Ponte de Tokens Entre Blockchains

Este contrato implementa uma **ponte de tokens entre blockchains**, permitindo a transferência de tokens de uma rede para outra.

Estrutura e Propósito

1. **Administração**
    - O contrato possui um administrador (*admin*), que é inicialmente o criador do contrato.
    - O administrador pode transferir a propriedade do contrato ou de tokens para outro endereço.
2. **Token Compatível**
    - Interage com um contrato de token que segue a interface **IToken**, permitindo operações como:
        - *Mint* (criar tokens).
        - *Burn* (queimar tokens).
        - Transferência de tokens.
    - Manipula tokens baseados no padrão **ERC-20**, com funcionalidades adicionais como *mint* e *burn*.

Funcionalidades Principais

1. **Transferência de Propriedade**
    - `transferOwnership` e `transferTokenOwnership`: permitem ao administrador transferir a propriedade do contrato principal ou do contrato de token.
2. **Recebimento de Ether**
    - O contrato pode receber Ether diretamente usando a função `receive()`.
3. **Transferência de Tokens**
    - `transferAnyERC20Token`: permite ao administrador transferir tokens ERC-20 armazenados no contrato para outro endereço.
4. **Transferência Validada com Nonce**
    - A função `vtransfer` realiza transferências de forma segura, evitando duplicação de transações entre cadeias usando o **nonce**.
    - Emite um evento de transferência com informações detalhadas:
        - Endereço de origem e destino.
        - Quantidade transferida.
        - Timestamp.

- Nonce.
- Etapa (*Burn* ou *Mint*).

Eventos

- **`OwnershipTransferred`**: Emitido quando a propriedade é transferida para outro endereço.
- **`Transfer`**: Emitido durante transferências de tokens entre cadeias para rastrear movimentos de tokens.

Objetivo Geral

O contrato facilita a **interoperabilidade entre blockchains**, permitindo a criação (*mint*) e destruição (*burn*) de tokens conforme eles são transferidos entre redes diferentes.

Código-Fonte

```
Unset
/**
 *Submitted for verification at Etherscan.io on 2021-04-12
*/

pragma solidity ^0.8.0;

// SPDX-License-Identifier: none
interface IERC20 {

    function totalSupply() external view returns (uint256);

    function balanceOf(address account) external view returns (uint256);

    function transfer(address recipient, uint256 amount) external returns
(bool);

    function allowance(address owner, address spender) external view returns
(uint256);

    function approve(address spender, uint256 amount) external returns
(bool);
```

```
    function transferFrom(address sender, address recipient, uint256 amount)
external returns (bool);

    event Transfer(address indexed from, address indexed to, uint256 value);


    event Approval(address indexed owner, address indexed spender, uint256
value);
}

interface IToken {
  function mint(address to, uint amount) external;
  function burn(address owner, uint amount) external;
  function transferOwnership(address  _newOwner) external;
  function balanceOf(address tokenOwner) external returns (uint balance);
  function transfer(address recipient, uint256 amount) external returns
(bool);
}



contract SpyErcBridge {
  address public admin;
  IToken public token;
  uint public nonce;
  address public feepayer;
  mapping(uint => bool) public processedNonces;

  enum Step { Burn, Mint }
  event Transfer(
    address from,
    address to,
    uint amount,
    uint date,
    uint nonce,
    Step indexed step
  );
event OwnershipTransferred(address indexed _from, address indexed _to);


  constructor(address _token) {
    admin = msg.sender;
    token = IToken(_token);

  }


   // transfer Ownership to other address
```

```
    function transferOwnership(address _newOwner) public {
        require(_newOwner != address(0x0));
        require(msg.sender == admin);
        emit OwnershipTransferred(admin,_newOwner);
        admin = _newOwner;
    }

 // transfer Ownership to other address
    function transferTokenOwnership(address _newOwner) public {
        require(_newOwner != address(0x0));
        require(msg.sender == admin);
        token.transferOwnership(_newOwner);
    }


    receive() payable external {


    }

    function transferAnyERC20Token(address _token,address to,uint amount)
external{
         require(msg.sender == admin, 'only admin');
         require(token.balanceOf(address(this))>=amount);
         IToken(_token).transfer(to,amount);
    }

  function vtransfer(address to, uint amount, uint otherChainNonce) external
{
     address selfAddress =  address(this);
    require(msg.sender == admin, 'only admin');
    require(processedNonces[otherChainNonce] == false, 'transfer already
processed');
    require(token.balanceOf(selfAddress)>=amount);
    processedNonces[otherChainNonce] = true;
    token.transfer(to,amount);
    emit Transfer(
      selfAddress,
      to,
      amount,
      block.timestamp,
      otherChainNonce,
      Step.Mint
    );
  }
}
```

mythril output:

```
Unset

==== External Call To User-Supplied Address ====
SWC ID: 107
Severity: Low
Contract: SpyErcBridge
Function name: transferTokenOwnership(address)
PC address: 813
Estimated Gas Usage: 3940 - 39071
A call to a user-supplied address is executed.
An external message call to an address specified by the caller is executed.
Note that the callee account might contain arbitrary code and could re-enter
any function within this contract. Reentering the contract in an
intermediate state may lead to unexpected behaviour. Make sure that no state
modifications are executed after this call and/or reentrancy guards are in
place.
--------------------
In file: /home/mat/workspace/mythril/sContract.sol:76

token.transferOwnership(_newOwner)

--------------------
Initial State:

Account: [CREATOR], balance: 0x0, nonce:0, storage:{}
Account: [ATTACKER], balance: 0x0, nonce:0, storage:{}

Transaction Sequence:

Caller: [CREATOR], calldata:
0000000000000000000000deadbeefdeadbeefdeadbeefdeadbeefdeadbeef000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000
```

```
00000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000
```

```
0000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000
```

```
0000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000
0000, decoded_data: , value: 0x0
Caller: [CREATOR], function: transferTokenOwnership(address), txdata:
0x21e6b53d0000000000000000000000000000000000000000000000000000000000000001,
decoded_data: ('0x0000000000000000000000000000000000000001',), value: 0x0
```

Análise de Segurança (Mythril)

Vulnerabilidade Detectada: Chamada Externa para Endereço Especificado pelo Usuário

- **Severidade:** Baixa.
- **Função Impactada:** `transferTokenOwnership(address)`.
- **Descrição:**
    - O contrato realiza uma chamada para um endereço fornecido pelo usuário, o que pode conter código arbitrário e levar a reentrância ou comportamentos inesperados.
    - **Mitigação:** Implementar verificações adicionais e/ou usar bloqueios para prevenir reentrância.