

# **DESARROLLO DAPP DE EXPEDIENTES ACADÉMICOS EN BLOCKCHAIN DE ETHEREUM**

**ADOLFO SANZ DE DIEGO**

**SEPTIEMBRE 2018**

# 2 INDICE

## 2.1 ¿QUÉ VAMOS A VER?

1. Parte teorica
2. Descripción DApp
3. Creación Smart Contracts
4. Testing Smart Contracts
5. Creación UI
6. Subida a entornos de prueba

# 3 TEORÍA

## 3.1 ¿QUÉ ES BITCOIN?

- Protocolo y red P2P = dinero digital.
- Claves privadas = transferir fondos.
- Descentralizado = no necesitan un tercero.

## 3.2 ¿QUÉ ES BLOCKCHAIN?

- Datos se guardan en **cadena de bloques** con información del anterior.
- **Histórico transacciones** difícilmente falsificable.
- Transacciones verificadas **de forma descentralizada** ¿cómo?

## 3.3 ¿QUÉ ES EL MINADO?

- Generación nuevos bloques.
- Problema elegir el bloque correcto ¿cómo?

## 3.4 ¿MECANISMOS DE CONSENSO?

- **Prueba de trabajo o PoW** = recompensa al primer minero en resolver problema gasto computacional elevado, pero verificación inmediata.
  - Elevado gasto energético.
- **Prueba de participación o PoS** = probabilidad de obtener recompensa proporcional a monedas acumuladas.
  - Problemas en caso de una bifurcación de la cadena.



## 3.5 ¿TIPOS DE BLOCKCHAINS?

- **públicas:** cualquiera puede minar y las transacciones son públicas.
- **privadas:** solo se puede minar por invitación y las transacciones solo las pueden ver los mineros.
- **mixtas:** solo se puede minar por invitación pero las transacciones son públicas.

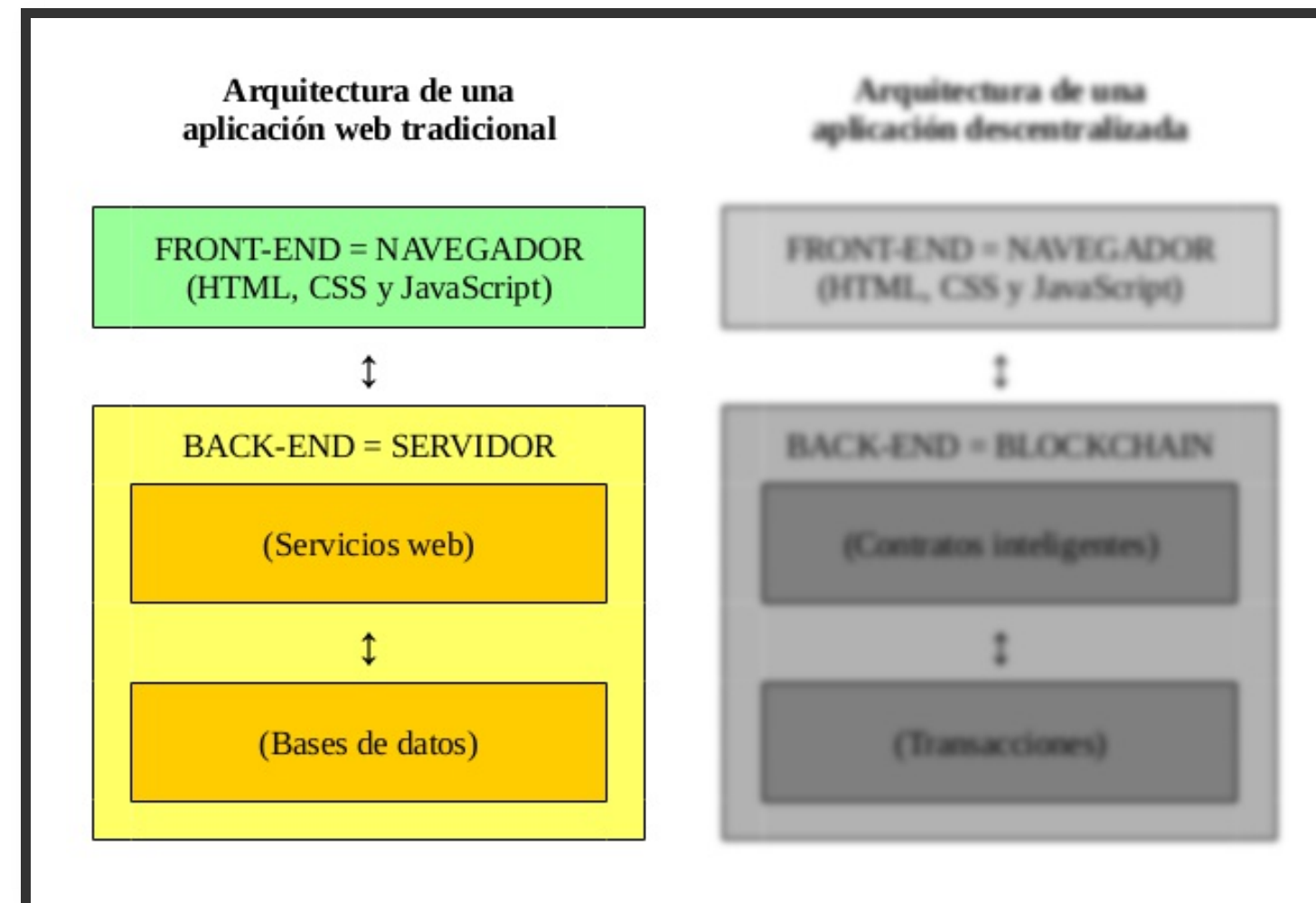
## 3.6 ¿QUÉ ES ETHEREUM?

- Blockchain pública que ejecuta código y guarda datos de forma descentralizada.
- **Solidity** = compila a bytecode interpreta Ethereum Virtual Machine (EVM).
- **Gas** = coste ejecución en Ethers.

## 3.7 ¿QUÉ ES UN SMART CONTRACT?

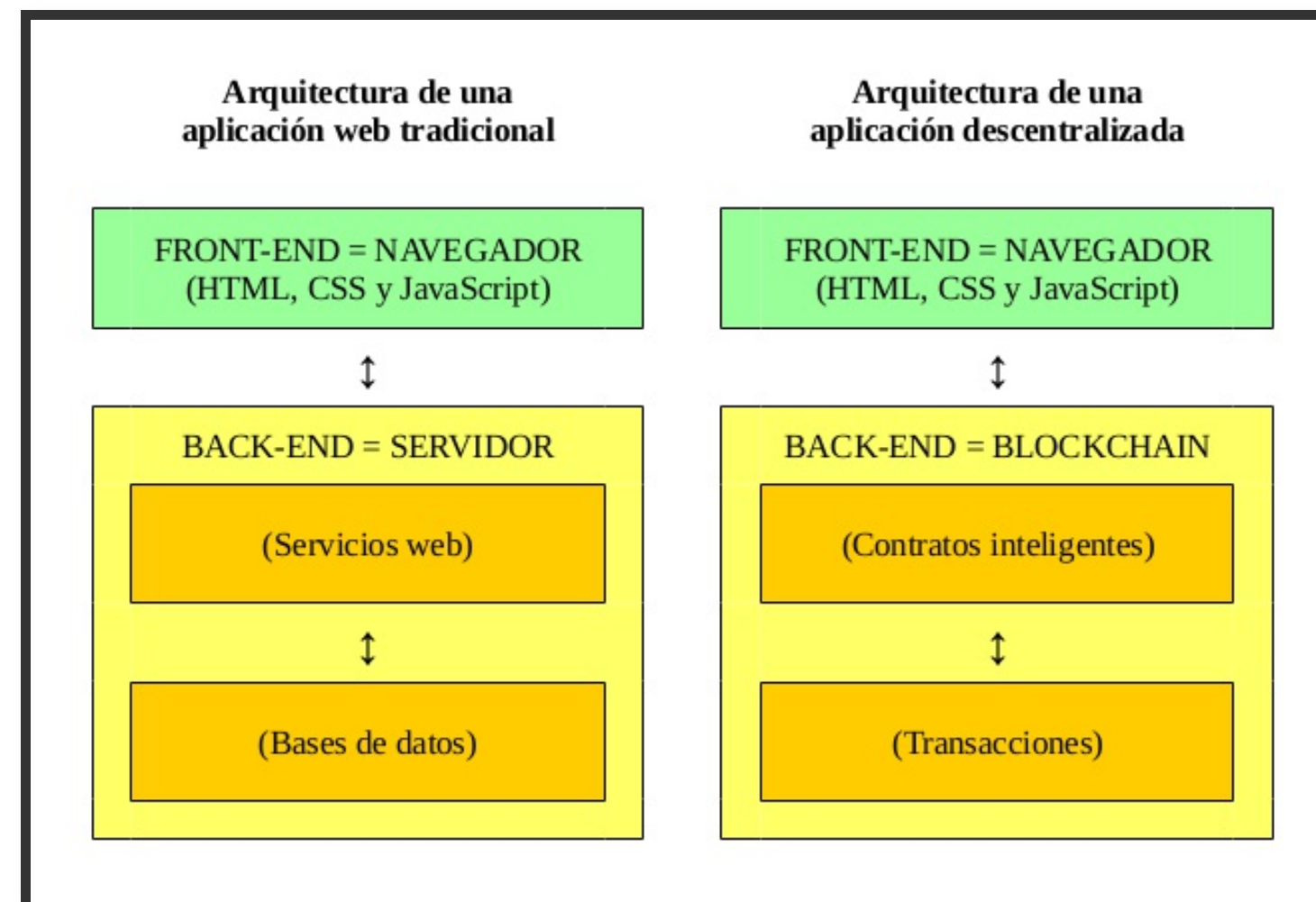
- Programa informático en blockchain.
  - **Autónomo:** no necesita ningún servidor.
  - **Confiable:** trazabilidad de los datos.
  - **Imparable:** ejecutarse siempre.
  - **Inmutable:** no se puede modificar.
  - **Descentralizado:** no necesita tercero para ser verificado.

## 3.8 ¿APPS TRADICIONALES?



Apps

# 3.9 ¿APPS DESCENTRALIZADAS?



Apps VS ÐApps

## 3.10 RESUMEN

- **Bitcoin** = dinero descentralizado.
- **Blockchain** = cadena de bloques difícilmente falsificable.
- **Minado** = generación bloques con mecanismos de consenso.
- **Ethereum** = blockchain pública permite ejecutar código y guardar datos.
- **Smart Contract** = programa que se ejecuta en una blockchain.
- **DApp** = aplicación que utiliza smart contracts.

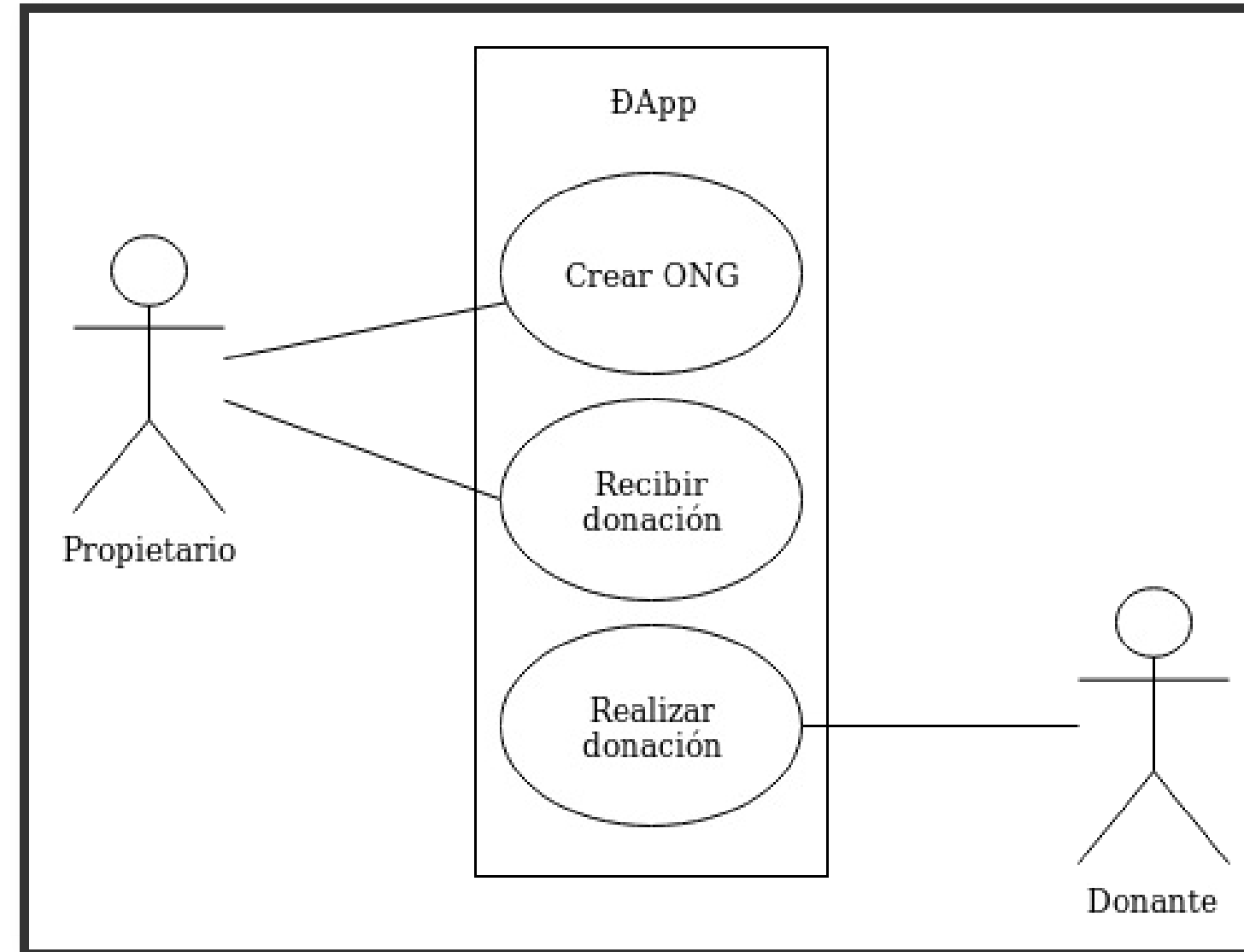
# 4 DESCRIPCIÓN DAPP

## 4.1 ÐAPP DE DONACIONES A ONG

- Vamos a desarrollar una ÐApp para gestionar donaciones a ONG con 2 tipos de usuarios:
  - **Propietarios:** crea la ONG y recibe las donaciones.
  - **Otros usuarios:** realizan donaciones a las ONG.



## 4.2 CASOS DE USO



## 4.3 DEMO (RINKEBY)

- El back desplegado en la red de pruebas de **Rinkeby**.
- El front desplegado en **GitHub Pages** (siendo puristas habría que usar **IPFS**).
  - <https://nongovernmentalorganizations.github.io>

# 5 CREACIÓN SMART CONTRACTS

## 5.1 ¿ENTORNO DE DESARROLLO?

- **Solidity**: lenguaje de programación.
- **Remix**: IDE en un navegador.
- **Visual Studio Code**: IDE Software Libre
- **Plugin de Solidity de Juan Blanco**: Plugin de Solidity para Visual Studio Code

## 5.2 ¿CÓMO GUARDAR DATOS?

- Los datos se guardan en “structs” o estructuras.
- Las estructuras de datos se guardan en arrays.
- Para las relaciones se utilizan los mappings.

## 5.3 EJEMPLO

```
// Estructura
struct Organization {
    uint id;
    address owner;
    string name;
}

// Array
Organization[] public organizations;

// Mapping
mapping(address => uint) public ownerToOrganizationId;
```

## 5.4 ¿OTROS ELEMENTOS?

- **constructores** : solo se ejecutan cuando el contrato inteligente es desplegado en la blockchain.
- **eventos**: permiten trazar lo que sucede en los contratos inteligentes.
- **modificadores personalizados**: permiten hacer chequeos antes de ejecutar la lógica de una función.

## 5.5 EJEMPLO

```
// Constructor
constructor() public {
    // to fix problem with nulls
    organizations.push(Organization(0, 0, "0"));
}

// Eventos
event OrganizationCreated(
    uint indexed id, address indexed owner, string name);

// Modificadores personalizados
modifier ownerNotExists() {
    require(ownerToOrganizationId[msg.sender] == 0,
        "suplied owner already have an organization");
    _;
}
```



## 5.6 ¿MODIFICADORES DE VISIBILIDAD?

- Para variables de estado y para funciones:
  - **public**: desde otros contratos y desde el propio contrato.
  - **external**: desde otros contratos pero no desde el propio contrato.
  - **internal**: desde el propio contrato o de contratos que hereden de él.
  - **private**: sólo desde el propio contrato.

## 5.7 ¿OTROS MODIFICADORES?

- Para variables de estado:
  - **constant**: pueden ser modificadas.
- Para funciones:
  - **view**: no pueden modificar ninguna variable de estado (no consumen Gas).
  - **pure**: no pueden ni ver ni modificar ninguna variable de estado (no consumen Gas).
  - **payable**: admiten envío de dinero.

## 5.8 EJEMPLO

```
function addOrganization(string _name) external
    ownerNotExists() {
        ...
        emit OrganizationCreated(organizationId, msg.sender, _name);
    }

function donation(uint _organizationId) external payable
    ownerExists(_organizationId) {
        ...
        emit DonationSubmitted(_organizationId, owner, msg.sender, msg.value);
    }

function getOrganizationsLength() external view returns(uint) {
    return organizations.length;
}
```

## 5.9 ¿COMENTARIOS GENERALES?

- Muchas limitaciones, por eso reducir la lógica al mínimo.
- Los bucles están muy desaconsejados (gas), por eso se usan los mappings.
- La ejecución es lenta, por eso implementar políticas de cacheo.
- Aspectos en proceso de mejora como tratamiento excepciones.

## 5.10 RESUMEN

- **Entorno:** Solidity, Remix, Plugin, Solium.
- **Datos:** estructuras, arrays y mappings.
- **Otros:** constructores y eventos.
- **Modificadores:** visibilidad, otros y personalizado.
- **Comentarios:** limitaciones, ejecución lenta, mejorando.

# **6 TESTING SMART CONTRACTS**

## 6.1 GANACHE

- **Ganache** es un nodo privado para desarrollar y testear sin coste.

```
# instalar  
npm install -g ganache-cli
```

```
# ejecutar  
ganache-cli --gasLimit 7000001 --mnemonic "$(cat wallet.mnemonic)"
```

## 6.2 TRUFFLE

- **Truffle** es un framework de desarrollo de smart contracts de Ethereum.

```
# instalar  
npm install -g truffle
```



## 6.3 COMPILAR

- Una vez creado los smart contracts hay que compilarlos:

```
# compilar  
truffle compile
```

## 6.4 MIGRAR

- Una vez levantado el nodo privado (Ganache) en una terminal independiente, tenemos que migrar los smart contracts compilados:

```
# migrar  
truffle migrate
```

## 6.5 TESTS

```
var NonGovernmentalOrganizations = artifacts
    .require("NonGovernmentalOrganizations");
contract("NonGovernmentalOrganizations", async (accounts) => {
    it("addOrganization - ok", async () => {
        let instance = await NonGovernmentalOrganizations.deployed();
        let tx = await instance.addOrganization(expectedName,
            { from: expectedOwner });
        assert.equal(tx.logs[0].event, "OrganizationCreated");
        let result = await instance.organizations.call(expectedId);
        assert.equal(result[2], expectedName);
        let ownerId = await instance.ownerToOrganizationId(expectedOwner);
        assert.equal(ownerId, expectedId);
        let length = await instance.getOrganizationsLength();
        assert.equal(length, expectedLength);
    });
});
```

## 6.6 TESTEAR

- Una vez creados los tests los lanzamos:

```
# testear  
truffle test
```

## 6.7 RESUMEN

- **Instalar Ganache:** `npm install -g ganache-cli`
- **Ejecutar Ganache:** `ganache-cli --gasLimit --mnemonic`
- **Instalar truffle:** `npm install -g truffle`
- **Compilar:** `truffle compile`
- **Migrar:** `truffle migrate`
- **Testear:** `truffle test`

# 7 CREACIÓN UI

## 7.1 TRUFFLE BOXES

- **Truffle boxes** proporciona boilerplates para no tener que empezar a desarrollar DApps desde cero.
- Hay para React, aunque yo soy más de Angular :-)

## 7.2 ANGULAR

- Aunque la UI se puede hacer con otros frameworks yo he usado **Angular y Angular Material**.

```
npm install -g @angular/cli
```



## 7.3 METAMASK

- **MetaMask**: es nodo ligero y wallet de Ethereum que permite ejecutar DApps en un navegador.

## 7.4 WEB3JS

- **web3js**: es una librería de comunicación entre la interfaz de usuario y un nodo de Ethereum.

## 7.5 ADDRESS USUARIO

```
getUserAddress() {  
  if (!this.web3) {  
    this.messagesService.sendMessage('Try MetaMask.');  }  
  this.web3.eth.getAccounts().then(accounts => {  
    if (!accounts || accounts.length === 0) {  
      this.messagesService.sendMessage('No user accounts.');    }  
    if (StorageUtil.getUserAddress() !== accounts[0]) {  
      StorageUtil.setUserAddress(accounts[0]);  
      this.messagesService.sendNewUserAddressMessage(accounts[0]);  
    }  
  }).catch(error => {  
    this.messagesService.sendMessage(error);  
  });  
}
```

## 7.6 CONTRACT INSTANCE

```
async getContractInstance(): Promise<any> {  
  if (!this.web3) {  
    throw new Error('web3 server not found. Try MetaMask.');  }  
  const ngoContract = contract(artifacts);  
  ngoContract.setProvider(this.web3.currentProvider);  
  try {  
    const ngoInstance = await ngoContract.deployed();  
    return ngoInstance;  
  } catch (error) {  
    console.log(error);  
    throw new Error('Contract has not been deployed to network.');  }  
}
```

## 7.7 ADD ORGANISATION

```
async add(organization: Organization): Promise<Organization> {
  const contractInstance = await this.web3Service.getContractInstance();
  const oldOrganization = await this.getCurrentUserOrganizationAsOwner();
  if (oldOrganization) {
    throw new Error('The user is already owner of an organization.');
```

```
  }
  const transaction = await contractInstance.addOrganization(
    organization.name, { from: this.senderAddress });
  const newOrganization = this._getOrganizationFromTransaction(transaction);
  this.organizations.push(newOrganization);
  console.log('OrganizationService->add', newOrganization);
  return newOrganization;
}
```

## 7.8 DONATION

```
async donation(id: number, ethValue: number): Promise<Donation> {  
  const organization = await this.getOne(id);  
  const contractInstance = await this.web3Service.getContractInstance();  
  const weiValue = this.web3Service.etherToWei(ethValue.toString());  
  const transaction = await contractInstance.donation(organization.id,  
    { value: weiValue, from: this.senderAddress });  
  const donation = await this._getDonationFromTransaction(transaction);  
  console.log('OrganizationService->donation', donation);  
  return donation;  
}
```

## 7.9 RESUMEN

- **Truffle boxes:** boilerplates.
- **Angular:** npm install -g @angular/cli
- **MetaMask:** nodo ligero y wallet de Ethereum.
- **web3js:** librería de comunicación.

# **8 SUBIDA A ENTORNOS DE PRUEBA**



## 8.1 INFURA

- **Infura**: simplifica el despliegue de DApps en redes de prueba y en la red principal.
- Te creas un usuario y te facilita un **API Key**.

## 8.2 RINKEBY

- **Rinkeby**: red de pruebas para probar DApps.
- Mediante **faucets** consigues ETH de la red.

## 8.3 TRUFFLE.JS

```
var HDWalletProvider = require("truffle-hdwallet-provider");
module.exports = {
  networks: {
    rinkeby: {
      provider: function () {
        let provider = new HDWalletProvider(
          walletMnemonic,
          "https://rinkeby.infura.io/v3/" + apiKey);
        return provider;
      },
      gas: 70000001,
      network_id: 4
    }
  }
};
```

## 8.4 MIGRAR A RINKEBY

- Para migrar a Rinkeby tenemos que usar la **apiKey** de Infura y una **walletMnemonic** de una wallet con saldo suficiente en Rinkeby y ejecutar:

```
truffle migrate --network rinkeby
```

# 9 RESUMEN

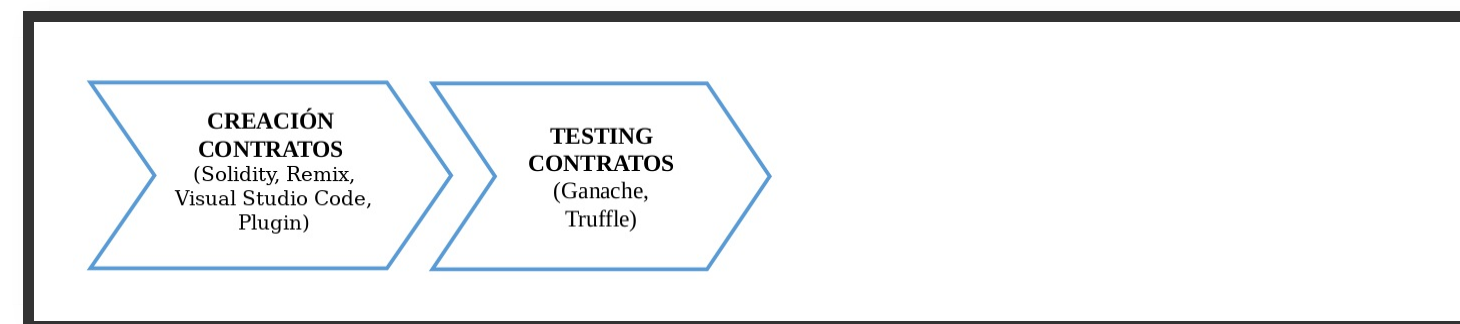
# 9.1 ¿CREACIÓN CONTRATOS INTELIGENTES?



Creación contratos inteligentes

- **Solidity**: lenguaje de programación.
- **Remix**: IDE en un navegador.
- **Visual Studio Code**: IDE Software Libre
- **Plugin de Solidity de Juan Blanco**: Plugin de Solidity para Visual Studio Code

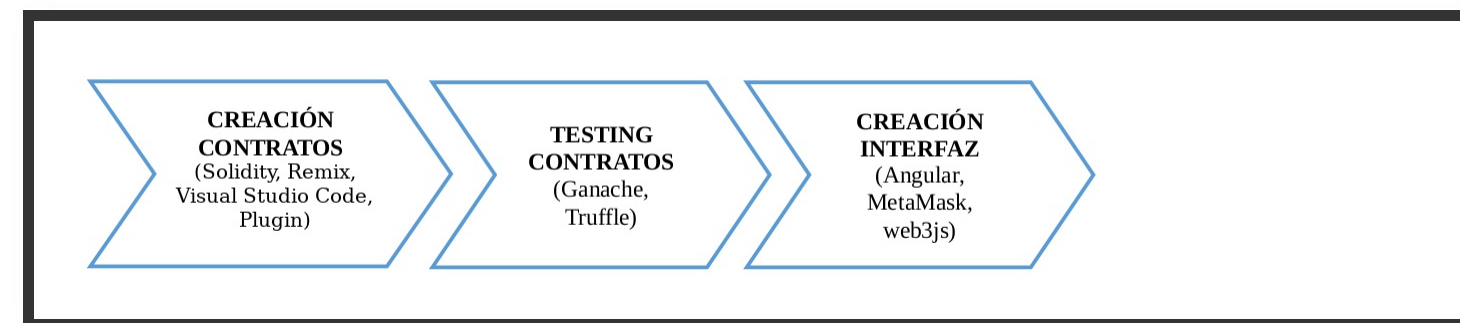
## 9.2 ¿TESTING CONTRATOS INTELIGENTES?



### Testing contratos inteligentes

- **Ganache**: nodo privado para desarrollar y testear sin coste.
- **Truffle**: framework de desarrollo de smart contracts de Ethereum.

## 9.3 ¿CREACIÓN INTERFAZ DE USUARIO?

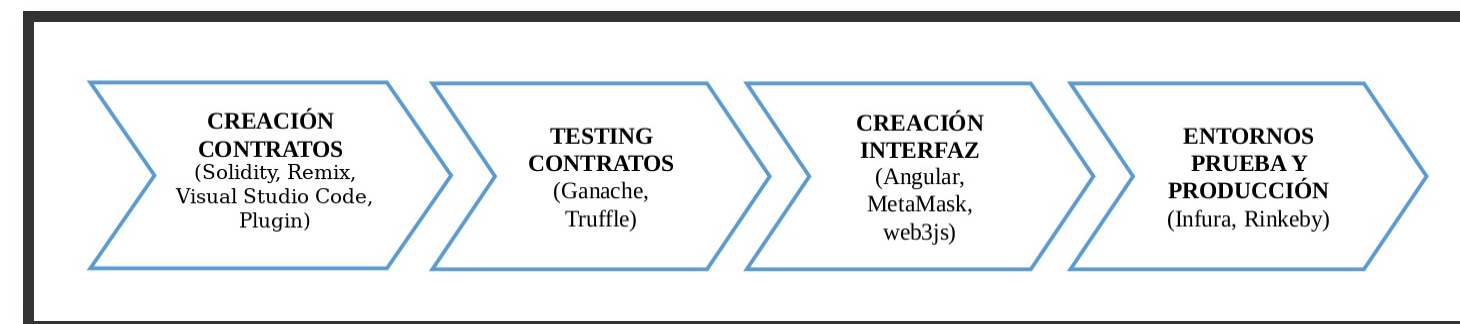


### Creación interfaz de usuario

- **Angular**: framework de desarrollo de interfaces de usuario.
- **MetaMask**: nodo ligero y wallet de Ethereum permite ejecutar DApps en navegador.
- **web3js**: librería comunicación entre interfaz de usuario y nodo de Ethereum.



## 9.4 ¿SUBIDA A ENTORNOS DE PRUEBA?



### Entornos de prueba

- **Infura**: simplifica el despliegue de  $\text{DApps}$  en redes de prueba y en la red principal.
- **Rinkeby**: red de pruebas para probar  $\text{DApps}$ .

## 9.5 ¿CONCLUSIONES?

- Tecnologías nuevas, pero ya se pueden empezar a implantar los primeros proyectos en producción.
- Tecnologías muy disruptivas por la descentralización y por la trazabilidad de los datos.
- Problemas de escalabilidad y de volatilidad de precios.

## 9.6 RESUMEN

- **Creación:** Solidity, Remix, VSCODE, Plugin.
- **Testing:** Ganache, Truffle.
- **UI:** Angular, MetaMask, web3js.
- **Prueba:** Infura, Rinkeby.
- **Conclusiones:** descentralización y trazabilidad.

**10 ACERCA DE**

# 10.1 LICENCIA

Creative Commons Reconocimiento-CompartirIgual 3.0

## 10.2 FUENTES

[github.com/asanzdiego/commit-conf-taller-blockchain](https://github.com/asanzdiego/commit-conf-taller-blockchain)

# 10.3 SLIDES

Las slides están hechas con **MarkdownSlides**.

# 11 PREGUNTAS



**12 GRACIAS**