

TP – Blockchain

1.d Réception d'1eth.

MetaMask Ether Faucet

faucet

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

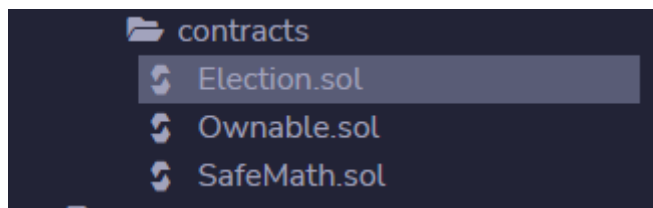
user

address: 0x069977cdc3d618343e5b7a1e9ee3f8fd07190eda
balance: 0.00 ether
donate to faucet:

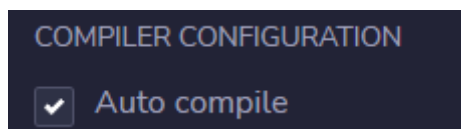
1 ether 10 ether 100 ether

transactions

1.j Import des fichier solidity.



1.l Déploiement et compilation du contrat.



Les frais de transaction ne sont pas les mêmes, elles sont de 554494 gaz qui sont à convertir.

1.o

Transaction details for 'ELECTION AT 0XD91...39138 (MEMOI)'. The transaction is 'addCandidate' with value 'CHHUON'. The transaction hash is '0x13a792d1c9ed7a1e2e54bbac6dcdf7b41f09d89315a284f7d8dfec3131cbb'. The transaction cost is 91382 gas. The execution cost is 91382 gas. The input is '0x462...00000'. The decoded input is '{ \"string_name\": \"CHHUON\" }'. The decoded output is '{}'. The transaction status is 'true Transaction mined and execution succeed'.

1.p

Transaction details for 'ELECTION AT 0XD91...39138 (MEMOI)'. The transaction is 'candidates' with value '1'. The transaction hash is '0x5262b75d51ac86034562c43bb28c4e7ac840af3ec390e481876b6da72bd0e2fb'. The transaction cost is 74270 gas. The execution cost is 74270 gas. The input is '0x347...00001'. The decoded input is '{ \"uint256\": \"1\" }'. The decoded output is '{ \"0\": \"uint256: id 1\", \"1\": \"string: name CHHUON\", \"2\": \"uint256: voteCount 0\" }'. The transaction status is 'true Transaction mined and execution succeed'.

1.q

Transaction details for 'ELECTION AT 0XD91...39138 (MEMOI)'. The transaction is 'addCandidate' with value 'CROCO'. The transaction hash is '0x5262b75d51ac86034562c43bb28c4e7ac840af3ec390e481876b6da72bd0e2fb'. The transaction cost is 74270 gas. The execution cost is 74270 gas. The input is '0x462...00000'. The decoded input is '{ \"string_name\": \"CROCO\" }'. The decoded output is '{}'. The transaction status is 'true Transaction mined and execution succeed'.

1.r

addCandidate

CROCO

transferOwner...

address newOwner

vote

uint256_candidateId

candidates

2

0: uint256: id 2

1: string: name CROCO

2: uint256: voteCount 0

candidatesCou...

owner

voters

address

CALL [call] from: 0x58380a6a701c568545dCfcB03FcB875f56beddC4 to: Election.candidates(uint256) data: 0x347...00002

from

0x58380a6a701c568545dCfcB03FcB875f56beddC4

to

Election.candidates(uint256) 0xd9145CCCE52D386f254917e481e844e9943f39138

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 CROCO",
 "2": "uint256: voteCount 0"
}

1.s

1: string: name CROCO

2: uint256: voteCount 0

candidatesCou...

owner

0: address: 0x58380a6a701c568545dCfcB03FcB875f56beddC4

voters

address

Low level interactions

CALLDATA

Transact

CALL [call] from: 0x58380a6a701c568545dCfcB03FcB875f56beddC4 to: Election.owner() data: 0x8da...5cb5b

from

0x58380a6a701c568545dCfcB03FcB875f56beddC4

to

Election.owner() 0xd9145CCCE52D386f254917e481e844e9943f39138

execution cost

23430 gas (Cost only applies when called by a contract)

input

0x8da...5cb5b

decoded input

{}

decoded output

{
 "0": "address: 0x58380a6a701c568545dCfcB03FcB875f56beddC4"
}

logs

[]

1.t

addCandidate

string_name

transferOwner...

address newOwner

vote

1

candidates

uint256

0: uint256: id 2

1: string: name CROCO

2: uint256: voteCount 0

candidatesCou...

owner

0: address: 0x58380a6a701c568545dCfcB03FcB875f56beddC4

voters

address

Low level interactions

CALLDATA

Transact

[vm] from: 0x583...eddC4 to: Election.vote(uint256) 0xd91...39138 value: 0 wei data: 0x012...00001 logs: 1 hash: 0xf15...897b5

status

true Transaction mined and execution succeed

transaction hash

0xf15ee719e9808e1fc78fe6ba84a8778eb6111d66fa98e6b0626dc520583897b5

from

0x58380a6a701c568545dCfcB03FcB875f56beddC4

to

Election.vote(uint256) 0xd9145CCCE52D386f254917e481e844e9943f39138

gas

80000000 gas

transaction cost

69467 gas

execution cost

69467 gas

input

0x012...00001

decoded input

{
 "uint256_candidateId": "1"
}

decoded output

{}

logs

[
 {
 "from": "0xd9145CCCE52D386f254917e481e844e9943f39138",
 "topic": "0xffff3c900d938d21d0990d786e819f29b8085c1ef587b462b939609625b684b16",
 "event": "votedEvent",
 "args": {
 "0": "1",
 "_candidateId": "1"
 }
 }
]

1.u Le vote a bien été pris en compte et qu'il est de 1 pour le candidat CHHUON.

The screenshot shows a transaction call to `Election.candidates(uint256)` with data `0x347...00001`. The input is `1`. The decoded output is:

```
{
  "0": "uint256: id 1",
  "1": "string: name CHHUON",
  "2": "uint256: voteCount 1"
}
```

1.v On peut voir que le vote a été pris en compte et qu'il est de 2 pour le candidat CHHUON.

The screenshot shows a transaction call to `Election.candidates(uint256)` with data `0x347...00001`. The input is `1`. The decoded output is:

```
{
  "0": "uint256: id 1",
  "1": "string: name CHHUON",
  "2": "uint256: voteCount 1"
}
```

1.w On transfère la propriété du contrat en utilisant la fonction « transferOwnership » et en entrant l'identifiant du wallet du nouveau propriétaire.

The screenshot shows a transaction call to `Election.transferOwnership(address)` with data `0xf2f...35cb2`. The input is `1`. The decoded output is:

```
{
  "address newOwner": "0xab8483f64d9c6d1ecf9b849ae677d03315835cb2"
}
```

1.x

On peut limiter la visibilité avec la mention « onlyOwner ».

1.y

```
function addCandidate (string memory _name) public onlyOwner {
```

Avec le wallet du propriétaire l'action addCandidate est bien effectué :

The screenshot shows a web interface on the left with a sidebar containing buttons: addCandidate, transferOwner..., vote, candidates, candidatesCou..., owner, and voters. The main area displays transaction details for a successful call to addCandidate. The transaction was mined and executed successfully. The decoded input shows the string name "aa".

| Field | Value |
|------------------|---|
| status | true Transaction mined and execution succeed |
| transaction hash | 0xbabe2aa3a7c17b1c9b35d30938c709c3c9d8b2e8c8e616fd11f5fbb0c835ec9e |
| from | 0x58380a6a701c56854dcfc803fc8875f56bedd4c4 |
| to | Election.addCandidate(string) 0xEf9f1ACE83dfb8f5590a621f4aEA72C6EB10eBf |
| gas | 80000000 gas |
| transaction cost | 93501 gas |
| execution cost | 93501 gas |
| input | 0x462...00000 |
| decoded input | { "string_name": "aa" } |
| decoded output | {} |

Avec un autre wallet l'action addCandidate est refusé :

The screenshot shows the same web interface as above, but the transaction failed. The status is false, indicating the transaction was mined but execution failed. The decoded input is the same as the successful transaction, but the status is false.

| Field | Value |
|------------------|---|
| status | false Transaction mined but execution failed |
| transaction hash | 0x2cc313a2cca14dc57188c766dd66aa32c5e8c8f18c8da8da8f9deda472bebe0 |
| from | 0xab8483f64d9C6d1EcF9b849Ae677d03315835cb2 |
| to | Election.addCandidate(string) 0xEf9f1ACE83dfb8f5590a621f4aEA72C6EB10eBf |
| gas | 80000000 gas |
| transaction cost | 24327 gas |
| execution cost | 24327 gas |
| input | 0x462...00000 |
| decoded input | { "string_name": "aa" } |
| decoded output | {} |