

Hélène KAING A2I

TP Blockchain :

e. Réception d'1 éther :

The screenshot shows the Etherscan website interface for a Ropsten Testnet transaction. The transaction details are as follows:

Field	Value
Transaction Hash	0xb9aef71b07043bd4b8a52732328d66324d31d0a67e14473ab4f4fd8be43f23c
Status	Success
Block	8636035 (3 Block Confirmations)
Timestamp	24 secs ago (Sep-07-2020 08:19:05 AM +UTC)
From	0x81b7e0865bd5648606c89998a9cc8164397647
To	0x7755414216938522c7dec813f143dbc0ad9dc849 (Adresse publique de mon portefeuille)
Value	1 Ether (\$0.00) (Montant transféré)
Transaction Fee	0.0000315 Ether (\$0.000000)

Below the transaction details, there is a note: "This website uses cookies to improve your experience and has an updated Privacy Policy. Got it."

f. Détail du bloc :

The screenshot shows the Etherscan website interface for a Ropsten Testnet block. The block details are as follows:

Field	Value
Block Height	8636035
Timestamp	1 hr 35 mins ago (Sep-07-2020 08:19:05 AM +UTC)
Transactions	7 transactions and 1 contract internal transaction in this block
Mined by	0xd34912efb0e7fedaed89390990d7ef023e0114fa in 11 secs
Block Reward	2.0034893365 Ether (2 + 0.0034893365)
Uncles Reward	0
Difficulty	552,816,284
Total Difficulty	31,436,515,898,201,997
Size	1,573 bytes
Gas Used	222,156 (2.80%)
Gas Limit	7,932,550
Extra Data	poolin.com (Hex: 0x706f6f5c596e2e636f5d)

Below the block details, there is a note: "This website uses cookies to improve your experience and has an updated Privacy Policy. Got it."

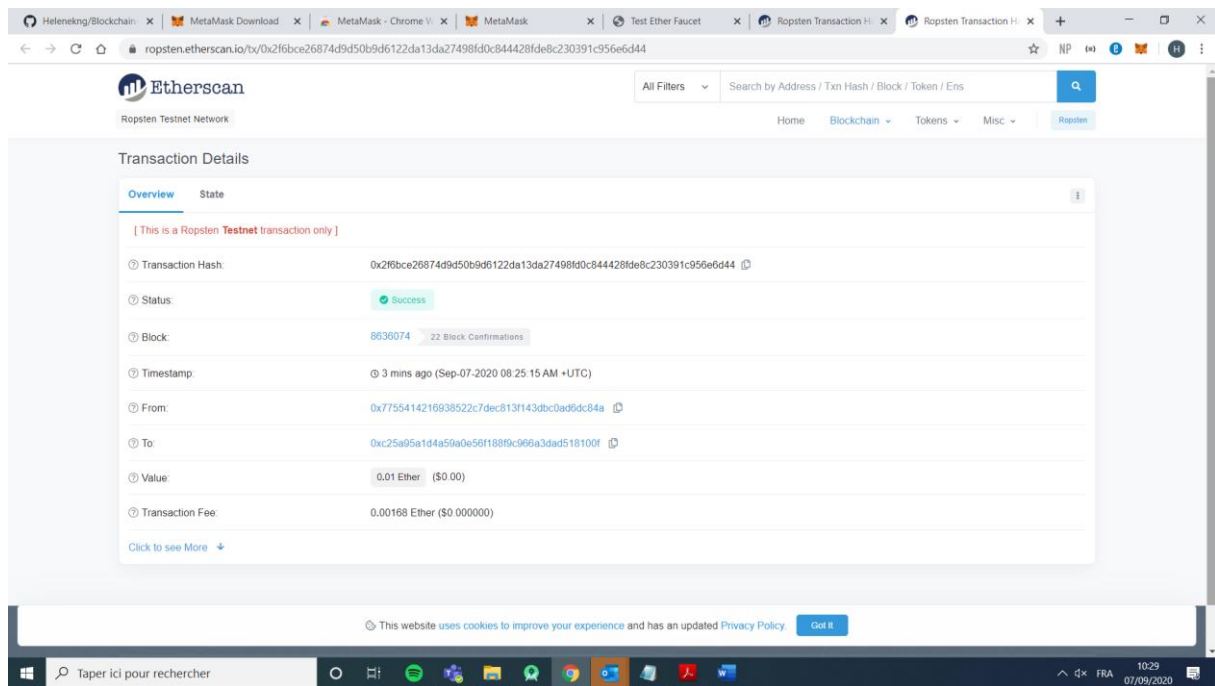
g. Envoie d'ethereum

The screenshot shows the MetaMask interface in a web browser. The top bar displays the MetaMask logo and the network 'Réseau de test Ropsten'. The main content area shows the account balance '6ETH' with a 'BUY' button and an 'ENVOYER' button. Below this, there is a section for 'File d'attente (1)' (Queue 1) with a transaction 'Envoyer des ETH' (Sending ETH) to '0xc25a...100f' with a status of 'En attente' (Waiting). The transaction history shows two 'Receive' transactions: one for 5 ETH from '0x78c1...ee78' and another for 1 ETH from '0x81b7...7647'.

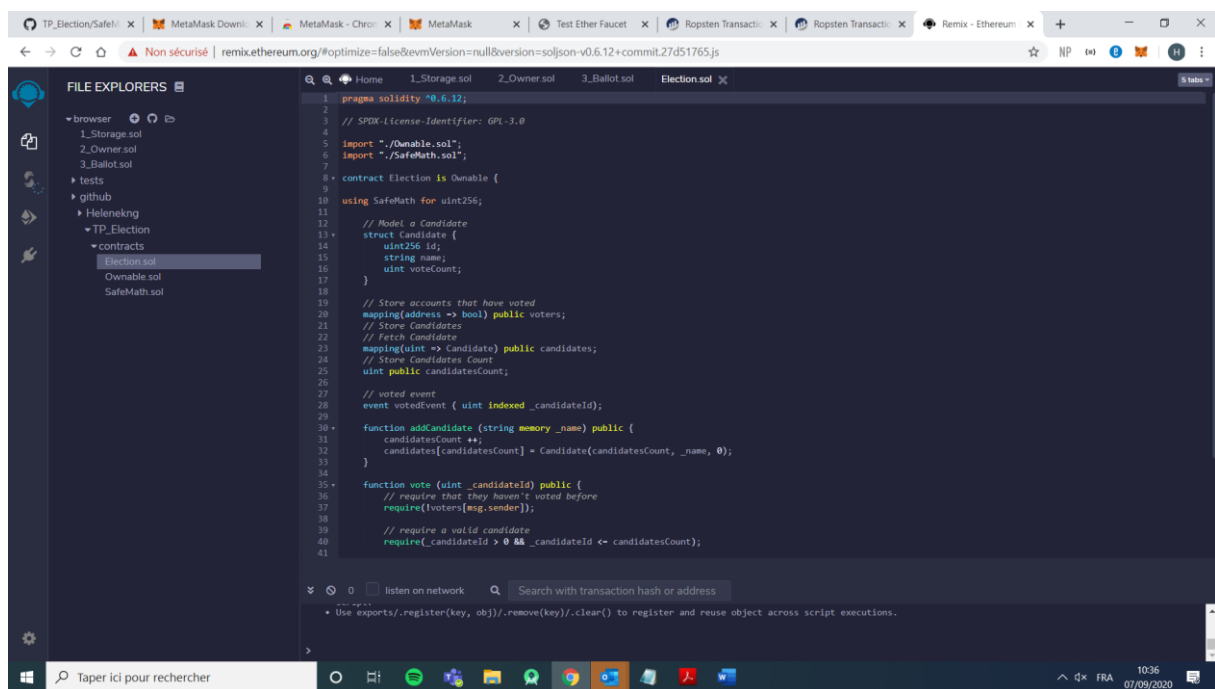
The screenshot shows the MetaMask interface with a transaction confirmation modal open. The modal is titled 'Envoyer des ETH' and displays the following details:

- Détails:** de: 0x77554142169385... > Destinataire: 0xc25a95...
- Transaction:**
 - Nonce: 0
 - Montant: 0.01 ETH
 - Quantité Max. De Gaz (Unités): 21000
 - Essence Utilisée (Unités): 21000
 - Prix du gaz (GWEI): 80
 - Total: 0.01168 ETH
- Log D'activité:**
 - Transaction créée avec une valeur de 0.01 ETH sur 10:25 on 9/7/2020.
 - Transaction envoyée sur 10:25 on 9/7/2020.
 - Transaction confirmée sur 10:26 on 9/7/2020.

The background interface shows the account balance and transaction history, with the 'Envoyer des ETH' transaction now listed in the history.



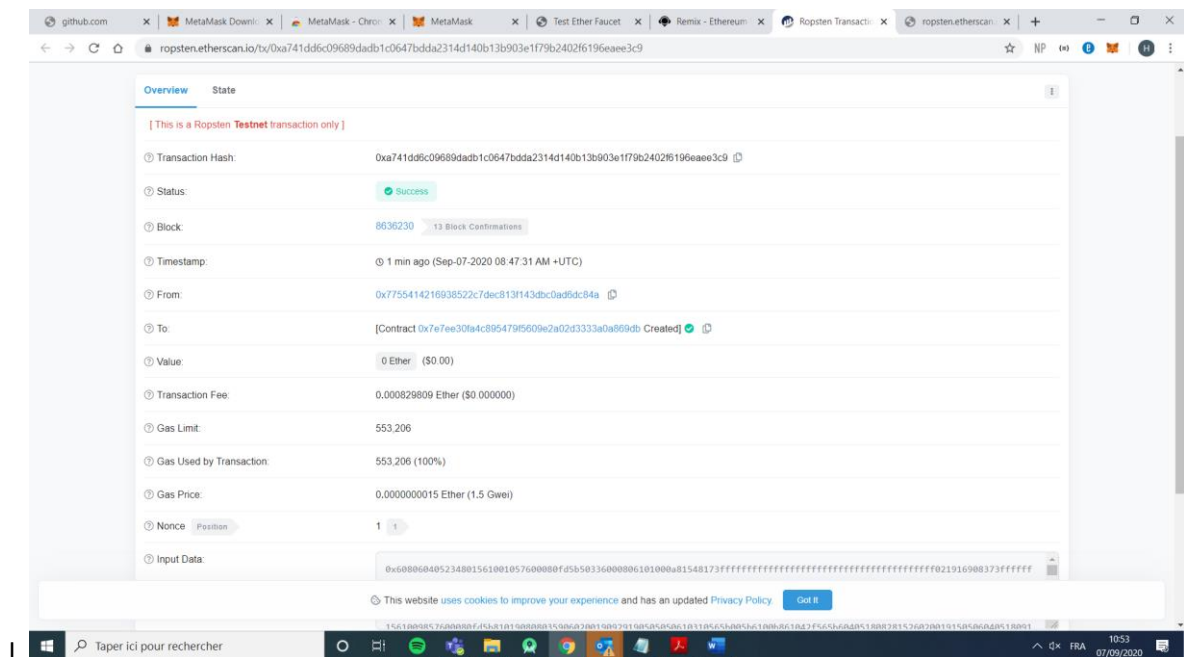
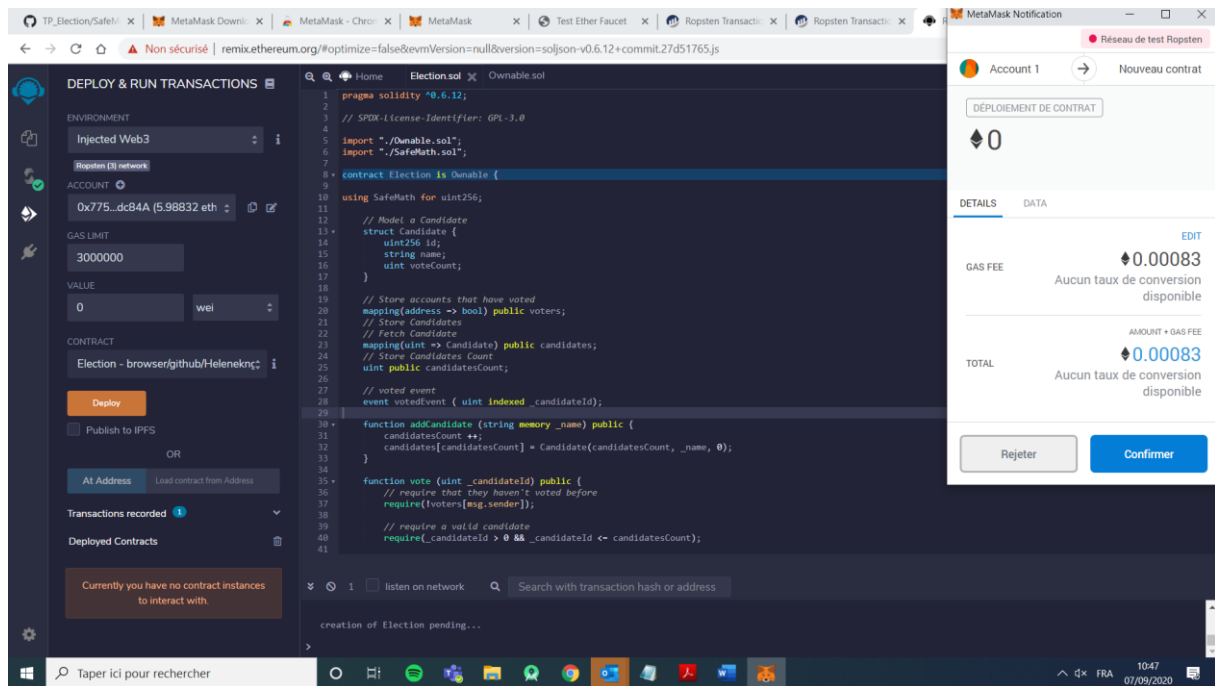
j.



k. Voir fichiers Election_ABI.json et Election_Bytecode.json :

https://github.com/Helenekng/Blockchain-TP2_smartcontract1

m. Déploiement du smart contract



m.

Les frais de transactions sont différents car ceux évoluent en fonction du nombre de transactions/de la saturation sur le réseau à l'instant T (voir ethereum.gasstation.org pour voir les frais à l'instant et estimer le bon moment, en fonction de la date de livraison également)

Adresse publique smartcontract : 0x7E7EE30Fa4c895479F5609e2a02d3333A0a869db

n. Add Candidates :

The screenshot shows the Remix IDE interface. On the left, the 'DEPLOY & RUN TRANSACTIONS' sidebar is visible, showing the 'addCandidate' function being executed. The main editor displays the Solidity code for the 'Election' contract. The code includes imports for 'SPDK-License-Identifier: GPL-3.0', 'Ownable.sol', and 'SafeMath.sol'. The contract 'Election' inherits from 'Ownable' and uses 'SafeMath' for 'uint256'. It defines a 'Candidate' struct with fields 'id', 'name', and 'voteCount'. The contract includes functions for 'addCandidate', 'vote', and 'candidates'. The 'addCandidate' function takes a 'memory_name' parameter and updates the 'candidates' array. The 'vote' function takes a 'candidateId' parameter and updates the 'voteCount' for the specified candidate. The 'candidates' function returns the list of candidates. The contract is deployed on the Ropsten Testnet, and the transaction details are shown at the bottom.

```

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
22     // Store Candidates
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
42         // record that voter has voted
43         voters[msg.sender] = true;
44     }
45 }

```

Transaction details: [block:863636 txIndex:2] from: 0x775...dc84A to: Election.addCandidate(string) 0x7e7...869db value: 0 wei data: 0x462...00000 logs: 0

The screenshot shows the Etherscan website interface. The 'Transaction Details' section is active, displaying the following information:

- Transaction Hash:** 0xf1bda56f82703d7f3c337273deee6c52652f948d15142596fc09d9c1b819e
- Status:** Success
- Block:** 863636 (3 Block Confirmations)
- Timestamp:** 32 secs ago (Sep-07-2020 09:02:19 AM +UTC)
- From:** 0x775414216938522c7dec813f143dbc0ad9dc848
- To:** Contract 0x7e7ee30fa4c895479f5609e2a02d3333a0a869db
- Value:** 0 Ether (\$0.00)
- Transaction Fee:** 0.000130005 Ether (\$0.000000)

Click to see More

p. CandidateID = 1 :

Heleneking/Blo... MetaMask Do... MetaMask - C... MetaMask Test Ether Fau... Remix - Ethere... Ropsten Trans... Ropsten Trans... Ropsten Trans...

Non sécurisé | remix.ethereum.org/#optimize=false&evmVersion=null&version=soljson-v0.6.12+commit.27d51765.js

DEPLOY & RUN TRANSACTIONS

At Address Load contract from Address

Transactions recorded 2

Deployed Contracts

ELECTION AT 0x7E7...8690B (BLOCKCHAIN)

addCandidate Kang

transferOwner... address newOwner

vote uint256 _candidateId

candidates 1

0: uint256 id 1

1: string name Kang

2: uint256 voteCount 0

candidatesCou...

owner

voters address

Low level interactions

Taper ici pour rechercher

```

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
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

```

uint256 candidatesCount 4 reference(s)

[call] from: 0x7755414216938522c7dec813f143dbc0ad9dc84a to: Election.candidates(uint256) data: 0x347...00001

Debug

listen on network Search with transaction hash or address

q. Ajout 2^{ème} candidat :

Heleneking/Blo... MetaMask Do... MetaMask - C... MetaMask Test Ether Fau... Remix - Ethere... Ropsten Trans... Ropsten Trans... Ropsten Trans... Ropsten Trans...

ropsten.etherscan.io/tx/0x4d61ce0515cb8f515dcb1b631155f853b0811937238d533cee9a105a7801cc04

Transaction Details

Overview State

[This is a Ropsten Testnet transaction only]

Transaction Hash: 0x4d61ce0515cb8f515dcb1b631155f853b0811937238d533cee9a105a7801cc04

Status: Success

Block: 8636457 1 Block Confirmation

Timestamp: 35 secs ago (Sep-07-2020 09:12:04 AM +UTC)

From: 0x7755414216938522c7dec813f143dbc0ad9dc84a

To: Contract 0x7ee30fa4c895479f5609e2a02d333a0a869db

Value: 0 Ether (\$0.00)

Transaction Fee: 0.000107523 Ether (\$0.000000)

Gas Limit: 73,165

Gas Used by Transaction: 71,682 (97.97%)

Gas Price: 0.000000015 Ether (1.5 Gwei)

Nonce: 3 12

This website uses cookies to improve your experience and has an updated Privacy Policy. Get it.

MethodID: 0x4d62e91ec

Taper ici pour rechercher

r. CandidateID : 2

The screenshot shows the Remix IDE interface. On the left, the 'DEPLOY & RUN TRANSACTIONS' panel is open, displaying the 'ELECTION AT 0x7E7...8690B (BLOCKCHAIN)' contract. The 'addCandidate' function is selected, and the 'candidates' array is visible with the following data:

- 0: uint256 id 2
- 1: string name Carus
- 2: uint256 voteCount 0

The 'candidatesCount' variable is also shown, with a value of 2. The 'owner' and 'voters' variables are also visible.

The main editor displays the Solidity code for the 'Election.sol' contract. The code defines a 'Candidate' struct and functions for adding candidates, voting, and managing the election. The 'vote' function is highlighted, showing the logic for recording a vote and updating the candidate's vote count.

s. Adresse propriétaire contrat = 0x7755414216938522c7dec813f143dbc0ad6dc84a (moi)

t. Vote :

The screenshot shows the Remix IDE interface with the 'Election.sol' contract. The 'vote' function is selected, and the 'candidates' array is visible with the following data:

- 0: uint256 id 2
- 1: string name Carus
- 2: uint256 voteCount 0

The 'candidatesCount' variable is also shown, with a value of 2. The 'owner' and 'voters' variables are also visible.

The main editor displays the Solidity code for the 'Election.sol' contract. The code defines a 'Candidate' struct and functions for adding candidates, voting, and managing the election. The 'vote' function is highlighted, showing the logic for recording a vote and updating the candidate's vote count.

On the right, a MetaMask notification window is open, showing a transaction confirmation. The transaction is labeled 'VOTE' and shows a gas fee of 0.000099 ETH. The total amount is 0.000099 ETH. The transaction is confirmed by the user.

The screenshot shows the Remix IDE interface. On the left, the 'DEPLOY & RUN TRANSACTIONS' sidebar is visible, showing options to 'Publish to IPFS' or 'At Address'. Below this, there are sections for 'Transactions recorded' and 'Deployed Contracts'. The main editor displays the Solidity code for the 'Election.sol' contract. The code includes a 'Candidate' struct, a 'voters' mapping, and functions for 'addCandidate', 'vote', and 'transferOwner'. The bottom console shows a transaction call: '[call] from: 0x7755414216938522c7dEC813F343d8c8ad6dc84A to: Election.candidates(uint256) data: 0x347...00001'.

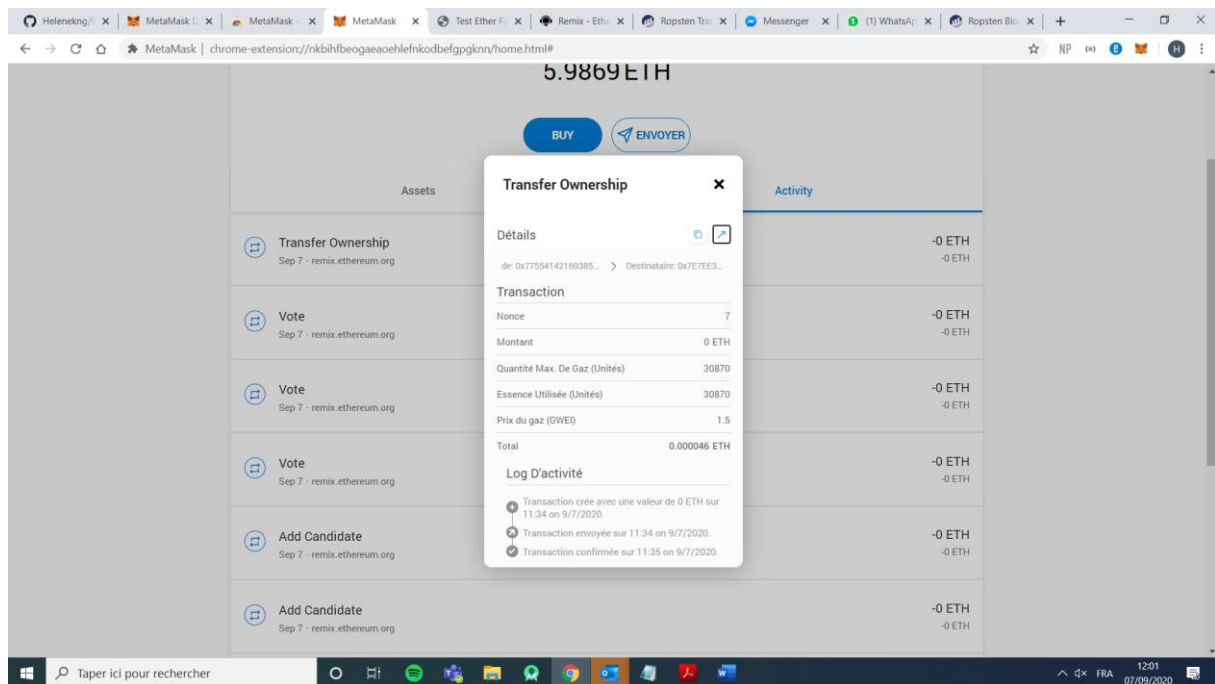
v. Vote sur le contrat d'un camarade :

This screenshot is similar to the first one, showing the Remix IDE interface. The left sidebar shows 'DEPLOY & RUN TRANSACTIONS' with options to 'Publish to IPFS' or 'At Address'. The main editor displays the Solidity code for the 'Election.sol' contract. The code includes a 'Candidate' struct, a 'voters' mapping, and functions for 'addCandidate', 'vote', and 'transferOwner'. The bottom console shows a transaction call: '[call] from: 0x7755414216938522c7dEC813F343d8c8ad6dc84A to: Election.candidates(uint256) data: 0x347...00001'.

w. Transfert de propriété à 0x542b817700C2A772E0DE966673fF6B5D39734677 :

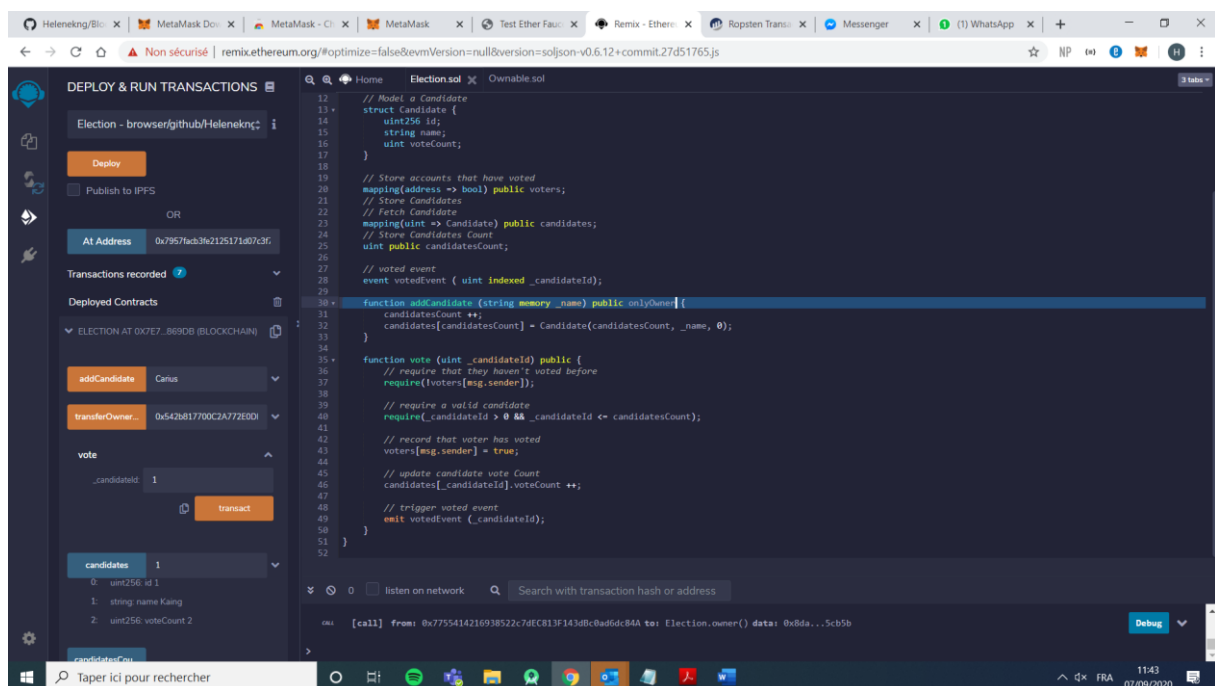
The screenshot shows the Remix IDE interface. On the left, the 'DEPLOY & RUN TRANSACTIONS' panel is active. Under 'Deployed Contracts', the 'ELECTION AT 0x7E7...869DB (BLOCKCHAIN)' is selected. The 'transferOwner' function is highlighted in the 'addCandidate' dropdown menu. The 'candidates' dropdown is set to '1'. The 'candidatesCount' dropdown is set to '1'. The 'candidates' list shows '0: uint256 id 1' and '1: string name Kang'. The 'candidatesCount' list shows '0: uint256 voteCount 2'. The 'transferOwner' transaction is being executed, with a tooltip showing 'transferOwnership - transaction (not payable)'. The main editor displays the Solidity code for the 'Election.sol' contract, which includes functions like 'addCandidate', 'vote', and 'transferOwner'. The bottom status bar shows the transaction details: '[call] from: 0x7755414216938522c7dEC813f343dc8ad6dc84A to: Election.owner() data: 0x8da...5cb5b'.

The screenshot shows the Remix IDE interface after the 'transferOwner' transaction has been executed. The 'transferOwner' function is now selected in the 'addCandidate' dropdown menu. The 'candidates' dropdown is set to '1'. The 'candidatesCount' dropdown is set to '1'. The 'candidates' list shows '0: uint256 id 1' and '1: string name Kang'. The 'candidatesCount' list shows '0: uint256 voteCount 2'. The 'transferOwner' transaction is now completed, and the 'owner' dropdown is set to '0: address: 0x542b817700C2A772E0DE966673fF6B5D39734677'. A tooltip shows 'Adresse publique du nouveau propriétaire'. The main editor displays the Solidity code for the 'Election.sol' contract, which includes functions like 'addCandidate', 'vote', and 'transferOwner'. The bottom status bar shows the transaction details: '[call] from: 0x7755414216938522c7dEC813f343dc8ad6dc84A to: Election.owner() data: 0x8da...5cb5b'.



x. De la même manière que la fonction `transferOwnership()`, on doit faire appel au modifier `onlyOwner`, présent `Ownable.sol`, dans la déclaration de la fonction.

y. Modification du code pour sécuriser la fonction `addCandidate` :



On recompile le contrat modifié, et on redéploie :

TP_Election x MetaMask x MetaMask x MetaMask x Test Ether x Remix - Eth x Ropsten Tru x Messenger x WhatsApp x Ropsten Blo x + -

MetaMask | chrome-extension://nkbihfboegaeaoehfknkodbefgpgknr/home.html#

Account 1
0x7755...c84A

5.986 ETH

BUY ENVOYER

Assets Activity

Déploiement de contrat Sep 7 · remix.ethereum.org	-0 ETH -0 ETH
Transfer Ownership Sep 7 · remix.ethereum.org	-0 ETH -0 ETH
Transfer Ownership Sep 7 · remix.ethereum.org	-0 ETH -0 ETH
Vote Sep 7 · remix.ethereum.org	-0 ETH -0 ETH
Vote	-0 ETH

Taper ici pour rechercher

TP_Election x MetaMask x MetaMask x MetaMask x Test Ether x Remix - E x Ropsten x Messenger x WhatsApp x Ropsten Blo x Ropsten Tru x + -

ropsten.etherscan.io/tx/0x1e4fa91b138568273bf408b66720bb402823db4b258ae13e5e9229c1b53ab3c6

Etherscan

Ropsten Testnet Network

All Filters Search by Address / Txn Hash / Block / Token / Ens

Home Blockchain Tokens Misc Ropsten

Transaction Details

Overview State

[This is a Ropsten Testnet transaction only]

Transaction Hash:	0x1e4fa91b138568273bf408b66720bb402823db4b258ae13e5e9229c1b53ab3c6
Status:	Success
Block:	8636930 3 Block Confirmations
Timestamp:	44 secs ago (Sep-07-2020 10:13:20 AM +UTC)
From:	0x7755414216938522c7dec813f143dbc0ad6dc84a
To:	[Contract 0xb595362555b3d8a1338fd504a40d089828e9cab Created]
Value:	0 Ether (\$0.00)
Transaction Fee:	0.000891714 Ether (\$0.000000)

Click to see More

This website uses cookies to improve your experience and has an updated Privacy Policy. Get It

Taper ici pour rechercher