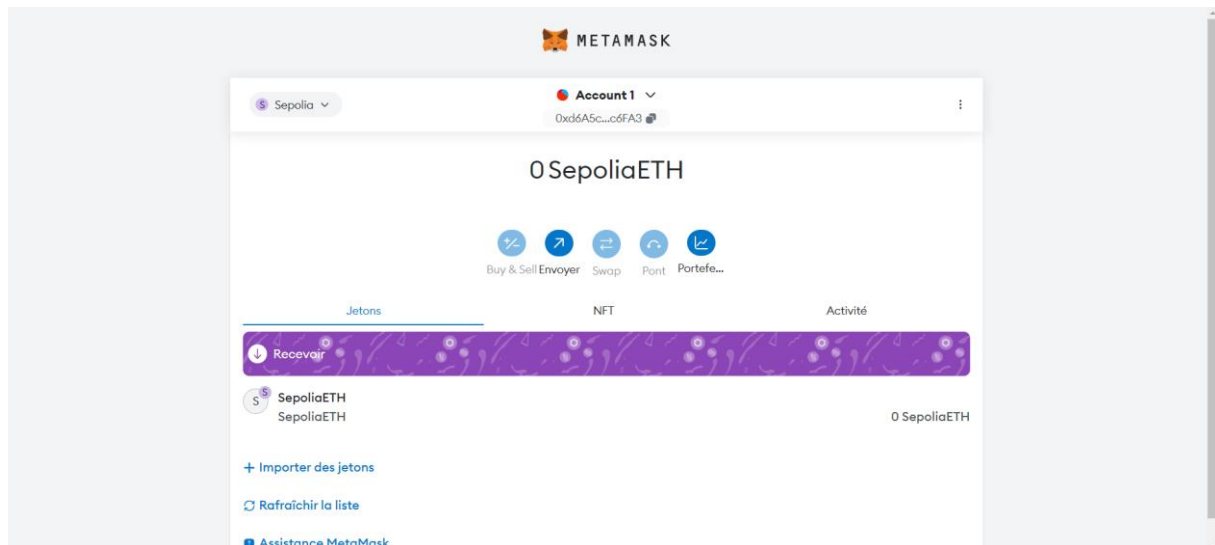


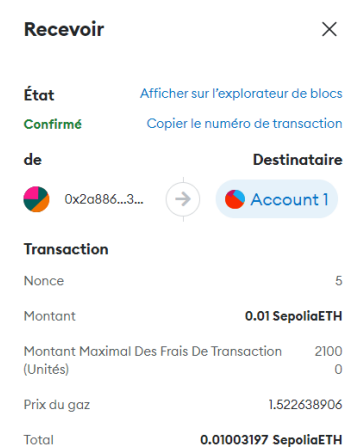
TP Smart contract










e. Envoyer l'identifiant public « clé publique » de votre portefeuille sur votre compte Metamask en communiquant à votre professeur votre portefeuille dans votre rapport.

0xd6A5c01C651d48A0026CFB3225179aEa5Cdc6FA3

g. Consulter la transaction générée vers votre compte et prenez en compte les détails de cette dernière. Fournissez également les détails de la transaction



h. Consulter ensuite le numéro de Block de votre transaction. Fournissez également les détails de la transaction

⑦ Block Height:	5702071 < >
⑦ Status:	Finalized
⑦ Timestamp:	⑦ 1 hr ago (Apr-15-2024 07:46:36 AM +UTC)
⑦ Proposed On:	Block proposed on slot 4786133, epoch 149566
⑦ Transactions:	102 transactions and 28 contract internal transactions in this block
⑦ Withdrawals:	16 withdrawals in this block
<hr/>	
⑦ Fee Recipient:	0x455E5AA18469bC6ccEF49594645666C587A3a71B  in 12 secs
⑦ Block Reward:	0.029805053409189903 ETH (0 + 0.030229200851855601 - 0.000424147442665698)
⑦ Total Difficulty:	17,000,018,015,853,232
⑦ Size:	211,514 bytes
<hr/>	
⑦ Gas Used:	18,735,333(62.45%)  +25% Gas Target
⑦ Gas Limit:	30,000,000
⑦ Base Fee Per Gas:	0.00000000022638906 ETH (0.022638906 Gwei)
⑦ Burnt Fees:	 0.000424147442665698 ETH
⑦ Extra Data:	—   geth  go1.21.7  linux (Hex:0xd883010d0e846765746888676f312e32312e37856c696e7578)

k. Récupérer le code source de votre premier smart contract :

https://github.com/cozcan/TP_Election

Mon fork est à l'adresse :

https://github.com/Yann-Desagnat/TP_Smart_Contract_Yann_Desagnat

m. Compiler votre smart contract « Election » et fournissez l'ABI ainsi que le Byte code du contrat.

ABI :

```
[
  {
    "constant": false,
    "inputs": [
      {
        "name": "_candidateId",
        "type": "uint256"
      }
    ],
    "name": "vote",
    "outputs": [],
    "payable": false,
    "stateMutability": "nonpayable",
    "type": "function"
  },
  {
    "constant": true,
    "inputs": [],
```

```

        "name": "candidatesCount",
        "outputs": [
            {
                "name": "",
                "type": "uint256"
            }
        ],
        "payable": false,
        "stateMutability": "view",
        "type": "function"
    },
    {
        "constant": true,
        "inputs": [
            {
                "name": "",
                "type": "uint256"
            }
        ],
        "name": "candidates",
        "outputs": [
            {
                "name": "id",
                "type": "uint256"
            },
            {
                "name": "name",
                "type": "string"
            },
            {
                "name": "voteCount",
                "type": "uint256"
            }
        ],
        "payable": false,
        "stateMutability": "view",
        "type": "function"
    },
    {
        "constant": false,
        "inputs": [
            {
                "name": "_name",
                "type": "string"
            }
        ],
        "name": "addCandidate",
        "outputs": [],
        "payable": false,
        "stateMutability": "nonpayable",
    }

```

```

        "type": "function"
    },
    {
        "constant": true,
        "inputs": [],
        "name": "owner",
        "outputs": [
            {
                "name": "",
                "type": "address"
            }
        ],
        "payable": false,
        "stateMutability": "view",
        "type": "function"
    },
    {
        "constant": true,
        "inputs": [
            {
                "name": "",
                "type": "address"
            }
        ],
        "name": "voters",
        "outputs": [
            {
                "name": "",
                "type": "bool"
            }
        ],
        "payable": false,
        "stateMutability": "view",
        "type": "function"
    },
    {
        "constant": false,
        "inputs": [
            {
                "name": "newOwner",
                "type": "address"
            }
        ],
        "name": "transferOwnership",
        "outputs": [],
        "payable": false,
        "stateMutability": "nonpayable",
        "type": "function"
    },
    {

```

```

        "anonymous": false,
        "inputs": [
            {
                "indexed": true,
                "name": "_candidateId",
                "type": "uint256"
            }
        ],
        "name": "votedEvent",
        "type": "event"
    },
    {
        "anonymous": false,
        "inputs": [
            {
                "indexed": true,
                "name": "previousOwner",
                "type": "address"
            },
            {
                "indexed": true,
                "name": "newOwner",
                "type": "address"
            }
        ],
        "name": "OwnershipTransferred",
        "type": "event"
    }
]

```

Byte code :

```

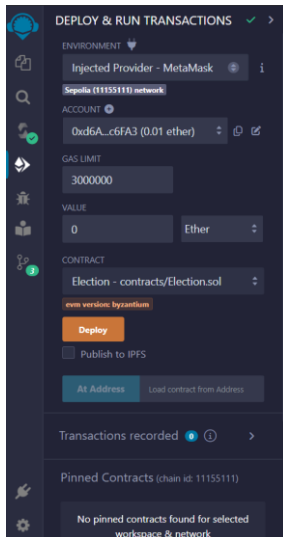
6080604052336000806101000a81548173ffffffffffffffffffffffffffffffff021916908373fff
ffffffffffffffffffffffffffffffff160217905550610897806100536000396000f3006080604052
60043610610083576000357c0100000000000000000000000000000000000000000000000000
000000000000900463ffffffff1680630121b93f146100885780632d35a8a2146100b55780
633477ee2e146100e0578063462e91ec146101945780638da5cb5b146101fd578063a3e
c138d14610254578063f2fde38b146102af575b600080fd5b34801561009457600080fd5
b506100b3600480360381019080803590602001909291905050506102f2565b005b348
0156100c157600080fd5b506100ca610415565b60405180828152602001915050604051
80910390f35b3480156100ec57600080fd5b5061010b600480360381019080803590602
0019092919050505061041b565b6040518084815260200180602001838152602001828
103825284818151815260200191508051906020019080838360005b838110156101575
7808201518184015260208101905061013c565b50505050905090810190601f16801561
01845780820380516001836020036101000a031916815260200191505b509450505050
5060405180910390f35b3480156101a057600080fd5b506101fb6004803603810190808
03590602001908201803590602001908080601f01602080910402602001604051908101

```

6040528093929190818152602001838380828437820191505050505050919291929050
50506104dd565b005b34801561020957600080fd5b5061021261055a565b6040518082
73ff1673ffffffffffffffffffffffffffffffff1681526020019150506
0405180910390f35b34801561026057600080fd5b506102956004803603810190808035
73ff16906020019092919050505061057f565b604051808215
151515815260200191505060405180910390f35b3480156102bb57600080fd5b506102f
0600480360381019080803573ffffffffffffffffffffffffffffffff16906020019092919050505
061059f565b005b600160003373ffffffffffffffffffffffffffffffff1673ffffffffffffffffffffffff
ffffffff16815260200190815260200160002060009054906101000a900460ff161515156
1034b57600080fd5b60008111801561035d57506003548111155b15156103685760008
0fd5b60018060003373ffffffffffffffffffffffffffffffff1673ffffffffffffffffffffffff168
15260200190815260200160002060006101000a81548160ff0219169083151502179055
5060026000828152602001908152602001600020600201600081548092919060010191
90505550807fff3c900d938d21d0990d786e819f29b8d05c1ef587b462b939609625b68
4b1660405160405180910390a250565b60035481565b60026020528060005260406000
2060009150905080600001549080600101805460018160011615610100020316600290
0480601f016020809104026020016040519081016040528092919081815260200182805
4600181600116156101000203166002900480156104cd5780601f106104a25761010080
83540402835291602001916104cd565b820191906000526020600020905b8154815290
600101906020018083116104b057829003601f168201915b50505050509080600201549
05083565b6003600081548092919060010191905055506060604051908101604052806
0035481526020018281526020016000815250600260006003548152602001908152602
0016000206000820151816000015560208201518160010190805190602001906105499
291906107c6565b506040820151816002015590505050565b6000809054906101000a9
00473ffffffffffffffffffffffffffffffff1681565b60016020528060005260406000206000915
054906101000a900460ff1681565b6000809054906101000a900473ffffffffffffffffffffff
ffffffff1673ffffffffffffffffffffffffffffffff163373ffffffffffffffffffffffff161415156
10663576040517f08c379a00
0000000081526004018080602001828103825260188152602001807f4e6f74206175746
86f72697a6564206f7065726174696f6e000000000000000081525060200191505060405
180910390fd5b600073ffffffffffffffffffffffffffffffff168173ffffffffffffffffffffff
614151515610708576040517f08c379a00000000000000000000000000000000000000
00000000000000000081526004018080602001828103825260198152602001807f41646
4726573732073686f756c646e2774206265207a65726f0000000000000000815250602001
91505060405180910390fd5b8073ffffffffffffffffffffffffffffffff16600080905490610100
0a900473ffffffffffffffffffffffffffffffff1673ffffffffffffffffffffffff167f8be0079c53
1659141344cd1fd0a4f28419497f9722a3daafe3b4186f6b6457e0604051604051809103
90a3806000806101000a81548173ffffffffffffffffffffffffffffffff021916908373ffffff
ffffffff16021790555050565b82805460018160011615610100020316600290
0490600052602060002090601f016020900481019282601f1061080757805160ff191683
8001178555610835565b82800160010185558215610835579182015b82811115610834

578251825591602001919060010190610819565b5b5090506108429190610846565b50
90565b61086891905b8082111561086457600081600090555060010161084c565b5090
565b905600a165627a7a72305820c2b1daaf1ae81292340b32ac261cca45ecfd2e95a4a
d3032438fcb078984ae80029

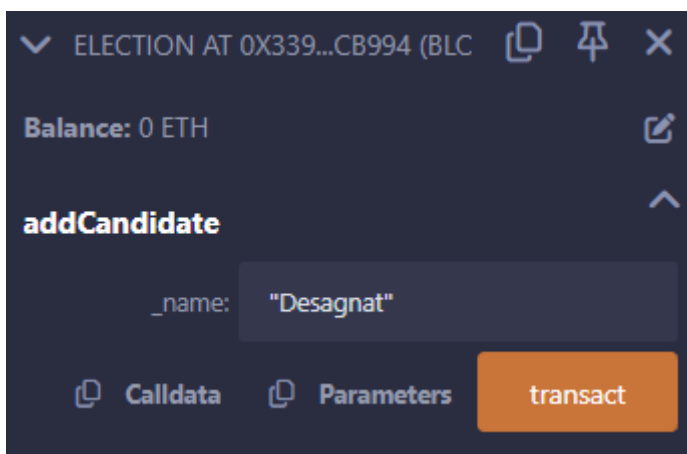
n. Déployer le smart contract « Election.sol » sur le réseau et fournissez les détails de la transaction. Assurez vous que vous n'êtes pas configuré en réseau local sur remix mais bien synchronisé avec votre réseau Metamask.



Quelle est l'adresse public de votre smart contract ?

0xd6A5c01C651d48A0026CFB3225179aEa5Cdc6FA3

o. Interagissez avec votre smart contract après l'avoir déployé en ajoutant le nom du premier candidat qui sera votre « Nom de famille »



p. Générer la transaction ensuite l'ajout du premier candidat et fournissez les détails de la transaction

0x3398d45343ca49B2B91c1CCA64adE46315Fcb994

+

Log d'activité

État

Afficher sur l'explorateur de blocs

Confirmé

Copier le numéro de transaction

de

Destinataire

0xd6A5c...c...

→

?

0x3398...

Transaction

Nonce

1

Montant

-0 SepoliaETH

Montant Maximal Des Frais De Transaction (Unités)

92245

Gaz Utilisé (Unités)

91300

Frais de base (GWEI)

0.058642776

Frais de priorité (GWEI)

1.5

Total des frais de transaction

0.000142 SepoliaETH

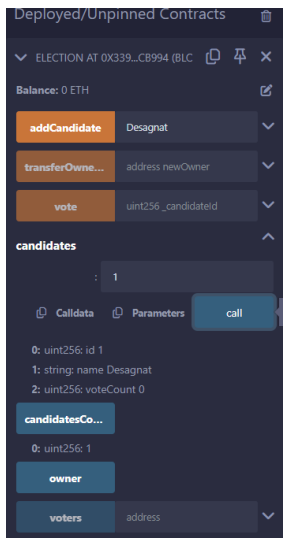
Frais maximaux par unité de gaz

0.000000002 SepoliaETH

Total

0.0001423 SepoliaETH

q. Consulter la valeur de votre CandidateID à l'aide de Remix et fournissez le détail.



r. Ajouter un second candidat de votre choix dans le smart contract et fournissez le détail de la transaction

0xd6A5c01C651d48A0026CFB3225179aEa5Cdc6FA3

Add Candidate

×

État

Afficher sur l'explorateur de blocs

Confirmé

Copier le numéro de transaction

de

0xd6A5c...c...

→

Destinataire

?

0x3398...

Transaction

Nonce	2
Montant	-0 SepoliaETH
Montant Maximal Des Frais De Transaction (Unités)	7505 3
Gaz Utilisé (Unités)	74176
Frais de base (GWEI)	0.052755889
Frais de priorité (GWEI)	1.5
Total des frais de transaction	0.000115 SepoliaETH
Frais maximaux par unité de gaz	0.000000002 SepoliaETH
Total	0.00011518 SepoliaETH

+

Log d'activité

s. Consulter la valeur du second CandidateID à l'aide de Remix et fournissez le détail.

t. Fournissez l'adresse du propriétaire du contract

0xd6A5c01C651d48A0026CFB3225179aEa5Cdc6FA3

u. Réaliser le premier vote pour l'un des candidats à travers Remix et fournissez le détail de la transaction

Vote

État

Afficher sur l'explorateur de blocs

Confirmé

Copier le numéro de transaction

de

0xd6A5c...

→

Destinataire

Desagnat

Transaction

Nonce	3
Montant	-0 SepoliaETH
Montant Maximal Des Frais De Transaction (Unités)	70299
Gaz Utilisé (Unités)	69441
Frais de base (GWEI)	0.046357589
Frais de priorité (GWEI)	1.5
Total des frais de transaction	0.000107 SepoliaETH
Frais maximaux par unité de gaz	0.000000002 SepoliaETH
Total	0.00010738 SepoliaETH

+

Log d'activité

v. Vérifier que votre vote a été prise en compte en fournissant la donnée du nombre de vote pour votre candidat.

candidates

"1"

Calldata

Parameters

call

0: uint256: id 1

1: string: name Desagnat

2: uint256: voteCount 1

w. Demander à votre camarade proche de vous d'intégrer avec votre contrat et de voter pour l'un des deux candidats en lui fournissant l'adresse publique de votre smart contract.

At Address

0x1a0797588d61D02A72330A6

ELECTION AT 0X1A0...EFF0E (BLO)

Balance: 0 ETH

addCandidate

string_name

transferOwne...

address newOwner

vote

..candidates

"1"

Calldata

Parameters

transact

candidates

uint256

candidatesCo...

owner

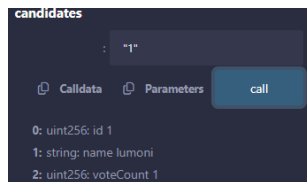
voters

address

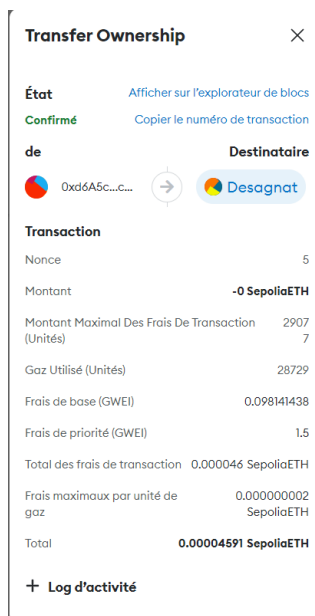
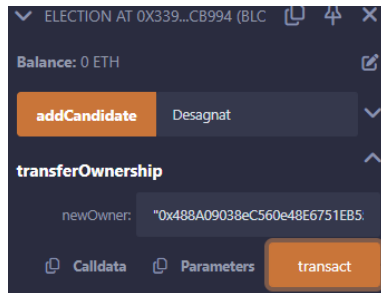
Low level interactions

CALLDATA

Transact



x. Réaliser ensuite le transfert de la propriété à votre camarade en lui demandant son adresse publique.



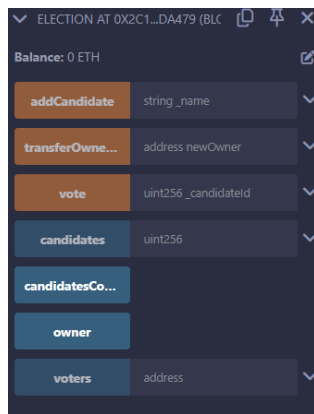
y. A votre avis comment pourrions nous sécurisé l'appel de la fonction addCandidate afin que vous soyez le seul à pouvoir gérer les candidats ?

Il suffit d'ajouter le modifier « onlyOwner » créé dans le fichier Ownable.sol à la fonction addCandidate initialisée dans le fichier Election.sol.

z. Modifier le code afin de faire en sorte que vous soyez uniquement le seul à pouvoir ajouter un nouveau candidat.

Compile and deploy new contract

0x2c195E3C8aADaC4848752A1ac18C2734317DA479



When trying to add a new candidate a message box appears

