

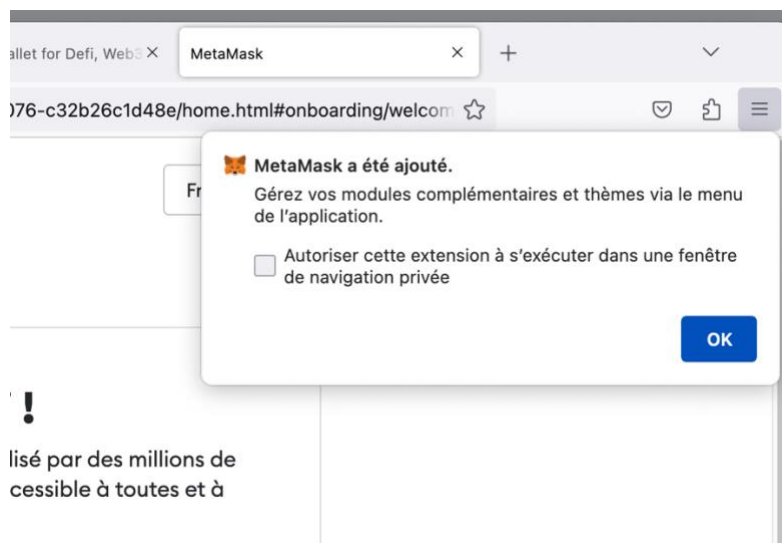
# GRIGRA Adam A2MSI

## TRAVAUX PRATIQUE :

### Développer, Deployer et Interagir avec un contrat intelligent sur Ethereum

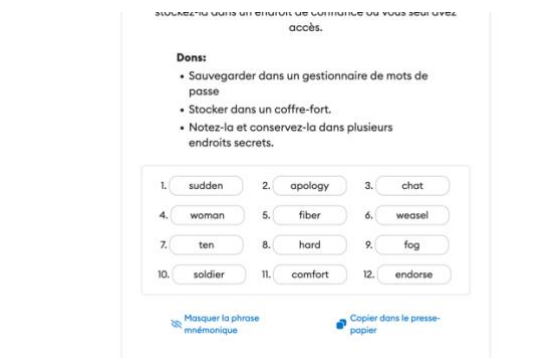
a)

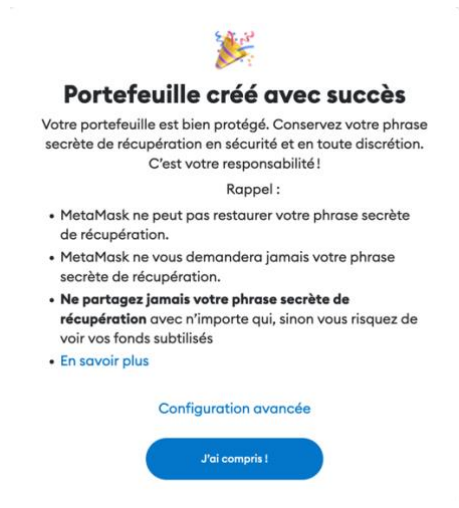
J'ai Installation Metamask via Firefox :



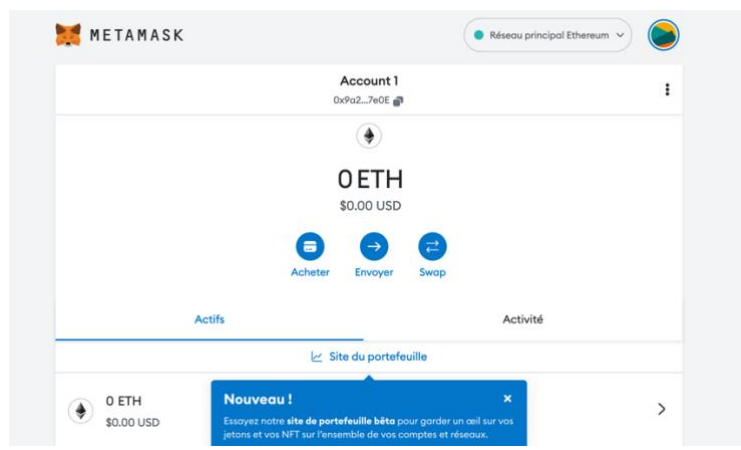
b)

J'ai suivi les étapes afin de générer mon portefeuille :

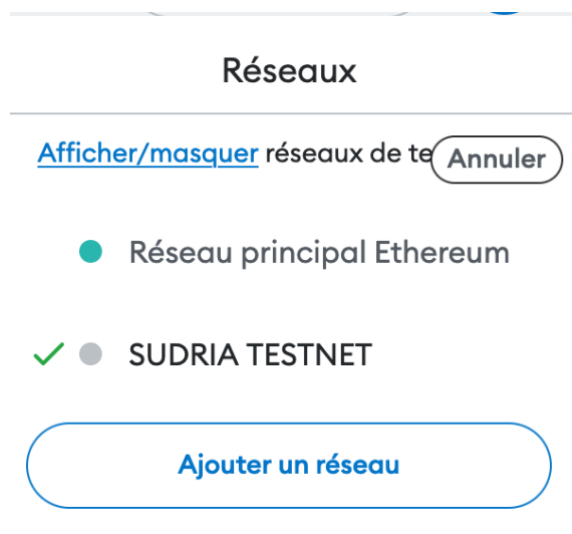




c) Nous voyons que mon compte wallet est bien créé :

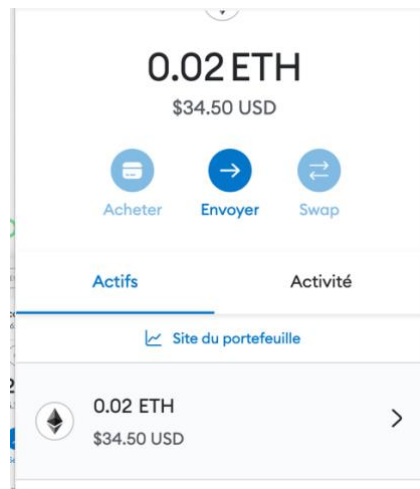


d) J'ai ensuite ajouté un réseau :

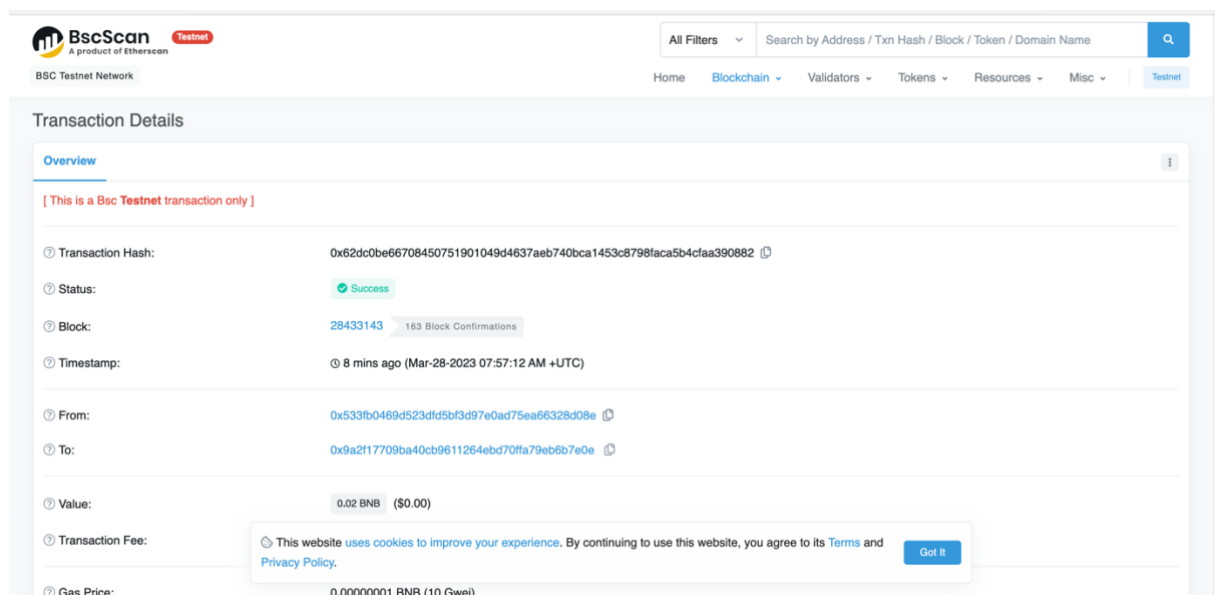


e) Portefeuille : 0x9a2f17709BA40cb9611264EbD70FFA79Eb6B7e0E mail envoyé au professeur M. Ozcan afin de recevoir mes ETH.

Transaction générée :



f) Je peux voir que du solde a été ajouté à mon portefeuille, voici le détail de la transaction :




g) Voici le détail du contenu se trouvant dans le bloc :


Overview	
[ This is a Bsc Testnet block only ]	
⑦ Block Height:	28433143 < >
⑦ Timestamp:	⌚ 9 mins ago (Mar-28-2023 07:57:12 AM +UTC)
⑦ Transactions:	10 transactions and 4 contract internal transactions in this block
⑦ Validated by:	0xa2959d3f95eae5dc7d70144ce1b73b403b7eb6e0 in 3 secs
⑦ Block Reward:	0.00305641 BNB
⑦ Difficulty:	2
⑦ Total Difficulty:	56,690,371
⑦ Size:	2,515 bytes
⑦ Gas Used:	297,119 (0.59%)
⑦ Fee Burnt:	🔥 0.000305641 BNB <a href="#">🔗</a>
⑦ Extra Data:	<div> Hex:  0xd883010114846765746888676f312e31392e36856c696e75780000008279af9afcb00691b247632784fb086719cb0775400cce7944124bc8f8fc9693de2af4be43257eee930f4289eef2c1e3b04815d878f9bef80ede95df7c9e0ee8de1818f400   ExtraVanity :  @geth@go1.19.6@Linux@y@  SignedData :  0xfcfh00601h247632784fb086719cfh0775400cce7044124bcrfrc0603de2af4bha43257eee930f4289eef2c1e3b04815d878f9bef80ede95df7c9e0ee8de1818f400 </div>
<a href="#">Click to see more</a> ↓	

J'ai envoyé 0,01 ETH à l'adresse : **0x533fB0469D523dfD5BF3D97e0Ad75ea66328D08E** :

h) Voici ma première transaction réalisée :



SUDRIA TESTNET




### Envoyer

✓

0x533fB0469D523dfD5BF3D97e0Ad75e  
a66328D08E

✕

Actif:

 ETH

Solde: 0.02 ETH

Montant:

0,01 ETH

\$17.26 USD

↕

Max.

Prix du gaz (GWEI)

10

Montant maximal des frais de transaction

21000

Carburant (estimé)

\$0.36

0.00021 ETH

Frais maximaux: 0.00021 ETH

Annuler

Suivant

File d'attente (1)



Envoyer

En attente · Vers : 0x533...d0...

-0.01 ETH

-\$17.26 USD

Accélérer

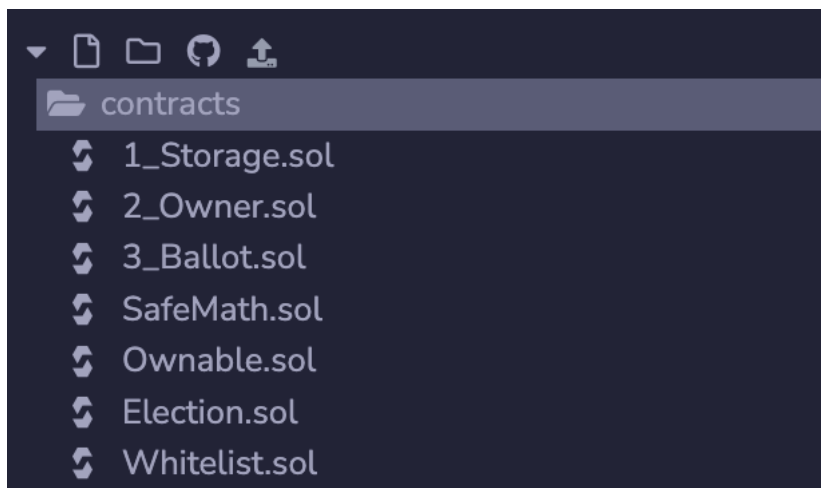
Annuler

l) Ouverture de l'IDE.

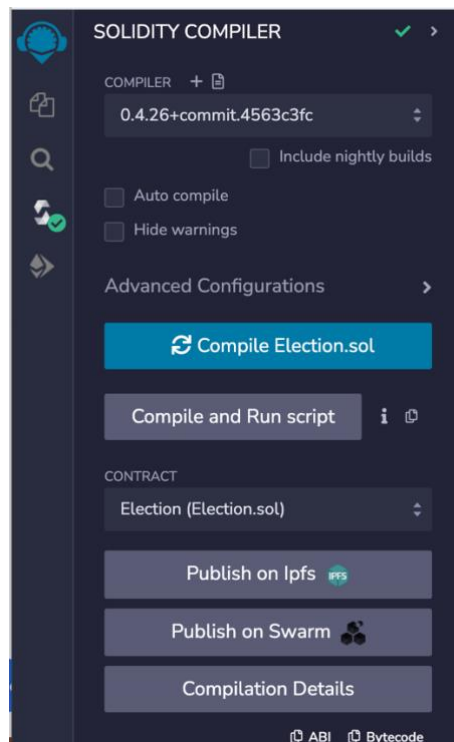
j) J'ai récupéré via le lien le zip contenant les contrats GitHub.



k) Les contrats ont été ajoutés dans l'environnement REMIX



l) On voit que le contrat Election.Sol compile bien :



Voici l'ABI :

```
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"
}
]

```

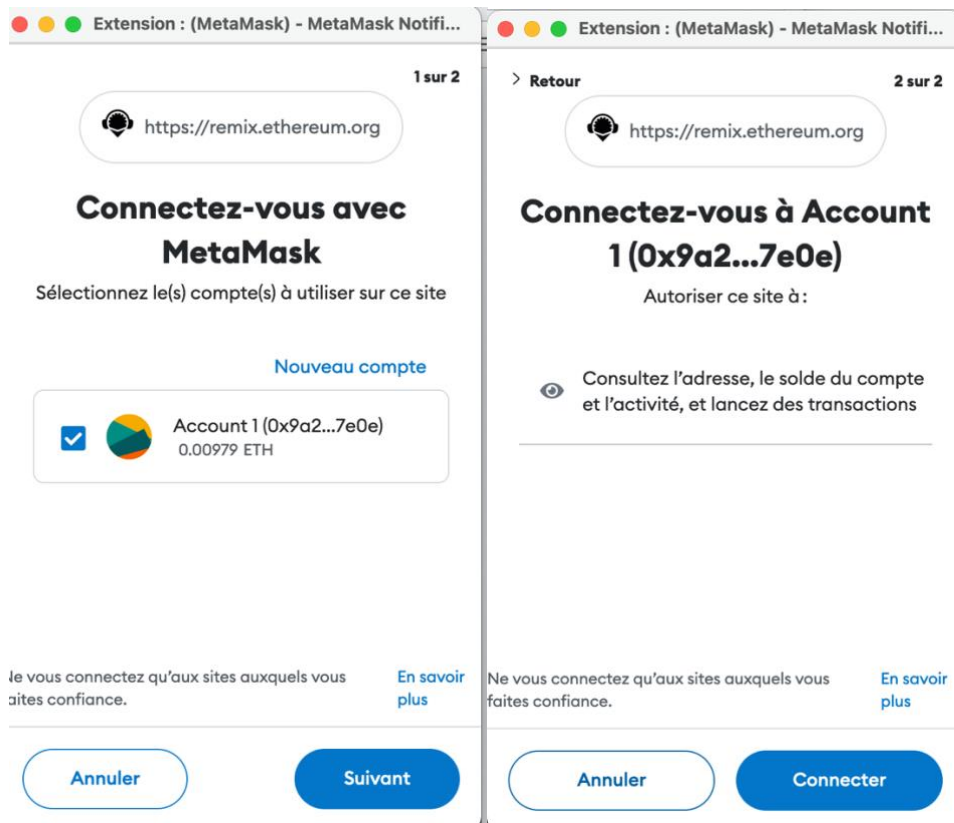
Voici le Bytecode :

```


6080604052336000806101000a81548173ffffffffffffffffffffffffffffffff021916908373ffffffffffffffffffffffffffffffff
ffffffff160217905550610897806100536000396000f300608060405260043610610083576000357c01000000000
00000000000000000000000000000000000000000000000000000000900463ffffffff1680630121b93f146100885780632d3
5a8a2146100b55780633477ee2e146100e0578063462e91ec146101945780638da5cb5b146101fd578063a3ec
138d14610254578063f2fde38b146102af575b600080fd5b34801561009457600080fd5b506100b3600480360
381019080803590602001909291905050506102f2565b005b3480156100c157600080fd5b506100ca61041556
5b6040518082815260200191505060405180910390f35b3480156100ec57600080fd5b5061010b60048036038
10190808035906020019092919050505061041b565b604051808481526020018060200183815260200182810
3825284818151815260200191508051906020019080838360005b83811015610157578082015181840152602
08101905061013c565b50505050905090810190601f1680156101845780820380516001836020036101000a03
1916815260200191505b5094505050505060405180910390f35b3480156101a057600080fd5b506101fb60048
0360381019080803590602001908201803590602001908080601f01602080910402602001604051908101604
052809392919081815260200183838082843782019150505050505091929192905050506104dd565b005b348
01561020957600080fd5b5061021261055a565b604051808273ffffffffffffffffffffffffffffffff1673fffffffffffff
ffffffffffffffffffffffff16815260200191505060405180910390f35b34801561026057600080fd5b5061029560048036
0381019080803573ffffffffffffffffffffffffffffffff16906020019092919050505061057f565b604051808215151
515815260200191505060405180910390f35b3480156102bb57600080fd5b506102f060048036038101908080
3573ffffffffffffffffffffffffffffffff16906020019092919050505061059f565b005b600160003373fffffffffffff
ffffffffffffffffffffffff1673ffffffffffffffffffffffffffffffff16815260200190815260200160002060009054906101000a9
00460ff1615151561034b57600080fd5b60008111801561035d57506003548111155b151561036857600080fd
5b60018060003373ffffffffffffffffffffffffffffffff1673ffffffffffffffffffffffffffffffff168152602001908152602
00160002060006101000a81548160ff0219169083151502179055506002600082815260200190815260200160
002060020160008154809291906001019190505550807ffff3c900d938d21d0990d786e819f29b8d05c1ef587b
462b939609625b684b1660405160405180910390a250565b60035481565b6002602052806000526040600020

```





Voici le détail de la transaction :

 [block:28434509 txIndex:10] from: 0x9a2...B7e0E to: Election.(constructor) value: 0 wei  
data: 0x608...80029 logs: 0 hash: 0x573...775a3

Overview

[ This is a Bsc Testnet transaction only ]

Transaction Hash:	0x7e77491b4413b32924a37d98e4ff01a7ecb9de2ed49a143957637dd3e650794
Status:	Success
Block:	28434509 49 Block Confirmations
Timestamp:	2 mins ago (Mar-28-2023 09:05:30 AM +UTC)
From:	0x9a2f17709ba40cb9611264ebd70ffa79eb6b7e0e
To:	[Contract 0x7ab1d0d176cf7a6bf4828de38950527851ee58f6 Created]
Value:	0 BNB (\$0.00)
Transaction Fee:	0.00548492 BNB (\$1.70)
Gas Price:	0.00000001 BNB (10 Gwei)

Click to see More

Lors du déploiement du contrat, les frais de transaction sont plus élevés car la création d'un nouveau contrat nécessite plus de ressources et de traitement par les mineurs du réseau.

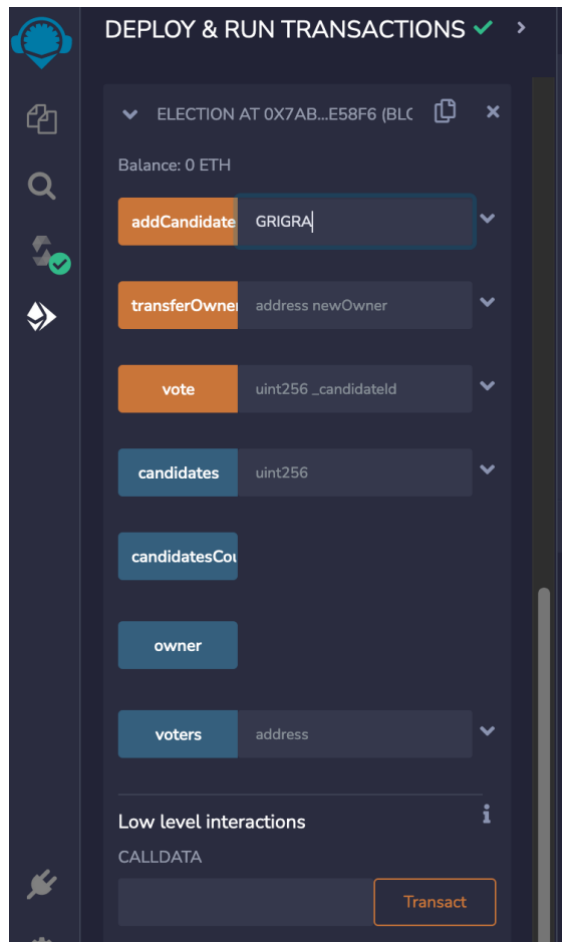
Pour l'envoi d'ETH à une adresse, les frais de transaction sont moins élevés car cette opération est moins complexe et nécessite moins de ressources.

*L'adresse public de mon smart contract est :*  
*0x7ab1d0d176cf7a6bf4828de38950527851ee58f6*

From:	0x9a2f17709ba40cb9611264ebd70ffa79eb6b7e0e
To:	[Contract 0x7ab1d0d176cf7a6bf4828de38950527851ee58f6 Created]

n)

Interaction avec mon smart contract en ayant ajouté le nom :



o)

Voici les transactions :

SUDRIA TESTNET

Account 1

0x7Ab...58f6

https://remix.ethereum.org

0x7Ab...58f6 : ADD CANDIDATE ⓘ

\$0.00

DÉTAILS

DONNÉES

HEX

MODIFIER

Frais de carburant estimés

\$1.52 0.000881 ETH

Site suggéré

Frais maximaux: 0.00088059 ETH

Total

\$1.52 0.00088059 ETH

Montant + frais de carburant

Montant maximal: 0.00088059 ETH

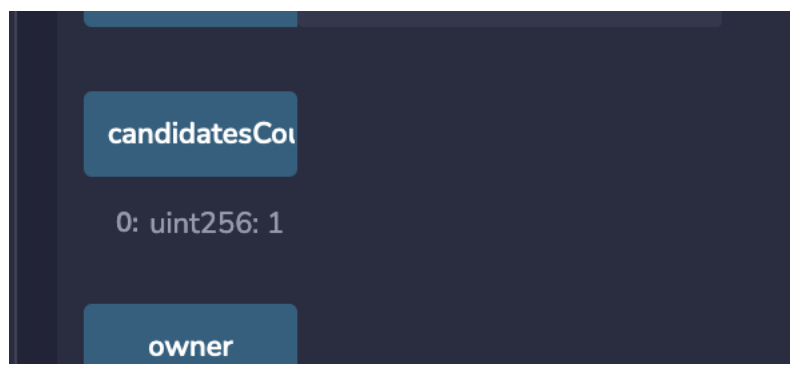
Rejeter

Confirmer

Overview	
[ This is a Bsc Testnet block only ]	
① Block Height:	28435173 < >
① Timestamp:	⌚ 56 secs ago (Mar-28-2023 09:38:42 AM +UTC)
① Transactions:	5 transactions and 60 contract internal transactions in this block
① Validated by:	0xa2959d3f95eae5dc7d70144ce1b73b403b7eb6e0 in 3 secs
① Block Reward:	0.00761765 BNB
① Difficulty:	2
① Total Difficulty:	56,694,431
① Size:	1,366 bytes
① Gas Used:	772,938 (1.55%)

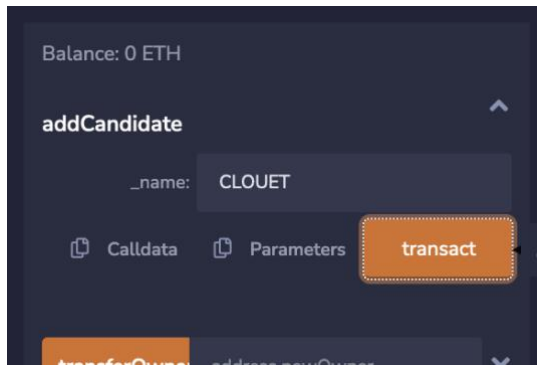
p)

Après avoir consulté la valeur, voici le détail :



q)

J'ai ajouté mon camarade CLOUET Baudouin :



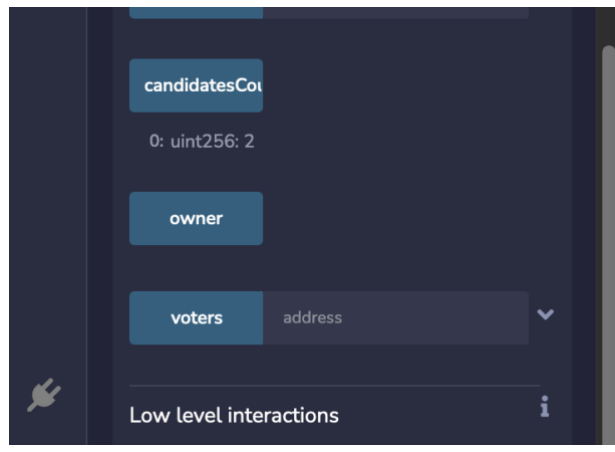
Voici le détail de la transaction :

Overview	
[ This is a Bsc Testnet block only ]	
Block Height:	28435262 < >
Timestamp:	23 secs ago (Mar-28-2023 09:43:09 AM +UTC)
Transactions:	10 transactions and 618 contract internal transactions in this block
Validated by:	0x96c5d20b2a975c050e4220be276ace4892f4b41a in 3 secs
Block Reward:	0.05358969000031932 BNB
Difficulty:	2
Total Difficulty:	56,694,609
Size:	6,861 bytes
Gas Used:	5,362,397 (10.77%)
Gas Limit:	49,803,929
Fee Burnt:	0.005358969000031932 BNB

r)

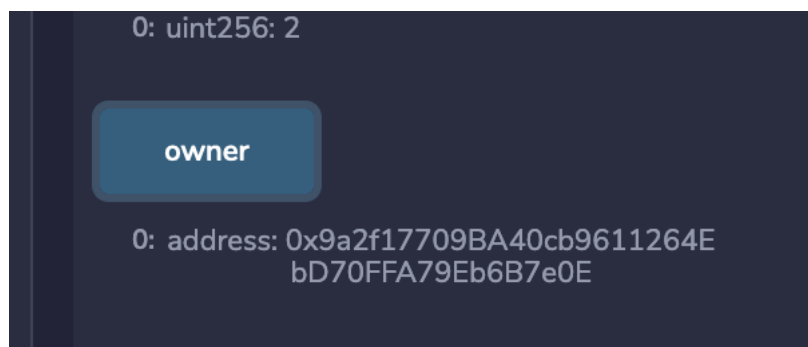
Nous pouvons voir la valeur du 2<sup>nd</sup> candidat :



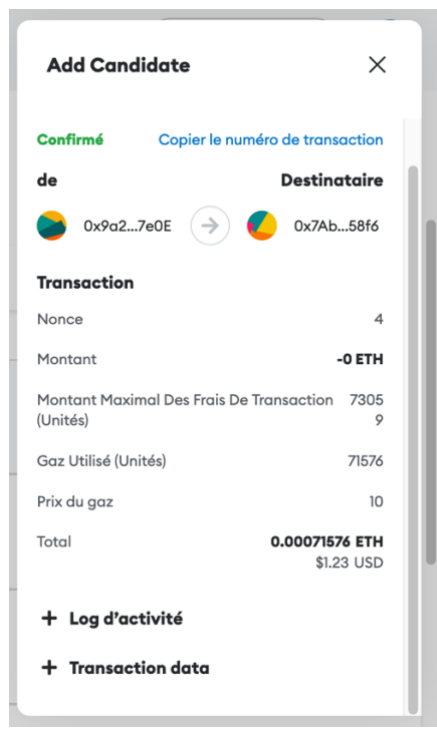


s)

On voit bien que l'adresse est la meme que la mienne

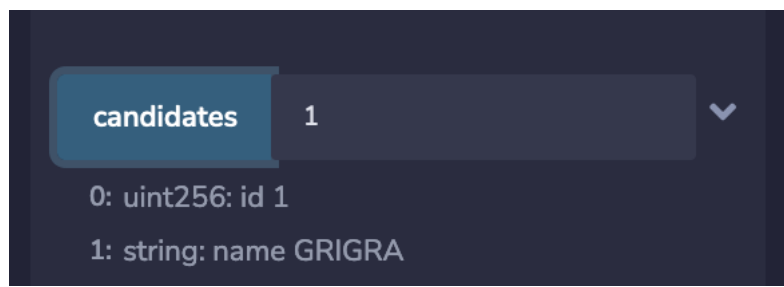


t)



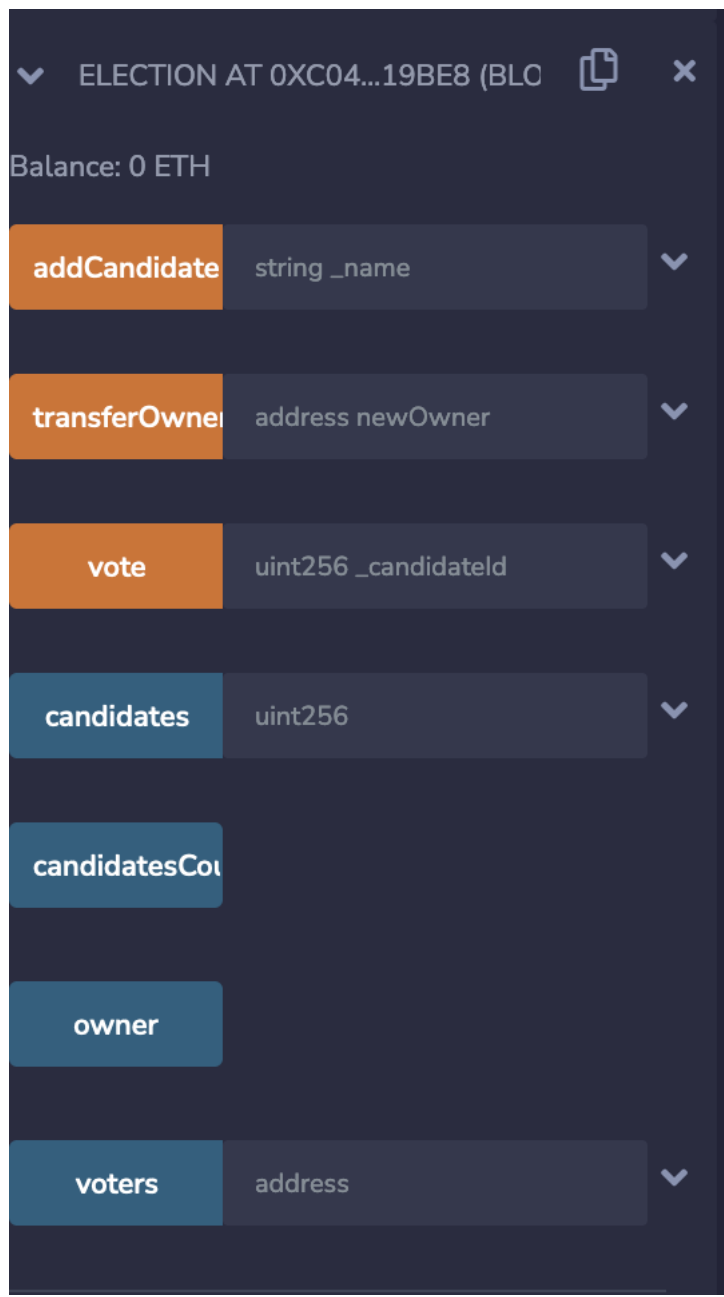
u)

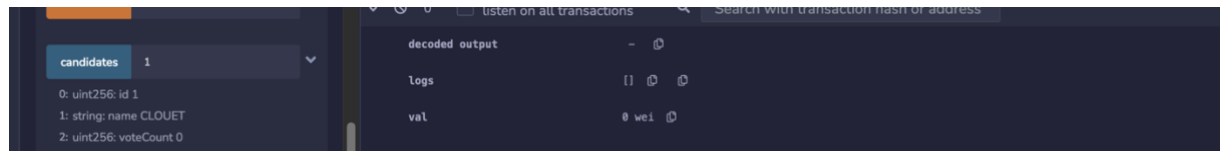
On voit via la capture que mon vote est pris en compte :



v)

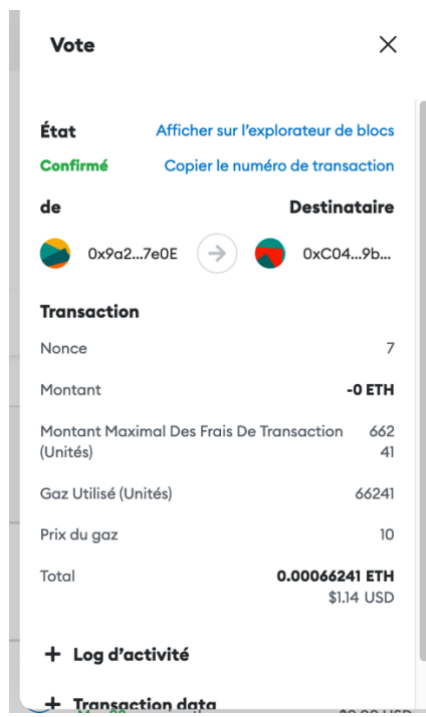
J'ai ajouté le contrat de Baudouin CLOUET, nous voyons que les interactions se font bien.





On voit que je peux communiquer avec le contrat de Baudouin CLOUET

On voit aussi que j'ai son vote via la transaction :



w)

Voici le changement d'owner :

État


Afficher sur l'explorateur de blocs

Confirmé


Copier le numéro de transaction

de

Destinataire


0x9a2...7e0E

→


0x7Ab...58f6

Transaction

Nonce	5
Montant	-0 ETH
Montant Maximal Des Frais De Transaction (Unités)	30929
Gaz Utilisé (Unités)	30929
Prix du gaz	10
Total	0.00030929 ETH \$0.53 USD

+ Log d'activité

+ Transaction data

x)

Je commence par ajouter une variable « admin » au début de mon contrat pour stocker l'identifiant de l'administrateur.

Ensuite j'initialise la variable « admin » dans le constructeur en définissant son identifiant que j'ai choisi.

Ensuite, je modifie la fonction « addCandidate » pour inclure une vérification d'authentification en ajoutant deux nouveaux paramètres à la fonction : un paramètre id pour l'identifiant et un paramètre « password » pour le mot de passe. Ensuite, j'ajouterai une instruction « require » au début de la fonction pour vérifier que l'identifiant et le mot de passe fournis sont corrects.

Enfin, je vais enregistrer les modifications apportées à votre contrat et le déployer à nouveau

y)

J'ai inscrit après la mention public : « only Owner »

```
event votedEvent ( uint indexed _candidateId);

function addCandidate (string memory _name) public only Owner {
    candidatesCount ++;
    candidates[candidatesCount] = Candidate(candidatesCount, _name, 0);
}

function vote (uint _candidateId) public {
    // require that they haven't voted before
```