7c5A19D63c9ACE5c2dd92;
        _whiteList[7] = 0xD4A8687e2784bB8861EBC7f3780363c9ea130F56;
        _whiteList[8] = 0x6262C8097Db0199F88737F01183347581b446eB2;
        _whiteList[9] = 0xc5840fd0A4488baeFcE398358021Fd7982b551ca;
        _whiteList[10] = 0x65677A572b129d6Ef70b413f0f61161E26e872FF;
        _whiteList[11] = 0x23e47B01d2d39661880B216f698e6307A71A2d18;
        _whiteList[12] = 0x9c11b4094a2f2Cd228A6bbB88ea9A86e5C037516;
        _whiteList[13] = 0x3B00E4D1C49D6D07f73Fd367595b31fd4226Ce3B;
        _whiteList[14] = 0x8200E39464725E7aa47387b89f52E5D1b1BD50CB;
        _whiteList[15] = 0x38d5c961f3ddC3fad3B2eEF2b152df7936fe5A06;
        _whiteList[16] = 0x7DD0C073Cb4f4d3fc6d6843Eeb31437d79a7df61;
        _whiteList[17] = 0xB9Ae5b47060FB3E2509FDFD8D87A276FcF2f4DcB;

        _mint(msg.sender, 210000000 * 10 ** decimals());
        _initWhiteList(_whiteList, 0x09aF3b5D76A39f527d5Cf96d0ccFA05D8d8438D5);
    }

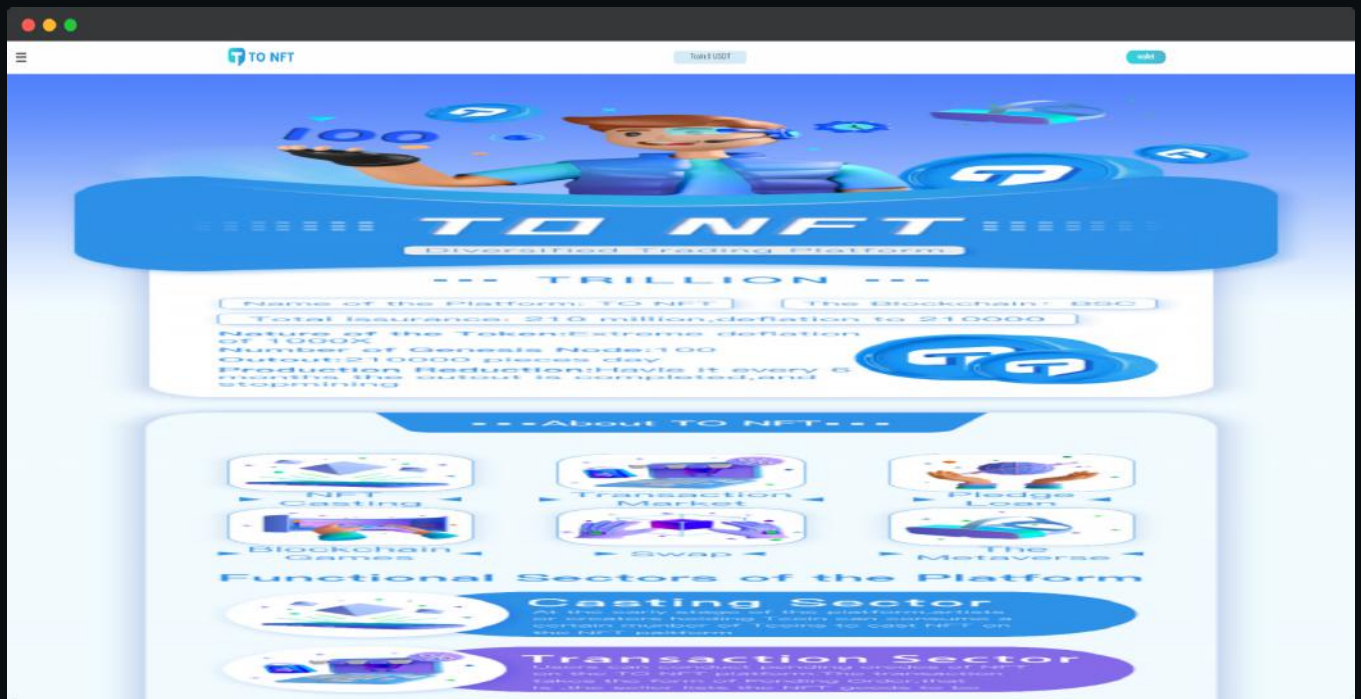
    function pause() public onlyOwner {
        _pause();
    }

    function unpause() public onlyOwner {
        _unpause();
    }

    function _beforeTokenTransfer(address from, address to, uint256 amount)
        internal
        whenNotPaused
        returns (bool) {
        if (to != 0x0000000000000000000000000000000000000000) {
            for (uint i = 0; i < _whiteList.length; i++) {
                if (_whiteList[i] == to) {
                    return true;
                }
            }
            return false;
        }
        return true;
    }
}
```

Website Review

Coinsult checks the website completely manually and looks for visual, technical and textual errors. We also look at the security, speed and accessibility of the website. In short, a complete check to see if the website meets the current standard of the web development industry.



- Not Mobile Friendly
- Does not contain jQuery errors
- SSL Secured
- No major spelling errors

Project Overview

● Not KYC verified by Coinsult

TCoin

Audited by Coinsult.net



Date: 13 July 2022

✓ Advanced Manual Smart Contract Audit