Curso de Smart Contracts en Ethereum

BLOCKCHAIN
ACADEMY
MÉXICO

Objetivo

Aprender los conceptos básicos de un blockchain levantando un blockchain local

Crearemos un sistema básico de votaciones utilizando una cadena de bloques personal de Ethereum para ejecutar pruebas, comandos e inspeccionar el estado mientras controlamos cómo funciona la cadena.

BLOCKCHAIN ACADEMY MÉXICO

Requisitos

- Sistema Operativo: **MacOS** o

Virtualbox

- Sistema Operativo: **Ubuntu**
- Node.js version >8 - nodejs.org
- npm / node package manager / latest version

  `npm install npm@latest -g`
- git / latest version
- Sublime Text o el editor de texto preferido

y sus respectivas dependencias (python, ruby, etc…)

BLOCKCHAIN ACADEMY MÉXICO

1. Instalar herramientas

Instalar Geth => Ethereum

Geth es la interface de línea de comandos para correr un nodo completo de ethereum implementado en Go. Es parte del lanzamiento de **Frontier.**

```
$ sudo apt-get install software-properties-common
$ sudo add-apt-repository -y ppa:ethereum/ethereum
$ sudo apt-get update
$ sudo apt-get install ethereum
```

Mac

```
$ brew tap ethereum/ethereum
$ brew install ethereum
```

Fuente: https://github.com/ethereum/go-ethereum/wiki

BLOCKCHAIN ACADEMY MÉXICO

Instalar herramientas complementarias

solc - Solidity Compiler

```
$ sudo npm install solc
```

```
$ sudo npm install -g solc
```

Alternativo: sudo snap install solc

Fuente: http://solidity.readthedocs.io/en/v0.4.21/installing-solidity.html

web3 - Ethereum Javascript API

```
$ sudo npm install web3@0.20.1
```

```
$ sudo npm install -g web3@0.20.1
```

***Nota: En este ejercicio,** es importante utilizar la versión **0.20.1** de web3

Fuente: https://github.com/ethereum/web3.js/

ganache - Personal blockchain

```
$ sudo npm install -g ganache-cli
```

BLOCKCHAIN ACADEMY MÉXICO

Crear un proyecto

Crear una carpeta y un proyecto para agregar dependencias al package.json

```
$ mkdir votaciones
$ cd votaciones
$ npm init
```

BLOCKCHAIN ACADEMY MÉXICO

2. Correr blockchain personal

Levantar blockchain local: **ganache**

En una pestaña de **terminal** correr **ganache-cli**

```
$ ganache-cli
```

BLOCKCHAIN ACADEMY MÉXICO

```
Available Accounts
==================
(0) 0xdafe303c1c0c54c685ae05a71be35fa4e2b67485
(1) 0x0361ab6a2c01ab3f1d01d7a973c0485f7b2c4509
(2) 0x30da6c95975487f511e25e37c42ad8b7864948f4
(3) 0x75d79b6988552a893b6952f7232d80f6a01727e4
(4) 0xcd53f7071ec14b9065228f19b568c68c5d30ed8d
(5) 0x1bf6104307651cbca6a8ae50cfbf7786628de1a0
(6) 0xa0465e79ed022cc7ac3503b52b55f2d99fc34197
(7) 0x9a3522a14e0141b165aaf88861a0a425c42cd859
(8) 0x496ffd48657ea688eda6f958b251ec67de176e77
(9) 0xbc3286a37f2dba6ef930808ab93a244836b7124d

Private Keys
==================
(0) b247cee26ec395f1aaf496216f14f2e9a2974b6df88437da4c3742fbc8bb0e0d
(1) 006f965d019495e3505a3dec5992ec5f4a681fd0283f581b673180e00667b16f
(2) 23d50ca14ef39cc9f5a1b53e874e872f1791a8a98bf59995938b3cf736d40c76
(3) 95c10882f90e4660b62dd630db0bc1eba704adb8aa538f120b6bfa9235ad0010
(4) 3b5e77759b8e2bbc5ed068c5b9ca32daa64402431d61f560dc3cdc99ff34f982
(5) d4a4e2a7b3fc171cc41058013748857a36ac3ab35b8812d2a52ac0553e05667e
(6) ae1df23c9c7a4268461d379ebd61beb42604c780f1c181cb19fcd4cf024a8a66
(7) 61c8ae60041ea69d72abe87ae1943dc176786366927b3c09c7737ed3d551468b
(8) 55da96ba30e81aa77aa27ae00a31ea4aff509d708b087c7883fa4b3a1c2cbc68
(9) b1364910313da048456259941f2c2a156e6a439aaaac1f02a3edcc4f557269d8

HD Wallet
==================
Mnemonic:      inhale ankle grocery claw coil immense outer fetch skill biology meat series
Base HD Path:  m/44'/60'/0'/0/{account_index}

Listening on localhost:8545
```

BLOCKCHAIN ACADEMY MÉXICO

4. Crear el smart contract

Crear un archivo **Voting.sol**

Creamos nuestro contrato **Voting.sol**

```
$ touch Voting.sol
$ sublime Voting.sol
```

BLOCKCHAIN ACADEMY MÉXICO

Smart Contract: Voting.sol

`Copiar código del siguiente smart contract`

Código: Voting.sol

https://codeshare.io/5Zydke

Cuentas de Ethereum

Corremos **nodejs**

```
$ node
```

Requerimos la librería **web3** y consultamos las cuentas de **ganache**

```
>  web3Library = require('web3');
```

```
> web3 = new web3Library(new web3Library.providers.HttpProvider('http://localhost:8545'));
```

```
>  web3.eth.accounts;
```

Dependiendo la version es: `web3.eth.getAccounts().then(console.log);`

BLOCKCHAIN ACADEMY MÉXICO

Compilar el contrato

Leemos el contrato y lo convertimos en una cadena de caracteres

```
> votingString = fs.readFileSync('Voting.sol').toString();
```

Requerimos la librería **solc**

```
> solc = require('solc');
```

Compilamos el contenido de la variable **code** y lo guardamos en **compiledCode**

```
> compiledCode = solc.compile(votingString);
```

BLOCKCHAIN ACADEMY MÉXICO

Definición ABI y bytecode

Tenemos que generar una definición **ABI** que es con la que vamos a interactuar.

```
> abiDefinition = JSON.parse(compiledCode.contracts[':Voting'].interface);

> VotingContract = web3.eth.contract(abiDefinition);
Otra version: VotingContract = new web3.eth.Contract(abiDefinition)
```

Se genera el **byte code** que es el que migramos al **blockchain**

```
> byteCode = compiledCode.contracts[':Voting'].bytecode;
```

BLOCKCHAIN ACADEMY MÉXICO

Deploy el contracto a ganache

Deployamos el contrato al blockchain con **.new**

```
> deployedContract = VotingContract.new(['Lopez', 'Anaya', 'Meade'], {data: byteCode, from: web3.eth.accounts[0], gas: 4700000})
```

Podemos consultar la **dirección del contrato**

```
> deployedContract.address
```

Almacenamos una **instancia** del contrato

```
> ContractInstance = VotingContract.at(deployedContract.address);
```

BLOCKCHAIN ACADEMY MÉXICO

INTERACTUAR CON EL CONTRATO

Interactuar con el contrato

Consultamos el total de votos de un candidato

```
> ContractInstance.totalVotesFor.call('Lopez')
```

Votamos por un candidato

```
> ContractInstance.voteForCandidate('Lopez', {from: web3.eth.accounts[0]})
```

BLOCKCHAIN ACADEMY MÉXICO

WEB INTERACTION

Código HTML y JS

Crear un archivo **index.html**
HTML: https://codeshare.io/GqKM1q

Crear un archivo **index.js**
JS: https://codeshare.io/5MwDM3

OJO: Sustituir la dirección de tu propio contrato deployado a ganache

BLOCKCHAIN ACADEMY MÉXICO