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 »

Une image contenant texte, capture d’écran, logiciel, Page web

Description générée automatiquement

g.

Une image contenant texte, logiciel, Page web, Icône d’ordinateur

Description générée automatiquement

h.

Une image contenant texte, logiciel, nombre, Page web

Description générée automatiquement

j.

Une image contenant texte, capture d’écran, logiciel, Logiciel multimédia

Description générée automatiquement

l.

Une image contenant texte, capture d’écran, logiciel, Logiciel multimédia

Description générée automatiquement

M.

Une image contenant texte, capture d’écran, logiciel, Logiciel multimédia

Description générée automatiquement

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 :



n.

Une image contenant texte, capture d’écran, logiciel, Logiciel multimédia

Description générée automatiquement

Une image contenant texte, Appareils électroniques, capture d’écran, logiciel

Description générée automatiquement

Une image contenant texte, logiciel, Page web, nombre

Description générée automatiquement

Une image contenant texte, logiciel, Page web, Icône d’ordinateur

Description générée automatiquement

Une image contenant texte, capture d’écran, logiciel, Logiciel multimédia

Description générée automatiquement

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 ?

0xd4d8701E037D97dAac63a5C760c78D72D2bF5AfUne image contenant texte, Police, nombre, logiciel

Description générée automatiquement

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

Une image contenant logiciel, Logiciel multimédia, texte, Logiciel de graphisme

Description générée automatiquement

Une image contenant texte, capture d’écran, logiciel, Page web

Description générée automatiquement

q.

Une image contenant capture d’écran, texte, logiciel, Logiciel multimédia

Description générée automatiquement

r.

Une image contenant texte, capture d’écran, logiciel, Page web

Description générée automatiquement

Une image contenant capture d’écran, texte, logiciel, Logiciel multimédia

Description générée automatiquement

s.

Une image contenant texte, capture d’écran, logiciel, Logiciel multimédia

Description générée automatiquement

t.

0x291DA01dF2137a3B616239E5E29fbaF7Fbf80AA0

Une image contenant texte, capture d’écran, logiciel, Page web

Description générée automatiquement

u.

Une image contenant texte, capture d’écran, logiciel, nombre

Description générée automatiquement

Une image contenant texte, capture d’écran, logiciel, Logiciel multimédia

Description générée automatiquement

v.

Une image contenant capture d’écran, texte, logiciel, Logiciel multimédia

Description générée automatiquement

w.

Une image contenant texte, capture d’écran, logiciel, nombre

Description générée automatiquement

Une image contenant texte, capture d’écran, logiciel, Logiciel multimédia

Description générée automatiquement

Une image contenant capture d’écran, texte, logiciel, Logiciel multimédia

Description générée automatiquement

x.

Une image contenant texte, capture d’écran, logiciel, nombre

Description générée automatiquementUne image contenant texte, capture d’écran, logiciel, Logiciel multimédia

Description générée automatiquement

y. A votre avis comment pourrions-nous sécurisé 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.

Une image contenant texte, capture d’écran, Police, ligne

Description générée automatiquement