



POLITÉCNICA

ETSIT  
UPM

*dit*  
UPM

# Blockchain: Desarrollo de Aplicaciones

# Caso de Estudio: Contador

BCDA 2018

Versión: 2018-10-03

# El Código del Contrato

```
pragma solidity ^0.4.25;

contract Contador {

    uint8 public valor = 0;

    event Tic(string msg, uint8 out);

    function incr() public {
        valor++;
        emit Tic("Actualizado", valor);
    }

    function() public {
        revert();
    }
}
```

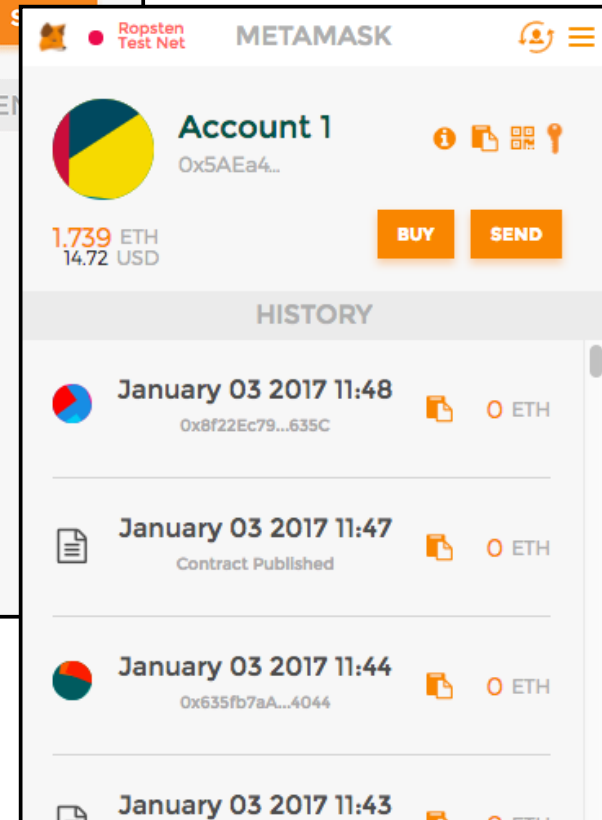
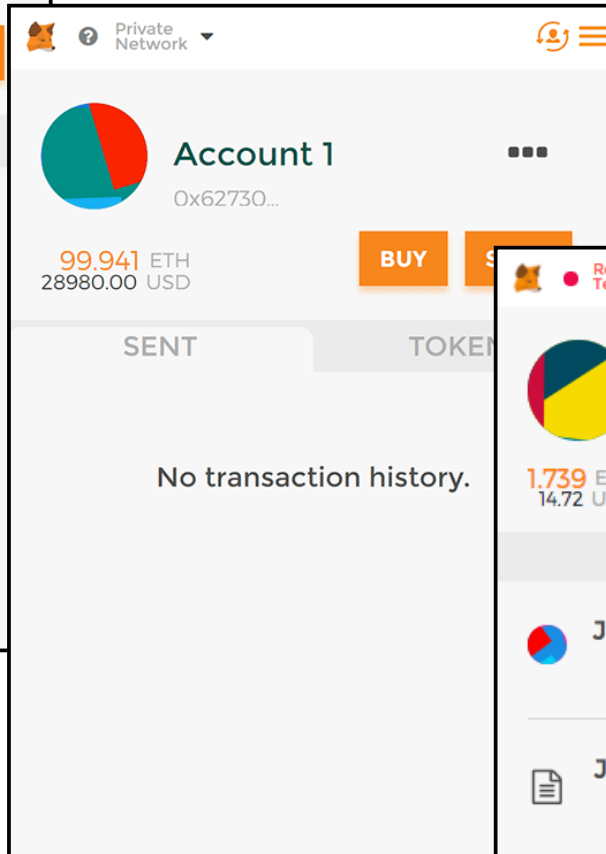
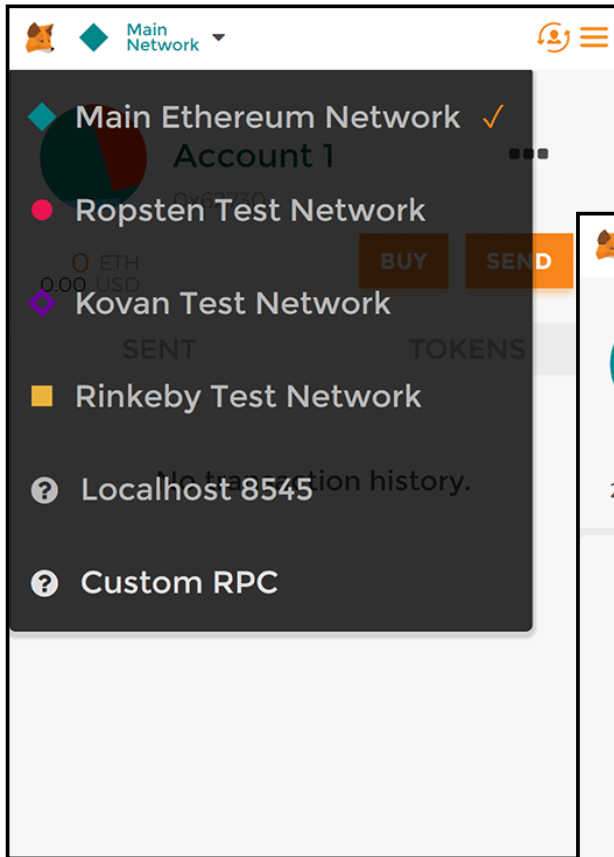
# ¿Qué sabemos hacer?

- Instalar la extensión MetaMask en el navegador (Chrome, Firefox)
  - para que Remix se pueda conectarse a la red Ethereum que queramos.
- Usando Remix sabemos editar, compilar, desplegar y usar el contrato.
- Otras opciones:
  - Ethereum Wallet, Mist, ...

# MetaMask

The screenshot shows the Chrome Web Store page for the MetaMask extension. At the top, there is a header with the MetaMask logo, the name "MetaMask", and the URL "ofrecido por <https://metamask.io>". Below this, there are star ratings (★★★★★ (37)) and the category "Productividad" with "4.332 usuarios". Navigation tabs include "DESCRIPCIÓN GENERAL", "OPINIONES", "AYUDA", and "RELACIONADOS". The main content area features a preview of the extension's interface, which includes a "Welcome To Community!" message and a "UNLOCK" button. To the right of the preview, there is a "Compatible con tu dispositivo" badge and a description of the extension as an "Ethereum Browser Extension". The description explains that MetaMask is an extension for accessing Ethereum-enabled distributed applications, or "Dapps", in a normal Chrome browser. It also mentions that the extension injects the Ethereum web3 API into every website's javascript context. Below the description, there are links for "Sitio web" and "Notificar uso inadecuado". Further down, there is a section for "Información adicional" which lists the version (2.13.11), the last update date (1 de diciembre de 2016), the size (3.89MIB), and supported languages (Ver todos (5)). At the bottom of the page, there is a section titled "LOS USUARIOS DE ESTA EXTENSIÓN TAMBIÉN HAN USADO" which lists other extensions: "Mailtrack para Gmail" (★★★★★ (3630)), "Traductor de inglés de LinguaLeo" (★★★★☆ (1505)), "Explica y Envía Capturas de Pantalla" (★★★★☆ (822)), and "SessionBox - Free multi login to any website" (★★★★★ (168)).

The image shows the MetaMask logo, which is a stylized orange fox head. Below the logo, the word "METAMASK" is written in a bold, sans-serif font. Underneath, there are two prominent orange buttons with white text: "CREATE NEW VAULT" and "RESTORE EXISTING VAULT". The word "OR" is centered between these two buttons, flanked by horizontal lines.



# Compilador online: Remix

The screenshot displays the Remix IDE interface. The main editor shows a Solidity contract named `Contador.sol` with the following code:

```
1 pragma solidity ^0.4.25;
2
3 contract Contador {
4
5     uint8 public valor = 0;
6
7     event Tic(string msg, uint8 out);
8
9     function incr() public {
10         valor++;
11         emit Tic("Actualizado", valor);
12     }
13
14     function() public {
15         revert();
16     }
17 }
18
```

The right-hand side of the interface contains several panels:

- Environment:** JavaScript VM, Account: 0xca3...a733c (99.999999999999730), Gas limit: 3000000, Value: 0 wei.
- Contador:** A dropdown menu showing the contract name, with a **Deploy** button below it.
- Transactions recorded:** 4 transactions.
- Deployed Contracts:** A list of deployed contracts, including **Contador at 0x692...77b3a (memory)**. Below this, there are buttons for **(fallback)**, **incr**, and **valor**. The **valor** button is currently selected, showing the value **0: uint8: 3**.

The bottom panel shows the transaction log with the following entries:

- transact to Contador.incr pending ...**
- [vm] from: 0xca3...a733c**  
**to: Contador.incr() 0x692...77b3a value: 0 wei**  
**data: 0x119...fbbd4 logs: 1 hash: 0x13e...25906**
- call to Contador.valor**
- [call] from: 0xca35b7d915458ef540ade6068dfe2f44e8fa733c**  
**to: Contador.valor() data: 0xecb...ac7cf**

# Ethereum Wallet

The screenshot displays the 'Contracts' section of an Ethereum wallet interface. At the top, there are navigation icons for 'BILLETERAS', 'ENVIAR', and 'CONTRATOS', along with a balance of '6,71 ETHER\*'. The 'CONTRATOS' icon is highlighted with a red arrow. Below the navigation bar, the 'Contracts' section features a 'DEPLOY NEW CONTRACT' button, also highlighted with a red arrow. A 'Custom Contracts' section follows, containing a list of three contracts: 'OWNED 6729', 'AFORO DE RI...', and 'SANTICOIN (ADMIN PAGE)'. Each contract entry shows a balance of '0,00 ether' and a partial hexadecimal address. At the bottom of the section is a 'WATCH CONTRACT' button.




**BILLETERAS** **ENVIAR** Rinkeby Remote | 3.084.957 7s **CONTRATOS** **SALDO** 6,71 ETHER\*

## Contracts

**+** **DEPLOY NEW CONTRACT**

Custom Contracts

In order to watch and interact with a contract already deployed on the blockchain you need to know its address and description of its interface in JSON format.

 <b>OWNED 6729</b> 0,00 ether 0x672917a996f31a1ca...	 <b>AFORO DE RI...</b> 0,00 ether 0x419CdB13175808c8...	 <b>SANTICOIN (ADMIN PAGE)</b> 0,00 ether 0x184d6866c88a60807d0539490B86aBEA20CACA88
---	--	---

**+** **WATCH CONTRACT**

BILLETAS ENVIAR Rinkeby Remote | 3.084.969 4s CONTRATOS 6,71 ETHER\*


```
1 pragma solidity ^0.4.24;
2
3 contract Contador {
4
5     uint8 public valor = 0;
6
7     event Tic(string msg, uint8 out);
8
9     function incr() public {
10        valor++;
11        emit Tic("Actualizado", valor);
12    }
13
14    function() public {
15        revert();
16    }
17 }
```

SELECT CONTRACT TO DEPLOY

Contador

SELECT FEE

0,000147983 ETHER



MÁS BARATO  MÁS RÁPIDO

TOTAL

0,000147983 ETHER

DESPLEGAR

This is the most amount of money that might be used to process this transaction. Your transaction will be mined **often within 30 seconds.**





BILLETERAS ENVIAR Rinkeby Remote 3.084.974 11s CONTRATOS SALDO 6,71 ETHER\*





## Contracts

**+** DEPLOY NEW CONTRACT


Custom Contracts

In order to watch and interact with a contract already deployed on the blockchain you need to know its address and description of its interface in JSON format.

**+** WATCH CONTRACT

 <b>: CONTADOR ...</b> 0,00 ether 0x3B4D3f847E4Efb5aA...	 <b>: OWNED 6729</b> 0,00 ether 0x672917a996f31a1ca...	 <b>AFORO DE RI...</b> 0,00 ether 0x419CdB13175808c8...
 <b>SANTICOIN (ADMIN PAGE)</b> 0,00 ether 0x184d6866c88a60807d0539490B86aBEA20CACA88		

BILLETAS ENVIAR Rinkeby Remote 3.084.980 4s CONTRATOS 6,71 ETHER\*

 : **Contador 3B4D**  
0x3B4D3f847E4Efb5aAB8599eCEeAf4c92EAc2Dc44  
0,00 ETHER\*

Deposit Ether  
Copy address  
Show QR-Code  
Show Interface

HIDE CONTRACT INFO

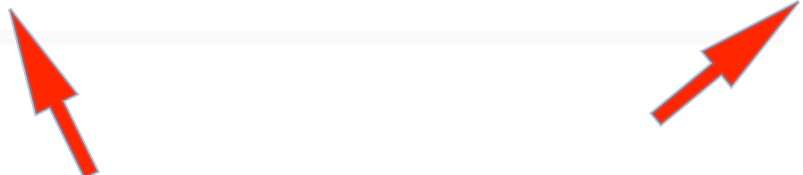
Read From Contract Write To Contract

Valor 0

Select function  
Incr

Execute from  
Account 1 - 6,71 ETHER

EXECUTE



# Trabajar en los nodos

- El navegador ejecutando Remix, la wallet, etc... son programas externos a los nodos de la red Ethereum.
- Se conectan con un nodo de la red y le envían comandos.

