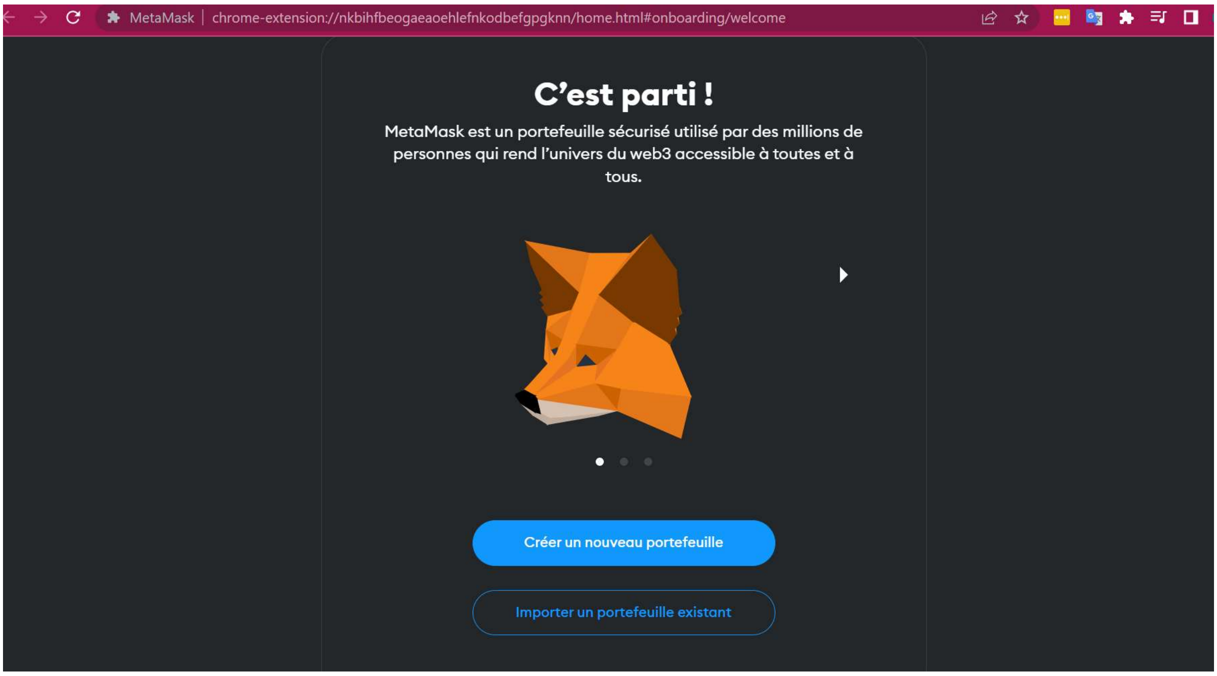
Esme sudria

TP- Smart contract

Développer, Deloyer et Interagir avec un contrat intelligent sur Ethereum

Juliette Aubourg

a. Page de connexion Metamask



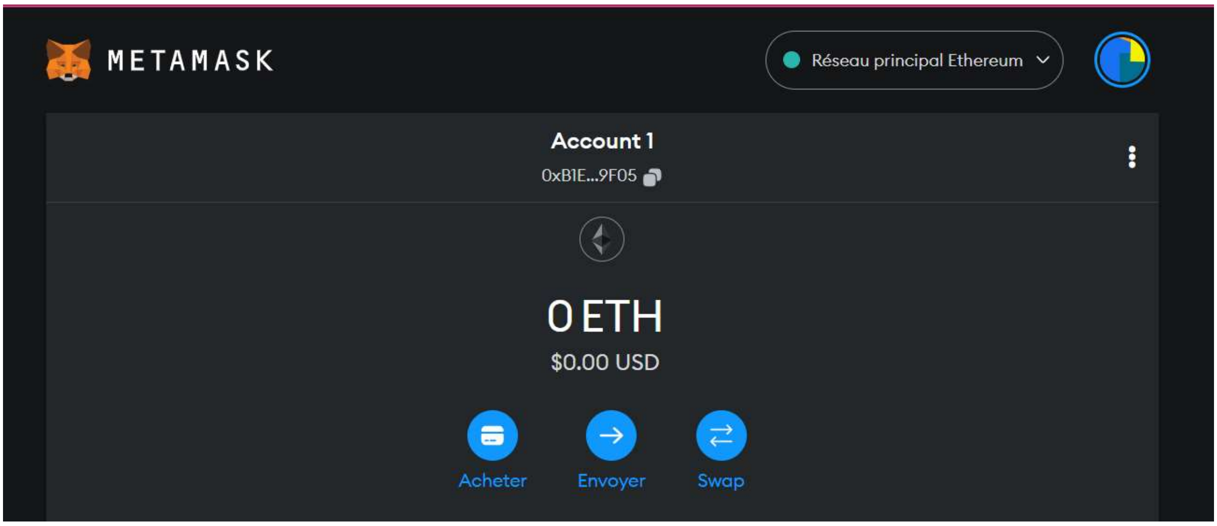
MetaMask | chrome-extension://nkbihfbeogaeaoehlefnkodbefgpgknn/home.html#onboarding/welcome

C’est parti !

MetaMask est un portefeuille sécurisé utilisé par des millions de personnes qui rend l’univers du web3 accessible à toutes et à tous.

Créer un nouveau portefeuille
Importer un portefeuille existant

c. Page d’accueil de Metamask



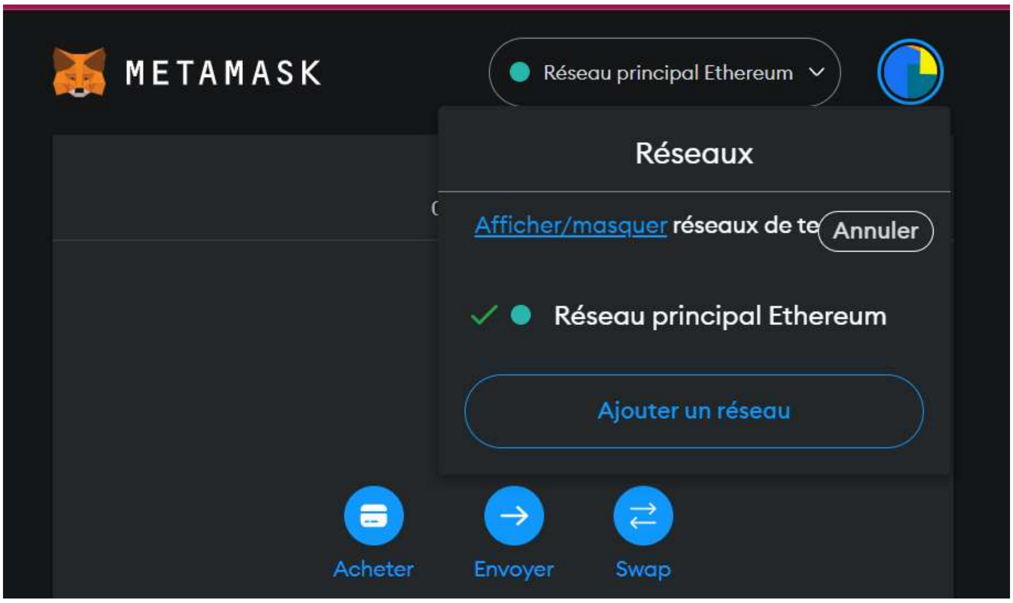
Account 1

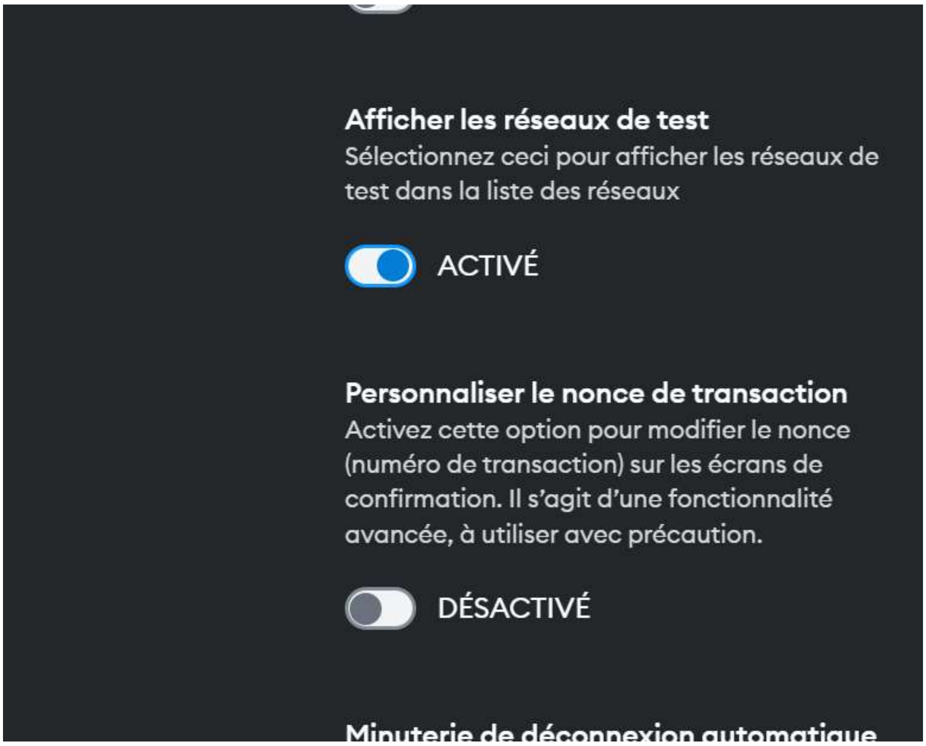
0xBIE...9F05

0 ETH

$0.00 USD

d. Afficher et masquer


METAMASK
Réseau principal Ethereum
Réseaux
Afficher/masquer réseaux de te
Annuler
✓ ● Réseau principal Ethereum
Ajouter un réseau
Acheter
Envoyer
Swap


Afficher les réseaux de test

Sélectionnez ceci pour afficher les réseaux de test dans la liste des réseaux

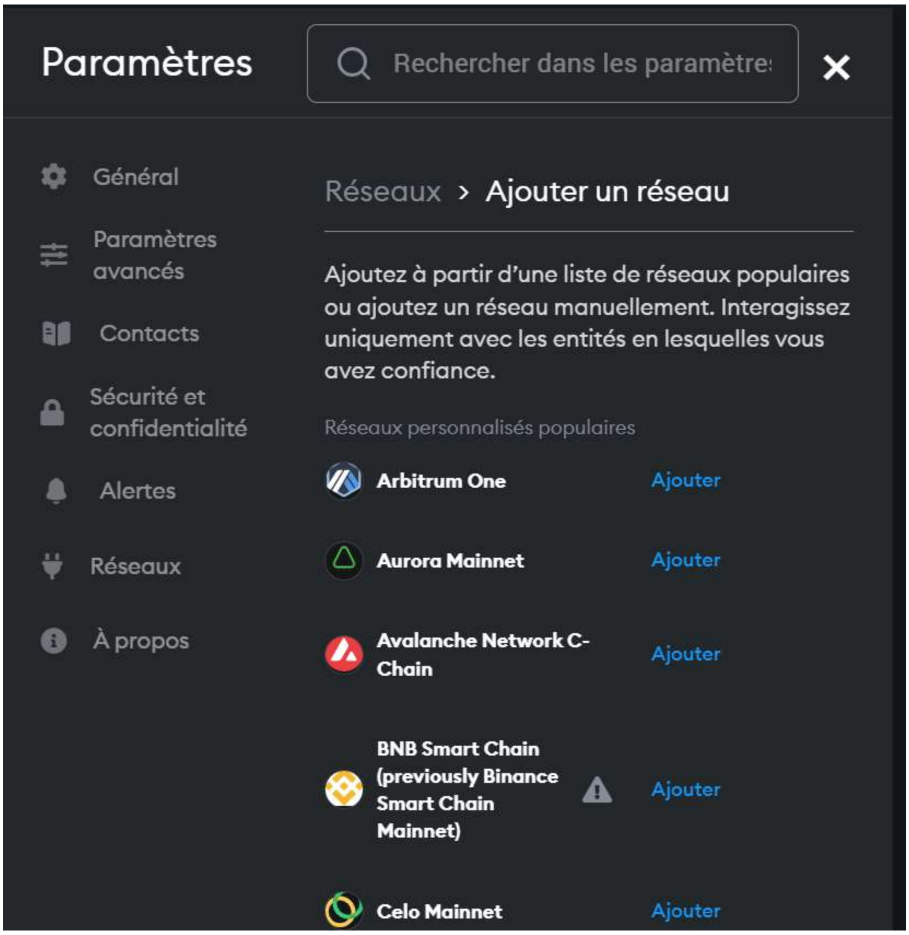
ACTIVÉ

Personnaliser le nonce de transaction

Activez cette option pour modifier le nonce (numéro de transaction) sur les écrans de confirmation. Il s'agit d'une fonctionnalité avancée, à utiliser avec précaution.

DÉSACTIVÉ

Minuterie de déconnexion automatique



Paramètres

Rechercher dans les paramètre:

✕

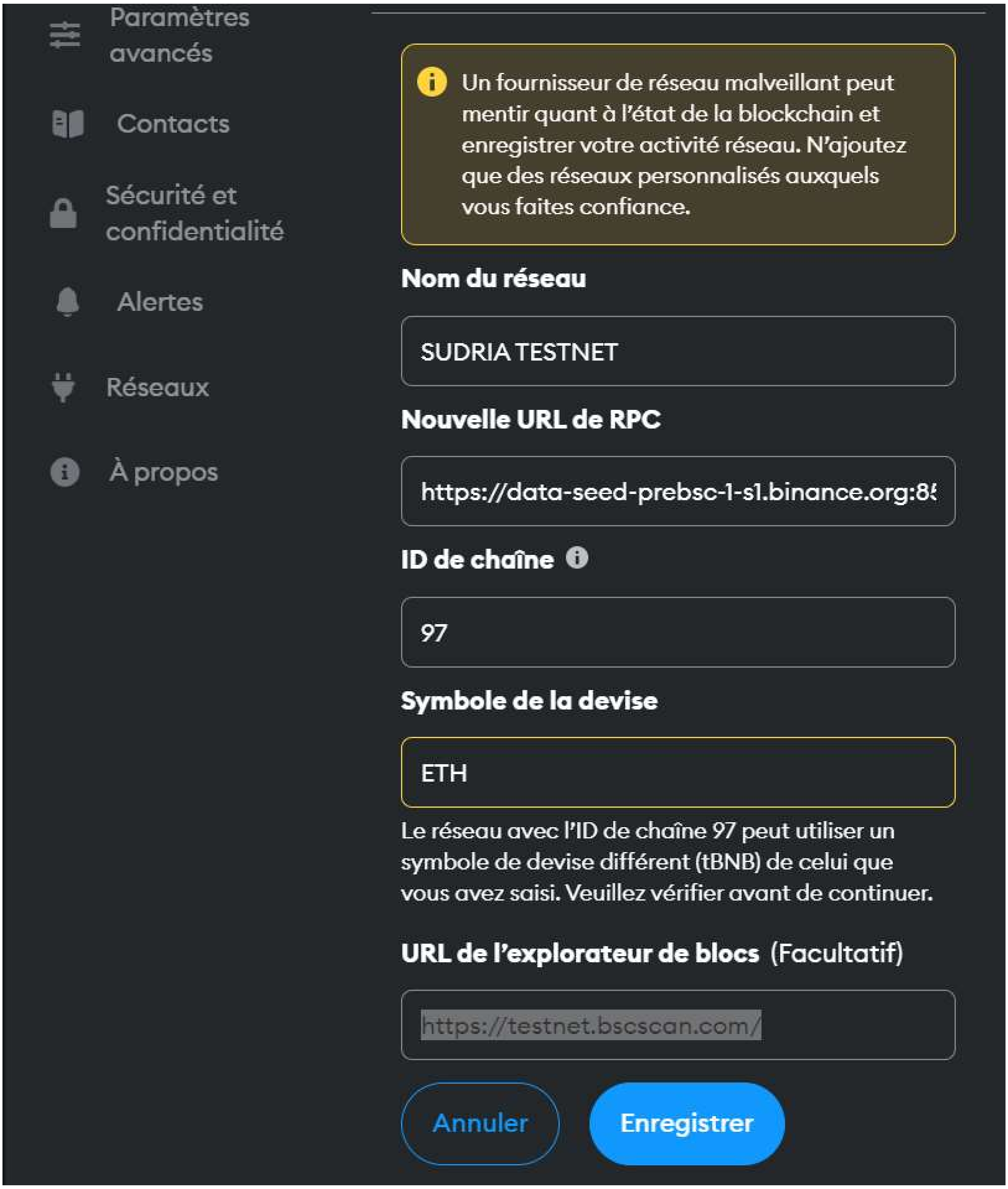
- Général
- Paramètres avancés
- Contacts
- Sécurité et confidentialité
- Alertes
- Réseaux
- À propos

Réseaux > Ajouter un réseau

Ajoutez à partir d'une liste de réseaux populaires ou ajoutez un réseau manuellement. Interagissez uniquement avec les entités en lesquelles vous avez confiance.

Réseaux personnalisés populaires

Arbitrum One	Ajouter
Aurora Mainnet	Ajouter
Avalanche Network C-Chain	Ajouter
BNB Smart Chain (previously Binance Smart Chain Mainnet) ⚠	Ajouter
Celo Mainnet	Ajouter



Un fournisseur de réseau malveillant peut mentir quant à l'état de la blockchain et enregistrer votre activité réseau. N'ajoutez que des réseaux personnalisés auxquels vous faites confiance.

Nom du réseau

SUDRIA TESTNET

Nouvelle URL de RPC

https://data-seed-prebsc-1-s1.binance.org:8

ID de chaîne

97

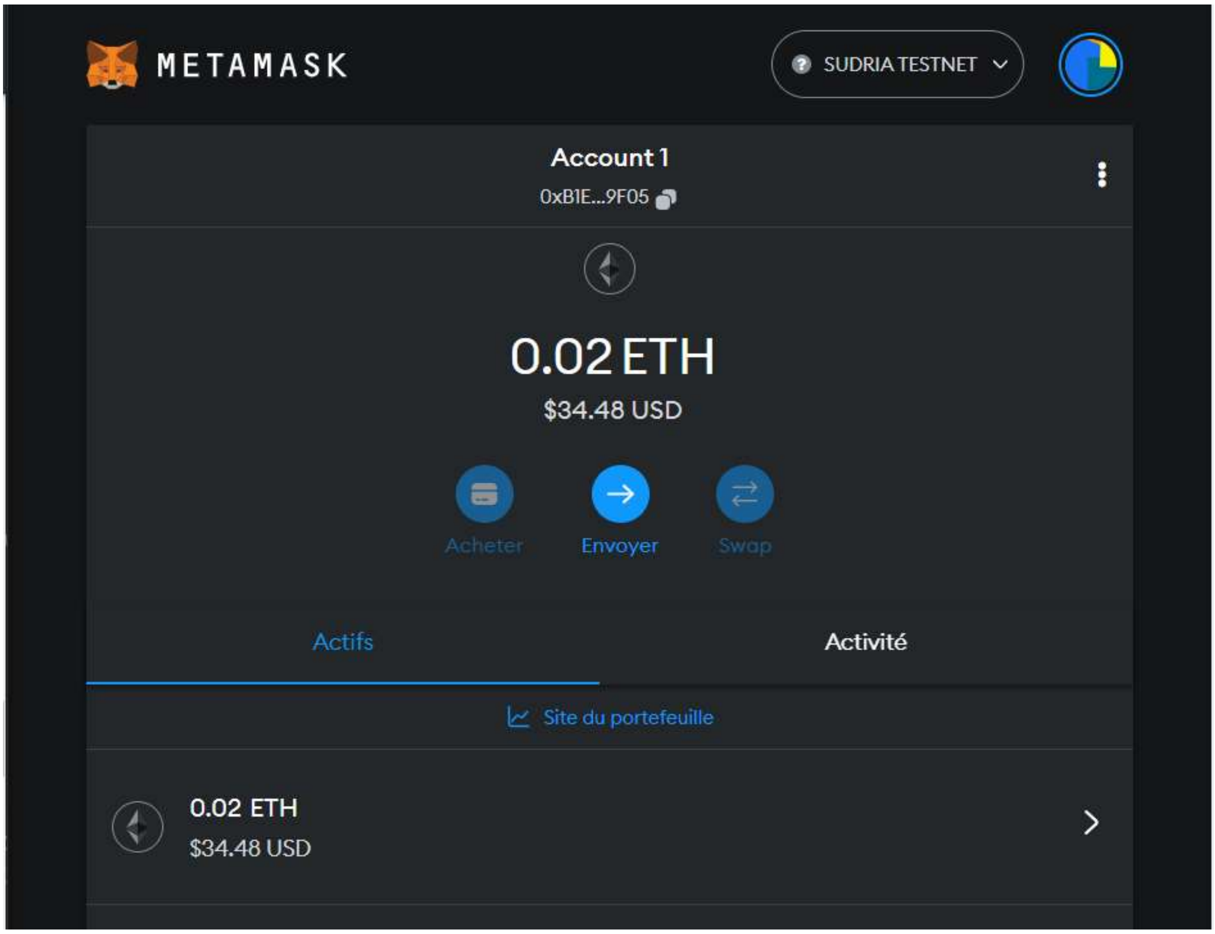
Symbole de la devise

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/



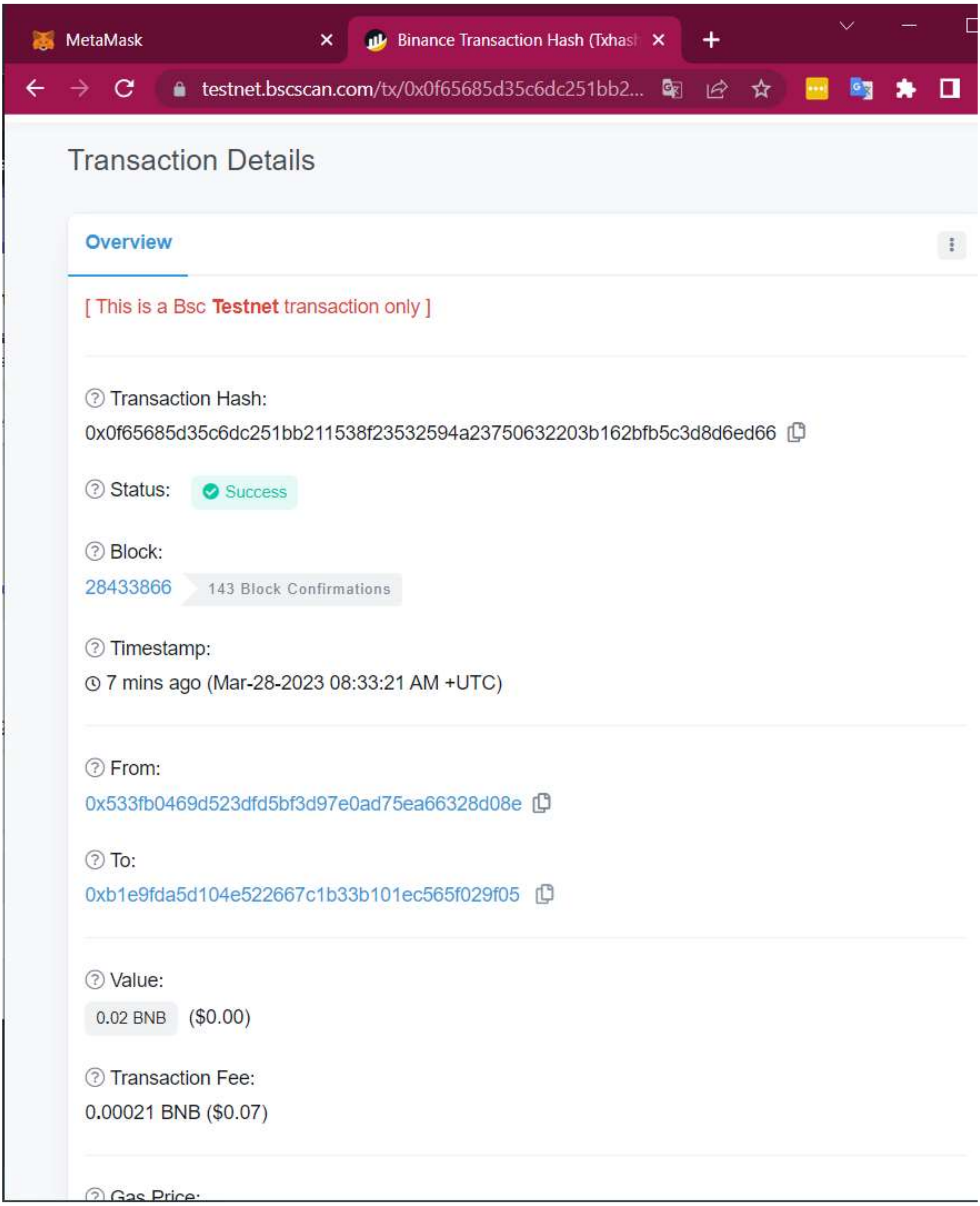
0.02 ETH

$34.48 USD

0.02 ETH

$34.48 USD

f. Détail de la transaction :
https://testnet.bscscan.com/tx/0x0f65685d35c6dc251bb211538f23532594a23750632203b162bfb5c3d8d6ed66


MetaMask
Binance Transaction Hash (Txhash
testnet.bscscan.com/tx/0x0f65685d35c6dc251bb2...

Transaction Details

Overview

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

Transaction Hash:
0x0f65685d35c6dc251bb211538f23532594a23750632203b162bfb5c3d8d6ed66

Status: ✓ Success

Block:
28433866 143 Block Confirmations

Timestamp:
7 mins ago (Mar-28-2023 08:33:21 AM +UTC)

From:
0x533fb0469d523dfd5bf3d97e0ad75ea66328d08e

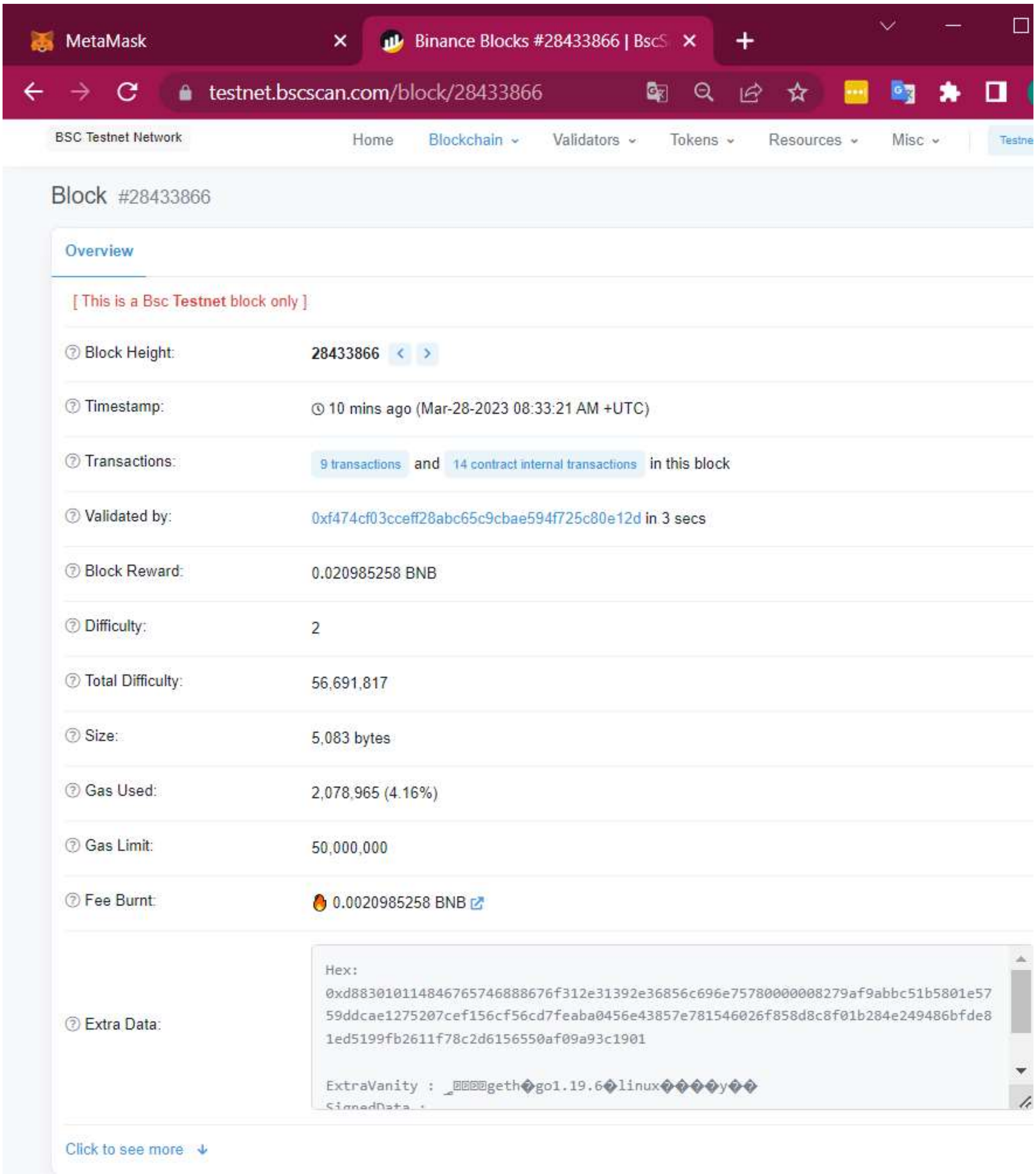
To:
0xb1e9fda5d104e522667c1b33b101ec565f029f05

Value:
0.02 BNB ($0.00)

Transaction Fee:
0.00021 BNB ($0.07)

Gas Price:

g.



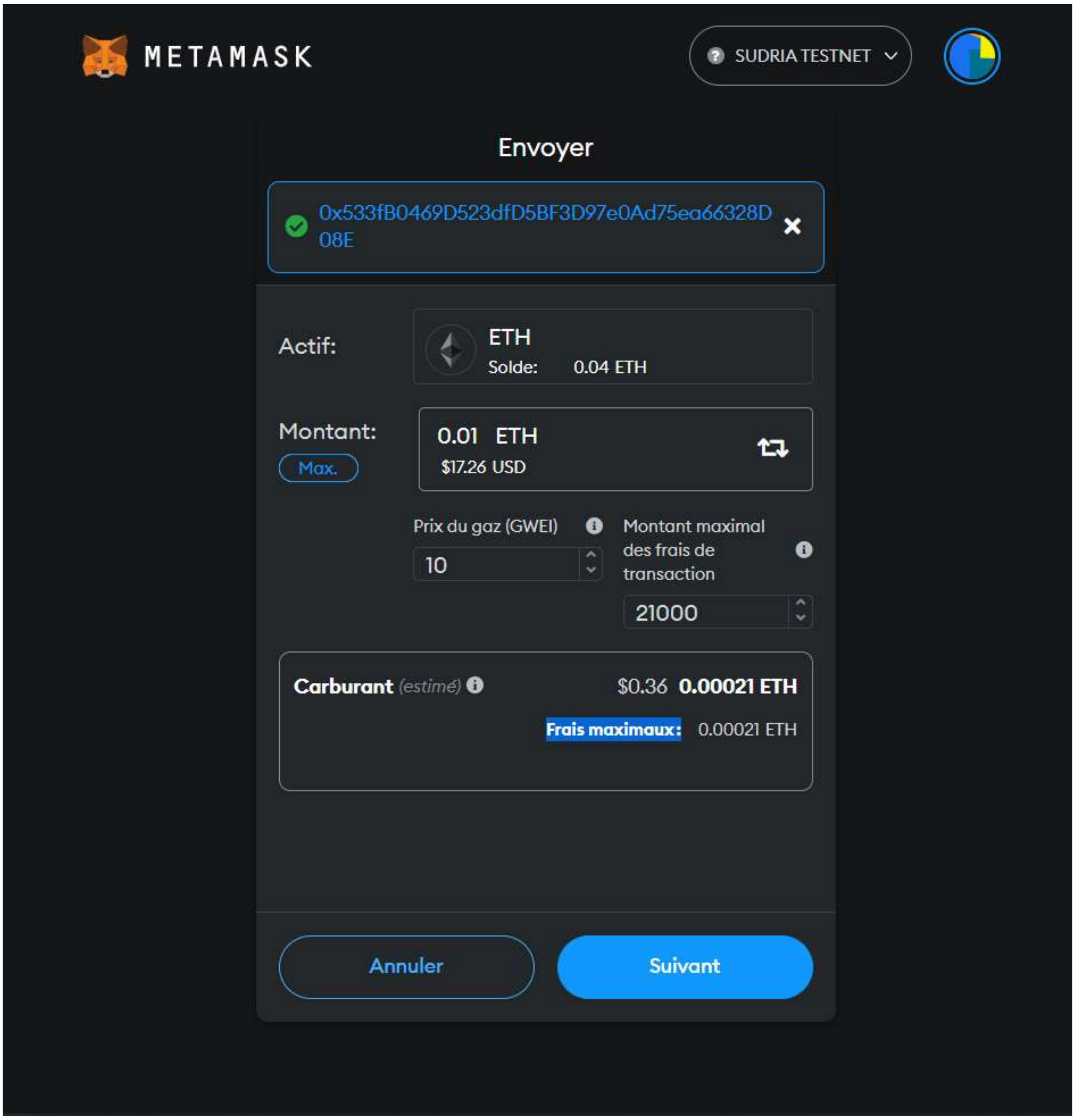
Block #28433866

[This is a Bsc **Testnet** block only]

Block Height:	**28433866**
Timestamp:	10 mins ago (Mar-28-2023 08:33:21 AM +UTC)
Transactions:	9 transactions and 14 contract internal transactions in this block
Validated by:	0xf474cf03cceff28abc65c9cbae594f725c80e12d in 3 secs
Block Reward:	0.020985258 BNB
Difficulty:	2
Total Difficulty:	56,691,817
Size:	5,083 bytes
Gas Used:	2,078,965 (4.16%)
Gas Limit:	50,000,000
Fee Burnt:	🔥 0.0020985258 BNB
Extra Data:	

```
Hex:
0xd883010114846765746888676f312e31392e36856c696e75780000008279af9abbc51b5801e57
59ddcae1275207cef156cf56cd7feaba0456e43857e781546026f858d8c8f01b284e249486bfde8
1ed5199fb2611f78c2d6156550af09a93c1901

ExtraVanity : _����geth�go1.19.6�linux����y��
SignedData :
```

h.



0x533fB0469D523dfD5BF3D97e0Ad75ea66328D08E

Actif: ETH Solde: 0.04 ETH

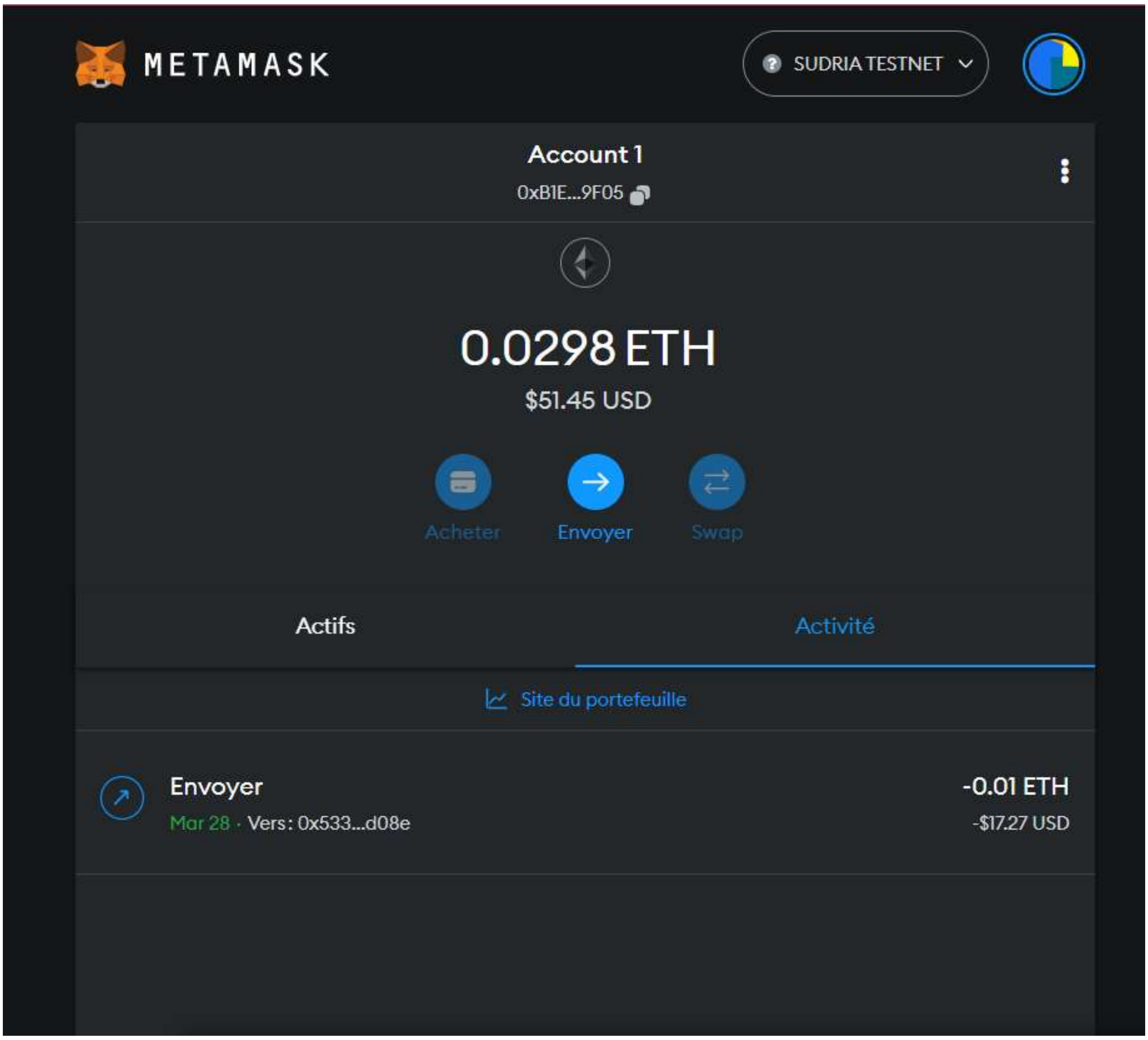
Montant: 0.01 ETH $17.26 USD

Prix du gaz (GWEI) 10

Montant maximal des frais de transaction 21000

Carburant *(estimé)* $0.36 **0.00021 ETH**

Frais maximaux: 0.00021 ETH



METAMASK

SUDRIA TESTNET

Account 1

0xB1E...9F05

0.0298 ETH

$51.45 USD

Acheter

Envoyer

Swap

Actifs

Activité

Site du portefeuille

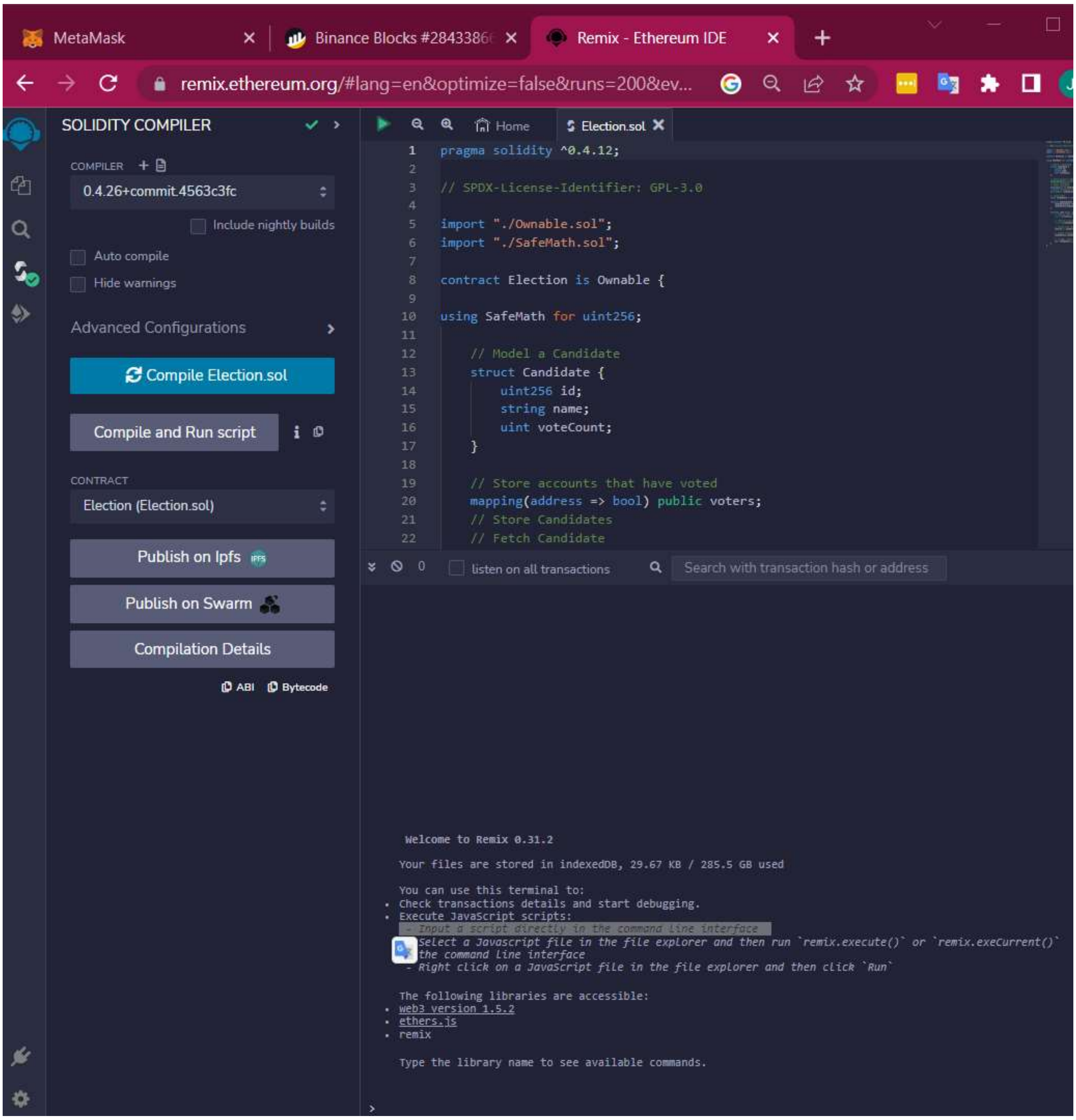
Envoyer

Mar 28 · Vers : 0x533...d08e

-0.01 ETH

-$17.27 USD

I.



COMPILER
0.4.26+commit.4563c3fc

□ Include nightly builds

□ Auto compile

□ Hide warnings

CONTRACT
Election (Election.sol)

```
pragma solidity ^0.4.12;

// SPDX-License-Identifier: GPL-3.0

import "./Ownable.sol";
import "./SafeMath.sol";

contract Election is Ownable {

using SafeMath for uint256;

    // Model a Candidate
    struct Candidate {
        uint256 id;
        string name;
        uint voteCount;
    }

    // Store accounts that have voted
    mapping(address => bool) public voters;
    // Store Candidates
    // Fetch Candidate
```

```
 Welcome to Remix 0.31.2

Your files are stored in indexedDB, 29.67 KB / 285.5 GB used

You can use this terminal to:
• Check transactions details and start debugging.
• Execute JavaScript scripts:
   - Input a script directly in the command line interface
   - Select a Javascript file in the file explorer and then run `remix.execute()` or `remix.exeCurrent()`
     the command line interface
   - Right click on a JavaScript file in the file explorer and then click `Run`

The following libraries are accessible:
• web3 version 1.5.2
• ethers.js
• remix

Type the library name to see available commands.
```

ABI : [

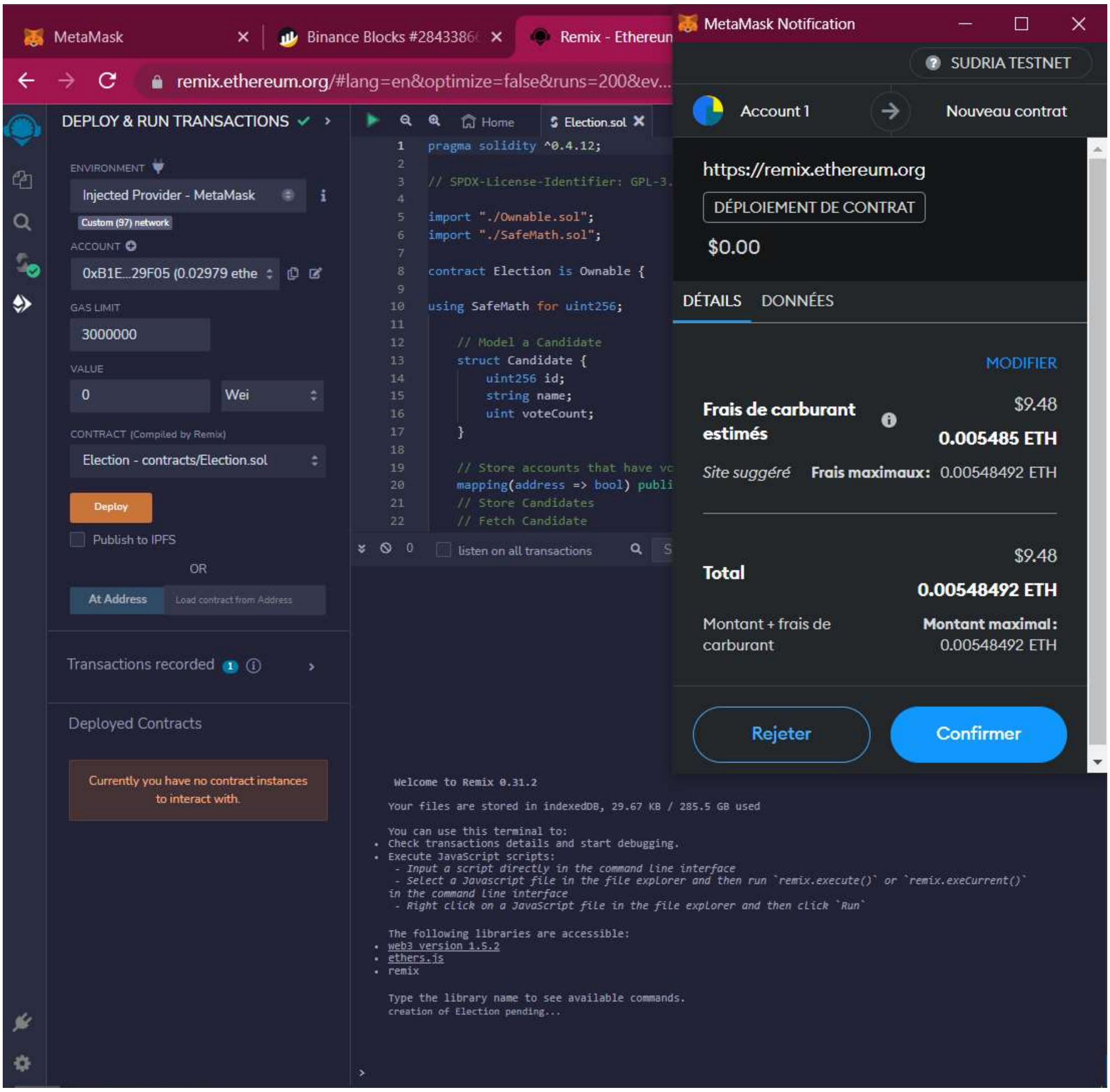
```
	{
		"constant": false,
		"inputs": [
			{
				"name": "_candidateId",
				"type": "uint256"
			}
		],
		"name": "vote",
		"outputs": [],
		"payable": false,
		"stateMutability": "nonpayable",
		"type": "function"
	},
{
        "constant": true,
        "inputs": [],
        "name": "candidatesCount",
        "outputs": [
                {
                        "name": "",
                        "type": "uint256"
                }
        ],
        "payable": false,
        "stateMutability": "view",
        "type": "function"
},
{
        "constant": true,
        "inputs": [
                {
                        "name": "",
                        "type": "uint256"
                }
        ],
        "name": "candidates",
        "outputs": [
                {
                        "name": "id",
                        "type": "uint256"
                },
                {
                        "name": "name",
                        "type": "string"
                },
                {
                        "name": "voteCount",
                        "type": "uint256"
                }
        ],
        "payable": false,
        "stateMutability": "view",
        "type": "function"
},
{
        "constant": false,
        "inputs": [
                {
                        "name": "_name",
                        "type": "string"
                }
        ],
        "name": "addCandidate",
        "outputs": [],
        "payable": false,
        "stateMutability": "nonpayable",
        "type": "function"
},
{
        "constant": true,
        "inputs": [],
        "name": "owner",
        "outputs": [
                {
                        "name": "",
                        "type": "address"
                }
        ],
        "payable": false,
        "stateMutability": "view",
        "type": "function"
},
{
        "constant": true,
        "inputs": [
                {
                        "name": "",
                        "type": "address"
                }
        ],
        "name": "voters",
        "outputs": [
                {
                        "name": "",
                        "type": "bool"
                }
        ],
        "payable": false,
        "stateMutability": "view",
        "type": "function"
},
{
        "constant": false,
        "inputs": [
                {
                        "name": "newOwner",
                        "type": "address"
                }
        ],
        "name": "transferOwnership",
        "outputs": [],
        "payable": false,
        "stateMutability": "nonpayable",
		"type": "function"
	},
	{
		"anonymous": false,
		"inputs": [
			{
				"indexed": true,
				"name": "_candidateId",
				"type": "uint256"
			}
		],
		"name": "votedEvent",
		"type": "event"
	},
	{
		"anonymous": false,
		"inputs": [
			{
				"indexed": true,
				"name": "previousOwner",
				"type": "address"
			},
			{
				"indexed": true,
				"name": "newOwner",
				"type": "address"
			}
		],
		"name": "OwnershipTransferred",
		"type": "event"
	}
]
```

Byte code :

```
6080604052336000806101000a81548173ffffffffffffffffffffffffffffffffffffffff021916908373ffffffffffffffff
ffffffffffffffffffffffff1602179055506108978061005360003960 00f3006080604052600436106100835760
00357c0100000000000000000000000000000000000000000000000000000000900463ffffffff168063
0121b93f146100885780632d35a8a2146100b55780633477ee2e146100e0578063462e91ec14610194
5780638da5cb5b146101fd578063a3ec138d1461025457806f2fde38b146102af575b600080fd5b348
015610094576000 80fd5b506100b3600480360381019080803590602001909291905050506102f2565
b005b3480156100c157600080fd5b506100ca610415565b6040518082815260200191505060405180
910390f35b3480156100ec57600080fd5b5061010b6004803603810190808035906020019092919050
505061041b565b60405180848152602001806020018381526020018281038252848181518152602001
91508051906020019080838360005b838110156101575780820151818401526020810190506101 3c
565b50505050905090810190601f1680156101845780820380516001836020036101000a031916815
260200191505b509450505050506040518091039 0f35b3480156101a057600080fd5b506101fb60048
0360381019080803590602001908201803590602001908080601f0160208091040260200160405190
8101604052809392919081815260200183838082843782019150505050505091929192905050506 10
```

```
4dd565b005b34801561020957600080fd5b5061021261055a565b604051808273fffffffffffffffffffffffffff
fffffffffffff1673ffffffffffffffffffffffffffffffffffffffff16815260200191505060405180910390f35b348015610
26057600080fd5b50610295600480360381019080803573ffffffffffffffffffffffffffffffffffffffff1690602001
90929190505050610057f565b604051808215151515815260200191505060405180910390f35b348015
6102bb57600080fd5b506102f0600480360381019080803573ffffffffffffffffffffffffffffffffffffffff1690602
00190929190505050610059f565b005b600160003373ffffffffffffffffffffffffffffffffffffffff1673fffffffffffffffff
fffffffffffffffffffffff16815260200190815260200160002060009054906101000a900460ff161515156103
4b57600080fd5b60008111801561035d5750600354811115b151561036857600080fd5b600180600
03373ffffffffffffffffffffffffffffffffffffffff1673ffffffffffffffffffffffffffffffffffffffff16815260200190815260200l
60002060006101000a81548160ff021916908315150217905550600260008281526020019081526020
0160002060020160008154809291906001019190505550807ffff3c900d938d21d0990d786e819f29b8
d05c1ef587b462b939609625b684b1660405160405180910390a250565b60035481565b6002602052
806000526040600020600091509050806000015490806001018054600181600116156101000203166
002900480601f01602080910402602001604051908101604052809291908181526020018280546001
81600116156101000203166002900480156104cd5780601f106104a2576101008083540402835291 6
02001916104cd565b820191906000526020600020905b8154815290600101906020018083116104b0
57829003601f168201915b5050505050908060020154905083565b6003600081548092919060010 19
190505550606060405190810160405280600354815260200182815260200160008152506002600060
035481526020019081526020016000206000820151816000015560208201518160010190805190602
001906105499291906107c6565b50604082015181600201559050505050565b6000809054906101000a
900473ffffffffffffffffffffffffffffffffffffffff1681565b60016020528060005260406000206000915054906 10
1000a900460ff1681565b6000809054906101000a900473ffffffffffffffffffffffffffffffffffffffff1673ffffffffff
ffffffffffffffffffffffffffffff163373ffffffffffffffffffffffffffffffffffffffff16141515610663576040517f08c379a000
00000000000000000000000000000000000000000000000000000081526004018080602001828103 8
25260188152602001807f4e6f7420617574686f72697a6564206f7065726174696f6e00000000000000
0081525060200191505060405180910390fd5b600073ffffffffffffffffffffffffffffffffffffffff168173fffffffffff
fffffffffffffffffffffffffffff161415151561070857604051 7f08c379a00000000000000000000000000000000
00000000000000000000000000815260040180806020018281038252601981526020018 07f41646472
6573732073686f756c646e2774206265207a65726f0000000000000081525060200191505060405180
910390fd5b8073ffffffffffffffffffffffffffffffffffffffff16600080905490610 1000a900473ffffffffffffffffffffffffff
ffffffffffffff1673ffffffffffffffffffffffffffffffffffffffff167f8be0079c531659141344cd1fd0a4f28419497f9722
a3daafe3b4186f6b6457e060405160405180910390a3806000806101000a81548173fffffffffffffffffffffffff
fffffffffffffff021916908373ffffffffffffffffffffffffffffffffffffffff16021790555050565b82805460018160011
6156101000203166002900490600052602060002090601f016020900481019282601f10610807578 05
160ff1916838001178555561083556 5b828001600101855558215610835579182015b828111156108345
78251825591602001919060010190610819565b5b5090506108429190610846565b5090565b610868
91905b8082111561086457600081600090555060010161084c565b5090565b905600a165627a7a723
05820c2b1daaf1ae81292340b32ac261cca45ecfd2e95a4ad3032438fcba078984ae80029
```

m. https://testnet.bscscan.com/address/0xf563e73a34f189ab8cb44c4c3acdd2cb7614dde4



ENVIRONMENT: Injected Provider - MetaMask (Custom (97) network)

ACCOUNT: 0xB1E...29F05 (0.02979 ethe

GAS LIMIT: 3000000

VALUE: 0 Wei

CONTRACT (Compiled by Remix): Election - contracts/Election.sol

□ Publish to IPFS

Transactions recorded 1

Deployed Contracts

Currently you have no contract instances to interact with.

```
pragma solidity ^0.4.12;

// SPDX-License-Identifier: GPL-3.

import "./Ownable.sol";
import "./SafeMath.sol";

contract Election is Ownable {

using SafeMath for uint256;

    // Model a Candidate
    struct Candidate {
        uint256 id;
        string name;
        uint voteCount;
    }

    // Store accounts that have vo
    mapping(address => bool) publi
    // Store Candidates
    // Fetch Candidate
```

https://remix.ethereum.org

DÉPLOIEMENT DE CONTRAT

$0.00

Frais de carburant estimés: $9.48 — 0.005485 ETH

Site suggéré — Frais maximaux : 0.00548492 ETH

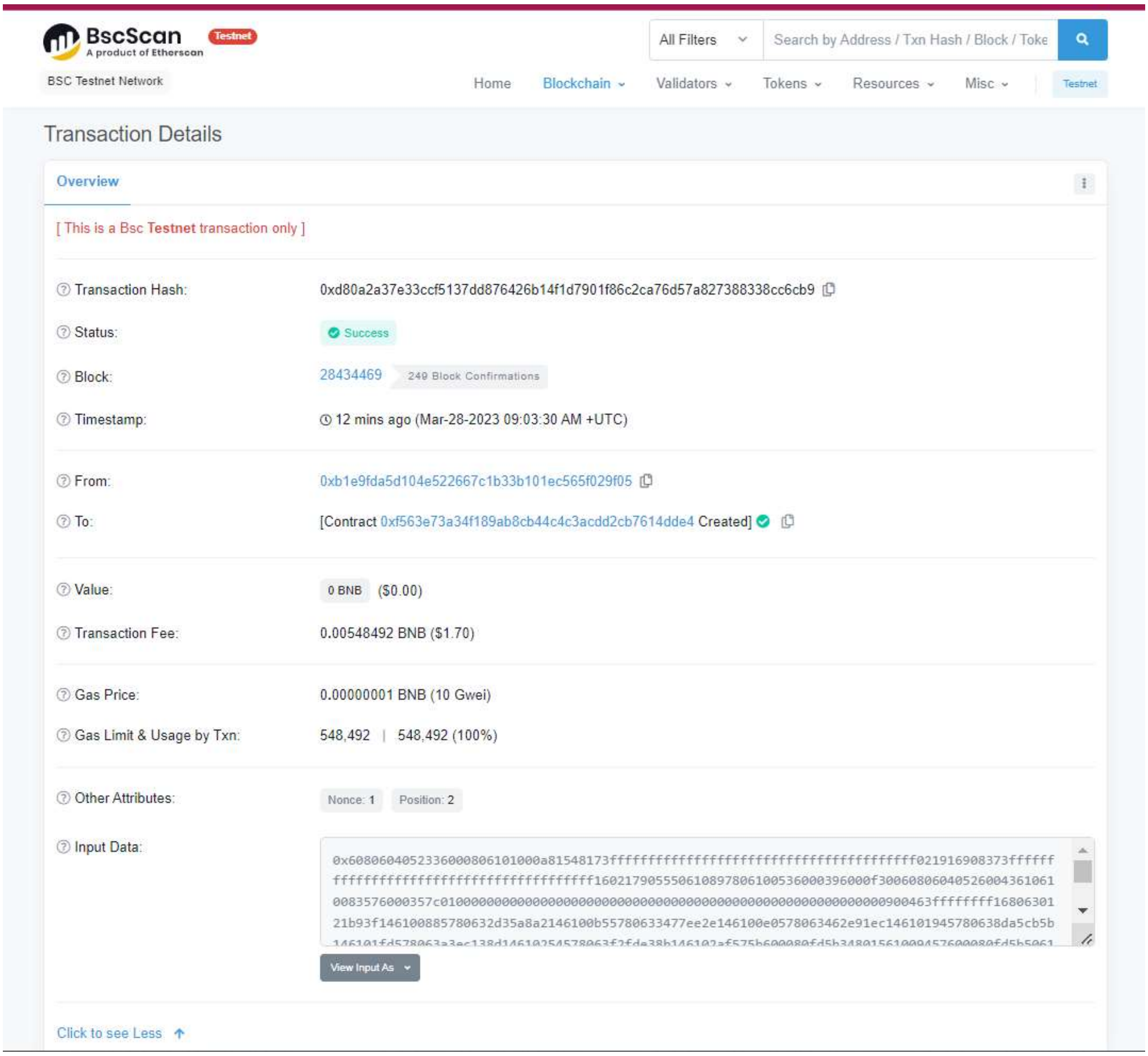
Total: $9.48 — 0.00548492 ETH

Montant + frais de carburant — Montant maximal : 0.00548492 ETH

```
Welcome to Remix 0.31.2

Your files are stored in indexedDB, 29.67 KB / 285.5 GB used

You can use this terminal to:
• Check transactions details and start debugging.
• Execute JavaScript scripts:
  - Input a script directly in the command line interface
  - Select a Javascript file in the file explorer and then run `remix.execute()` or `remix.exeCurrent()`
in the command line interface
  - Right click on a JavaScript file in the file explorer and then click `Run`

The following libraries are accessible:
• web3 version 1.5.2
• ethers.js
• remix

Type the library name to see available commands.
creation of Election pending...
```

Les « Transaction fees » ne sont pas les mêmes entre les deux transactions. Ces frais permettent de publier le smart contract.

L’adresse publique de mon smart contract est la suivante : 0xF563e73a34F189aB8cb44c4C3AcDD2cB7614Dde4



Transaction Details

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

Transaction Hash: 0xd80a2a37e33ccf5137dd876426b14f1d7901f86c2ca76d57a827388338cc6cb9

Status: Success

Block: 28434469 249 Block Confirmations

Timestamp: 12 mins ago (Mar-28-2023 09:03:30 AM +UTC)

From: 0xb1e9fda5d104e522667c1b33b101ec565f029f05

To: [Contract 0xf563e73a34f189ab8cb44c4c3acdd2cb7614dde4 Created] ✓

Value: 0 BNB ($0.00)

Transaction Fee: 0.00548492 BNB ($1.70)

Gas Price: 0.00000001 BNB (10 Gwei)

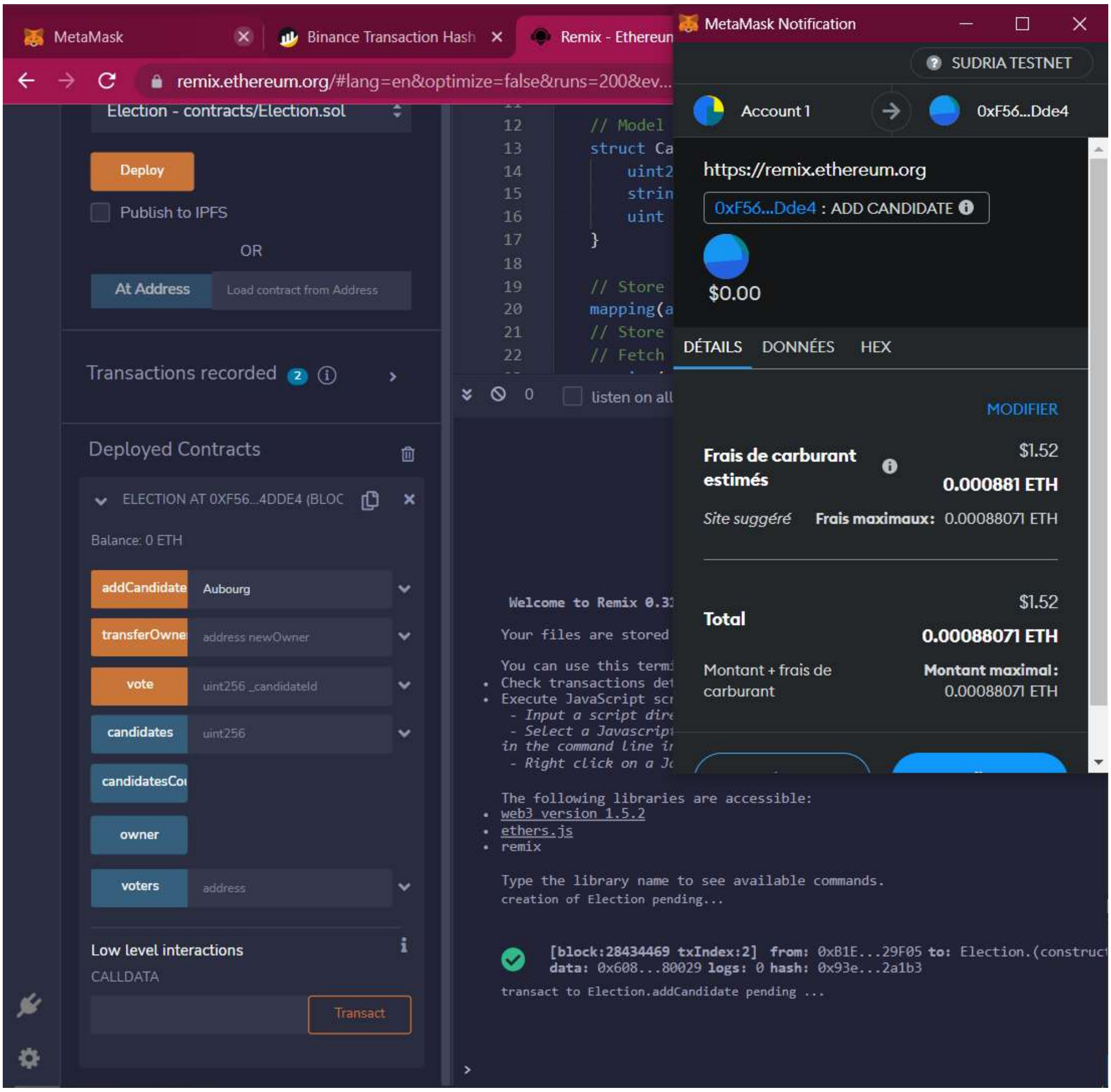
Gas Limit & Usage by Txn: 548,492 | 548,492 (100%)

Other Attributes: Nonce: 1 Position: 2

Input Data:

```
0x6080604052336000806101000a81548173ffffffffffffffffffffffffffffffffffffffff021916908373ffffff
ffffffffffffffffffffffffffffffffff1602179055506108978061005360003960000f3006080604052600436106
10083576000357c0100000000000000000000000000000000000000000000000000000000900463ffffffff16806301
21b93f146100885780632d35a8a2146100b55780633477ee2e146100e0578063462e91ec14610194578063 8da5cb5b
146101fd578063a3ec138d14610254578063f2fde38b146102af575b600080fd5b348015610094576000 80fd5b5061
```

n.



Balance: 0 ETH

addCandidate: Aubourg

```
// Model
struct Ca
    uint2
    strin
    uint
}

// Store
mapping(a
// Store
// Fetch
```

```
Welcome to Remix 0.3

Your files are stored

You can use this termi
 • Check transactions det
 • Execute JavaScript scr
    - Input a script dire
    - Select a Javascript
 in the command line in
    - Right click on a Jc

The following libraries are accessible:
 • web3 version 1.5.2
 • ethers.js
 • remix

Type the library name to see available commands.
creation of Election pending...

[block:28434469 txIndex:2] from: 0xB1E...29F05 to: Election.(construct
data: 0x608...80029 logs: 0 hash: 0x93e...2a1b3
transact to Election.addCandidate pending ...
```

https://remix.ethereum.org

0xF56...Dde4 : ADD CANDIDATE

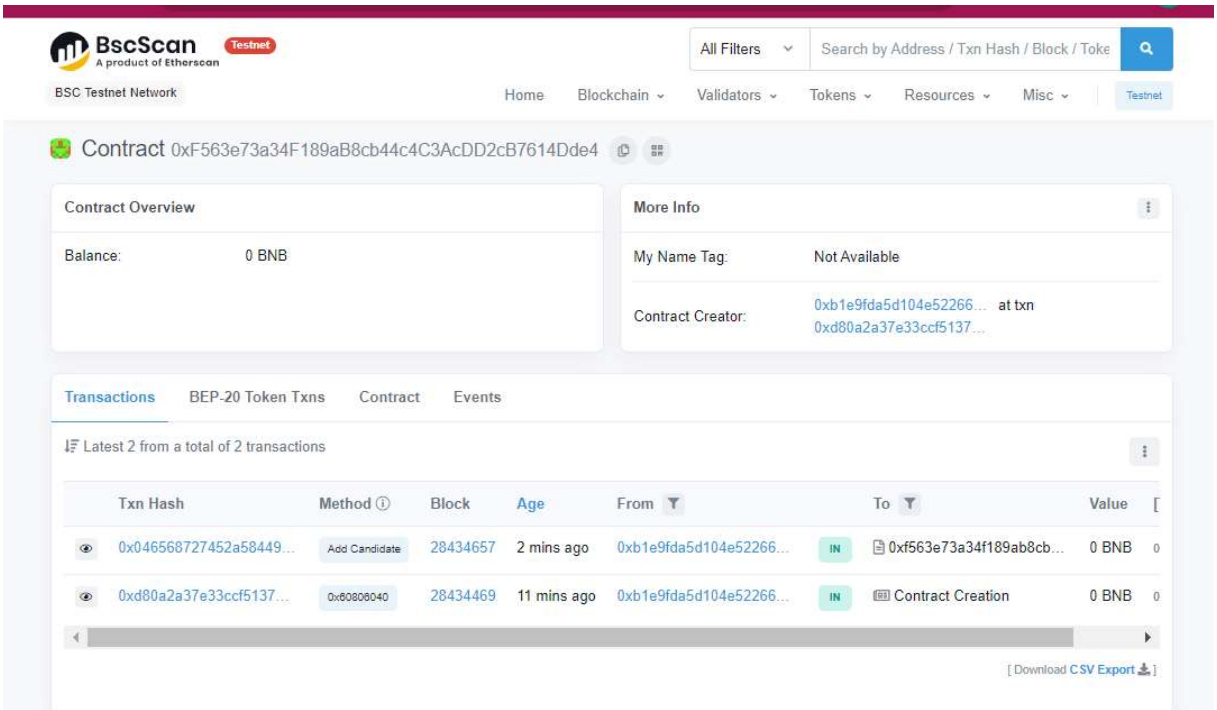
$0.00

Frais de carburant estimés $1.52 **0.000881 ETH**

Site suggéré **Frais maximaux:** 0.00088071 ETH

Total $1.52 **0.00088071 ETH**

Montant + frais de carburant **Montant maximal:** 0.00088071 ETH



Contract 0xF563e73a34F189aB8cb44c4C3AcDD2cB7614Dde4

Contract Overview

Balance: 0 BNB

More Info

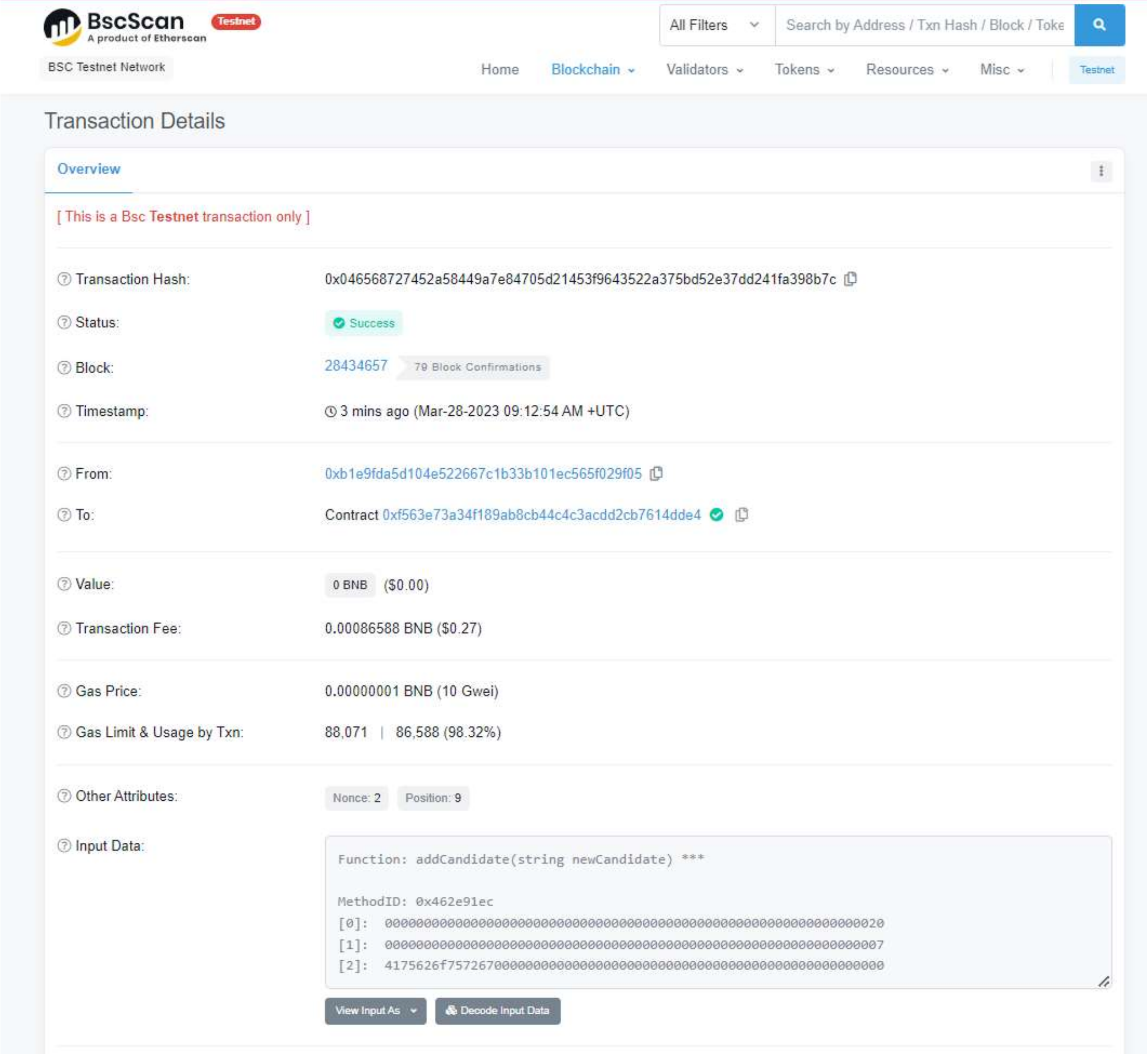
My Name Tag: Not Available

Contract Creator: 0xb1e9fda5d104e52266... at txn 0xd80a2a37e33ccf5137...

Latest 2 from a total of 2 transactions

	Txn Hash	Method	Block	Age	From		To	Value	[
👁	0x046568727452a58449...	Add Candidate	28434657	2 mins ago	0xb1e9fda5d104e52266...	IN	0xf563e73a34f189ab8cb...	0 BNB	0
👁	0xd80a2a37e33ccf5137...	0x60806040	28434469	11 mins ago	0xb1e9fda5d104e52266...	IN	Contract Creation	0 BNB	0

o.



Transaction Details

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

Transaction Hash: 0x046568727452a58449a7e84705d21453f9643522a375bd52e37dd241fa398b7c

Status: Success

Block: 28434657 79 Block Confirmations

Timestamp: 3 mins ago (Mar-28-2023 09:12:54 AM +UTC)

From: 0xb1e9fda5d104e522667c1b33b101ec565f029f05

To: Contract 0xf563e73a34f189ab8cb44c4c3acdd2cb7614dde4

Value: 0 BNB ($0.00)

Transaction Fee: 0.00086588 BNB ($0.27)

Gas Price: 0.00000001 BNB (10 Gwei)

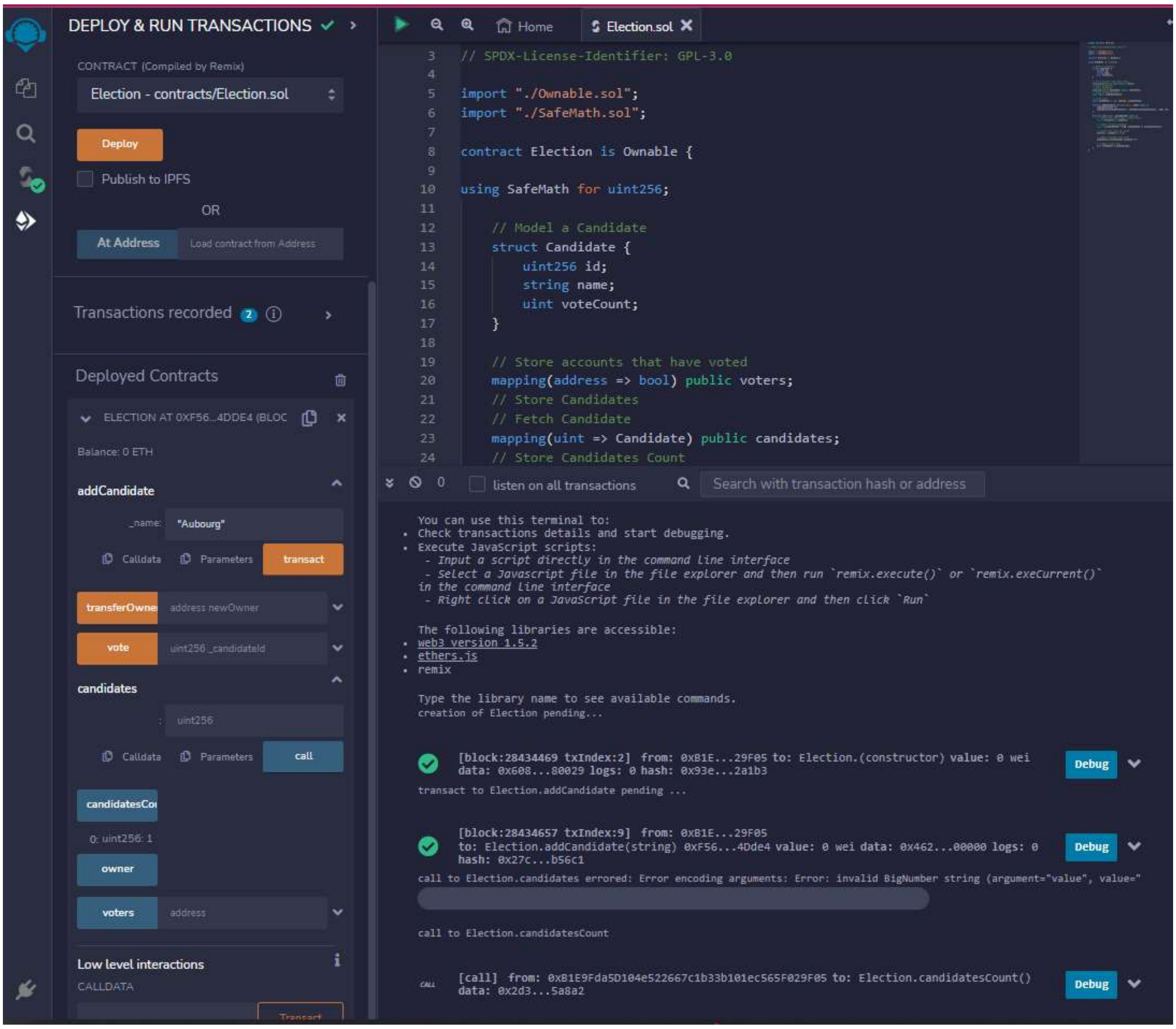
Gas Limit & Usage by Txn: 88,071 | 86,588 (98.32%)

Other Attributes: Nonce: 2 Position: 9

Input Data:

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

MethodID: 0x462e91ec
[0]:  0000000000000000000000000000000000000000000000000000000000000020
[1]:  0000000000000000000000000000000000000000000000000000000000000007
[2]:  4175626f75726700000000000000000000000000000000000000000000000000
```

p.



Election - contracts/Election.sol

ELECTION AT 0XF56...4DDE4 (BLOC

Balance: 0 ETH

addCandidate

_name: "Aubourg"

transferOwnership: address newOwner

vote: uint256 _candidateId

candidates: uint256

candidatesCount

0: uint256: 1

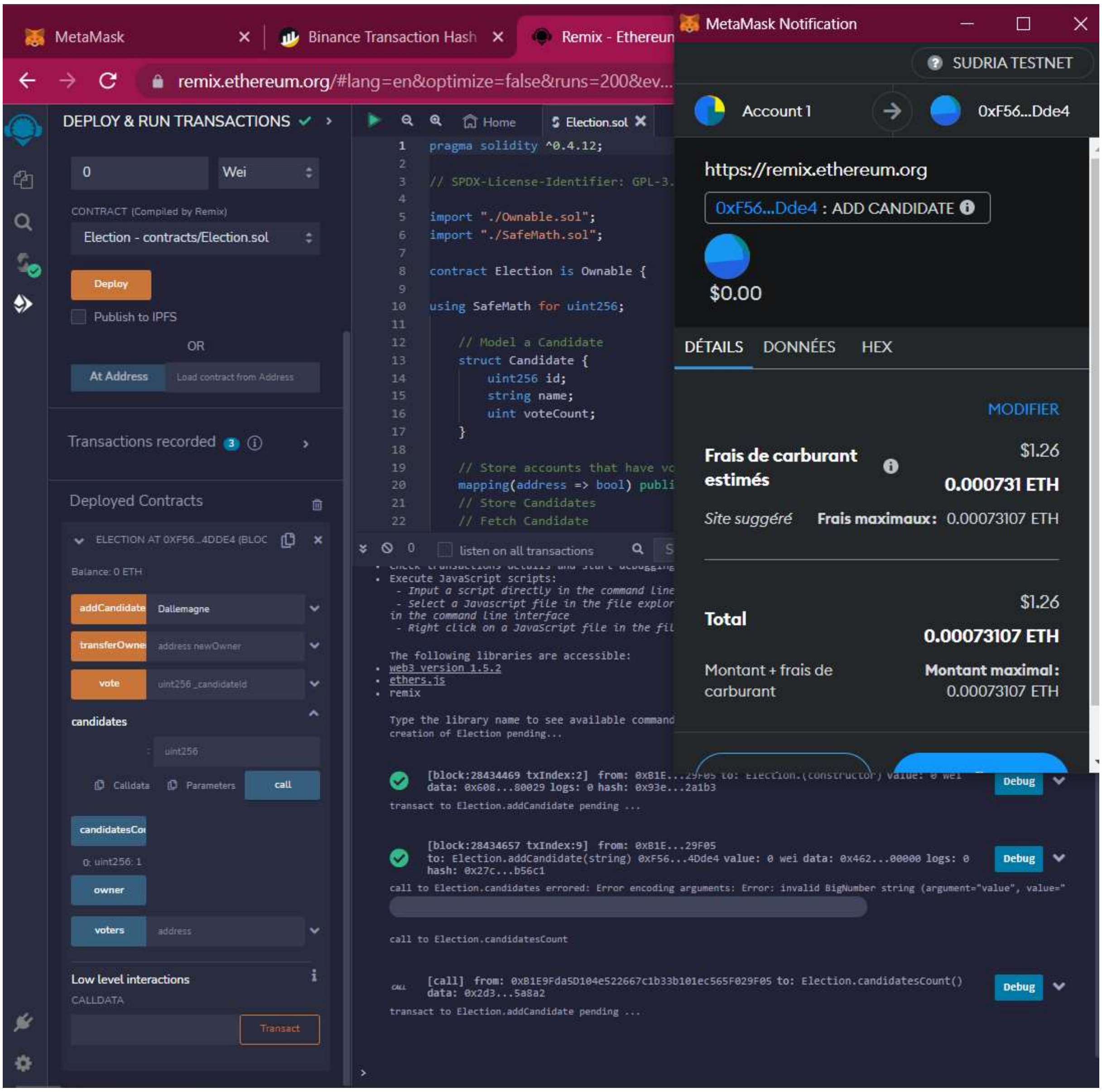
voters: address

```
// SPDX-License-Identifier: GPL-3.0

import "./Ownable.sol";
import "./SafeMath.sol";

contract Election is Ownable {

using SafeMath for uint256;

    // Model a Candidate
    struct Candidate {
        uint256 id;
        string name;
        uint voteCount;
    }

    // Store accounts that have voted
    mapping(address => bool) public voters;
    // Store Candidates
    // Fetch Candidate
    mapping(uint => Candidate) public candidates;
    // Store Candidates Count
```

```
You can use this terminal to:
• Check transactions details and start debugging.
• Execute JavaScript scripts:
  - Input a script directly in the command line interface
  - Select a Javascript file in the file explorer and then run `remix.execute()` or `remix.execCurrent()`
in the command line interface
  - Right click on a JavaScript file in the file explorer and then click `Run`

The following libraries are accessible:
• web3 version 1.5.2
• ethers.js
• remix

Type the library name to see available commands.
creation of Election pending...

[block:28434469 txIndex:2] from: 0xB1E...29F05 to: Election.(constructor) value: 0 wei
data: 0x608...80029 logs: 0 hash: 0x93e...2a1b3
transact to Election.addCandidate pending ...

[block:28434657 txIndex:9] from: 0xB1E...29F05
to: Election.addCandidate(string) 0xF56...4Dde4 value: 0 wei data: 0x462...00000 logs: 0
hash: 0x27c...b56c1
call to Election.candidates errored: Error encoding arguments: Error: invalid BigNumber string (argument="value", value="

call to Election.candidatesCount

CALL [call] from: 0xB1E9Fda5D104e522667c1b33b101ec565F029F05 to: Election.candidatesCount()
data: 0x2d3...5a8a2
```

CandidateID = 1

q.



0 Wei

CONTRACT (Compiled by Remix)
Election - contracts/Election.sol

ELECTION AT 0XF56...4DDE4 (BLOC

Balance: 0 ETH

addCandidate: Dallemagne

0: uint256: 1

```
pragma solidity ^0.4.12;

// SPDX-License-Identifier: GPL-3.

import "./Ownable.sol";
import "./SafeMath.sol";

contract Election is Ownable {

using SafeMath for uint256;

    // Model a Candidate
    struct Candidate {
        uint256 id;
        string name;
        uint voteCount;
    }

    // Store accounts that have vo
    mapping(address => bool) publi
    // Store Candidates
    // Fetch Candidate
```

```
• Execute JavaScript scripts:
   - Input a script directly in the command line
   - Select a Javascript file in the file explor
  in the command line interface
   - Right click on a JavaScript file in the fil

  The following libraries are accessible:
• web3 version 1.5.2
• ethers.js
• remix

  Type the library name to see available command
  creation of Election pending...

  [block:28434469 txIndex:2] from: 0xB1E...29F05 to: Election.(constructor) value: 0 wei
  data: 0x608...80029 logs: 0 hash: 0x93e...2a1b3
  transact to Election.addCandidate pending ...

  [block:28434657 txIndex:9] from: 0xB1E...29F05
  to: Election.addCandidate(string) 0xF56...4Dde4 value: 0 wei data: 0x462...00000 logs: 0
  hash: 0x27c...b56c1
  call to Election.candidates errored: Error encoding arguments: Error: invalid BigNumber string (argument="value", value="

  call to Election.candidatesCount

  CALL [call] from: 0xB1E9Fda5D104e522667c1b33b101ec565F029F05 to: Election.candidatesCount()
  data: 0x2d3...5a8a2
  transact to Election.addCandidate pending ...
```

https://remix.ethereum.org

0xF56...Dde4 : ADD CANDIDATE

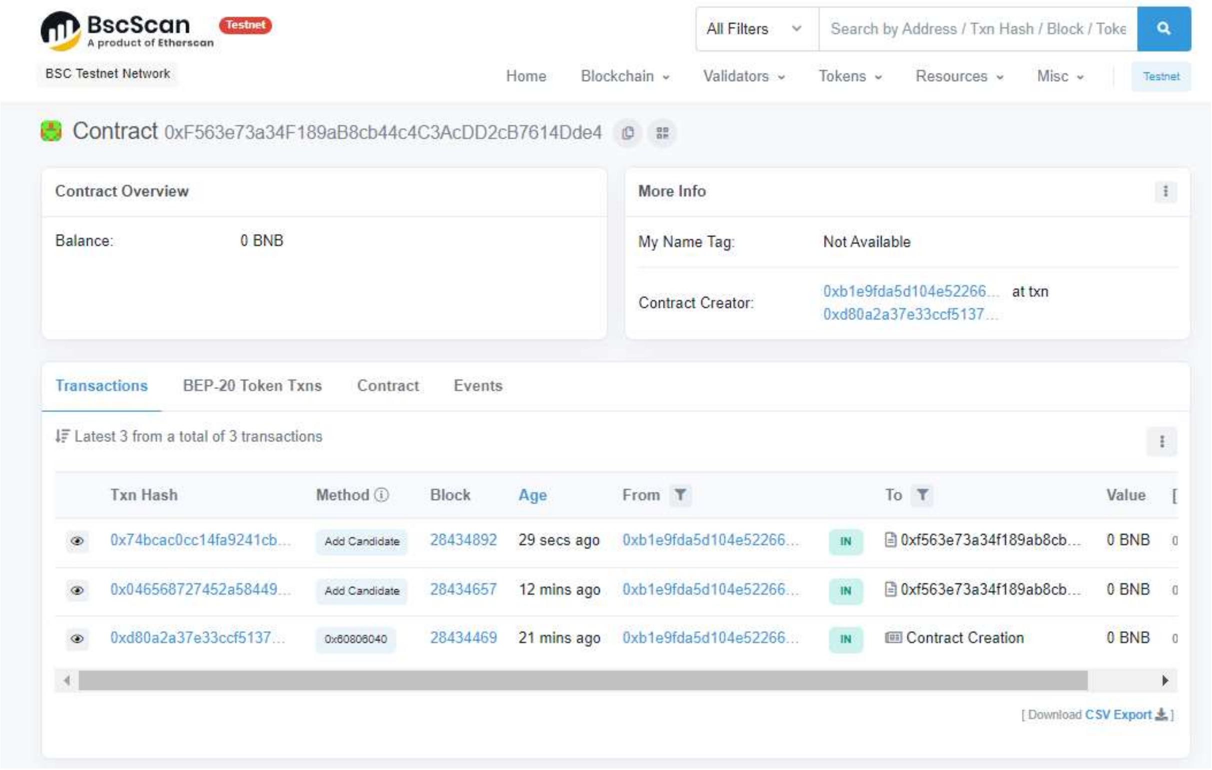
$0.00

Frais de carburant estimés — $1.26 — 0.000731 ETH

Site suggéré — Frais maximaux : 0.00073107 ETH

Total — $1.26 — 0.00073107 ETH

Montant + frais de carburant — Montant maximal : 0.00073107 ETH



Contract 0xF563e73a34F189aB8cb44c4C3AcDD2cB7614Dde4

Contract Overview

Balance: 0 BNB

More Info

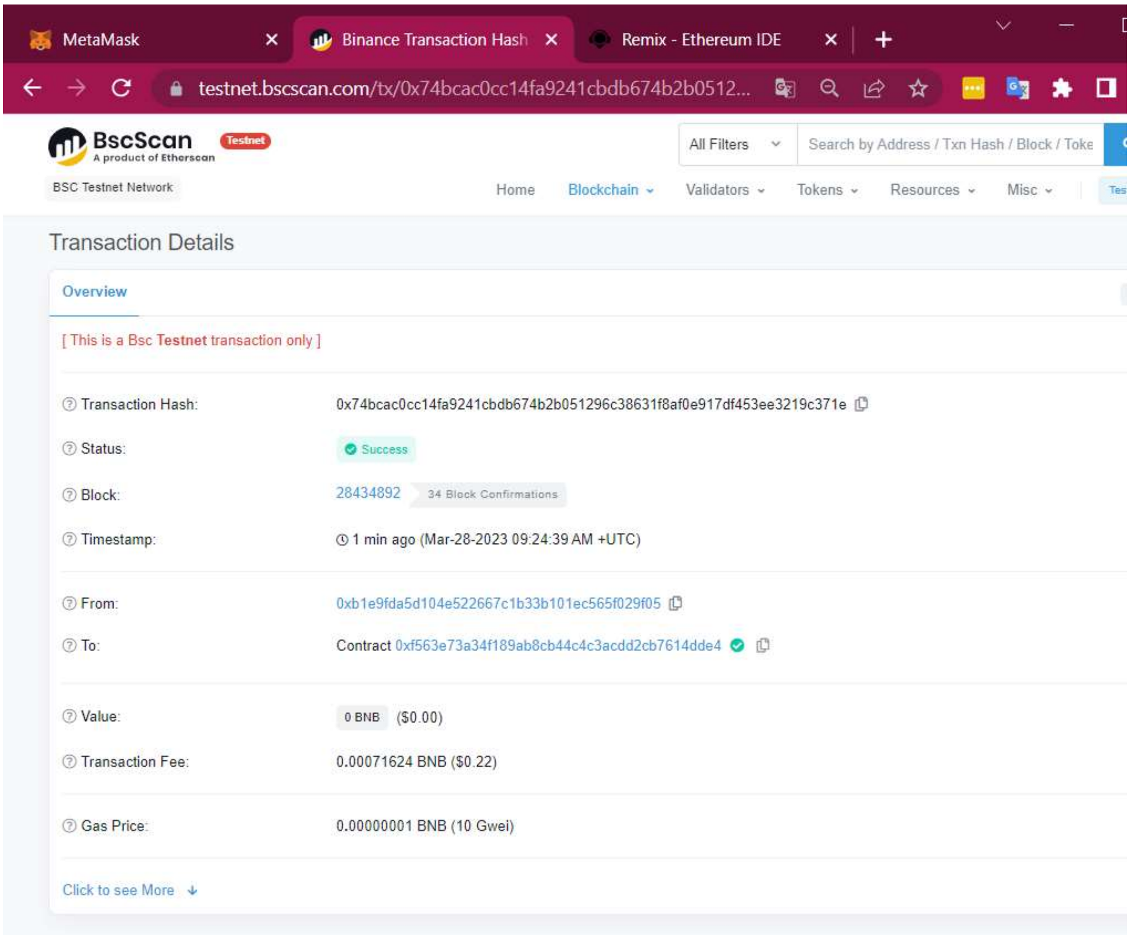
My Name Tag: Not Available

Contract Creator: 0xb1e9fda5d104e52266... at txn 0xd80a2a37e33ccf5137...

Latest 3 from a total of 3 transactions

Txn Hash	Method	Block	Age	From		To	Value	[
0x74bcac0cc14fa9241cb...	Add Candidate	28434892	29 secs ago	0xb1e9fda5d104e52266...	IN	0xf563e73a34f189ab8cb...	0 BNB	0
0x046568727452a58449...	Add Candidate	28434657	12 mins ago	0xb1e9fda5d104e52266...	IN	0xf563e73a34f189ab8cb...	0 BNB	0
0xd80a2a37e33ccf5137...	0x60806040	28434469	21 mins ago	0xb1e9fda5d104e52266...	IN	Contract Creation	0 BNB	0

[Download CSV Export]



Transaction Details

Overview

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

Transaction Hash: 0x74bcac0cc14fa9241cbdb674b2b051296c38631f8af0e917df453ee3219c371e

Status: Success

Block: 28434892 34 Block Confirmations

Timestamp: 1 min ago (Mar-28-2023 09:24:39 AM +UTC)

From: 0xb1e9fda5d104e522667c1b33b101ec565f029f05

To: Contract 0xf563e73a34f189ab8cb44c4c3acdd2cb7614dde4

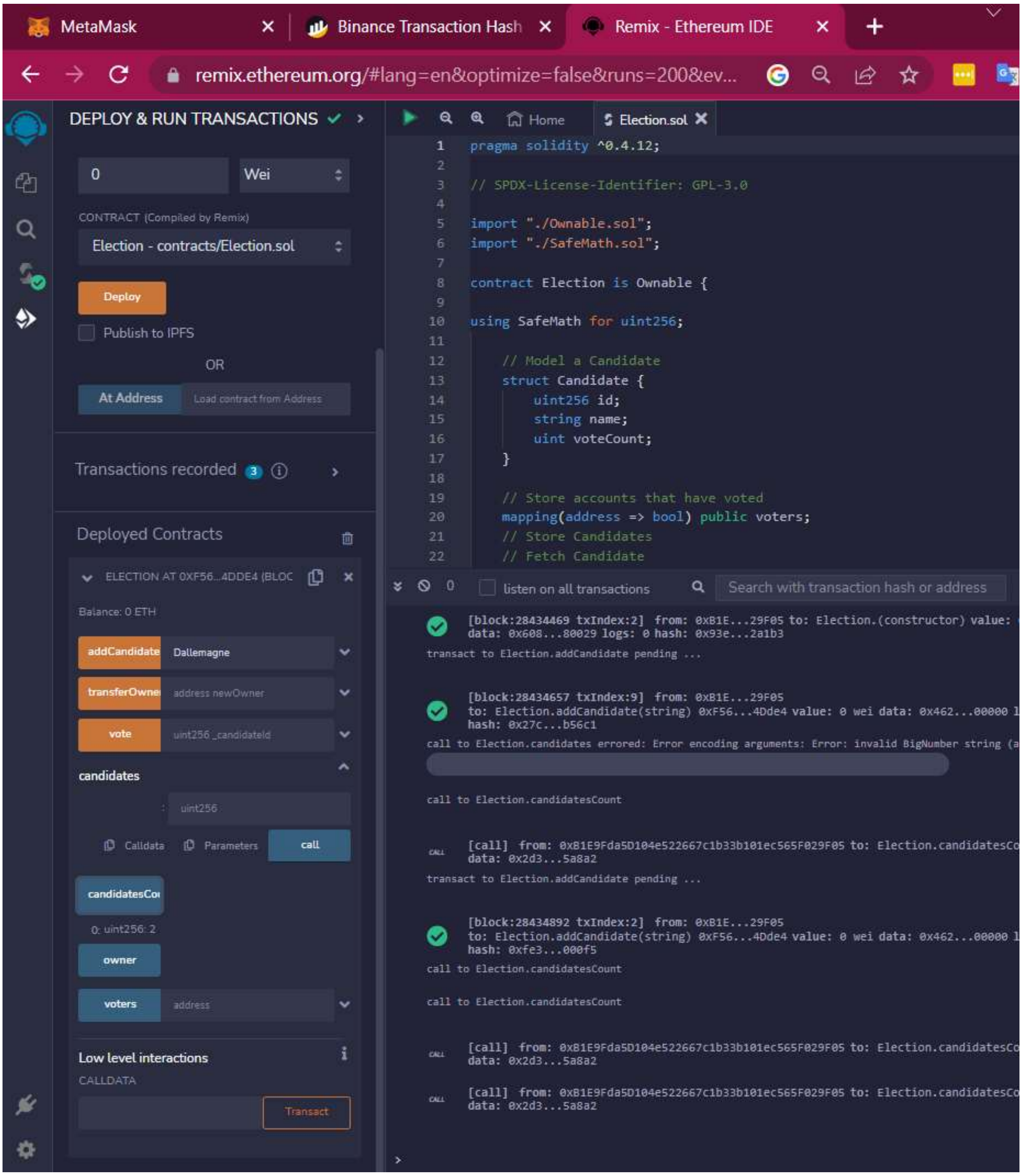
Value: 0 BNB ($0.00)

Transaction Fee: 0.00071624 BNB ($0.22)

Gas Price: 0.00000001 BNB (10 Gwei)

Click to see More

r.



VALUE: 0 Wei

CONTRACT (Compiled by Remix): Election - contracts/Election.sol

ELECTION AT 0XF56...4DDE4 (BLOC

Balance: 0 ETH

addCandidate: Dallemagne

transferOwne: address newOwner

vote: uint256 _candidateId

candidates: uint256

candidatesCou

0: uint256: 2

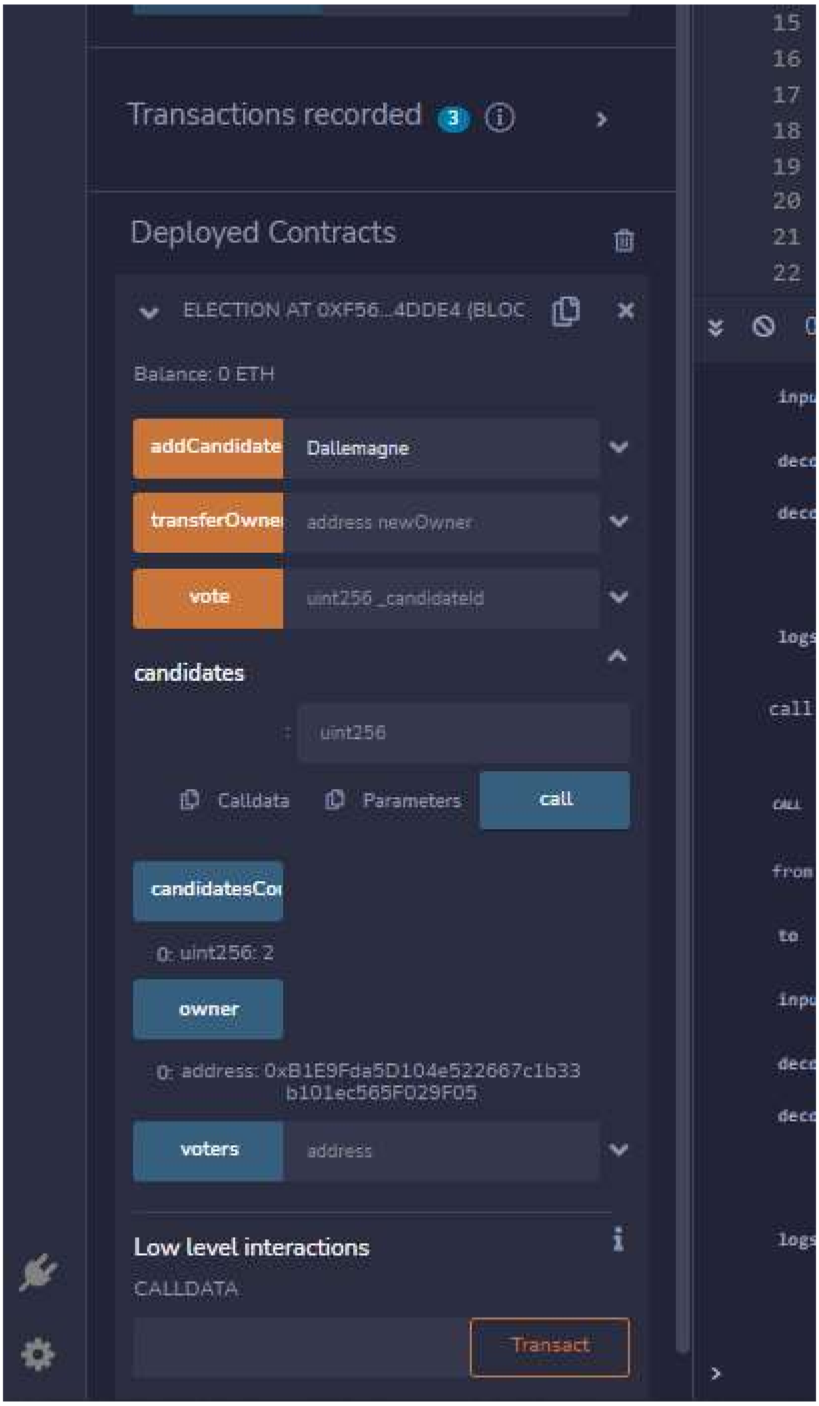
voters: address

```
pragma solidity ^0.4.12;

// SPDX-License-Identifier: GPL-3.0

import "./Ownable.sol";
import "./SafeMath.sol";

contract Election is Ownable {

using SafeMath for uint256;

    // Model a Candidate
    struct Candidate {
        uint256 id;
        string name;
        uint voteCount;
    }

    // Store accounts that have voted
    mapping(address => bool) public voters;
    // Store Candidates
    // Fetch Candidate
```

```
0   listen on all transactions   Search with transaction hash or address

[block:28434469 txIndex:2] from: 0xB1E...29F05 to: Election.(constructor) value:
data: 0x608...80029 logs: 0 hash: 0x93e...2a1b3
transact to Election.addCandidate pending ...

[block:28434657 txIndex:9] from: 0xB1E...29F05
to: Election.addCandidate(string) 0xF56...4Dde4 value: 0 wei data: 0x462...00000 l
hash: 0x27c...b56c1
call to Election.candidates errored: Error encoding arguments: Error: invalid BigNumber string (a

call to Election.candidatesCount

CALL [call] from: 0xB1E9Fda5D104e522667c1b33b101ec565F029F05 to: Election.candidatesCo
data: 0x2d3...5a8a2
transact to Election.addCandidate pending ...

[block:28434892 txIndex:2] from: 0xB1E...29F05
to: Election.addCandidate(string) 0xF56...4Dde4 value: 0 wei data: 0x462...00000 l
hash: 0xfe3...000f5
call to Election.candidatesCount

call to Election.candidatesCount

CALL [call] from: 0xB1E9Fda5D104e522667c1b33b101ec565F029F05 to: Election.candidatesCo
data: 0x2d3...5a8a2

CALL [call] from: 0xB1E9Fda5D104e522667c1b33b101ec565F029F05 to: Election.candidatesCo
data: 0x2d3...5a8a2
```

Candidate ID = 2 car il y a 2 candidates

s.



Balance: 0 ETH

addCandidate: Dallemagne

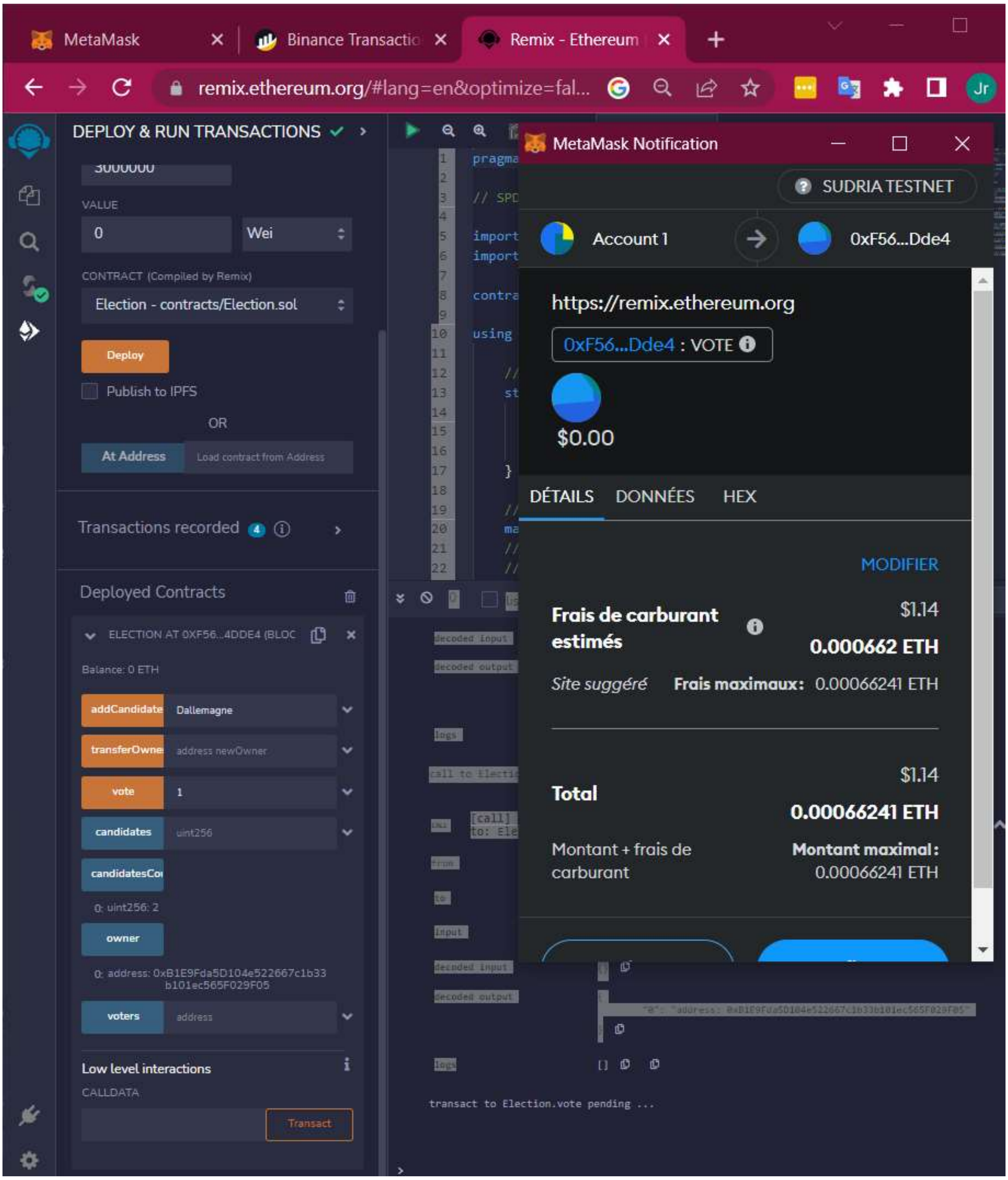
candidatesCo

0: uint256: 2

owner

0: address: 0xB1E9Fda5D104e522667c1b33b101ec565F029F05

t.



MetaMask
Binance Transactio
Remix - Ethereum
remix.ethereum.org/#lang=en&optimize=fal...
DEPLOY & RUN TRANSACTIONS

3000000

VALUE: 0 Wei

CONTRACT (Compiled by Remix): Election - contracts/Election.sol

ELECTION AT 0XF56...4DDE4 (BLOC

Balance: 0 ETH

addCandidate: Dallemagne

transferOwne: address newOwner

vote: 1

candidates: uint256

candidatesCo

0: uint256: 2

owner

0: address: 0xB1E9Fda5D104e522667c1b33b101ec565F029F05

voters: address

Low level interactions

CALLDATA

```
pragma
// SPD
import
import
contra
using
transact to Election.vote pending ...
```

MetaMask Notification

SUDRIA TESTNET

Account 1 → 0xF56...Dde4

https://remix.ethereum.org

0xF56...Dde4 : VOTE

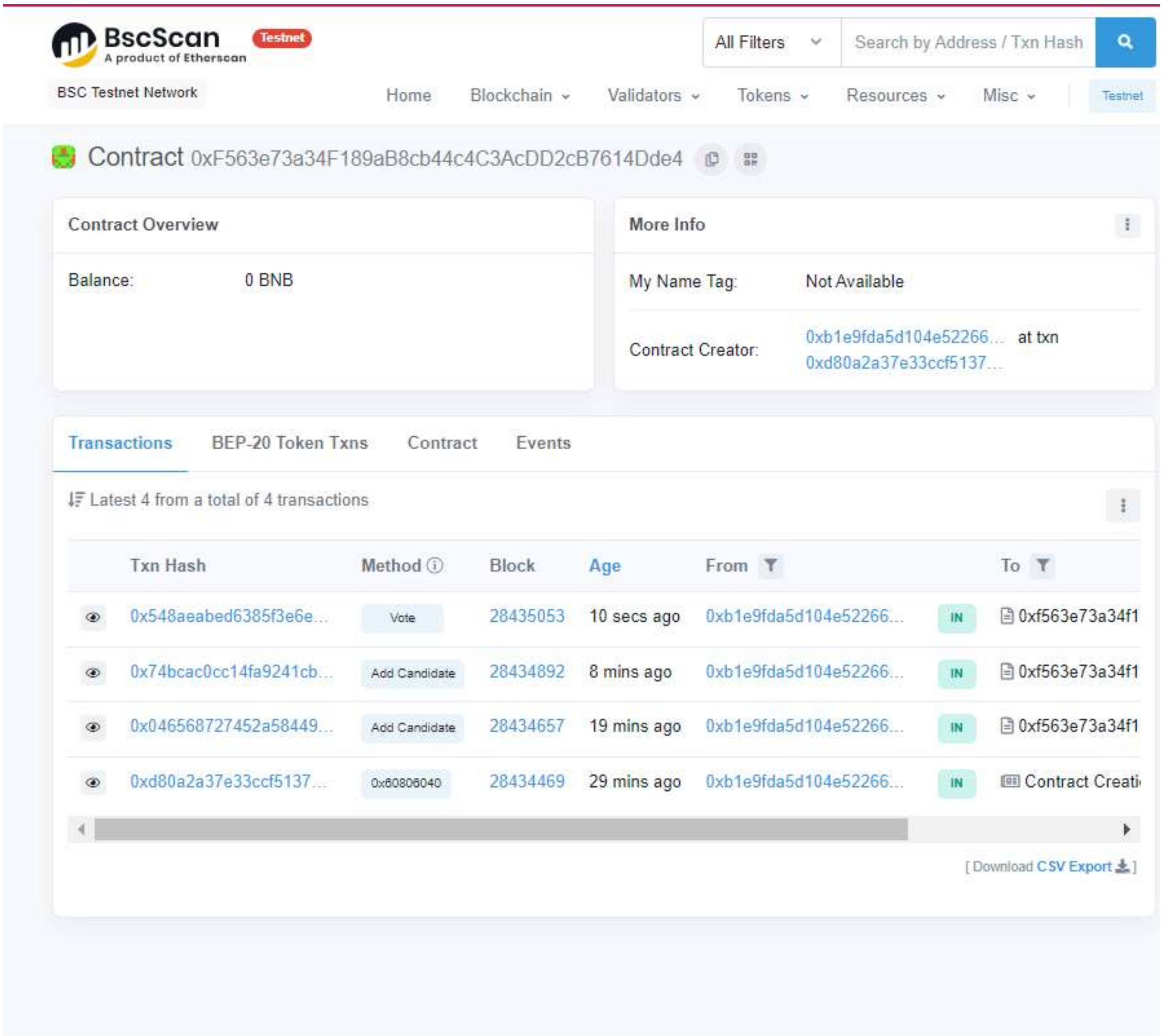
$0.00

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



Contract 0xF563e73a34F189aB8cb44c4C3AcDD2cB7614Dde4

Contract Overview

Balance: 0 BNB

More Info

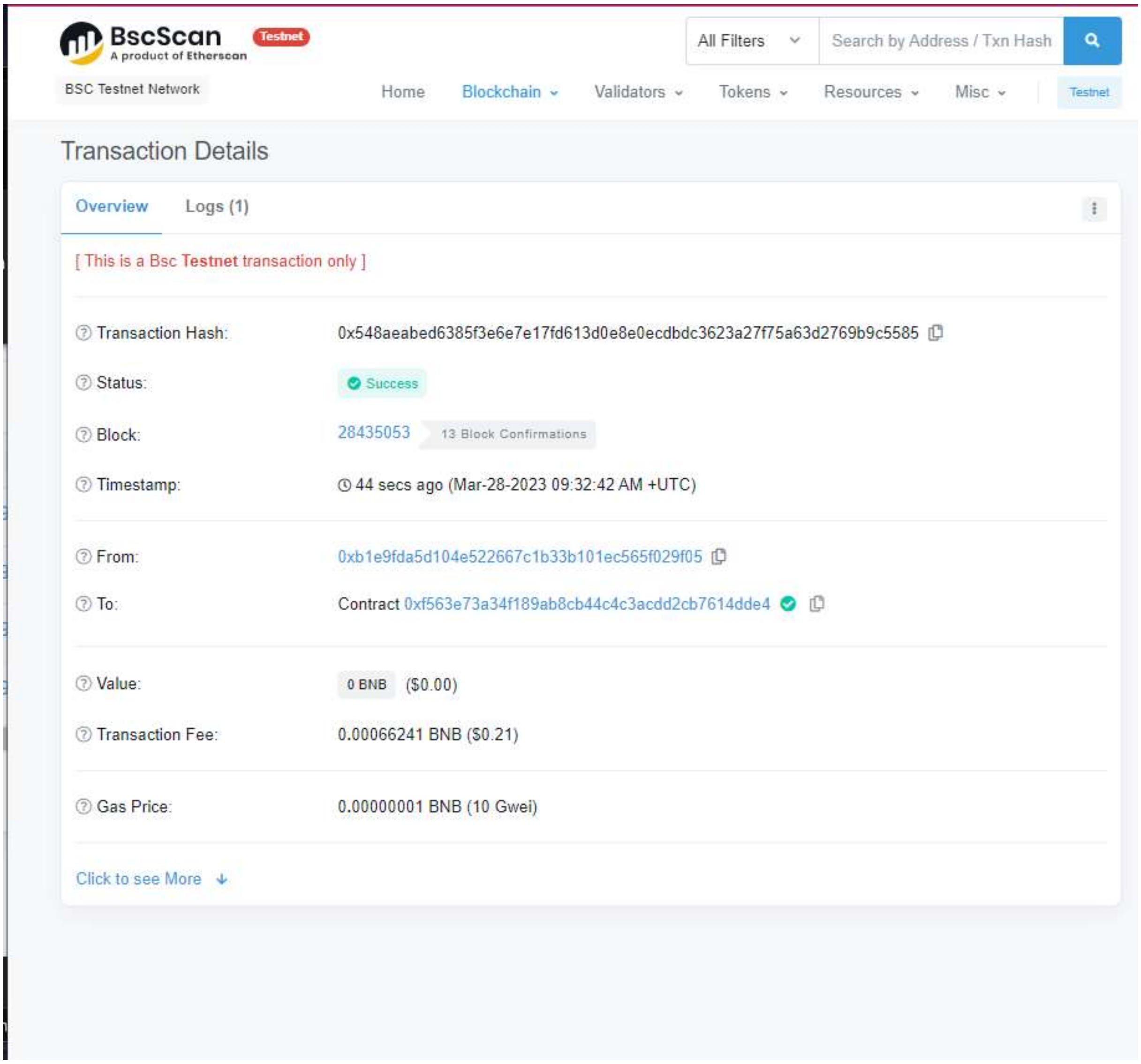
My Name Tag: Not Available

Contract Creator: 0xb1e9fda5d104e52266... at txn 0xd80a2a37e33ccf5137...

Latest 4 from a total of 4 transactions

	Txn Hash	Method	Block	Age	From		To
👁	0x548aeabed6385f3e6e...	Vote	28435053	10 secs ago	0xb1e9fda5d104e52266...	IN	0xf563e73a34f1
👁	0x74bcac0cc14fa9241cb...	Add Candidate	28434892	8 mins ago	0xb1e9fda5d104e52266...	IN	0xf563e73a34f1
👁	0x046568727452a58449...	Add Candidate	28434657	19 mins ago	0xb1e9fda5d104e52266...	IN	0xf563e73a34f1
👁	0xd80a2a37e33ccf5137...	0x60806040	28434469	29 mins ago	0xb1e9fda5d104e52266...	IN	Contract Creati

[Download CSV Export]

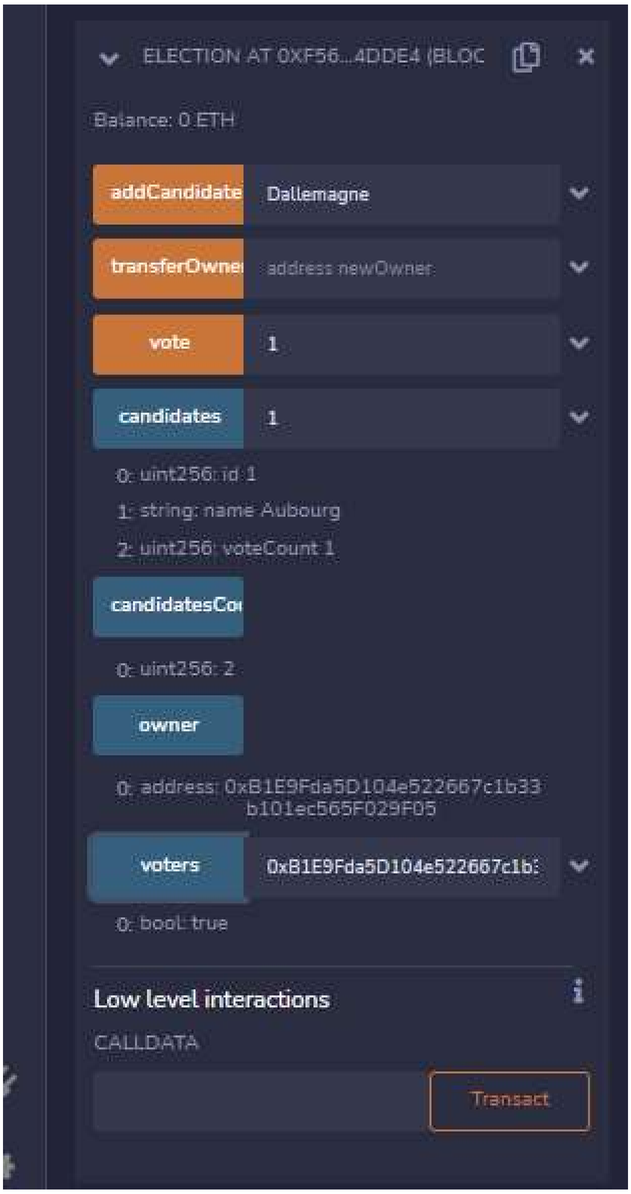


Transaction Details

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

Transaction Hash:	0x548aeabed6385f3e6e7e17fd613d0e8e0ecdbdc3623a27f75a63d2769b9c5585
Status:	Success
Block:	28435053 13 Block Confirmations
Timestamp:	44 secs ago (Mar-28-2023 09:32:42 AM +UTC)
From:	0xb1e9fda5d104e522667c1b33b101ec565f029f05
To:	Contract 0xf563e73a34f189ab8cb44c4c3acdd2cb7614dde4
Value:	0 BNB ($0.00)
Transaction Fee:	0.00066241 BNB ($0.21)
Gas Price:	0.00000001 BNB (10 Gwei)

u.



ELECTION AT 0XF56...4DDE4 (BLOC

Balance: 0 ETH

addCandidate: Dallemagne

transferOwner: address newOwner

vote: 1

candidates: 1

```
0: uint256: id 1
1: string: name Aubourg
2: uint256: voteCount 1
```

candidatesCo

```
0: uint256: 2
```

owner

```
0: address: 0xB1E9Fda5D104e522667c1b33
            b101ec565F029F05
```

voters: 0xB1E9Fda5D104e522667c1b:

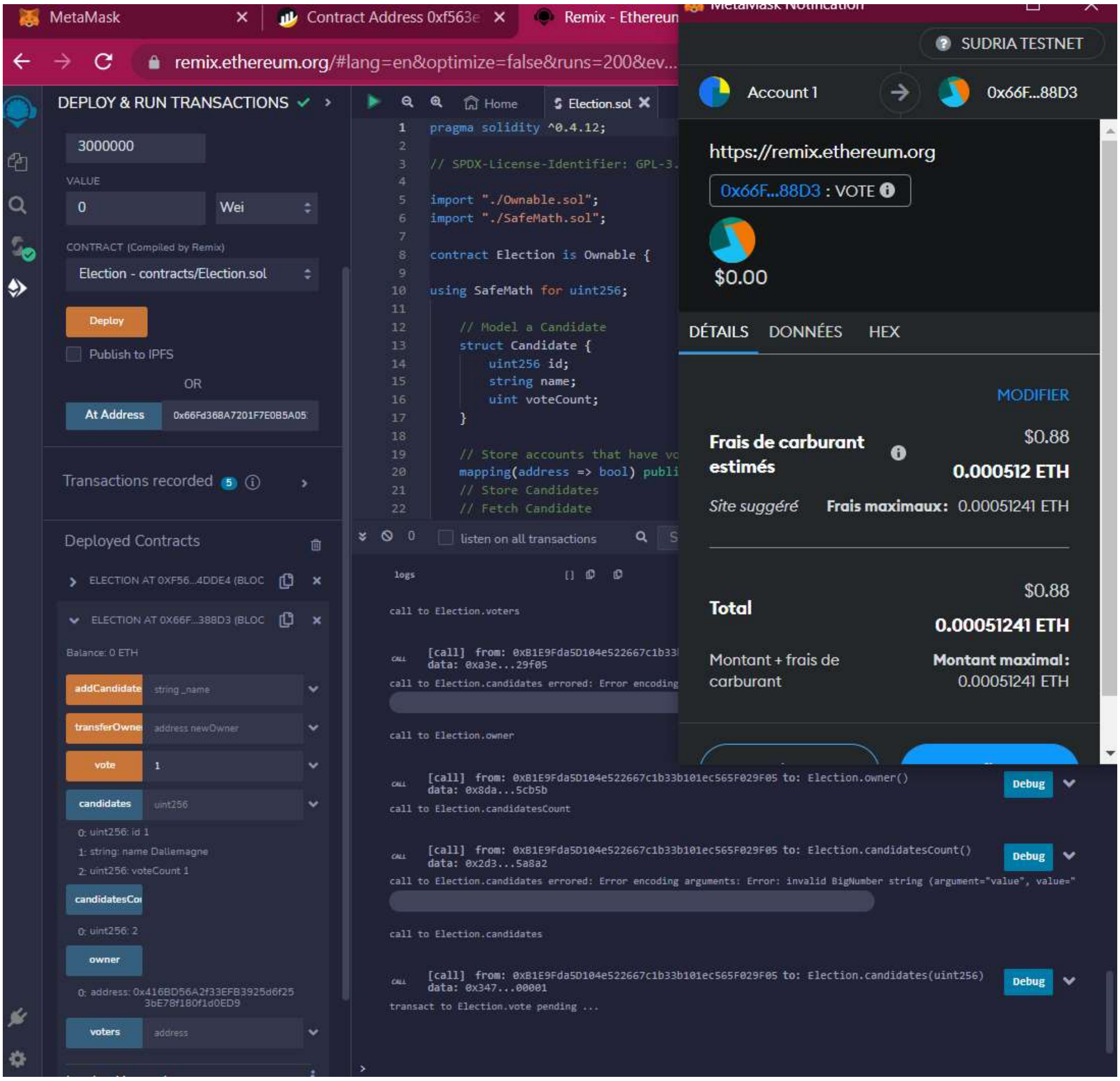
```
0: bool: true
```

Low level interactions

CALLDATA

On voit que voteCount = 1

v. Adresse contrat Cassandra Dallemagne : 0x66Fd368A7201F7E0B5A052Ebcf255314D6D388D3



3000000

VALUE: 0 Wei

CONTRACT (Compiled by Remix): Election - contracts/Election.sol

Deploy

□ Publish to IPFS

OR

At Address 0x66Fd368A7201F7E0B5A05

Transactions recorded 5

Deployed Contracts

ELECTION AT 0XF56...4DDE4 (BLOC

ELECTION AT 0X66F...388D3 (BLOC

Balance: 0 ETH

addCandidate: string _name

transferOwne: address newOwner

vote: 1

candidates: uint256

0: uint256: id 1

1: string: name Dallemagne

2: uint256: voteCount 1

candidatesCo

0: uint256: 2

owner

0: address: 0x416BD56A2f33EFB3925d6f25 3bE78f180f1d0ED9

voters: address

```
pragma solidity ^0.4.12;

// SPDX-License-Identifier: GPL-3.

import "./Ownable.sol";
import "./SafeMath.sol";

contract Election is Ownable {

using SafeMath for uint256;

    // Model a Candidate
    struct Candidate {
        uint256 id;
        string name;
        uint voteCount;
    }

    // Store accounts that have vo
    mapping(address => bool) publi
    // Store Candidates
    // Fetch Candidate
```

0 □ listen on all transactions

```
logs

call to Election.voters

CALL  [call] from: 0xB1E9Fda5D104e522667c1b33
      data: 0xa3e...29f05
call to Election.candidates errored: Error encoding

call to Election.owner

CALL  [call] from: 0xB1E9Fda5D104e522667c1b33b101ec565F029F05 to: Election.owner()          Debug
      data: 0x8da...5cb5b
call to Election.candidatesCount

CALL  [call] from: 0xB1E9Fda5D104e522667c1b33b101ec565F029F05 to: Election.candidatesCount()  Debug
      data: 0x2d3...5a8a2
call to Election.candidates errored: Error encoding arguments: Error: invalid BigNumber string (argument="value", value="

call to Election.candidates

CALL  [call] from: 0xB1E9Fda5D104e522667c1b33b101ec565F029F05 to: Election.candidates(uint256)  Debug
      data: 0x347...00001
transact to Election.vote pending ...
```

https://remix.ethereum.org

0x66F...88D3 : VOTE

$0.00

DÉTAILS DONNÉES HEX

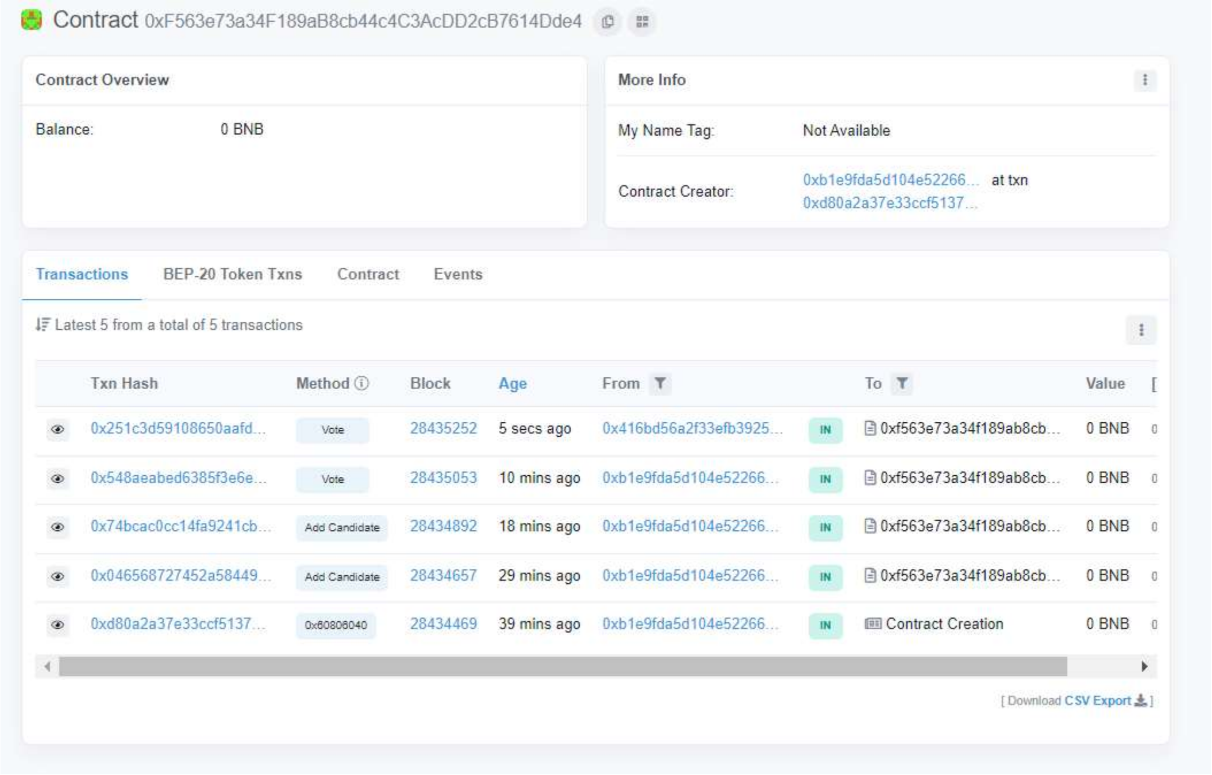
MODIFIER

Frais de carburant estimés $0.88 **0.000512 ETH**

Site suggéré **Frais maximaux:** 0.00051241 ETH

Total $0.88 **0.00051241 ETH**

Montant + frais de carburant **Montant maximal:** 0.00051241 ETH



Contract 0xF563e73a34F189aB8cb44c4C3AcDD2cB7614Dde4

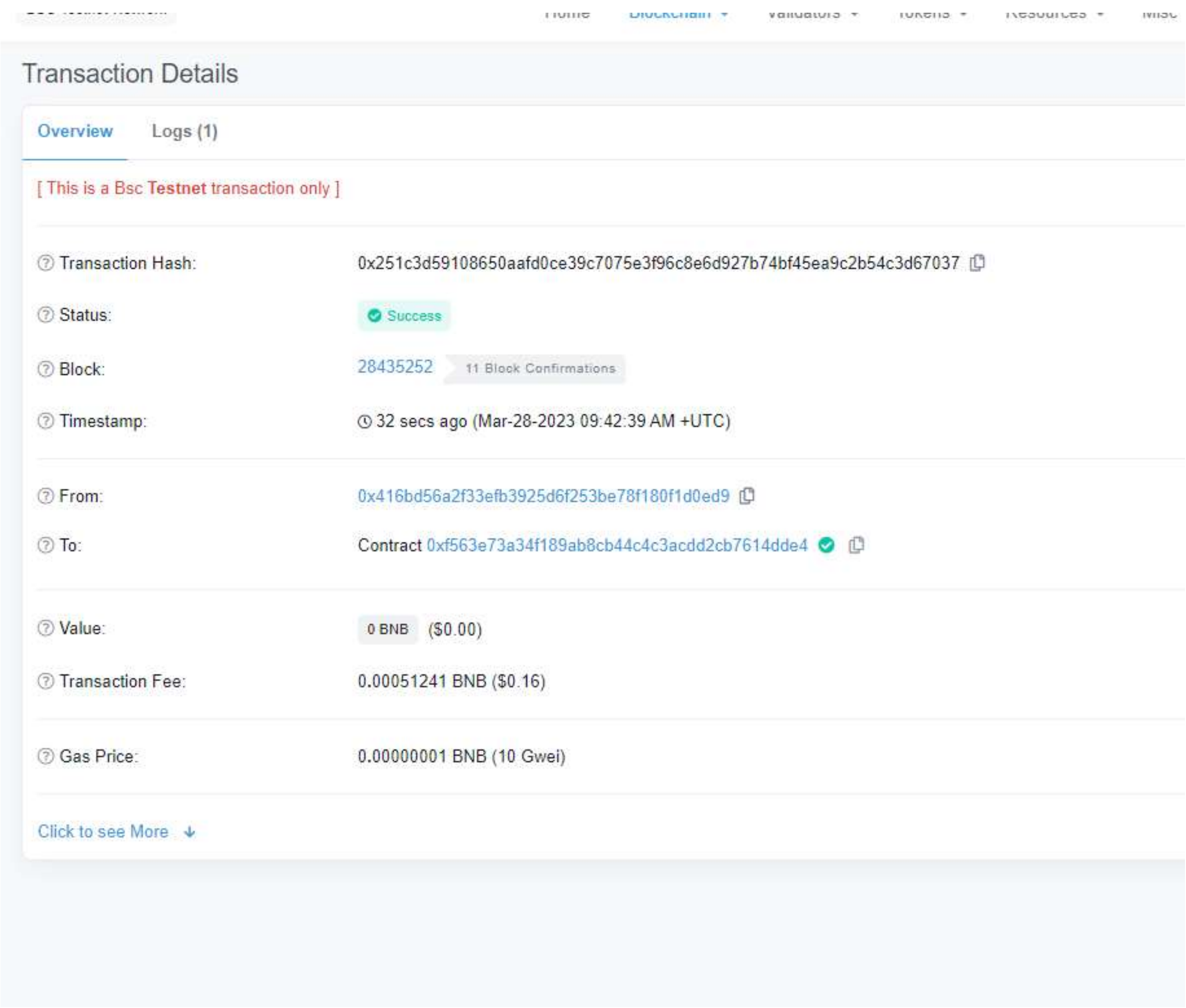
Contract Overview	
Balance:	0 BNB

More Info	
My Name Tag:	Not Available
Contract Creator:	0xb1e9fda5d104e52266... at txn 0xd80a2a37e33ccf5137...

Latest 5 from a total of 5 transactions

Txn Hash	Method	Block	Age	From		To	Value	[
0x251c3d59108650aafd...	Vote	28435252	5 secs ago	0x416bd56a2f33efb3925...	IN	0xf563e73a34f189ab8cb...	0 BNB	0
0x548aeabed6385f3e6e...	Vote	28435053	10 mins ago	0xb1e9fda5d104e52266...	IN	0xf563e73a34f189ab8cb...	0 BNB	0
0x74bcac0cc14fa9241cb...	Add Candidate	28434892	18 mins ago	0xb1e9fda5d104e52266...	IN	0xf563e73a34f189ab8cb...	0 BNB	0
0x046568727452a58449...	Add Candidate	28434657	29 mins ago	0xb1e9fda5d104e52266...	IN	0xf563e73a34f189ab8cb...	0 BNB	0
0xd80a2a37e33ccf5137...	0x60806040	28434469	39 mins ago	0xb1e9fda5d104e52266...	IN	Contract Creation	0 BNB	0

[Download CSV Export]



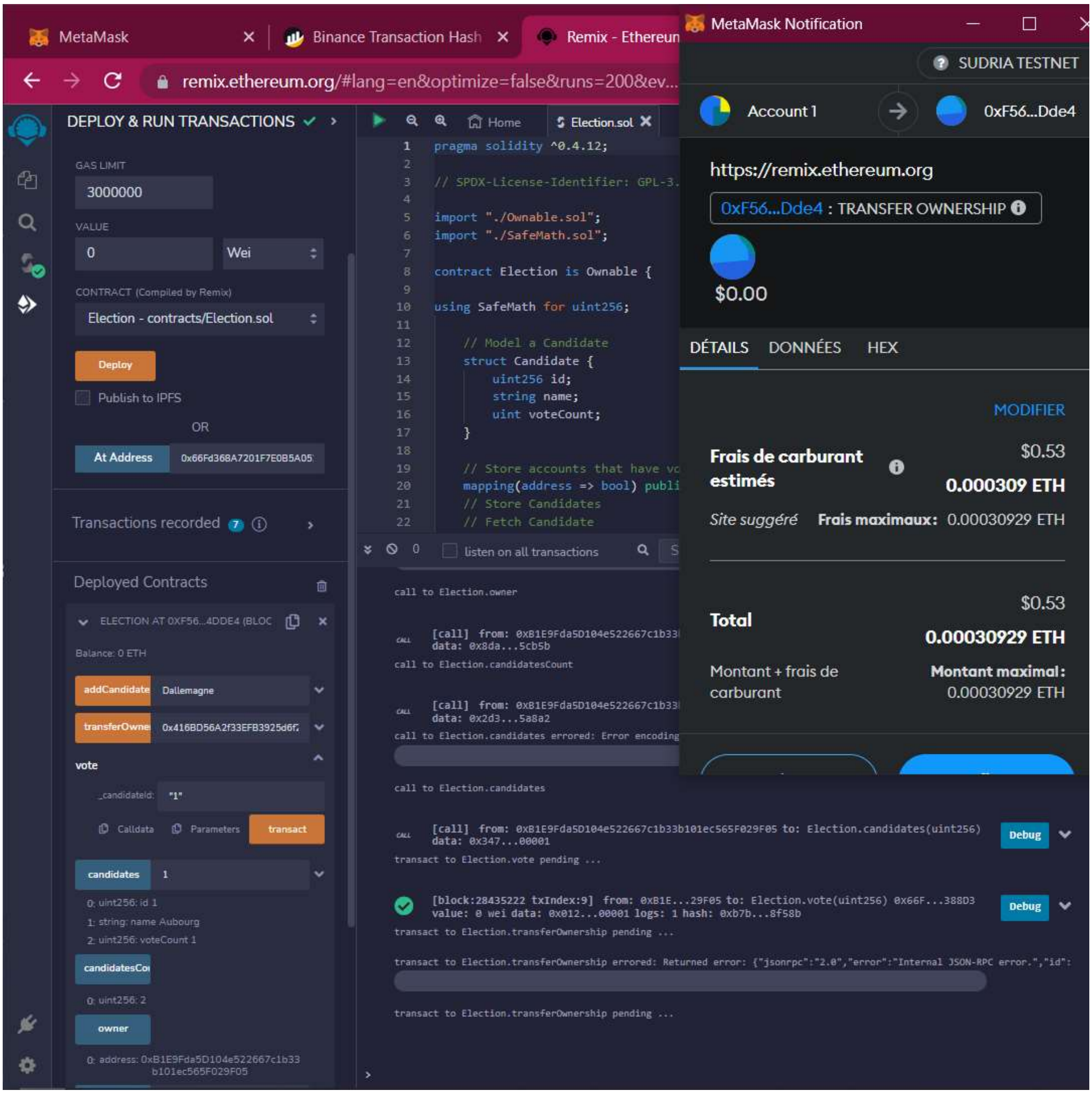
Transaction Details

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

Transaction Hash:	0x251c3d59108650aafd0ce39c7075e3f96c8e6d927b74bf45ea9c2b54c3d67037
Status:	Success
Block:	28435252 11 Block Confirmations
Timestamp:	32 secs ago (Mar-28-2023 09:42:39 AM +UTC)
From:	0x416bd56a2f33efb3925d6f253be78f180f1d0ed9
To:	Contract 0xf563e73a34f189ab8cb44c4c3acdd2cb7614dde4
Value:	0 BNB ($0.00)
Transaction Fee:	0.00051241 BNB ($0.16)
Gas Price:	0.00000001 BNB (10 Gwei)

Click to see More

w. adresse portefeuille Cassandra Dallemagne : 0x416BD56A2f33EFB3925d6f253bE78f180f1d0ED9



MetaMask
Binance Transaction Hash
Remix - Ethereum
remix.ethereum.org/#lang=en&optimize=false&runs=200&ev...
DEPLOY & RUN TRANSACTIONS
Home
Election.sol

GAS LIMIT 3000000

VALUE 0 Wei

CONTRACT (Compiled by Remix) Election - contracts/Election.sol

0x66Fd368A7201F7E0B5A05

Transactions recorded 7

Deployed Contracts

ELECTION AT 0XF56...4DDE4 (BLOC

Balance: 0 ETH

addCandidate Dallemagne

transferOwne 0x416BD56A2f33EFB3925d6f2

vote

_candidateId: "1"

candidates 1

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

candidatesCo

0: uint256: 2

owner

0: address: 0xB1E9Fda5D104e522667c1b33b101ec565F029F05

```
pragma solidity ^0.4.12;

// SPDX-License-Identifier: GPL-3.

import "./Ownable.sol";
import "./SafeMath.sol";

contract Election is Ownable {

using SafeMath for uint256;

    // Model a Candidate
    struct Candidate {
        uint256 id;
        string name;
        uint voteCount;
    }

    // Store accounts that have vo
    mapping(address => bool) publi
    // Store Candidates
    // Fetch Candidate
```

```
call to Election.owner

[call] from: 0xB1E9Fda5D104e522667c1b33
data: 0x8da...5cb5b
call to Election.candidatesCount

[call] from: 0xB1E9Fda5D104e522667c1b33
data: 0x2d3...5a8a2
call to Election.candidates errored: Error encoding

call to Election.candidates

[call] from: 0xB1E9Fda5D104e522667c1b33b101ec565F029F05 to: Election.candidates(uint256)    Debug
data: 0x347...00001
transact to Election.vote pending ...

[block:28435222 txIndex:9] from: 0xB1E...29F05 to: Election.vote(uint256) 0x66F...388D3    Debug
value: 0 wei data: 0x012...00001 logs: 1 hash: 0xb7b...8f58b
transact to Election.transferOwnership pending ...

transact to Election.transferOwnership errored: Returned error: {"jsonrpc":"2.0","error":"Internal JSON-RPC error.","id":

transact to Election.transferOwnership pending ...
```

MetaMask Notification

SUDRIA TESTNET

Account 1 → 0xF56...Dde4

https://remix.ethereum.org

0xF56...Dde4 : TRANSFER OWNERSHIP

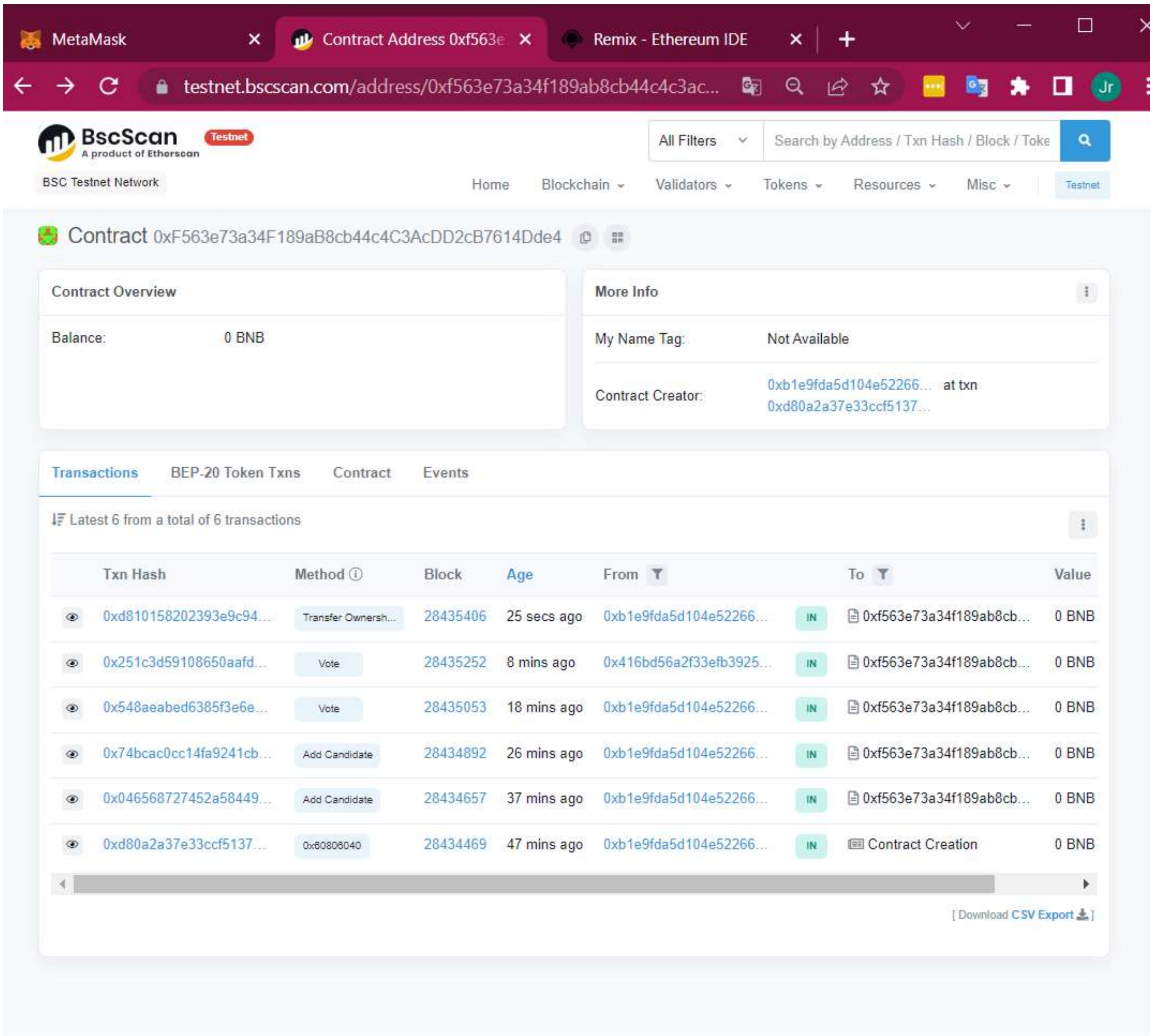
$0.00

Frais de carburant estimés $0.53 **0.000309 ETH**

Site suggéré **Frais maximaux:** 0.00030929 ETH

Total $0.53 **0.00030929 ETH**

Montant + frais de carburant **Montant maximal:** 0.00030929 ETH



Contract 0xF563e73a34F189aB8cb44c4C3AcDD2cB7614Dde4

Contract Overview

Balance: 0 BNB

More Info

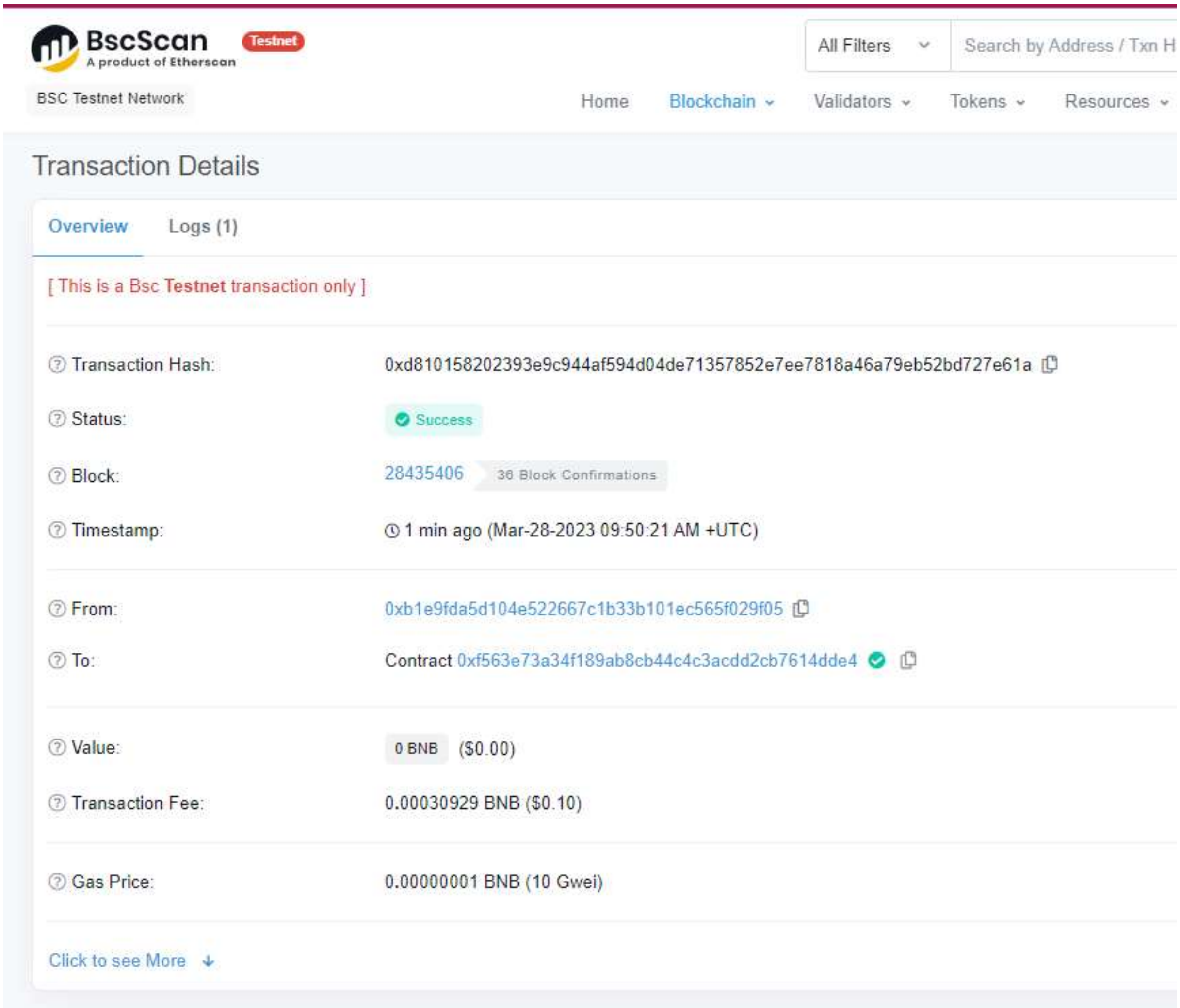
My Name Tag: Not Available

Contract Creator: 0xb1e9fda5d104e52266... at txn 0xd80a2a37e33ccf5137...

Latest 6 from a total of 6 transactions

Txn Hash	Method	Block	Age	From		To	Value
0xd810158202393e9c94...	Transfer Ownersh...	28435406	25 secs ago	0xb1e9fda5d104e52266...	IN	0xf563e73a34f189ab8cb...	0 BNB
0x251c3d59108650aafd...	Vote	28435252	8 mins ago	0x416bd56a2f33efb3925...	IN	0xf563e73a34f189ab8cb...	0 BNB
0x548aeabed6385f3e6e...	Vote	28435053	18 mins ago	0xb1e9fda5d104e52266...	IN	0xf563e73a34f189ab8cb...	0 BNB
0x74bcac0cc14fa9241cb...	Add Candidate	28434892	26 mins ago	0xb1e9fda5d104e52266...	IN	0xf563e73a34f189ab8cb...	0 BNB
0x046568727452a58449...	Add Candidate	28434657	37 mins ago	0xb1e9fda5d104e52266...	IN	0xf563e73a34f189ab8cb...	0 BNB
0xd80a2a37e33ccf5137...	0x60806040	28434469	47 mins ago	0xb1e9fda5d104e52266...	IN	Contract Creation	0 BNB

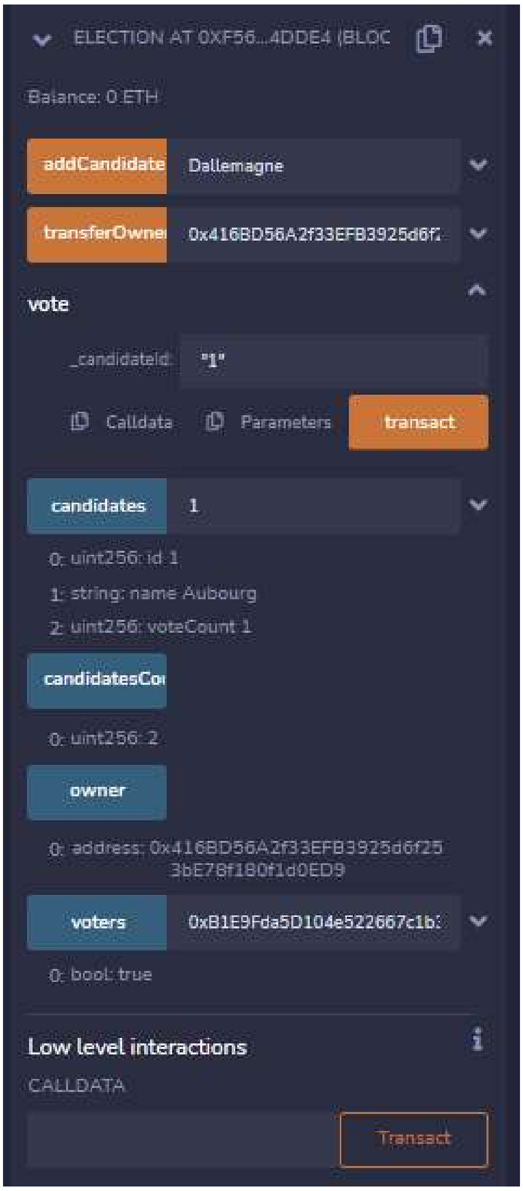
[Download CSV Export]



Transaction Details

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

Transaction Hash:	0xd810158202393e9c944af594d04de71357852e7ee7818a46a79eb52bd727e61a
Status:	Success
Block:	28435406 36 Block Confirmations
Timestamp:	1 min ago (Mar-28-2023 09:50:21 AM +UTC)
From:	0xb1e9fda5d104e522667c1b33b101ec565f029f05
To:	Contract 0xf563e73a34f189ab8cb44c4c3acdd2cb7614dde4 ✓
Value:	0 BNB ($0.00)
Transaction Fee:	0.00030929 BNB ($0.10)
Gas Price:	0.00000001 BNB (10 Gwei)

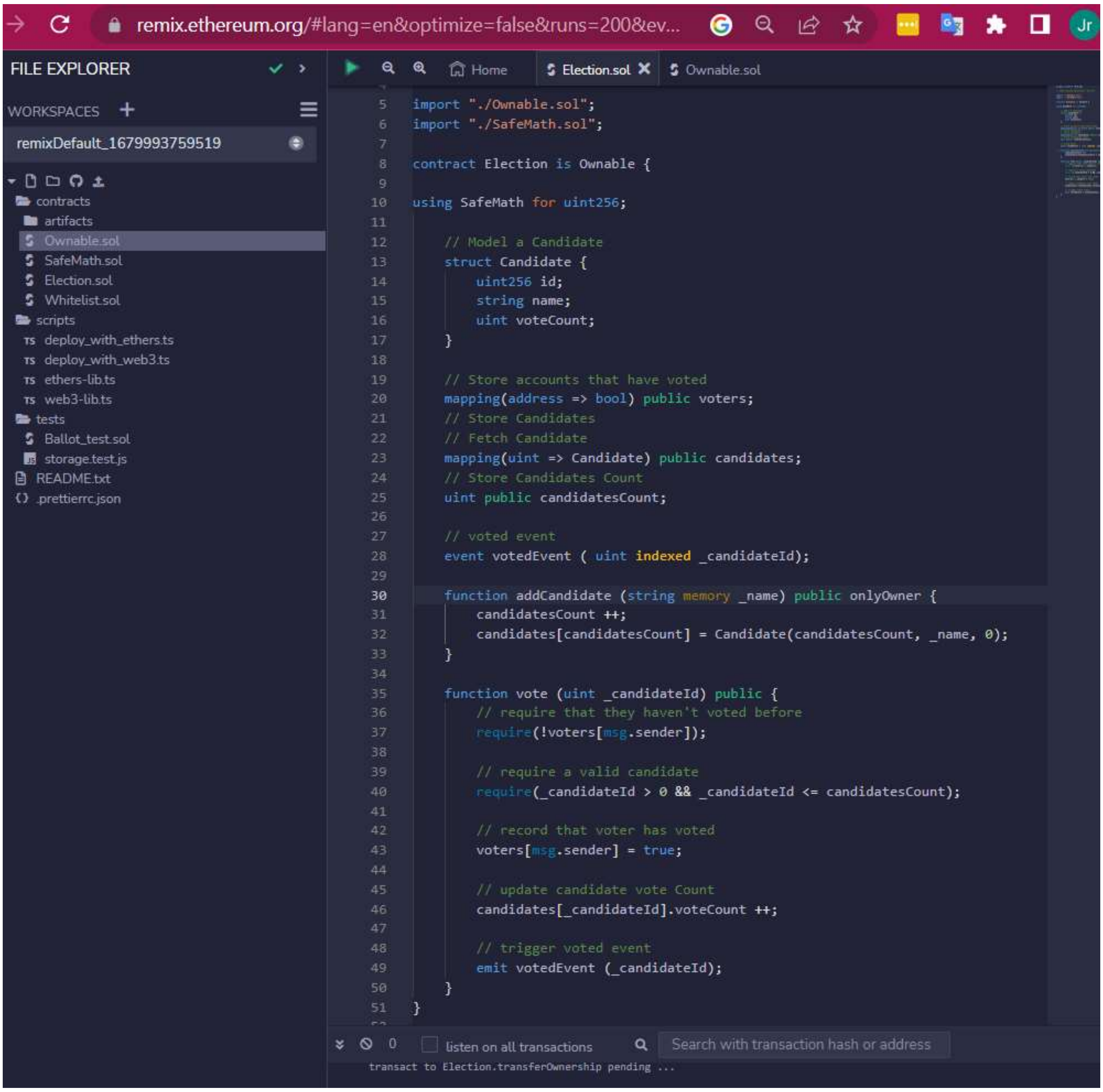


```
Balance: 0 ETH
addCandidate  Dallemagne
transferOwne  0x416BD56A2f33EFB3925d6f2
vote
  _candidateId: "1"
candidates  1
  0: uint256: id 1
  1: string: name Aubourg
  2: uint256: voteCount 1
candidatesCo
  0: uint256: 2
owner
  0: address: 0x416BD56A2f33EFB3925d6f25
              3bE78f180f1d0ED9
voters  0xB1E9Fda5D104e522667c1b
  0: bool: true
```

L’adresse de l’owner est bien celle de Cassandra Dallemagne.

x. La fonction addCandidate est une fonction publique donc toute personne peut ajouter un candidat. Après recherche sur internet, il existe un module « onlyOwner » qui me permet d’être la seule personne capable d'ajouter un nouveau candidat.

y.



```
import "./Ownable.sol";
import "./SafeMath.sol";

contract Election is Ownable {

using SafeMath for uint256;

    // Model a Candidate
    struct Candidate {
        uint256 id;
        string name;
        uint voteCount;
    }

    // Store accounts that have voted
    mapping(address => bool) public voters;
    // Store Candidates
    // Fetch Candidate
    mapping(uint => Candidate) public candidates;
    // Store Candidates Count
    uint public candidatesCount;

    // voted event
    event votedEvent ( uint indexed _candidateId);

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

    function vote (uint _candidateId) public {
        // require that they haven't voted before
        require(!voters[msg.sender]);

        // require a valid candidate
        require(_candidateId > 0 && _candidateId <= candidatesCount);

        // record that voter has voted
        voters[msg.sender] = true;

        // update candidate vote Count
        candidates[_candidateId].voteCount ++;

        // trigger voted event
        emit votedEvent (_candidateId);
    }
}
```

```
transact to Election.transferOwnership pending ...
```