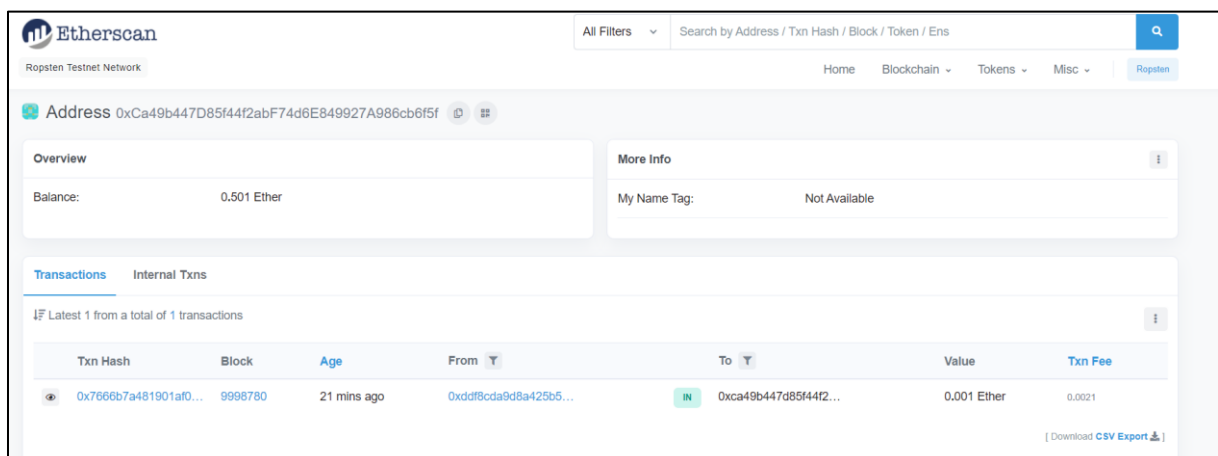
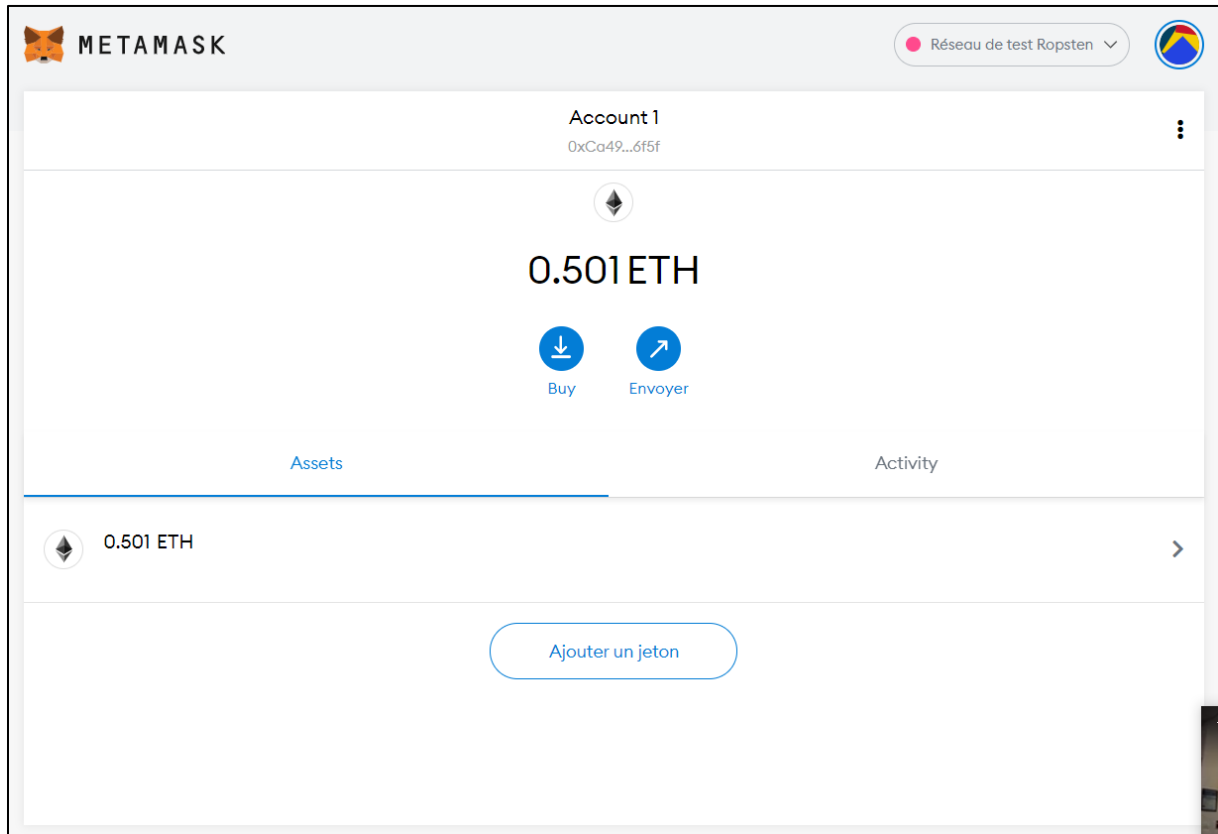


## TP BLOCKCHAIN – Smart Contract

Gist : <https://gist.github.com/Yassdrk>

### 1. Prise en main des outils Remix et Metamask



Overview

State

[ This is a Ropsten Testnet transaction only ]

Transaction Hash:

0x7666b7a481901af07021092675c4f60fc1dc80943d8b6bd425c7192578d00cad

Status:

Success

Block:

999878019 Block Confirmations

Timestamp:

35 mins ago (Apr-08-2021 12:34:22 PM +UTC)

From:

0xddf80da9d8a425b5a8fb64bfc79857ba9b57083

To:

0xca49b447d85f442abf74d6e849927a986cb6f5f

Value:

0.001 Ether (\$0.00)

Transaction Fee:

0.0021 Ether (\$0.00)

Gas Price:

0.0000001 Ether (100 Gwei)

Click to see More

Abi :

```
[
  {
    "anonymous": false,
    "inputs": [
      {
        "indexed": true,
        "internalType": "address",
        "name": "previousOwner",
        "type": "address"
      },
      {
        "indexed": true,
        "internalType": "address",
        "name": "newOwner",
        "type": "address"
      }
    ],
    "name": "OwnershipTransferred",
    "type": "event"
  },
  {
    "anonymous": false,
    "inputs": [
      {
        "indexed": true,
        "internalType": "uint256",
        "name": "_candidateId",
        "type": "uint256"
      }
    ],
    "name": "votedEvent",
    "type": "event"
  },
  {
    "inputs": [
      {
        "internalType": "string",
        "name": "_name",
        "type": "string"
      }
    ],
    "name": "addCandidate",
    "outputs": [],
    "stateMutability": "nonpayable",
    "type": "function"
  },
]
```

```

{
  "inputs": [
    {
      "internalType": "uint256",
      "name": "",
      "type": "uint256"
    }
  ],
  "name": "candidates",
  "outputs": [
    {
      "internalType": "uint256",
      "name": "id",
      "type": "uint256"
    },
    {
      "internalType": "string",
      "name": "name",
      "type": "string"
    },
    {
      "internalType": "uint256",
      "name": "voteCount",
      "type": "uint256"
    }
  ],
  "stateMutability": "view",
  "type": "function"
},
{
  "inputs": [],
  "name": "candidatesCount",
  "outputs": [
    {
      "internalType": "uint256",
      "name": "",
      "type": "uint256"
    }
  ],
  "stateMutability": "view",
  "type": "function"
},
{
  "inputs": [],
  "name": "owner",
  "outputs": [
    {
      "internalType": "address",
      "name": "",
      "type": "address"
    }
  ],
  "stateMutability": "view",
  "type": "function"
},
{
  "inputs": [
    {
      "internalType": "address",
      "name": "newOwner",
      "type": "address"
    }
  ],
  "name": "transferOwnership",
  "outputs": [],
  "stateMutability": "nonpayable",
  "type": "function"
},
{
  "inputs": [

```

```

        "internalType": "uint256",
        "name": "_candidateId",
        "type": "uint256"
    }
},
{
    "name": "vote",
    "outputs": [],
    "stateMutability": "nonpayable",
    "type": "function"
},
{
    "inputs": [
        {
            "internalType": "address",
            "name": "",
            "type": "address"
        }
    ],
    "name": "voters",
    "outputs": [
        {
            "internalType": "bool",
            "name": "",
            "type": "bool"
        }
    ],
    "stateMutability": "view",
    "type": "function"
}
]

```

**Bytecode :**

[illegible]

```
ffffffffffffffff166008054906101000a900473ffffffffffffffffffffffffffffffff1673ffffffffffffffffffffffffffffffff167f8be0079c53165
9141344cd1fd0a4f28419497f9722a3daafe3b4186fb6457e060405160405180910390a3806000806101000a81548173fffffffffffffffffffff
ffffffffffffffff021916908373ffffffffffffffffffffffffffffffff16021790555050565b82805460018160011615610100020316600290049060
0052602060002090601f016020900481019282601f1061081957805160ff1916838001178555610847565b828001600101855582156108
47579182015b8281111561084657825182559160200191906001019061082b565b5b5090506108549190610858565b5090565b5b8082
1115610871576000816000905550600101610859565b509056fea2646970667358221220153ffb07d0822dcd0f95c2d0b6de288190ae59
b0e17bd9f285d40261585b950064736fc634300060c0033",
"opcodes": "PUSH1 0x80 PUSH1 0x40 MSTORE CALLVALUE DUP1 ISZERO PUSH2 0x10 JUMPI PUSH1 0x0 DUP1 REVERT
JUMPDEST POP CALLER PUSH1 0x0 DUP1 PUSH2 0x100 EXP DUP2 SLOAD DUP2 PUSH20 0xffffffffffffffffffffffffffffffff
MUL NOT AND SWAP1 DUP4 PUSH20 0xffffffffffffffffffffffffffffffff AND MUL OR SWAP1 SSTORE POP PUSH2 0x8AB
DUP1 PUSH2 0x60 PUSH1 0x0 CODECOPY PUSH1 0x0 RETURN INVALID PUSH1 0x80 PUSH1 0x40 MSTORE CALLVALUE DUP1 ISZERO
PUSH2 0x10 JUMPI PUSH1 0x0 DUP1 REVERT JUMPDEST POP PUSH1 0x4 CALLDATASIZE LT PUSH2 0x7D JUMPI PUSH1 0x0
CALLDATALOAD PUSH1 0xE0 SHR DUP1 PUSH4 0x462E91EC GT PUSH2 0x5B JUMPI DUP1 PUSH4 0x462E91EC EQ PUSH2 0x183 JUMPI
DUP1 PUSH4 0x8DA5CB5B EQ PUSH2 0x23E JUMPI DUP1 PUSH4 0xA3EC138D EQ PUSH2 0x272 JUMPI DUP1 PUSH4 0xF2FDE38B EQ
PUSH2 0x2CC JUMPI PUSH2 0x7D JUMP JUMPDEST DUP1 PUSH4 0x121B93F EQ PUSH2 0x82 JUMPI DUP1 PUSH4 0x2D35A8A2 EQ
PUSH2 0xB0 JUMPI DUP1 PUSH4 0x3477EE2E EQ PUSH2 0xCE JUMPI JUMPDEST PUSH1 0x0 DUP1 REVERT JUMPDEST PUSH2 0xAE
PUSH1 0x4 DUP1 CALLDATASIZE SUB PUSH1 0x20 DUP2 LT ISZERO PUSH2 0x98 JUMPI PUSH1 0x0 DUP1 REVERT JUMPDEST DUP2 ADD
SWAP1 DUP1 DUP1 CALLDATALOAD SWAP1 PUSH1 0x20 ADD SWAP1 SWAP3 SWAP2 SWAP1 POP POP POP PUSH2 0x310 JUMP
JUMPDEST STOP JUMPDEST PUSH2 0xB8 PUSH2 0x42F JUMP JUMPDEST PUSH1 0x40 MLOAD DUP1 DUP3 DUP2 MSTORE PUSH1 0x20
ADD SWAP2 POP POP PUSH1 0x40 MLOAD DUP1 SWAP2 SUB SWAP1 RETURN JUMPDEST PUSH2 0xFA PUSH1 0x4 DUP1 CALLDATASIZE
SUB PUSH1 0x20 DUP2 LT ISZERO PUSH2 0xE4 JUMPI PUSH1 0x0 DUP1 REVERT JUMPDEST DUP2 ADD SWAP1 DUP1 DUP1
CALLDATALOAD SWAP1 PUSH1 0x20 ADD SWAP1 SWAP3 SWAP2 SWAP1 POP POP POP PUSH2 0x435 JUMP JUMPDEST PUSH1 0x40
MLOAD DUP1 DUP5 DUP2 MSTORE PUSH1 0x20 ADD DUP1 PUSH1 0x20 ADD DUP4 DUP2 MSTORE PUSH1 0x20 ADD DUP3 DUP2 SUB
DUP3 MSTORE DUP5 DUP2 DUP2 MLOAD DUP2 MSTORE PUSH1 0x20 ADD SWAP2 POP DUP1 MLOAD SWAP1 PUSH1 0x20 ADD SWAP1
DUP1 DUP4 DUP4 PUSH1 0x0 JUMPDEST DUP4 DUP2 LT ISZERO PUSH2 0x146 JUMPI DUP1 DUP3 ADD MLOAD DUP2 DUP5 ADD
MSTORE PUSH1 0x20 DUP2 ADD SWAP1 POP PUSH2 0x12B JUMP JUMPDEST POP POP POP POP SWAP1 POP SWAP1 DUP2 ADD SWAP1
PUSH1 0x1F AND DUP1 ISZERO PUSH2 0x173 JUMPI DUP1 DUP3 SUB DUP1 MLOAD PUSH1 0x1 DUP4 PUSH1 0x20 SUB PUSH2 0x100
EXP SUB NOT AND DUP2 MSTORE PUSH1 0x20 ADD SWAP2 POP JUMPDEST POP SWAP5 POP POP POP POP POP PUSH1 0x40 MLOAD
DUP1 SWAP2 SUB SWAP1 RETURN JUMPDEST PUSH2 0x23C PUSH1 0x4 DUP1 CALLDATASIZE SUB PUSH1 0x20 DUP2 LT ISZERO PUSH2
0x199 JUMPI PUSH1 0x0 DUP1 REVERT JUMPDEST DUP2 ADD SWAP1 DUP1 DUP1 CALLDATALOAD SWAP1 PUSH1 0x20 ADD SWAP1
PUSH5 0x100000000 DUP2 GT ISZERO PUSH2 0x1B6 JUMPI PUSH1 0x0 DUP1 REVERT JUMPDEST DUP3 ADD DUP4 PUSH1 0x20 DUP3
ADD GT ISZERO PUSH2 0x1C8 JUMPI PUSH1 0x0 DUP1 REVERT JUMPDEST DUP1 CALLDATALOAD SWAP1 PUSH1 0x20 ADD SWAP2 DUP5
PUSH1 0x1 DUP4 MUL DUP5 ADD GT PUSH5 0x100000000 DUP4 GT OR ISZERO PUSH2 0x1EA JUMPI PUSH1 0x0 DUP1 REVERT
JUMPDEST SWAP2 SWAP1 DUP1 DUP1 PUSH1 0x1F ADD PUSH1 0x20 DUP1 SWAP2 DIV MUL PUSH1 0x20 ADD PUSH1 0x40 MLOAD
SWAP1 DUP2 ADD PUSH1 0x40 MSTORE DUP1 SWAP4 SWAP3 SWAP2 SWAP1 DUP2 DUP2 MSTORE PUSH1 0x20 ADD DUP4 DUP4 DUP1
DUP3 DUP5 CALLDATACOPY PUSH1 0x0 DUP2 DUP5 ADD MSTORE PUSH1 0x1F NOT PUSH1 0x1F DUP3 ADD AND SWAP1 POP DUP1
DUP4 ADD SWAP3 POP POP POP POP POP POP SWAP2 SWAP3 SWAP2 SWAP3 SWAP1 POP POP POP PUSH2 0x4F7 JUMP
JUMPDEST STOP JUMPDEST PUSH2 0x246 PUSH2 0x573 JUMP JUMPDEST PUSH1 0x40 MLOAD DUP1 DUP3 PUSH20
0xffffffffffffffffffffffffffffffff AND DUP2 MSTORE PUSH1 0x20 ADD SWAP2 POP POP PUSH1 0x40 MLOAD DUP1
SWAP2 SUB SWAP1 RETURN JUMPDEST PUSH2 0x2B4 PUSH1 0x4 DUP1 CALLDATASIZE SUB PUSH1 0x20 DUP2 LT ISZERO PUSH2 0x288
JUMPI PUSH1 0x0 DUP1 REVERT JUMPDEST DUP2 ADD SWAP1 DUP1 DUP1 CALLDATALOAD PUSH20
0xffffffffffffffffffffffffffffffff AND SWAP1 PUSH1 0x20 ADD SWAP1 SWAP3 SWAP2 SWAP1 POP POP POP PUSH2
0x597 JUMP JUMPDEST PUSH1 0x40 MLOAD DUP1 DUP3 ISZERO ISZERO DUP2 MSTORE PUSH1 0x20 ADD SWAP2 POP POP PUSH1 0x40
MLOAD DUP1 SWAP2 SUB SWAP1 RETURN JUMPDEST PUSH2 0x30E PUSH1 0x4 DUP1 CALLDATASIZE SUB PUSH1 0x20 DUP2 LT ISZERO
PUSH2 0x2E2 JUMPI PUSH1 0x0 DUP1 REVERT JUMPDEST DUP2 ADD SWAP1 DUP1 DUP1 CALLDATALOAD PUSH20
0xffffffffffffffffffffffffffffffff AND SWAP1 PUSH1 0x20 ADD SWAP1 SWAP3 SWAP2 SWAP1 POP POP POP PUSH2
0x5B7 JUMP JUMPDEST STOP JUMPDEST PUSH1 0x1 PUSH1 0x0 CALLER PUSH20 0xffffffffffffffffffffffffffffffff AND
PUSH20 0xffffffffffffffffffffffffffffffff AND DUP2 MSTORE PUSH1 0x20 ADD SWAP1 DUP2 MSTORE PUSH1 0x20 ADD
PUSH1 0x0 KECCAK256 PUSH1 0x0 SWAP1 SLOAD SWAP1 PUSH2 0x100 EXP SWAP1 DIV PUSH1 0xFF AND ISZERO PUSH2 0x367 JUMPI
PUSH1 0x0 DUP1 REVERT JUMPDEST PUSH1 0x0 DUP2 GT DUP1 ISZERO PUSH2 0x379 JUMPI POP PUSH1 0x3 SLOAD DUP2 GT ISZERO
JUMPDEST PUSH2 0x382 JUMPI PUSH1 0x0 DUP1 REVERT JUMPDEST PUSH1 0x1 DUP1 PUSH1 0x0 CALLER PUSH20
0xffffffffffffffffffffffffffffffff AND PUSH20 0xffffffffffffffffffffffffffffffff AND DUP2 MSTORE
PUSH1 0x20 ADD SWAP1 DUP2 MSTORE PUSH1 0x20 ADD PUSH1 0x0 KECCAK256 PUSH1 0x0 PUSH2 0x100 EXP DUP2 SLOAD DUP2
PUSH1 0xFF MUL NOT AND SWAP1 DUP4 ISZERO ISZERO MUL OR SWAP1 SSTORE POP PUSH1 0x2 PUSH1 0x0 DUP3 DUP2 MSTORE
PUSH1 0x20 ADD SWAP1 DUP2 MSTORE PUSH1 0x20 ADD PUSH1 0x0 KECCAK256 PUSH1 0x2 ADD PUSH1 0x0 DUP2 SLOAD DUP1
SWAP3 SWAP2 SWAP1 PUSH1 0x1 ADD SWAP2 SWAP1 POP SSTORE POP DUP1 PUSH32
0xFFf3C900D938D21D0990D786E819F29B8D05C1EF587B462B939609625B684B16 PUSH1 0x40 MLOAD PUSH1 0x40 MLOAD DUP1
SWAP2 SUB SWAP1 LOG2 POP JUMP JUMPDEST PUSH1 0x3 SLOAD DUP2 JUMP JUMPDEST PUSH1 0x2 PUSH1 0x20 MSTORE DUP1
PUSH1 0x0 MSTORE PUSH1 0x40 PUSH1 0x0 KECCAK256 PUSH1 0x0 SWAP2 POP SWAP1 POP DUP1 PUSH1 0x0 ADD SLOAD SWAP1
DUP1 PUSH1 0x1 ADD DUP1 SLOAD PUSH1 0x1 DUP2 PUSH1 0x1 AND ISZERO PUSH2 0x100 MUL SUB AND PUSH1 0x2 SWAP1 DIV DUP1
PUSH1 0x1F ADD PUSH1 0x20 DUP1 SWAP2 DIV MUL PUSH1 0x20 ADD PUSH1 0x40 MLOAD SWAP1 DUP2 ADD PUSH1 0x40 MSTORE
DUP1 SWAP3 SWAP2 SWAP1 DUP2 DUP2 MSTORE PUSH1 0x20 ADD DUP3 DUP1 SLOAD PUSH1 0x1 DUP2 PUSH1 0x1 AND ISZERO
PUSH2 0x100 MUL SUB AND PUSH1 0x2 SWAP1 DIV DUP1 ISZERO PUSH2 0x4E7 JUMPI DUP1 PUSH1 0x1F LT PUSH2 0x4BC JUMPI
PUSH2 0x100 DUP1 DUP4 SLOAD DIV MUL DUP4 MSTORE SWAP2 PUSH1 0x20 ADD SWAP2 PUSH2 0x4E7 JUMP JUMPDEST DUP3 ADD
SWAP2 SWAP1 PUSH1 0x0 MSTORE PUSH1 0x20 PUSH1 0x0 KECCAK256 SWAP1 JUMPDEST DUP2 SLOAD DUP2 MSTORE SWAP1 PUSH1
0x1 ADD SWAP1 PUSH1 0x20 ADD DUP1 DUP4 GT PUSH2 0x4CA JUMPI DUP3 SWAP1 SUB PUSH1 0x1F AND DUP3 ADD SWAP2
JUMPDEST POP POP POP POP POP SWAP1 DUP1 PUSH1 0x2 ADD SLOAD SWAP1 POP DUP4 JUMP JUMPDEST PUSH1 0x3 PUSH1 0x0
DUP2 SLOAD DUP1 SWAP3 SWAP2 SWAP1 PUSH1 0x1 ADD SWAP2 SWAP1 POP SSTORE POP PUSH1 0x40 MLOAD DUP1 PUSH1 0x60
ADD PUSH1 0x40 MSTORE DUP1 PUSH1 0x3 SLOAD DUP2 MSTORE PUSH1 0x20 ADD DUP3 DUP2 MSTORE PUSH1 0x20 ADD PUSH1 0x0
DUP2 MSTORE POP PUSH1 0x2 PUSH1 0x0 PUSH1 0x3 SLOAD DUP2 MSTORE PUSH1 0x20 ADD SWAP1 DUP2 MSTORE PUSH1 0x20 ADD
PUSH1 0x0 KECCAK256 PUSH1 0x0 DUP3 ADD MLOAD DUP2 PUSH1 0x0 ADD SSTORE PUSH1 0x20 DUP3 ADD MLOAD DUP2 PUSH1 0x1
```

[illegible]

### m. Déploiement du Smart Contract :

### DEPLOY & RUN TRANSACTIONS

be saved and replayed in another environment. e.g Transactions created in Javascript VM can be replayed in the Injected Web3.

Deployed Contracts

▼ ELECTION AT 0xD8B...B08E7 (BLOCK)

addCandidate string\_name

transferOwner... address newOwner

vote uint256 \_candidateId

candidates uint256

candidatesCou...

owner

0 address 0xCa49b447D8954442abf74d6E849927A986cb6f5

voters address

Low level interactions

CALLDATA

Transact

```

28 event votedEvent ( uint indexed _candidateId);
29
30 function addCandidate(string memory _name) public {
31     candidatesCount ++;
32     candidates[candidatesCount] = Candidate(candidatesCount, _name, 0);
33 }
34
35 function vote (uint _candidateId) public {
36     // require that they haven't voted before
37     require(!voters[msg.sender]);
38
39     // require a valid candidate
40     require(_candidateId > 0 && _candidateId <= candidatesCount);
41
42     // record that voter has voted
43     voters[msg.sender] = true;
44
45     // update candidate vote Count
46     candidates[_candidateId].voteCount ++;
47
48     // trigger voted event
49     emit votedEvent (_candidateId);
50 }
51 }
52

```

listen on network

creation of Election pending...

creation of Election errored: MetaMask Tx Signature: User denied transaction signature.

✓ [block:999887 txIndex:13] from: 0xCa4...b6f5 to: Election.(constructor) value: 0 wei data: 0x688...0033 logs: 0x36e...d7c82





call to Election.owner

[call] from: 0xCa49b447D854442abf74d6E849927A986cb6f5 to: Election.owner() data: 0x8da...5cb5b

L'adresse publique du smart contract est : 0xdB85daB990cc1bB101BfcDC5d2732Dd7FdFb08e7

n. Ajout du candidat portant mon nom de famille :

addCandidate DERKAOUI

Overview	State
[ This is a Ropsten <b>Testnet</b> transaction only ]	
Transaction Hash:	0xddddd1d599faaf036ca0f28786cf1dc8893b1b98d552a216116b50ecb50fb73 
Status:	<span>Success</span>
Block:	998947 <span>1 Block Confirmation</span>
Timestamp:	23 secs ago (Apr-08-2021 02:01:42 PM +UTC)
From:	0xca49b447d85f4f2abf74d6e849927a986cb6f5f 
To:	Contract 0xdb85dab990cc1bb101bfcdc5d2732dd7dfb08e7  
Value:	0 Ether (\$0.00)
Transaction Fee:	0.0091406 Ether (\$0.00)
Gas Price:	0.0000001 Ether (100 Gwei)
Gas Limit:	91,489
Gas Used by Transaction:	91,406 (99.91%)
Nonce	2 <span>Position 5</span>
Input Data:	Function: addCandidate(string name) ***

[illegible]

p. La valeur du CandidateID est 1.

q. Ajout du candidat ESME.

[illegible]

r. L'id du candidat ESME est : 2.

[illegible]

s. L'adresse du propriétaire du contrat est (en cliquant sur owner) : 0xCa49b447D85f44f2abF74d6E849927A986cb6f5f

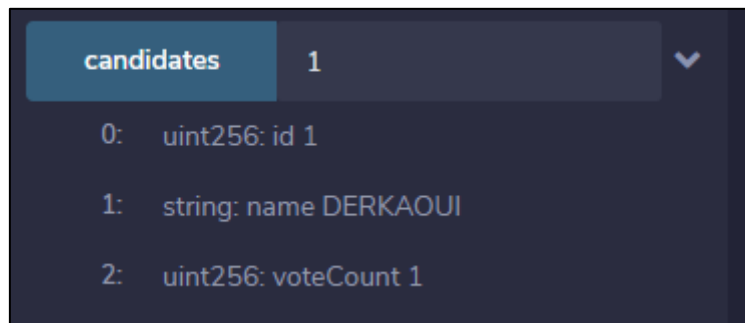
```
0:  address: 0xCa49b447D85f44f2abF74d6E849927A986cb6f5f
```

t. Nous réalisons un vote pour le candidat  $id = 1$  (DERKAoui). Le détail de la transaction est :



[illegible]

u. Le vote a bien été pris en compte (voteCount 1)



v. J'ai demandé à benjamin de voter pour le candidat numéro 1 :

[illegible]

w. J'ai transféré la propriété de mon contrat à benjamin grâce à son adresse publique : 0x9E52C528D0a82675b4c54261Ee6a0CA328319569

x. Il faudrait vérifier que celui qui ajoute le candidat est le propriétaire du contrat (owner).

y. J'ai ajouté la fonction OnlyOwner de Ownable.sol dans election sur la fonction AddCandidate.

```

*/
modifier onlyOwner() {
    require(msg.sender == owner, "Not authorized operation");
}

```

Ce qui donne :

```

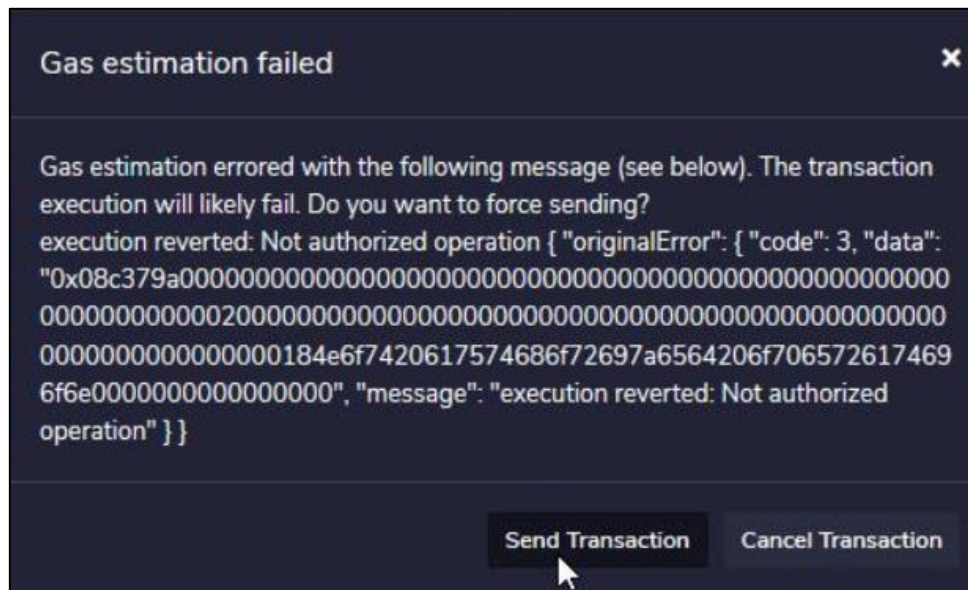
function addCandidate (string memory _name) public onlyOwner {
    candidatesCount ++;
    candidates[candidatesCount] = Candidate(candidatesCount, _name, 0);
}







```

En recompilant et en redéployant mon contrat j'ai réussi à ajouter le candidat :

Transaction Hash:	0x0c222c4912375b451daa70f11748d0c06284abc650440aba2091ae71a50db
Status:	Success
Block:	9999209 10 Block Confirmations
Timestamp:	2 mins ago (Apr-08-2021 03:30:21 PM +UTC)
From:	0xc4f9b447d859442abf74d5e849627a986cb6f5
To:	Contract 0x0c08c56cee69a904fe541764c8386b59e303096
Value:	0 Ether (\$0.00)
Transaction Fee:	0.00093573 Ether (\$0.00)
Gas Price:	0.00000001 Ether (10 Gwei)
Gas Limit:	93,656
Gas Used by Transaction:	93,573 (99.91%)
Nonce	11
Input Data:	Function: addCandidate(string name) *** MethodID: 0x62271ee5

Mon camarade benjamin a tenté d'ajouter un candidat et ça n'a pas marché :



Transaction Hash:	0x5d03cab85f07eae5b7da490cc2f1643d9f395e7fa3036ecd5106c7667a85e0f 
Status:	 Fail with error 'Not authorized operation'
Block:	9999291 <span>2 Block Confirmations</span>
Timestamp:	49 secs ago (Apr-08-2021 03:34:21 PM +UTC)
From:	0x9e52c528d0a82675b4c54261ee6a0ca328319569 
To:	Contract 0x0c08c56cee69a904fe54176a4c8386b59e303096   <span>Warning! Error encountered during contract execution [Reverted] </span>
Value:	0 Ether (\$0.00)
Transaction Fee:	0.000024387 Ether (\$0.00)
Gas Price:	0.000000001 Ether (1 Gwei)
Gas Limit:	3,000,000
Gas Used by Transaction:	24,387 (0.81%)
Nonce <span>Position</span>	10 <span>11</span>
Input Data:	<pre>Function: addCandidate(string name) *** MethodID: 8x463e91ec</pre>