DefiDappsDao

Proyecto para el Sptint 1 , 2 y 3

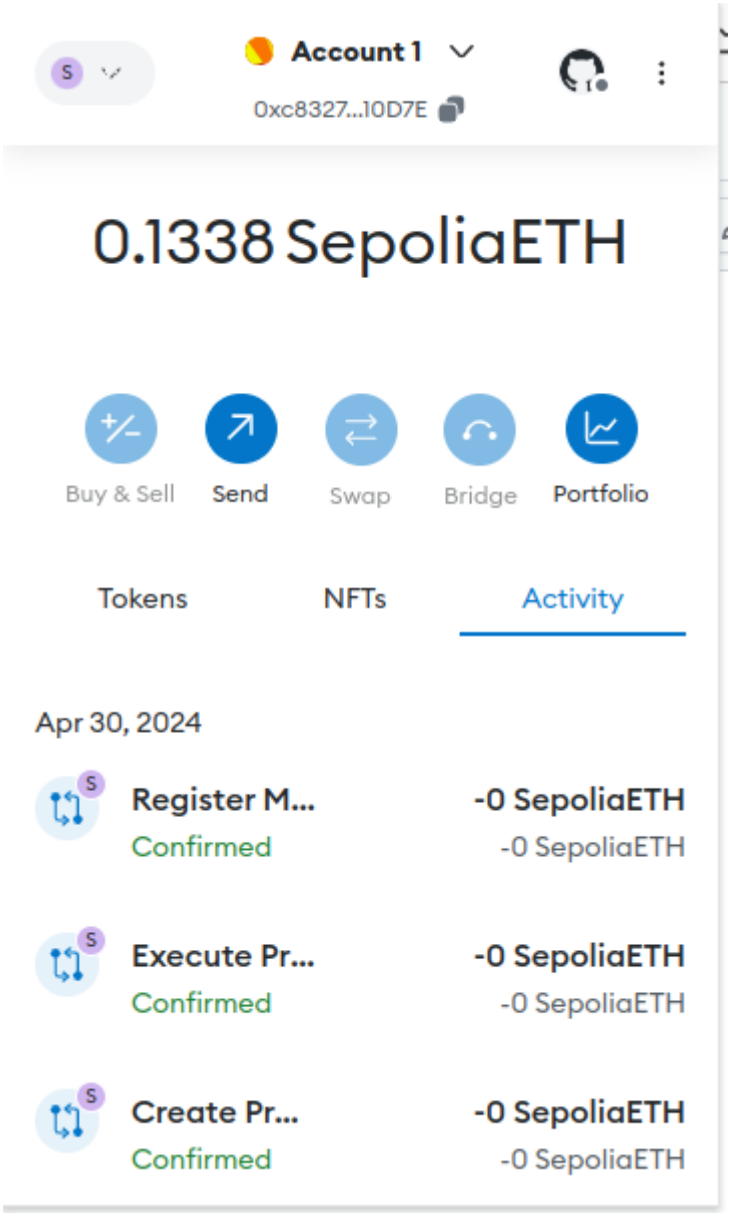
En este sprint instalarás tú mismo un Smart Contract en una testnet de Ethereum en concreto, Sepolia*. El Smart Contract representa una subasta de una obra de arte en la que cualquier usuario con una cuenta de Ethereum puede realizar una puja para hacerse con su propiedad. A continuación se muestran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

Sprint 1

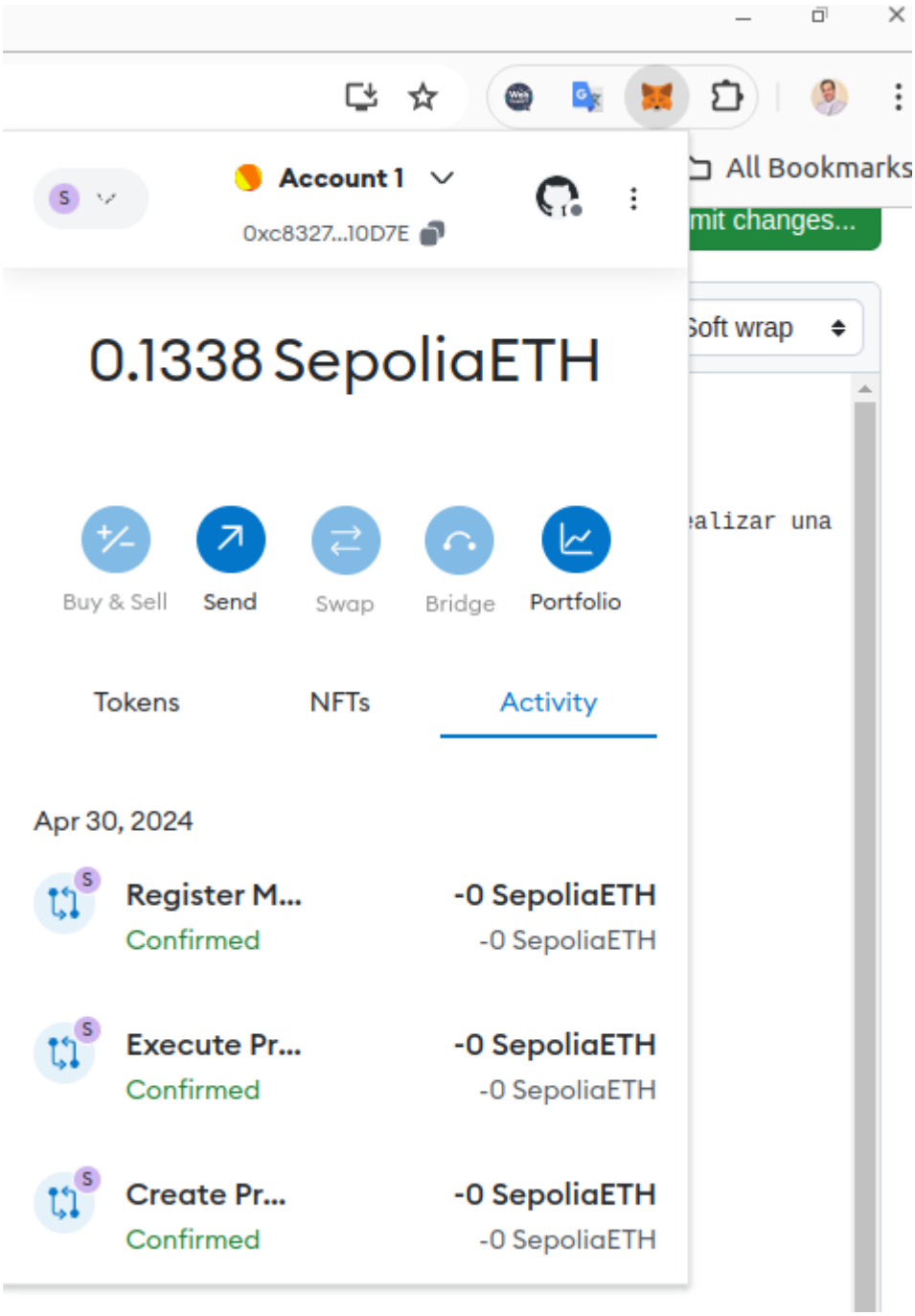
1 Instalar Metamask

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



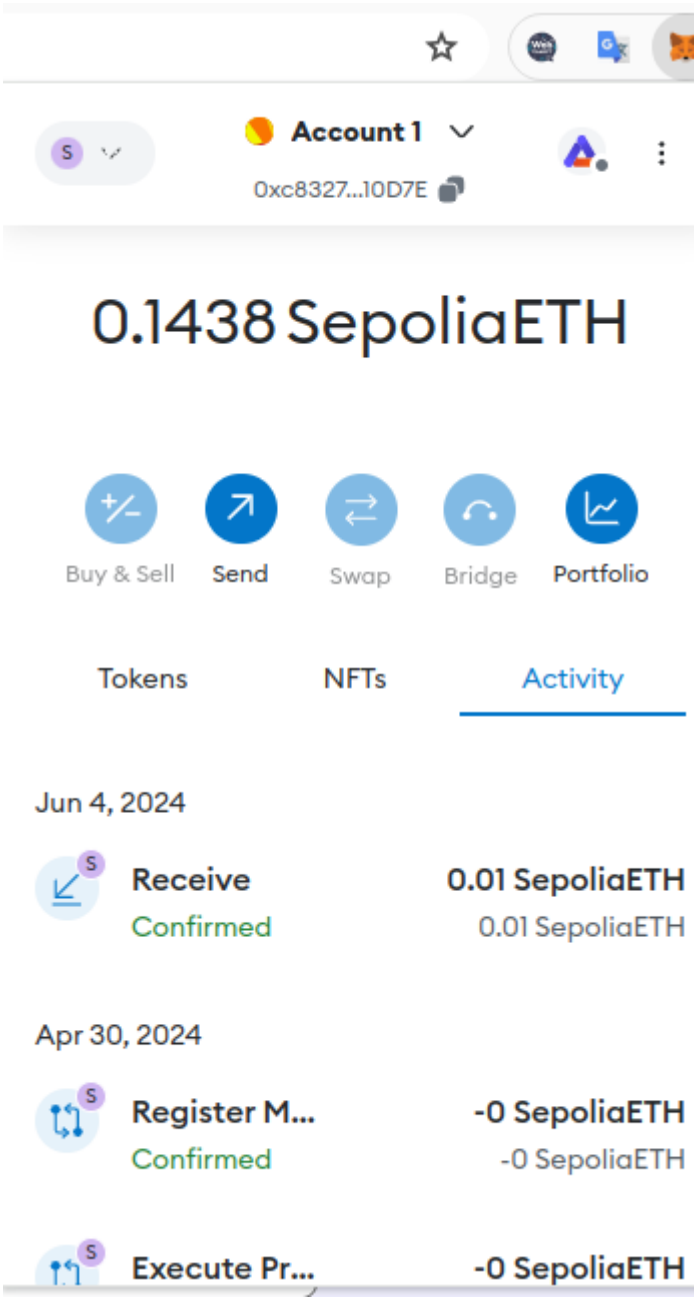
2 Crear una cuenta de Ethereum a través de Metamask

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

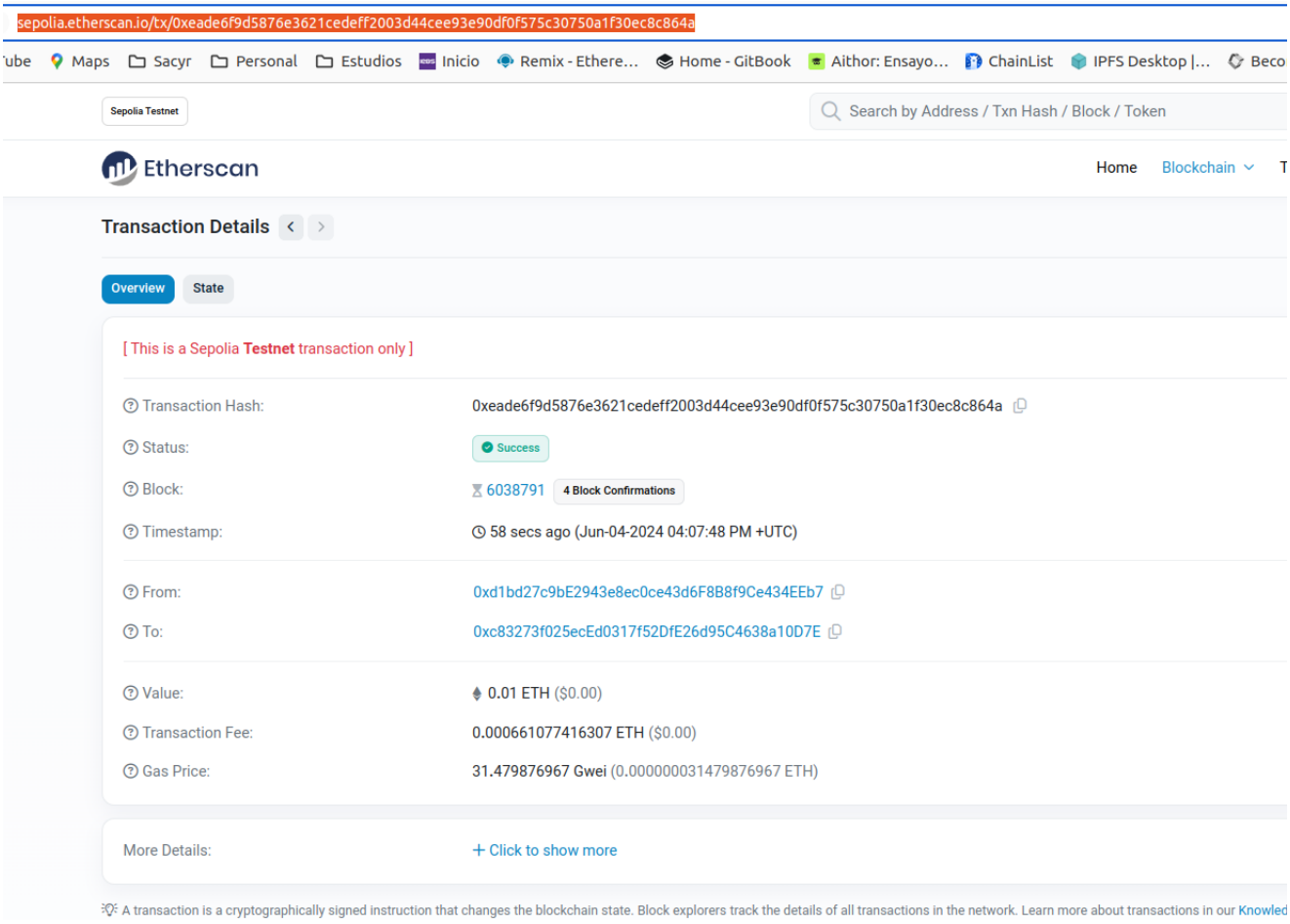
Para desplegar contratos y enviar transacciones a la red, es necesario gastar Gas. A través de un faucet o grifo se puede obtener Ether para redes de prueba. Últimamente, los faucets se han protegido frente a los bots que demandan continuamente Ether de prueba y, por lo tanto, ahora la mayoría exigen 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

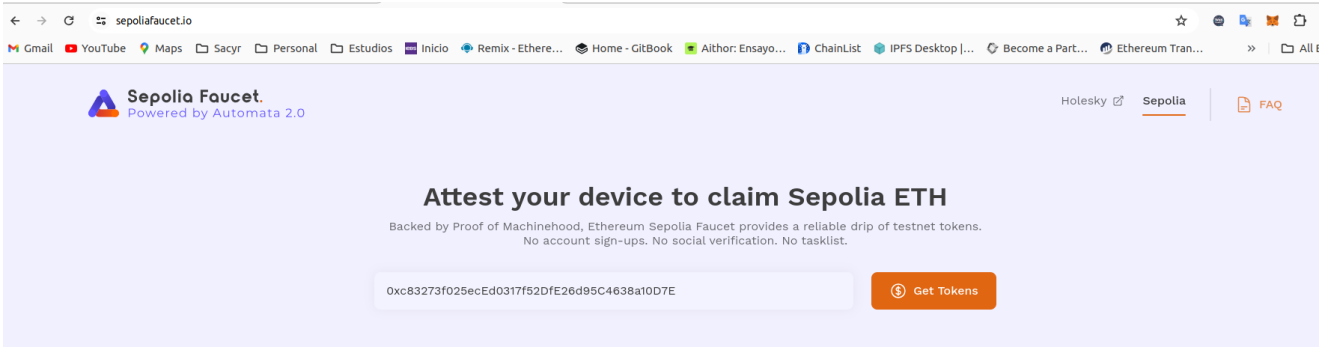
dispones de saldo en la Mainnet, escribe tu dirección pública de tu cuenta en el debate del sprint o en el foro de dudas, para que te pueda hacer una transferencia de Ether de prueba (o pídele saldo a algún compañero).



TX : xeade6f9d5876e3621cedeff2003d44cee93e90df0f575c30750a1f30ec8c864a

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

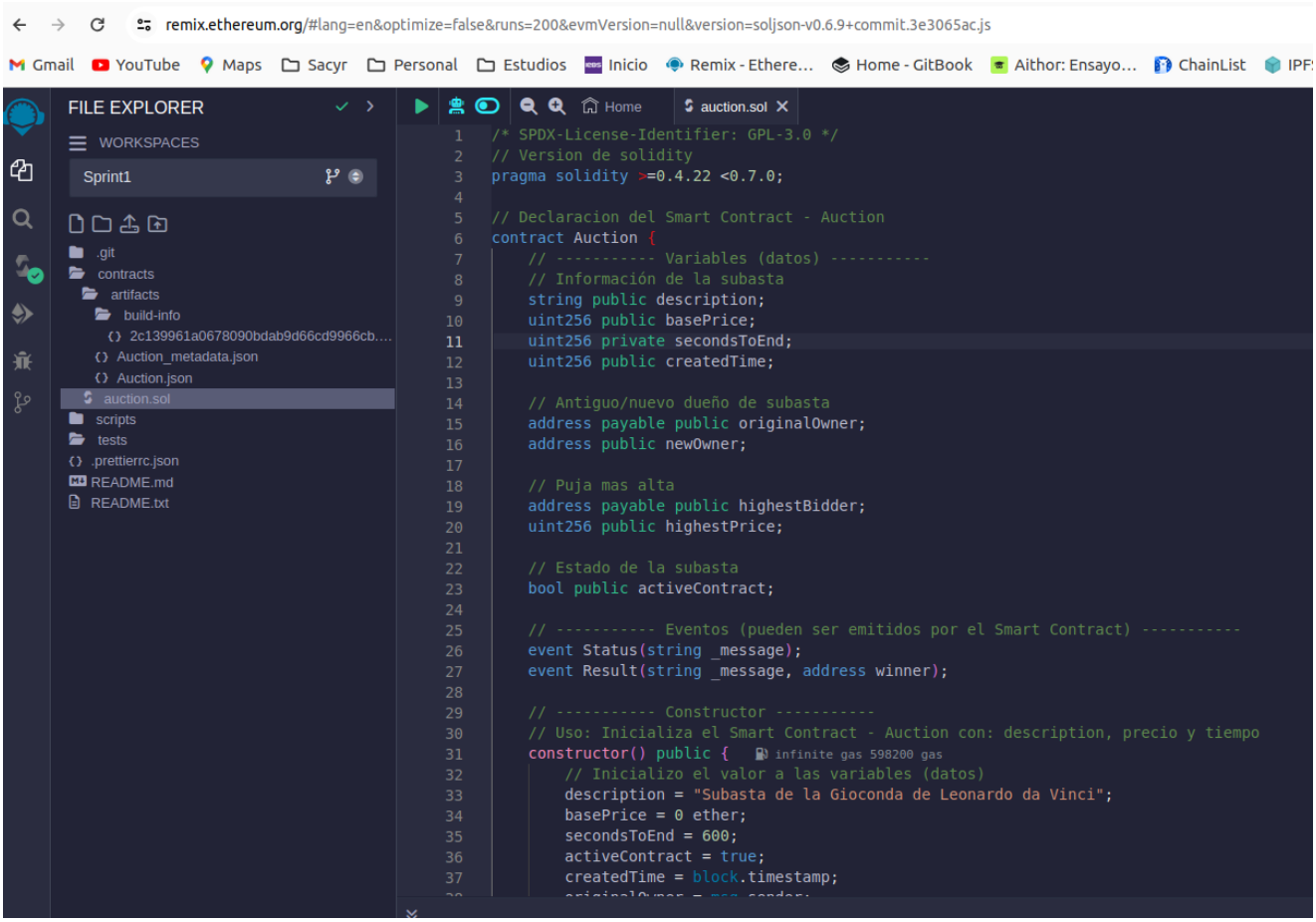




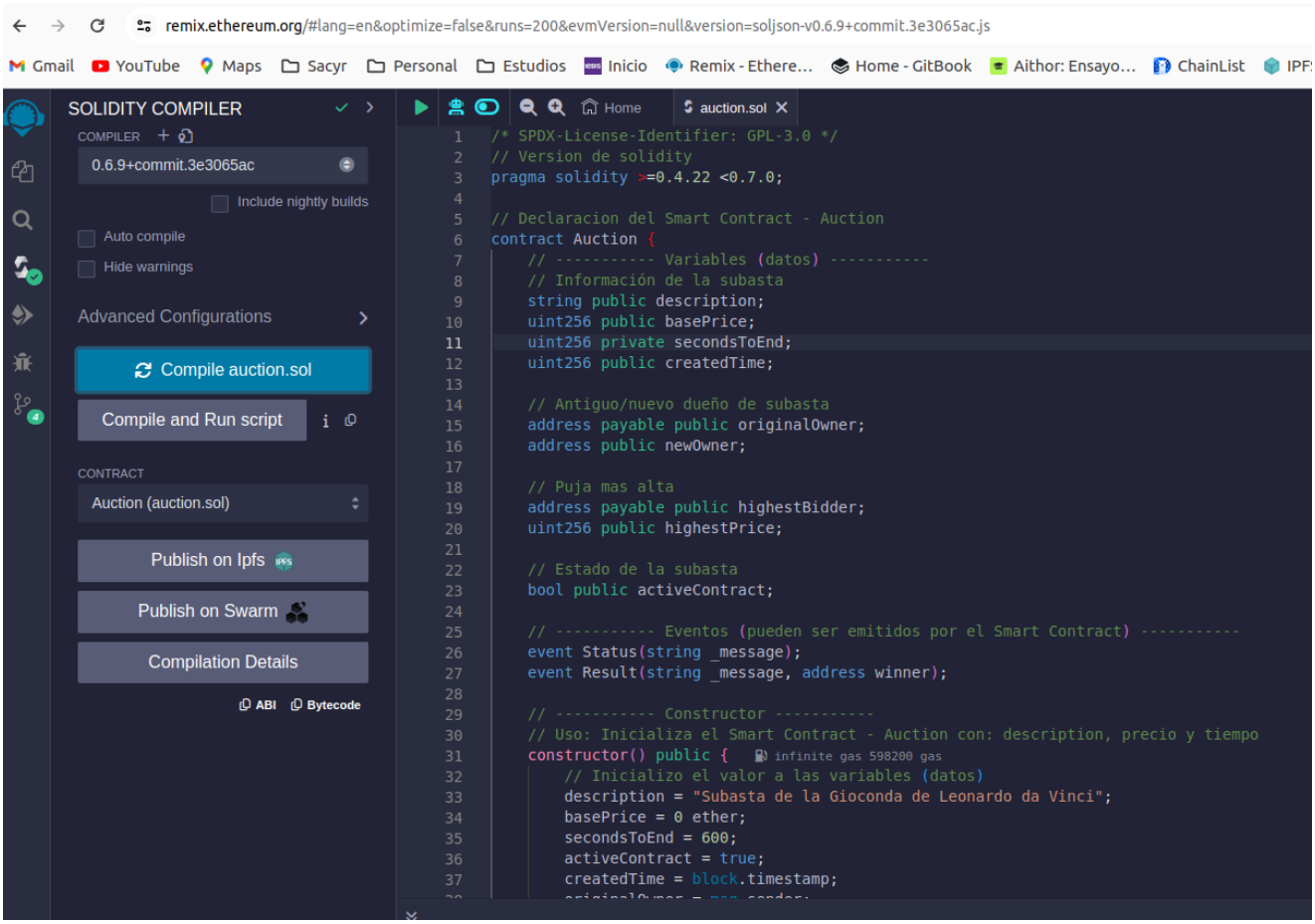
4 Copiar el Smart Contract en Remix IDE

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



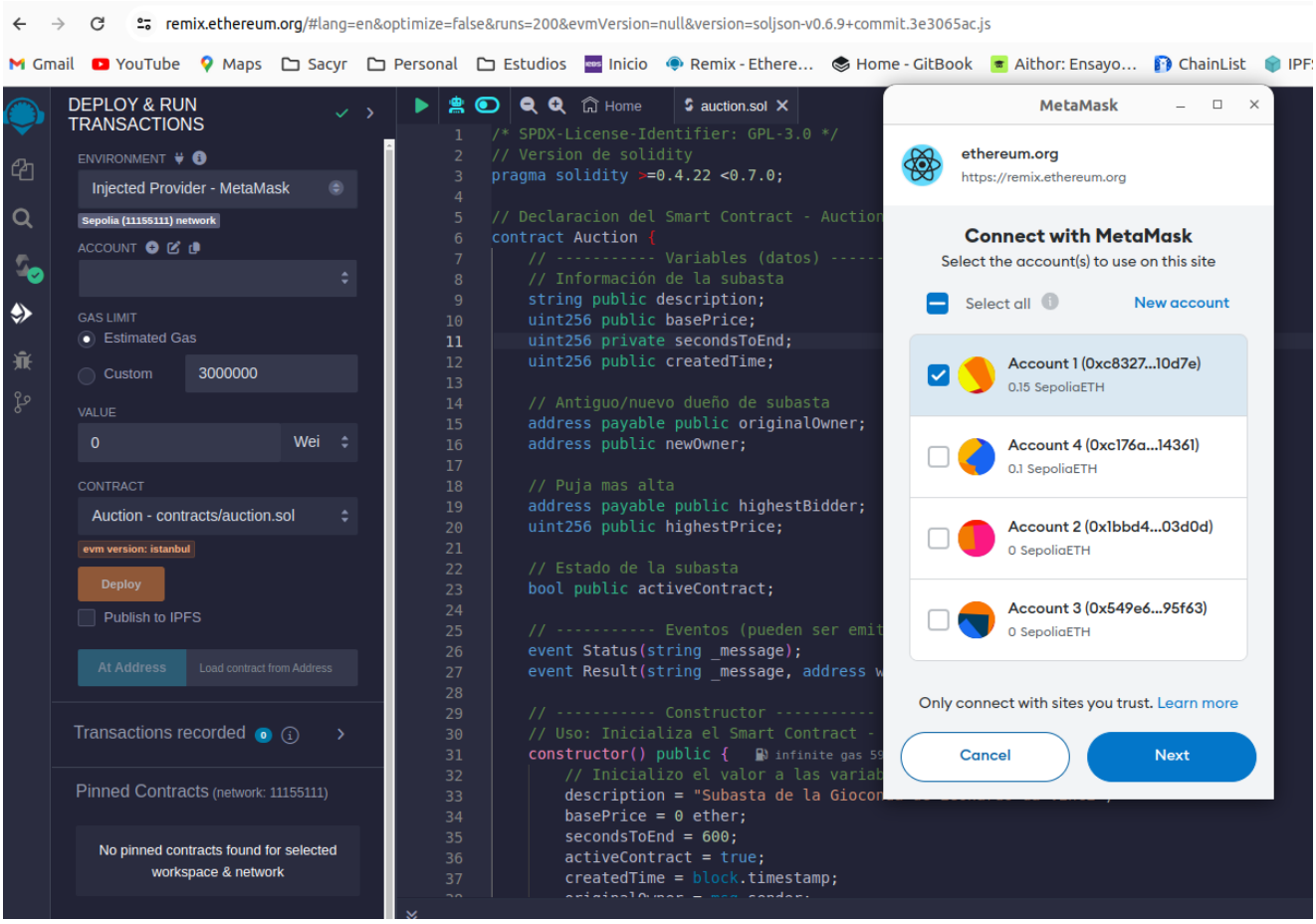
Se compila con version 0.0.6.9 menor que la que se exige



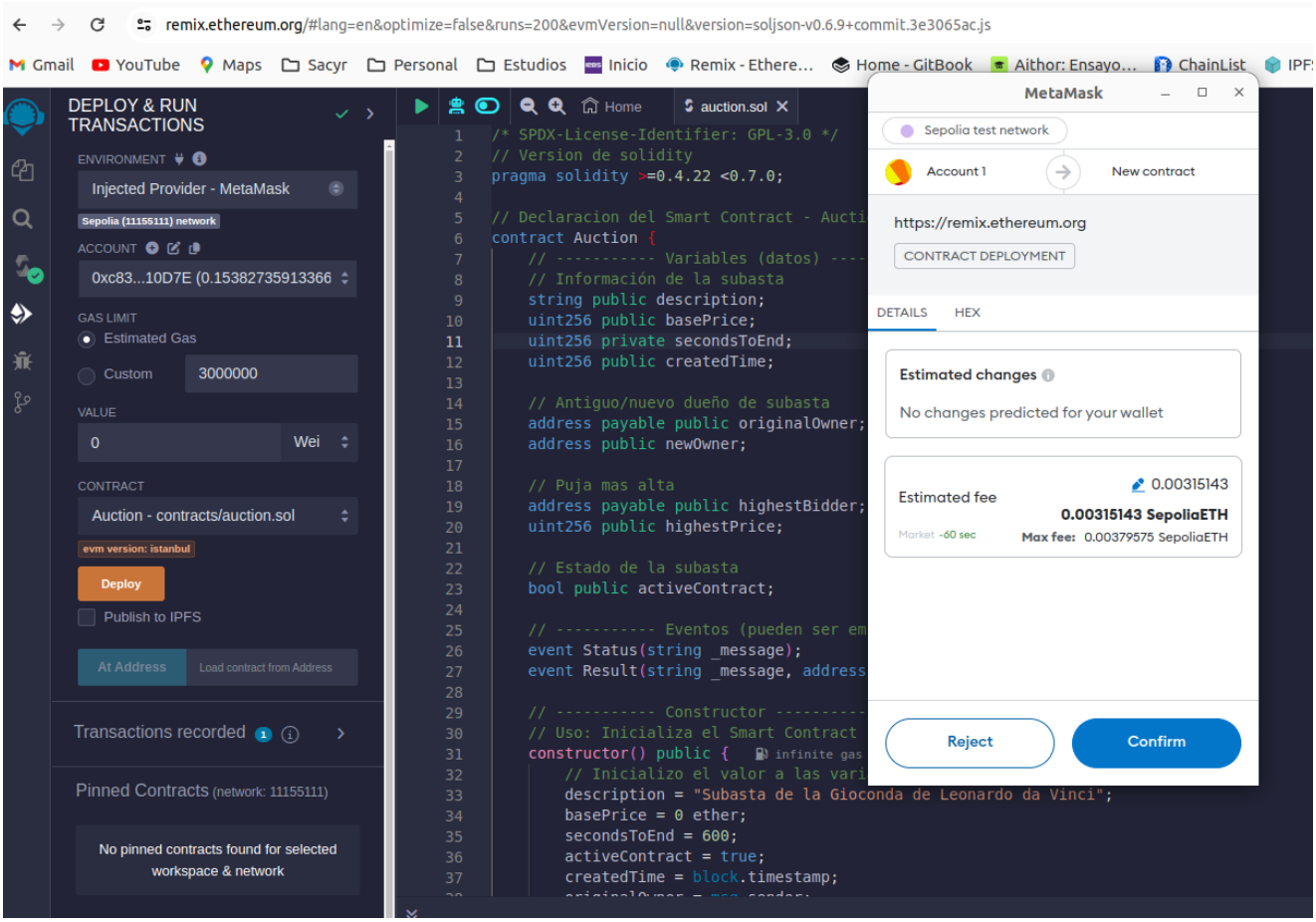
5 Compilar y desplegar el Smart Contract en Remix IDE

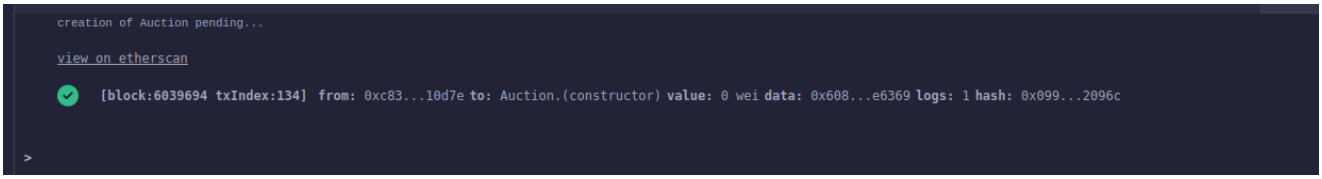
Compilación a bytecode y despliegue del código del smart contract en la red de Ethereum para poder interactuar con él.

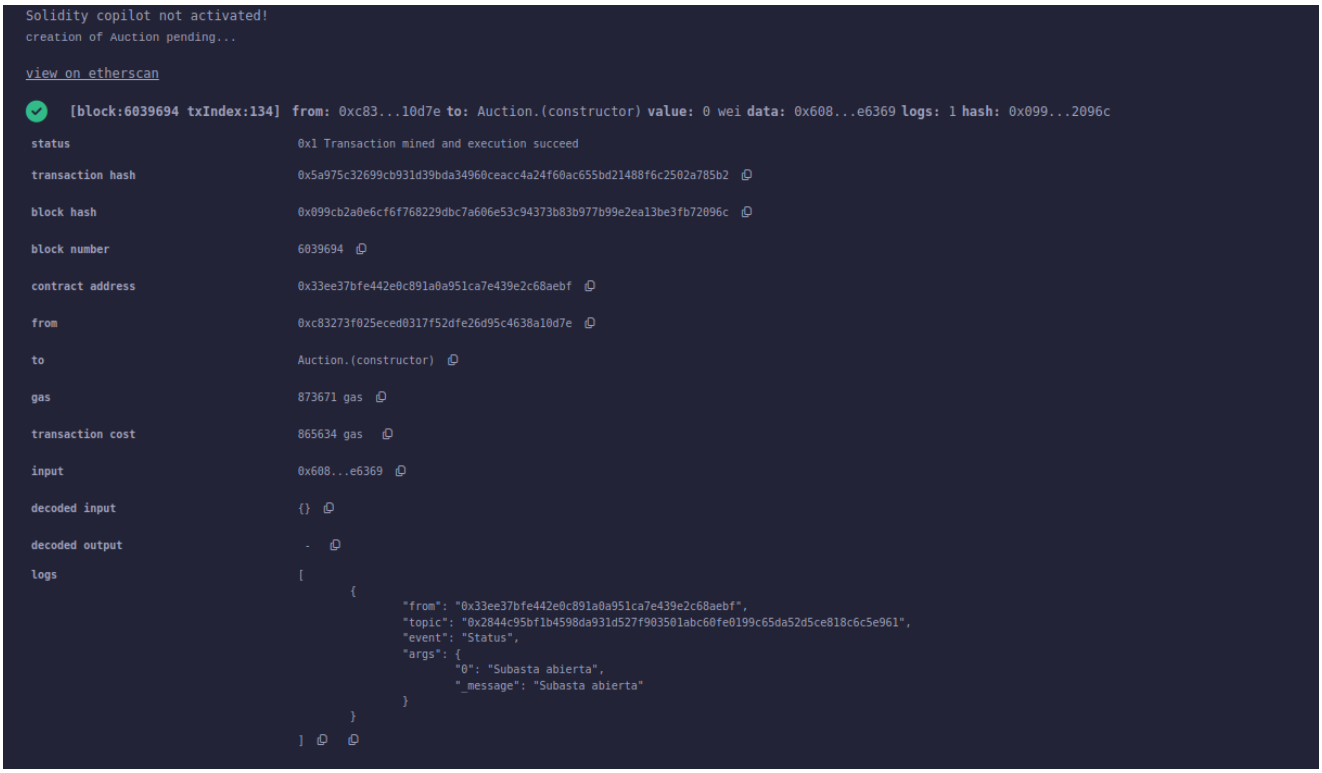
Despliegue en TestNet Sepolia usando Metamask



Deploy:


remix.ethereum.org/#lang=en&optimize=false&runs=200&evmVersion=null&version=soljson-v0.6.9+commit.3e3065ac.js
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
auction.sol
/* SPDX-License-Identifier: GPL-3.0 */
// Version de solidity
pragma solidity >=0.4.22 <0.7.0;
// Declaracion del Smart Contract - Aucti
contract Auction {
// Información de la subasta
string public description;
uint256 public basePrice;
uint256 private secondsToEnd;
uint256 public createdTime;
// Antiguo/nuevo dueño de subasta
address payable public originalOwner;
address public newOwner;
// Puja mas alta
address payable public highestBidder;
uint256 public highestPrice;
// Estado de la subasta
bool public activeContract;
event Status(string _message);
event Result(string _message, address
// Uso: Inicializa el Smart Contract
constructor() public {
description = "Subasta de la Gioconda de Leonardo da Vinci";
basePrice = 0 ether;
secondsToEnd = 600;
activeContract = true;
createdTime = block.timestamp;
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
Max fee: 0.00379575 SepoliaETH
Reject
Confirm

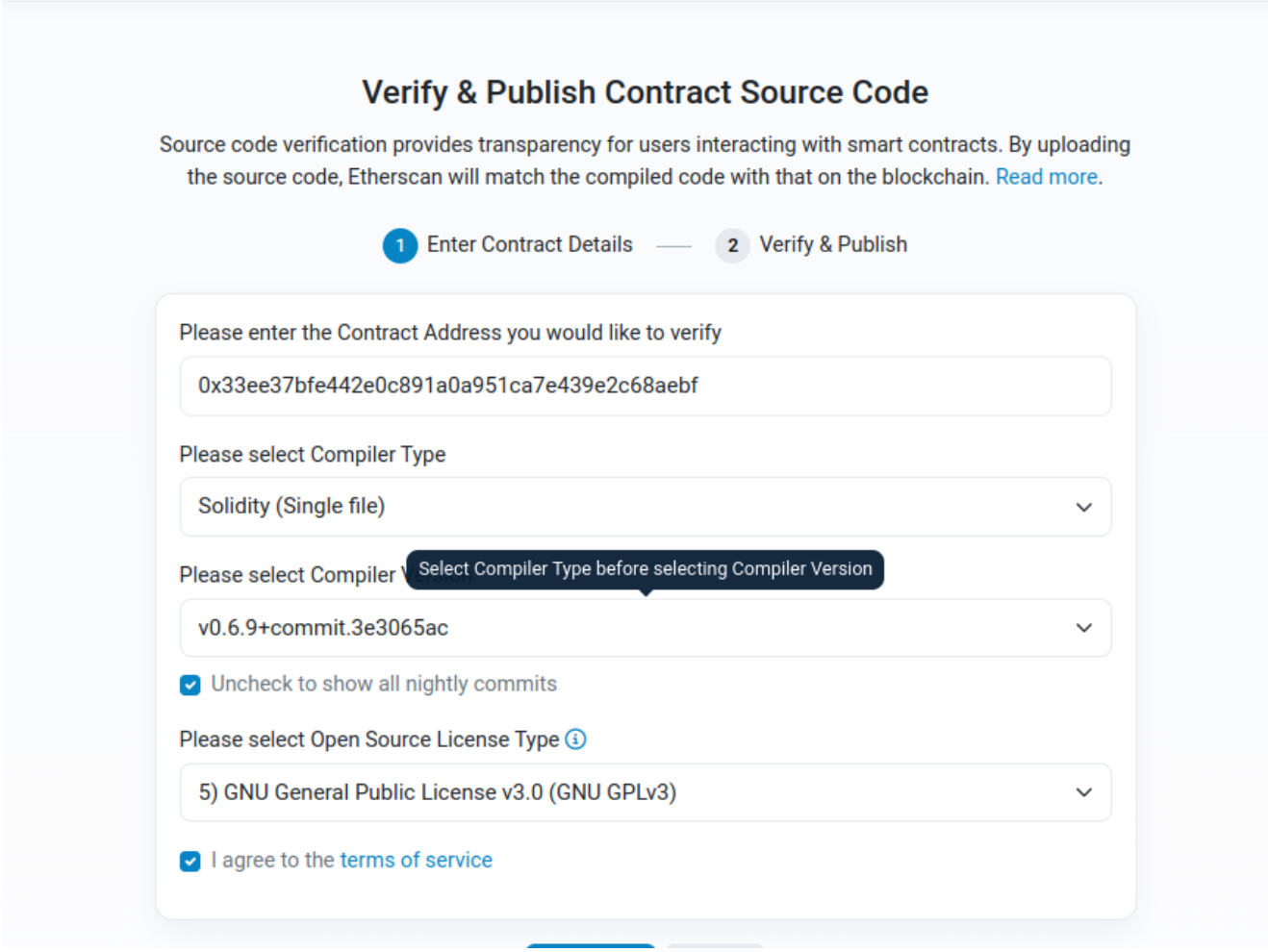

creation of Auction pending...
view on etherscan
[block:6039694 txIndex:134] from: 0xc83...10d7e to: Auction.(constructor) value: 0 wei data: 0x608...e6369 logs: 1 hash: 0x099...2096c

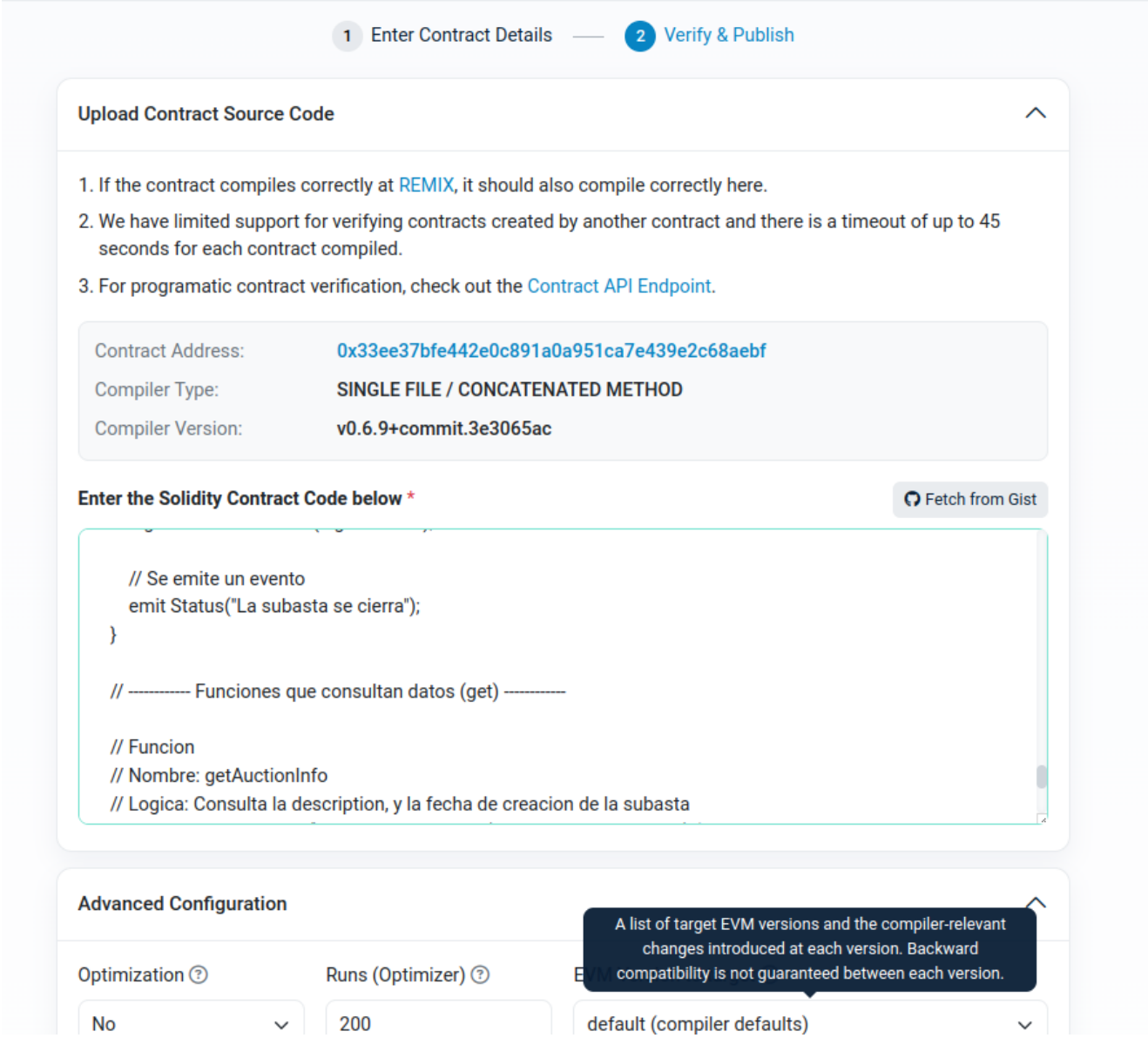

Solidity copilot not activated!
creation of Auction pending...
view on etherscan
[block:6039694 txIndex:134] from: 0xc83...10d7e to: Auction.(constructor) value: 0 wei data: 0x608...e6369 logs: 1 hash: 0x099...2096c
status 0x1 Transaction mined and execution succeed
transaction hash 0x5a975c32699cb931d39bda34960ceacc4a24f60ac655bd21488f6c2502a785b2
block hash 0x099cb2a0e6cf6f768229dbc7a606e53c94373b83b977b99e2ea13be3fb72096c
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": "0x2844c95bf1b4598da931d527f903501abc60fe0199c65da52d5ce818c6c5e961",
"event": "Status",
"args": {
"0": "Subasta abierta",
"_message": "Subasta abierta"

TX en xplorer :
https://sepolia.etherscan.io/tx/0x5a975c32699cb931d39bda34960ceacc4a24f60ac655bd21488f6c2502a785b2

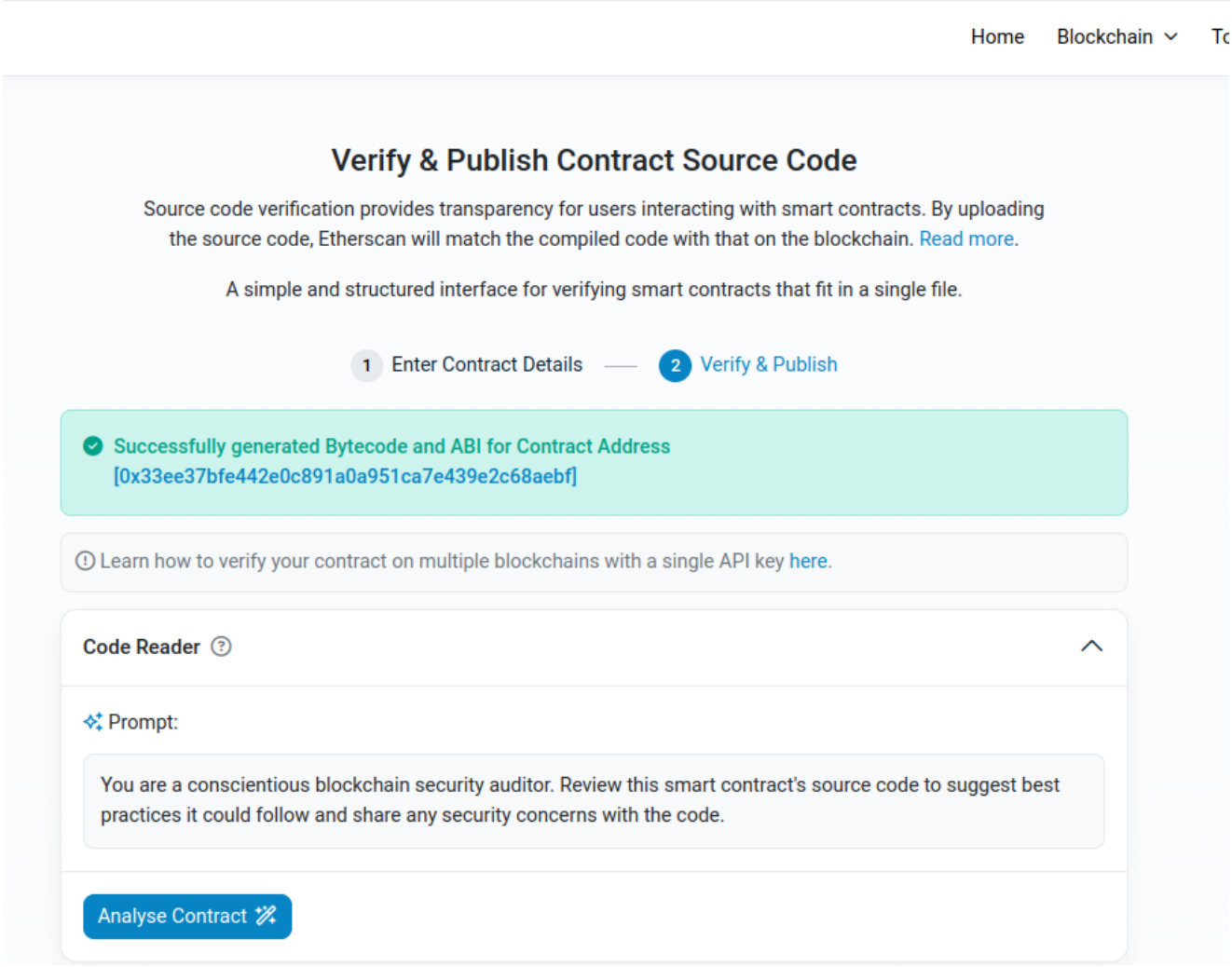
URL Contrato:
https://sepolia.etherscan.io/address/0x33ee37bfe442e0c891a0a951ca7e439e2c68aebf

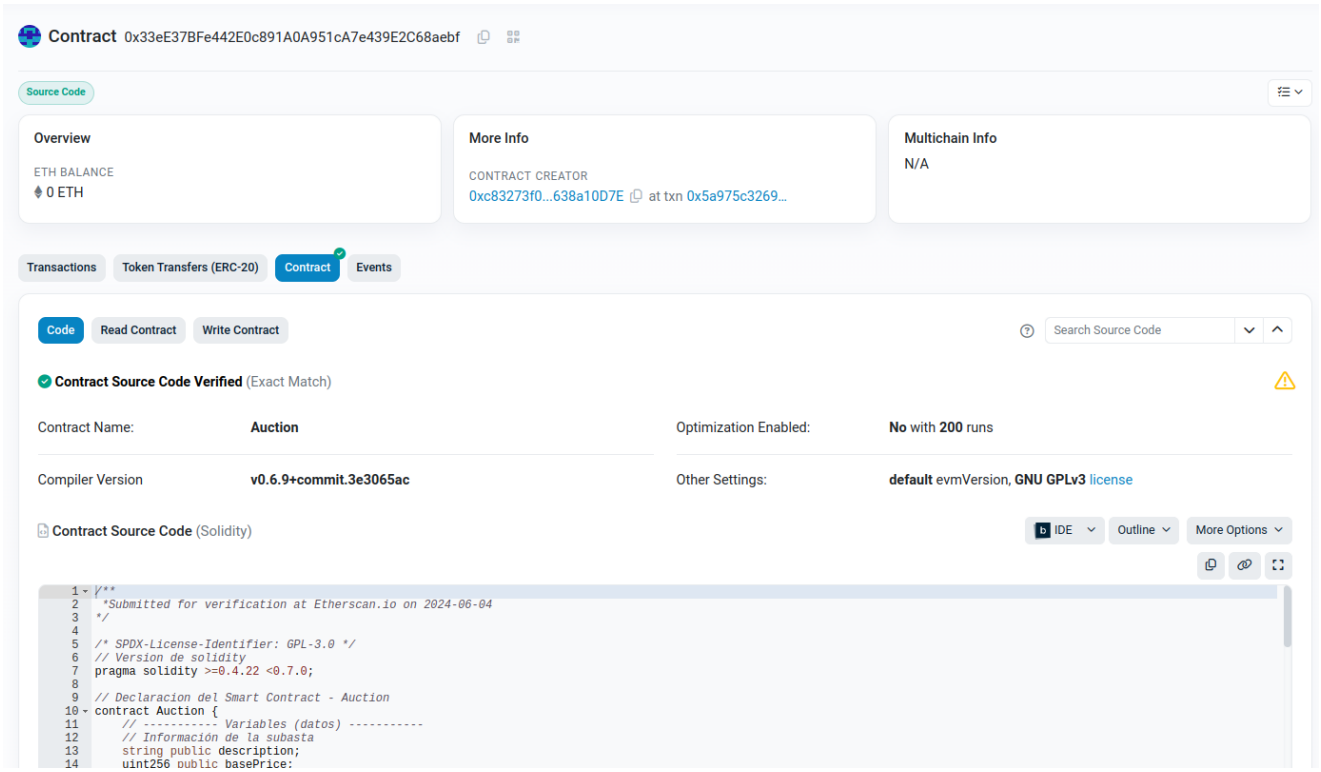
Verificación y Publicar contrato:



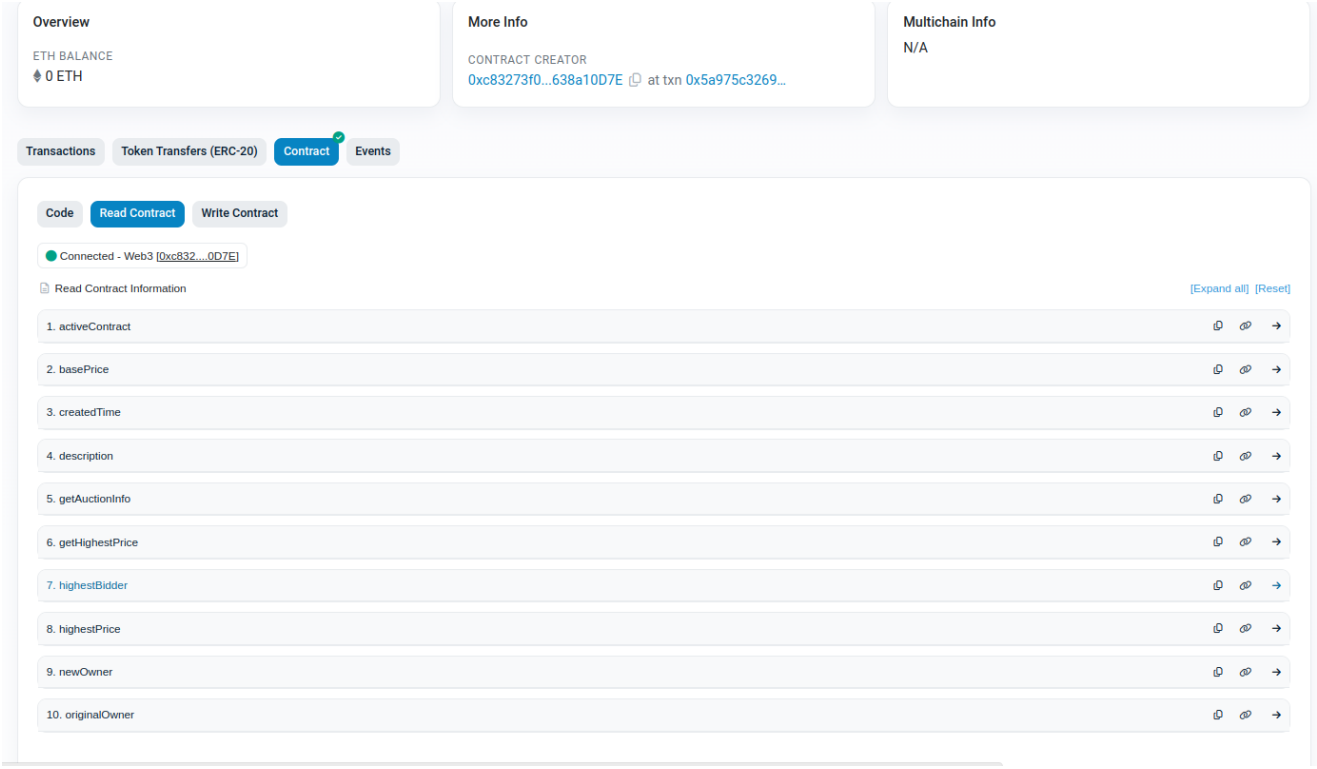


Resultado verificación y publicación

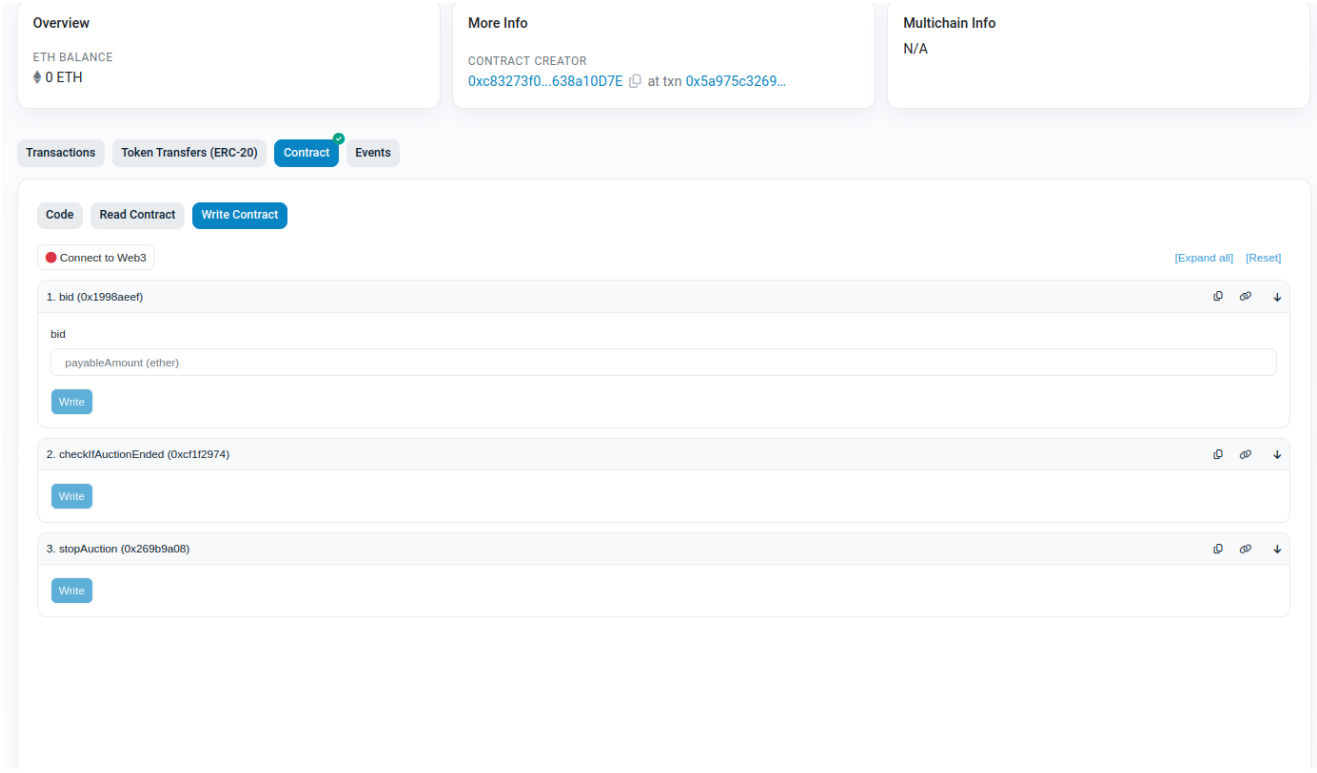

Home
Blockchain
Verify & Publish Contract Source Code
Source code verification provides transparency for users interacting with smart contracts. By uploading the source code, Etherscan will match the compiled code with that on the blockchain. Read more.
A simple and structured interface for verifying 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 0x33eE37BFe442E0c891A0A951cA7e439E2C68aebf
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
/**
*Submitted for verification at Etherscan.io on 2024-06-04
*/
/* SPDX-License-Identifier: GPL-3.0 */
// Version de solidity
pragma solidity >=0.4.22 <0.7.0;
// Declaracion del Smart Contract - Auction
contract Auction {
// ---------- Variables (datos) ----------
// Información de la subasta
string public description;
uint256 public basePrice;

Metodos de consultas READ



Metodos de Escritura : Write



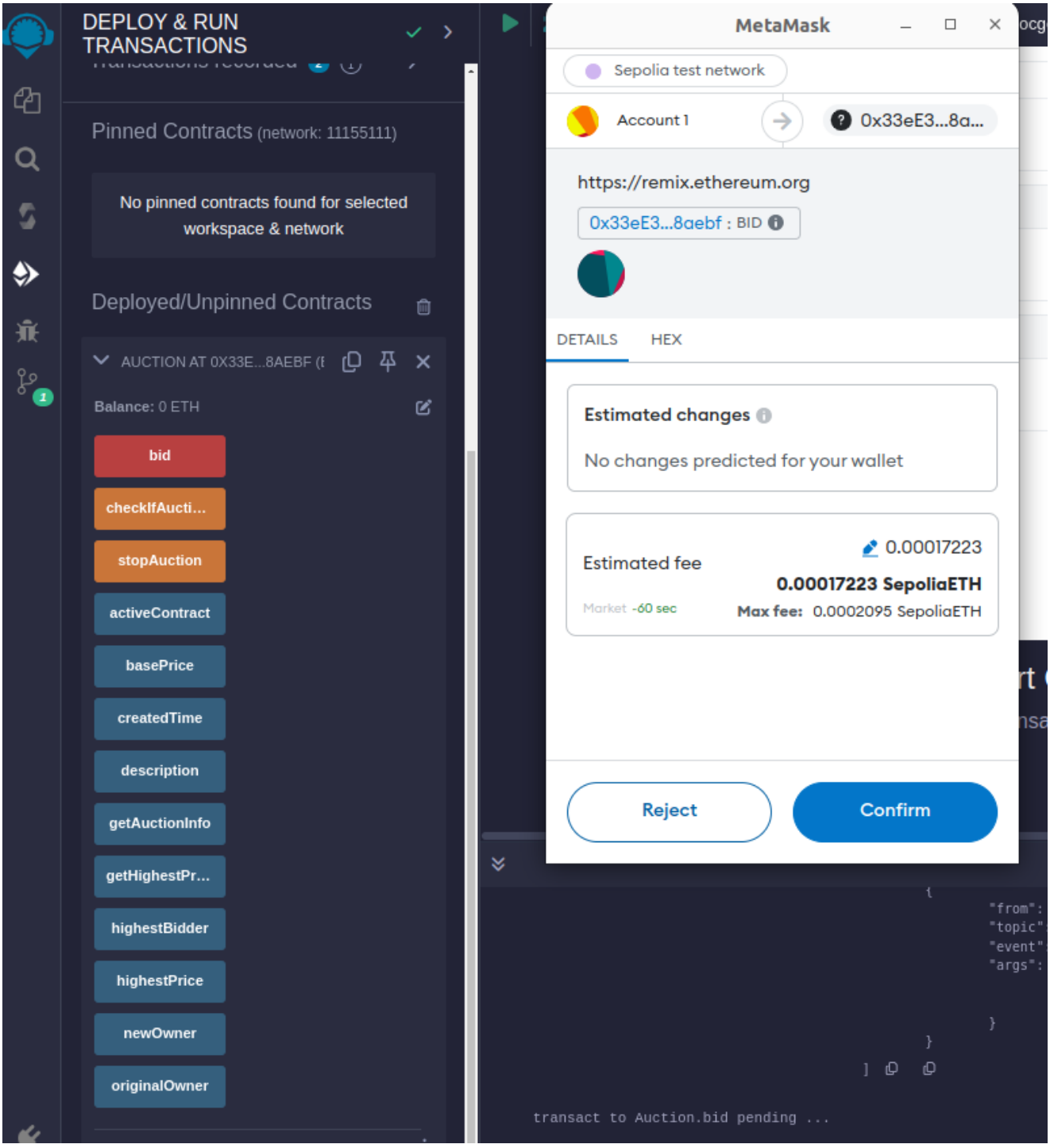
6 Envío de transacciones al Smart Contract con Remix IDE

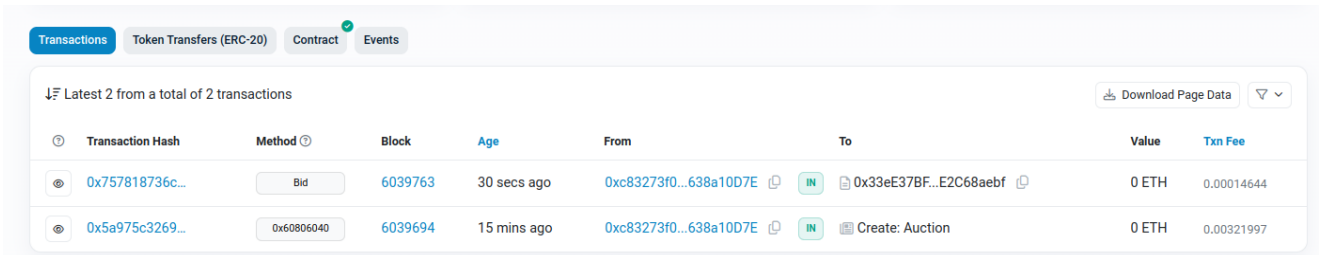
Para utilizar el smart contract hay que generar transacciones, en este caso realizarás con tu cuenta una transacción de puja a través del método bid.

Transacciones del Contrato creado:

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

Ejecuta metodo Bid:





From: 0xc83273f025ecEd0317f52DfE26d95C4638a10D7E

To: 0x33eE37BFe442E0c891A0A951cA7e439E2C68aebf

Value: 0.0000000000003 ETH ($0.00)

Transaction Fee: 0.0002456555587375 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: 0.0000444654753318 45 ETH ($0.00)

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

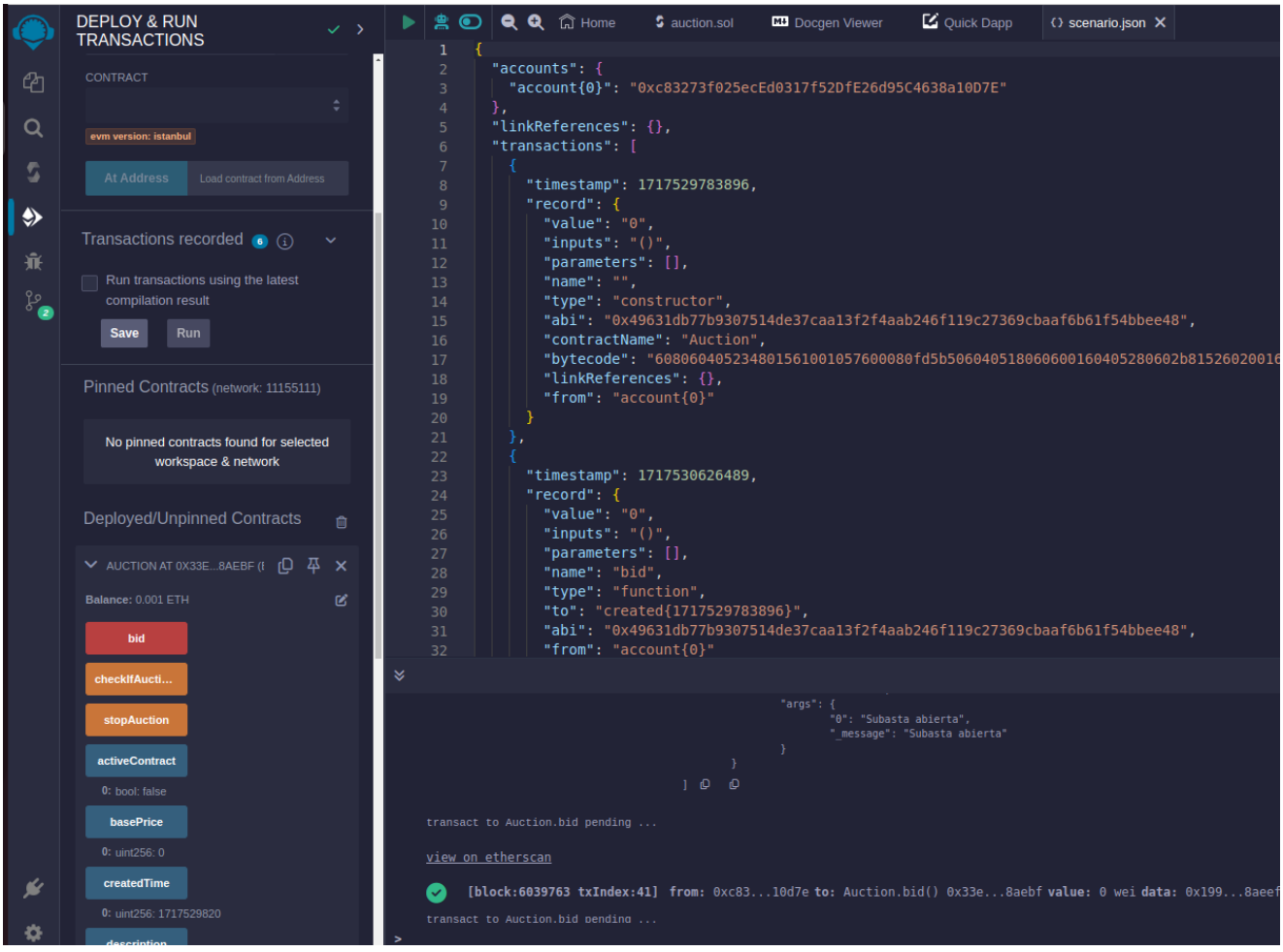
Input Data:

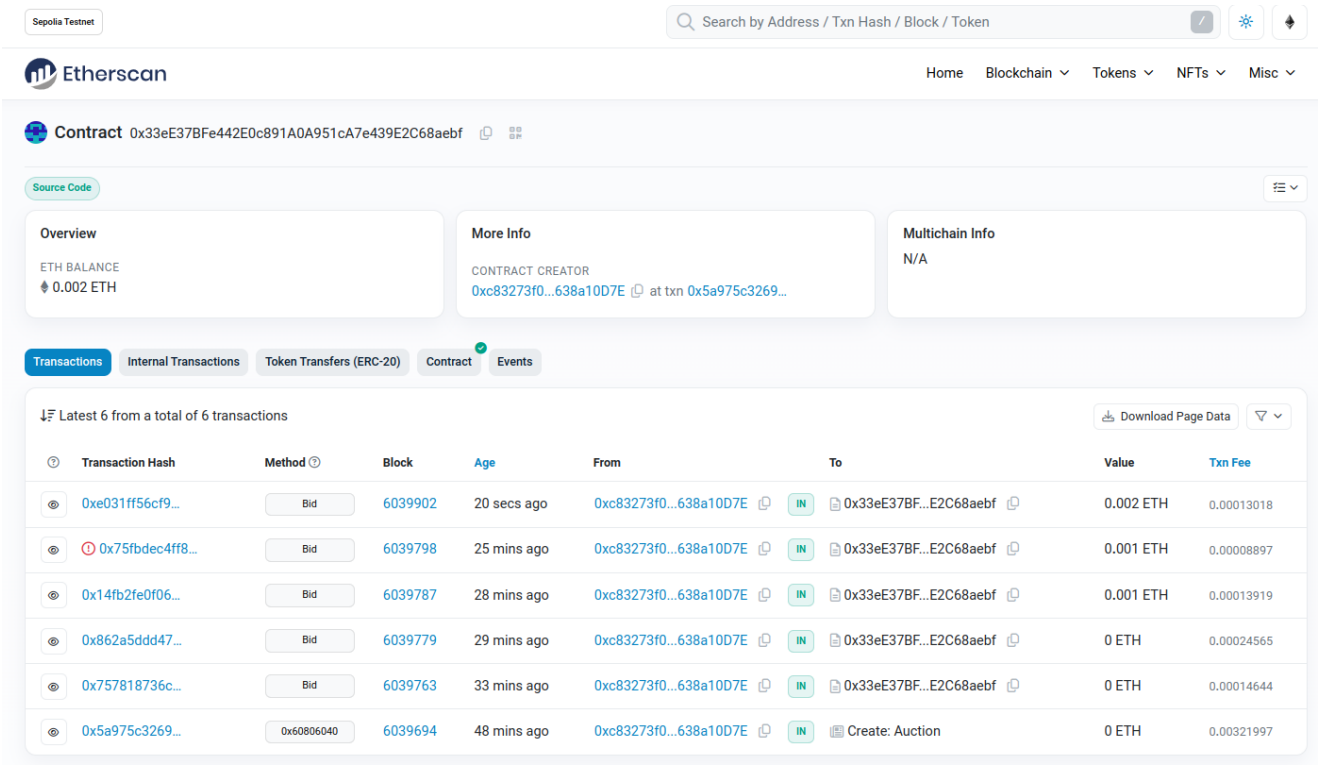
```
Function: bid()

MethodID: 0x1998aeef
```

View Input As

More Details: — Click to show less




Sepolia Testnet
Search by Address / Txn Hash / Block / Token
Etherscan
Home
Blockchain
Tokens
NFTs
Misc
Contract 0x33eE37BFe442E0c891A0A951cA7e439E2C68aebf
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 IN 0x33eE37BF...E2C68aebf 0.002 ETH 0.00013018
0x75fbdec4ff8... Bid 6039798 25 mins ago 0xc83273f0...638a10D7E IN 0x33eE37BF...E2C68aebf 0.001 ETH 0.00008897
0x14fb2fe0f06... Bid 6039787 28 mins ago 0xc83273f0...638a10D7E IN 0x33eE37BF...E2C68aebf 0.001 ETH 0.00013919
0x862a5ddd47... Bid 6039779 29 mins ago 0xc83273f0...638a10D7E IN 0x33eE37BF...E2C68aebf 0 ETH 0.00024565
0x757818736c... Bid 6039763 33 mins ago 0xc83273f0...638a10D7E IN 0x33eE37BF...E2C68aebf 0 ETH 0.00014644
0x5a975c3269... 0x60806040 6039694 48 mins ago 0xc83273f0...638a10D7E IN Create: Auction 0 ETH 0.00321997