# ERC20 代币合约

pragma solidity ^0.4.16;

interface tokenRecipient { function receiveApproval(address \_from, uint256 \_value, address \_token, bytes \_extraData) external; }

contract TokenERC20 {

// Public variables of the token

string public name;

string public symbol;

uint8 public decimals = 18;

// 18 decimals is the strongly suggested default, avoid changing it

uint256 public totalSupply;

// This creates an array with all balances

mapping (address => uint256) public balanceOf;

mapping (address => mapping (address => uint256)) public allowance;

// This generates a public event on the blockchain that will notify clients

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

// This generates a public event on the blockchain that will notify clients

event Approval(address indexed \_owner, address indexed \_spender, uint256 \_value);

// This notifies clients about the amount burnt

event Burn(address indexed from, uint256 value);

/\*\*

\* Constructor function

\*

\* Initializes contract with initial supply tokens to the creator of the contract

\*/

function TokenERC20(

uint256 initialSupply,

string tokenName,

string tokenSymbol

) public {

totalSupply = initialSupply \* 10 \*\* uint256(decimals); /\*Update total supply with the

decimal amount\*/

balanceOf[msg.sender] = totalSupply; // Give the creator all initial tokens

name = tokenName; // Set the name for display purposes

symbol = tokenSymbol; // Set the symbol for display purposes

}

/\*\*

\* Internal transfer, only can be called by this contract

\*/

function \_transfer(address \_from, address \_to, uint \_value) internal {

// Prevent transfer to 0x0 address. Use burn() instead

require(\_to != 0x0);

// Check if the sender has enough

require(balanceOf[\_from] >= \_value);

// Check for overflows

require(balanceOf[\_to] + \_value >= balanceOf[\_to]);

// Save this for an assertion in the future

uint previousBalances = balanceOf[\_from] + balanceOf[\_to];

// Subtract from the sender

balanceOf[\_from] -= \_value;

// Add the same to the recipient

balanceOf[\_to] += \_value;

emit Transfer(\_from, \_to, \_value);

// Asserts are used to use static analysis to find bugs in your code. They should never fail

assert(balanceOf[\_from] + balanceOf[\_to] == previousBalances);

}

/\*\*

\* Transfer tokens

\*

\* Send `\_value` tokens to `\_to` from your account

\*

\* @param \_to The address of the recipient

\* @param \_value the amount to send

\*/

function transfer(address \_to, uint256 \_value) public returns (bool success) {

\_transfer(msg.sender, \_to, \_value);

return true;

}

/\*\*

\* Transfer tokens from other address

\*

\* Send `\_value` tokens to `\_to` on behalf of `\_from`

\*

\* @param \_from The address of the sender

\* @param \_to The address of the recipient

\* @param \_value the amount to send

\*/

function transferFrom(address \_from, address \_to, uint256 \_value) public returns (bool success) {

require(\_value <= allowance[\_from][msg.sender]); // Check allowance

allowance[\_from][msg.sender] -= \_value;

\_transfer(\_from, \_to, \_value);

return true;

}

/\*\*

\* Set allowance for other address

\*

\* Allows `\_spender` to spend no more than `\_value` tokens on your behalf

\*

\* @param \_spender The address authorized to spend

\* @param \_value the max amount they can spend

\*/

function approve(address \_spender, uint256 \_value) public

returns (bool success) {

allowance[msg.sender][\_spender] = \_value;

emit Approval(msg.sender, \_spender, \_value);

return true;

}

/\*\*

\* Set allowance for other address and notify

\*

\* Allows `\_spender` to spend no more than `\_value` tokens on your behalf, and then ping the contract about it

\*

\* @param \_spender The address authorized to spend

\* @param \_value the max amount they can spend

\* @param \_extraData some extra information to send to the approved contract

\*/

function approveAndCall(address \_spender, uint256 \_value, bytes \_extraData)

public

returns (bool success) {

tokenRecipient spender = tokenRecipient(\_spender);

if (approve(\_spender, \_value)) {

spender.receiveApproval(msg.sender, \_value, this, \_extraData);

return true;

}

}

/\*\*

\* Destroy tokens

\*

\* Remove `\_value` tokens from the system irreversibly

\*

\* @param \_value the amount of money to burn

\*/

function burn(uint256 \_value) public returns (bool success) {

require(balanceOf[msg.sender] >= \_value); // Check if the sender has enough

balanceOf[msg.sender] -= \_value; // Subtract from the sender

totalSupply -= \_value; // Updates totalSupply

emit Burn(msg.sender, \_value);

return true;

}

/\*\*

\* Destroy tokens from other account

\*

\* Remove `\_value` tokens from the system irreversibly on behalf of `\_from`.

\*

\* @param \_from the address of the sender

\* @param \_value the amount of money to burn

\*/

function burnFrom(address \_from, uint256 \_value) public returns (bool success) {

require(balanceOf[\_from] >= \_value); // Check if the targeted balance is enough

require(\_value <= allowance[\_from][msg.sender]); // Check allowance

balanceOf[\_from] -= \_value; // Subtract from the targeted balance

allowance[\_from][msg.sender] -= \_value; // Subtract from the sender's allowance

totalSupply -= \_value; // Update totalSupply

emit Burn(\_from, \_value);

return true;

}

}