

TP

Développer, Deloyer et Interagir avec un contrat intelligent sur Ethereum

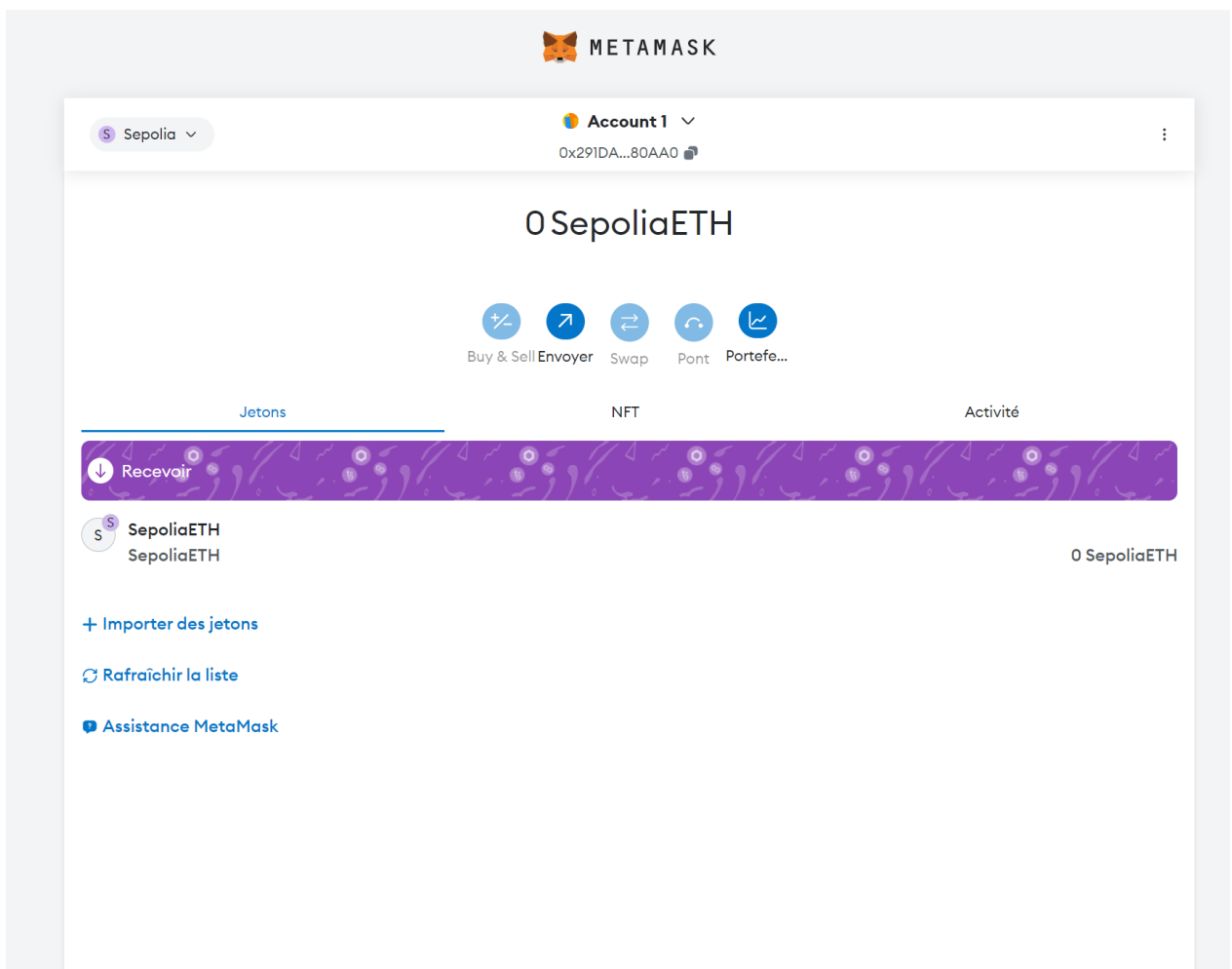
Michel PENG
A2MSI

15/04/2024

Clef publique : 0x291DA01dF2137a3B616239E5E29fbaF7Fbf80AA0

1. Prise en main des outils Remix et Metamask

- a. Naviguer sur le site et télécharger Metamask
- b. Suivez les étapes de génération du portefeuille en sauvegardant bien votre seed phrase
- c. Vous devrez ensuite avoir accès à votre premier compte « wallet » dont la clé publique commence par « 0x... » (voir illustration ci-dessous).
- d. Afficher/masquer les réseaux de tests et cliquez sur « Select Network »



g.

Transaction Details

Overview

State

[This is a Sepolia Testnet transaction only]

Transaction Hash:

0x8b48fc28c00ed84578cb00a3e44f0091bc96601fa1780c75e2890bbe4a3bab6c

Status:

Success

Block:

57020699 Block Confirmations

Timestamp:

1 min ago (Apr-15-2024 07:46:12 AM +UTC)

From:

0x2a88690AaBB7fC771970A27Cf0784f500cF3aEa5

To:

0x291DA01dF2137a3B616239E5E29fbaF7Fbf80AA0

Value:

0.01 ETH (\$0.00)

Transaction Fee:

0.000031972331055 ETH (\$0.00)

Gas Price:

1.522491955 Gwei (0.000000001522491955 ETH)

More Details:

+ Click to show more

A transaction is a cryptographically signed instruction that changes the blockchain state. Block explorers track the details of all transactions in the network. Learn more about transactions in our Knowledge Base.

h.

Overview

Consensus Info

Blob Info

[This is a Sepolia Testnet block only]

Block Height:

5702069

Status:

Unfinalized

Timestamp:

2 mins ago (Apr-15-2024 07:46:12 AM +UTC)

Proposed On:

Block proposed on slot 4786131, epoch 149566

Transactions:

68 transactions and 10 contract internal transactions in this block

Withdrawals:

16 withdrawals in this block

Fee Recipient:

0x9B984D5a03980D8dc0a24506c968465424c81DbE in 12 secs

Block Reward:

0.036599003805825361 ETH (0 + 0.037157533681434056 - 0.000558529875608695)

Total Difficulty:

17,000,018,015,853,232

Size:

99,402 bytes

Gas Used:

24,832,429 (82.77%) +66% Gas Target

Gas Limit:

30,000,000

Base Fee Per Gas:

0.00000000022491955 ETH (0.022491955 Gwei)

Burnt Fees:

0.000558529875608695 ETH

Extra Data:

gethgo1.21.7linux (Hex:0xd883010d0e846765746888676f312e32312e37856c696e7578)

More Details:







+ Click to show more

j.

The image shows the Remix IDE interface, a web-based development environment for Ethereum. The interface is divided into several sections:

- Left Panel (Gestionnaire de fichiers):** Displays the file system structure, including folders like `.deps`, `contracts`, `scripts`, `tests`, and files like `.prettierrc.json` and `README.txt`.
- Top Bar:** Contains the Remix logo and navigation links for Website, Documentation, Remix Plugin, and Remix Desktop.
- Main Panel:**
 - Files:** Includes buttons for `Start Coding`, `Open File`, and `Access File System`.
 - Recent workspaces:** Shows the current workspace as `default_workspace`.
 - Load from:** Provides options to load code from `GitHub`, `Gist`, `IPFS`, or `HTTPS`.
 - Learn:** Offers resources for learning, including `Remix Basics` (with a `Get Started` button), `Intro to Solidity`, and `Deploying with Libraries`.
- Right Panel:**
 - Featured:** Promotes `WATCH TO LEARN` with a video tip from the Remix Team.
 - Project Templates:** Lists various templates such as `MULTISIG` (Gnosis Safe), `ERC20` (0xProject), `ERC20` (OpenZeppelin), and `ERC721` (OpenZeppelin).
 - Featured Plugins:** Highlights plugins like `SOLIDITY ANALYZERS`, `COOKBOOK`, `SOLIDITY`, and `SOURCIFY`.
 - Scam Alert:** A warning box stating that the only URL for Remix is `remix.ethereum.org` and advising users to be wary of online videos promoting "liquidity front runner bots".
- Bottom Panel:** A command line area for running Solidity commands, currently showing `solidity copilot not activated!`.

l.







GESTIONNAIRE DE FICHIERS

✓ >

ESPACE DE TRAVAIL

default_workspace



.deps

contracts

artifacts

TP_Election-master

TP_Election-master

build

contracts

contracts

migrations

node_modules

.bin

accepts

after

test

.npmignore

.travis.yml

index.js

LICENCE

package.json

README.md

ajv

dist

lib

compile

dot

v5

_limit.jst

_limitItems.jst

_limitLength.jst

_limitProperties.jst

allof.jst

anyOf.jst

coerce.def

custom.jst

defaults.def




definitions.def

dependencies.jst

enum.jst

errors.def

format.jst



REM

The Native

Website Doc

Search Do

Files

Start Cod

Recent works

default_wor

Load from

GitHub

Learn


Remix Ba

An introdu

Get Start

Intro to S

Deployin

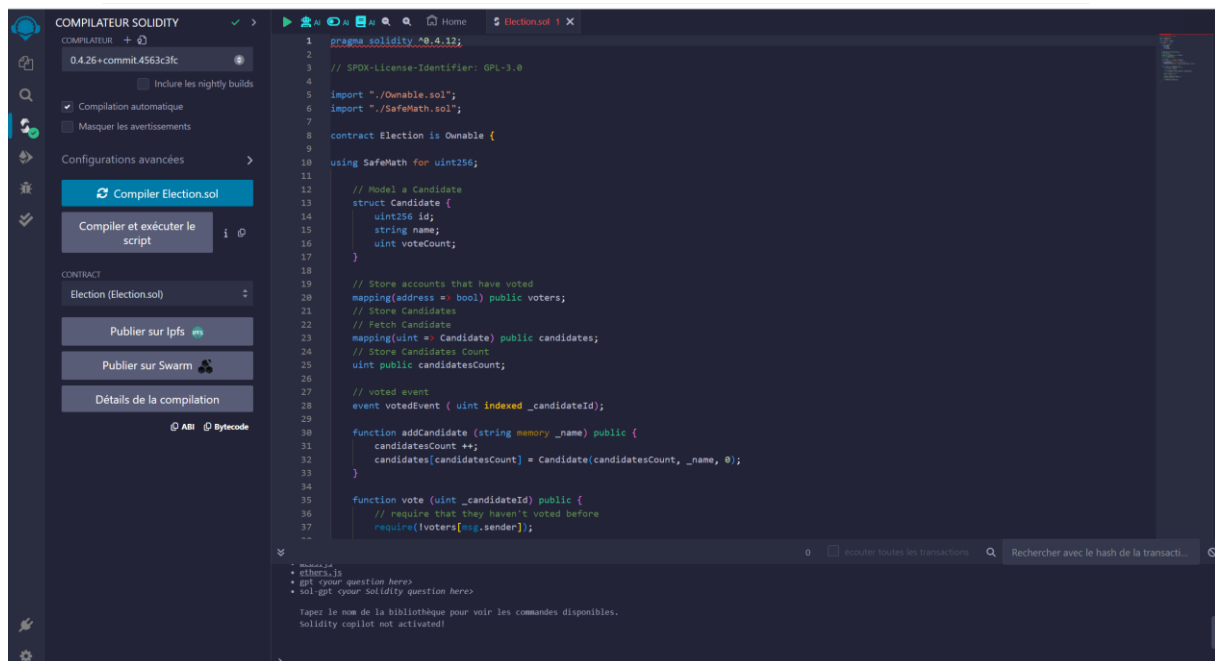


- ethers.js
- gpt <your
- sol-gpt <

Tapez le

Solidity

M.



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"
    }
  ]
}

```

```
6080604052336000806101000a81548173fffffffffffffffffffffffffffff021916908373fffffffffffffffffffff  

ffffffffffffff160217905550610897806100536000396000f3006080604052600436106100835760003  

57c010000000000000000000000000000000000000000000000000000000000000000000000000000000000900463ffffff16806301  

21b93f146100885780632d35a8a2146100b55780633477ee2e146100e0578063462e91ec146101945  

780638da5cb5b146101fd578063a3ec138d14610254578063f2fde38b146102af575b600080fd5b3480  

1561009457600080fd5b506100b3600480360381019080803590602001909291905050506102f256  

5b005b3480156100c157600080fd5b506100ca610415565b60405180828152602001915050604051  

80910390f35b3480156100ec57600080fd5b5061010b600480360381019080803590602001909291  

9050505061041b565b6040518084815260200180602001838152602001828103825284818151815  

260200191508051906020019080838360005b838110156101575780820151818401526020810190  

5061013c565b50505050905090810190601f1680156101845780820380516001836020036101000a  

031916815260200191505b5094505050505060405180910390f35b3480156101a057600080fd5b50  

6101fb600480360381019080803590602001908201803590602001908080601f0160208091040260  

2001604051908101604052809392919081815260200183838082843782019150505050505091929  

192905050506104dd565b005b34801561020957600080fd5b5061021261055a565b604051808273ff  

ffffffffffffff1673fffffffffffffffffffffffffffff16815260200191505060405180910390f3  

5b34801561026057600080fd5b50610295600480360381019080803573fffffffffffffffffffffffffffff  

16906020019092919050505061057f565b6040518082151515158152602001915050604051809103  

90f35b3480156102bb57600080fd5b506102f0600480360381019080803573fffffffffffffffffffffffffffff  

ffff16906020019092919050505061059f565b005b600160003373fffffffffffffffffffffffffffff1673fffff  

ffffffffffffff16815260200190815260200160002060009054906101000a900460ff161515  

1561034b57600080fd5b60008111801561035d57506003548111155b151561036857600080fd5b60  

018060003373fffffffffffffffffffffffffffff1673fffffffffffffffffffffffffffff168152602001908152602  

00160002060006101000a81548160ff0219169083151502179055506002600082815260200190815  

260200160002060020160008154809291906001019190505550807fff3c900d938d21d0990d786e8  

19f29b8d05c1ef587b462b939609625b684b1660405160405180910390a250565b60035481565b600  

2602052806000526040600020600091509050806000015490806001018054600181600116156101
```

n.



MetaMask

Réseau de test Sepolia

Account 1

Nouveau contrat

https://remix.ethereum.org

DÉPLOIEMENT DE CONTRAT

DÉTAILS

HEX

Estimated fee

0.00086251

0.00086251 SepoliaETH

Marché -30 s **Frais maximaux:** 0.00087276 SepoliaETH

Total

0.00086251

0.00086251 SepoliaETH

Montant + frais de carburant **Montant maximal:** 0.00087276 SepoliaETH

Rejeter

Confirmer

Etherscan

HomeBlockchainTokensNFTsMisc

Transaction Details

Overview

[This is a Sepolia Testnet transaction only]

Transaction Hash:

0x4e259b1c7dd3062f3f2563a0dc6996dfb13870d0d500c040d07af6d1abe375ff

Status:

Indexing

This transaction has been included and will be reflected in a short while.

Block:

5702186

From:

0x291DA01dF2137a3B616239E5E29fbaF7FbF80AA0

To:

[Contract Creation]

Value:

0 ETH (\$0.00)

Gas Price:

1.550470369 Gwei (0.000000001550470369 ETH)

A transaction is a cryptographically signed instruction that changes the blockchain state. Block explorers track the details of all transactions in the network. Learn more about transactions in our Knowledge Base.

OverviewState

[This is a Sepolia Testnet transaction only]

Transaction Hash:

0x4e259b1c7dd3062f3f2563a0dc6996dfb13870d0500c040d07af6d1abe375ff

Status:

Success

Block:

570218615 Block Confirmations

Timestamp:

3 mins ago (Apr-15-2024 08:09:36 AM +UTC)

Transaction Action:

Call 0x60806040 Method by 0x291DA01d...7Fb80AA0

From:

0x291DA01dF2137a38616239E5E29fba77Fb80AA0

To:

[0xd4d8701e037d97daac63a5c760c78d72d2bf5af9 Created]

Value:

0 ETH (\$0.00)

Transaction Fee:

0.000852659472846384 ETH (\$0.00)

Gas Price:

1.550470369 Gwei (0.000000001550470369 ETH)

More Details:

+ Click to show more

A transaction is a cryptographically signed instruction that changes the blockchain state. Block explorers track the details of all transactions in the network. Learn more about transactions in our Knowledge Base.

DÉPLOYER ET EXÉCUTER DES TRANSACTIONS

ENVIRONNEMENT

Injected Provider - MetaMask

Sepolia (11155111) network

COMPTES

0x291...80AA0 (0.00914734052)

GAS LIMIT

3000000

VALEUR

0Wei

CONTRACT

Election - contracts/TP_Election-master2

version de l'exé: byzantium

Déployer

Publier vers IPFS

At Address

Charger le contrat à partir de l'ad.

Transactions enregistrées

Pinned Contracts (chain id: 11155111)

No pinned contracts found for selected workspace & network

Contrats déployés

Actuellement, vous n'avez aucune instance de contrat avec laquelle interagir.

1

pragma solidity ^0.4.12;

2

// SPDX-License-Identifier: GPL-3.0

3

import "../Ownable.sol";

4

import "../SafeMath.sol";

5

contract Election is Ownable {

6

using SafeMath for uint256;

7

10

11

12

// Model a Candidate

13

struct Candidate {

14

uint256 id;

15

string name;

16

uint voteCount;

17

}

18

19

// Store accounts that have voted

20

mapping(address => bool) public voters;

21

// Store Candidates

22

// Fetch Candidate

23

mapping(uint => Candidate) public candidates;

24

// Store Candidates Count

25

uint public candidatesCount;

26

27

// voted event

28

event votedEvent (uint indexed _candidateId);

29

30

function addCandidate (string memory _name) public {

31

candidatesCount ++;

32

candidates[candidatesCount] = Candidate(candidatesCount, _name, 0);

33

}

34

35

function vote (uint _candidateId) public {

36

// require that they haven't voted before

37

require(!voters[msg.sender]);

38

39

40

41

42

43

44

45

46

47

48

49

50

51

52

53

54

55

56

57

58

59

60

61

62

63

64

65

66

67

68

69

70

71

72

73

74

75

76

77

78

79

80

81

82

83

84

85

86

87

88

89

90

91

92

93

94

95

96

97

98

99

100

creation of Election pending...

view on etherscan

[block:578186 txIndex:27] from: 0x291...80aa0 to: Election.(constructor) value: 0 wei data: 0x608...80029 logs: 0 hash: 0x817...2672e

status

0x1 Transaction mine et exécutée avec succès

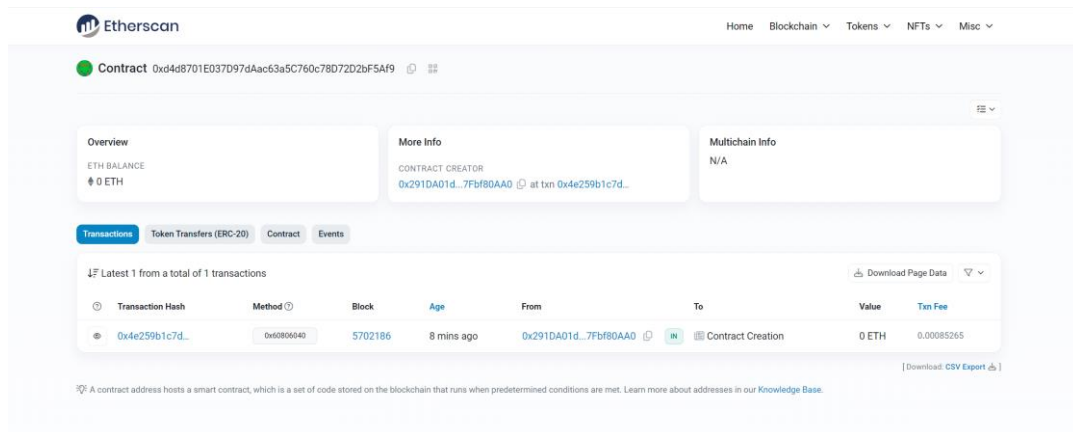
débugage

Justifier les frais de transactions « Transaction fees » que vous avez payés. Sont-elles identiques à celle de la précédente transaction ?

Les frais ne sont pas identiques

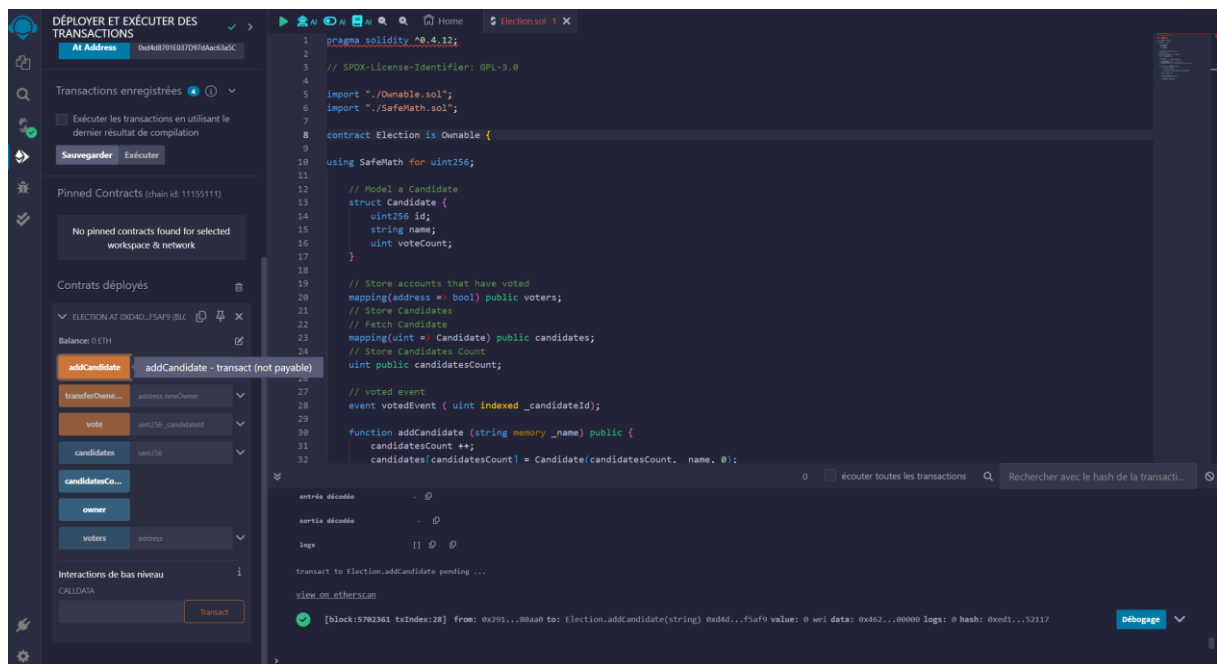
Quelle est l'adresse public de votre smart contract ?

0xd4d8701E037D97dAac63a5C760c78D72D2bF5Af



The screenshot shows the Etherscan interface for a smart contract. The contract address is 0xd4d8701E037D97dAac63a5C760c78D72D2bF5Af. The overview section shows an ETH balance of 0 ETH. The more info section shows the contract creator as 0x291DA01d...7Fb80AA0 at transaction 0x4e259b1c7d... The transactions section shows a single transaction, 0x4e259b1c7d..., which is a contract creation transaction. The transaction details show it was created by 0x291DA01d...7Fb80AA0, resulting in a new contract at the given address with a gas fee of 0.00085265 ETH.

o. Interagissez avec votre smart contract après l'avoir déployé en ajoutant le nom du premier candidat qui sera votre « Nom de famille »



The screenshot shows the Remix IDE interface. On the left, the 'Déployer et exécuter des transactions' panel is active, showing the contract 'ELECTION AT 0XD4D...F5AF9' with a balance of 0 ETH. The 'Interactions de bas niveau' section shows the 'addCandidate' function being called. The main editor displays the Solidity code for the 'Election' contract, which includes a 'Candidate' struct, a 'voters' mapping, and functions for adding candidates and voting. The console at the bottom shows the transaction details for the 'addCandidate' function call, including the block number, transaction index, from address, to address, value, and gas used.

OverviewState

[This is a Sepolia Testnet transaction only]

Transaction Hash:

0xc50d6926d8c7166893b554d1ee57b4882d177653500d44d0bfa2f15cd054e7ac

Status:

Success

Block:

57023611 Block Confirmation

Timestamp:

6 secs ago (Apr-15-2024 08:44:36 AM +UTC)

Transaction Action:

CallAdd CandidateFunction by 0x291DA01d...7FbF80AA0 on 0xd4d8701E...2D2bF5A9

From:

0x291DA01dF2137a3B616239E5E29baF7FbF80AA0

To:

0xd4d8701E037D97dAac63a5C760c78D72D2bF5A9

Value:

0 ETH (\$0.00)

Transaction Fee:

0.00018977696599148 ETH (\$0.00)

Gas Price:

2.07970199 Gwei (0.00000000207970199 ETH)

Gas Limit & Usage by Txn:

92,197 | 91,252 (98.98%)

Gas Fees:

Base: 0.57970199 Gwei | Max: 2.12004353 Gwei | Max Priority: 1.5 Gwei

Burnt & Txn Savings Fees:

Burnt: 0.00005289896599148 ETH (\$0.00)Txn Savings: 0.00000368124620808 ETH (\$0.00)

Other Attributes:

Txn Type: 2 (EIP-1559) | Nonce: 3 | Position in Block: 28

Input Data:

Function: addCandidate(string name) ***
MethodID: 0x462e91ec
[0]: 0020
[1]: 0004
[2]: 50454e4700
View Input AsDecode Input Data

q.

DÉPLOYER ET EXÉCUTER DES TRANSACTIONS

Exécuter les transactions en utilisant le dernier résultat de compilation

SauvegarderExécuter

Pinned Contracts (chain id: 11155111)

No pinned contracts found for selected workspace & network

Contrats déployés

ELECTION AT 0XD4D...F5A9 (ERC)

Balance: 0 ETH

addCandidatePENDING

transferOwner...address: newOwner

voteuint256: candidateId

candidates

1

CallData

CallData

1pragmasolidity ^0.4.12;

2

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

4

5import "../Ownable.sol";

6import "../SafeMath.sol";

7

8contract Election is Ownable {

9

10using SafeMath for uint256;

11

12// Model a Candidate

13struct Candidate {

14uint256 id;

15string name;

16uint voteCount;

17}

18

19// Store accounts that have voted

20mapping(address => bool) public voters;

21// Store Candidates

22// Fetch Candidate

23mapping(uint => Candidate) public candidates;

24// Store Candidates Count

25uint public candidatesCount;

26

27// voted event

28event votedEvent (uint indexed _candidateId);

29

30function addCandidate (string memory _name) public {

31candidatesCount++;

32candidates[candidatesCount] = Candidate(candidatesCount, _name, 0);

from0x291DA01dF2137a3B616239E5E29baF7FbF80AA0

toElection.candidates(uint256) 0xd4d8701E037D97dAac63a5C760c78D72D2bF5A9

entrée0x347...00001

entrée décodée{"uint256": "1"}

sortie décodée{"candidatesCount": "1", "name": "PENG", "voteCount": "0"}

[illegible]

DÉPLOYER ET EXÉCUTER DES TRANSACTIONS

Exécuter les transactions en utilisant le dernier résultat de compilation

Sauvegarder Exécuter

Pinned Contracts (chain id: 11155111)

No pinned contracts found for selected workspace & network

Contrats déployés

ELECTION AT ONDARD...PSAFS (BLC)

Balance: 0 ETH

addCandidate CROZUG

transferOwner address newOwner

vote uint256_candidateId

candidates

uint256

CallData **Parameters** **Call**

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

candidatesCo...

owner

voters address

Interactions de bas niveau

CALLDATA

Transact

```

1  pragma solidity ^0.4.12;
2
3  // SPDX-License-Identifier: GPL-3.0
4
5  import "./Ownable.sol";
6  import "./SafeMath.sol";
7
8  contract Election is Ownable {
9
10     using SafeMath for uint256;
11
12     // Model a Candidate
13     struct Candidate {
14         uint256 id;
15         string name;
16         uint voteCount;
17     }
18
19     // Store accounts that have voted
20     mapping(address => bool) public voters;
21     // Store Candidates
22     // Fetch Candidate
23     mapping(uint => Candidate) public candidates;
24     // Store Candidates Count
25     uint public candidatesCount;
26
27     // voted event
28     event votedEvent ( uint indexed_candidateId);
29
30     function addCandidate (string memory _name) public {
31         candidatesCount ++;
32         candidatesCount[] = Candidate(candidatesCount, name, 0);

```

from 0x29da616f2137a3b636239c5c29f9a779f8baad

to Election.addCandidate(string) 0x040701e037d97daac3dc70bc70d724db75ef9

gas 75865 gas

Coût de la transaction 74188 gas

entrée 0x0407...00000

entrée décodée

```

(
    "string_name": "CRIZU,36"
)

```

0 Exécuter toutes les transactions Rechercher avec le hash de la transacti...

s.

The screenshot displays the Remix IDE interface. On the left, the 'Déployer et exécuter des transactions' (Deploy and execute transactions) panel is active, showing the 'Election' contract deployed on the 'Sepolia' network. The contract's state is visible, including the 'candidates' array and the 'candidatesCount' variable. The main editor shows the Solidity code for the 'Election' contract, which includes a 'Candidate' struct and functions for adding candidates and voting. The bottom panel shows the 'Interactions de bas niveau' (Low-level interactions) section, displaying the 'call' function being executed.

t.

0x291DA01dF2137a3B616239E5E29fbaF7FbF80AA0

The screenshot shows the 'Transaction Details' page on Etherscan. The transaction is identified by the hash 0x4e259b1c7dd3062f3f2563a0dc6996dfb13870dd500c040d07af6d1abe375ff. The transaction is successful and has 218 block confirmations. The transaction action is a 'Call' to the method 'addCandidate' of the contract at address 0x291DA01dF2137a3B616239E5E29fbaF7FbF80AA0. The transaction value is 0 ETH, and the gas price is 1.550470369 Gwei. The page also includes a 'More Details' section with a '+ Click to show more' button.

U.

Transaction Details

Overview

Logs (1)

State

[This is a Sepolia Testnet transaction only]

Transaction Hash:

0x9c4b5aa2cf33e9a7c87563fe2bca1dbbcaad92645e6ea241663eee93c6b9b2bb

Status:

Success

Block:

57024243 Block Confirmations

Timestamp:

34 secs ago (Apr-15-2024 08:57:12 AM +UTC)

Transaction Action:

Call Vote Function by 0x291DA01d...7FbF80AA0 on 0xd4d8701E...2D2bF5A9

From:

0x291DA01dF2137a3B616239E5E29fbaF7FbF80AA0

To:

0xd4d8701E037D97dAac63a5C760c78D72D2bF5A9

Value:

0 ETH (\$0.00)

Transaction Fee:

0.000178166095301112 ETH (\$0.00)

Gas Price:

2.565719032 Gwei (0.000000002565719032 ETH)

Gas Limit & Usage by Txn:

70,299 | 69,441 (98.78%)

Gas Fees:

Base: 1.065719032 Gwei | Max: 2.813587011 Gwei | Max Priority: 1.5 Gwei

Burnt & Txn Savings Fees:

Burnt: 0.000074004595301112 ETH (\$0.00)Txn Savings: 0.000017212200329739 ETH (\$0.00)

Other Attributes:

Txn Type: 2 (EIP-1559) | Nonce: 5 | Position In Block: 48

Input Data:

Function: vote(uint256 yes) ***
MethodID: 0x0121b93f
[0]: 0001
View Input As | Decode Input Data

More Details:

Click to show less

DÉPLOYER ET EXÉCUTER DES TRANSACTIONS

Exécuter les transactions en utilisant le dernier résultat de compilation

SauvegarderExécuter

Pinned Contracts (chain id: 11155111)

No pinned contracts found for selected workspace & network

Contrats déployés

ELECTION AT 0xD4D...F5A9 (ERC)

Balance: 0 ETH

addCandidate

transferCand...

vote

candidates

2

call

Interactions de bas niveau

CALLDATA

Transact

election.sol

```
1 pragma solidity ^0.4.12;
2
3 // SPDX-License-Identifier: GPL-3.0
4
5 import "./Ownable.sol";
6 import "./SafeMath.sol";
7
8 contract Election is Ownable {
9
10     using SafeMath for uint256;
11
12     // Model a Candidate
13     struct Candidate {
14         uint256 id;
15         string name;
16         uint voteCount;
17     }
18
19     // Store accounts that have voted
20     mapping(address => bool) public voters;
21     // Store Candidates
22     // Fetch Candidate
23     mapping(uint => Candidate) public candidates;
24     // Store Candidates Count
25     uint public candidatesCount;
26
27     // voted event
28     event votedEvent ( uint indexed _candidateId);
29
30     function addCandidate (string memory _name) public {
31         candidatesCount++;
32         candidates[candidatesCount] = Candidate(candidatesCount, _name, 0);
33     }
34 }
```

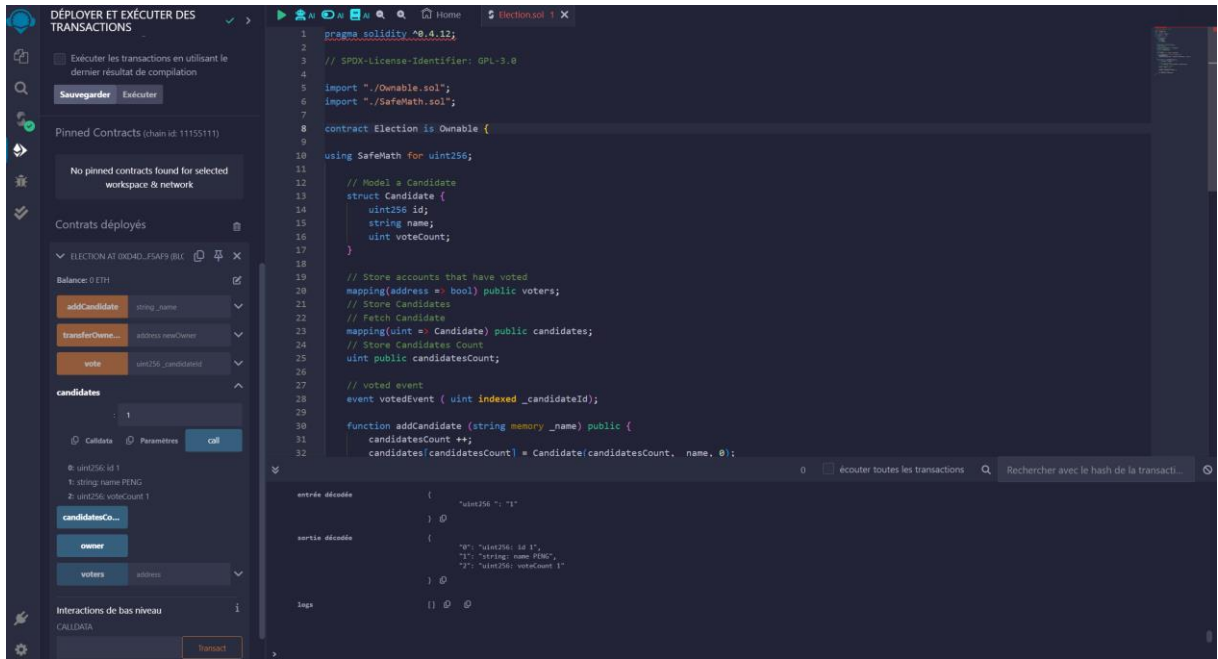
sortie décodée

logs

écouter toutes les transactions

Rechercher avec le hash de la transac...

V.



W.

Transaction Details

<>

OverviewState

⌵

[This is a Sepolia Testnet transaction only]

Transaction Hash:

0x856482c01e8e337e47afcccec1082f584e94f092d78ae934a565f127f64d9285

🔗

Status:

Success

Block:

5702466

2 Block Confirmations

Timestamp:

23 secs ago (Apr-15-2024 09:05:36 AM +UTC)

Transaction Action:

Call 0x0121b93f Method by 0x291DA01d...7Fbf80AA0 on 0xB984005b...264779286

🔗✎

From:

0x291DA01dF2137a3B616239E5E29fbaF7Fbf80AA0

🔗

To:

0xB984005bB89bb0f914A64c28fB9fffe264779286

🔗

Value:

0 ETH (\$0.00)

Transaction Fee:

0.000063134951687064 ETH (\$0.00)

Gas Price:

2.977501966 Gwei (0.000000002977501966 ETH)

Gas Limit & Usage by Txn:

21,370 | 21,204 (99.22%)

Gas Fees:

Base: 1.477501966 Gwei | Max: 3.271303552 Gwei | Max Priority: 1.5 Gwei

Burnt & Txn Savings Fees:

Burnt: 0.000031328951687064 ETH (\$0.00)Txn Savings: 0.000006229768829544 ETH (\$0.00)

Other Attributes:

Txn Type: 2 (EIP-1559) | Nonce: 6 | Position in Block: 35

Input Data:

0x0121b93f0001

View Input As

More Details:

Click to show less

DÉPLOYER ET EXÉCUTER DES TRANSACTIONS

owner

voters address

Interactions de bas niveau

CALLDATA

Transaction

ELECTION AT 0x896...79266 (BLD)

Balance: 0.00847094486728956 ETH

addCandidate string_name

transferOwner... address newOwner

vote

_candidateId 1

Calldata Paramètres Transaction

candidates uint256

1: string_name

2: uint256: voteCount 0

candidatesCo...

owner

voters address

Interactions de bas niveau

CALLDATA

Transaction

```
1 pragma solidity ^0.4.12;
2
3 // SPDX-License-Identifier: GPL-3.0
4
5 import "./Ownable.sol";
6 import "./SafeMath.sol";
7
8 contract Election is Ownable {
9
10     using SafeMath for uint256;
11
12     // Model a Candidate
13     struct Candidate {
14         uint256 id;
15         string name;
16         uint voteCount;
17     }
18
19     // Store accounts that have voted
20     mapping(address => bool) public voters;
21     // Store Candidates
22     // Fetch Candidate
23     mapping(uint => Candidate) public candidates;
24     // Store Candidates Count
25     uint public candidatesCount;
26
27     // voted event
28     event votedEvent ( uint indexed _candidateId);
29
30     function addCandidate (string memory _name) public {
31         candidatesCount++;
32         candidates[candidatesCount] = Candidate(candidatesCount, _name, 0);
33     }
```

0 ☐ écouter toutes les transactions Rechercher avec le hash de la transacti... **Debugpage**

0x [call] from: 0x2910A81dF2137a38616238E5E29Fba77f8f80A0 to: Storage.(fallback) data: 0x347...00001

from 0x2910A81dF2137a38616238E5E29Fba77f8f80A0

to Storage.(fallback) 0x2910A81dF2137a38616238E5E29Fba77f8f80A0

entrée 0x347...00001

entrée décodée -

sortie décodée -

logs []

DÉPLOYER ET EXÉCUTER DES TRANSACTIONS

Pinned Contracts (chain id: 11155111)

No pinned contracts found for selected workspace & network

Contrats déployés

ELECTION AT 0x04D...F5A99 (BLD)

Balance: 0 ETH

addCandidate string_name

transferOwner... address newOwner

vote uint256: _candidateId

candidates

1

Calldata Paramètres call

uint256: id 1

1: string: name: PING

2: uint256: voteCount: 2

candidatesCo...

owner

voters address

Interactions de bas niveau

CALLDATA

Transaction

ELECTION AT 0x896...79266 (BLD)

```
30 function addCandidate (string memory _name) public {
31     candidatesCount++;
32     candidates[candidatesCount] = Candidate(candidatesCount, _name, 0);
33 }
34
35 function vote (uint _candidateId) public {
36     // require that they haven't voted before
37     require(!voters[msg.sender]);
38
39     // require a valid candidate
40     require(_candidateId > 0 && _candidateId <= candidatesCount);
41
42     // record that voter has voted
43     voters[msg.sender] = true;
44
45     // update candidate vote Count
46     candidates[_candidateId].voteCount++;
47
48     // trigger voted event
49     emit votedEvent (_candidateId);
50 }
51
52 }
```

0 ☐ écouter toutes les transactions Rechercher avec le hash de la transacti...

entrée décodée { "uint256": "1" }

sortie décodée { "log": { "topics": ["uint256: id 1", "1", "string: name: PING", "2", "uint256: voteCount: 2"] }, "data": "" } }

logs []

X.

Transaction Details

Overview

Logs (1)

State

[This is a Sepolia Testnet transaction only]

Transaction Hash:

0xaf840b9ea70f15f129dfdc21b9a335dc124c0f971e1751f73b4738ac9b4a1f9d

Status:

Success

Block:

57024831 Block Confirmation

Timestamp:

7 secs ago (Apr-15-2024 09:09:00 AM +UTC)

Transaction Action:

CallTransfer OwnershipFunction by 0x291DA01d...7FbF80AA0 on 0xd4d8701E...2D2bF5Af9

From:

0x291DA01dF2137a3B616239E5E29fbaF7FbF80AA0

To:

0xd4d8701E037D97dAac63a5C760c78D72D2bF5Af9

Value:

0 ETH (\$0.00)

Transaction Fee:

0.000080512627746629 ETH (\$0.00)

Gas Price:

2.803657337 Gwei (0.00000002803657337 ETH)

Gas Limit & Usage by Txn:

29,065 | 28,717 (98.8%)

Gas Fees:

Base: 1.303657337 Gwei | Max: 3.431416139 Gwei | Max Priority: 1.5 Gwei

Burnt & Txn Savings Fees:

Burnt: 0.000037437127746629 ETH (\$0.00)Txn Savings: 0.000018027349517034 ETH (\$0.00)

Other Attributes:

Txn Type: 2 (EIP-1559) | Nonce: 7 | Position in Block: 77

Input Data:

Function: transferOwnership(address newOwner) ***
MethodID: 0xf2fde38b
[0]: 000000000000000000000000b984005bb89bb0f914a64c28fb9fffe264779286
View Input AsDecode Input Data

More Details:

Click to show less

DEPLOYER ET EXECUTER DES TRANSACTIONS

Exécuter les transactions en utilisant le dernier résultat de compilation

SauvegarderExécuter

Pinned Contracts (chain id: 11155111)

No pinned contracts found for selected workspace & network

Contrats déployés

ELECTION AT 0xd4d...f5af9 (BLC)

Balance: 0 ETH

addCandidatestring_name

transferOwnershipnewOwner: 0xd8940028892b09146A-20E

CallDataParamètresTransact

voteuint256_candidateId

candidatesuint256

CallDataParamètresCall

0: uint256: id 1

1: string name: PENG

2: uint256: voteCount: 2

candidateCount

owner

votersaddress

30function addCandidate (string memory _name) public {

31candidatesCount ++;

32candidates[candidatesCount] = Candidate(candidatesCount, _name, 0);

33}

34

35function vote (uint _candidateId) public {

36// require that they haven't voted before

37require(!voters[msg.sender]);

38

39// require a valid candidate

40require(_candidateId > 0 && _candidateId == candidatesCount);

41

42// record that voter has voted

43voters[msg.sender] = true;

44

45// update candidate vote Count

46candidates[_candidateId].voteCount ++;

47

48// trigger voted event

49emit votedEvent (_candidateId);

50}

51}

52}

0écouter toutes les transactionsRechercher avec le hash de la transacti...

transact to Election.transferOwnership pending ...

view on etherscan

[block: 5702483 txIndex: 77] from: 0x291...8baa0 to: Election.transferOwnership(address) 0xd4d...f5af9 value: 0 wei data: 0xf2f...79286 logs: 1 hash: 0x55c...107f4

Débugage

statut

0x1 Transaction mined et exécutée avec succès

hash de transaction

0xaf840b9ea70f15f129dfdc21b9a335dc124c0f971e1751f73b4738ac9b4a1f9d

Hash du bloc

0xd3c0a06c208c9022f8648014093421a7a0f0b3f8e3283729780278a6a30714

numéro du bloc

5702483

y. A votre avis comment pourrions-nous sécuriser l'appel de la fonction addCandidate afin que vous soyez le seul à pouvoir gérer les candidats ?

On peut ajouter un mécanisme d'authentification pour vérifier l'identité de l'appelant. Cela peut être réalisé en utilisant une paire de clés publiques/privées ou des signatures cryptographiques.

Z.

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

```

1  pragma solidity ^0.4.12;
2
3  // SPDX-License-Identifier: GPL-3.0
4
5  import "./Ownable.sol";
6  import "./SafeMath.sol";
7
8  contract Election is Ownable {
9
10     using SafeMath for uint256;
11
12     // Model a Candidate
13     struct Candidate {
14         uint256 id;
15         string name;
16         uint voteCount;
17     }
18
19     // Store accounts that have voted
20     mapping(address => bool) public voters;
21     // Store Candidates
22     // Fetch Candidate
23     mapping(uint => Candidate) public candidates;
24     // Store Candidates Count
25     uint public candidatesCount;
26
27     // voted event
28     event votedEvent ( uint indexed _candidateId);
29
30     function addCandidate (string memory _name) public onlyOwner{
31         candidatesCount ++;
32         candidates[candidatesCount] = Candidate(candidatesCount, _name, 0);
33     }
34
35     function vote (uint _candidateId) public {
36         // require that they haven't voted before
37         require(!voters[msg.sender]);
38
39         // require a valid candidate
40         require(_candidateId > 0 && _candidateId <= candidatesCount);
41
42         // record that voter has voted
43         voters[msg.sender] = true;
44
45         // update candidate vote Count
46         candidates[_candidateId].voteCount ++;
47
48         // trigger voted event
49         emit votedEvent (_candidateId);
50     }
51 }
52

```