

RAPPORT TP1

a. b.



Confirmez votre phrase mnémotechnique

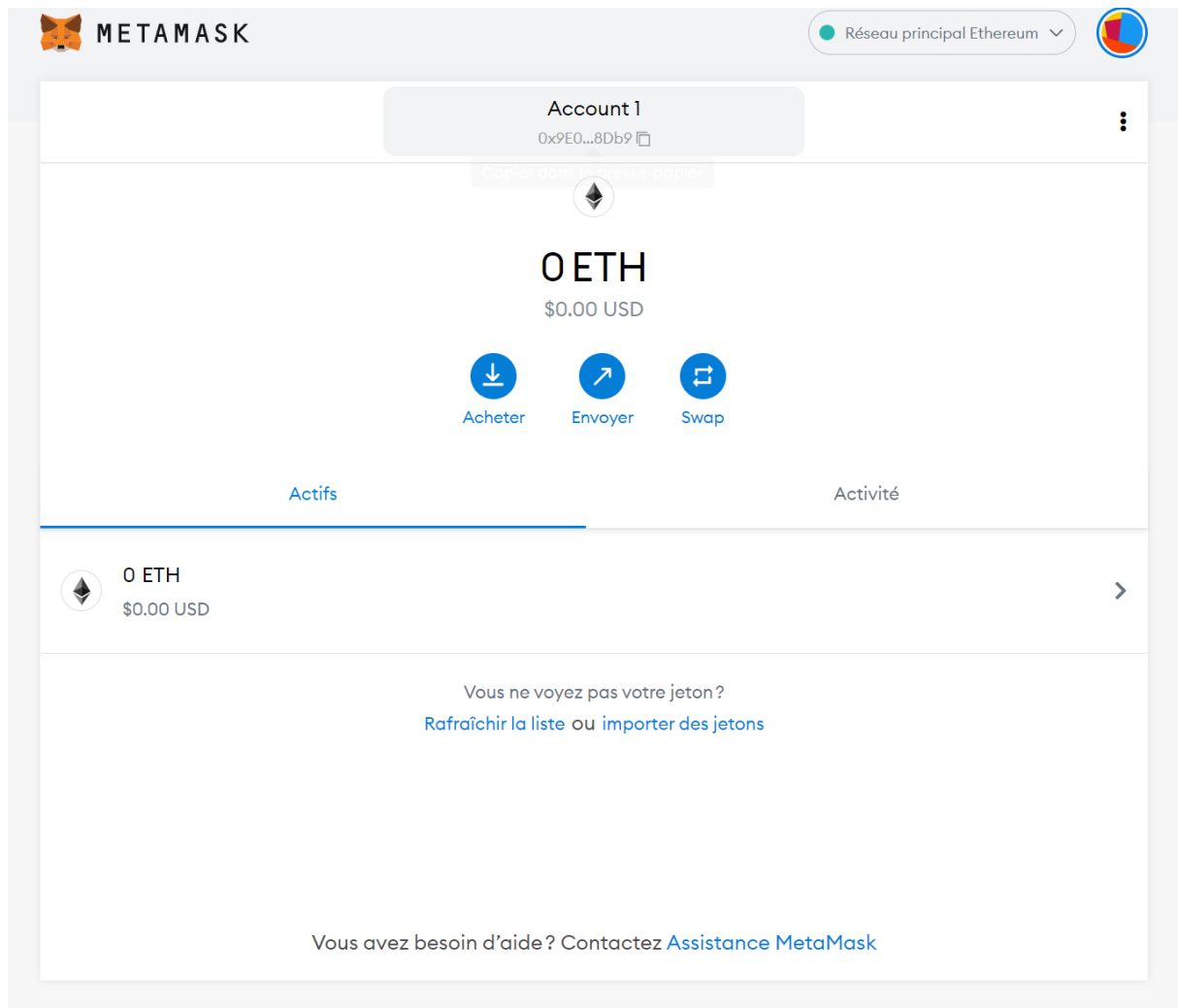
Veuillez sélectionner chaque phrase afin de vous assurer qu'elle est correcte.

oak	frog	upgrade	guard
uphold	few	client	wonder
mention	task	budget	spell

budget	client	few	frog
guard	mention	oak	spell
task	upgrade	uphold	wonder

Confirmer

c.



d.

MetaMask Ether Faucet

faucet

address: 0x81b7e08f65bdf5648606c89998a9cc8164397647
balance: 81144371.40 ether
request 1 ether from faucet

user

address: 0x9e0bbac92816133e231805e9427fdd8b7c868db9
balance: 0.00 ether
donate to faucet:

1 ether10 ether100 ether

transactions

e.

Transaction Details

Overview

State

[This is a Ropsten Testnet transaction only]

Transaction Hash:

0xd2eaf55ca6e04b91c9be3170d35ef0c6105ca33c76404fc25537cd6a2ec282b5

Status:

Success

Block:

121296612950 Block Confirmations

Timestamp:

1 day 18 mins ago (Mar-24-2022 12:21:30 PM +UTC)

From:

0x533fb0469d523dfd5bf3d97e0ad75ea66328d08e

To:

0x9e0bbac92816133e231805e9427fd8b7c868db9

Value:

0.1 Ether (\$0.00)

Transaction Fee:

0.001520763707127 Ether (\$0.00)

Gas Price:

0.000000072417319387 Ether (72.417319387 Gwei)

Click to see More

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

f. Numéro de block : [12129661](#)

Etherscan

Ropsten Testnet Network

All Filters

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

HomeBlockchainTokensMisc

Block #12129661

Overview

[This is a Ropsten Testnet block only]

Block Height:

12129661

Timestamp:

1 day 27 mins ago (Mar-24-2022 12:21:30 PM +UTC)

Transactions:

22 transactions and 117 contract internal transactions in this block

Mined by:

0x169d07d5c0703733aa505008e9627577c087eb63 in 74 secs

Block Reward:

2.740187147475936741 Ether (2 + 0.740939374077385085 - 0.000752226601448344)

Uncles Reward:

0

Difficulty:

27,569,595,689

Total Difficulty:

40,853,860,416,674,391

Size:

28,714 bytes

Gas Used:

7,990,534 (99.88%) +100% Gas Target

Gas Limit:

8,000,000

Base Fee Per Gas:

0.000000000094139716 Ether (0.094139716 Gwei)

g.

[< Modifier](#)

Réseau de test Ropsten

Account 1 → Prof

ENVOI DE ETH

0.000001

MODIFIER

Frais de carburant estimés

0.00110809

0.001108 ETH

Probablement dans < 30 secondes

Frais maximaux: 0.00137276 ETH

Total

0.00111809

0.00111809 ETH

Montant + frais de carburant

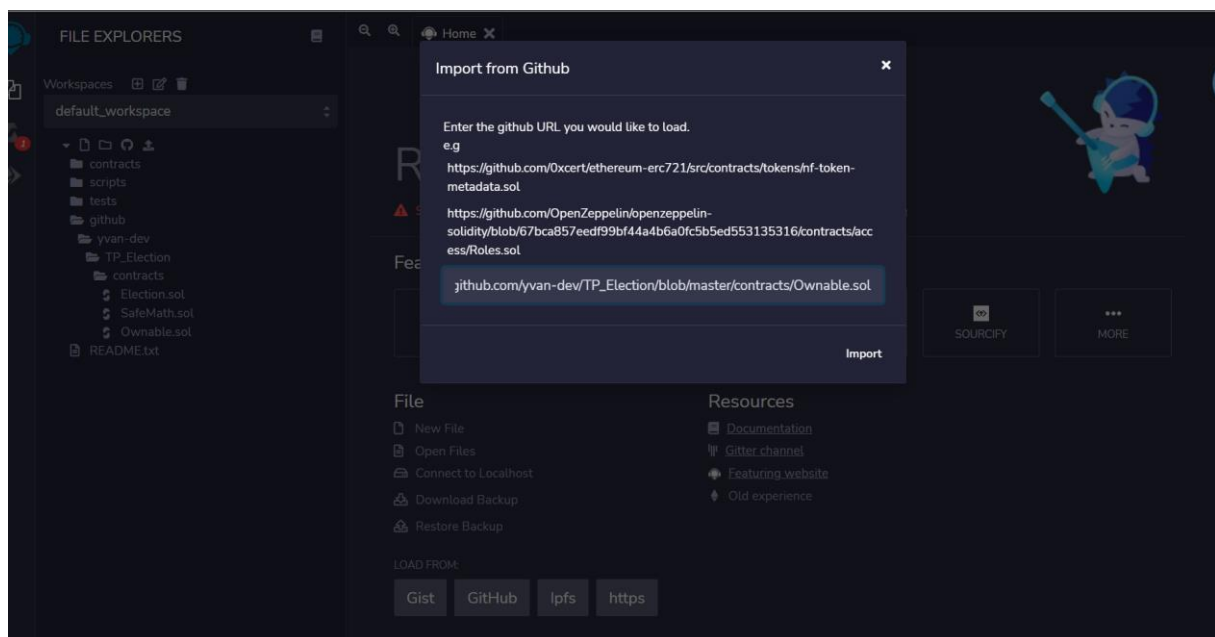
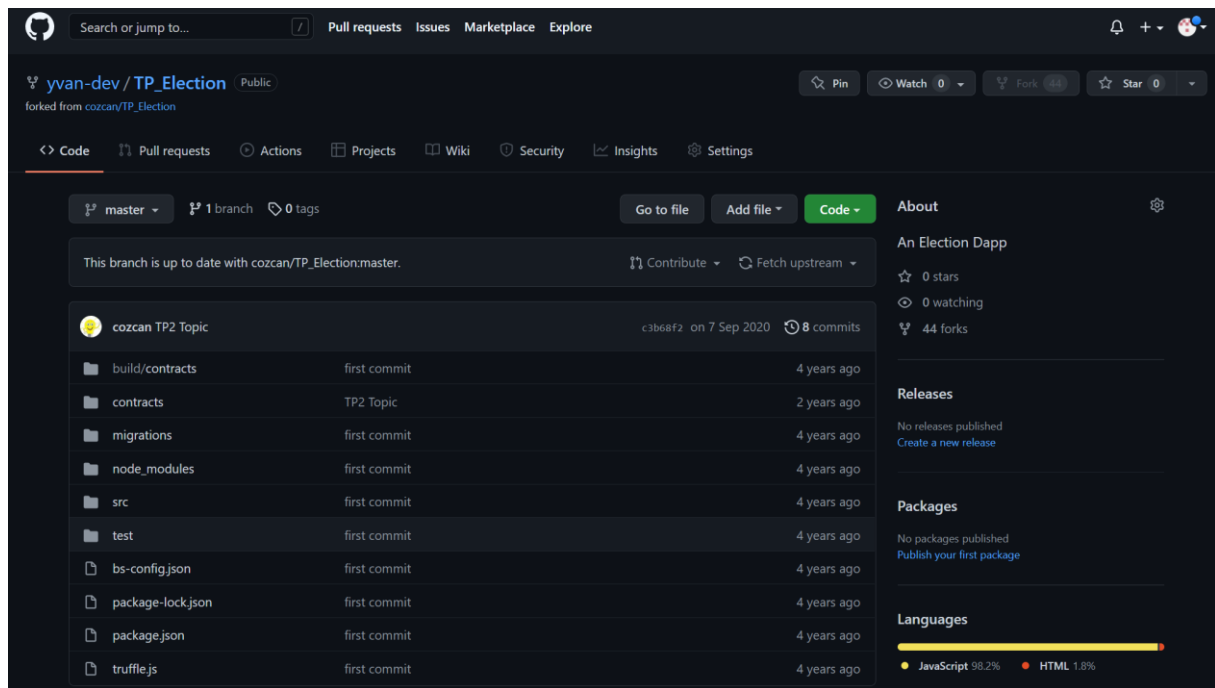
Montant maximal: 0.00138276 ETH

Rejeter





Confirmer

h. i. j.

Fork du projet sur mon compte GitHub et ajout des fichiers sur Remix.



k. Fichiers byte code et ABI sur le github [yvan-dev/TP Election: An Election Dapp](https://github.com/yvan-dev/TP_Election) (github.com)




DEPLOY & RUN TRANSACTIONS

ENVIRONMENT

JavaScript VM (London)

VM

ACCOUNT 

0x5B3...eddC4 (100 ether)

GAS LIMIT

3000000

VALUE

0 Wei

CONTRACT

Election - Election.sol

Deploy

☐ Publish to IPFS

OR

At Address Load contract from Address

Transactions recorded 0

Deployed Contracts

Currently you have no contract instances to interact with.

m. L'adresse public du smart contract : 0xd9145CCE52D386f254917e481eB44e9943F39138

✓ [vm] from: 0x5B3...eddC4 to: Election.(constructor) value: 0 wei data: 0x608...c0033 logs: 0 hash: 0xe22...1ecf5

creation of Election pending...

Debug ▼

✓ [vm] from: 0x5B3...eddC4 to: Election.(constructor) value: 0 wei data: 0x608...c0033 logs: 0 hash: 0x657...40f1a

Debug ▲

status	true Transaction mined and execution succeed
transaction hash	0x6578c5523e9086018e42d917da66f80a1db9b0b1155c76f73260f907ee140f1a
from	0x5B38Da6a701c568545dCfcB03FcB875f56beddC4
to	Election.(constructor)
gas	80000000 gas
transaction cost	554494 gas
execution cost	554494 gas
input	0x608...c0033
decoded input	{}
decoded output	-
logs	[]
val	0 wei

n.

Transactions recorded 1

Deployed Contracts

ELECTION AT 0XD91...39138 (MEMOIF)

addCandidate

GUNEWOU TAKAM

transferOwner...

address newOwner

vote

uint256 _candidateId

candidates

uint256

candidatesCou...

owner

voters

address

Low level interactions

CALLDATA

Transact

o.

✓

[vm] from: 0x5B3...eddC4 to: Election.addCandidate(string) 0xd91...39138 value: 0 wei data: 0x462...00000 logs: 0 hash: 0x107...2c22e

Debug

^

status	true Transaction mined and execution succeed
transaction hash	0x1078e5aaae75b77825617c514155c7e2a969687abea01f305b6c3c805912c22e 🔗
from	0x5B38Da6a701c568545dCfcB03FcB875f56beddC4 🔗
to	Election.addCandidate(string) 0xd9145CCE52D386f254917e481e844e9943F39138 🔗
gas	80000000 gas 🔗
transaction cost	91466 gas 🔗
execution cost	91466 gas 🔗
input	0x462...00000 🔗
decoded input	<pre>{ "string _name": "GUNEWOU TAKAM" }</pre> 🔗
decoded output	<pre>{}</pre> 🔗
logs	<pre>[]</pre> 🔗 🔗
val	0 wei 🔗

p.

call [call] from: 0x5B38Da6a701c568545dCfcB03FcB875f56beddC4 to: Election.candidates(uint256) data: 0x347...00001

Debug

^

from	0x5B38Da6a701c568545dCfcB03FcB875f56beddC4 🔗
to	Election.candidates(uint256) 0xd9145CCE52D386f254917e481e844e9943F39138 🔗
execution cost	28814 gas (Cost only applies when called by a contract) 🔗
input	0x347...00001 🔗
decoded input	<pre>{ "uint256 ": "1" }</pre> 🔗
decoded output	<pre>{ "0": "uint256: id 1", "1": "string: name GUNEWOU TAKAM", "2": "uint256: voteCount 0" }</pre> 🔗
logs	<pre>[]</pre> 🔗 🔗

q.

[vm] from: 0x5B3...eddC4 to: Election.addCandidate(string) 0xd91...39138 value: 0 wei data: 0x462...00000 logs: 0 hash: 0xc5c...a33a8
Debug ^

status	true Transaction mined and execution succeed
transaction hash	0xc5cb46b9ce31bafef721c5469c721d75154949782f9cc137fff0f22e7aa33a8
from	0x5B38Da6a701c568545dCfcB03FcB875f56beddC4
to	Election.addCandidate(string) 0xd9145CCE52D386f254917e481eB44e9943F39138
gas	80000000 gas
transaction cost	74258 gas
execution cost	74258 gas
input	0x462...00000
decoded input	{ "string _name": "Yvan" }
decoded output	{}
logs	[]
val	0 wei

r.

CALL [call] from: 0x5B38Da6a701c568545dCfcB03FcB875f56beddC4 to: Election.candidates(uint256) data: 0x347...00002
Debug ^

from	0x5B38Da6a701c568545dCfcB03FcB875f56beddC4
to	Election.candidates(uint256) 0xd9145CCE52D386f254917e481eB44e9943F39138
execution cost	28814 gas (Cost only applies when called by a contract)
input	0x347...00002
decoded input	{ "uint256 ": "2" }
decoded output	{ "0": "uint256: id 2", "1": "string: name Yvan", "2": "uint256: voteCount 0" }
logs	[]

s. Adresse du propriétaire du contrat : 0x5B38Da6a701c568545dCfcB03FcB875f56beddC4

CALL [call] from: 0x5B38Da6a701c568545dCfcB03FcB875f56beddC4 to: Election.owner() data: 0x8da...5cb5b
Debug ^

from	0x5B38Da6a701c568545dCfcB03FcB875f56beddC4
to	Election.owner() 0xd9145CCE52D386f254917e481eB44e9943F39138
execution cost	23430 gas (Cost only applies when called by a contract)
input	0x8da...5cb5b
decoded input	{}
decoded output	{ "0": "address: 0x5B38Da6a701c568545dCfcB03FcB875f56beddC4" }
logs	[]

t.

```

[vm] from: 0x5B3...eddc4 to: Election.vote(uint256) 0xd91...39138 value: 0 wei data: 0x012...00001 logs: 1 hash: 0xf2f...84da1
status true Transaction mined and execution succeed
transaction hash 0xf2f4d8ad3d4b7757994095b2d55ebb474780c1e505209d2546301c95ea384da1
from 0x5B38Da6a701c568545dCfcB03FcB875f56beddC4
to Election.vote(uint256) 0xd9145CCE52D386f254917e481eB44e9943F39138
gas 80000000 gas
transaction cost 69467 gas
execution cost 69467 gas
input 0x012...00001
decoded input {
  "uint256 _candidateId": "1"
}
decoded output {}
logs [
  {
    "from": "0xd9145CCE52D386f254917e481eB44e9943F39138",
    "topic": "0xffff3c900d938d21d0990d786e819f29b8d05c1ef587b462b939609625b684b16",
    "event": "votedEvent",
    "args": {
      "0": "1",
      "_candidateId": "1"
    }
  }
]

```

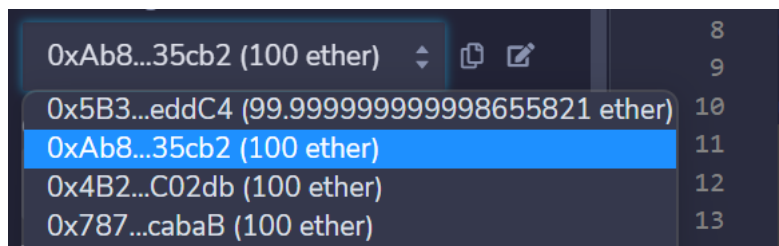
u. voteCount = 1

```

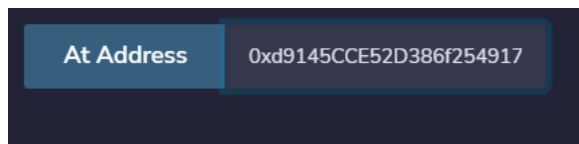
CALL [call] from: 0x5B38Da6a701c568545dCfcB03FcB875f56beddC4 to: Election.candidates(uint256) data: 0x347...00001
from 0x5B38Da6a701c568545dCfcB03FcB875f56beddC4
to Election.candidates(uint256) 0xd9145CCE52D386f254917e481eB44e9943F39138
execution cost 28814 gas (Cost only applies when called by a contract)
input 0x347...00001
decoded input {
  "uint256 ": "1"
}
decoded output {
  "0": "uint256: id 1",
  "1": "string: name GUNEWOU TAKAM",
  "2": "uint256: voteCount 1"
}
logs []

```

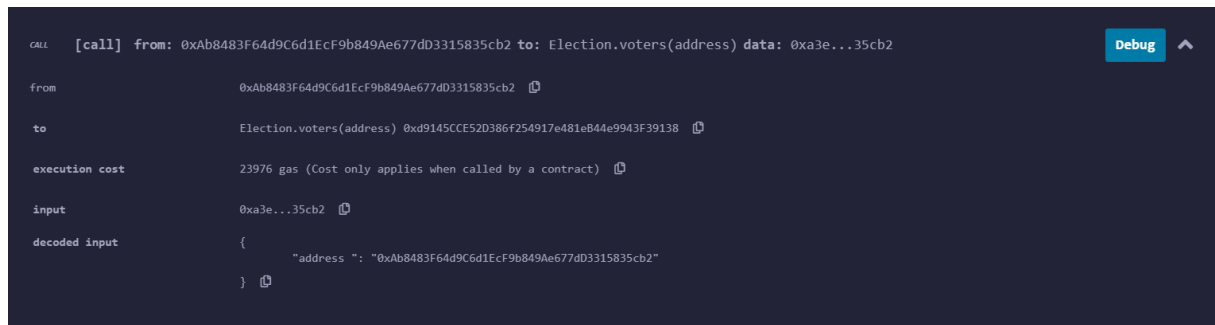
v. On change de compte sur remix



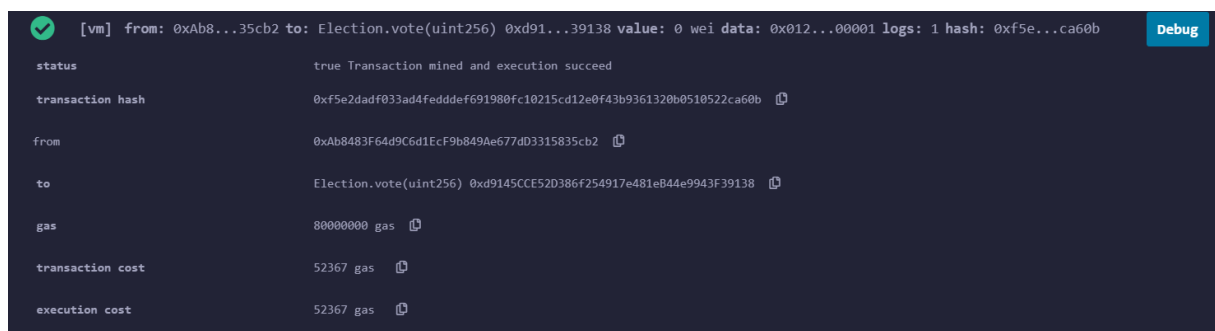
On passe l'adresse publique du smart contract



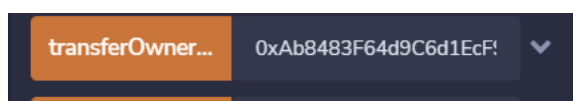
On change de votant



On utilise la fonction vote pour voter avec le nouveau votant



w. On reviens sur le compte propriétaire et on passe l'adresse publique du deuxième compte la fonction transferOwner



```
[vm] from: 0x5B3...eddC4 to: Election.transferOwnership(address) 0xd91...39138 value: 0 wei data: 0xf2f...35cb2 logs: 1
hash: 0x360...852e3 Debug ^

status      true Transaction mined and execution succeed

transaction hash  0x360e9fe527d67ab29a34293e85bfd18f3e67c435e781ff6a7941f7e9f4852e3

from          0x5B380a6a701c568545dCfcB03FcB875f56beddC4

to            Election.transferOwnership(address) 0xd9145CCE52D386f254917e481e844e9943f39138

gas           80000000 gas

transaction cost 28682 gas

execution cost  28682 gas

input          0xf2f...35cb2

decoded input   {
  "address newOwner": "0xab8483f64d9c6d1EcF9b849Ae677d03315835cb2"
}

decoded output  {}

logs           [
  {
    "from": "0xd9145CCE52D386f254917e481e844e9943f39138",
    "topic": "0x8be0079c53165914134cd1fd0a4f28419497f9722a3daafe3b4186f6b6457e0",
    "event": "OwnershipTransferred",
    "args": {
      "0": "0x5B380a6a701c568545dCfcB03FcB875f56beddC4",
      "1": "0xab8483f64d9c6d1EcF9b849Ae677d03315835cb2",
      "previousOwner": "0x5B380a6a701c568545dCfcB03FcB875f56beddC4",
      "newOwner": "0xab8483f64d9c6d1EcF9b849Ae677d03315835cb2"
    }
  }
]

val           0 wei
```

Si on réessaye de faire la transaction, elle ne fonctionne pas. C'est normal le propriétaire du contrat à été changé

```
[vm] from: 0x5B3...eddC4 to: Election.transferOwnership(address) 0xd91...39138 value: 0 wei data: 0xf2f...35cb2 logs: 0
hash: 0x47c...161cf Debug ^

status      false Transaction mined but execution failed

transaction hash  0x47c257e4629e3e773e6aadf691cd36f50a2fca3963d0e30416cec90fc56161cf

from          0x5B380a6a701c568545dCfcB03FcB875f56beddC4

to            Election.transferOwnership(address) 0xd9145CCE52D386f254917e481e844e9943f39138

gas           80000000 gas

transaction cost 24010 gas

execution cost  24010 gas

input          0xf2f...35cb2

decoded input   {
  "address newOwner": "0xab8483f64d9c6d1EcF9b849Ae677d03315835cb2"
}

decoded output  {}

logs           []

val           0 wei
```

x. Il faut changer l'accessibilité de la fonction addCandidate en la rendant exécutable que par le propriétaire du smart contract

y.

```
function addCandidate (string memory _name) public onlyOwner{  
    candidatesCount ++;  
    candidates[candidatesCount] = Candidate(candidatesCount, _name, 0);  
    require(msg.sender == owner, "Not authorized operation");  
}
```