

Blockchain A2IR

Compte rendu TP Smart Contract

william berenguer
07/09/2020

Table des matières

1 Prise en main des outils Remix et Metamask.....	2
Première transaction.....	2
Details Block 8636029	3
Déploiement Smart Contract	4
Interaction avec un contrat	5
Ajout d'un premier candidat	5
Ajout d'un second candidat.....	6
Vote pour un candidat.....	7
Voter pour le candidat d'un autre contrat.....	8
Transfert de propriétaire.....	9
Sécuriser la fonction addCandidate	9
Table des illustrations.....	10

1 Prise en main des outils Remix et Metamask

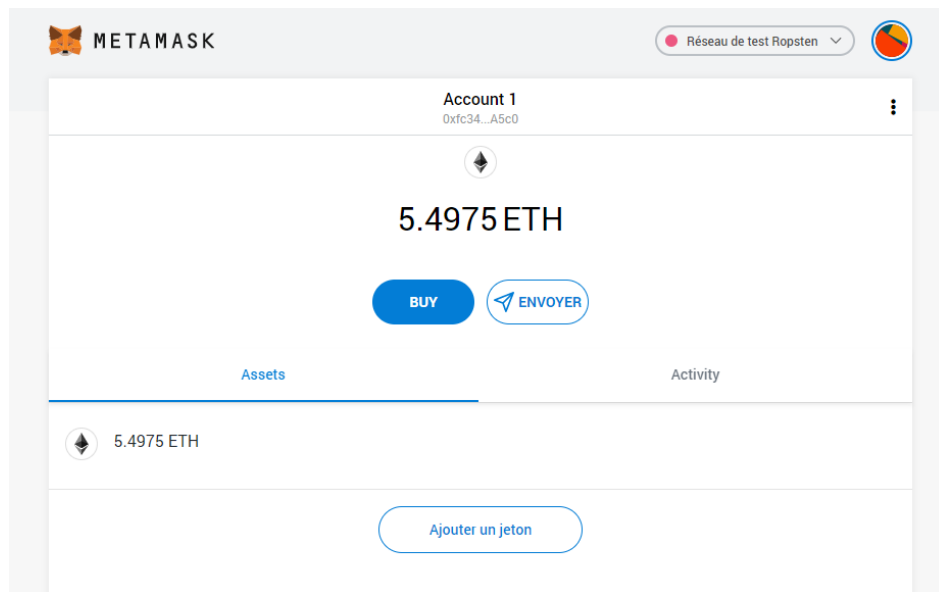


Figure 1 Capture d'écran de mon Wallet Ethereum

La clé public de mon compte est : 0xfc3439E460a4F8B4E0E1E56EcE901d353B9FA5c0

Première transaction

Sur faucet en ligne, j'ai saisi ma clé publique est j'ai reçu des Ether.

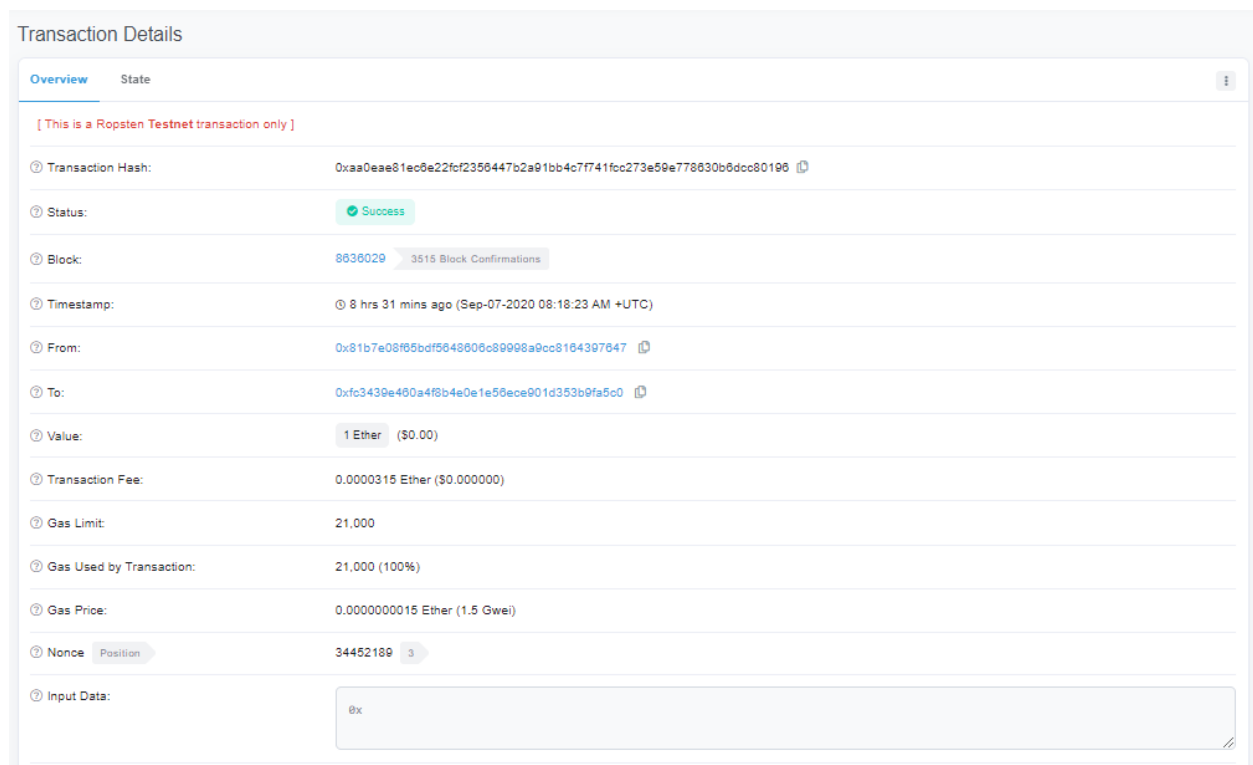


Figure 2 Détails de la première transaction

Details Block 8636029

Ma première transaction a été faites via le block 8636029.

Block #8636029	
Overview	
[This is a Ropsten Testnet block only]	
Block Height:	8636029 < >
Timestamp:	8 hrs 35 mins ago (Sep-07-2020 08:18:23 AM +UTC)
Transactions:	5 transactions and 7 contract internal transactions in this block
Mined by:	0xd34912efb0e7fedaedb9390990d7efb23e01f4fa in 11 secs
Block Reward:	2.0169083135 Ether (2 + 0.0169083135)
Uncles Reward:	0
Difficulty:	551,738,015
Total Difficulty:	31,436,512,584,000,689
Size:	1,121 bytes
Gas Used:	237,593 (2.98%)
Gas Limit:	7,961,005
Extra Data:	poolin.com (Hex:0x706f6fc696e2e636f6d)
Hash:	0x33a83f648261a2c3372e37ac1617da3b75e7855caa296de2b213f42b28d1535
Parent Hash:	0x3e2b25e5b44a13bbb603d929bc8c9a963bb7372512fa548b18c388ad22d21ee1
Sha3Uncles:	0x1d0c4de8dec75d7aab85b567b8cccd41ad312451b948a7413f0a142fd40d49347
StateRoot:	0xaf84e7621cfe6066b6715301bd967baef61d5052fc6317fbb1aae49e37cbe78
Nonce:	0x5a4fed00007a51d
Click to see less ↑	

Figure 3 Détails concernant le block 8636029

Déploiement Smart Contract

The screenshot shows a 'Transaction Details' page with two tabs: 'Overview' and 'State'. A red warning message at the top states: '[This is a Ropsten Testnet transaction only]'. The transaction is confirmed as 'Success' with 3399 block confirmations. The transaction hash is 0x8297aec95814fb8c8bea3e5c203e45835b8970526f5046fea3b9db4cda77ca58. It was sent from 0xfc3439e460a4f8b4e0e1e58ece901d353b9fa5c0 to a contract address 0x2e55162d5c93c2fa668216446eb7255adddd6d92. The transaction value is 0 Ether (\$0.00) and the fee is 0.000829809 Ether (\$0.000000). The gas limit is 553,206, and the gas used is 553,206 (100%). The gas price is 0.000000015 Ether (1.5 Gwei). The nonce is 1. The input data is a long hexadecimal string representing the contract deployment bytecode.

Field	Value
Transaction Hash:	0x8297aec95814fb8c8bea3e5c203e45835b8970526f5046fea3b9db4cda77ca58
Status:	Success
Block:	8836202 (3399 Block Confirmations)
Timestamp:	8 hrs 14 mins ago (Sep-07-2020 08:44:33 AM +UTC)
From:	0xfc3439e460a4f8b4e0e1e58ece901d353b9fa5c0
To:	[Contract 0x2e55162d5c93c2fa668216446eb7255adddd6d92 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:	0.000000015 Ether (1.5 Gwei)
Nonce	1
Input Data:	0x608060405234801561001057600080fd5b50336000806101000a81548173fff021916908373fffffffff...

Figure 4 Détails déploiement du smart contract

Les frais de transaction : 0.000829809 Ether

Ils sont différents de ceux de la capture d'écran du TP car ils dépendent du nombre de personnes qui interagissent avec le réseau à l'instant où la transaction est effectuée.

Adresse publique du contrat : [0x2e55162d5c93c2fa668216446eb7255adddd6d92](https://ropsten.etherscan.io/address/0x2e55162d5c93c2fa668216446eb7255adddd6d92)

L'ABI ainsi que le Bytecode se situe dans les fichiers texte sur mon Github personnel dans le dossier TP_SmartContract.

Interaction avec un contrat

Ajout d'un premier candidat

Transaction Details

Overview State

[This is a Ropsten Testnet transaction only]

Transaction Hash:	0xc1028714f57511aec08453369fcc8928b496c59c935000357be351c85fe07031
Status:	Success
Block:	8636462 3151 Block Confirmations
Timestamp:	7 hrs 47 mins ago (Sep-07-2020 09:13:47 AM +UTC)
From:	0xfc3430e460a4f8b4e0e1e56ece901d353b9fa5c0
To:	Contract 0x2e55162d5c93c2fa668216446eb7255adddd6d92
Value:	0 Ether (\$0.00)
Transaction Fee:	0.000130077 Ether (\$0.000000)
Gas Limit:	88,201
Gas Used by Transaction:	86,718 (98.32%)
Gas Price:	0.0000000015 Ether (1.5 Gwei)
Nonce	2
Input Data:	<pre>Function: addCandidate(string name) *** MethodID: 0x462e91ec [0]: 0020 [1]: 0009 [2]: 426572656e6775657200</pre>

View Input As

Figure 5 Détails ajout d'un premier candidat "Berenguer"

Le candidatID du premier candidat est 1 car il est le premier candidat créé sur le contrat.

```
[block:8636462 txIndex:20] from: 0xfc3...FA5c0 to: Election.addCandidate(string) 0x2E5...d6d92 value: 0 wei
data: 0x462...00000 logs: 0 hash: 0xc10...07031

status      true Transaction mined and execution succeed
transaction hash  0xc1028714f57511aec08453369fcc8928b496c59c935000357be351c85fe07031
from        0xfc3439E460a4F8B4E0E1E56EcE901d353B9FA5c0
to          Election.addCandidate(string) 0x2E55162d5C93C2FA668216446EB7255Adddd6d92
gas         88201 gas
transaction cost 86718 gas
hash        0xc1028714f57511aec08453369fcc8928b496c59c935000357be351c85fe07031
input       0x462...00000
decoded input { "string _name": "Berenguer" }
decoded output -
logs        []
value       0 wei
```

Figure 6 Détails ajout premier candidat sur Remix

Ajout d'un second candidat

The screenshot shows the 'Transaction Details' page for a Ropsten Testnet transaction. The 'Overview' tab is selected. The transaction is successful and has 15 block confirmations. The input data shows a function call to addCandidate with the name 'Bubble'.

Field	Value
Transaction Hash	0x04a3240bd23f27e6270ab45d3cf0383c7c6208e79cb805885421dffb85c1ab0d
Status	Success
Block	8636546 (15 Block Confirmations)
Timestamp	2 mins ago (Sep-07-2020 09:24:42 AM +UTC)
From	0xfc3439e460a4f8b4e0e1e56ece901d353b9fa5c0
To	Contract 0x2e55162d5c93c2fa068216446eb7255adddd6d92
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
Input Data	Function: addCandidate(string name) *** MethodID: 0x462e91ec [0]: 00 [1]: 00

Figure 7 Détails ajout d'un second candidat "Bubble"

Le candidatID du second candidat est 2.

The screenshot shows the transaction details on the Remix IDE. The transaction is successful and has been mined. The input data shows a function call to Election.addCandidate with the name 'Bubble'.

Field	Value
status	true Transaction mined and execution succeed
transaction hash	0x04a3240bd23f27e6270ab45d3cf0383c7c6208e79cb805885421dffb85c1ab0d
from	0xfc3439e460a4f8b4e0e1e56ece901d353b9fa5c0
to	Election.addCandidate(string) 0x2E55162d5C93C2fA668216446EB7255Adddd6d92
gas	73165 gas
transaction cost	71682 gas
hash	0x04a3240bd23f27e6270ab45d3cf0383c7c6208e79cb805885421dffb85c1ab0d
input	0x462...0000
decoded input	{ "string _name": "Bubble" }
decoded output	-
logs	[]
value	0 wei

Figure 8 Détails de l'ajout du second candidat sur Remix

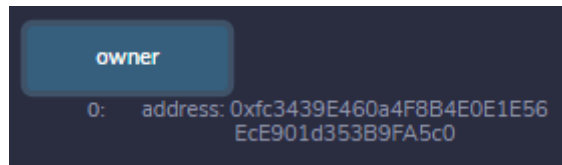


Figure 9 Capture d'écran de l'adresse du propriétaire du contrat

L'adresse publique du propriétaire du contrat : 0xfc3439E460a4F8B4E0E1E56EcE901d353B9FA5c0

Vote pour un candidat

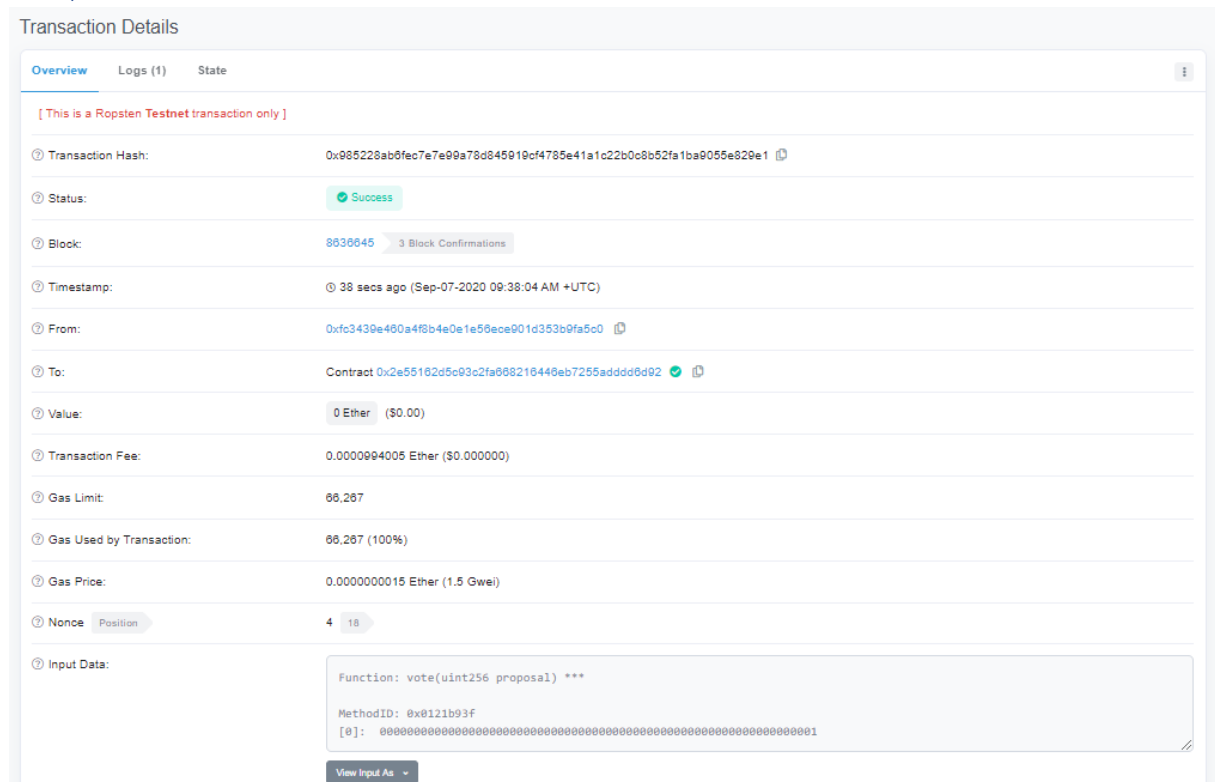


Figure 10 Détails de l'interaction Vote sur le contrat

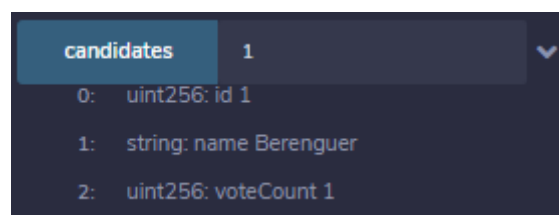


Figure 11 Capture d'écran montrant le candidat "Berenguer" ainsi que son nombre de voix

Suite à l'interaction le candidat Berenguer a reçu 1 vote.

Voter pour le candidat d'un autre contrat

The screenshot shows the 'Transaction Details' page for a Ropsten Testnet transaction. The transaction is successful and has 67 block confirmations. The 'To' field shows a contract address: 0xe245533dcf3f4fbefa28882bf99cd66b66ac45d0. The 'Input Data' section shows the function call: `Function: vote(uint256 proposal) ***` with a method ID of 0x8121b93f. The input data array is `[0]: 0001`.

Transaction Hash:	0xeb18ca260ebc85c527c40fd3f2593118d1d0fcd1ff116da009e9cb46d36036e5
Status:	Success
Block:	8636759 67 Block Confirmations
Timestamp:	8 mins ago (Sep-07-2020 09:52:20 AM +UTC)
From:	0xfc3439e460a4f8b4e0e1e58ece901d353b9fa5c0
To:	Contract 0xe245533dcf3f4fbefa28882bf99cd66b66ac45d0
Value:	0 Ether (\$0.00)
Transaction Fee:	0.0000769005 Ether (\$0.000000)
Gas Limit:	51,267
Gas Used by Transaction:	51,267 (100%)
Gas Price:	0.0000000015 Ether (1.5 Gwei)
Nonce:	0 7
Input Data:	Function: vote(uint256 proposal) *** MethodID: 0x8121b93f [0]: 0001

Figure 12 Détails de l'interaction du vote pour le candidat sur un autre contrat

L'interaction s'est effectuée sur le contrat de Marc Betum dont l'adresse publique du contrat est : [0xe245533dcf3f4fbefa28882bf99cd66b66ac45d0](https://ropsten.etherscan.io/address/0xe245533dcf3f4fbefa28882bf99cd66b66ac45d0)

The screenshot shows a list of candidates. The first candidate is 'Marc' with 2 votes. The list is titled 'candidates' and shows the count '1'.

id	name	voteCount
0: uint256: id 1	1: string: name Marc	2: uint256: voteCount 2

Figure 13 Capture d'écran montrant le candidat "Marc" et son nombre de voie

Le candidat numéro 1 « Marc » du contrat de Marc a été incrémenté de 1 voix.

Transaction Details	
Overview	Logs (1) State
[This is a Ropsten Testnet transaction only]	
⑦ Transaction Hash:	0xc3c556bb1d889eefbdce7a00eb3edb56239c1a6de66f180e213b98cfb619af1 ⓘ
⑦ Status:	✓ Success
⑦ Block:	8636691 ▶ 9 Block Confirmations
⑦ Timestamp:	⌚ 1 min ago (Sep-07-2020 09:43:40 AM +UTC)
⑦ From:	0xfc3439e400a4fb4e0e1e56ece901d353b9fa5c0 ⓘ
⑦ To:	Contract 0x2e55162d5c93c2fa968216446eb7255adddd6d92 ✓ ⓘ
⑦ Value:	0 Ether (\$0.00)
⑦ Transaction Fee:	0.000046323 Ether (\$0.000000)
⑦ Gas Limit:	30,882
⑦ Gas Used by Transaction:	30,882 (100%)
⑦ Gas Price:	0.0000000015 Ether (1.5 Gwei)
⑦ Nonce	Position 5 0 ▶
⑦ Input Data:	Function: transferOwnership(address newOwner) *** MethodID: 0xf2fde38b [0]: 0000000000000000000000004d89b8375a3690d2a970ba6519b0111ed8441726
View Input As →	

Le propriétaire initial avait l'adresse publique : 0xfc3439E460a4F8B4E0E1E56EcE901d353B9FA5c0



Sécuriser la fonction addCandidate

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

Après la compilation et le redéploiement du contrat, il est impossible pour un utilisateur non-propriétaire du contrat d'ajouter des candidats.

Table des illustrations

Figure 1 Capture d'écran de mon Wallet Ethereum	2
Figure 2 Détails de la première transaction	2
Figure 3 Détails concernant le block 8636029	3
Figure 4 Détails déploiement du smart contract.....	4
Figure 5 Détails ajout d'un premier candidat "Berenguer"	5
Figure 6 Détails ajout premier candidat sur Remix	5
Figure 7 Détails ajout d'un second candidat "Bubble"	6
Figure 8 Détails de l'ajout du second candidat sur Remix.....	6
Figure 9 Capture d'écran de l'adresse du propriétaire du contrat.....	7
Figure 10 Détails de l'interaction Vote sur le contrat	7
Figure 11 Capture d'écran montrant le candidat "Berenguer" ainsi que son nombre de voix.....	7
Figure 12 Détails de l'interaction du vote pour le candidat sur un autre contrat	8
Figure 13 Capture d'écran montrant le candidat "Marc" et son nombre de voie	8
Figure 14 Détails du transfert de propriété du contrat.....	9
Figure 15 Capture d'écran de l'adresse du propriétaire du contrat.....	9
Figure 16 Capture d'écran du code de la fonction addCandidate modifier	9