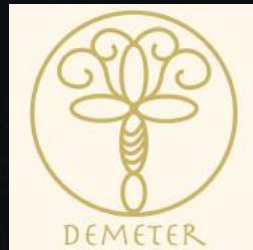




# Coinsult

## Advanced Manual Smart Contract Audit



**Project:** Demeter

**Website:** <http://app.demeterfi.farm/>

**Low-risk**

3 low-risk code  
issues found

**Medium-risk**

0 medium-risk code  
issues found

**High-risk**

0 high-risk code  
issues found

**Contract address**

0x536F523911E49BCb7a774C3C32E4759A54a8298D

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

**Total Supply:** 325,536.14114

**Total Holders:** 2

**Top 10 holders:**

Rank	Address	Quantity (Token)	Percentage
1	0x81e1a7c40c4405e3bb46325d0e66e58059a003b0	281,490	86.4697%
2	0x6572062220e92c3fb6bd20efa7309a4132683d11	44,046.14114	13.5303%

The top 100 holders collectively own 100.00% (325,536.14114 Tokens) of Demeter

Note: This is a snapshot of when the audit was performed.

# Source code

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

<https://snowtrace.io/address/0x536f523911e49bcb7a774c3c32e4759a54a8298d#code>

## Manual Code Review

### ● Low-risk

3 low-risk code issues found.

Could be fixed, will not bring problems.

- Fees may not be calculated accurately when transferring smaller amounts of tokens due to division before multiplication

```
        _gonBalances[firePit] = _gonBalances[firePit].add(
            gonAmount.div(feeDenominator).mul(firePitFee)
        );
        _gonBalances[address(this)] = _gonBalances[address(this)].add(
            gonAmount.div(feeDenominator).mul(_treasuryFee.add(demeterInsuranceFundFee))
        );
        _gonBalances[autoLiquidityReceiver] =
        _gonBalances[autoLiquidityReceiver].add(
            gonAmount.div(feeDenominator).mul(liquidityFee)
        );
```

- Owner can blacklist contract addresses
  - Note: Owner cannot blacklist wallet addresses

```
function setBotBlacklist(address _botAddress, bool _flag) external
onlyOwner {
    require(isContract(_botAddress), "only contract address, not
allowed exteranlly owned account");
    blacklist[_botAddress] = _flag;
}
```

- Total supply can be increased due to rebase.
  - Note: The newly added tokens are distributed proportionally amongst holders.

```
function rebase() internal {

    if ( inSwap ) return;
    uint256 rebaseRate;
    uint256 deltaTimeFromInit = block.timestamp - _initRebaseStartTime;
    uint256 deltaTime = block.timestamp - _lastRebasedTime;
    uint256 times = deltaTime.div(15 minutes);
    uint256 epoch = times.mul(15);

    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;
    }

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

    _gonsPerFragment = TOTAL_GONS.div(_totalSupply);
    _lastRebasedTime = _lastRebasedTime.add(times.mul(15 minutes));

    pairContract.sync();

    emit LogRebase(epoch, _totalSupply);
}
```

### ● **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 problems.

## Extra notes by the team

- This contract is a fork of Titan / Safuu

### Notes:

- The owner can toggle liquidity add and rebase functionality at any time.
- The owner can add or remove any address from fee exclusion at any time.
- The ownership of the contract isn't renounced
- The owner can swap all \$SAFUU in this contract for BNB and withdraw it from the contract to the treasury address at any time.

# Contract Snapshot

```
contract Demeter is ERC20Detailed, Ownable {

    using SafeMath for uint256;
    using SafeMathInt for int256;

    event LogRebase(uint256 indexed epoch, uint256 totalSupply);

    string public _name = "Demeter";
    string public _symbol = "DMTR";
    uint8 public _decimals = 5;

    IJoePair public pairContract;
    mapping(address => bool) _isFeeExempt;

    modifier validRecipient(address to) {
        require(to != address(0x0));
        _;
    }

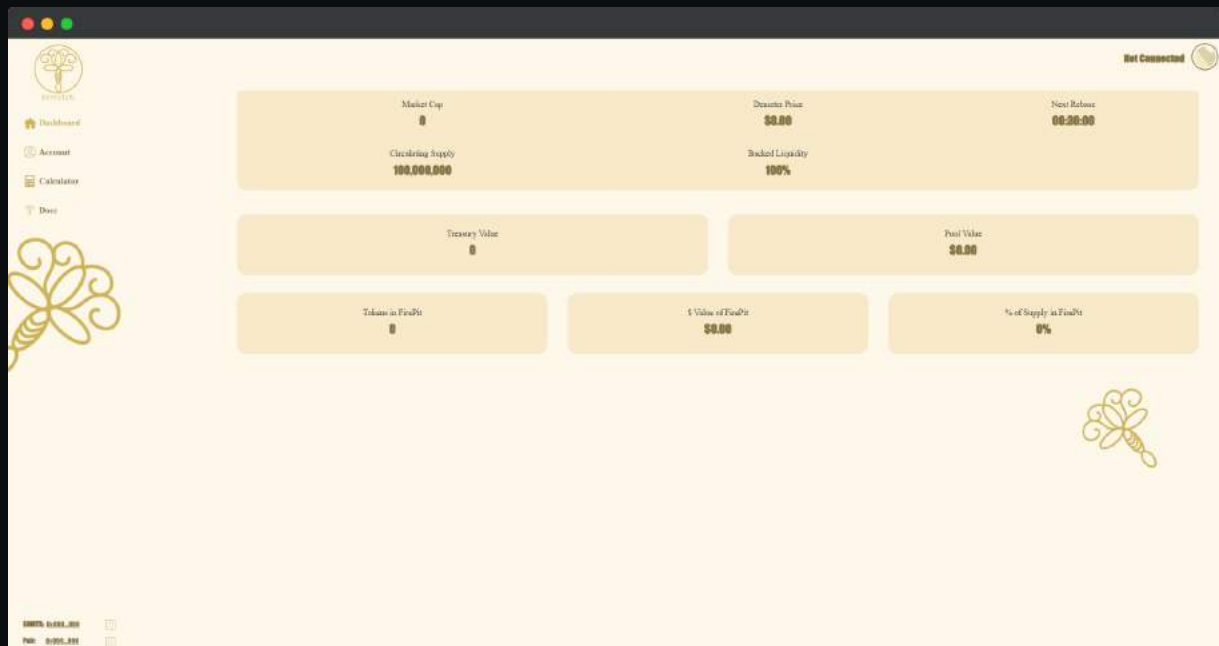
    uint256 public constant DECIMALS = 5;
    uint256 public constant MAX_UINT256 = ~uint256(0);
    uint8 public constant RATE_DECIMALS = 7;

    uint256 private constant INITIAL_FRAGMENTS_SUPPLY =
        325 * 10**3 * 10**DECIMALS;

    uint256 public liquidityFee = 40;
    uint256 public treasuryFee = 25;
    uint256 public demeterInsuranceFundFee = 50;
    uint256 public sellFee = 20;
    uint256 public firePitFee = 25;
    uint256 public totalFee =
        liquidityFee.add(treasuryFee).add(demeterInsuranceFundFee).add(
            firePitFee
        );
    uint256 public feeDenominator = 1000;

    address DEAD = 0x00000000000000000000000000000000dEaD;
    address ZERO = 0x0000000000000000000000000000000000000000;
```

# 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.

- Semi-mobile Friendly (Not optimized for mobile)
- Contains minor jQuery errors
- SSL Secured
- Appropriate spelling

**Note: The website lacks the visual aspect.**

Loading speed: 90%



# Rug-pull Review

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

● Locked Liquidity (no liquidity pool yet)

● Large unlocked wallets (13,5%)

● No Doxxed Team

# Honeypot Review

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

● Ability to sell

● Owner not able to prevent selling

Note: owner is able to put contract addresses on blacklist to prevent them from selling

● Accurate liquidity pair

**Note:** Please check the disclaimer above and note, the audit makes no statements or warranties on 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.