CROP Finance Liquidity Mining - Audit Report

SUMMARY

CROP Finance is building a DeFi yield aggregator for the lending platforms so users can reap maximum yields.

For this audit, we analyzed the project's liquidity mining platform. We reviewed the team's code at commit e90ddd353ab6accd5a2158c5ad9fe56e9b34e68d and later at commit aef55c12ecac3c4365ccc05d695d440cb907bd8c on GitHub.

> *Notes on the Contracts:*
>
> - *Users can stake USDC, USDT, and DAI tokens into the staking contract into order to earn CROP tokens. The logic for each of these staking*

- *Rewards earned by users depend on the amount of tokens sent to fund the contract, and the reward rate set by the team.*
- *The team will set the rewards end date upon deployment. This date can be extended, however, by the team via funding the contract and updating reward rates. Once the end block is reached the team will not be able to extend the rewards period.*
- *The owner has the ability to update the reward rate to any amount at any time. No other ownership-related functions exist.*
- *The "YearnContract" acts as a wrapper for the Yearn USDC, USDT, and DAI vaults; allowing the contract to deposit and withdraw from the vaults.*
- *The contract properly utilizes SafeMath to prevent overflows and SafeERC20 to ensure successful transfers.*
- *The team has worked with us to solve some logical issues and implement gas optimizations.*

Audit Findings Summary:

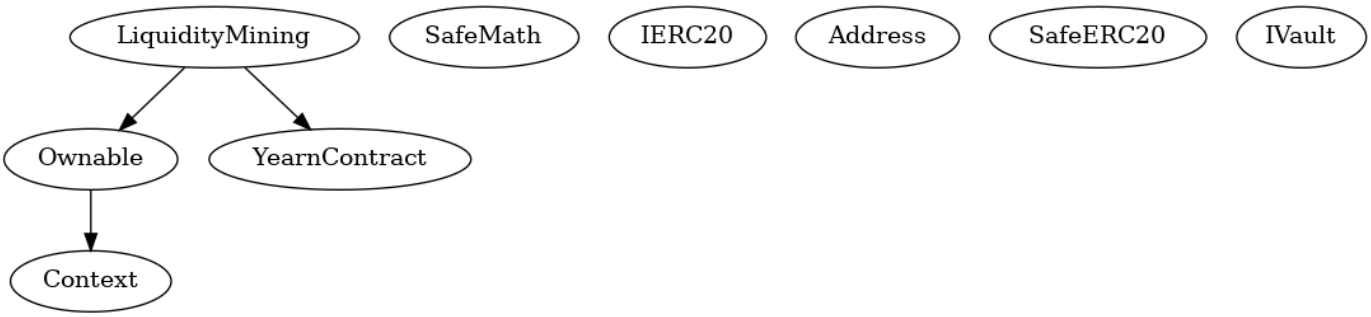
- *No security issues from outside attackers were identified.*
- *Ensure trust in the team as they have some control over the ecosystem.*
- *Date: March 18th, 2021*

COMBINED EXTERNAL THREAT RESULTS

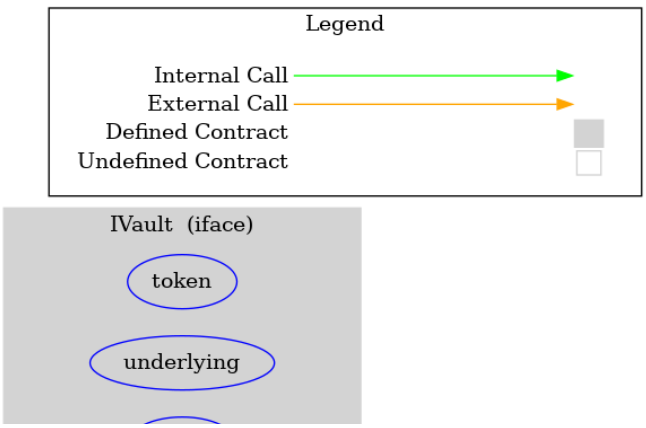
Vulnerability Category	Notes	Result
Arbitrary Jump	N/A	PASS
Delegate Call to Untrusted Contract	N/A	PASS
Dependence on Predictable Variables	N/A	PASS
Deprecated Opcodes	N/A	PASS
Ether Thief	N/A	PASS
Exceptions	N/A	PASS
External Calls	N/A	PASS
Integer Over/Underflow	N/A	PASS
Multiple Sends	N/A	PASS
Reentrancy	N/A	PASS
Suicide	N/A	PASS
State Change External Calls	N/A	PASS
Unchecked Retval	N/A	PASS

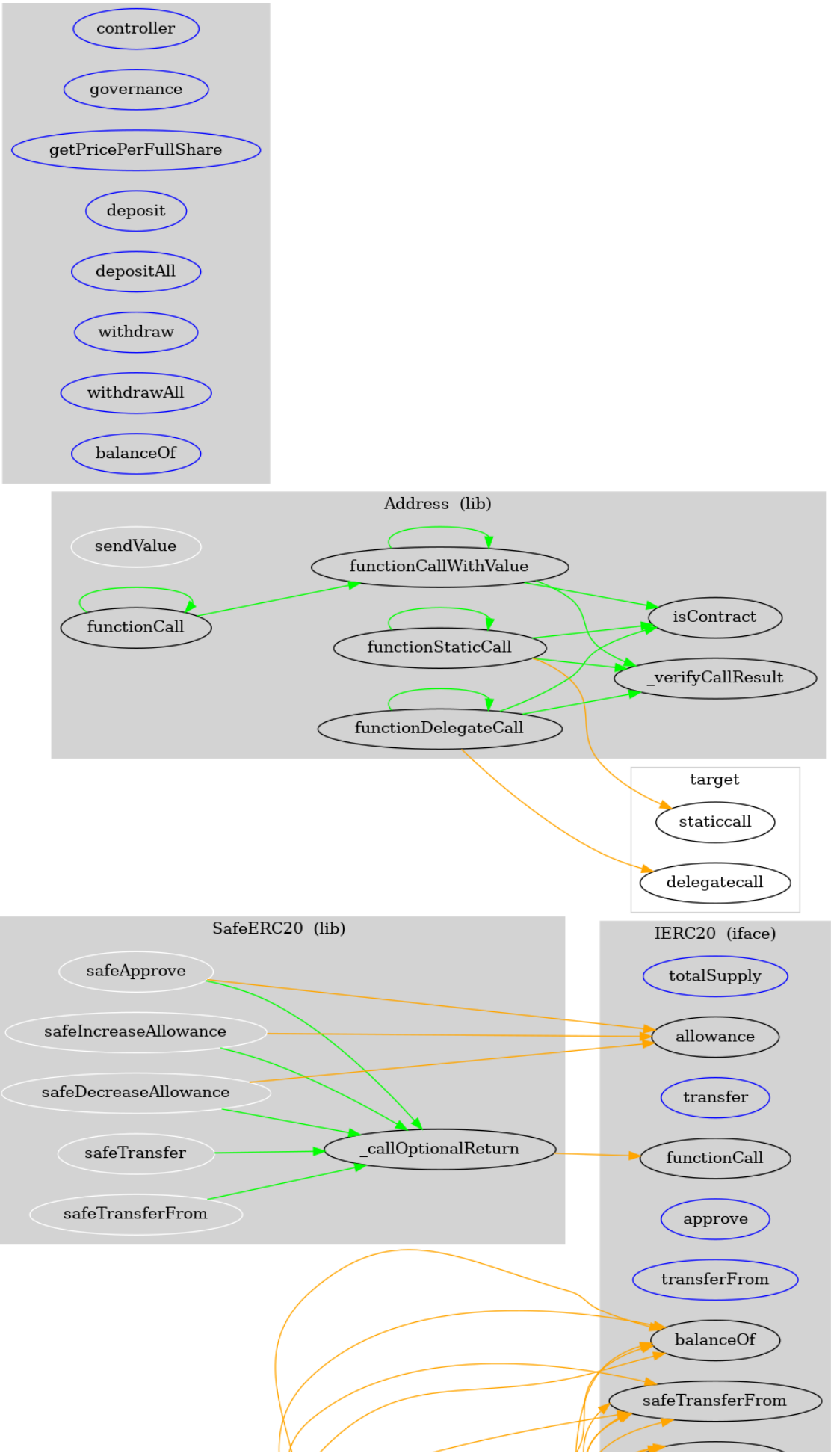
Vulnerability Category	Notes	Result
Critical Solidity Compiler	N/A	PASS
Overall Contract Safety		PASS

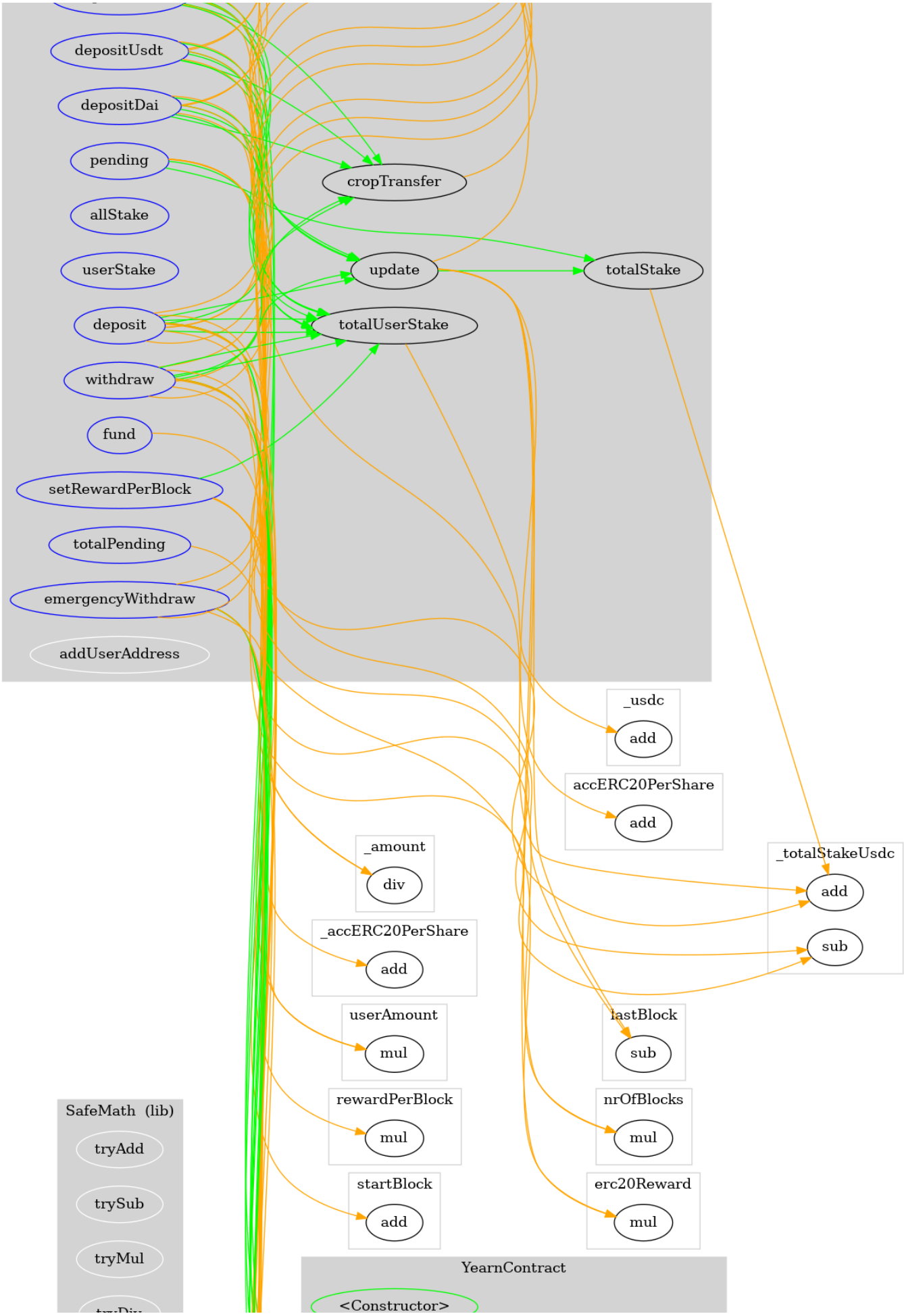
Inheritence Chart

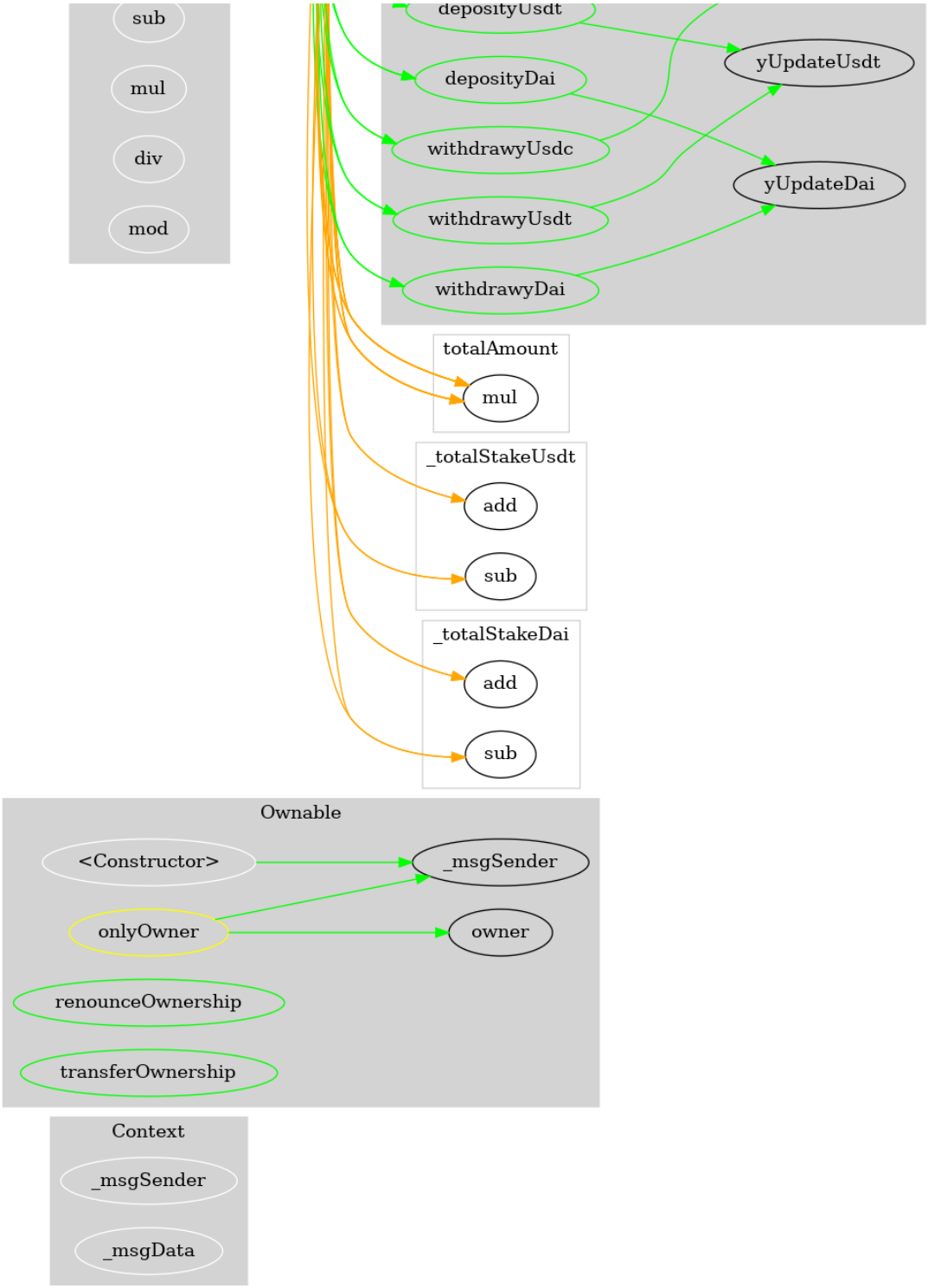


Function Graph









Functions Overview

```
# = non-constant function

Int = Internal
Ext = External
Pub = Public

+  Context
   - [Int] _msgSender
   - [Int] _msgData

+  Ownable (Context)
   - [Int]  #
   - [Pub] owner
   - [Pub] renounceOwnership #
      - modifiers: onlyOwner
   - [Pub] transferOwnership #
      - modifiers: onlyOwner

+ [Lib] SafeMath
   - [Int] tryAdd
   - [Int] trySub
   - [Int] tryMul
   - [Int] tryDiv
   - [Int] tryMod
   - [Int] add
   - [Int] sub
   - [Int] mul
   - [Int] div
   - [Int] mod
   - [Int] sub
   - [Int] div
   - [Int] mod
```

```
    - [Ext] transfer #
    - [Ext] allowance
    - [Ext] approve #
    - [Ext] transferFrom #

+  ERC20 (Context, IERC20)
    - [Pub]  #
    - [Pub] name
    - [Pub] symbol
    - [Pub] decimals
    - [Pub] totalSupply
    - [Pub] balanceOf
    - [Pub] transfer #
    - [Pub] allowance
    - [Pub] approve #
    - [Pub] transferFrom #
    - [Pub] increaseAllowance #
    - [Pub] decreaseAllowance #
    - [Int] _transfer #
    - [Int] _mint #
    - [Int] _burn #
    - [Int] _approve #
    - [Int] _setupDecimals #
    - [Int] _beforeTokenTransfer #

+ [Lib] Address
    - [Int] isContract
    - [Int] sendValue #
    - [Int] functionCall #
    - [Int] functionCall #
    - [Int] functionCallWithValue #
    - [Int] functionCallWithValue #
```

```
    - [Prv] _verifyCallResult

+ [Lib] SafeERC20
    - [Int] safeTransfer #
    - [Int] safeTransferFrom #
    - [Int] safeApprove #
    - [Int] safeIncreaseAllowance #
    - [Int] safeDecreaseAllowance #
    - [Prv] _callOptionalReturn #

+  ReentrancyGuard
    - [Int]  #

+ [Int] IVault
    - [Ext] token
    - [Ext] underlying
    - [Ext] name
    - [Ext] symbol
    - [Ext] decimals
    - [Ext] controller
    - [Ext] governance
    - [Ext] getPricePerFullShare
    - [Ext] deposit #
    - [Ext] depositAll #
    - [Ext] withdraw #
    - [Ext] withdrawAll #
    - [Ext] balanceOf

+  LiquidityMining (ReentrancyGuard, Ownable)
    - [Pub]  #
    - [Pub] fund #
    - [Ext] pending
```

- [Ext] userStake
- [Pub] totalStake
- [Pub] totalUserStake
- [Pub] depositUsdc #
- [Pub] depositUsdt #
- [Pub] depositDai #
- [Pub] deposit #
- [Pub] withdraw #
- [Pub] emergencyWithdraw #
- [Prv] update #
- [Int] addUserAddress #
- [Int] cropTransfer #
- [Pub] deposityUsdt #
- [Pub] deposityUsdc #
- [Pub] deposityDai #
- [Pub] withdrawyUsdt #
- [Pub] withdrawyUsdc #
- [Pub] withdrawyDai #

GO HOME