TP Blockchain

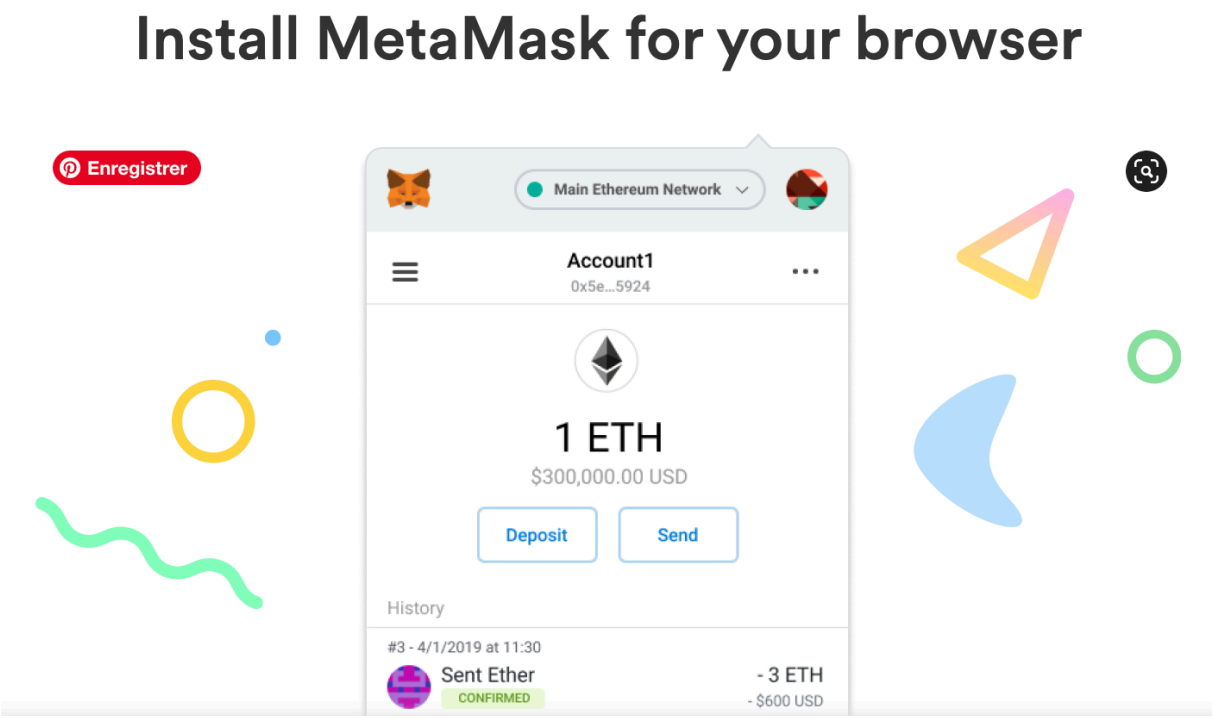
Développer, Deployer et Interagir avec un contrat intelligent sur Ethereum

8 SEPTEMBRE

ESME Sudria
A2IR
Charles COLIN

ESME sudria
PARIS | BORDEAUX | LILLE | LYON

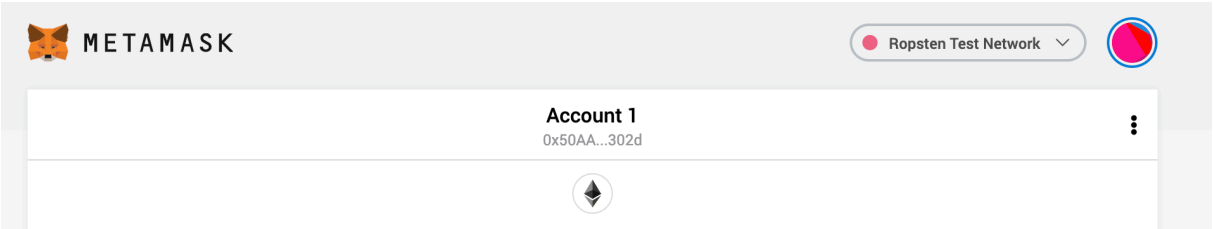
1.a) Naviguer sur le site et télécharger Metamask sur le site suivant :
https://metamask.io/



1.b) Suivez les étapes de génération du portefeuille en sauvegardant bien votre seed phrase :

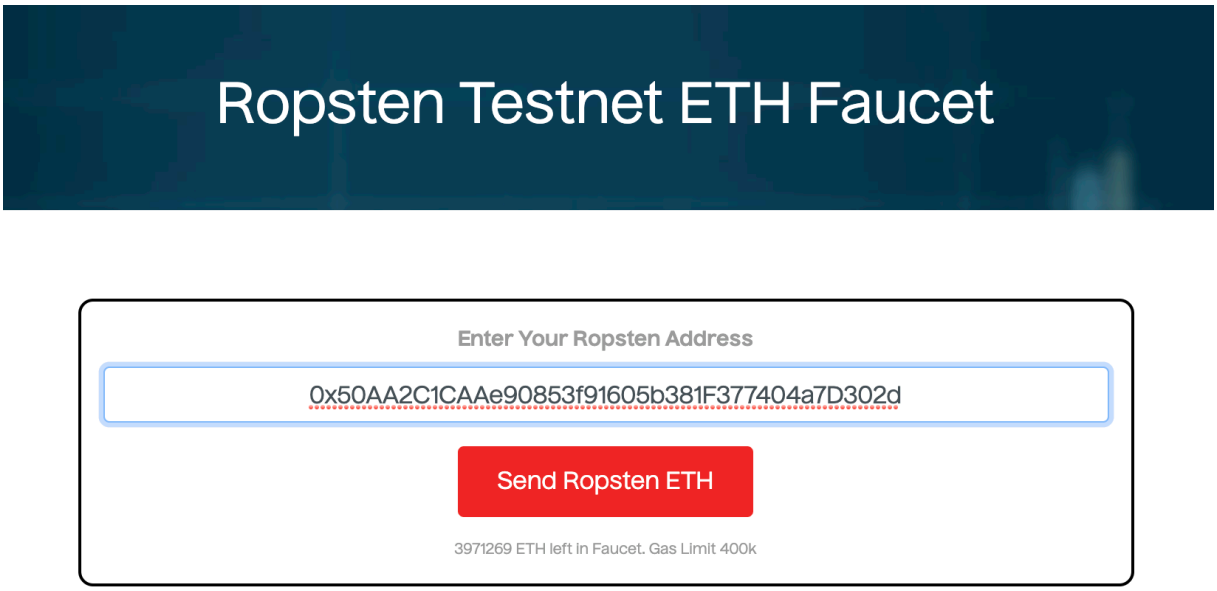
Seed phrase : “nasty defy armor pet spawn toddler sample reflect void wild expose machine”

1.c) Vous devrez ensuite avoir accès à votre premier compte « wallet » dont la clé publique commence par « 0x... »

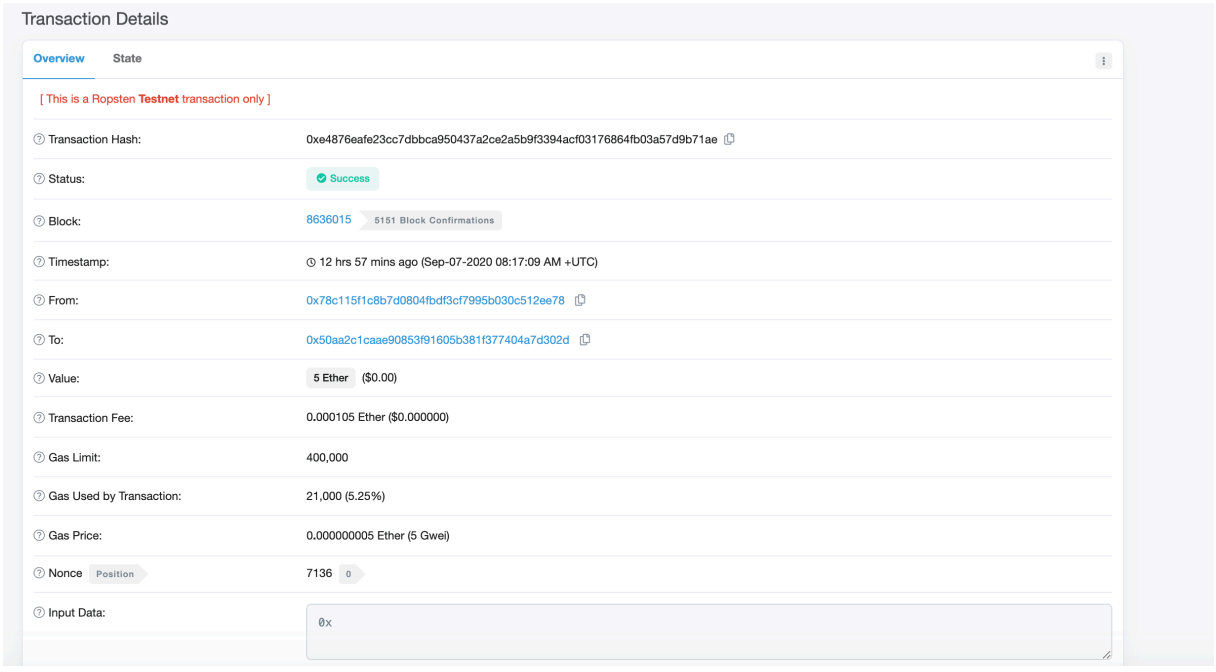


Clé publique : 0x50AA2C1CAAe90853f91605b381F377404a7D302d

1.d) 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.



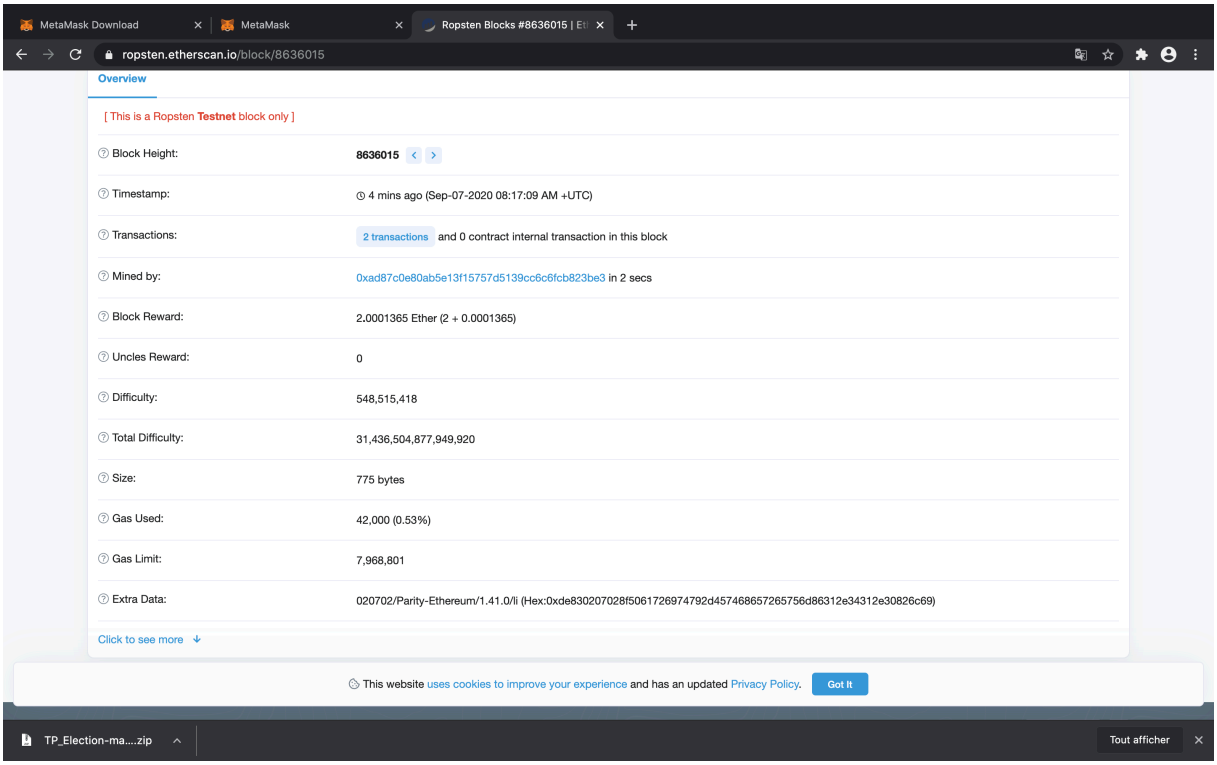
1.e) Consulter la transaction générée vers votre compte et prenez en compte les détails de cette dernière. Fournissez également les détails de la transaction



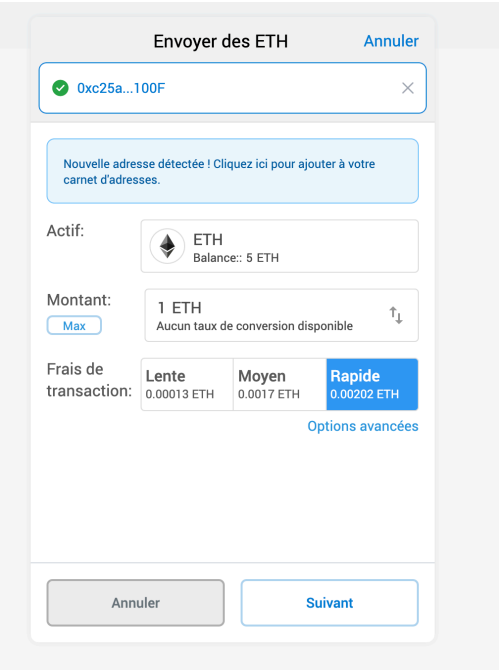
Lien :
https://ropsten.etherscan.io/tx/0xe4876eafe23cc7dbbca950437a2ce2a5b9f3394acf03176864fb03a57d9b71ae

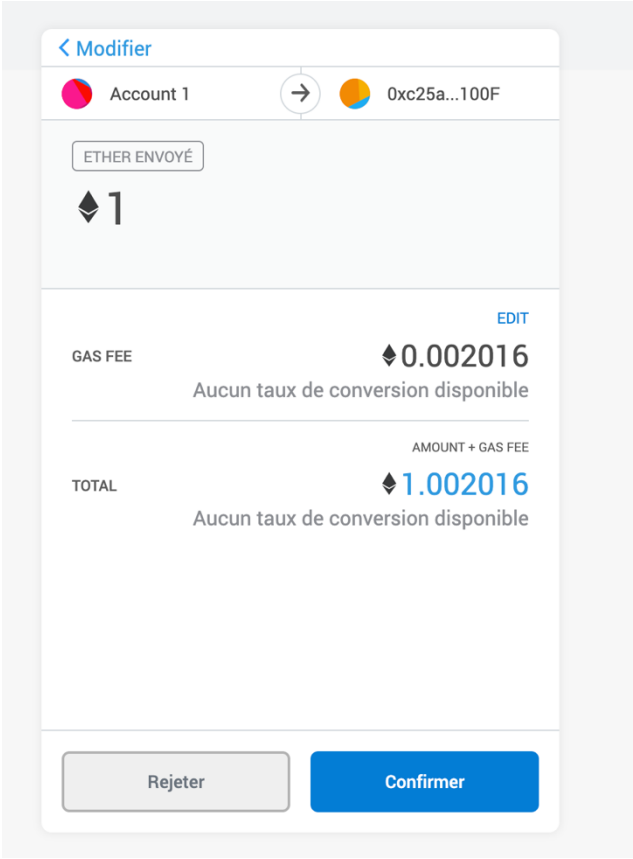
1.f Consulter ensuite le numéro de Block de votre transaction. Fournissez également les détails de la transaction.

Block : 8636015
Lien : https://ropsten.etherscan.io/block/8636015



1.g) Générer votre première transaction Ethereum sur le réseau Rospten envoyant 1 ETH à l'adresse suivante « 0xc25a95A1D4a59A0E56f188f9C966A3Dad518100F ».

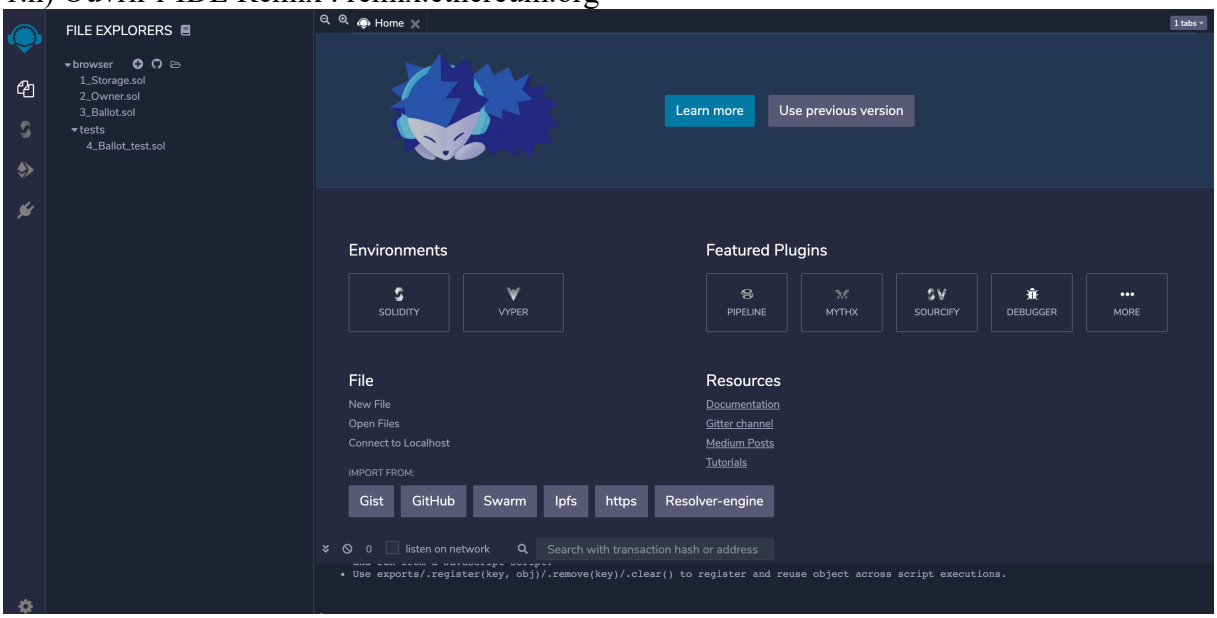




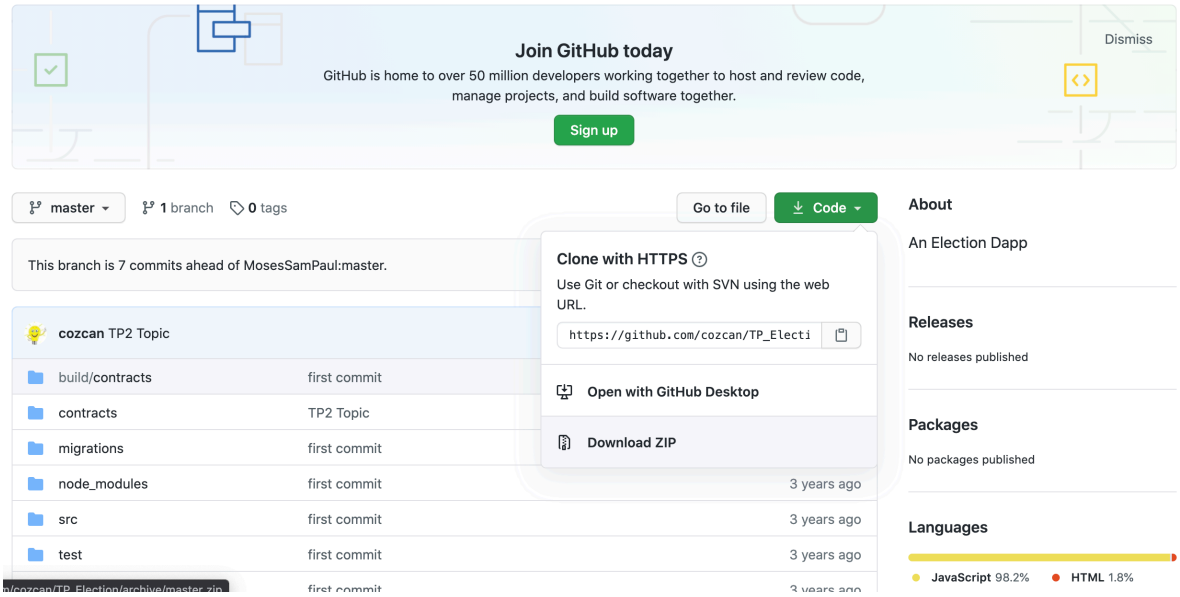
Lien :

https://ropsten.etherscan.io/tx/0x04920bea20fee9b10d2377e7f2426d7311d0ae47fabf65080dc455d9230c3f83

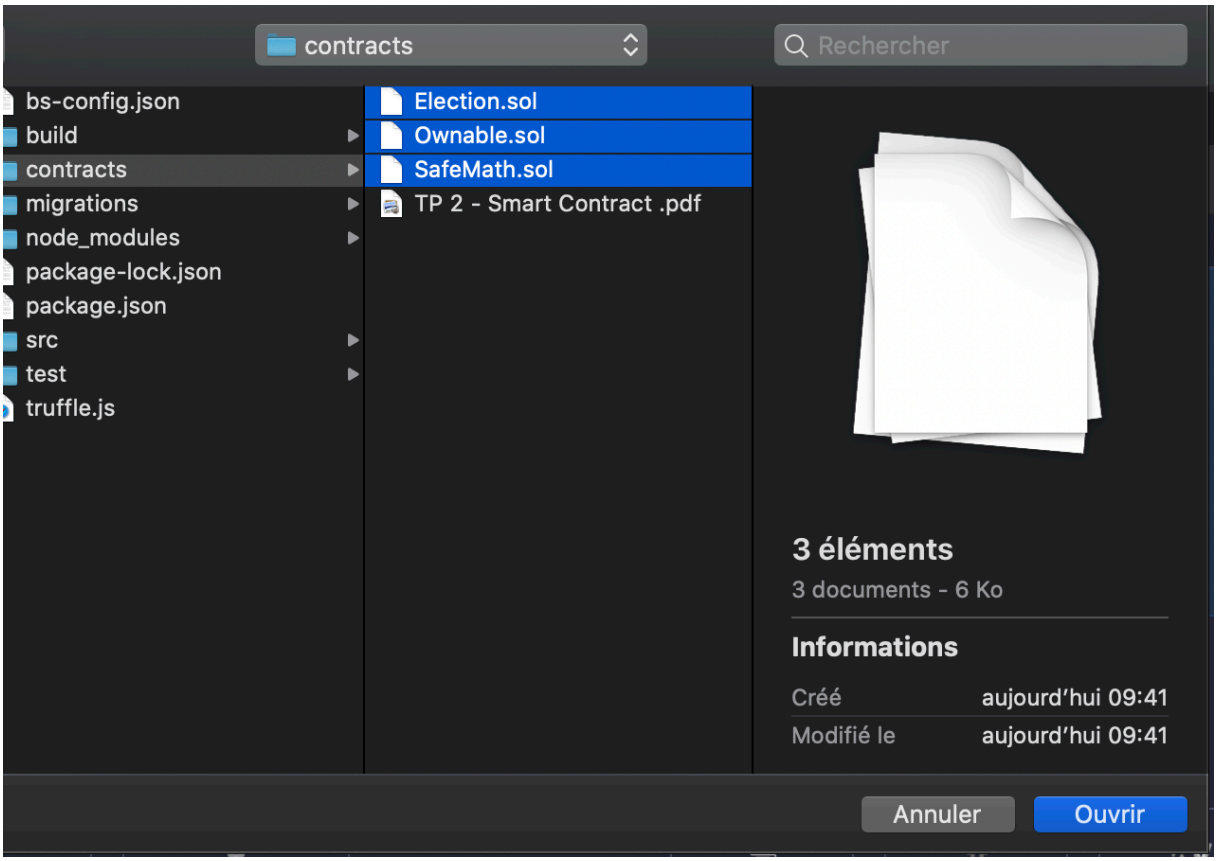
1.h) Ouvrir l'IDE Remix : remix.ethereum.org



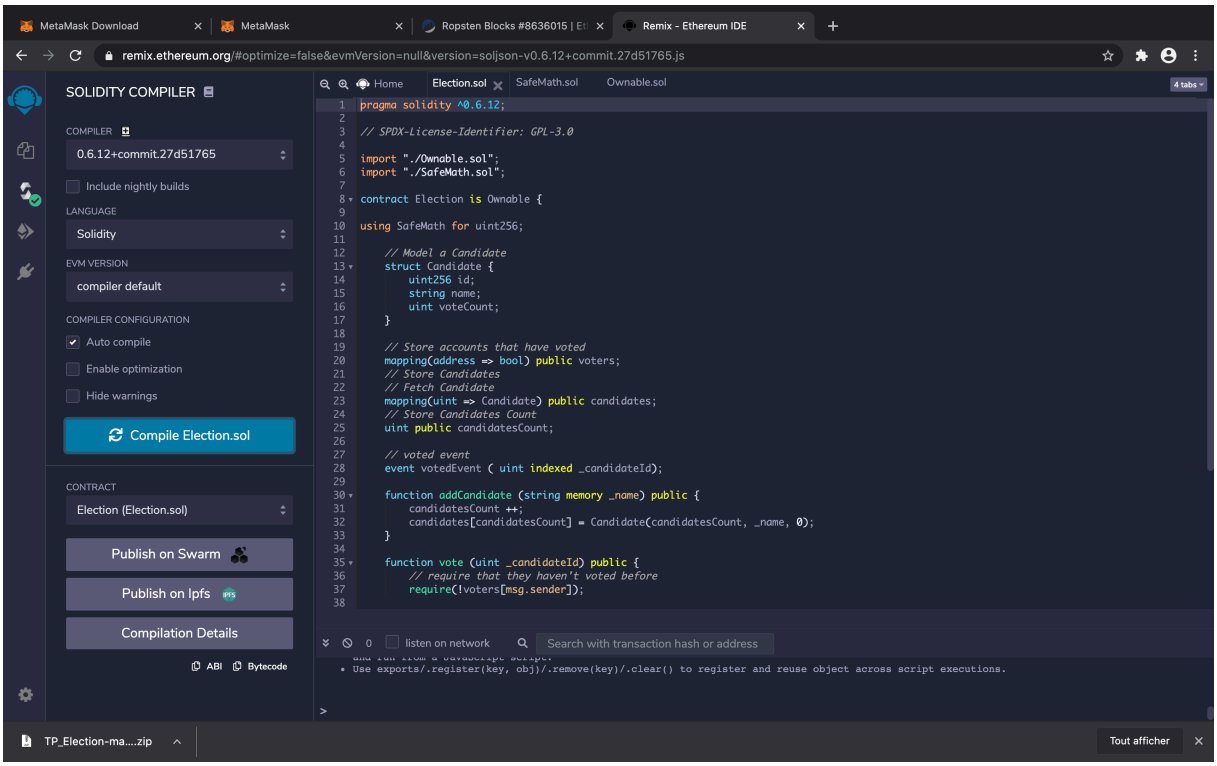
1.i) Récupérer le code source de votre premier smart contract : https://github.com/cozcan/TP_Election



1.j) Ajouter l'ensemble des fichiers Solidity sur votre environnement Remix.



1.k) 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":
"60806040523480156100105760008fd5b50336000806101000a81548173ffffffffffffffffffffff
ffffffffffffffff021916908373ffffffffffffffffffffffffffffffffffffffff160217905550610ab8061006
06000396000f3fe6080604052348015610010576000fd5b506004361061007d5760003560e
01c8063462e91ec1161005b578063462e91ec146101835780638da5cb5b1461023e578063a3ec
138d14610272578063f2fde38b146102cc5761007d565b80630121b93f146100825780632d35a
8a2146100b05780633477ee2e146100ce575b600080fd5b6100ae600480360360208110156100
09857600080fd5b810190808035906020019092919050505061031056 5b005b6100b861042f5
65b604051808281526020019150506040518091039 0f35b6100fa600480360360208110156100
0e457600080fd5b810190808035906020019092919050505061043556 5b6040518084815260
200180602001838152602001828103825284818151815260200191508051906020019080838
360005b838110156101465780820151818401526020810190506101 2b565b50505050905090
810190601f168015610173578082038051600183602003610100 0a031916815260200191505
b509450505050506040518091039 0f35b61023c600480360360208110156101995760008 0fd5
b810190808035906020019064010000000081111561 01b657600080fd5b8201836020820111
156101c857600080fd5b803590602001918460018302840111640100000000831117156101ea
57600080fd5b91908080601f016020809104026020016040519081016040528093929190818 1
526020018383808284376000818401526 01f19601f8201169050808301925050505050505091
92919290505050610 4f7565b005b610246610573565b604051808273ffffffffffffffffffffffffffffff
ffffffffff1681526020019150506040518091039 0f35b6102b46004803603602081101561028 8
```

57600080fd5b81019080803573ffffffffffffffffffffffffffffffffffffffff169060200190929190505050
0610597565b604051808215158152602001915050604051809103 90f35b61030e6004803603
60208110156102e257600080fd5b81019080803573ffffffffffffffffffffffffffffffffffffffff1690602
00190929190505050506105b7565b005b600160003373ffffffffffffffffffffffffffffffffffffffff1673ff
ffffffffffffffffffffffffffffffffffffffff168152602001908152602001600020600090549061010 00a90
0460ff16156103675760008 0fd5b60008111801561037957506003548111155b610382576000
80fd5b60018060003373ffffffffffffffffffffffffffffffffffffffff1673ffffffffffffffffffffffffffffffffffffffff
fff168152602001908152602001600020600061010 00a8154816 0ff021916908 3151502179055
506002600082815260200190815260200160002060020160008154809291906001019190505
550807ffff3c900d938d21d0990d786e819f29b8d05c1ef587b462b939609625b684b166040516
0405180910390a250565b60035481565b600260205280600526040600020600091509050 80
60000154908060010180546001816001161561010002031660029004806 01f0160208091040
26020016040519081016040528092919081815260200182805460018160011615610100020 3
166002900480156104e75780601f106104bc576101008083540402835291602001916104e756
5b820191906000526020600020905b81548152906001019060200180831161 04ca578290036
01f168201915b5050505050908060020154905083565b600360008154809291906001019190
505550604051806060016040528060035481526020018281526020016000815250600260006
003548152602001908152602001600020600082015181600001556020820151816001019080
519060200190610562929190610 7d8565b506040820151816002015590505050565b6000805
4906101000a900473ffffffffffffffffffffffffffffffffffffffff1681565b600160205280600052604060
0020600091505490610 1000a900460ff1681565b6000805490610 1000a900473ffffffffffffffffff
ffffffffffffffffffff1673ffffffffffffffffffffffffffffffffffffffff163373ffffffffffffffffffffffffffffffffffffffff
ffff161461067857604051 7f08c379a0000000000000000000000000000000000000000000000000
0000000000815260040180806020018281038252601881526020018 07f4e6f7420617574686
f72697a6564206f7065726174696f6e0000000000000000815250602001915050604051809 10
390fd5b600073ffffffffffffffffffffffffffffffffffffffff168173ffffffffffffffffffffffffffffffffffffffff161
41561071b576040517f08c379a0000000000000000000000000000000000000000000000000000
0000008152600401808060200182810382526019815260200180 7f41646472657373207368
6f756c646e2774206265207a65726f0000000000000081525060200191505060405180910390
fd5b8073ffffffffffffffffffffffffffffffffffffffff166000805490610 1000a900473ffffffffffffffffffffffff
ffffffffffffffff1673ffffffffffffffffffffffffffffffffffffffff167f8be0079c531659141344cd1fd0a4f28
419497f9722a3daafe3b4186f6b6457e060405160405180910390a3806000806101000a815481
73ffffffffffffffffffffffffffffffffffffffff02191690837 3ffffffffffffffffffffffffffffffffffffffff16021790
555050565b828054600181600116156101000203166002900490600052602060002090601f0
160209004810192826 01f106108 1957805160ff191683800117855561084 7565b82800160010
185558215610847579182015b828111156108465782518255916020019190600 1019061082b
565b5b509050610854919061085856 5b5090565b5b808211156108715760008160009055506
00101610859565b509056fea2646970667358221220f7a57d6c373310ecf2f73db1c19ac3e00b8
66f0f324542bdc0895b85109f303964736f6c634300060c0033",
"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

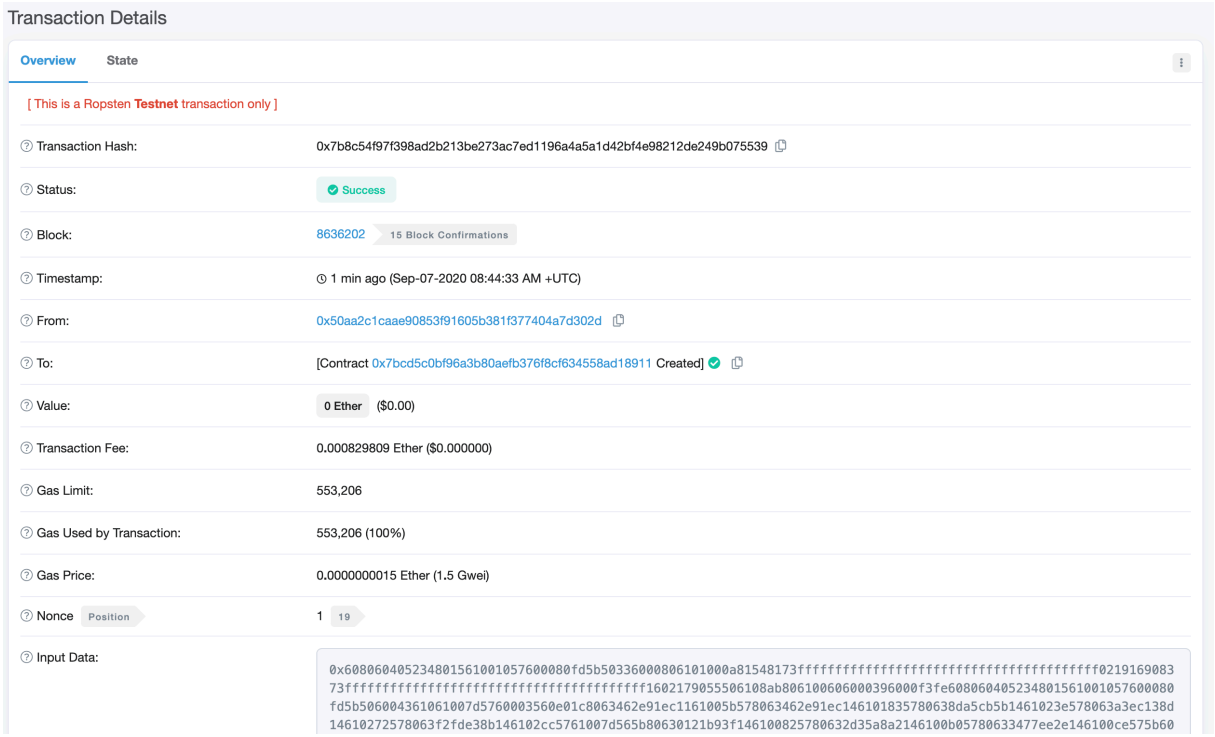
PUSH4 0xA3EC138D EQ PUSH2 0x272 JUMPI DUP1 PUSH4 0xF2FDE38B EQ PUSH2 0x2CC JUMPI PUSH2 0x7D JUMP JUMPDEST DUP1 PUSH4 0x121B93F EQ PUSH2 0x82 JUMPI DUP1 PUSH4 0x2D35A8A2 EQ PUSH2 0xB0 JUMPI DUP1 PUSH4 0x3477EE2E EQ PUSH2 0xCE JUMPI JUMPDEST PUSH1 0x0 DUP1 REVERT JUMPDEST PUSH2 0xAE PUSH1 0x4 DUP1 CALLDATASIZE 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 0x8C379A0000000000000000000000000000000000000000000000000000000000000000 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 0x8C379A0000000000000000000000000000000000000000000000000000000000000000 DUP2 MSTORE PUSH1 0x4 ADD DUP1 DUP1 PUSH1 0x20 ADD DUP3 DUP2 SUB DUP3 MSTORE PUSH1 0x19 DUP2 MSTORE PUSH1 0x20 ADD DUP1 PUSH32 0x4164647265737320686F756C646E2774206265207A65726F00000000000000 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 0xF7 0xA5 PUSH30 0x6C373310ECF2F73DB1C19AC3E00B866F0F324542BDC0895B85109F303964 PUSH20 0x6F6C634300060C0033",

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

}

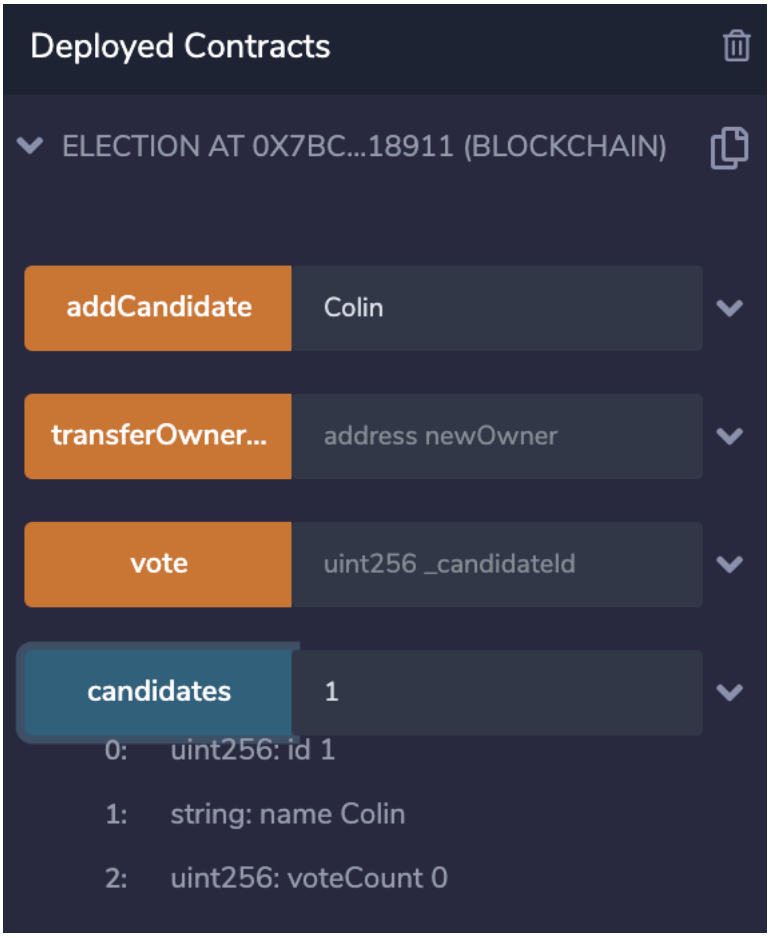


1.m) Justifier les frais de transactions « Transaction fees » que vous avez payés. Sont elles identiques à celle de ma transaction ? Quelle est l'adresse public de votre smart contract ?

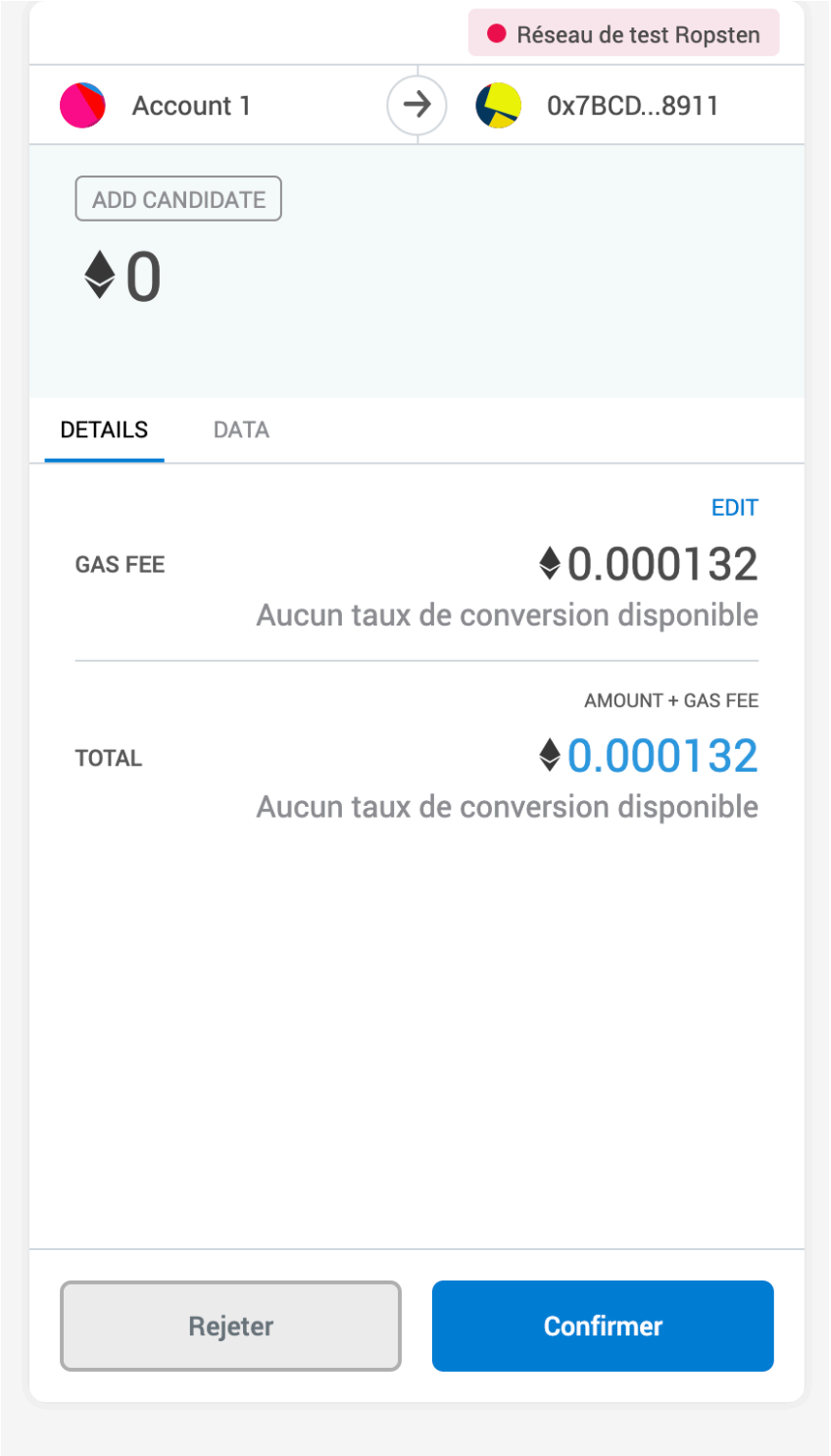
Les frais de transcations servent à rémunérer la proof of work du mineur.
Les frais de transactions varient en fonction du réseau.

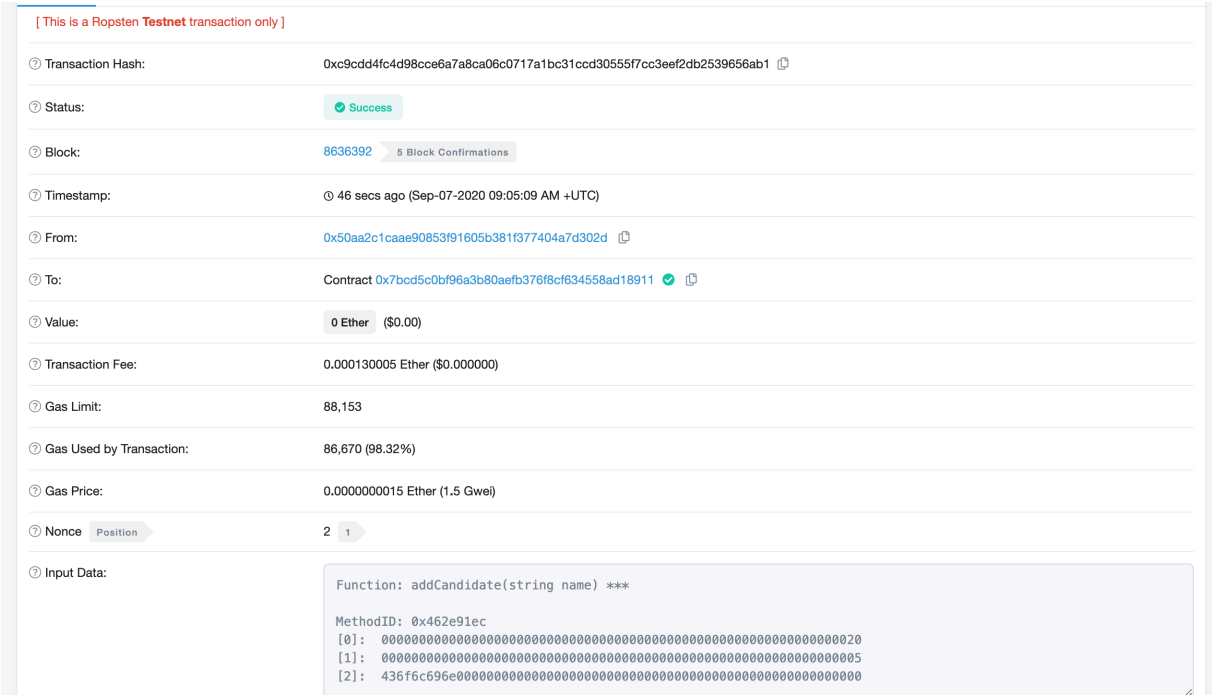
Addresse du contrat : 0x7bcd5c0bf96a3b80aefb376f8cf634558ad18911

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



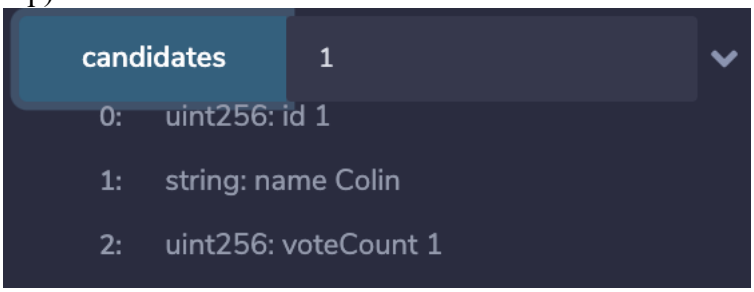
1.o) Générer la transaction ensuite l'ajout du premier candidat et fournissez les détails de la transaction



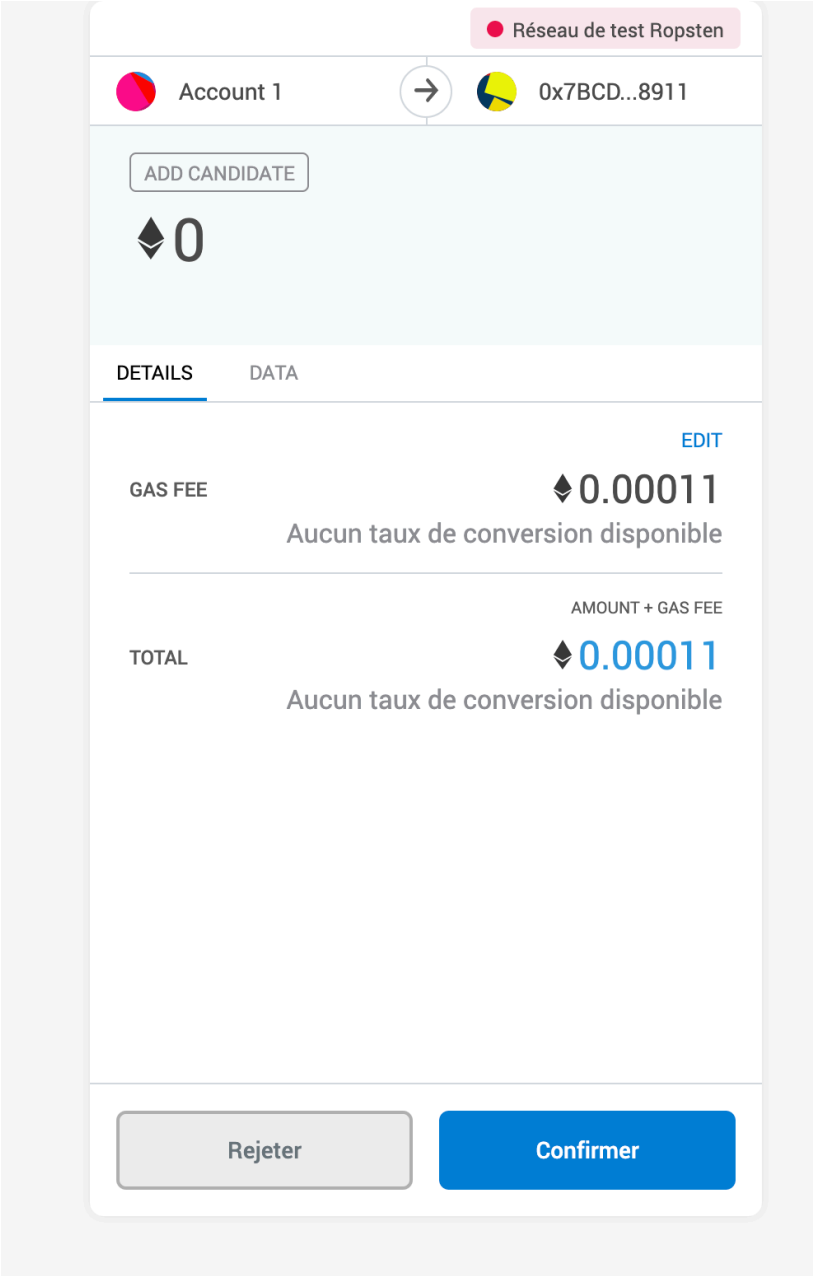


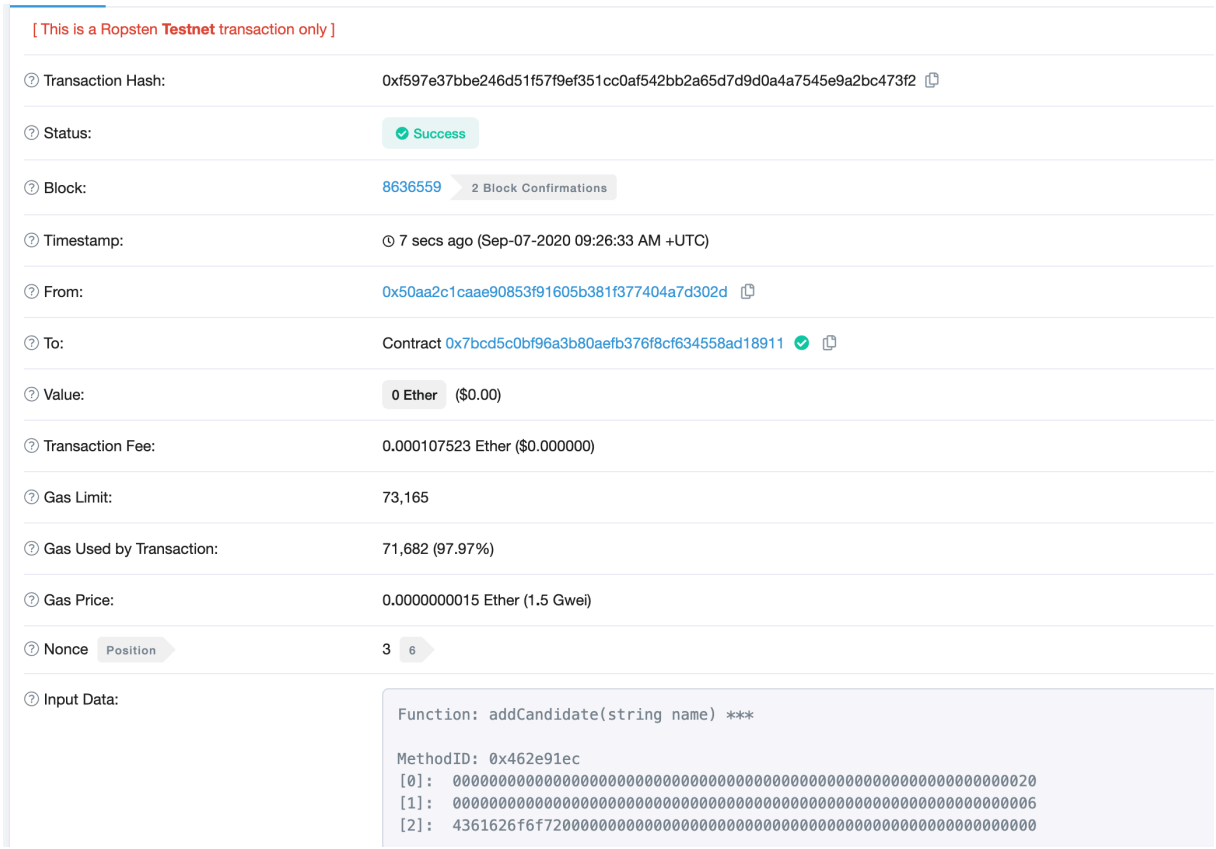
Lien : https://ropsten.etherscan.io/address/0x7bcd5c0bf96a3b80aefb376f8cf634558ad18911

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



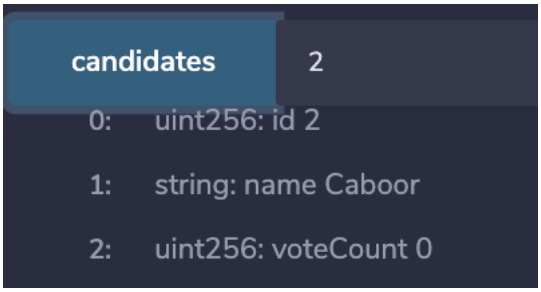
1.q) Ajouter un second candidat de votre choix dans le smart contract et fournissez le détail de la transaction


Réseau de test Ropsten
Account 1
0x7BCD...8911
ADD CANDIDATE
0
DETAILS
DATA
EDIT
GAS FEE
0.00011
Aucun taux de conversion disponible
AMOUNT + GAS FEE
TOTAL
0.00011
Aucun taux de conversion disponible
Rejeter
Confirmer



Lien :
https://ropsten.etherscan.io/tx/0xf597e37bbe246d51f57f9ef351cc0af542bb2a65d7d9d0a4a7545e9a2bc473f2

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

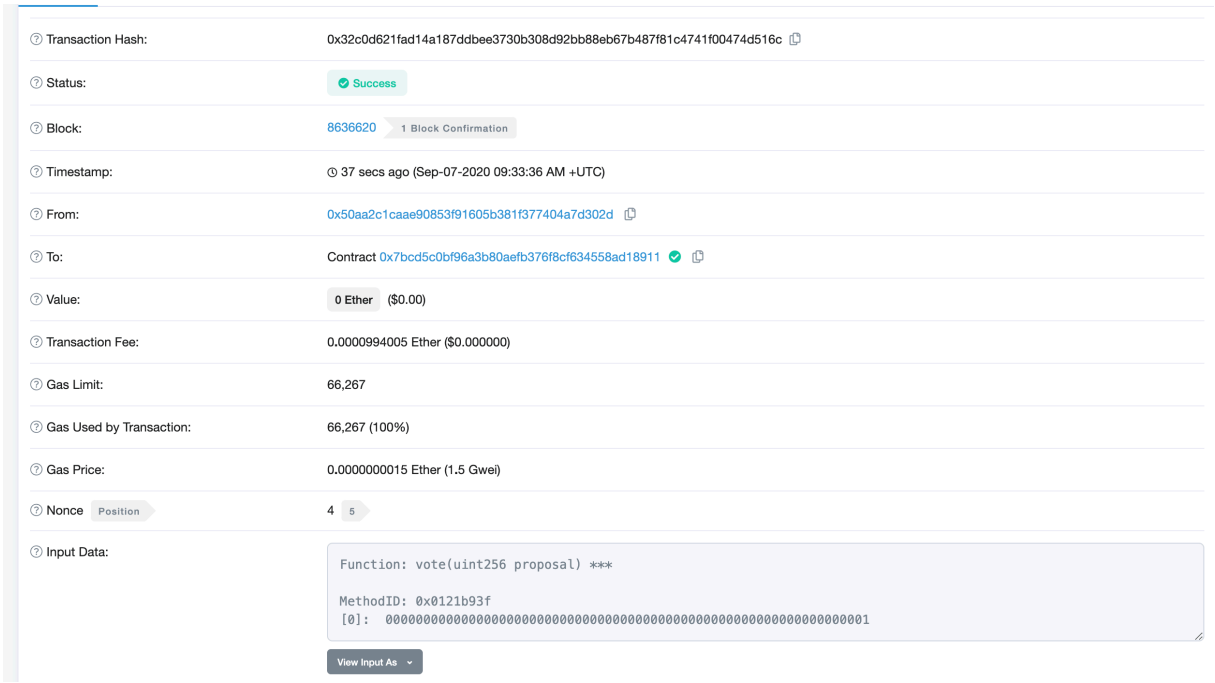


1.s) Fournissez l'adresse du propriétaire du contract

Contract creator :

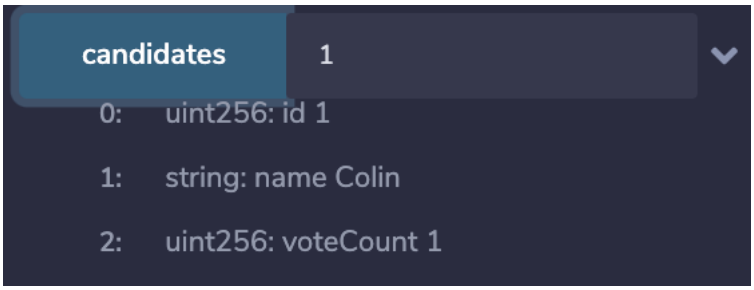
0x50AA2C1CAAe90853f91605b381F377404a7D302d

1.t) Réaliser le premier vote pour l'un des candidats à travers Remix et fournissez le détail de la transaction

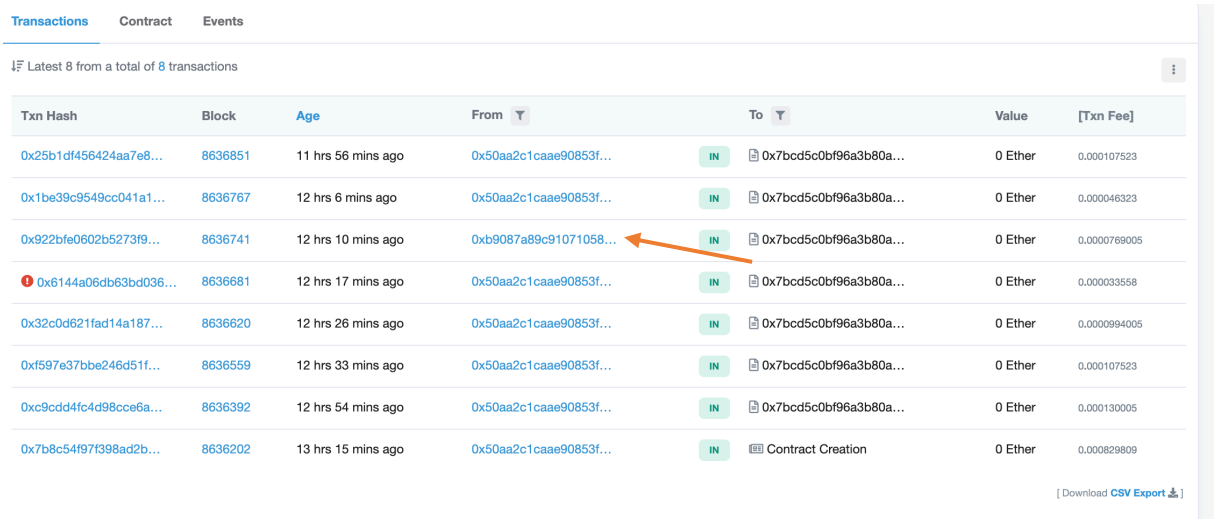


Lien : https://ropsten.etherscan.io/tx/0x32c0d621fad14a187ddbee3730b308d92bb88eb67b487f81c4741f00474d516c

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



1.v) 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.

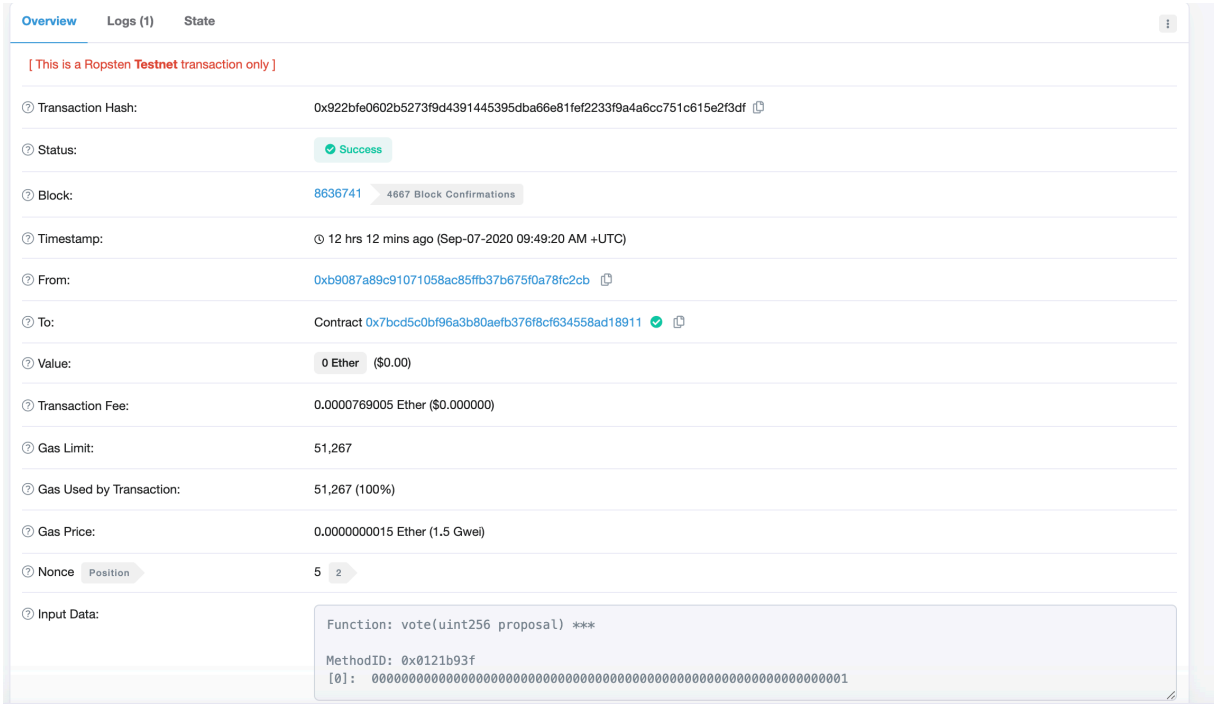


Transactions | Contract | Events

Latest 8 from a total of 8 transactions

Txn Hash	Block	Age	From		To	Value	[Txn Fee]
0x25b1df456424aa7e8…	8636851	11 hrs 56 mins ago	0x50aa2c1caae90853f…	IN	0x7bcd5c0bf96a3b80a…	0 Ether	0.000107523
0x1be39c9549cc041a1…	8636767	12 hrs 6 mins ago	0x50aa2c1caae90853f…	IN	0x7bcd5c0bf96a3b80a…	0 Ether	0.000046323
0x922bfe0602b5273f9…	8636741	12 hrs 10 mins ago	0xb9087a89c91071058…	IN	0x7bcd5c0bf96a3b80a…	0 Ether	0.0000769005
0x6144a06db63bd036…	8636681	12 hrs 17 mins ago	0x50aa2c1caae90853f…	IN	0x7bcd5c0bf96a3b80a…	0 Ether	0.000033558
0x32c0d621fad14a187…	8636620	12 hrs 26 mins ago	0x50aa2c1caae90853f…	IN	0x7bcd5c0bf96a3b80a…	0 Ether	0.0000994005
0xf597e37bbe246d51f…	8636559	12 hrs 33 mins ago	0x50aa2c1caae90853f…	IN	0x7bcd5c0bf96a3b80a…	0 Ether	0.000107523
0xc9cdd4fc4d98cce6a…	8636392	12 hrs 54 mins ago	0x50aa2c1caae90853f…	IN	0x7bcd5c0bf96a3b80a…	0 Ether	0.000130005
0x7b8c54f97f398ad2b…	8636202	13 hrs 15 mins ago	0x50aa2c1caae90853f…	IN	Contract Creation	0 Ether	0.000829809

[Download CSV Export]



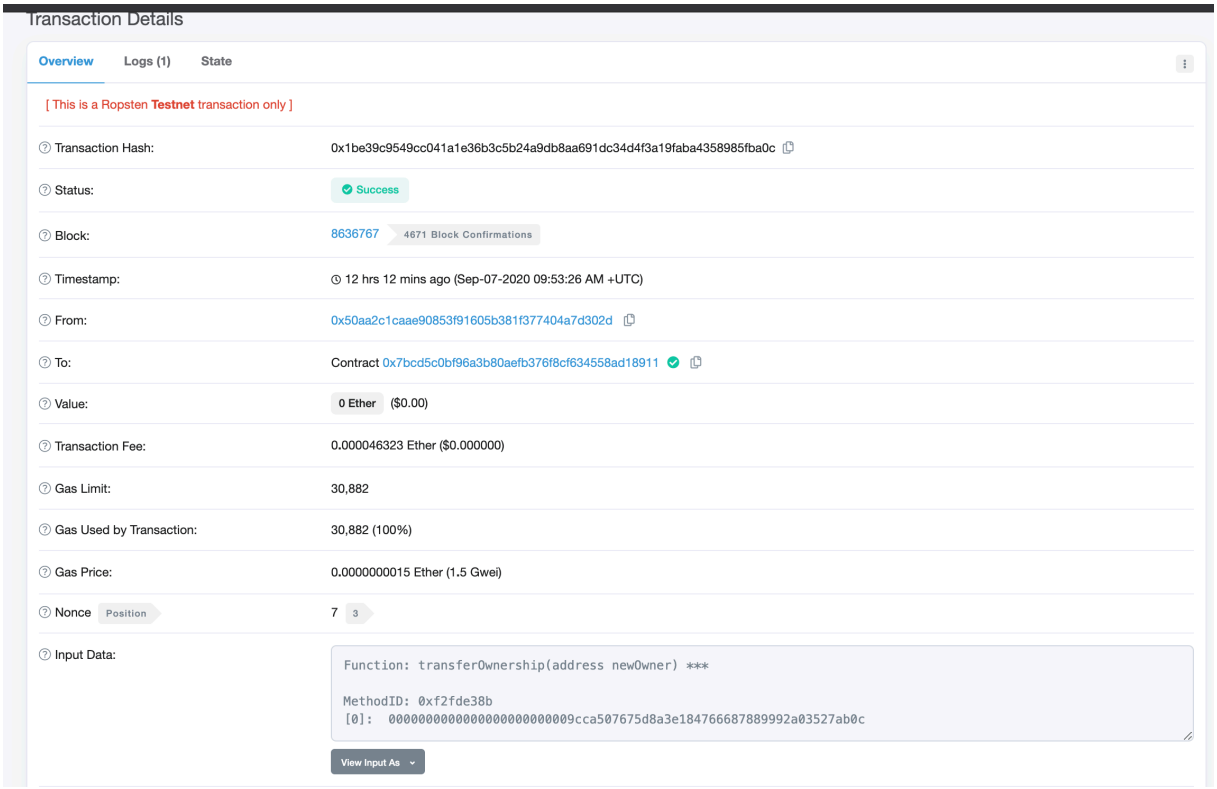
Overview | Logs (1) | State

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

Transaction Hash:	0x922bfe0602b5273f9d4391445395dba66e81fef2233f9a4a6cc751c615e2f3df
Status:	Success
Block:	8636741 4667 Block Confirmations
Timestamp:	12 hrs 12 mins ago (Sep-07-2020 09:49:20 AM +UTC)
From:	0xb9087a89c91071058ac85ffb37b675f0a78fc2cb
To:	Contract 0x7bcd5c0bf96a3b80aefb376f8cf634558ad18911
Value:	0 Ether ($0.00)
Transaction Fee:	0.0000769005 Ether ($0.000000)
Gas Limit:	51,267
Gas Used by Transaction:	51,267 (100%)
Gas Price:	0.0000000015 Ether (1.5 Gwei)
Nonce Position	5 2
Input Data:	Function: vote(uint256 proposal) *** MethodID: 0x0121b93f [0]: 0000000000000000000000000000000000000000000000000000000000000001

Lien :
https://ropsten.etherscan.io/tx/0x922bfe0602b5273f9d4391445395dba66e81fef2233f9a4a6cc751c615e2f3df

1.w) Réaliser ensuite le transfert de la propriété à votre camarade en lui demandant son adresse publique.



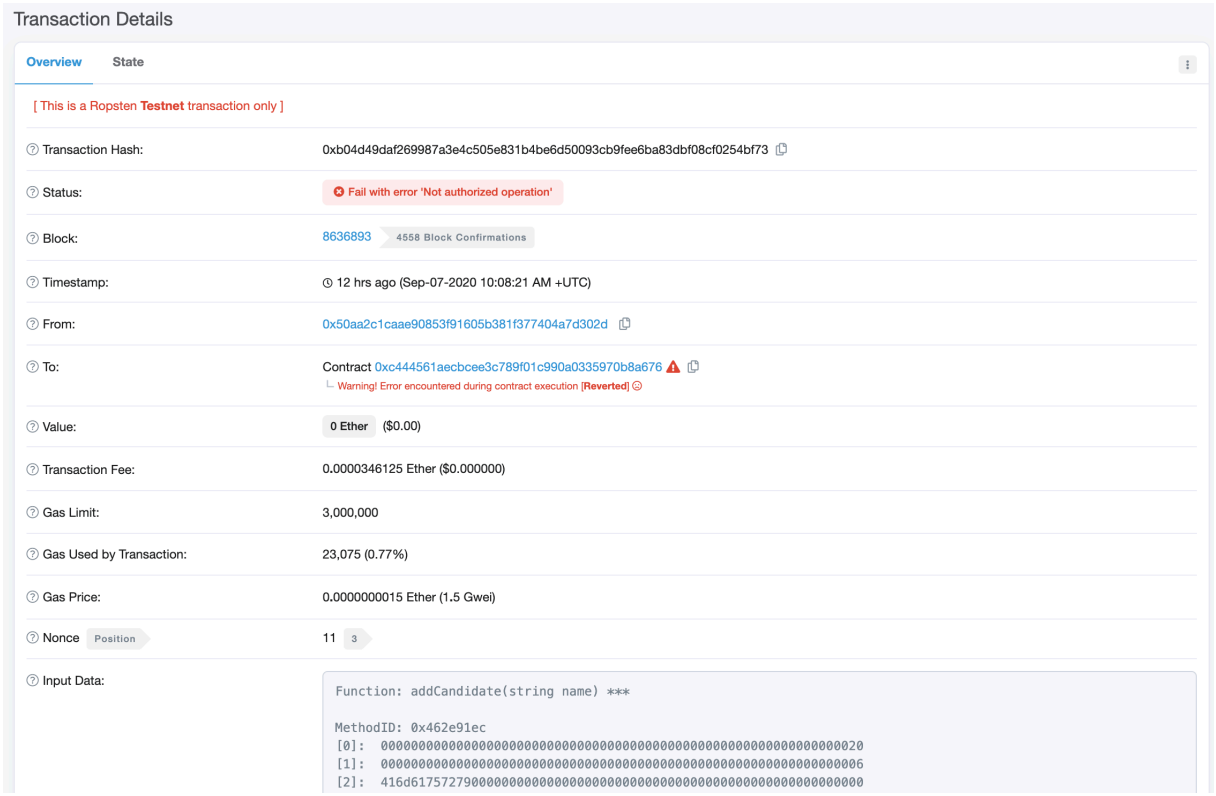
Lien :
https://ropsten.etherscan.io/tx/0x1be39c9549cc041a1e36b3c5b24a9db8aa691dc34d4f3a19faba4358985fba0c

1.x) A votre avis comment pourrions nous sécurisé l'appel de la fonction addCandidate afin que vous soyez le seul à pouvoir gérer les candidats ?

Il faut ajouter le modifier « onlyOwner » à la fonction addCandidate

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

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



Lien :
https://ropsten.etherscan.io/tx/0xb04d49daf269987a3e4c505e831b4be6d50093cb9fee6ba83dbf08cf0254bf73