



Desarrollo de Tarea Web 3.0 - Blockchain

Alejandro Beltran
Victor Manchola



Proceso de Diseño - Parte 1 (Invidividual)

- Toma de notas de clases, revisando grabaciones
- Contrato en *Solidity* siguiendo estándar ERC-20
- Decidiendo un nombre para nuestras criptomonedas
- Escribiendo el contrato en código utilizando *OpenZeppelin*
- Funciones de:
 - Constructor
 - Pausa y Reanudo
 - Mint
 - Antes de Transferencia

DEPLOY & RUN
TRANSACTIONS

3000000

VALUE

0Wei

CONTRACT

ALejobzCOIN - ALejobzCOIN.sol

Deploy

☐ Publish to IPFS

OR

At AddressLoad contract from Address

Transactions recorded 1

Deployed Contracts

Currently you have no contract instances to interact with.

```
1 // SPDX-License-Identifier: MIT
2 pragma solidity ^0.8.4;
3
4 import "@openzeppelin/contracts@4.7.3/token/ERC20/ERC20.sol";
5 import "@openzeppelin/contracts@4.7.3/token/ERC20/extensions/ERC20Burnable.sol";
6 import "@openzeppelin/contracts@4.7.3/security/Pausable.sol";
7 import "@openzeppelin/contracts@4.7.3/access/Ownable.sol";
8
9 contract ALejobzCOIN is ERC20, ERC20Burnable, Pausable, Ownable {
10     constructor() ERC20("ALejobzCOIN", "ABZ") {
11         _mint(msg.sender, 1000000 * 10 ** decimals());
12     }
13
14     function pause() public onlyOwner {
15         _pause();
16     }
17
18     function unpause() public onlyOwner {
19         _unpause();
20     }
21
22     function mint(address to, uint256 amount) public onlyOwner {
23         _mint(to, amount);
24     }
25
26     function _beforeTokenTransfer(address from, address to, uint256 amount)
27         internal
```

MetaMask Notification

Ropsten Test Network

Account 1New Contract

https://remix.ethereum.org

CONTRACT DEPLOYMENT

DETAILSDATA

Estimated gas fee0.004739770.00474 RopstenETH

Site suggestedVery likely in < 15 seconds

Max fee:0.00473977 RopstenETH

Total0.004739770.00473977 RopstenETH

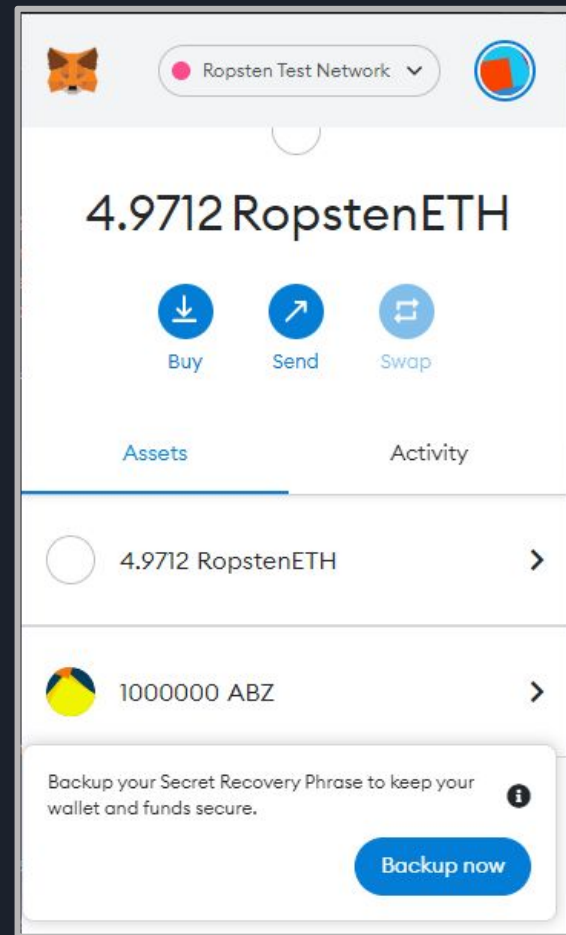
Amount + gas feeMax amount:0.00473977 RopstenETH

RejectConfirm

Código en Funcionamiento (ALejobzCOIN)

transfer	address to, uint256 amount	▼
transferFr...	address from, address to, uint256 amount	▼
transferO...	address newOwner	▼
unpause		
allowance	address owner, address spends	▼
balanceOf	address account	▼
decimals		
name		
0: string: ALLejobzCOIN		
owner		
paused		
symbol		
0: string: ABZ		
totalSupply		

allowance	address owner, address spends
balanceOf	address account
decimals	
name	0: string: ALJobzCOIN
owner	
paused	
symbol	0: string: ABZ
totalSupply	0: uint256: 1000000000000000000000000



Identificador, símbolo de la moneda y suministro total la conexión con METAMASK

approve	address spender, uint256 amou	▼
burn	uint256 amount	▼
burnFrom	address account, uint256 amou	▼
decreaseA...	address spender, uint256 subtr	▼
increaseAL...	address spender, uint256 adde	▼
mint	address to, uint256 amount	▼
pause		
renounce...		
transfer	address to, uint256 amount	▼
transferFr...	address from, address to, uint2	▼
transferO...	address newOwner	▼
unpause		

transferO...	address newOwner	▼
unpause		
allowance	address owner, address spende	▼
balanceOf	0x13838D84EB4D394f33A7E	▼
0: uint256: 10000000000000000000000000000000		
decimals		
name		
0: string: ALejobzCOIN		
owner		
paused		
symbol		

allowance	address owner, address spende	▼
balanceOf	0x8125831a52C2f5EB22c609	▼
0: uint256: 0		
decimals		
0: string: ALejobzCOIN		
owner		
paused		
symbol		

Control de emisiones, balance de mi address y de la address de mi compañero

DEPLOY & RUN
TRANSACTIONS

decreaseA...

address spender, uint256 subtr

increaseAL...

address spender, uint256 addde

mint

address to, uint256 amount

pause

renounce...

transfer

to: 0x8125831a52C2f5EB22c609Cf

amount: 50000000000000000000

CalldataParameterstransact

transferFr...

address from, address to, uint256

transferO...

address newOwner

unpause

allowance

address owner, address spends

MetaMask Notification

< Edit

Ropsten Test Network

Account 1

0x812...de80

New address detected! Click here to add to your address book.

https://remix.ethereum.org

0xa1b...C171 : TRANSFER ⓘ

50 ABZ

DETAILSDATAHEX

Estimated gas fee

0.00013656

0.000137 RopstenETH

Site suggested
Very likely in < 15 seconds

Max fee: 0.00013656 RopstenETH

allowance

address owner, address spends

balanceOf

0x8125831a52C2f5EB22c609

0: uint256: 50000000000000000000

decimals

name

0: string: ALejobzCOIN

owner

paused

symbol

0: string: ABZ

totalSupply

Transfiriendo la moneda

Código en Funcionamiento (VCoin)

```
// Desarrollo de Tarea 3 de Tecnologías Emergentes
// Victor Manchola
// Licencia del programa:
// ---SPDX-License-Identifier: MIT

// Pragma, Imports
pragma solidity ^0.8.4;
import "@openzeppelin/contracts@4.7.3/token/ERC20/ERC20.sol";
import "@openzeppelin/contracts@4.7.3/token/ERC20/extensions/ERC20Burnable.sol";
import "@openzeppelin/contracts@4.7.3/security/Pausable.sol";
import "@openzeppelin/contracts@4.7.3/access/Ownable.sol";

// Contrato
contract VCoin is ERC20, ERC20Burnable, Pausable, Ownable {
    constructor() ERC20("VCoin", "VAM") {}

    _mint(msg.sender, 1000000 * 10 ** decimals());

    function pause() public onlyOwner {
        _pause();
    }

    function unpause() public onlyOwner {
        _unpause();
    }

    function mint(address to, uint256 amount) public onlyOwner {
        _mint(to, amount);
    }

    function _beforeTokenTransfer(address from, address to, uint256 amount)
        internal
        whenNotPaused
        override
    {
        super._beforeTokenTransfer(from, to, amount);
    }
}
```



Proceso de Diseño - Parte 2 (Grupos)

- Desarrollo de la interfaz en *JavaScript* primero
 - Campos de entrada de texto
 - Búsqueda
 - Botones con acciones
- Desarrollo del contrato en *Solidity*
 - Funcionalidad para cada entrada en Blockchain
 - Funcionalidad de búsqueda
- Creación de un servidor con express
- Uniendo el contrato con la interfaz

DISEÑO

DEPLOY & RUN
TRANSACTIONS

Transactions recorded 1

Deployed Contracts

ISSUANCECERTIFICATES AT 0XD9:

Balance: 0 ETH

addCretific... string _name, string _id, string _

certificates uint256

compareSt... string _s1, string _s2

numCertifi...

verifyCerti... string _search

Low level interactions

CALLDATA

Transact

contract-b32c30adac.sol

ALejobzCOIN.sol

cretificado.sol

```
17 constructor() public {
18     owner = msg.sender;
19 }
20
21 function addCretificate(string _name, string _id, string _date, string _course) public{
22     certificates.push(certificate(_name, _id, _date, _course));
23     nCertificates = nCertificates + 1;
24 }
25
26
27 function numCertificates() public view returns(uint){
28     return (certificates.length);
29 }
30
31 function compareStrings(string memory _s1, string memory _s2) public pure returns(bool areEual){
32     return keccak256(abi.encodePacked(_s1)) == keccak256(abi.encodePacked(_s2));
33 }
34
35 function verifyCertificate(string _search) public view returns(string cer){
36     uint quantity = 0;
37     for (uint i; i < certificates.length; i++) {
38         if((compareStrings(_search,certificates[i].name)) || (compareStrings(_search,certificates[
39             quantity += 1;
40     }
41 }
42 if(quantity > 0){
```

listen on all transactions

Search with transaction hash or address

DISEÑO

```
//Deploy del contrato en la interfaz
const Address = "0x74B8e13C1Fc19da6d1a2816bf0DA72625832ea80";
window.web3 = await new Web3(window.ethereum);
window.contract = await new window.web3.eth.Contract( ABI, Address);
document.getElementById("contractArea").innerHTML = "connected to smart contract";
```

```
const ABI = [
{
  "constant": false,
  "inputs": [
    {
      "name": "_name",
      "type": "string"
    },
    {
      "name": "_id",
      "type": "string"
    },
    {
      "name": "_date",
      "type": "string"
    },
    {
      "name": "_course",
      "type": "string"
    }
  ],
  "name": "addCretificate",
  "outputs": [],
  "payable": false,
  "stateMutability": "nonpayable",
  "type": "function"
},
```

http://127.0.0.1:5000

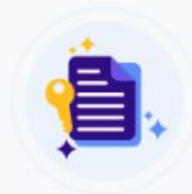
Connect With MetaMask

Select the account(s) to use on this site

[New Account](#)



Account 1 (0x138...ef4...)
0 ETH



Soporte de emisión de certificados

Soporte de emisión de certificados de asistencia a un curso para agregar y verificar la existencia de certificados.

Emision de certificados

Nombre del estudiante

Número de identificación

Fecha de participación

Nombre del curso

Emitir certificado

Conectar metamask

0x13838d84eb4d394f33a7e3a8a13cb54f28beef4b

Conectar contrato

connected to smart contract

Verificar existencia

Buscar

Verificar número de contratos

Numero de certificados

0

Emission de certificados

Nombre del estudiante

Alejandro Beltrán

Número de identificación

1007489283

Fecha de participación

22/09/2022

Nombre del curso

Tecnologías emergentes

Emitir certificado

Certificado agregado con éxito

Verificar existencia

1007489283

Buscar

Exists!

Verificar existencia

Victor Manchola

Buscar

Dont Exists!

Código en Funcionamiento

Emission de certificados

Nombre del estudiante

Victor Manchola

Número de identificación

123456789

Fecha de participación

22/09/2022

Nombre del curso

Tecnologías emergentes

Emitir certificado

Certificado agregado con éxito

Verificar existencia

123456789

Buscar

Exists!

Verificar número de contratos

Numero de certificados

2

Verificar existencia

Victor Manchola

Buscar

Exists!

Código en Funcionamiento



Problemas Encontrados

- Pocas dificultades en Parte 1 gracias a *OpenZeppelin*
- Comparación de strings en *Solidity* por lo que se dificultó realizar la parte de la creación del contrato inteligente
- **Integración** (interfaz web gráfica y contrato inteligente) fue la parte que tomó más tiempo
 - Diferentes problemas en cuanto a la **testnet**
 - Integración diferente a la vista en clase
 - Problemas al agregar nuevos certificados



CONCLUSIONES

Muchas gracias...

