**TRAVAUX PRATIQUE :**

**Développer, Deloyer et Interagir avec un contrat intelligent sur Ethereum**

**À la fin de votre exercice, poussez le code du contrat intelligent sur votre projet github que vous devez créer avec le répertoire principale « Système distribué : Blockchain & Contrat intelligent ».**

**Lorsque vous avez terminé la quête, veuillez inviter le professeur dont l’identifiant est le suivant @cozcan à collaborer à votre compte github. Tous les fichiers (fichiers de configuration, code de contrat intelligent…) créés pour ce TP devront y figurer. Vous redigérer un rapport avec chacune des étapes, il faudra réaliser un imprime écran de chacune des étapes comme illustrer dans le TP ainsi que fournir le lien Etherscan de chaque transaction réalisée.**

**Les objectifs de votre TP :**

1. **Prise en main des outils Remix et Metamask**
2. **Développement du smart contract**
3. **Déploiement du smart contract**
4. **Intéraction avec le smart contract**

**Rappel :**

**Il existe différents environnements de développement pour réaliser ce TP. Nous utiliserons uniquement l’outil IDE en ligne** [**Remix**](https://remix.ethereum.org/) **et le portefeuille électronique Metamask sur votre navigateur Chrome ou Firefox.**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **Functionalities** | **Remix** | **MyEtherWallet** | **Geth** |
| 1 | Configure the Blockchain Network | - | - | + |
|  |
| 2 | Deploy a private Blockchain | - | - | + |
| 3 | Develop a smart contract | + | - | + |
| 4 | Compile a smart contract | + | - | + |
| 5 | Create a user account “Wallet” | + | + | + |
| 6 | Deploy a smart contract | + | + | + |
| 7 | Create the UI for interacting | + | + | + |
| 8 | Run the Node client | - | - | + |
| 9 | Interact with the smart contract | + | + | + |
| 10 | Monitor the execution | - | - | + |

# Prise en main des outils Remix et Metamask

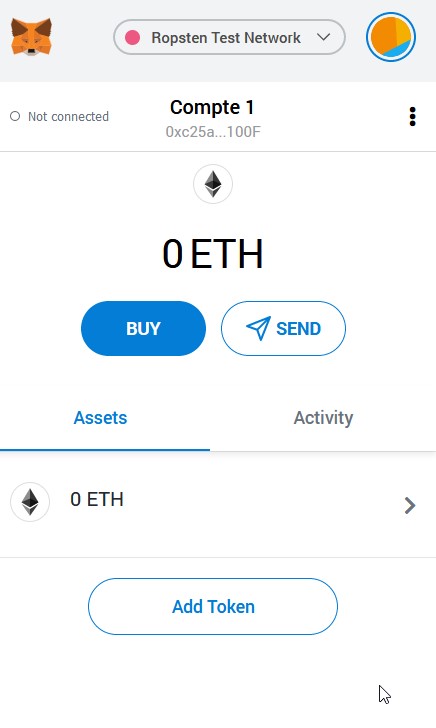
L’objectif de cette session est de prendre en main les outils permettant d’interagir avec une Blockchain de type publique.

Dans notre cas nous partirons sur une blockchain de type Ethereum et plus particulièrement sur l’environnement de test nommé « Ethereum Ropsten » permettant de pouvoir réaliser des transactions, déployer et interagir avec un smart contract gratuitement.

1. Naviguer sur le site et télécharger Metamask sur le site suivant : <https://metamask.io/>
2. Suivez les étapes de génération du portefeuille en sauvegardant bien votre seed

phrase

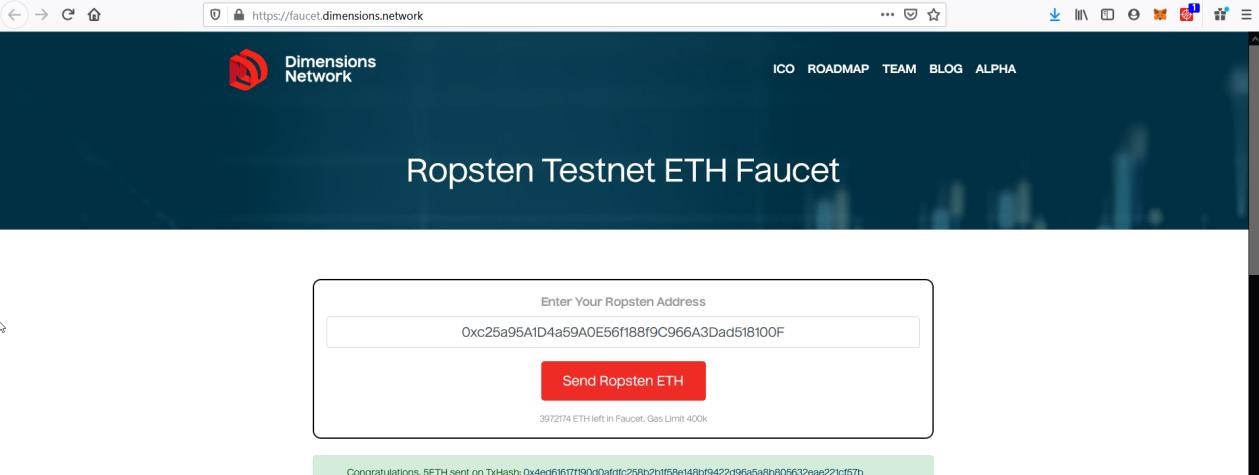
1. Vous devrez ensuite avoir accès à votre premier compte « wallet » dont la clé publique commence par « 0x… » (voir illustration ci-dessous).



Vous disposez d’un compte avec zero ETH (Ether) qui représente la cryptomonnaie du réseau Ethereum. Afin de pouvoir réaliser des transactions et déployer un smart contract sur Ethereum il est nécessaire comme vu en cours d’avoir des ETH sur son compte.

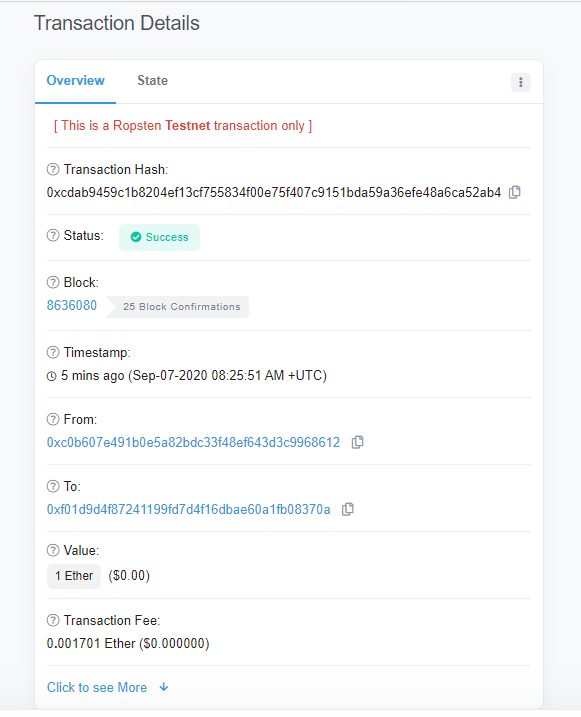
1. Recevez vos premiers ETH sur votre compte Metamask en allant sur la faucet en ligne <https://faucet.dimensions.network/>puis copier la clée publique de votre compte.

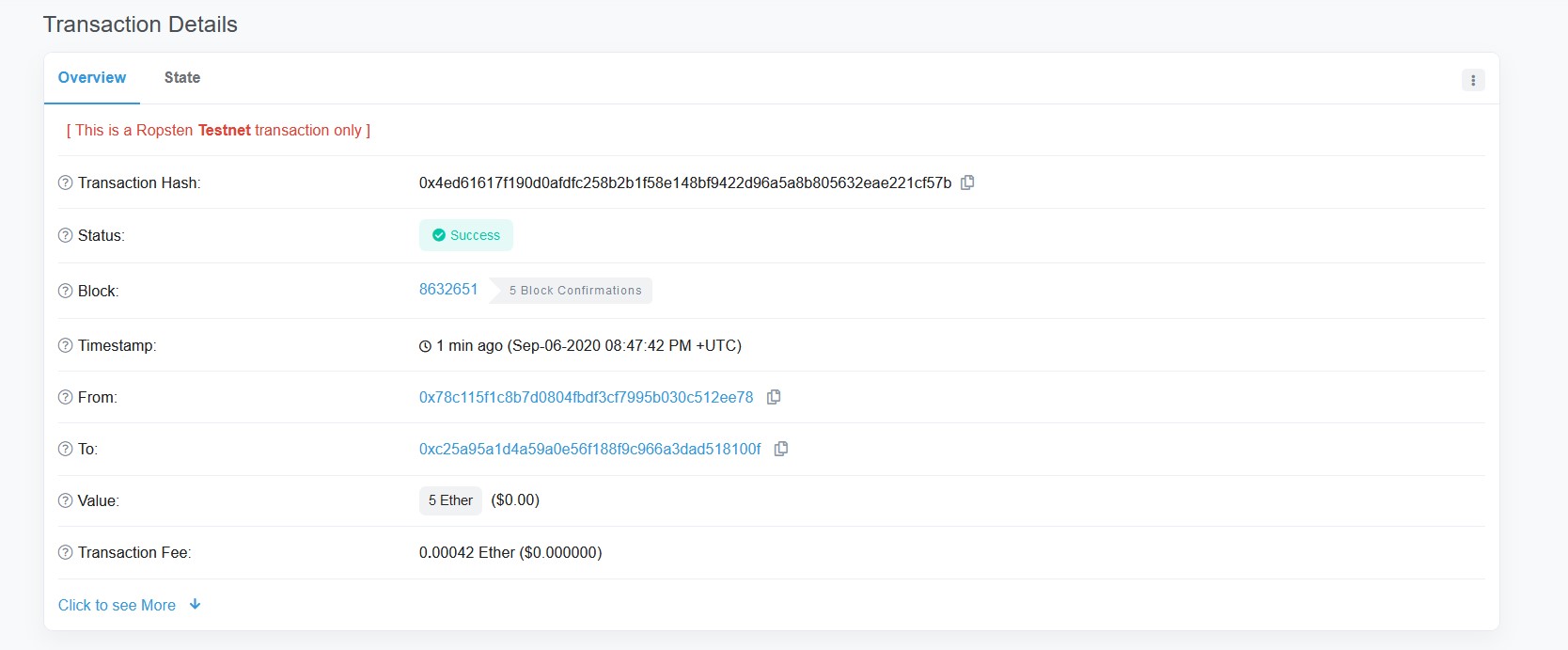
0xf01d9d4F87241199fD7d4F16dBAe60A1Fb08370a



1. Consulter la transaction générée vers votre compte et prenez en compte les détails de cette dernière. Fournissez également les détails de la transaction

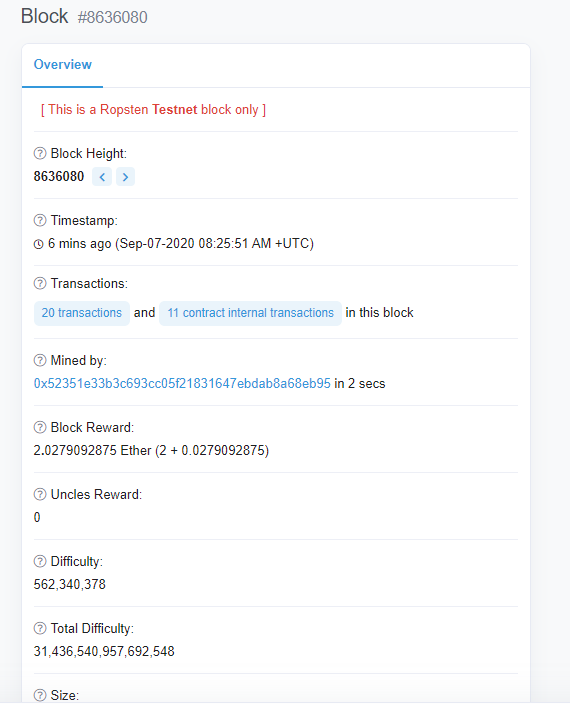
My transaction

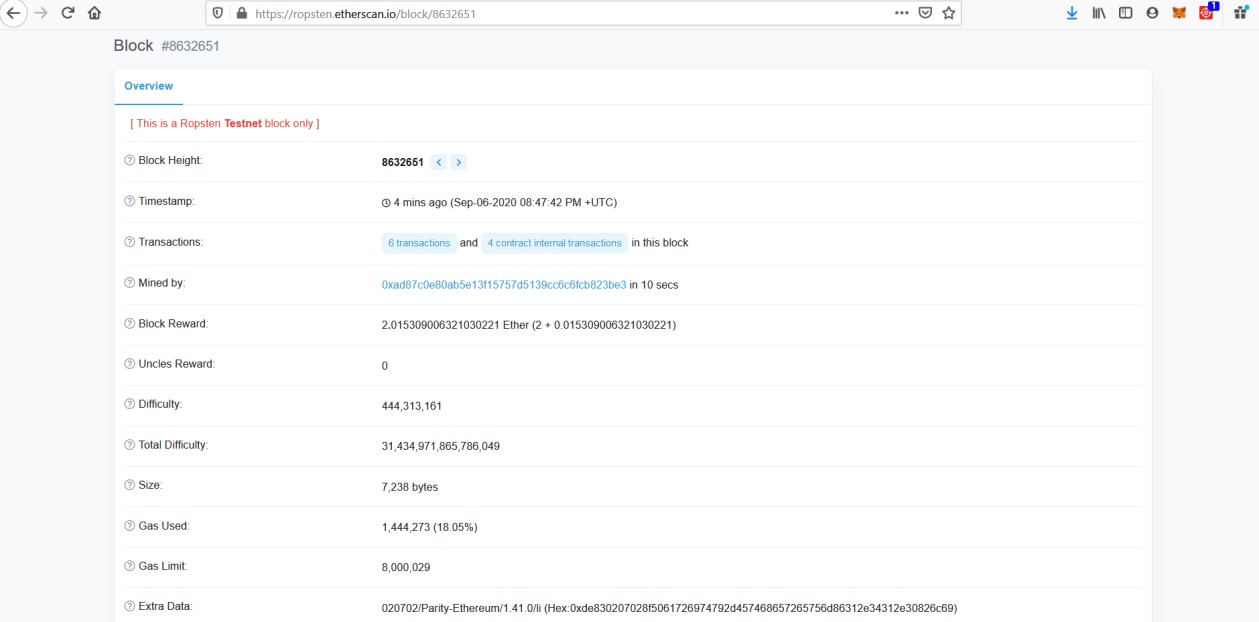




1. Consulter ensuite le numéro de Block de votre transaction. Fournissez également les détails de la transaction

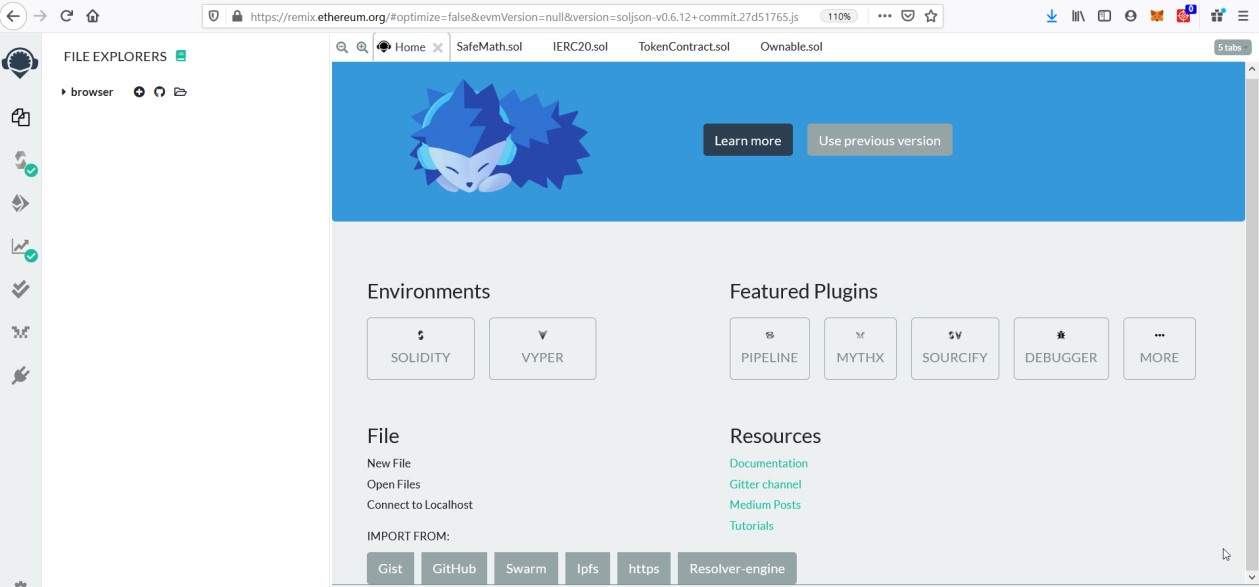
My Block





1. Générer votre première transaction Ethereum sur le réseau Rospten envoyant 1 ETH à l’adresse suivante « 0xc25a95A1D4a59A0E56f188f9C966A3Dad518100 ».

1. Ouvrir l’IDE Remix : remix.ethereum.org



1. Récupérer le code source de votre premier smart contract : https://github.com/cozcan/TP\_Election
2. Ajouter l’ensemble des fichiers Solidity sur votre environnement Remix.
3. Compiler votre smart contract « Election » et fournissez l’ABI ainsi que le Byte code du contrat.

ABI

[

{

"anonymous": false,

"inputs": [

{

"indexed": true,

"internalType": "address",

"name": "previousOwner",

"type": "address"

},

{

"indexed": true,

"internalType": "address",

"name": "newOwner",

"type": "address"

}

],

"name": "OwnershipTransferred",

"type": "event"

},

{

"anonymous": false,

"inputs": [

{

"indexed": true,

"internalType": "uint256",

"name": "\_candidateId",

"type": "uint256"

}

],

"name": "votedEvent",

"type": "event"

},

{

"inputs": [

{

"internalType": "string",

"name": "\_name",

"type": "string"

}

],

"name": "addCandidate",

"outputs": [],

"stateMutability": "nonpayable",

"type": "function"

},

{

"inputs": [

{

"internalType": "uint256",

"name": "",

"type": "uint256"

}

],

"name": "candidates",

"outputs": [

{

"internalType": "uint256",

"name": "id",

"type": "uint256"

},

{

"internalType": "string",

"name": "name",

"type": "string"

},

{

"internalType": "uint256",

"name": "voteCount",

"type": "uint256"

}

],

"stateMutability": "view",

"type": "function"

},

{

"inputs": [],

"name": "candidatesCount",

"outputs": [

{

"internalType": "uint256",

"name": "",

"type": "uint256"

}

],

"stateMutability": "view",

"type": "function"

},

{

"inputs": [],

"name": "owner",

"outputs": [

{

"internalType": "address",

"name": "",

"type": "address"

}

],

"stateMutability": "view",

"type": "function"

},

{

"inputs": [

{

"internalType": "address",

"name": "newOwner",

"type": "address"

}

],

"name": "transferOwnership",

"outputs": [],

"stateMutability": "nonpayable",

"type": "function"

},

{

"inputs": [

{

"internalType": "uint256",

"name": "\_candidateId",

"type": "uint256"

}

],

"name": "vote",

"outputs": [],

"stateMutability": "nonpayable",

"type": "function"

},

{

"inputs": [

{

"internalType": "address",

"name": "",

"type": "address"

}

],

"name": "voters",

"outputs": [

{

"internalType": "bool",

"name": "",

"type": "bool"

}

],

"stateMutability": "view",

"type": "function"

}

]

ByteCode

{

"linkReferences": {},

"object": "",

"opcodes": "PUSH1 0x80 PUSH1 0x40 MSTORE CALLVALUE DUP1 ISZERO PUSH2 0x10 JUMPI PUSH1 0x0 DUP1 REVERT JUMPDEST POP CALLER PUSH1 0x0 DUP1 PUSH2 0x100 EXP DUP2 SLOAD DUP2 PUSH20 0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF MUL NOT AND SWAP1 DUP4 PUSH20 0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF AND MUL OR SWAP1 SSTORE POP PUSH2 0x8AB DUP1 PUSH2 0x60 PUSH1 0x0 CODECOPY PUSH1 0x0 RETURN INVALID PUSH1 0x80 PUSH1 0x40 MSTORE CALLVALUE DUP1 ISZERO PUSH2 0x10 JUMPI PUSH1 0x0 DUP1 REVERT JUMPDEST POP PUSH1 0x4 CALLDATASIZE LT PUSH2 0x7D JUMPI PUSH1 0x0 CALLDATALOAD PUSH1 0xE0 SHR DUP1 PUSH4 0x462E91EC GT PUSH2 0x5B JUMPI DUP1 PUSH4 0x462E91EC EQ PUSH2 0x183 JUMPI DUP1 PUSH4 0x8DA5CB5B EQ PUSH2 0x23E JUMPI DUP1 PUSH4 0xA3EC138D EQ PUSH2 0x272 JUMPI DUP1 PUSH4 0xF2FDE38B EQ PUSH2 0x2CC JUMPI PUSH2 0x7D JUMP JUMPDEST DUP1 PUSH4 0x121B93F EQ PUSH2 0x82 JUMPI DUP1 PUSH4 0x2D35A8A2 EQ PUSH2 0xB0 JUMPI DUP1 PUSH4 0x3477EE2E EQ PUSH2 0xCE JUMPI JUMPDEST PUSH1 0x0 DUP1 REVERT JUMPDEST PUSH2 0xAE PUSH1 0x4 DUP1 CALLDATASIZE SUB PUSH1 0x20 DUP2 LT ISZERO PUSH2 0x98 JUMPI PUSH1 0x0 DUP1 REVERT JUMPDEST DUP2 ADD SWAP1 DUP1 DUP1 CALLDATALOAD SWAP1 PUSH1 0x20 ADD SWAP1 SWAP3 SWAP2 SWAP1 POP POP POP PUSH2 0x310 JUMP JUMPDEST STOP JUMPDEST PUSH2 0xB8 PUSH2 0x42F JUMP JUMPDEST PUSH1 0x40 MLOAD DUP1 DUP3 DUP2 MSTORE PUSH1 0x20 ADD SWAP2 POP POP PUSH1 0x40 MLOAD DUP1 SWAP2 SUB SWAP1 RETURN JUMPDEST PUSH2 0xFA PUSH1 0x4 DUP1 CALLDATASIZE SUB PUSH1 0x20 DUP2 LT ISZERO PUSH2 0xE4 JUMPI PUSH1 0x0 DUP1 REVERT JUMPDEST DUP2 ADD SWAP1 DUP1 DUP1 CALLDATALOAD SWAP1 PUSH1 0x20 ADD SWAP1 SWAP3 SWAP2 SWAP1 POP POP POP PUSH2 0x435 JUMP JUMPDEST PUSH1 0x40 MLOAD DUP1 DUP5 DUP2 MSTORE PUSH1 0x20 ADD DUP1 PUSH1 0x20 ADD DUP4 DUP2 MSTORE PUSH1 0x20 ADD DUP3 DUP2 SUB DUP3 MSTORE DUP5 DUP2 DUP2 MLOAD DUP2 MSTORE PUSH1 0x20 ADD SWAP2 POP DUP1 MLOAD SWAP1 PUSH1 0x20 ADD SWAP1 DUP1 DUP4 DUP4 PUSH1 0x0 JUMPDEST DUP4 DUP2 LT ISZERO PUSH2 0x146 JUMPI DUP1 DUP3 ADD MLOAD DUP2 DUP5 ADD MSTORE PUSH1 0x20 DUP2 ADD SWAP1 POP PUSH2 0x12B JUMP JUMPDEST POP POP POP POP SWAP1 POP SWAP1 DUP2 ADD SWAP1 PUSH1 0x1F AND DUP1 ISZERO PUSH2 0x173 JUMPI DUP1 DUP3 SUB DUP1 MLOAD PUSH1 0x1 DUP4 PUSH1 0x20 SUB PUSH2 0x100 EXP SUB NOT AND DUP2 MSTORE PUSH1 0x20 ADD SWAP2 POP JUMPDEST POP SWAP5 POP POP POP POP POP PUSH1 0x40 MLOAD DUP1 SWAP2 SUB SWAP1 RETURN JUMPDEST PUSH2 0x23C PUSH1 0x4 DUP1 CALLDATASIZE SUB PUSH1 0x20 DUP2 LT ISZERO PUSH2 0x199 JUMPI PUSH1 0x0 DUP1 REVERT JUMPDEST DUP2 ADD SWAP1 DUP1 DUP1 CALLDATALOAD SWAP1 PUSH1 0x20 ADD SWAP1 PUSH5 0x100000000 DUP2 GT ISZERO PUSH2 0x1B6 JUMPI PUSH1 0x0 DUP1 REVERT JUMPDEST DUP3 ADD DUP4 PUSH1 0x20 DUP3 ADD GT ISZERO PUSH2 0x1C8 JUMPI PUSH1 0x0 DUP1 REVERT JUMPDEST DUP1 CALLDATALOAD SWAP1 PUSH1 0x20 ADD SWAP2 DUP5 PUSH1 0x1 DUP4 MUL DUP5 ADD GT PUSH5 0x100000000 DUP4 GT OR ISZERO PUSH2 0x1EA JUMPI PUSH1 0x0 DUP1 REVERT JUMPDEST SWAP2 SWAP1 DUP1 DUP1 PUSH1 0x1F ADD PUSH1 0x20 DUP1 SWAP2 DIV MUL PUSH1 0x20 ADD PUSH1 0x40 MLOAD SWAP1 DUP2 ADD PUSH1 0x40 MSTORE DUP1 SWAP4 SWAP3 SWAP2 SWAP1 DUP2 DUP2 MSTORE PUSH1 0x20 ADD DUP4 DUP4 DUP1 DUP3 DUP5 CALLDATACOPY PUSH1 0x0 DUP2 DUP5 ADD MSTORE PUSH1 0x1F NOT PUSH1 0x1F DUP3 ADD AND SWAP1 POP DUP1 DUP4 ADD SWAP3 POP POP POP POP POP POP POP SWAP2 SWAP3 SWAP2 SWAP3 SWAP1 POP POP POP PUSH2 0x4F7 JUMP JUMPDEST STOP JUMPDEST PUSH2 0x246 PUSH2 0x573 JUMP JUMPDEST PUSH1 0x40 MLOAD DUP1 DUP3 PUSH20 0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF AND DUP2 MSTORE PUSH1 0x20 ADD SWAP2 POP POP PUSH1 0x40 MLOAD DUP1 SWAP2 SUB SWAP1 RETURN JUMPDEST PUSH2 0x2B4 PUSH1 0x4 DUP1 CALLDATASIZE SUB PUSH1 0x20 DUP2 LT ISZERO PUSH2 0x288 JUMPI PUSH1 0x0 DUP1 REVERT JUMPDEST DUP2 ADD SWAP1 DUP1 DUP1 CALLDATALOAD PUSH20 0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF AND SWAP1 PUSH1 0x20 ADD SWAP1 SWAP3 SWAP2 SWAP1 POP POP POP PUSH2 0x597 JUMP JUMPDEST PUSH1 0x40 MLOAD DUP1 DUP3 ISZERO ISZERO DUP2 MSTORE PUSH1 0x20 ADD SWAP2 POP POP PUSH1 0x40 MLOAD DUP1 SWAP2 SUB SWAP1 RETURN JUMPDEST PUSH2 0x30E PUSH1 0x4 DUP1 CALLDATASIZE SUB PUSH1 0x20 DUP2 LT ISZERO PUSH2 0x2E2 JUMPI PUSH1 0x0 DUP1 REVERT JUMPDEST DUP2 ADD SWAP1 DUP1 DUP1 CALLDATALOAD PUSH20 0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF AND SWAP1 PUSH1 0x20 ADD SWAP1 SWAP3 SWAP2 SWAP1 POP POP POP PUSH2 0x5B7 JUMP JUMPDEST STOP JUMPDEST PUSH1 0x1 PUSH1 0x0 CALLER PUSH20 0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF AND PUSH20 0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF AND DUP2 MSTORE PUSH1 0x20 ADD SWAP1 DUP2 MSTORE PUSH1 0x20 ADD PUSH1 0x0 KECCAK256 PUSH1 0x0 SWAP1 SLOAD SWAP1 PUSH2 0x100 EXP SWAP1 DIV PUSH1 0xFF AND ISZERO PUSH2 0x367 JUMPI PUSH1 0x0 DUP1 REVERT JUMPDEST PUSH1 0x0 DUP2 GT DUP1 ISZERO PUSH2 0x379 JUMPI POP PUSH1 0x3 SLOAD DUP2 GT ISZERO JUMPDEST PUSH2 0x382 JUMPI PUSH1 0x0 DUP1 REVERT JUMPDEST PUSH1 0x1 DUP1 PUSH1 0x0 CALLER PUSH20 0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF AND PUSH20 0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF AND DUP2 MSTORE PUSH1 0x20 ADD SWAP1 DUP2 MSTORE PUSH1 0x20 ADD PUSH1 0x0 KECCAK256 PUSH1 0x0 PUSH2 0x100 EXP DUP2 SLOAD DUP2 PUSH1 0xFF MUL NOT AND SWAP1 DUP4 ISZERO ISZERO MUL OR SWAP1 SSTORE POP PUSH1 0x2 PUSH1 0x0 DUP3 DUP2 MSTORE PUSH1 0x20 ADD SWAP1 DUP2 MSTORE PUSH1 0x20 ADD PUSH1 0x0 KECCAK256 PUSH1 0x2 ADD PUSH1 0x0 DUP2 SLOAD DUP1 SWAP3 SWAP2 SWAP1 PUSH1 0x1 ADD SWAP2 SWAP1 POP SSTORE POP DUP1 PUSH32 0xFFF3C900D938D21D0990D786E819F29B8D05C1EF587B462B939609625B684B16 PUSH1 0x40 MLOAD PUSH1 0x40 MLOAD DUP1 SWAP2 SUB SWAP1 LOG2 POP JUMP JUMPDEST PUSH1 0x3 SLOAD DUP2 JUMP JUMPDEST PUSH1 0x2 PUSH1 0x20 MSTORE DUP1 PUSH1 0x0 MSTORE PUSH1 0x40 PUSH1 0x0 KECCAK256 PUSH1 0x0 SWAP2 POP SWAP1 POP DUP1 PUSH1 0x0 ADD SLOAD SWAP1 DUP1 PUSH1 0x1 ADD DUP1 SLOAD PUSH1 0x1 DUP2 PUSH1 0x1 AND ISZERO PUSH2 0x100 MUL SUB AND PUSH1 0x2 SWAP1 DIV DUP1 PUSH1 0x1F ADD PUSH1 0x20 DUP1 SWAP2 DIV MUL PUSH1 0x20 ADD PUSH1 0x40 MLOAD SWAP1 DUP2 ADD PUSH1 0x40 MSTORE DUP1 SWAP3 SWAP2 SWAP1 DUP2 DUP2 MSTORE PUSH1 0x20 ADD DUP3 DUP1 SLOAD PUSH1 0x1 DUP2 PUSH1 0x1 AND ISZERO PUSH2 0x100 MUL SUB AND PUSH1 0x2 SWAP1 DIV DUP1 ISZERO PUSH2 0x4E7 JUMPI DUP1 PUSH1 0x1F LT PUSH2 0x4BC JUMPI PUSH2 0x100 DUP1 DUP4 SLOAD DIV MUL DUP4 MSTORE SWAP2 PUSH1 0x20 ADD SWAP2 PUSH2 0x4E7 JUMP JUMPDEST DUP3 ADD SWAP2 SWAP1 PUSH1 0x0 MSTORE PUSH1 0x20 PUSH1 0x0 KECCAK256 SWAP1 JUMPDEST DUP2 SLOAD DUP2 MSTORE SWAP1 PUSH1 0x1 ADD SWAP1 PUSH1 0x20 ADD DUP1 DUP4 GT PUSH2 0x4CA JUMPI DUP3 SWAP1 SUB PUSH1 0x1F AND DUP3 ADD SWAP2 JUMPDEST POP POP POP POP POP SWAP1 DUP1 PUSH1 0x2 ADD SLOAD SWAP1 POP DUP4 JUMP JUMPDEST PUSH1 0x3 PUSH1 0x0 DUP2 SLOAD DUP1 SWAP3 SWAP2 SWAP1 PUSH1 0x1 ADD SWAP2 SWAP1 POP SSTORE POP PUSH1 0x40 MLOAD DUP1 PUSH1 0x60 ADD PUSH1 0x40 MSTORE DUP1 PUSH1 0x3 SLOAD DUP2 MSTORE PUSH1 0x20 ADD DUP3 DUP2 MSTORE PUSH1 0x20 ADD PUSH1 0x0 DUP2 MSTORE POP PUSH1 0x2 PUSH1 0x0 PUSH1 0x3 SLOAD DUP2 MSTORE PUSH1 0x20 ADD SWAP1 DUP2 MSTORE PUSH1 0x20 ADD PUSH1 0x0 KECCAK256 PUSH1 0x0 DUP3 ADD MLOAD DUP2 PUSH1 0x0 ADD SSTORE PUSH1 0x20 DUP3 ADD MLOAD DUP2 PUSH1 0x1 ADD SWAP1 DUP1 MLOAD SWAP1 PUSH1 0x20 ADD SWAP1 PUSH2 0x562 SWAP3 SWAP2 SWAP1 PUSH2 0x7D8 JUMP JUMPDEST POP PUSH1 0x40 DUP3 ADD MLOAD DUP2 PUSH1 0x2 ADD SSTORE SWAP1 POP POP POP JUMP JUMPDEST PUSH1 0x0 DUP1 SLOAD SWAP1 PUSH2 0x100 EXP SWAP1 DIV PUSH20 0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF AND DUP2 JUMP JUMPDEST PUSH1 0x1 PUSH1 0x20 MSTORE DUP1 PUSH1 0x0 MSTORE PUSH1 0x40 PUSH1 0x0 KECCAK256 PUSH1 0x0 SWAP2 POP SLOAD SWAP1 PUSH2 0x100 EXP SWAP1 DIV PUSH1 0xFF AND DUP2 JUMP JUMPDEST PUSH1 0x0 DUP1 SLOAD SWAP1 PUSH2 0x100 EXP SWAP1 DIV PUSH20 0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF AND PUSH20 0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF AND CALLER PUSH20 0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF AND EQ PUSH2 0x678 JUMPI PUSH1 0x40 MLOAD PUSH32 0x8C379A000000000000000000000000000000000000000000000000000000000 DUP2 MSTORE PUSH1 0x4 ADD DUP1 DUP1 PUSH1 0x20 ADD DUP3 DUP2 SUB DUP3 MSTORE PUSH1 0x18 DUP2 MSTORE PUSH1 0x20 ADD DUP1 PUSH32 0x4E6F7420617574686F72697A6564206F7065726174696F6E0000000000000000 DUP2 MSTORE POP PUSH1 0x20 ADD SWAP2 POP POP PUSH1 0x40 MLOAD DUP1 SWAP2 SUB SWAP1 REVERT JUMPDEST PUSH1 0x0 PUSH20 0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF AND DUP2 PUSH20 0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF AND EQ ISZERO PUSH2 0x71B JUMPI PUSH1 0x40 MLOAD PUSH32 0x8C379A000000000000000000000000000000000000000000000000000000000 DUP2 MSTORE PUSH1 0x4 ADD DUP1 DUP1 PUSH1 0x20 ADD DUP3 DUP2 SUB DUP3 MSTORE PUSH1 0x19 DUP2 MSTORE PUSH1 0x20 ADD DUP1 PUSH32 0x416464726573732073686F756C646E2774206265207A65726F00000000000000 DUP2 MSTORE POP PUSH1 0x20 ADD SWAP2 POP POP PUSH1 0x40 MLOAD DUP1 SWAP2 SUB SWAP1 REVERT JUMPDEST DUP1 PUSH20 0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF AND PUSH1 0x0 DUP1 SLOAD SWAP1 PUSH2 0x100 EXP SWAP1 DIV PUSH20 0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF AND PUSH20 0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF AND PUSH32 0x8BE0079C531659141344CD1FD0A4F28419497F9722A3DAAFE3B4186F6B6457E0 PUSH1 0x40 MLOAD PUSH1 0x40 MLOAD DUP1 SWAP2 SUB SWAP1 LOG3 DUP1 PUSH1 0x0 DUP1 PUSH2 0x100 EXP DUP2 SLOAD DUP2 PUSH20 0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF MUL NOT AND SWAP1 DUP4 PUSH20 0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF AND MUL OR SWAP1 SSTORE POP POP JUMP JUMPDEST DUP3 DUP1 SLOAD PUSH1 0x1 DUP2 PUSH1 0x1 AND ISZERO PUSH2 0x100 MUL SUB AND PUSH1 0x2 SWAP1 DIV SWAP1 PUSH1 0x0 MSTORE PUSH1 0x20 PUSH1 0x0 KECCAK256 SWAP1 PUSH1 0x1F ADD PUSH1 0x20 SWAP1 DIV DUP2 ADD SWAP3 DUP3 PUSH1 0x1F LT PUSH2 0x819 JUMPI DUP1 MLOAD PUSH1 0xFF NOT AND DUP4 DUP1 ADD OR DUP6 SSTORE PUSH2 0x847 JUMP JUMPDEST DUP3 DUP1 ADD PUSH1 0x1 ADD DUP6 SSTORE DUP3 ISZERO PUSH2 0x847 JUMPI SWAP2 DUP3 ADD JUMPDEST DUP3 DUP2 GT ISZERO PUSH2 0x846 JUMPI DUP3 MLOAD DUP3 SSTORE SWAP2 PUSH1 0x20 ADD SWAP2 SWAP1 PUSH1 0x1 ADD SWAP1 PUSH2 0x82B JUMP JUMPDEST JUMPDEST POP SWAP1 POP PUSH2 0x854 SWAP2 SWAP1 PUSH2 0x858 JUMP JUMPDEST POP SWAP1 JUMP JUMPDEST JUMPDEST DUP1 DUP3 GT ISZERO PUSH2 0x871 JUMPI PUSH1 0x0 DUP2 PUSH1 0x0 SWAP1 SSTORE POP PUSH1 0x1 ADD PUSH2 0x859 JUMP JUMPDEST POP SWAP1 JUMP INVALID LOG2 PUSH5 0x6970667358 0x22 SLT KECCAK256 MSIZE STATICCALL 0xFC SSTORE CHAINID 0x48 PUSH22 0x348051D2417BEF924244D10E68F7925058EB099787DF RETURNDATASIZE 0x2A SWAP2 PUSH5 0x736F6C6343 STOP MOD 0xC STOP CALLER ",

"sourceMap": "113:1147:0:-:0;;;;;;;;;;;;;579:10:1;571:5;;:18;;;;;;;;;;;;;;;;;;113:1147:0;;;;;;"

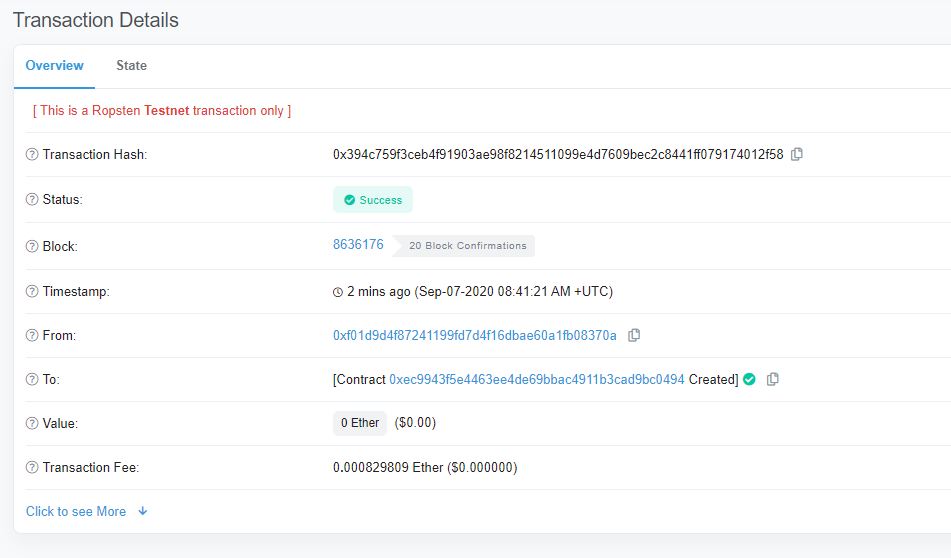
}

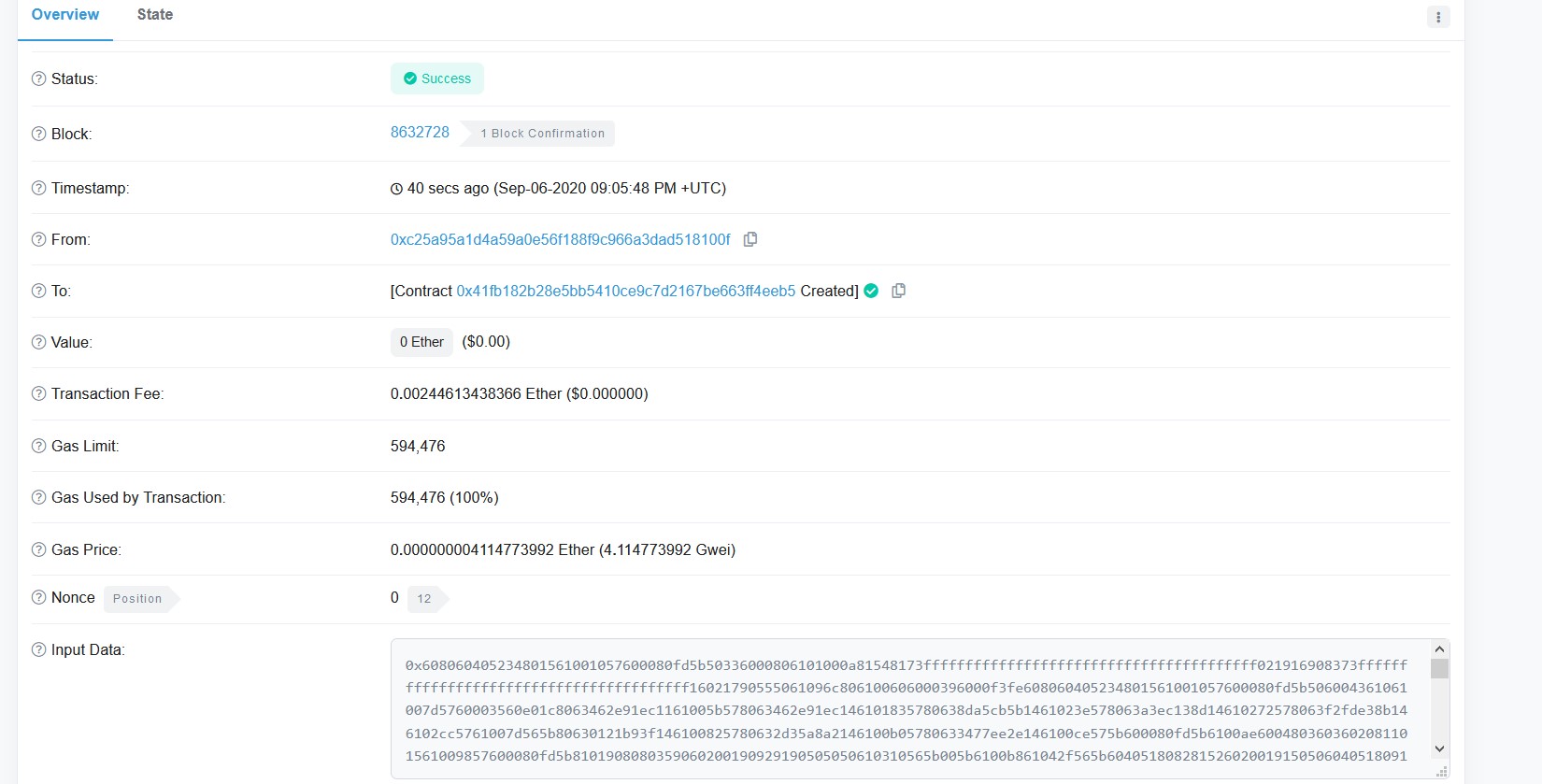


1. Déployer le smart contract « Election.sol » sur le réseau Ropsten et fournissez les

détails de la transaction

My details





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

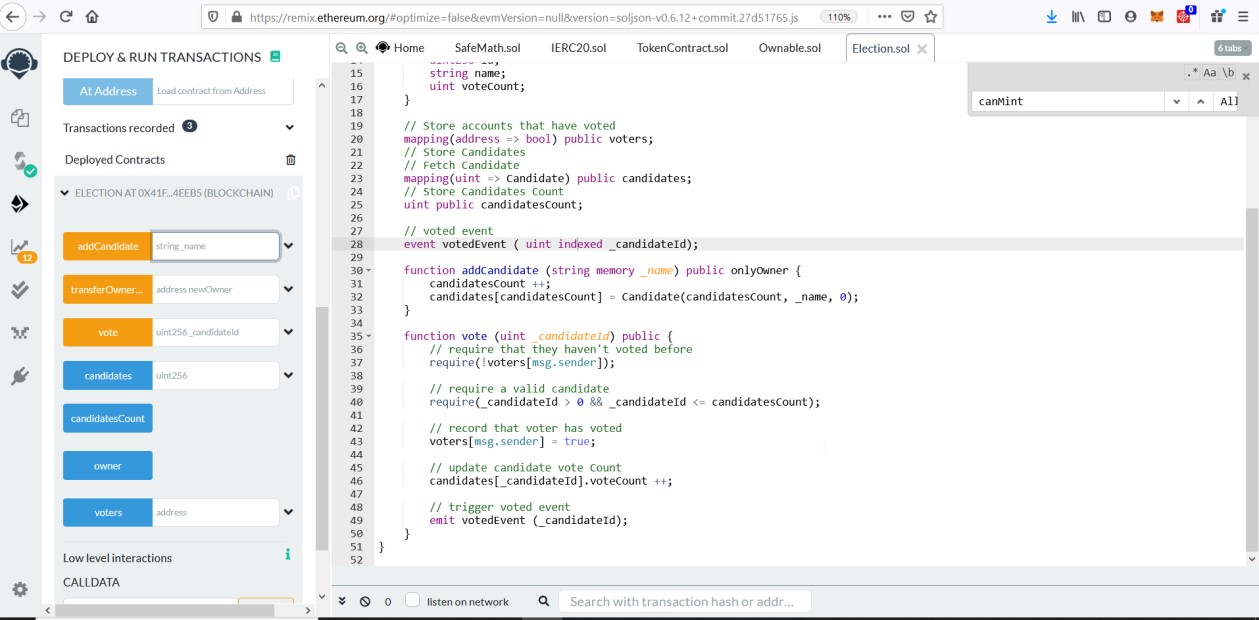


Frais variable en fonction du reseaux.

Quelle est l’adresse public de votre smart contract ?

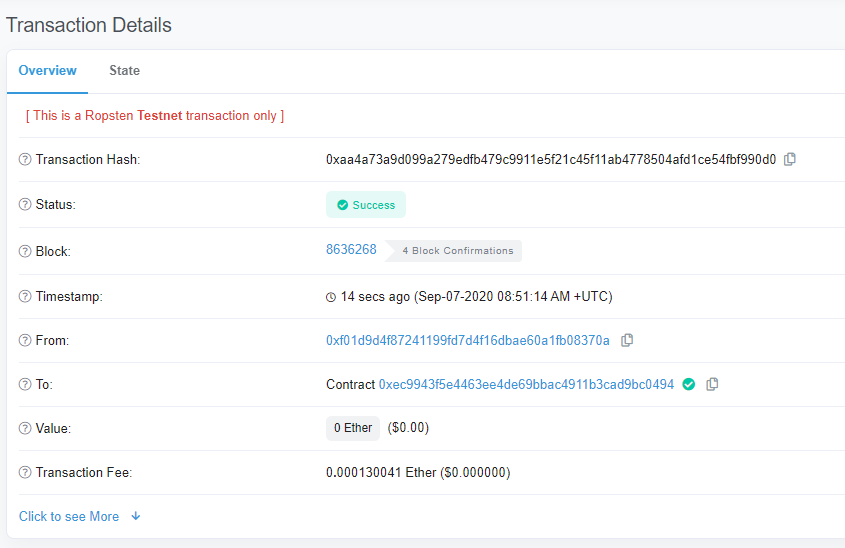
0xec9943f5e4463ee4de69bbac4911b3cad9bc0494

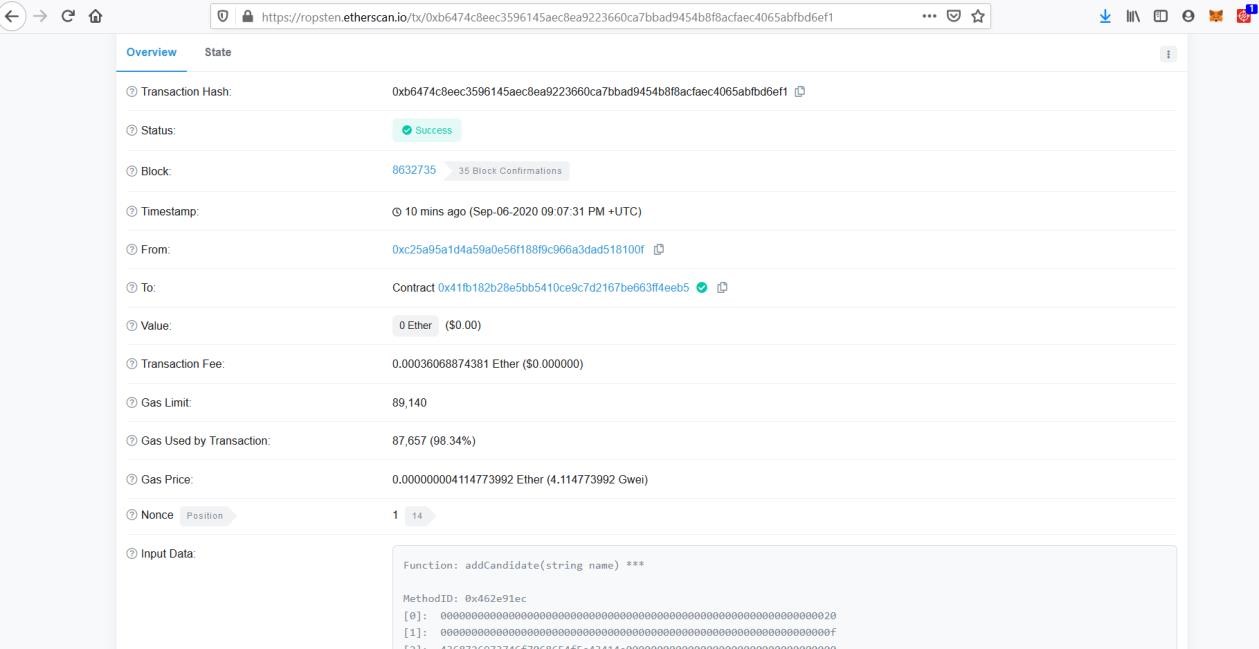
1. Interagissez avec votre smart contract après l’avoir déployé en ajoutant le nom du premier candidat qui sera votre « Nom de famille »



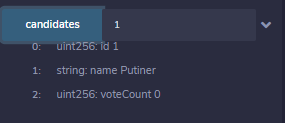
1. Générer la transaction ensuite l’ajout du premier candidat et fournissez les détails de la transaction

My Transaction :

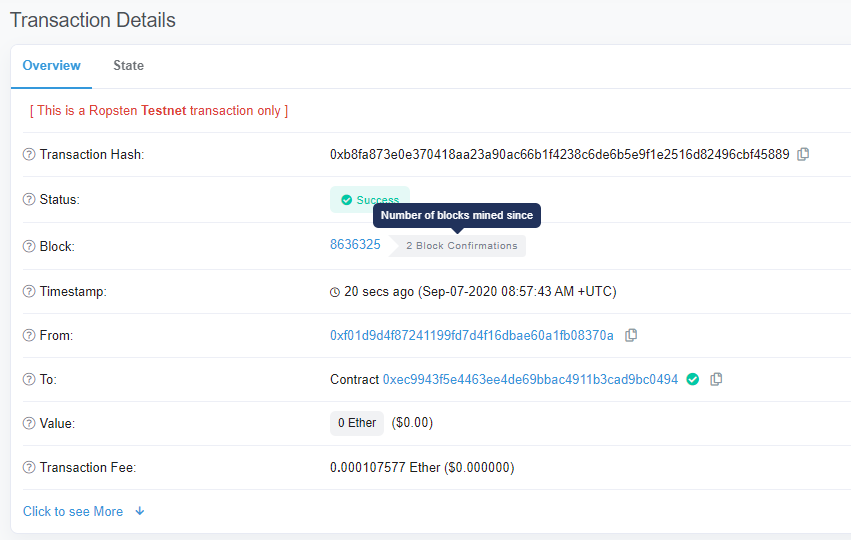




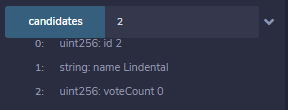
1. Consulter la valeur de votre CandidateID à l’aide de Remix et fournissez le détail.



1. Ajouter un second candidat de votre choix dans le smart contract et fournissez le détail de la transaction



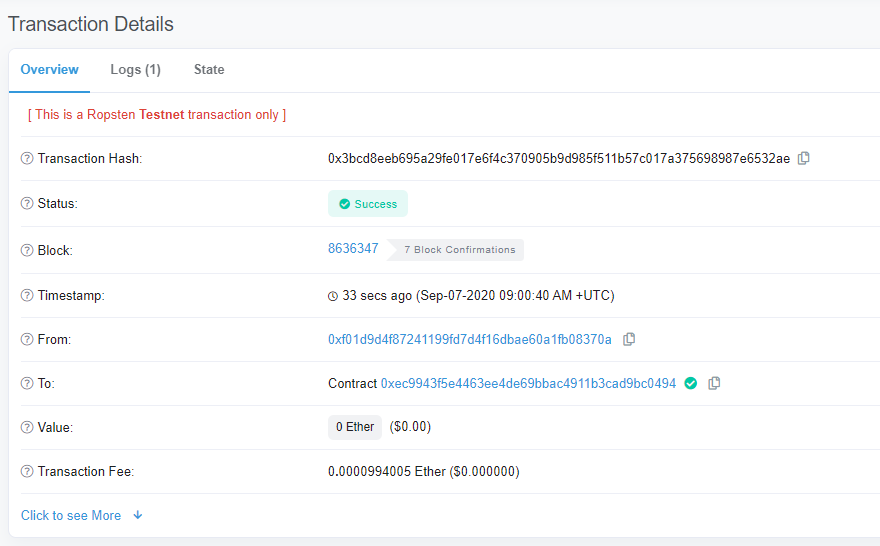
1. Consulter la valeur du second CandidateID à l’aide de Remix et fournissez le détail.



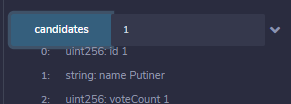
1. Fournissez l’adresse du propriétaire du contract

0xf01d9d4F87241199fD7d4F16dBAe60A1Fb08370a

1. Réaliser le premier vote pour l’un des candidats à travers Remix et fournissez le détail de la transaction



1. Vérifier que votre vote a été prise en compte en fournissant la donnée du nombre de vote pour votre candidat.



1. Demander à votre camarade proche de vous d’intéragir avec votre contrat et de voter pour l’un des deux candidats en lui fournissant l’adresse publique de votre smart contract.
2. Réaliser ensuite le transfert de la propriété à votre camarade en lui demandant son adresse publique.
3. A votre avis comment pourrions nous sécurisé l’appel de la fonction addCandidate afin que vous soyez le seul à pouvoir gérer les candidats ?

En ajoutant un verification du owner du smart Contract

1. Modifier le code afin de faire en sorte que vous soyez uniquement le seul à pouvoir ajouter un nouveau candidat.

<https://ropsten.etherscan.io/tx/0xbfbb301fe15fe2625fcc8604c23c93ab16a81d38247eae59f818fc24dbbbdae6>

ABI

[

{

"anonymous": false,

"inputs": [

{

"indexed": true,

"internalType": "address",

"name": "previousOwner",

"type": "address"

},

{

"indexed": true,

"internalType": "address",

"name": "newOwner",

"type": "address"

}

],

"name": "OwnershipTransferred",

"type": "event"

},

{

"anonymous": false,

"inputs": [

{

"indexed": true,

"internalType": "uint256",

"name": "\_candidateId",

"type": "uint256"

}

],

"name": "votedEvent",

"type": "event"

},

{

"inputs": [

{

"internalType": "string",

"name": "\_name",

"type": "string"

}

],

"name": "addCandidate",

"outputs": [],

"stateMutability": "nonpayable",

"type": "function"

},

{

"inputs": [

{

"internalType": "uint256",

"name": "",

"type": "uint256"

}

],

"name": "candidates",

"outputs": [

{

"internalType": "uint256",

"name": "id",

"type": "uint256"

},

{

"internalType": "string",

"name": "name",

"type": "string"

},

{

"internalType": "uint256",

"name": "voteCount",

"type": "uint256"

}

],

"stateMutability": "view",

"type": "function"

},

{

"inputs": [],

"name": "candidatesCount",

"outputs": [

{

"internalType": "uint256",

"name": "",

"type": "uint256"

}

],

"stateMutability": "view",

"type": "function"

},

{

"inputs": [],

"name": "owner",

"outputs": [

{

"internalType": "address",

"name": "",

"type": "address"

}

],

"stateMutability": "view",

"type": "function"

},

{

"inputs": [

{

"internalType": "address",

"name": "newOwner",

"type": "address"

}

],

"name": "transferOwnership",

"outputs": [],

"stateMutability": "nonpayable",

"type": "function"

},

{

"inputs": [

{

"internalType": "uint256",

"name": "\_candidateId",

"type": "uint256"

}

],

"name": "vote",

"outputs": [],

"stateMutability": "nonpayable",

"type": "function"

},

{

"inputs": [

{

"internalType": "address",

"name": "",

"type": "address"

}

],

"name": "voters",

"outputs": [

{

"internalType": "bool",

"name": "",

"type": "bool"

}

],

"stateMutability": "view",

"type": "function"

}

]

Bytecode

{

"linkReferences": {},

"object": "",

"opcodes": "PUSH1 0x80 PUSH1 0x40 MSTORE CALLVALUE DUP1 ISZERO PUSH2 0x10 JUMPI PUSH1 0x0 DUP1 REVERT JUMPDEST POP CALLER PUSH1 0x0 DUP1 PUSH2 0x100 EXP DUP2 SLOAD DUP2 PUSH20 0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF MUL NOT AND SWAP1 DUP4 PUSH20 0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF AND MUL OR SWAP1 SSTORE POP PUSH2 0x96C DUP1 PUSH2 0x60 PUSH1 0x0 CODECOPY PUSH1 0x0 RETURN INVALID PUSH1 0x80 PUSH1 0x40 MSTORE CALLVALUE DUP1 ISZERO PUSH2 0x10 JUMPI PUSH1 0x0 DUP1 REVERT JUMPDEST POP PUSH1 0x4 CALLDATASIZE LT PUSH2 0x7D JUMPI PUSH1 0x0 CALLDATALOAD PUSH1 0xE0 SHR DUP1 PUSH4 0x462E91EC GT PUSH2 0x5B JUMPI DUP1 PUSH4 0x462E91EC EQ PUSH2 0x183 JUMPI DUP1 PUSH4 0x8DA5CB5B EQ PUSH2 0x23E JUMPI DUP1 PUSH4 0xA3EC138D EQ PUSH2 0x272 JUMPI DUP1 PUSH4 0xF2FDE38B EQ PUSH2 0x2CC JUMPI PUSH2 0x7D JUMP JUMPDEST DUP1 PUSH4 0x121B93F EQ PUSH2 0x82 JUMPI DUP1 PUSH4 0x2D35A8A2 EQ PUSH2 0xB0 JUMPI DUP1 PUSH4 0x3477EE2E EQ PUSH2 0xCE JUMPI JUMPDEST PUSH1 0x0 DUP1 REVERT JUMPDEST PUSH2 0xAE PUSH1 0x4 DUP1 CALLDATASIZE SUB PUSH1 0x20 DUP2 LT ISZERO PUSH2 0x98 JUMPI PUSH1 0x0 DUP1 REVERT JUMPDEST DUP2 ADD SWAP1 DUP1 DUP1 CALLDATALOAD SWAP1 PUSH1 0x20 ADD SWAP1 SWAP3 SWAP2 SWAP1 POP POP POP PUSH2 0x310 JUMP JUMPDEST STOP JUMPDEST PUSH2 0xB8 PUSH2 0x42F JUMP JUMPDEST PUSH1 0x40 MLOAD DUP1 DUP3 DUP2 MSTORE PUSH1 0x20 ADD SWAP2 POP POP PUSH1 0x40 MLOAD DUP1 SWAP2 SUB SWAP1 RETURN JUMPDEST PUSH2 0xFA PUSH1 0x4 DUP1 CALLDATASIZE SUB PUSH1 0x20 DUP2 LT ISZERO PUSH2 0xE4 JUMPI PUSH1 0x0 DUP1 REVERT JUMPDEST DUP2 ADD SWAP1 DUP1 DUP1 CALLDATALOAD SWAP1 PUSH1 0x20 ADD SWAP1 SWAP3 SWAP2 SWAP1 POP POP POP PUSH2 0x435 JUMP JUMPDEST PUSH1 0x40 MLOAD DUP1 DUP5 DUP2 MSTORE PUSH1 0x20 ADD DUP1 PUSH1 0x20 ADD DUP4 DUP2 MSTORE PUSH1 0x20 ADD DUP3 DUP2 SUB DUP3 MSTORE DUP5 DUP2 DUP2 MLOAD DUP2 MSTORE PUSH1 0x20 ADD SWAP2 POP DUP1 MLOAD SWAP1 PUSH1 0x20 ADD SWAP1 DUP1 DUP4 DUP4 PUSH1 0x0 JUMPDEST DUP4 DUP2 LT ISZERO PUSH2 0x146 JUMPI DUP1 DUP3 ADD MLOAD DUP2 DUP5 ADD MSTORE PUSH1 0x20 DUP2 ADD SWAP1 POP PUSH2 0x12B JUMP JUMPDEST POP POP POP POP SWAP1 POP SWAP1 DUP2 ADD SWAP1 PUSH1 0x1F AND DUP1 ISZERO PUSH2 0x173 JUMPI DUP1 DUP3 SUB DUP1 MLOAD PUSH1 0x1 DUP4 PUSH1 0x20 SUB PUSH2 0x100 EXP SUB NOT AND DUP2 MSTORE PUSH1 0x20 ADD SWAP2 POP JUMPDEST POP SWAP5 POP POP POP POP POP PUSH1 0x40 MLOAD DUP1 SWAP2 SUB SWAP1 RETURN JUMPDEST PUSH2 0x23C PUSH1 0x4 DUP1 CALLDATASIZE SUB PUSH1 0x20 DUP2 LT ISZERO PUSH2 0x199 JUMPI PUSH1 0x0 DUP1 REVERT JUMPDEST DUP2 ADD SWAP1 DUP1 DUP1 CALLDATALOAD SWAP1 PUSH1 0x20 ADD SWAP1 PUSH5 0x100000000 DUP2 GT ISZERO PUSH2 0x1B6 JUMPI PUSH1 0x0 DUP1 REVERT JUMPDEST DUP3 ADD DUP4 PUSH1 0x20 DUP3 ADD GT ISZERO PUSH2 0x1C8 JUMPI PUSH1 0x0 DUP1 REVERT JUMPDEST DUP1 CALLDATALOAD SWAP1 PUSH1 0x20 ADD SWAP2 DUP5 PUSH1 0x1 DUP4 MUL DUP5 ADD GT PUSH5 0x100000000 DUP4 GT OR ISZERO PUSH2 0x1EA JUMPI PUSH1 0x0 DUP1 REVERT JUMPDEST SWAP2 SWAP1 DUP1 DUP1 PUSH1 0x1F ADD PUSH1 0x20 DUP1 SWAP2 DIV MUL PUSH1 0x20 ADD PUSH1 0x40 MLOAD SWAP1 DUP2 ADD PUSH1 0x40 MSTORE DUP1 SWAP4 SWAP3 SWAP2 SWAP1 DUP2 DUP2 MSTORE PUSH1 0x20 ADD DUP4 DUP4 DUP1 DUP3 DUP5 CALLDATACOPY PUSH1 0x0 DUP2 DUP5 ADD MSTORE PUSH1 0x1F NOT PUSH1 0x1F DUP3 ADD AND SWAP1 POP DUP1 DUP4 ADD SWAP3 POP POP POP POP POP POP POP SWAP2 SWAP3 SWAP2 SWAP3 SWAP1 POP POP POP PUSH2 0x4F7 JUMP JUMPDEST STOP JUMPDEST PUSH2 0x246 PUSH2 0x634 JUMP JUMPDEST PUSH1 0x40 MLOAD DUP1 DUP3 PUSH20 0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF AND DUP2 MSTORE PUSH1 0x20 ADD SWAP2 POP POP PUSH1 0x40 MLOAD DUP1 SWAP2 SUB SWAP1 RETURN JUMPDEST PUSH2 0x2B4 PUSH1 0x4 DUP1 CALLDATASIZE SUB PUSH1 0x20 DUP2 LT ISZERO PUSH2 0x288 JUMPI PUSH1 0x0 DUP1 REVERT JUMPDEST DUP2 ADD SWAP1 DUP1 DUP1 CALLDATALOAD PUSH20 0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF AND SWAP1 PUSH1 0x20 ADD SWAP1 SWAP3 SWAP2 SWAP1 POP POP POP PUSH2 0x658 JUMP JUMPDEST PUSH1 0x40 MLOAD DUP1 DUP3 ISZERO ISZERO DUP2 MSTORE PUSH1 0x20 ADD SWAP2 POP POP PUSH1 0x40 MLOAD DUP1 SWAP2 SUB SWAP1 RETURN JUMPDEST PUSH2 0x30E PUSH1 0x4 DUP1 CALLDATASIZE SUB PUSH1 0x20 DUP2 LT ISZERO PUSH2 0x2E2 JUMPI PUSH1 0x0 DUP1 REVERT JUMPDEST DUP2 ADD SWAP1 DUP1 DUP1 CALLDATALOAD PUSH20 0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF AND SWAP1 PUSH1 0x20 ADD SWAP1 SWAP3 SWAP2 SWAP1 POP POP POP PUSH2 0x678 JUMP JUMPDEST STOP JUMPDEST PUSH1 0x1 PUSH1 0x0 CALLER PUSH20 0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF AND PUSH20 0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF AND DUP2 MSTORE PUSH1 0x20 ADD SWAP1 DUP2 MSTORE PUSH1 0x20 ADD PUSH1 0x0 KECCAK256 PUSH1 0x0 SWAP1 SLOAD SWAP1 PUSH2 0x100 EXP SWAP1 DIV PUSH1 0xFF AND ISZERO PUSH2 0x367 JUMPI PUSH1 0x0 DUP1 REVERT JUMPDEST PUSH1 0x0 DUP2 GT DUP1 ISZERO PUSH2 0x379 JUMPI POP PUSH1 0x3 SLOAD DUP2 GT ISZERO JUMPDEST PUSH2 0x382 JUMPI PUSH1 0x0 DUP1 REVERT JUMPDEST PUSH1 0x1 DUP1 PUSH1 0x0 CALLER PUSH20 0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF AND PUSH20 0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF AND DUP2 MSTORE PUSH1 0x20 ADD SWAP1 DUP2 MSTORE PUSH1 0x20 ADD PUSH1 0x0 KECCAK256 PUSH1 0x0 PUSH2 0x100 EXP DUP2 SLOAD DUP2 PUSH1 0xFF MUL NOT AND SWAP1 DUP4 ISZERO ISZERO MUL OR SWAP1 SSTORE POP PUSH1 0x2 PUSH1 0x0 DUP3 DUP2 MSTORE PUSH1 0x20 ADD SWAP1 DUP2 MSTORE PUSH1 0x20 ADD PUSH1 0x0 KECCAK256 PUSH1 0x2 ADD PUSH1 0x0 DUP2 SLOAD DUP1 SWAP3 SWAP2 SWAP1 PUSH1 0x1 ADD SWAP2 SWAP1 POP SSTORE POP DUP1 PUSH32 0xFFF3C900D938D21D0990D786E819F29B8D05C1EF587B462B939609625B684B16 PUSH1 0x40 MLOAD PUSH1 0x40 MLOAD DUP1 SWAP2 SUB SWAP1 LOG2 POP JUMP JUMPDEST PUSH1 0x3 SLOAD DUP2 JUMP JUMPDEST PUSH1 0x2 PUSH1 0x20 MSTORE DUP1 PUSH1 0x0 MSTORE PUSH1 0x40 PUSH1 0x0 KECCAK256 PUSH1 0x0 SWAP2 POP SWAP1 POP DUP1 PUSH1 0x0 ADD SLOAD SWAP1 DUP1 PUSH1 0x1 ADD DUP1 SLOAD PUSH1 0x1 DUP2 PUSH1 0x1 AND ISZERO PUSH2 0x100 MUL SUB AND PUSH1 0x2 SWAP1 DIV DUP1 PUSH1 0x1F ADD PUSH1 0x20 DUP1 SWAP2 DIV MUL PUSH1 0x20 ADD PUSH1 0x40 MLOAD SWAP1 DUP2 ADD PUSH1 0x40 MSTORE DUP1 SWAP3 SWAP2 SWAP1 DUP2 DUP2 MSTORE PUSH1 0x20 ADD DUP3 DUP1 SLOAD PUSH1 0x1 DUP2 PUSH1 0x1 AND ISZERO PUSH2 0x100 MUL SUB AND PUSH1 0x2 SWAP1 DIV DUP1 ISZERO PUSH2 0x4E7 JUMPI DUP1 PUSH1 0x1F LT PUSH2 0x4BC JUMPI PUSH2 0x100 DUP1 DUP4 SLOAD DIV MUL DUP4 MSTORE SWAP2 PUSH1 0x20 ADD SWAP2 PUSH2 0x4E7 JUMP JUMPDEST DUP3 ADD SWAP2 SWAP1 PUSH1 0x0 MSTORE PUSH1 0x20 PUSH1 0x0 KECCAK256 SWAP1 JUMPDEST DUP2 SLOAD DUP2 MSTORE SWAP1 PUSH1 0x1 ADD SWAP1 PUSH1 0x20 ADD DUP1 DUP4 GT PUSH2 0x4CA JUMPI DUP3 SWAP1 SUB PUSH1 0x1F AND DUP3 ADD SWAP2 JUMPDEST POP POP POP POP POP SWAP1 DUP1 PUSH1 0x2 ADD SLOAD SWAP1 POP DUP4 JUMP JUMPDEST PUSH1 0x0 DUP1 SLOAD SWAP1 PUSH2 0x100 EXP SWAP1 DIV PUSH20 0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF AND PUSH20 0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF AND CALLER PUSH20 0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF AND EQ PUSH2 0x5B8 JUMPI PUSH1 0x40 MLOAD PUSH32 0x8C379A000000000000000000000000000000000000000000000000000000000 DUP2 MSTORE PUSH1 0x4 ADD DUP1 DUP1 PUSH1 0x20 ADD DUP3 DUP2 SUB DUP3 MSTORE PUSH1 0x18 DUP2 MSTORE PUSH1 0x20 ADD DUP1 PUSH32 0x4E6F7420617574686F72697A6564206F7065726174696F6E0000000000000000 DUP2 MSTORE POP PUSH1 0x20 ADD SWAP2 POP POP PUSH1 0x40 MLOAD DUP1 SWAP2 SUB SWAP1 REVERT JUMPDEST PUSH1 0x3 PUSH1 0x0 DUP2 SLOAD DUP1 SWAP3 SWAP2 SWAP1 PUSH1 0x1 ADD SWAP2 SWAP1 POP SSTORE POP PUSH1 0x40 MLOAD DUP1 PUSH1 0x60 ADD PUSH1 0x40 MSTORE DUP1 PUSH1 0x3 SLOAD DUP2 MSTORE PUSH1 0x20 ADD DUP3 DUP2 MSTORE PUSH1 0x20 ADD PUSH1 0x0 DUP2 MSTORE POP PUSH1 0x2 PUSH1 0x0 PUSH1 0x3 SLOAD DUP2 MSTORE PUSH1 0x20 ADD SWAP1 DUP2 MSTORE PUSH1 0x20 ADD PUSH1 0x0 KECCAK256 PUSH1 0x0 DUP3 ADD MLOAD DUP2 PUSH1 0x0 ADD SSTORE PUSH1 0x20 DUP3 ADD MLOAD DUP2 PUSH1 0x1 ADD SWAP1 DUP1 MLOAD SWAP1 PUSH1 0x20 ADD SWAP1 PUSH2 0x623 SWAP3 SWAP2 SWAP1 PUSH2 0x899 JUMP JUMPDEST POP PUSH1 0x40 DUP3 ADD MLOAD DUP2 PUSH1 0x2 ADD SSTORE SWAP1 POP POP POP JUMP JUMPDEST PUSH1 0x0 DUP1 SLOAD SWAP1 PUSH2 0x100 EXP SWAP1 DIV PUSH20 0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF AND DUP2 JUMP JUMPDEST PUSH1 0x1 PUSH1 0x20 MSTORE DUP1 PUSH1 0x0 MSTORE PUSH1 0x40 PUSH1 0x0 KECCAK256 PUSH1 0x0 SWAP2 POP SLOAD SWAP1 PUSH2 0x100 EXP SWAP1 DIV PUSH1 0xFF AND DUP2 JUMP JUMPDEST PUSH1 0x0 DUP1 SLOAD SWAP1 PUSH2 0x100 EXP SWAP1 DIV PUSH20 0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF AND PUSH20 0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF AND CALLER PUSH20 0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF AND EQ PUSH2 0x739 JUMPI PUSH1 0x40 MLOAD PUSH32 0x8C379A000000000000000000000000000000000000000000000000000000000 DUP2 MSTORE PUSH1 0x4 ADD DUP1 DUP1 PUSH1 0x20 ADD DUP3 DUP2 SUB DUP3 MSTORE PUSH1 0x18 DUP2 MSTORE PUSH1 0x20 ADD DUP1 PUSH32 0x4E6F7420617574686F72697A6564206F7065726174696F6E0000000000000000 DUP2 MSTORE POP PUSH1 0x20 ADD SWAP2 POP POP PUSH1 0x40 MLOAD DUP1 SWAP2 SUB SWAP1 REVERT JUMPDEST PUSH1 0x0 PUSH20 0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF AND DUP2 PUSH20 0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF AND EQ ISZERO PUSH2 0x7DC JUMPI PUSH1 0x40 MLOAD PUSH32 0x8C379A000000000000000000000000000000000000000000000000000000000 DUP2 MSTORE PUSH1 0x4 ADD DUP1 DUP1 PUSH1 0x20 ADD DUP3 DUP2 SUB DUP3 MSTORE PUSH1 0x19 DUP2 MSTORE PUSH1 0x20 ADD DUP1 PUSH32 0x416464726573732073686F756C646E2774206265207A65726F00000000000000 DUP2 MSTORE POP PUSH1 0x20 ADD SWAP2 POP POP PUSH1 0x40 MLOAD DUP1 SWAP2 SUB SWAP1 REVERT JUMPDEST DUP1 PUSH20 0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF AND PUSH1 0x0 DUP1 SLOAD SWAP1 PUSH2 0x100 EXP SWAP1 DIV PUSH20 0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF AND PUSH20 0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF AND PUSH32 0x8BE0079C531659141344CD1FD0A4F28419497F9722A3DAAFE3B4186F6B6457E0 PUSH1 0x40 MLOAD PUSH1 0x40 MLOAD DUP1 SWAP2 SUB SWAP1 LOG3 DUP1 PUSH1 0x0 DUP1 PUSH2 0x100 EXP DUP2 SLOAD DUP2 PUSH20 0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF MUL NOT AND SWAP1 DUP4 PUSH20 0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF AND MUL OR SWAP1 SSTORE POP POP JUMP JUMPDEST DUP3 DUP1 SLOAD PUSH1 0x1 DUP2 PUSH1 0x1 AND ISZERO PUSH2 0x100 MUL SUB AND PUSH1 0x2 SWAP1 DIV SWAP1 PUSH1 0x0 MSTORE PUSH1 0x20 PUSH1 0x0 KECCAK256 SWAP1 PUSH1 0x1F ADD PUSH1 0x20 SWAP1 DIV DUP2 ADD SWAP3 DUP3 PUSH1 0x1F LT PUSH2 0x8DA JUMPI DUP1 MLOAD PUSH1 0xFF NOT AND DUP4 DUP1 ADD OR DUP6 SSTORE PUSH2 0x908 JUMP JUMPDEST DUP3 DUP1 ADD PUSH1 0x1 ADD DUP6 SSTORE DUP3 ISZERO PUSH2 0x908 JUMPI SWAP2 DUP3 ADD JUMPDEST DUP3 DUP2 GT ISZERO PUSH2 0x907 JUMPI DUP3 MLOAD DUP3 SSTORE SWAP2 PUSH1 0x20 ADD SWAP2 SWAP1 PUSH1 0x1 ADD SWAP1 PUSH2 0x8EC JUMP JUMPDEST JUMPDEST POP SWAP1 POP PUSH2 0x915 SWAP2 SWAP1 PUSH2 0x919 JUMP JUMPDEST POP SWAP1 JUMP JUMPDEST JUMPDEST DUP1 DUP3 GT ISZERO PUSH2 0x932 JUMPI PUSH1 0x0 DUP2 PUSH1 0x0 SWAP1 SSTORE POP PUSH1 0x1 ADD PUSH2 0x91A JUMP JUMPDEST POP SWAP1 JUMP INVALID LOG2 PUSH5 0x6970667358 0x22 SLT KECCAK256 NOT 0xEF 0xCC LT 0x28 PUSH28 0xF826C0EF80FD1DA5C5066EB33590825F447B25D06EFE80F14F516473 PUSH16 0x6C634300060C00330000000000000000 ",

"sourceMap": "113:1166:0:-:0;;;;;;;;;;;;;579:10:1;571:5;;:18;;;;;;;;;;;;;;;;;;113:1166:0;;;;;;"

}