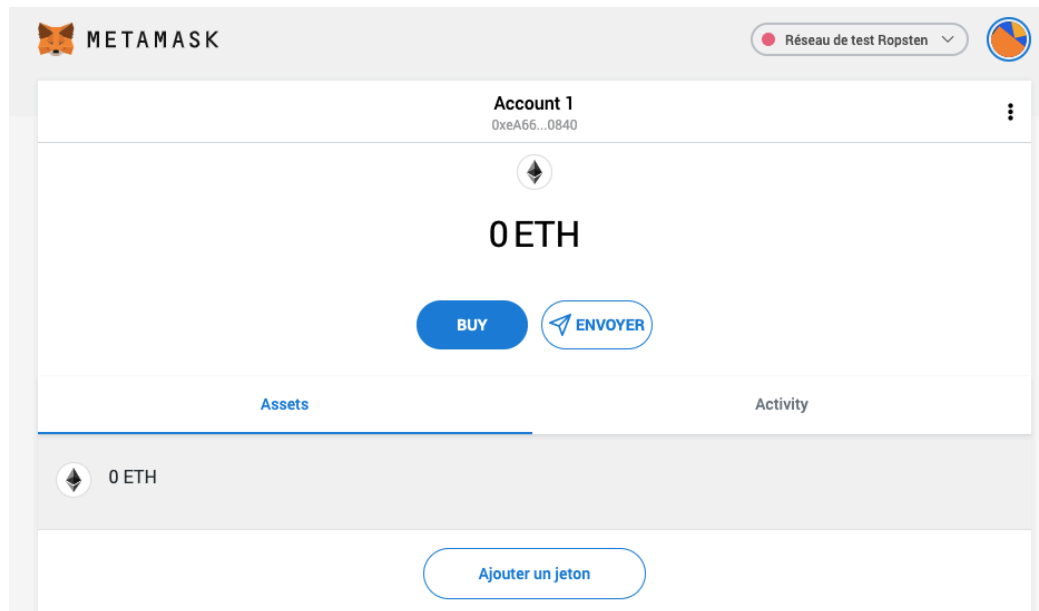


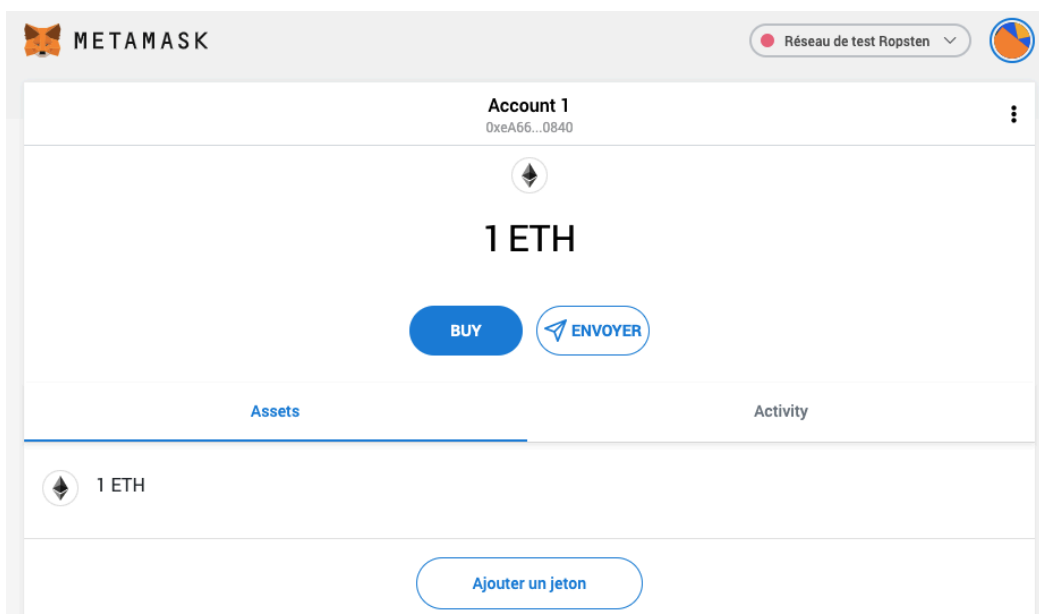
TP Blockchain : Election

- a)
- b)
- c)

Après la création d'un compte GitHub, on installe Metamask :



- d) On génère un ETH



e)

f) Les détails de la transaction sont :

Transaction Details

Overview

State

[This is a Ropsten Testnet transaction only]

Transaction Hash:

0x970f0bc39cf306f58412e77d2fbc94f9031c55aa86be3ad362b35690505fe30

Status:

Success

Block:

8636012

30 Block Confirmations

Timestamp:

3 mins ago (Sep-07-2020 08:16:59 AM +UTC)

From:

0x81b7e08f65bdf5648606c89998a9cc8164397647

To:

0xea6618c37820d147a56498b641d2c1e96a270840

Value:

1 Ether (\$0.00)

Transaction Fee:

0.0000315 Ether (\$0.000000)

Gas Limit:

21,000

Gas Used by Transaction:

21,000 (100%)

Gas Price:

0.000000015 Ether (1.5 Gwei)

Nonce

Position

34452161

7

Input Data:

0x

The binary data that formed the input to the transaction, either the input data if it was a message call or the contract initialisation if it was a contract creation

g) La transaction a bien été effectuée :

Envoyer des ETH

Détails

de: 0xeA6618C37820d1... > Destinataire: 0xc25a95...

Transaction

Nonce

0

Montant

0.5 ETH

Quantité Max. De Gaz (Unités)

21000

Essence Utilisée (Unités)

21000

Prix du gaz (GWEI)

81

Total

0.501701 ETH

Log D'activité

+

Transaction crée avec une valeur de 0.5 ETH sur 10:23 on 9/7/2020.

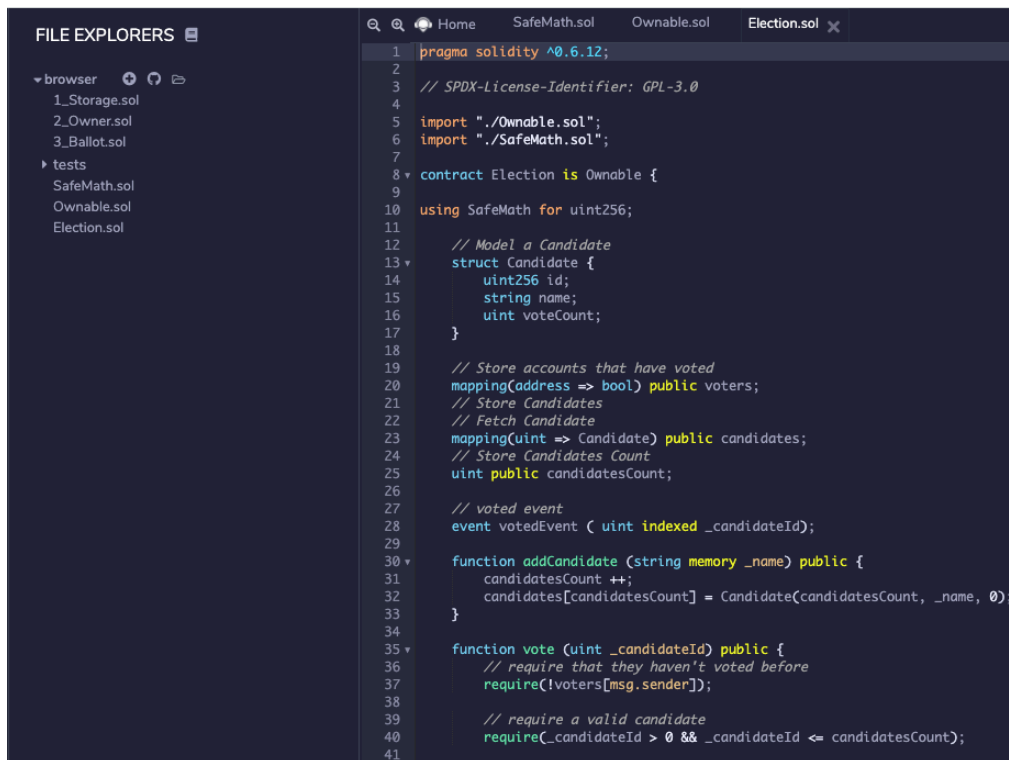
→

Transaction envoyée sur 10:23 on 9/7/2020.

✓

Transaction confirmée sur 10:23 on 9/7/2020.

- h)
i)
j) Après ouverture et importation des smart contract :



```

1 pragma solidity ^0.6.12;
2
3 // SPDX-License-Identifier: GPL-3.0
4
5 import "../Ownable.sol";
6 import "../SafeMath.sol";
7
8 contract Election is Ownable {
9
10     using SafeMath for uint256;
11
12     // Model a Candidate
13     struct Candidate {
14         uint256 id;
15         string name;
16         uint voteCount;
17     }
18
19     // Store accounts that have voted
20     mapping(address => bool) public voters;
21     // Store Candidates
22     // Fetch Candidate
23     mapping(uint => Candidate) public candidates;
24     // Store Candidates Count
25     uint public candidatesCount;
26
27     // voted event
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

```

k) ABI et ByteCode : [https://github.com/MaxDebarle/TP Election](https://github.com/MaxDebarle/TP_Election)

l) Déploiement du contrat :

Déploiement de contrat

Détails

de: 0xeA6618C37820d1... > Nouveau contrat

Transaction

Nonce	1
Montant	0 ETH
Quantité Max. De Gaz (Unités)	553206
Essence Utilisée (Unités)	553206
Prix du gaz (GWEI)	1.5
Total	0.00083 ETH

Log D'activité

- Transaction créée avec une valeur de 0 ETH sur 10:50 on 9/7/2020.
- Transaction envoyée sur 10:50 on 9/7/2020.
- Transaction confirmée sur 10:50 on 9/7/2020.

m) On peut voir les détails suivants :

Transaction Details

Overview

State

[This is a Ropsten Testnet transaction only]

Transaction Hash:

0xac56a246c472085b09dce9c12fa21af84904fa20ae0a10bbcbc6b075e58ddab9

Status:

Success

Block:

8636259

18 Block Confirmations

Timestamp:

2 mins ago (Sep-07-2020 08:50:26 AM +UTC)

From:

0xea6618c37820d147a56498b641d2c1e96a270840

To:

[Contract 0xf397e490cda7a776496f53cae84b8d865964dea6 Created]

Value:

0 Ether (\$0.00)

Transaction Fee:

0.000829809 Ether (\$0.000000)

Gas Limit:

553,206

Gas Used by Transaction:

553,206 (100%)

Gas Price:

0.0000000015 Ether (1.5 Gwei)

Nonce

Position

1

10

Input Data:

0x608060405234801561001057600000fd5b50336000806101000a81548173f73fff1602179055506108ab806fd5b506004361061007d5760003560e01c8063462e91ec1161005b57806346214610272578063f2fde38b146102cc5761007d565b80630121b93f1461008250080fd5b6100ae6004803603602081101561009857600080fd5b810190808080

Les frais de transactions sont différents car ils dépendent du flux de transactions sur le réseau. Ils peuvent donc être très différents.

L'adresse publique de mon smart contract est :

To: [Contract 0xf397e490cda7a776496f53cae84b8d865964dea6 Created]

n) Ajout d'un candidat du nom de DEBARLE :

Add Candidate

Détails

de: 0xeA6618C37820d1... > Destinataire: 0xf397E49...

Transaction

Nonce

2

Montant

0 ETH

Quantité Max. De Gaz (Unités)

88177

Essence Utilisée (Unités)

86694

Prix du gaz (GWEI)

1.5

Total

0.00013 ETH

Log D'activité

Transaction créée avec une valeur de 0 ETH sur 11:02 on 9/7/2020.

Transaction envoyée sur 11:02 on 9/7/2020.

Transaction confirmée sur 11:02 on 9/7/2020.

Maxime DEBARLE

A2 - IR

4/9

o) Les détails de la transaction sont :

Overview	State
[This is a Ropsten Testnet transaction only]	
Transaction Hash:	0x0e603a6f1feb0b6b2c4c8990c0a7f75f6800f5daabd60e2e3bac15e713a86821
Status:	Success
Block:	8636368 11 Block Confirmations
Timestamp:	1 min ago (Sep-07-2020 09:02:24 AM +UTC)
From:	0xea6618c37820d147a56498b641d2c1e96a270840
To:	Contract 0xf397e490cda7a776496f53cae84b8d865964dea6
Value:	0 Ether (\$0.00)
Transaction Fee:	0.000130041 Ether (\$0.000000)
Gas Limit:	88,177
Gas Used by Transaction:	86,694 (98.32%)
Gas Price:	0.0000000015 Ether (1.5 Gwei)
Nonce	2 15
Input Data:	<pre>Function: addCandidate(string name) *** MethodID: 0x462e91ec [0]: 0020 [1]: 0007 [2]: 44454241524c4500</pre>

p)

candidates	1
0:	uint256: id 1
1:	string: name DEBARLE
2:	uint256: voteCount 0

q) Détails de l'ajout du candidat ALVES

Overview	State
[This is a Ropsten Testnet transaction only]	
Transaction Hash:	0x55b50d4544367dc9b7b535836a809b5f556617529c40362da3061dd1fde94391
Status:	Success
Block:	8636406 6 Block Confirmations
Timestamp:	1 min ago (Sep-07-2020 09:06:52 AM +UTC)
From:	0xea6618c37820d147a56498b641d2c1e96a270840
To:	Contract 0xf397e490cda7a776496f53cae84b8d865964dea6
Value:	0 Ether (\$0.00)
Transaction Fee:	0.000107505 Ether (\$0.000000)
Gas Limit:	73,153
Gas Used by Transaction:	71,670 (97.97%)
Gas Price:	0.0000000015 Ether (1.5 Gwei)
Nonce	Position 3 6
Input Data:	<p>Function: addCandidate(string name) ***</p> <p>MethodID: 0x462e91ec</p> <p>[0]: 0020</p> <p>[1]: 0005</p> <p>[2]: 414c56455300</p>

r)

candidates	2
0:	uint256: id 2
1:	string: name ALVES
2:	uint256: voteCount 0

s)

owner
0: address: 0xEA6618C37820d147A56498B641d2c1E96a270840

t)

Transaction Details

[Overview](#) [Logs \(1\)](#) [State](#)

[This is a Ropsten Testnet transaction only]

Transaction Hash:	0xac87961313c300305f9db1085ca03c780bff484d2beffea414c30b64250ad11 📄
Status:	✓ Success
Block:	8636450 5 Block Confirmations
Timestamp:	40 secs ago (Sep-07-2020 09:11:01 AM +UTC)
From:	0xea6618c37820d147a56498b641d2c1e96a270840 📄
To:	Contract 0xf397e490cda7a776496f53cae84b8d865964dea6 ✓ 📄
Value:	0 Ether (\$0.00)
Transaction Fee:	0.0000994005 Ether (\$0.000000)
Gas Limit:	66,267
Gas Used by Transaction:	66,267 (100%)
Gas Price:	0.0000000015 Ether (1.5 Gwei)
Nonce	<div>Position</div> 411
Input Data:	<div>Function: vote(uint256 proposal) *** MethodID: 0x0121b93f [0]: 0001</div>

u) Le vote est bien passé à 1 :

candidates

1

0:

uint256: id 1

1:

string: name DEBARLE

2:

uint256: voteCount 1

v) Détails du vote sur le contrat d'un camarade :

Overview	
[This is a Ropsten Testnet transaction only]	
Transaction Hash:	0xd43daa24073c2fcbf4f0174ca21dd956b45c1e8b710ae6f53191390ada95d193 🔗
Status:	Pending
Block:	(Pending)
Time Last Seen:	⌚ 00 days 00 hr 00 min 47 secs ago (Sep-07-2020 09:17:12 AM)
From:	0xea6618c37820d147a56498b641d2c1e96a270840 🔗
To:	0xc503d5ad7d094fb0d7e6d8266124156bf0ff50f9 🔗
Value:	0 Ether (\$0.000000)
Max Txn Cost/Fee:	0.000031806 Ether (\$0.000000)
Gas Limit:	21204
Gas Used by Transaction:	Pending
Gas Price:	0.000000015 Ether (1.5 Gwei)
Nonce Position	5 Pending
Input Data:	<pre>Function: vote(uint256 proposal) *** MethodID: 0x0121b93f [0]: 00</pre> View Input As ▾

w) transfert de propriété :

Transaction Details

Overview

Logs (1)

State

[This is a Ropsten Testnet transaction only]

Transaction Hash:

0xd250f13609c5c5d547f2536ddcea26fedcfd27804e51a9fd0bd3ed860aba04a

Status:

Success

Block:

8636513

3 Block Confirmations

Timestamp:

35 secs ago (Sep-07-2020 09:21:46 AM +UTC)

From:

0xea6618c37820d147a56498b641d2c1e96a270840

To:

Contract 0xf397e490cda7a776496f53cae84b8d865964dea6

Value:

0 Ether (\$0.00)

Transaction Fee:

0.000046323 Ether (\$0.000000)

Gas Limit:

30,882

Gas Used by Transaction:

30,882 (100%)

Gas Price:

0.000000015 Ether (1.5 Gwei)

Nonce

Position

7

5

Input Data:

Function: transferOwnership(address newOwner) ***

MethodID: 0xf2fde38b

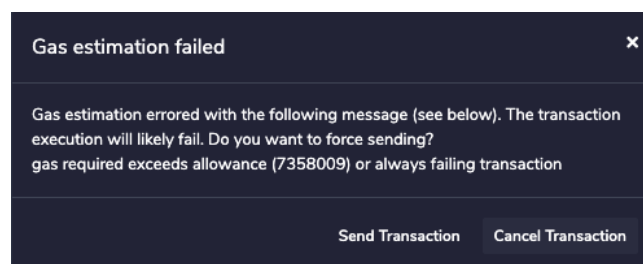
[0]: 000000000000000000000000c503d5ad7d094fb0d7e6d8266124156bf0ff5f09f

x) Afin de sécuriser l'appel de la fonction et par conséquent être le seul à pouvoir gérer les candidats, il suffit de poser une condition à l'appel de la fonction qui demande si la personne qui appelle la fonction est le owner ou non.

y) On rajoute onlyOwner :

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

Ce qui a pour conséquence après un transfert de propriété :



Overview		State
[This is a Ropsten Testnet transaction only]		
Transaction Hash:	0x570c5f868a40bdd144accfb2128411f220bc52c45f1ad8572a24916e82c1e87d	
Status:	Fail with error 'Not authorized operation'	
Block:	8636726 3 Block Confirmations	
Timestamp:	43 secs ago (Sep-07-2020 09:47:23 AM +UTC)	
From:	0xea6618c37820d147a56498b641d2c1e96a270840	
To:	Contract 0xdab15a3c800e7691846eaf57c75ce102e320c436 Warning! Error encountered during contract execution [Reverted]	
Value:	0 Ether (\$0.00)	
Transaction Fee:	0.0000345945 Ether (\$0.000000)	
Gas Limit:	3,000,000	
Gas Used by Transaction:	23,063 (0.77%)	
Gas Price:	0.0000000015 Ether (1.5 Gwei)	
Nonce	Position	14 7
Input Data:	Function: addCandidate(string name) *** MethodID: 0x462e91ec [0]: 0020 [1]: 0005 [2]: 414c56455300	