

DefiDappsDao

Proyecto para el Sprint 1 , 2 y 3

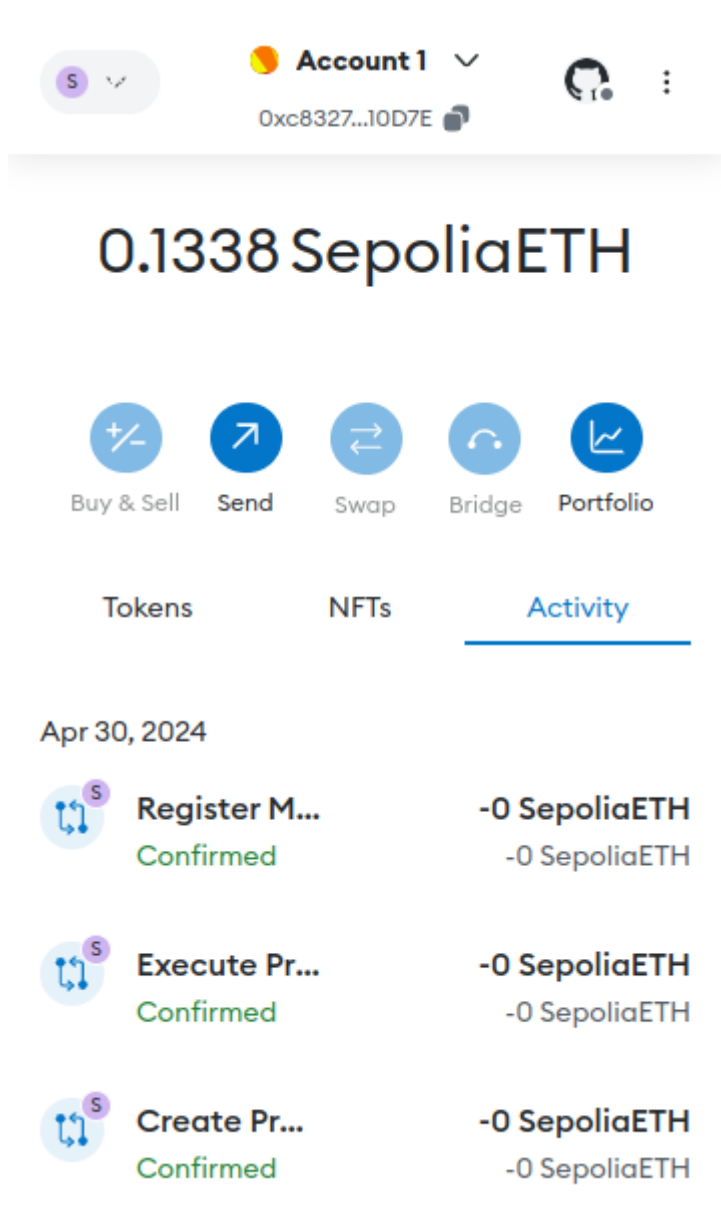
En este sprint instalarás tú mismo un Smart Contract en una testnet de Ethereum en concreto, Sepolia*. El Smart Contract representa una subasta de una obra de arte en la que cualquier usuario con una cuenta de Ethereum puede realizar una puja para hacerse con su propiedad. A continuación se muestran los diferentes pasos que debes seguir. Cada uno de los siguientes puntos han sido explicados y realizados en los diferentes temas teóricos.

Sprint 1

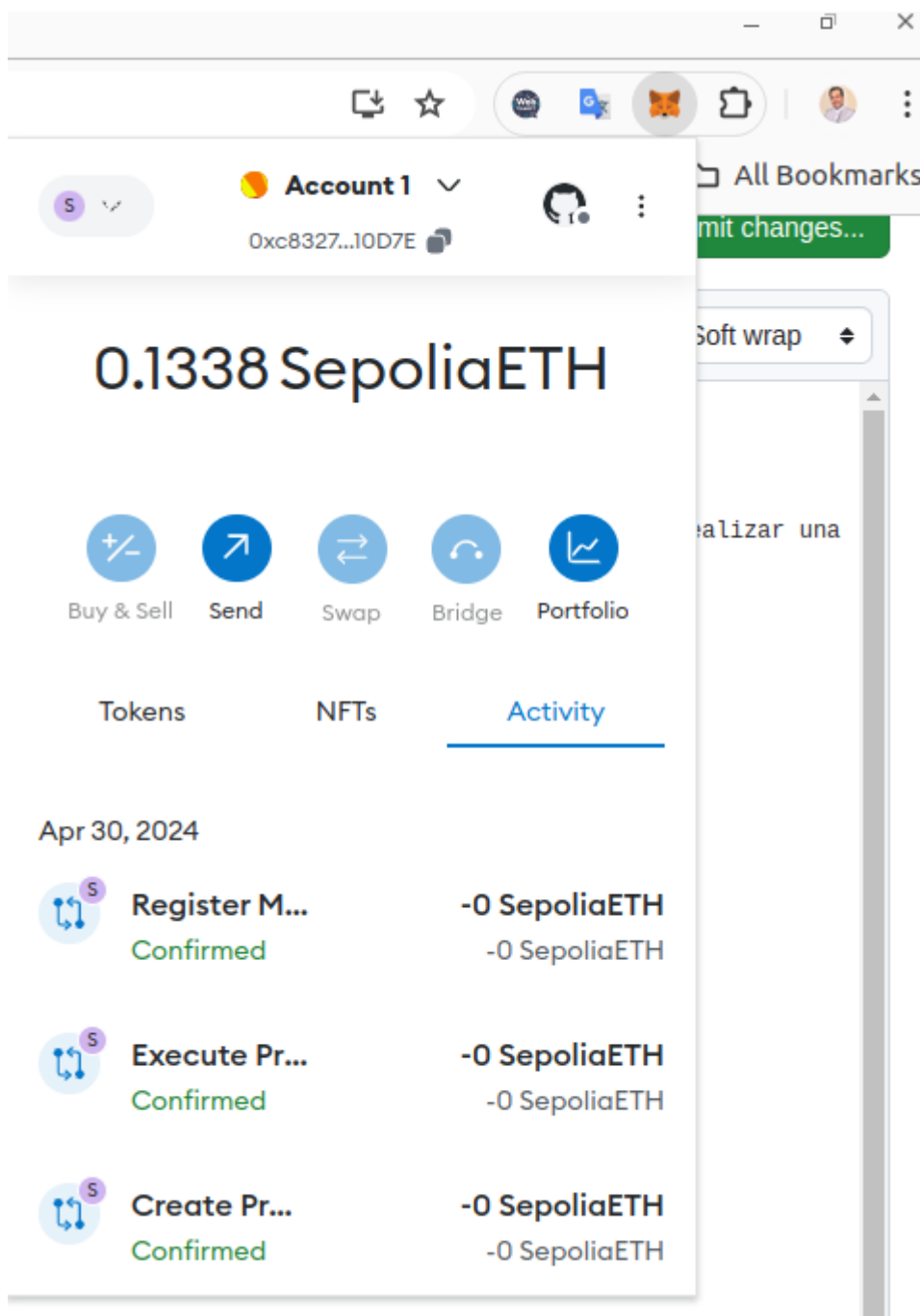
1 Instalar Metamask

Es esencial disponer de un Wallet en el que podamos crear y gestionar nuestras cuentas de Ethereum para enviar transacciones a la red.

En nuestro caso usaremos una cuenta actual que tiene Ether en la TestNet Sepolia:



Usaremos el complemento de MetaMask en Chrome



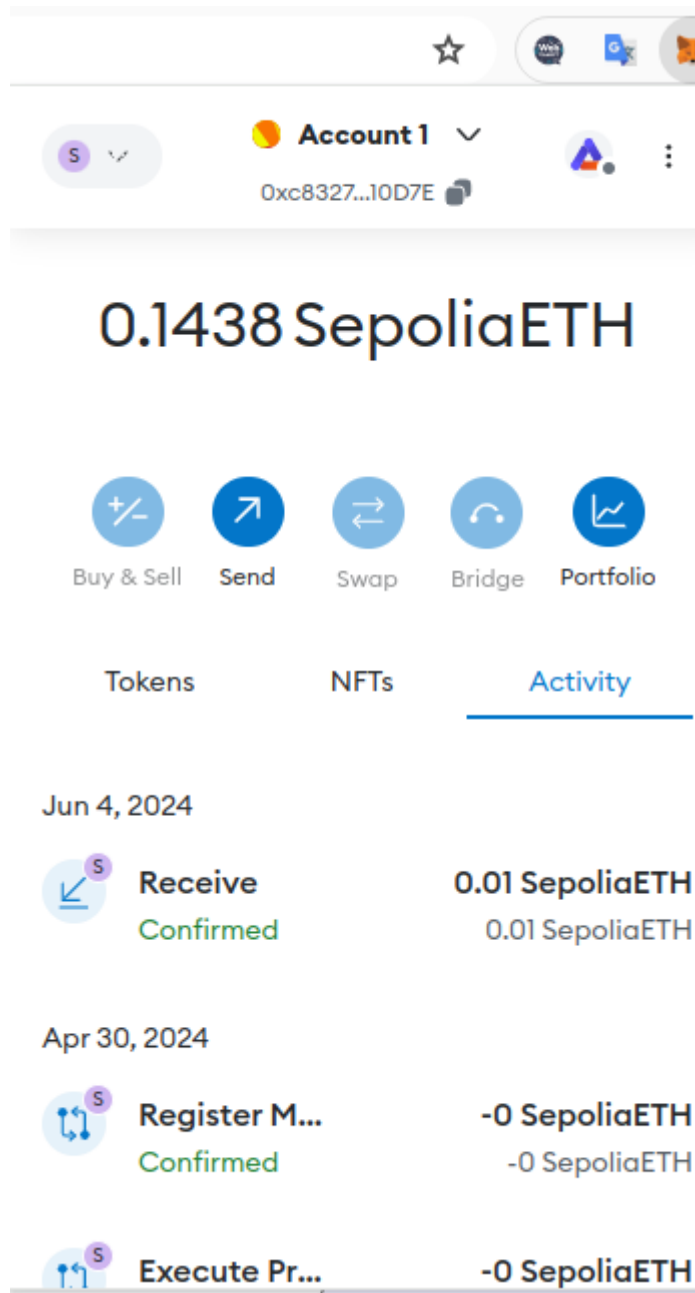
2 Crear una cuenta de Ethereum a través de Metamask

Para crear transacciones en Ethereum hay que hacerlo a través de una cuenta. La cuenta que usaremos para este Sprint es 0xc83273f025ecEd0317f52DfE26d95C4638a10D7E

3 Obtener Ether a través de un faucet

Para desplegar contratos y enviar transacciones a la red, es necesario gastar Gas. A través de un faucet o grifo se puede obtener Ether para redes de prueba. Últimamente, los faucets se han protegido frente a los bots que demandan continuamente Ether de prueba y, por lo tanto, ahora la mayoría exigen tener algo de saldo en la mainnet para poder pedir Ether de prueba. Ni para la realización de este sprint ni para el de ningún otro, es necesario adquirir Ether en la Mainnet pero por si por algún casual, dispones de una cantidad de Ether en la mainnet que te permite pedir Ether de prueba, utiliza el siguiente faucet de Alchemy para hacerlo <https://www.alchemy.com/faucets/ethereum-sepolia>. Si por el contrario, no

dispones de saldo en la Mainnet, escribe tu dirección pública de tu cuenta en el debate del sprint o en el foro de dudas, para que te pueda hacer una transferencia de Ether de prueba (o pídele saldo a algún compañero).



TX : xead6f9d5876e3621cedeff2003d44cee93e90df0f575c30750a1f30ec8c864a

<https://sepolia.etherscan.io/tx/0xeade6f9d5876e3621cedeff2003d44cee93e90df0f575c30750a1f30ec8c864a>

sepolia.etherscan.io/tx/0xeade6f9d5876e3621cedeff2003d44cee93e90df0f575c30750a1f30ec8c864a

Tube Maps Sacyr Personal Estudios Inicio Remix - Ethere... Home - GitBook Aithor: Ensayo... ChainList IPFS Desktop |... Beco

Sepolia Testnet Search by Address / Txn Hash / Block / Token

Etherscan Home Blockchain T

Transaction Details

Overview State

[This is a Sepolia Testnet transaction only]

Transaction Hash: 0xeade6f9d5876e3621cedeff2003d44cee93e90df0f575c30750a1f30ec8c864a

Status: Success

Block: 6038791 4 Block Confirmations

Timestamp: 58 secs ago (Jun-04-2024 04:07:48 PM +UTC)

From: 0xd1bd27c9bE2943e8ec0ce43d6F8B8f9Ce434EEb7

To: 0xc83273f025ecEd0317f52DfE26d95C4638a10D7E

Value: 0.01 ETH (\$0.00)

Transaction Fee: 0.000661077416307 ETH (\$0.00)

Gas Price: 31.479876967 Gwei (0.000000031479876967 ETH)

More Details: + Click to show more

A transaction is a cryptographically signed instruction that changes the blockchain state. Block explorers track the details of all transactions in the network. Learn more about transactions in our [Knowledge](#)

sepoliafaucet.io

Gmail YouTube Maps Sacyr Personal Estudios Inicio Remix - Ethere... Home - GitBook Aithor: Ensayo... ChainList IPFS Desktop |... Become a Part... Ethereum Tran...

Sepolia Faucet. Powered by Automata 2.0

Holesky Sepolia FAQ

Attest your device to claim Sepolia ETH

Backed by Proof of Machinehood, Ethereum Sepolia Faucet provides a reliable drip of testnet tokens. No account sign-ups. No social verification. No tasklist.

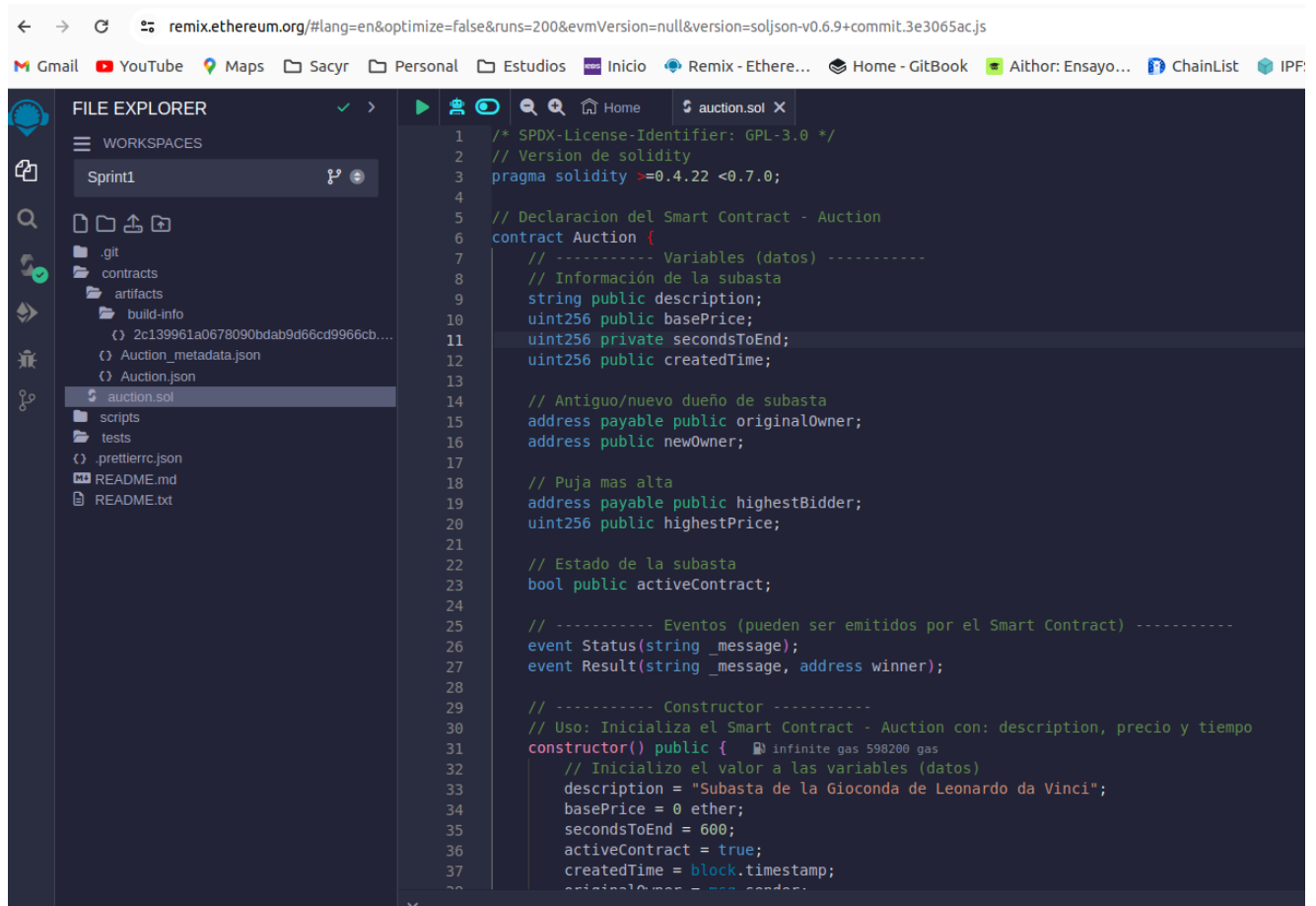
0xc83273f025ecEd0317f52DfE26d95C4638a10D7E

Get Tokens

4 Copiar el Smart Contract en Remix IDE

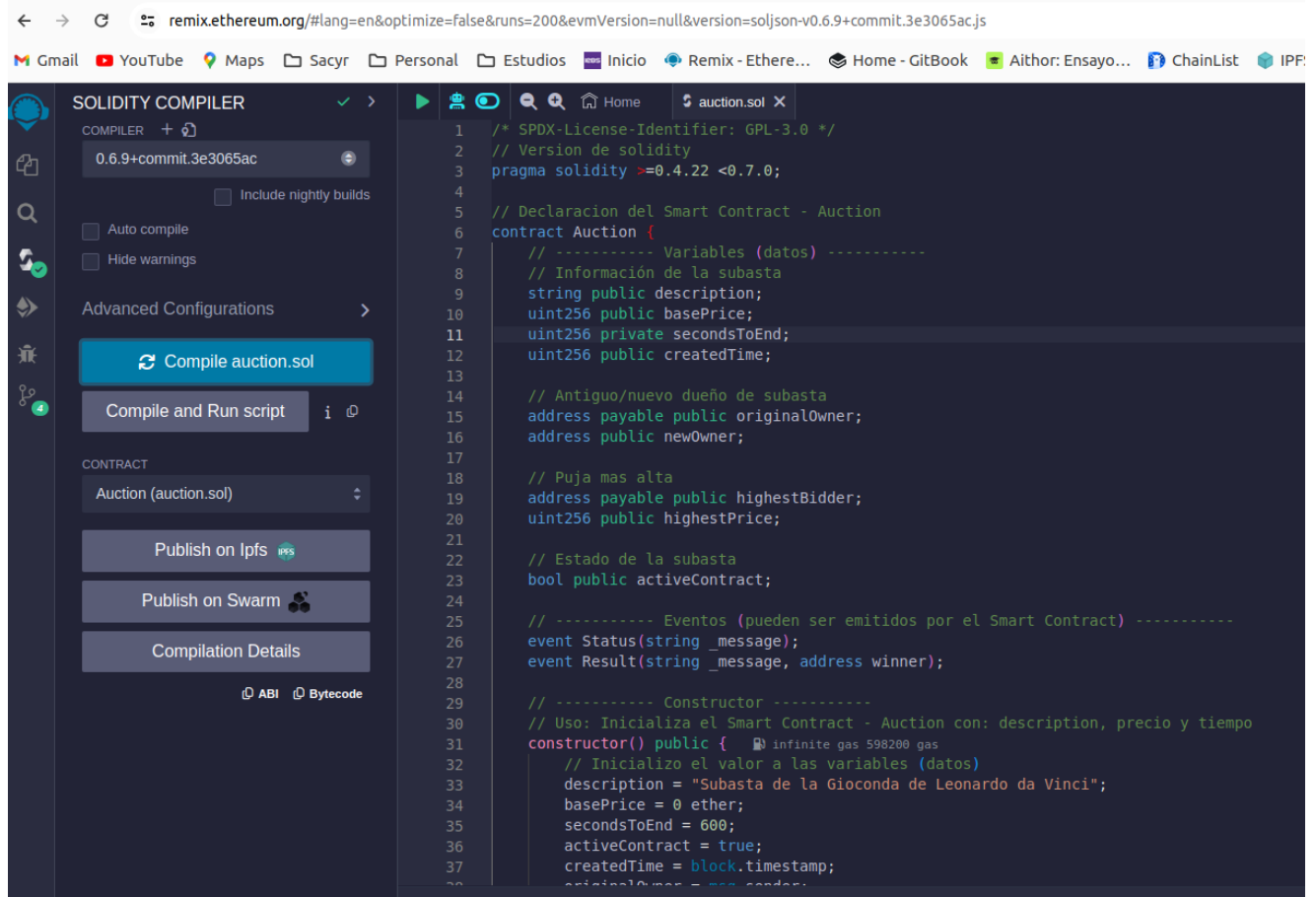
Generación de un archivo con extensión .sol con el contenido del smart contract en Remix IDE. El código del smart contract puedes encontrarlo aquí: <https://github.com/CesRC/auction-example-solidity>

Fichero Auction.sol



```
1  /* SPDX-License-Identifier: GPL-3.0 */
2  // Version de solidity
3  pragma solidity >=0.4.22 <0.7.0;
4
5  // Declaracion del Smart Contract - Auction
6  contract Auction {
7      // ----- Variables (datos) -----
8      // Información de la subasta
9      string public description;
10     uint256 public basePrice;
11     uint256 private secondsToEnd;
12     uint256 public createTime;
13
14     // Antiguo/nuevo dueño de subasta
15     address payable public originalOwner;
16     address public newOwner;
17
18     // Puja mas alta
19     address payable public highestBidder;
20     uint256 public highestPrice;
21
22     // Estado de la subasta
23     bool public activeContract;
24
25     // ----- Eventos (pueden ser emitidos por el Smart Contract) -----
26     event Status(string _message);
27     event Result(string _message, address winner);
28
29     // ----- Constructor -----
30     // Uso: Inicializa el Smart Contract - Auction con: description, precio y tiempo
31     constructor() public {
32         // Inicializo el valor a las variables (datos)
33         description = "Subasta de la Gioconda de Leonardo da Vinci";
34         basePrice = 0 ether;
35         secondsToEnd = 600;
36         activeContract = true;
37         createTime = block.timestamp;
38         originalOwner = msg.sender;
```

Se compila con version 0.0.6.9 menor que la que se exige



```
1  /* SPDX-License-Identifier: GPL-3.0 */
2  // Version de solidity
3  pragma solidity >=0.4.22 <0.7.0;
4
5  // Declaracion del Smart Contract - Auction
6  contract Auction {
7      // ----- Variables (datos) -----
8      // Información de la subasta
9      string public description;
10     uint256 public basePrice;
11     uint256 private secondsToEnd;
12     uint256 public createTime;
13
14     // Antiguo/nuevo dueño de subasta
15     address payable public originalOwner;
16     address public newOwner;
17
18     // Puja mas alta
19     address payable public highestBidder;
20     uint256 public highestPrice;
21
22     // Estado de la subasta
23     bool public activeContract;
24
25     // ----- Eventos (pueden ser emitidos por el Smart Contract) -----
26     event Status(string _message);
27     event Result(string _message, address winner);
28
29     // ----- Constructor -----
30     // Uso: Inicializa el Smart Contract - Auction con: description, precio y tiempo
31     constructor() public {
32         // Inicializo el valor a las variables (datos)
33         description = "Subasta de la Gioconda de Leonardo da Vinci";
34         basePrice = 0 ether;
35         secondsToEnd = 600;
36         activeContract = true;
37         createTime = block.timestamp;
38         originalOwner = msg.sender;
```

5 Compilar y desplegar el Smart Contract en Remix IDE

Compilación a bytecode y despliegue del código del smart contract en la red de Ethereum para poder interactuar con él.

Despliegue en TestNet Sepolia usando Metamask

The screenshot displays the Remix IDE interface with the following components:

- Left Panel (DEPLOY & RUN TRANSACTIONS):**
 - ENVIRONMENT:** Injected Provider - MetaMask.
 - ACCOUNT:** Sepolia (11155111) network.
 - GAS LIMIT:** Estimated Gas (3000000).
 - VALUE:** 0 Wei.
 - CONTRACT:** Auction - contracts/auction.sol.
 - Buttons:** Deploy, Publish to IPFS, At Address, Load contract from Address.
 - Transactions recorded:** 0.
 - Pinned Contracts:** No pinned contracts found for selected workspace & network.
- Center Panel (Code Editor):** Contains the Solidity code for the 'Auction' smart contract, including variables, events, and a constructor.
- Right Panel (MetaMask):** A modal window titled 'Connect with MetaMask' showing a list of accounts. The first account, 'Account 1 (0xc8327...10d7e)', is selected.

Deploy:

remix.ethereum.org/#lang=en&optimize=false&runs=200&evmVersion=null&version=soljson-v0.6.9+commit.3e3065ac.js

Gmail YouTube Maps Sacry Personal Estudios Inicio Remix - Ethere... Home - GitBook Aithor: Ensayo... ChainList IPF:

DEPLOY & RUN TRANSACTIONS

ENVIRONMENT

Injected Provider - MetaMask

Sepolia (11155111) network

ACCOUNT

0xc83...10D7E (0.15382735913366)

GAS LIMIT

☒ Estimated Gas

☐ Custom 3000000

VALUE

0 Wei

CONTRACT

Auction - contracts/auction.sol

evm version: istanbul

Deploy

☐ Publish to IPFS

At Address Load contract from Address

Transactions recorded

Pinned Contracts (network: 11155111)

No pinned contracts found for selected workspace & network

```
1  /* SPDX-License-Identifier: GPL-3.0 */
2  // Version de solidity
3  pragma solidity >=0.4.22 <0.7.0;
4
5  // Declaracion del Smart Contract - Auction
6  contract Auction {
7      // ----- Variables (datos) -----
8      // Información de la subasta
9      string public description;
10     uint256 public basePrice;
11     uint256 private secondsToEnd;
12     uint256 public createdTime;
13
14     // Antiguo/nuevo dueño de subasta
15     address payable public originalOwner;
16     address public newOwner;
17
18     // Puja mas alta
19     address payable public highestBidder;
20     uint256 public highestPrice;
21
22     // Estado de la subasta
23     bool public activeContract;
24
25     // ----- Eventos (pueden ser empujados) -----
26     event Status(string _message);
27     event Result(string _message, address _winner);
28
29     // ----- Constructor -----
30     // Uso: Inicializa el Smart Contract
31     constructor() public {  infinite gas
32         // Inicializo el valor a las variables
33         description = "Subasta de la Gioconda de Leonardo da Vinci";
34         basePrice = 0 ether;
35         secondsToEnd = 600;
36         activeContract = true;
37         createdTime = block.timestamp;
38         originalOwner = msg.sender;
39     }
```

MetaMask

Sepolia test network

Account 1 New contract

https://remix.ethereum.org

CONTRACT DEPLOYMENT

DETAILS HEX

Estimated changes

No changes predicted for your wallet

Estimated fee 0.00315143

0.00315143 SepoliaETH

Market -60 sec Max fee: 0.00379575 SepoliaETH

Reject Confirm

```
creation of Auction pending...
view on etherscan
[block:6039694 txIndex:134] from: 0xc83...10d7e to: Auction.(constructor) value: 0 wei data: 0x608...e6369 logs: 1 hash: 0x099...2096c
```

```
Solidity copilot not activated!
creation of Auction pending...
view on etherscan
[block:6039694 txIndex:134] from: 0xc83...10d7e to: Auction.(constructor) value: 0 wei data: 0x608...e6369 logs: 1 hash: 0x099...2096c

status 0x1 Transaction mined and execution succeed
transaction hash 0x5a975c32699cb931d39bda34960ceacc4a24f60ac655bd21488f6c2502a785b2
block hash 0x099cb2a0e6cf6f768229dbc7a606e53c94373b083b977b99e2eal3be3fb72096c
block number 6039694
contract address 0x33ee37bfe442e0c891a0a951ca7e439e2c68aebf
from 0xc83273f025eced0317f52dfe26d95c4638a10d7e
to Auction.(constructor)
gas 873671 gas
transaction cost 865634 gas
input 0x608...e6369
decoded input {}
decoded output -
logs [
  {
    "from": "0x33ee37bfe442e0c891a0a951ca7e439e2c68aebf",
    "topic": "0x2844c95bf1b4598da931d527f903501abc00fe0199c65da52d5ce818c6c5e961",
    "event": "Status",
    "args": {
      "0": "Subasta abierta",
      "_message": "Subasta abierta"
    }
  }
]
```


TX en xplorer :

<https://sepolia.etherscan.io/tx/0x5a975c32699cb931d39bda34960ceacc4a24f60ac655bd21488f6c2502a785b2>

URL Contrato:

<https://sepolia.etherscan.io/address/0x33ee37bfe442e0c891a0a951ca7e439e2c68aebf>

Verificación y Publicar contrato:

Verify & Publish Contract Source Code

Source code verification provides transparency for users interacting with smart contracts. By uploading the source code, Etherscan will match the compiled code with that on the blockchain. [Read more.](#)

1

Enter Contract Details

2

Verify & Publish

Please enter the Contract Address you would like to verify

0x33ee37bfe442e0c891a0a951ca7e439e2c68aebf

Please select Compiler Type

Solidity (Single file)

Please select Compiler

Select Compiler Type before selecting Compiler Version

v0.6.9+commit.3e3065ac

☒ Uncheck to show all nightly commits

Please select Open Source License Type ⓘ

5) GNU General Public License v3.0 (GNU GPLv3)

☒ I agree to the [terms of service](#)

Upload Contract Source Code

1. If the contract compiles correctly at [REMIX](#), it should also compile correctly here.
2. We have limited support for verifying contracts created by another contract and there is a timeout of up to 45 seconds for each contract compiled.
3. For programatic contract verification, check out the [Contract API Endpoint](#).

Contract Address: **0x33ee37bfe442e0c891a0a951ca7e439e2c68aebf**
 Compiler Type: **SINGLE FILE / CONCATENATED METHOD**
 Compiler Version: **v0.6.9+commit.3e3065ac**

Enter the Solidity Contract Code below *

[Fetch from Gist](#)

```
// Se emite un evento
emit Status("La subasta se cierra");
}

// ----- Funciones que consultan datos (get) -----

// Funcion
// Nombre: getAuctionInfo
// Logica: Consulta la description, y la fecha de creacion de la subasta
```

Advanced Configuration

Optimization ?

No

Runs (Optimizer) ?

200

EVM version ?

default (compiler defaults)

A list of target EVM versions and the compiler-relevant changes introduced at each version. Backward compatibility is not guaranteed between each version.

Resultado verificación y publicación

Verify & Publish Contract Source Code

Source code verification provides transparency for users interacting with smart contracts. By uploading the source code, Etherscan will match the compiled code with that on the blockchain. [Read more.](#)

A simple and structured interface for verifying smart contracts that fit in a single file.

1 Enter Contract Details — 2 **Verify & Publish**

✓ **Successfully generated Bytecode and ABI for Contract Address**
[0x33ee37bfe442e0c891a0a951ca7e439e2c68aebf]


🕒 Learn how to verify your contract on multiple blockchains with a single API key [here](#).

Code Reader ?

✦ Prompt:

You are a conscientious blockchain security auditor. Review this smart contract's source code to suggest best practices it could follow and share any security concerns with the code.

Analyse Contract ✎

 **Contract** 0x33eE37BFfe442E0c891A0A951cA7e439E2C68aebf

Source Code

Overview

ETH BALANCE
0 ETH

More Info

CONTRACT CREATOR
0xc83273f0...638a10D7E at txn 0x5a975c3269...

Multichain Info

N/A

Transactions

Token Transfers (ERC-20)

Contract

Events

Code

Read Contract

Write Contract

🔍 Search Source Code

✓ **Contract Source Code Verified** (Exact Match)

⚠️

Contract Name: **Auction**

Optimization Enabled: **No** with 200 runs

Compiler Version: **v0.6.9+commit.3e3065ac**

Other Settings: **default evmVersion, GNU GPLv3 license**

📄 Contract Source Code (Solidity)

IDE

Outline

More Options

```
1- /**
2-  *Submitted for verification at Etherscan.io on 2024-06-04
3-  */
4-
5-  /* SPDX-License-Identifier: GPL-3.0 */
6-  // Version de solidity
7-  pragma solidity >=0.4.22 <0.7.0;
8-
9-  // Declaración del Smart Contract - Auction
10- contract Auction {
11-    // ----- Variables (datos) -----
12-    // Información de la subasta
13-    string public description;
14-    uint256 public basePrice;
```

Metodos de consultas READ

Overview

ETH BALANCE
0 ETH

More Info

CONTRACT CREATOR
0xc83273f0...638a10D7E at txn 0x5a975c3269...

Multichain Info

N/A

Transactions

Token Transfers (ERC-20)

Contract

Events

Code

Read Contract

Write Contract

Connected - Web3 [0xc832...0D7E]

Read Contract Information

[Expand all] [Reset]

1. activeContract

2. basePrice

3. createdTime

4. description

5. getAuctionInfo

6. getHighestPrice

7. highestBidder

8. highestPrice

9. newOwner

10. originalOwner

Metodos de Escritura : Write

Overview

ETH BALANCE
0 ETH

More Info

CONTRACT CREATOR
0xc83273f0...638a10D7E at txn 0x5a975c3269...

Multichain Info

N/A

Transactions

Token Transfers (ERC-20)

Contract

Events

Code

Read Contract

Write Contract

Connect to Web3

1. bid (0x1998aeeF)

bid

payableAmount (ether)

Write

2. checkIfAuctionEnded (0xc1f12974)

Write

3. stopAuction (0x269b9a08)

Write

6 Envío de transacciones al Smart Contract con Remix IDE

Para utilizar el smart contract hay que generar transacciones, en este caso realizarás con tu cuenta una transacción de puja a través del método bid.

Transacciones del Contrato creado:

https://sepolia.etherscan.io/address/0x33ee37bfe442e0c891a0a951ca7e439e2c68aebf

Ejecuta metodo Bid:

DEPLOY & RUN
TRANSACTIONS

Pinned Contracts (network: 11155111)

No pinned contracts found for selected workspace & network

Deployed/Unpinned Contracts

▼ AUCTION AT 0X33E...8AEBF (t

Balance: 0 ETH

bid

checkIfAucti...

stopAuction

activeContract

basePrice

createdTime

description

getAuctionInfo

getHighestPr...

highestBidder

highestPrice

newOwner

originalOwner

MetaMask

Sepolia test network

Account 1 → 0x33eE3...8a...

https://remix.ethereum.org

0x33eE3...8aebf : BID ⓘ

DETAILS HEX

Estimated changes ⓘ

No changes predicted for your wallet

Estimated fee ⓘ 0.00017223

0.00017223 SepoliaETH

Market -60 sec Max fee: 0.0002095 SepoliaETH

Reject Confirm

Transactions Token Transfers (ERC-20) Contract Events

Latest 2 from a total of 2 transactions

Download Page Data

Transaction Hash	Method	Block	Age	From	To	Value	Txn Fee
0x757818736c...	Bid	6039763	30 secs ago	0xc83273f0...638a10D7E	0x33eE37BF...E2C68aebf	0 ETH	0.00014644
0x5a975c3269...	0x60806040	6039694	15 mins ago	0xc83273f0...638a10D7E	Create: Auction	0 ETH	0.00321997

From:
0xc83273f025ed0317f52dfE26d95C4638a10D7E

To:
0x33eE37BF442E0c891A0A951cA7e439E2C68aebf

Value:
0.00000000000003 ETH (\$0.00)

Transaction Fee:
0.000245655587375 ETH (\$0.00)

Gas Price:
3.1137025 Gwei (0.0000000031137025 ETH)

Gas Limit & Usage by Txn:
79,791 | 78,895 (98.88%)

Gas Fees:
Base: 1.6137025 Gwei | Max: 3.677305711 Gwei | Max Priority: 1.5 Gwei

Burnt & Txn Savings Fees:
Burnt: 0.0001273130587375 ETH (\$0.00) Txn Savings: 0.000044465475331845 ETH (\$0.00)

Other Attributes:
Txn Type: 2 (EIP-1559) Nonce: 46 Position In Block: 48

Input Data:
Function: bid()
MethodID: 0x1998aeeF
View Input As

More Details:
Click to show less

DEPLOY & RUN TRANSACTIONS

CONTRACT

evm version: istanbul

At Address Load contract from Address

Transactions recorded 6

Run transactions using the latest compilation result

Save Run

Pinned Contracts (network: 11155111)

No pinned contracts found for selected workspace & network

Deployed/Unpinned Contracts

Auction AT 0x33E...8AEBF (i)

Balance: 0.001 ETH

bid

checkIfAucti...

stopAuction

activeContract

0: bool: false

basePrice

0: uint256: 0

createdTime

0: uint256: 1717529820

description

Home auction.sol Docgen Viewer Quick Dapp scenario.json

```

1 {
2   "accounts": {
3     "account{0}": "0xc83273f025ed0317f52dfE26d95C4638a10D7E"
4   },
5   "linkReferences": {},
6   "transactions": [
7     {
8       "timestamp": 1717529783896,
9       "record": {
10        "value": "0",
11        "inputs": "()",
12        "parameters": [],
13        "name": "",
14        "type": "constructor",
15        "abi": "0x49631db77b9307514de37caa13f2f4aab246f119c27369cbaaf6b61f54bbee48",
16        "contractName": "Auction",
17        "bytecode": "608060405234801561001057600080fd5b50604051806000160405280602b815260200160
18        "linkReferences": {},
19        "from": "account{0}"
20      },
21    },
22    {
23      "timestamp": 1717530626489,
24      "record": {
25        "value": "0",
26        "inputs": "()",
27        "parameters": [],
28        "name": "bid",
29        "type": "function",
30        "to": "created{1717529783896}",
31        "abi": "0x49631db77b9307514de37caa13f2f4aab246f119c27369cbaaf6b61f54bbee48",
32        "from": "account{0}"
33      },
34    },
35  ],
36  "args": {
37    "0": "Subasta abierta",
38    "_message": "Subasta abierta"
39  },
40  "data": "0x1998aeeF"
41  }
42  }

```

transact to Auction.bid pending ...

view on etherscan

[block:6039763 txIndex:41] from: 0xc83...10d7e to: Auction.bid() 0x33e...8aebf value: 0 wei data: 0x199...8aeeF

transact to Auction.bid pending ...

Sepolia Testnet

Search by Address / Txn Hash / Block / Token

Etherscan

HomeBlockchainTokensNFTsMisc

Contract0x33eE37BFfe442E0c891A0A951cA7e439E2C68aebf

Source Code

Overview

ETH BALANCE
0.002 ETH

More Info

CONTRACT CREATOR
0xc83273f0...638a10D7E at txn 0x5a975c3269...

Multichain Info

N/A

Transactions

Internal Transactions

Token Transfers (ERC-20)

Contract

Events

Latest 6 from a total of 6 transactions

Download Page Data

Transaction Hash	Method	Block	Age	From	To	Value	Txn Fee
0xe031ff56cf9...	Bid	6039902	20 secs ago	0xc83273f0...638a10D7E	0x33eE37BF...E2C68aebf	0.002 ETH	0.00013018
0x75fbdec4ff8...	Bid	6039798	25 mins ago	0xc83273f0...638a10D7E	0x33eE37BF...E2C68aebf	0.001 ETH	0.00008897
0x14fb2fe0f06...	Bid	6039787	28 mins ago	0xc83273f0...638a10D7E	0x33eE37BF...E2C68aebf	0.001 ETH	0.00013919
0x862a5ddd47...	Bid	6039779	29 mins ago	0xc83273f0...638a10D7E	0x33eE37BF...E2C68aebf	0 ETH	0.00024565
0x757818736c...	Bid	6039763	33 mins ago	0xc83273f0...638a10D7E	0x33eE37BF...E2C68aebf	0 ETH	0.00014644
0x5a975c3269...	0x60806040	6039694	48 mins ago	0xc83273f0...638a10D7E	Create: Auction	0 ETH	0.00321997