

COMPTE RENDU DU TP 1

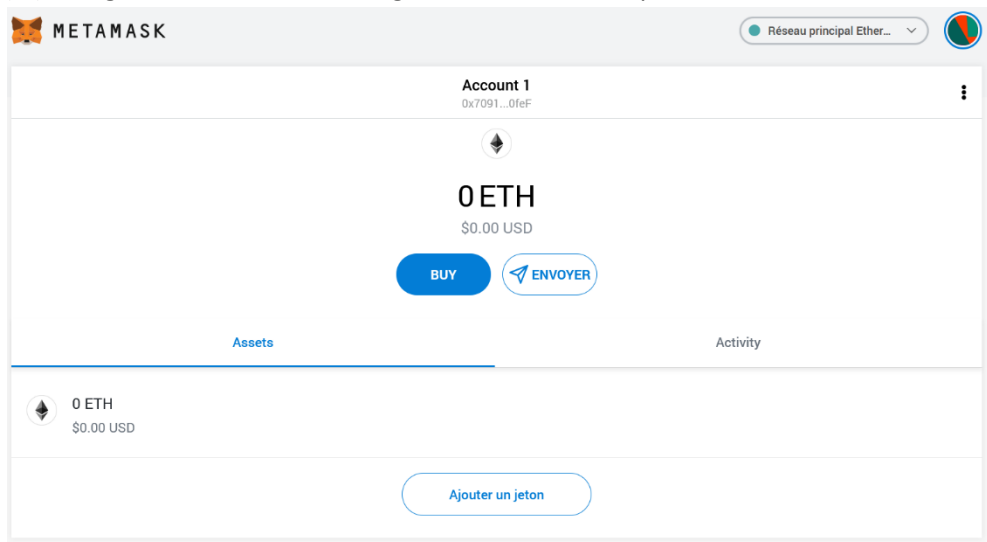
Nom : KASSI

Date : 07 / 09 /2020

Prénoms : Adjoua Paule Marcelle

1- Prise en main des outils Remix et Metamask

a) b) c) Navigation sur metamask et génération d'un compte



- Création d'Ether pour mon compte

MetaMask Ether Faucet

faucet

address: 0x81b7e08f65bdf5648606c89998a9cc8164397647

balance: 87798224.38 ether

request 1 ether from faucet

user

address: 0x70912d4f56112fd098577f6498e9bb03a2ca0fef

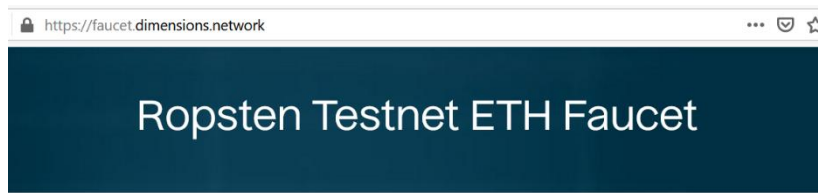
balance: 3.00 ether

donate to faucet:

1 ether

10 ether

100 ether



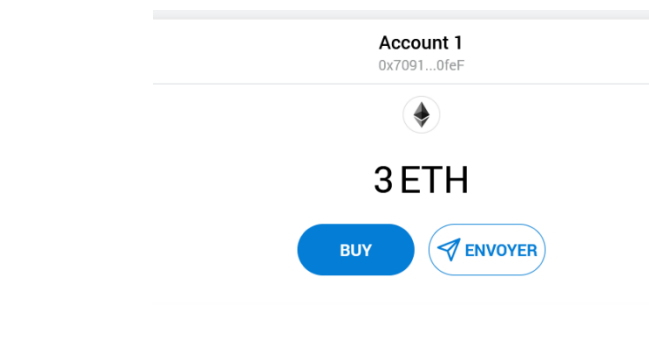
Enter Your Ropsten Address

0x70912D4F56112FD098577F6498E9Bb03a2cA0feF

Send Ropsten ETH

3971729 ETH left in Faucet. Gas Limit 400k

d) Le nombre des premiers ethers obtenus:



e) Transaction d'obtention d'ether

Transaction Details	
Overview	State
[This is a Ropsten Testnet transaction only]	
Transaction Hash:	0xb045f943b377b8f6254760178c428653cd8479125273829773d171868da9e26c
Status:	Success
Block:	8636025 19 Block Confirmations
Timestamp:	⌚ 3 mins ago (Sep-07-2020 08:17:51 AM +UTC)
From:	0x81b7e08f65bdf5648606c89998a9cc8164397647
To:	0x70912d4f56112fd098577f6498e9bb03a2ca0fef
Value:	1 Ether (\$0.00)
Transaction Fee:	0.0000315 Ether (\$0.000000)
Click to see More	

f) Détails du bloc de la transaction précédente

Block #8636025

Overview

[This is a Ropsten Testnet block only]

Block Height:

8636025 < >

Timestamp:

4 mins ago (Sep-07-2020 08:17:51 AM +UTC)

Transactions:

13 transactions and 7 contract internal transactions in this block

Mined by:

0xd34912efb0e7fedaedb9390990d7ef623e01f4fa in 6 secs

Block Reward:

2.024766875 Ether (2 + 0.024766875)

Uncles Reward:

0

Difficulty:

551,199,604

Total Difficulty:

31,436,510,377,856,311

g) Génération de la première transaction

Envoyer des ETHAnnuler

✓ 0xc25a...100F

X

Nouvelle adresse détectée ! Cliquez ici pour ajouter à votre carnet d'adresses.

Actif:

ETH

Balance:: 3 ETH

Montant:

1 | ETH

Aucun taux de conversion disponible

Max

Frais de transaction:

Prix du gaz (GWEI)

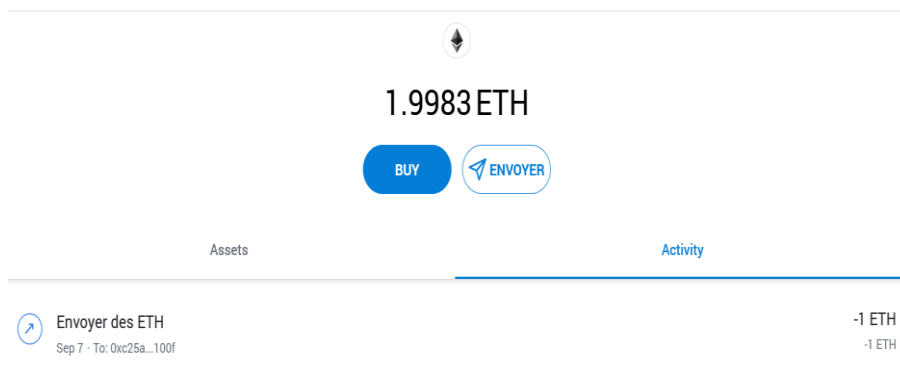
Quantité max. de gaz

81

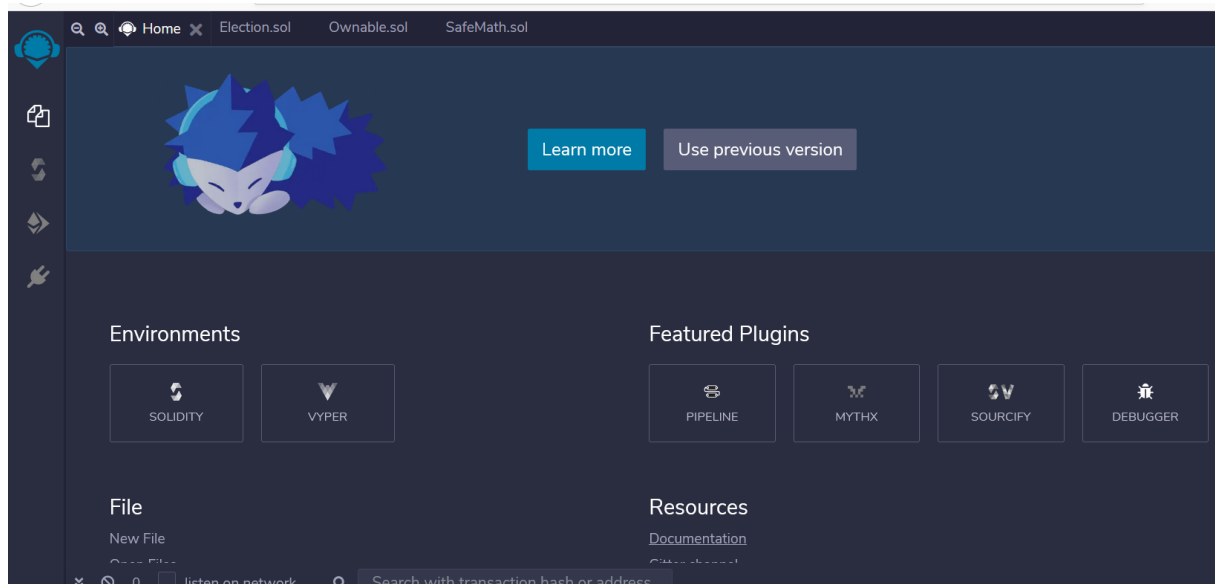
21000

Annuler

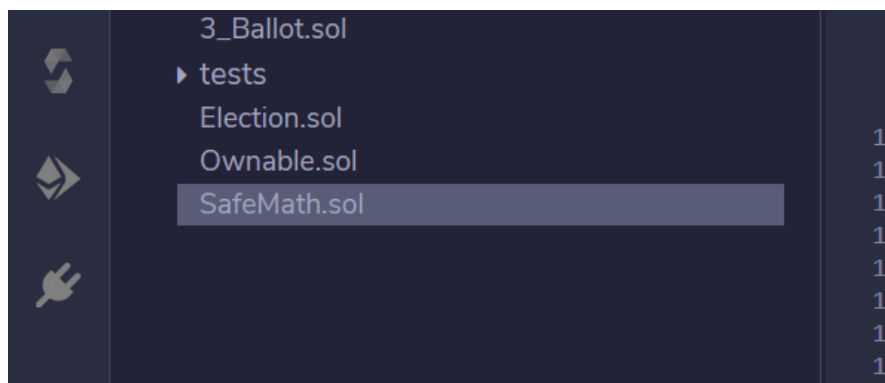
Suivant



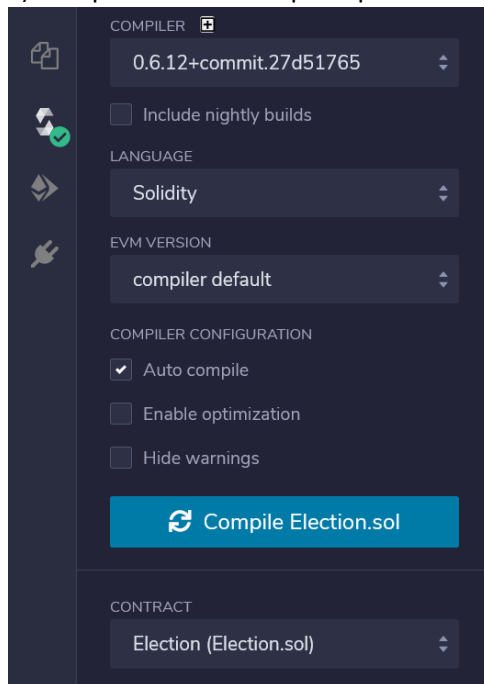
h) IDE Remix



- i) Et j) Récupération du code source et importation dans l'IDE



k) Compilation du code principal Election.sol



The screenshot shows the Solidity compiler interface with the following settings:

- COMPILER:** 0.6.12+commit.27d51765
- ☐ Include nightly builds
- LANGUAGE:** Solidity
- EVM VERSION:** compiler default
- COMPILER CONFIGURATION:**
 - ☒ Auto compile
 - ☐ Enable optimization
 - ☐ Hide warnings
- Compile Election.sol** (button)
- CONTRACT:** Election (Election.sol)

Génération de l' 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": [
```

Génération du Bytecode

```
{
  "linkReferences": {},
  "object": "608060405234801561001057600080fd5b50336000806101000a81546
  "opcodes": "PUSH1 0x80 PUSH1 0x40 MSTORE CALLVALUE DUP1 ISZERO PUSH2
  "sourceMap": "120:1190:0:-:0;,,,,,,579:10:1;571:5;,:18;,,,,,,;"
}
```

I) Déploiement

Les étapes :

- choix de Inject Web3
- Connexion a Ropsten Test Network

The screenshot displays the Remix IDE interface. On the left, the 'DEPLOY & RUN TRANSACTIONS' sidebar is active, showing the 'ENVIRONMENT' set to 'Injected Web3' and the 'ACCOUNT' as '0x709...A0feF (6.998299 ether)'. The 'GAS LIMIT' is set to 3000000, and the 'VALUE' is 0 wei. The 'CONTRACT' dropdown shows 'Election - browser/Election.sol'. The 'Deploy' button is highlighted. On the right, the 'Election.sol' file is open, showing Solidity code for a voting system. The code includes a 'Candidate' struct, a 'voters' mapping, and functions for adding candidates and voting. The bottom right shows a 'MetaMask' overlay displaying the account balance of 6.9983 ETH and a list of transactions.

- Détail de la transaction

Transaction Details

[Overview](#) [State](#)

[This is a Ropsten **Testnet** transaction only]

Transaction Hash:	0x774e5059c93969ddd94814594a24754d294fda6ae21aac8a25c88fd63a16bb33
Status:	Success
Block:	8636228 6 Block Confirmations
Timestamp:	33 secs ago (Sep-07-2020 08:47:22 AM +UTC)
From:	0x70912d4f56112fd098577f6498e9bb03a2ca0fef
To:	[Contract 0x48df149f8c7de8e9f02a59dce9e3243f0febbc22 Created]
Value:	0 Ether (\$0.00)
Transaction Fee:	0.000829809 Ether (\$0.000000)

[Click to see More](#)

m)

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	1
Input Data:	<div>0x608060405234801561001057600080fd5b5033600080610100a81548173fff021916908373fff1602179055506108ab806100606000396000f3fe08060405234801561001057600080fd5b506004361061007d5760003560e01c8063462e91ec1161005b578063462e91ec146101835780638da5cb5b1461023e578063a3ec138d14610272578063f2fde38b146102cc5761007d565b80630121b93f146100825780632d35a8a2146100b05780633477ee2e146100ce575b600080fd5b6100ae6004803603602081101561009857600080fd5b81019080803590602001909291905050506</div> <div>View Input As</div>

Mes frais de transactions sont de 0 .000829809 Ether tandis que les vôtres sont d'environ 0.0024 Ether. En effet cette différence est due au trafic sur le réseau. Vous étiez probablement seul sur votre réseau lors de la création de votre contrat. Tandis que moi je suis sur le même réseau que mes autres collègues et ça coûte plus cher.

Adresse publique du Smart Contract : [0x48df149f8c7de8e9f02a59dce9e3243f0febbc22](#)

Transaction Hash:	0x774e5059c93969ddd94814594a24754d294fda6ae21aac8a25c88fd63a16bb33
Status:	Success
Block:	8636228 6 Block Confirmations
Timestamp:	33 secs ago (Sep-07-2020 08:47:22 AM +UTC)
From:	0x70912d4f56112fd098577f6498e9bb03a2ca0fef
To:	[Contract 0x48df149f8c7de8e9f02a59dce9e3243f0febbc22 Created]
Value:	0 Ether (\$0.00)
Transaction Fee:	0.000829809 Ether (\$0.000000)

n) Création du premier candidat

ELECTION AT 0X48D...BBC22 (BLOCKCHAIN)

addCandidate

KASSI

transferOwner...

address newOwner

vote

uint256 _candidateId

candidates

uint256

```



1 pragma solidity ^0.4.12;
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

```

Add Candidate

Sep 7 · remix.ethereum.org

-0 ETH
-0 ETH

② To: Contract [0x48df149f8c7de8e9f02a59dce9e3243f0febbc22](#)  

② Value: 0 Ether (\$0.00)

② Transaction Fee: 0.000107505 Ether (\$0.000000)

② Gas Limit: 73,153

② Gas Used by Transaction: 71,670 (97.97%)

② Gas Price: 0.0000000015 Ether (1.5 Gwei)

② Nonce Position 5 11

② Input Data:

```
Function: addCandidate(string name) ***

MethodID: 0x462e91ec
[0]: 0000000000000000000000000000000000000000000000000000000000000020
[1]: 0000000000000000000000000000000000000000000000000000000000000005
[2]: 4b4153534900000000000000000000000000000000000000000000000000000000
```

p) CandidateID

candidates 1

0: uint256: id 1

1: string: name KASSI

2: uint256: voteCount 0

q) Autre candidat

② Transaction Fee: 0.000107505 Ether (\$0.000000)

② Gas Limit: 73,153

② Gas Used by Transaction: 71,670 (97.97%)


② Gas Price: 0.0000000015 Ether (1.5 Gwei)

② Nonce Position 7 4

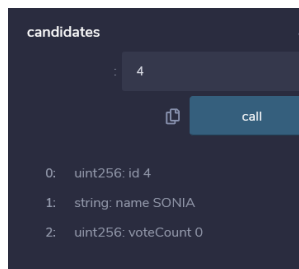
② Input Data:

```
Function: addCandidate(string name) ***

MethodID: 0x462e91ec
[0]: 0000000000000000000000000000000000000000000000000000000000000020
[1]: 0000000000000000000000000000000000000000000000000000000000000005
[2]: 536f6e696100000000000000000000000000000000000000000000000000000000
```

[View Input As](#) 

r) Affichage d'un autre candidat



s) Adresse du propriétaire du contrat : [0x70912d4f56112fd098577f6498e9bb03a2ca0fef](https://etherscan.io/address/0x70912d4f56112fd098577f6498e9bb03a2ca0fef)

t) Vote d'un candidat

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	9 14
Input Data:	<div>Function: vote(uint256 proposal) *** MethodID: 0x0121b93f [0]: 0001</div> <div>View Input As</div>

Transaction Details

[Overview](#) [State](#)

[This is a Ropsten **Testnet** transaction only]

Transaction Hash:	0x774e5059c93969ddd94814594a24754d294fda6ae21aac8a25c88fd63a16bb33 📋
Status:	✓ Success
Block:	8636228 467 Block Confirmations
Timestamp:	🕒 57 mins ago (Sep-07-2020 08:47:22 AM +UTC)
From:	0x70912d4f56112fd098577f6498e9bb03a2ca0fef 📋
To:	[Contract 0x48df149f8c7de8e9f02a59dce9e3243f0febbc22 Created] ✓ 📋
Value:	0 Ether (\$0.00)
Transaction Fee:	0.000829809 Ether (\$0.000000)

[Click to see More](#) ↓

u)

candidates

1

▼

0: uint256: id 1

1: string: name KASSI

2: uint256: voteCount 1

v) l'adresse du contrat de Sonia est : [0x8f3a4bef616c81e78f1a5c4b7cad413ce907e02e](#)

From:	0x70912d4f56112fd098577f6498e9bb03a2ca0fef
To:	Contract 0x8f3a4bef616c81e78f1a5c4b7cad413ce907e02e
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	Position 10
Input Data:	<p>Function: vote(uint256 proposal) ***</p> <p>MethodID: 0x0121b93f</p>

ELECTION AT 0X8F3...7E02E (BLOCKCHAIN)

addCandidate

string _name

transferOwner...

address newOwner

vote

1

candidates

uint256

candidatesCou...

owner

voters

address




Low level interactions

w) Transfert de la propriété

Transfer Ownership

Sep 7 · remix.ethereum.org

-0 ETH
-0 ETH

Timestamp:	38 secs ago (Sep-07-2020 10:13:20 AM +UTC)
From:	0x70912d4f56112fd098577f6498e9bb03a2ca0fef 
To:	Contract 0x48df149f8c7de8e9f02a59dce9e3243f0febbc22  
Value:	0 Ether (\$0.00)
Transaction Fee:	0.000046305 Ether (\$0.000000)
Gas Limit:	30,870
Gas Used by Transaction:	30,870 (100%)
Gas Price:	0.0000000015 Ether (1.5 Gwei)
Nonce Position	11 9
Input Data:	<div> Function: transferOwnership(address newOwner) *** MethodID: 0xf2fde38b [0]: 000000000000000000000000c1c015aa59303363a8238200c630a28b1ffff395 </div>

x) Pour sécuriser la méthode `addCandidate` nous pouvons ajouter la propriété « `onlyOwner` » pour qu'il n'y ai que le propriétaire du contrat qui puisse appeler la méthode.

y) Modification du code
(Voir le code `Election.sol` sur github)