**ACTIVIDAD PRÁCTICA # 1**

**Tipo actividad: Desarrollo en plataforma**

**Actividad práctica 1: Implementación de Técnicas de Anonimización de Transacciones en Ethereum**

**Descripción:**

Los participantes aprenderán a implementar técnicas de anonimización de transacciones en la red Ethereum utilizando un smart contract y una plataforma de desarrollo como Remix.

**Pasos:**

**Configuración del Entorno:**

Acceder a [Remix](https://remix.ethereum.org/), una plataforma en línea para el desarrollo de contratos inteligentes en Ethereum.

Crear un nuevo archivo llamado Anonimizador.sol y asegurarse de seleccionar la versión del compilador de Solidity adecuada.

### 

// SPDX-License-Identifier: MIT

pragma solidity ^0.8.0;

contract Anonimizador {

mapping(address => address) private \_anonimizaciones;

function anonimizar() public payable {

// Generar una dirección de billetera aleatoria para anonimizar la transacción

address direccionAnonima = address(uint160(uint256(keccak256(abi.encodePacked(block.timestamp, block.difficulty, msg.sender)))));

// Asignar la dirección de billetera original a la dirección anónima generada

\_anonimizaciones[msg.sender] = direccionAnonima;

// Transferir los fondos a la dirección anónima

payable(direccionAnonima).transfer(msg.value);

}

function obtenerDireccionAnonima() public view returns (address) {

// Obtener la dirección anónima asociada a la dirección de billetera del usuario

return \_anonimizaciones[msg.sender];

}

}

Este contrato inteligente permite a los usuarios anonimizar sus transacciones al generar una dirección de billetera aleatoria y transferir los fondos a esta dirección.

**Compilar y Desplegar el Contrato:**

Compilar el contrato haciendo clic en el botón "Compile" en Remix.

Desplegar el contrato seleccionando la pestaña "Deploy & run transactions" y ajustar los parámetros de despliegue según sea necesario.

Interactuar con el Contrato:

Utilizar MetaMask u otra billetera Ethereum para interactuar con el contrato desplegado.

Llamar a la función anonimizar() para anonimizar una transacción y transferir fondos a una dirección aleatoria.

Utilizar la función obtenerDireccionAnonima() para obtener la dirección anónima asociada a la dirección de billetera del usuario.

Solución en Remix:

**Configuración del Entorno:**

Accede a Remix.

Crea un nuevo archivo llamado Anonimizador.sol y selecciona la versión del compilador de Solidity 0.8.0.

### 

// SPDX-License-Identifier: MIT

pragma solidity ^0.8.0;

contract Anonimizador {

mapping(address => address) private \_anonimizaciones;

function anonimizar() public payable {

// Generar una dirección de billetera aleatoria para anonimizar la transacción

address direccionAnonima = address(uint160(uint256(keccak256(abi.encodePacked(block.timestamp, block.difficulty, msg.sender)))));

// Asignar la dirección de billetera original a la dirección anónima generada

\_anonimizaciones[msg.sender] = direccionAnonima;

// Transferir los fondos a la dirección anónima

payable(direccionAnonima).transfer(msg.value);

}

function obtenerDireccionAnonima() public view returns (address) {

// Obtener la dirección anónima asociada a la dirección de billetera del usuario

return \_anonimizaciones[msg.sender];

}

}

**Compilar y Desplegar el Contrato:**

Haz clic en la pestaña "Solidity Compiler" y compila el contrato.

Ve a la pestaña "Deploy & run transactions", elige el ambiente (por ejemplo, JavaScript VM), ajusta los parámetros de despliegue y haz clic en "Deploy".

Interactuar con el Contrato:

Utiliza MetaMask u otra billetera Ethereum conectada a Remix.

Haz clic en el botón "**anonimizar()**" para anonimizar una transacción y transferir fondos a una dirección aleatoria.

Haz clic en el botón "**obtenerDireccionAnonima()**" para obtener la dirección anónima asociada a tu dirección de billetera.