

Travaux pratique :

Développer, Deloyer et Interagir avec
un contrat intelligent sur Ethereum

Gabriel Kundid

A2MSI – 28/03/2023

Question a) à f) :

Pour la création de mon compte, j'ai juste suivi les étapes décrites dans l'énoncé du TP.

Nom du réseau

SUDRIA TESTNET

Nouvelle URL de RPC

https://data-seed-prebsc-1-s1.binance.org:8545/

ID de chaîne ⓘ

97

Symbole de la devise

ETH

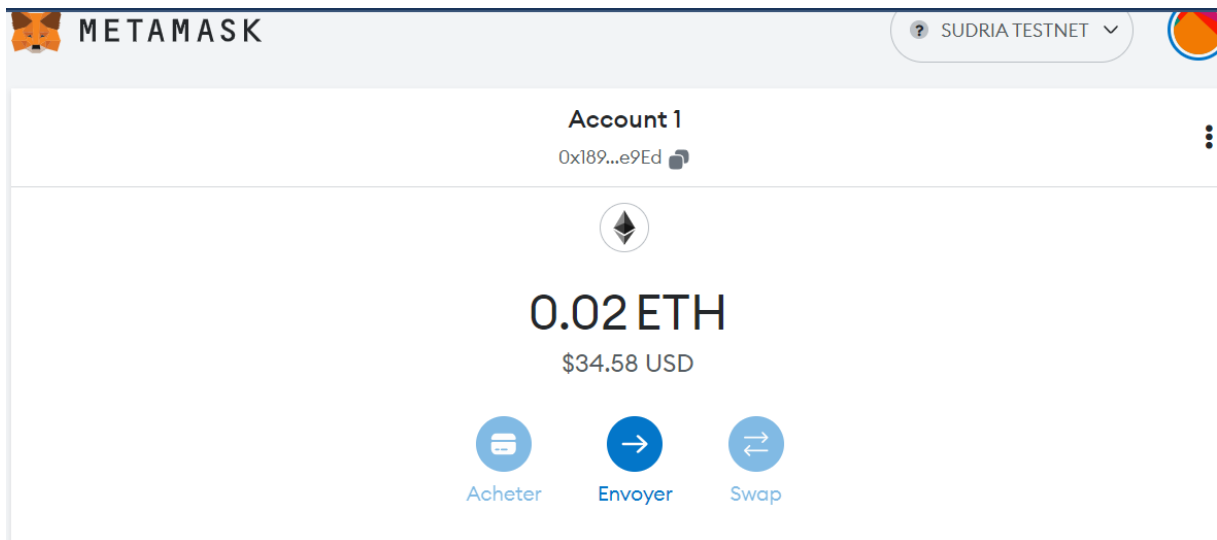
Le réseau avec l'ID de chaîne 97 peut utiliser un symbole de devise différent (tBNB) de celui que vous avez saisi. Veuillez vérifier avant de continuer.

URL de l'explorateur de blocs (Facultatif)

https://testnet.bscscan.com/|

Annuler

Enregistrer




Overview	
[This is a Bsc Testnet transaction only]	
Transaction Hash:	0x804e98b246cde60f0181e30f271895b70aaa9d20a24f57cf660bf0ad955e36f5
Status:	Success
Block:	28434383 144 Block Confirmations
Timestamp:	7 mins ago (Mar-28-2023 08:59:12 AM +UTC)
From:	0x533fb0469d523dfd5bf3d97e0ad75ea66328d08e
To:	0x1892e87039dc38cabf75e13a2aadf502f190e9ed
Value:	0.02 BNB (\$0.00)
Transaction Fee:	0.00021 BNB (\$0.07)
Gas Price:	0.00000001 BNB (10 Gwei)
Click to see More	

Question g) :

Overview

[This is a Bsc Testnet block only]

Block Height:	28434383 < >
Timestamp:	11 mins ago (Mar-28-2023 08:59:12 AM +UTC)
Transactions:	14 transactions and 12 contract internal transactions in this block
Validated by:	0xb71b214cb885500844365e95cd9942c7276e7fd8 in 3 secs
Block Reward:	0.027527959999993 BNB
Difficulty:	2
Total Difficulty:	56,692,851
Size:	7,512 bytes
Gas Used:	2,756,969 (5.51%)
Gas Limit:	50,000,000
Fee Burnt:	 0.002752795999993 BNB 🔗

Extra Data:

```
Hex:
0xd883010114846765746888676f312e31392e36856c696e75780000008279af9ac3c7f5d6ebaaaf38f64d75c284f5cb14b54cf9de314f5e3a1e218143
2289891589e427afb2d21611d1f10e9af3d68f73715bb58017e253e7f6cc739050908601

ExtraVanity : _8888geth-go1.19.6-linux-yy
SignedData :
0xc73e1e7f5d6ebaaaf38f64d75c284f5cb14b54cf9de314f5e3a1e2181432289891589e427afb2d21611d1f10e9af3d68f73715bb58017e253e7f6cc739050908601
```

Hash:	0x5c44393577cfd6d319af3910933f6d829d8274e697a461d36b280878a46a1943
Parent Hash:	0x46861f39e9b00fb395e5b4c2edb73c45b689c11a22acabe5a2eaf4160deddbd6
Sha3Uncles:	0x1dcc4de8dec75d7aab85b567b6ccd41ad312451b948a7413f0a142fd40d49347
Nonce:	0x0000000000000000

[Click to see less](#) ↑

Envoyer

0x533fB0469D523dfD5BF3D97e0Ad75ea66328D08E

Actif:

ETH

Solde: 0.02 ETH

Montant:

0.01 ETH

\$17.27 USD

Max.

Prix du gaz (GWEI)

10

Montant maximal des frais de transaction

21000

Carburant (estimé)

\$0.36 0.00021 ETH

Frais maximaux: 0.00021 ETH

Annuler

Suivant

Modifier

Account 1

0x533...D08E

ENVOI DE ETH

0.01

\$17.27

MODIFIER

Frais de carburant estimés

\$0.36 0.00021 ETH

Frais maximaux: 0.00021 ETH

Total

\$17.64 0.01021 ETH

Montant + frais de carburant

Montant maximal: 0.01021 ETH

Rejeter

Confirmer

File d'attente (1)

Envoyer

En attente • Vers: 0x533...d08e

Accélérer

Annuler

-0.01 ETH

-\$17.27 USD

Envoyer

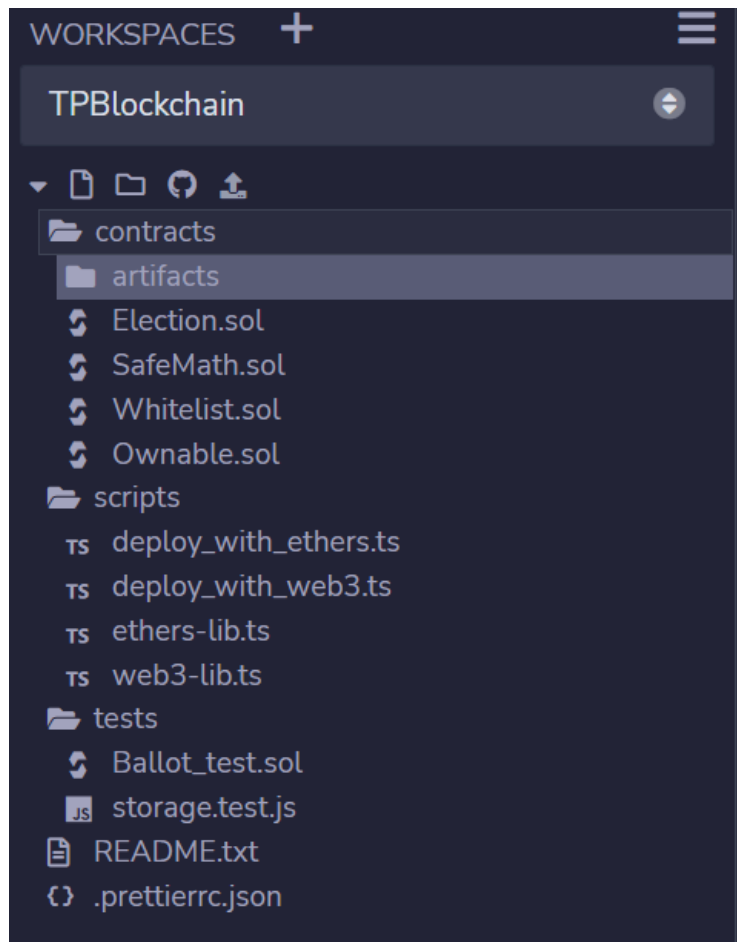
Mar 28 • Vers: 0x533...d08e

-0.01 ETH

-\$17.27 USD

Question h) à l) :

Ci-dessous mon workspace dédié au TP Blockchain. On peut voir que j'ai mis les 4 fichiers .sol dans le dossier « contracts ». Le bytecode et l'ABI sont disponibles sur mon dépôt Github.



Question m) :

SUDRIA TESTNET

Account 1

Nouveau contrat

https://remix.ethereum.org

DÉPLOIEMENT DE CONTRAT

\$0.00

DÉTAILS

DONNÉES

MODIFIER

Frais de carburant estimés

\$9.46

0.005485 ETH

Site suggéré

Frais maximaux: 0.00548492 ETH

Total

\$9.46

0.00548492 ETH

Montant + frais de carburant

Montant maximal: 0.00548492 ETH

Rejeter

Confirmer

Balance: 0 ETH

addCandidate

_name:

"Kundid"

Calldata

Parameters

transact

MetaMask Notification

SUDRIA TESTNET

Account 1

0xc53...35ed

0xc53...35ed : ADD CANDIDATE

\$0.00

DÉTAILS

DONNÉES

HEX

MODIFIER

Frais de carburant estimés

\$1.51

0.000881 ETH

Site suggéré

Frais maximaux: 0.00088059 ETH

Total

\$1.51

0.00088059 ETH

Montant + frais de carburant

Montant maximal: 0.00088059 ETH

Rejeter

Confirmer

Actifs

Activité

[Site du portefeuille](#)

Add Candidate

Mar 28 · remix.ethereum.org

-0 ETH
-\$0.00 USD

Transaction Details

Overview

[This is a Bsc Testnet transaction only]

Transaction Hash:

0xfe5cb78055de3c4fb6fe17e7435ec1159a95e9f4b2fcd7d5d3ee26c32c400fde

Status:

Success

Block:

28435384 22 Block Confirmations

Timestamp:

1 min ago (Mar-28-2023 09:49:15 AM +UTC)

From:

0x1892e87039dc38cab775a13a2aadf502f190e9ed

To:

Contract 0xc5383960d680bb32a20904e078489f3484b935ed

Value:

0 BNB (\$0.00)

Transaction Fee:

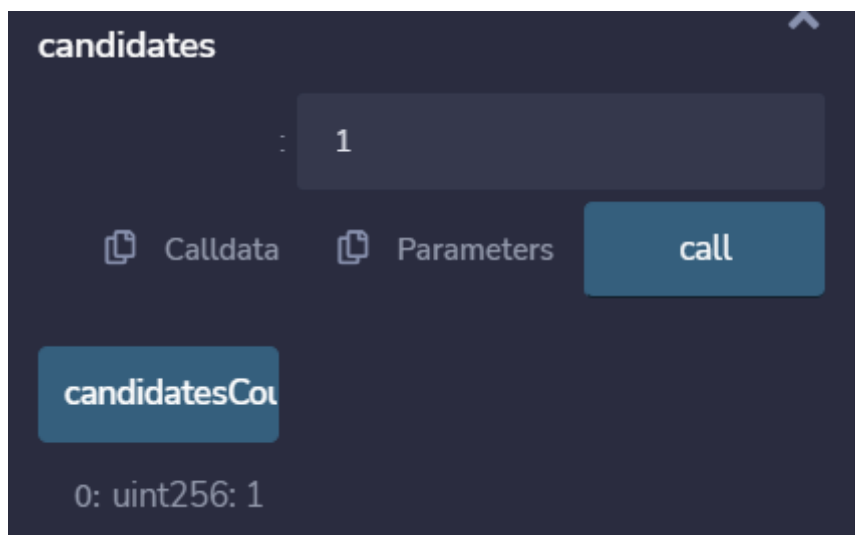
0.00086576 BNB (\$0.27)

Gas Price:

0.00000001 BNB (10 Gwei)

[Click to see More](#)

Question p) :



Ici, on passe le paramètre 1 à « candidates » car on a un seul candidat en toute logique d'après la question m). Le candidat est Kundid donc lorsqu'on appuie sur call, on devrait trouver le nom « Kundid » dans le debug.

```
call to Election.candidates

CALL [call] from: 0x1892e87039DC38CAbf75A13a2AAdF502F190e9Ed to: Election.candidates(uint256)
data: 0x347...00001

from 0x1892e87039DC38CAbf75A13a2AAdF502F190e9Ed

to Election.candidates(uint256) 0xc5383960D680Bb32a20904E078489F3484b935ed

input 0x347...00001

decoded input {
  "uint256 ": "1"
}

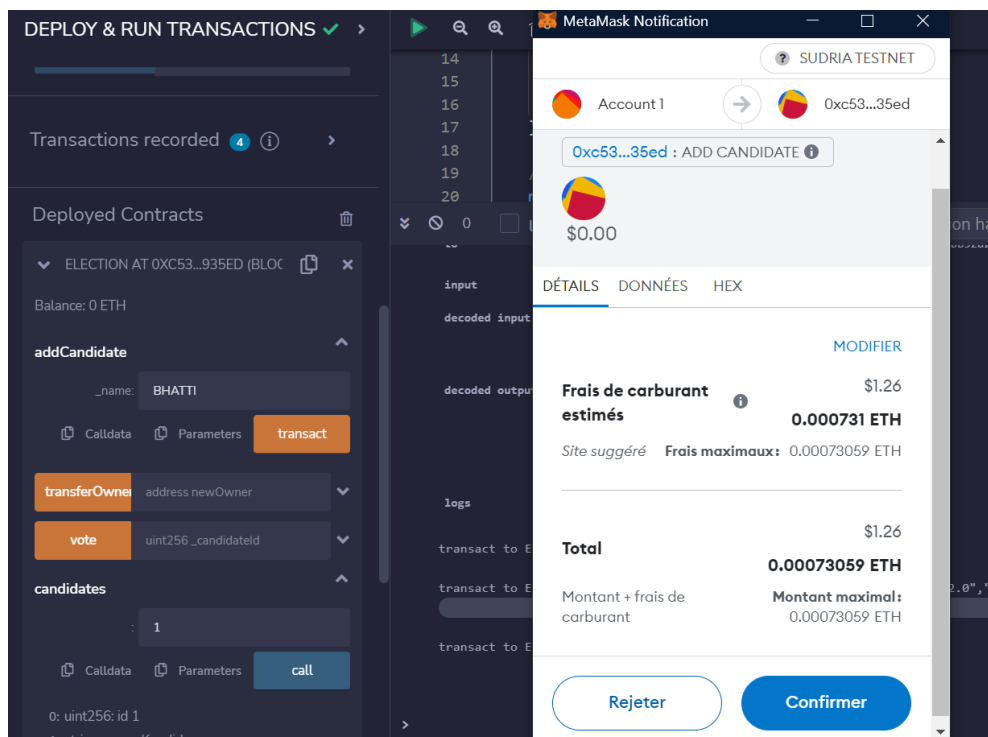
decoded output {
  "0": "uint256: id 1",
  "1": "string: name Kundid",
  "2": "uint256: voteCount 0"
}

logs []
```

Le nom Kundid est bien présent.

Question q) :

Dans cette partie, j'ai ajouté le candidat « BHATTI ».



Add Candidate

×

État

Afficher sur l'explorateur de blocs

Confirmé

Copier le numéro de transaction

de

Destinataire

0x189...e9Ed

→

0xc53...35ed

Transaction

Nonce	3
Montant	-0 ETH
Montant Maximal Des Frais De Transaction (Unités)	73059
Gaz Utilisé (Unités)	71576
Prix du gaz	10
Total	0.00071576 ETH \$1.23 USD

+ Log d'activité

+ Transaction data

Question s) :

From:

0x1892e87039dc38cabf75a13a2aadf502f190e9ed

To:

Contract 0xc5383960d680bb32a20904e078489f3484b935ed

L'adresse du propriétaire du contrat est : 0x1892e87039dc38cabf75a13a2aadf502f190e9ed

Question t) :

J'ai voté pour Kupid dans cette partie.

vote

1

candidates

1

Calldata

Parameters

call

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

MetaMask Notification

SUDRIA TESTNET

Account 1

0xc53...35ed

https://remix.ethereum.org

0xc53...35ed : VOTE

\$0.00

DÉTAILS

DONNÉES

HEX

MODIFIER

Frais de carburant estimés

\$1.14

0.000662 ETH

Site suggéré

Frais maximaux:

0.00066241 ETH

Total

\$1.14

0.00066241 ETH

Montant + frais de carburant

Montant maximal:

0.00066241 ETH

Overview
Logs (1)

[This is a Bsc Testnet transaction only]

Transaction Hash:
0x7782e5bb1fd4c171f30497d4111779e6c17dbe303fbeb52665883dc134a164e

Status:
Success

Block:
28435725
6 Block Confirmations

Timestamp:
19 secs ago (Mar-28-2023 10:06:18 AM +UTC)

From:
0x1892e87039dc38cabf75a13a2aadf502f190e9ed

To:
Contract 0xc5383960d680bb32a20904e078489f3484b935ed

Value:
0 BNB (\$0.00)

Transaction Fee:
0.00066241 BNB (\$0.20)

Gas Price:
0.00000001 BNB (10 Gwei)

Click to see More

Question u) :

On peut voir dans cette capture d'écran ci-dessous que mon vote a bien été pris en compte vu qu'on a voteCount égal à 1 pour Kundid, alors que dans la capture d'écran suivante, pour le nom BHATTI, on a le voteCount à 0.

candidates
1

Calldata
Parameters
call

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

candidatesContract
owner

voters
0x1892e87039dc38cabf75a13a

Calldata
Parameters
call

0: bool: true

Low level interactions
CALLDATA

19
20
0
listen on all transactions
Search with transaction hash or address

// Store accounts that have voted
mapping(address => bool) public voters:

candidates - call

CALL
[call] from: 0x1892e87039DC38CABf75A13a2AAdF502F190e9Ed to: Election.candidates(uint256) data: 0x347...00001

from
0x1892e87039DC38CABf75A13a2AAdF502F190e9Ed

to
Election.candidates(uint256) 0xc5383960d680bb32a20904e078489f3484b935ed

input
0x347...00001

decoded input
{
"uint256 ": "1"
}



decoded output
{
"0": "uint256: id 1",
"1": "string: name Kundid",
"2": "uint256: voteCount 1"
}

logs
[]

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

Question v :

Dans cette partie, j'ai interagi avec ma camarade Christine Luu.

▼ ELECTION AT 0XEDC...A26E4 (BLOK)  

Balance: 0.00206115 ETH

addCandidate

string _name

▼

transferOwner

address newOwner


▼


vote

▲

_candidateId:

"1"

 Calldata

 Parameters

transact

MetaMask Notification

Modifier

SUDRIA TESTNET

Account 1

→

0xDc...26E4

ENVOI DE ETH

0

\$0.00

DÉTAILS

DONNÉES

HEX

MODIFIER

Frais de carburant estimés

\$0.36

0.000212 ETH

Site suggéré

Frais maximaux: 0.00021204 ETH

Total

\$0.36

0.00021204 ETH

Montant + frais de carburant

Montant maximal: 0.00021204 ETH

Rejeter

Confirmer

[Site du portefeuille](#)



Envoyer

Mar 28 · Vers: 0xedc...26e4

-0 ETH

-\$0.00 USD

✓

[block:28436120 txIndex:6] from: 0x189...0e9Ed to: Election.vote(uint256) 0xeDc...a26E4 value: 0 wei data: 0x012...00001 logs: 0 hash: 0x155...a4ba7

Debug

status

true Transaction mined and execution succeed

transaction hash

0xed99980d9565274a5ec37ac8fcae482da927e6d30587c99a236326abc54e9968

from

0x1892e87039DC38CABf75A13a2AAdF502F190e9Ed

to

Election.vote(uint256) 0xeDc1c50114951430006144a92a577Cfb67a26E4

gas

21204 gas

transaction cost

21204 gas

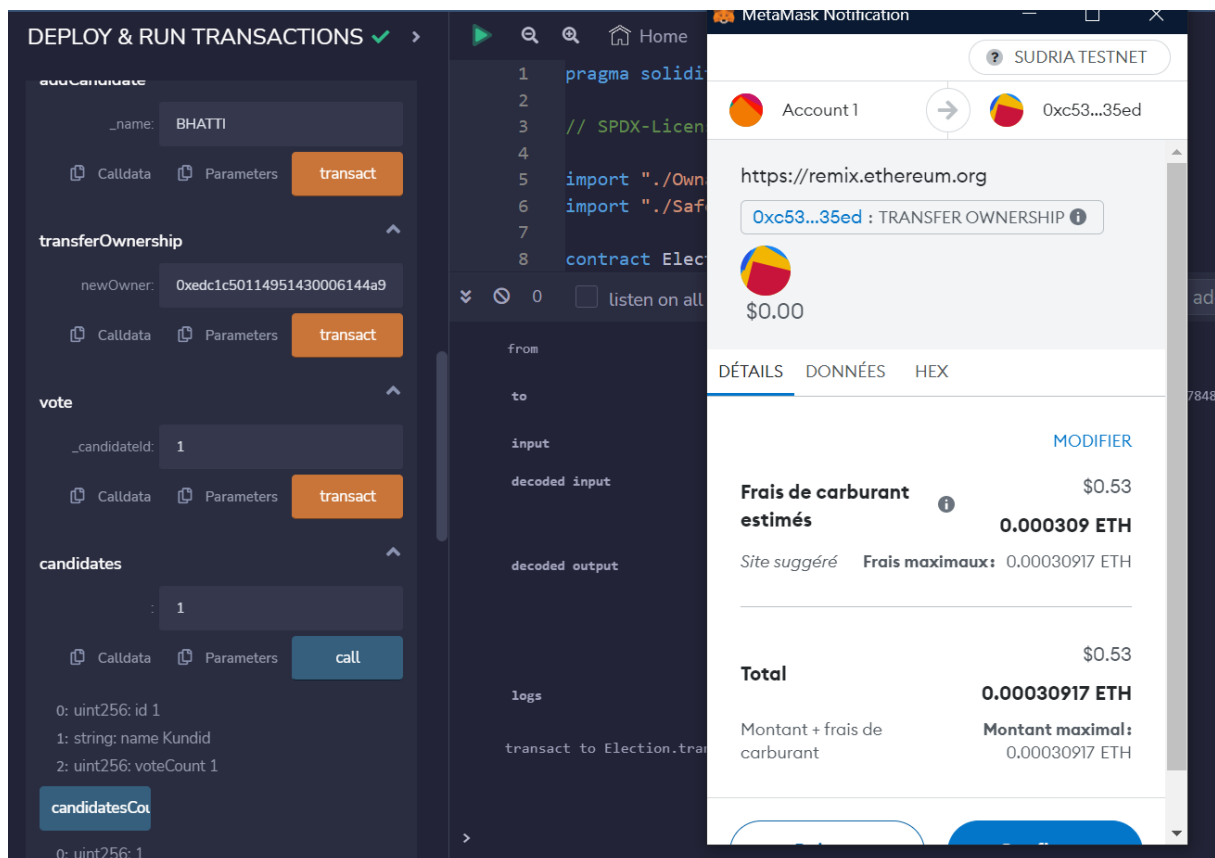
input

0x012...00001

decoded input

{
 "uint256_candidateId": "1"
}

Question w) :






Transfer Ownership ✕

État [Afficher sur l'explorateur de blocs](#)

Confirmé [Copier le numéro de transaction](#)

de **Destinataire**

 0x189...e9Ed   0xc53...35ed

Transaction

Nonce	6
Montant	-0 ETH
Montant Maximal Des Frais De Transaction (Unités)	30917
Gaz Utilisé (Unités)	30917
Prix du gaz	10
Total	0.00030917 ETH \$0.53 USD

+ Log d'activité

+ Transaction data

Overview	Logs (1)
Transaction Hash:	0x9e2f90609c886517021ab11eb800dd77010cc0f4b4486b9db4b6eef8ad8fe2dd 🔗
Status:	Success
Block:	28436174 22 Block Confirmations
Timestamp:	1 min ago (Mar-28-2023 10:28:45 AM +UTC)
From:	0x1892e87039dc38cabf75a13a2aadf502f190e9ed 🔗
To:	Contract 0xc5383960d680bb32a20904e078489f3484b935ed ✔️ 🔗
Value:	0 BNB (\$0.00)
Transaction Fee:	0.00030917 BNB (\$0.10)
Gas Price:	0.00000001 BNB (10 Gwei)
Gas Limit & Usage by Txn:	30,917 30,917 (100%)
Other Attributes:	Nonce: 6 Position: 5
Input Data:	<pre>Function: transferOwnership(address newOwner) *** MethodID: 0xf2fde38b [0]: 000000000000000000000000edc1c50114951430006144a92a577cfbd67a26e4</pre>

Les modifications pour la question y) se trouvent directement sur le dépôt Github (dernier commit).