CA-2

Name:- Surendra Khyalia

Section:- K22CS

Course Code:-CSC307

Reg No.:- 12222968

Submitted To:- Piyush Gururani

Problem Statement

Prepare a Solidity smart contract with a function to transfer tokens, update it to ensure that only the owner can perform the transfer. Write the necessary code to restrict the function to the owner and modify it to log the transfer events. Assume the necessary variables and structures are already in place.

Contract code

```
// SPDX-License-Identifier: MIT
pragma solidity ^0.8.0;


contract TokenTransfer {
    address public owner;
    mapping(address => uint256) public balances;


    event Transfer(address indexed from, address indexed to, uint256 amount);
    constructor(uint256 initialSupply) {
        owner = msg.sender;
        balances[owner] = initialSupply;
    }

    modifier onlyOwner() {
        require(msg.sender == owner, "Only owner can perform this action");
        _;
    }

    function transfer(address to, uint256 amount) public onlyOwner {
        require(balances[owner] >= amount, "Insufficient balance");
        balances[owner] -= amount;
        balances[to] += amount;

        emit Transfer(owner, to, amount);
    }
}
```

Contract Overview

This smart contract is a token transfer system on the Ethereum blockchain. Designed for simplicity, it allows only the contract owner to initiate token transfers to other accounts. The contract includes basic functions for token storage and transfer and incorporates security measures to restrict specific actions to the owner.

Basic Implementaon

owner : Stores the address of the contract's owner.

balances : Maps addresses to their corresponding token balances.

from: The address sending the tokens.

to: The address receiving the tokens.

amount: The number of tokens transferred. The indexed keyword allows filtering based on these parameters when querying events.

initialSupply: This parameter sets the initial token supply for the contract.

Modifier

onlyOwner

It Restricts access to transfer functions, ensuring only the owner can execute transfer. Verifies the caller's identity (msg.sender == owner); if the caller is not the owner, the transaction reverts with the message "Only owner can perform this action."

Transfer Function

Allows the owner to transfer tokens to any specified address. Parameters used are (to: Recipient's address and amount: Amount of tokens to transfer). The function (require(balances[owner] >= amount)) checks that the owner has a sufficient balance for the transfer.

References

Solidity Documentation: https://soliditylang.org/

OpenZeppelin Contracts: https://www.openzeppelin.com/solidity-contracts/