Homework1

Programming a Faucet contract on the Sepolia testnet using Remix

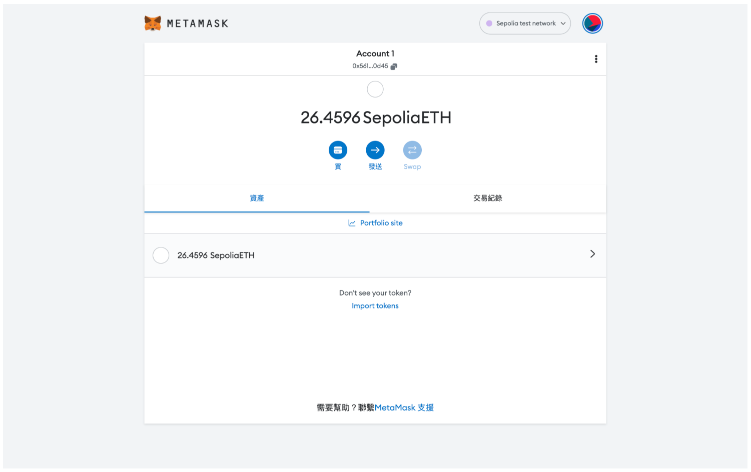
108321033吳明騰
108321056唐泳烽
108321062許恩慈

General sending and withdrawing Money

Introduction: We will show the process of sending and withdrawing between the wallet (0x5616d8...794f0d45) and the smart contract(0x2Dc571...31aF1052).Our source code on GitHub.

<step 1> metamask

We make a wallet (0x5616d8...794f0d45) and we get test coins from the Sepolia PoW Faucet.



26.4596 SepoliaETH

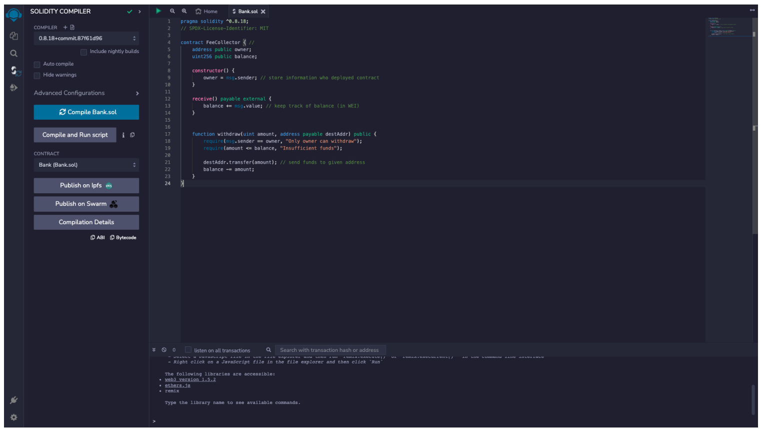
26.4596 SepoliaETH

Don't see your token?

需要幫助？聯繫MetaMask 支援

<step 2> Remix

Compiler original.sol on remix



COMPILER: 0.8.18+commit.87f61d96

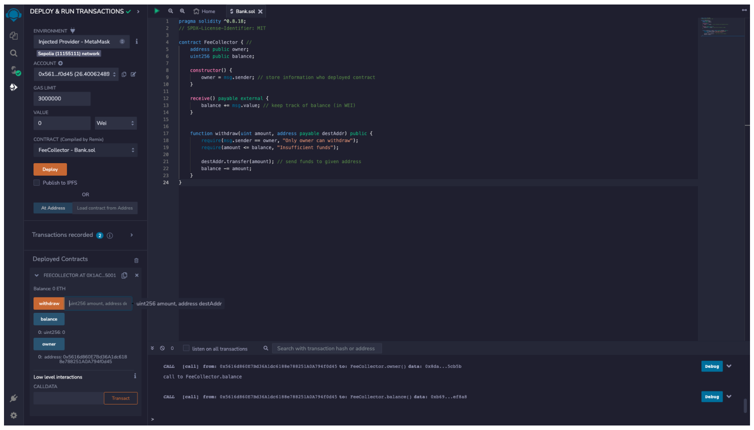
CONTRACT: Bank (Bank.sol)

```
pragma solidity ^0.8.18;
// SPDX-License-Identifier: MIT

contract FeeCollector { //
    address public owner;
    uint256 public balance;

    constructor() {
        owner = msg.sender; // store information who deployed contract
    }

    receive() payable external {
        balance += msg.value; // keep track of balance (in WEI)
    }


    function withdraw(uint amount, address payable destAddr) public {
        require(msg.sender == owner, "Only owner can withdraw");
        require(amount <= balance, "Insufficient funds");

        destAddr.transfer(amount); // send funds to given address
        balance -= amount;
    }
}
```

```
  - Right click on a JavaScript file in the file explorer and then click `Run`

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

 Type the library name to see available commands.

>
```

<step 3> Link to our wallet

ENVIRONMENT chooses Injected Provider - MetaMask, and links its own matamask



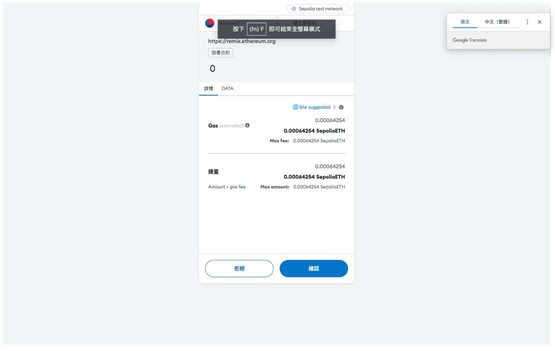
ENVIRONMENT: Injected Provider - MetaMask
Sepolia (11155111) network
ACCOUNT: 0x561...f0d45 (26.40062489
GAS LIMIT: 3000000
VALUE: 0 Wei
CONTRACT (Compiled by Remix): FeeCollector - Bank.sol
Publish to IPFS
FEECOLLECTOR AT 0X1AC...5001
Balance: 0 ETH
uint256 amount, address destAddr
0: uint256: 0
0: address: 0x5616d860E7Bd36A1dc6188e788251A0A794f0d45
CALLDATA

```
pragma solidity ^0.8.18;
// SPDX-License-Identifier: MIT

contract FeeCollector { //
    address public owner;
    uint256 public balance;

    constructor() {
        owner = msg.sender; // store information who deployed contract
    }

    receive() payable external {
        balance += msg.value; // keep track of balance (in WEI)
    }


    function withdraw(uint amount, address payable destAddr) public {
        require(msg.sender == owner, "Only owner can withdraw");
        require(amount <= balance, "Insufficient funds");

        destAddr.transfer(amount); // send funds to given address
        balance -= amount;
    }
}
```

```
CALL  [call]  from: 0x5616d860E7Bd36A1dc6188e788251A0A794f0d45 to: FeeCollector.owner() data: 0x8da...5cb5b
call to FeeCollector.balance

CALL  [call]  from: 0x5616d860E7Bd36A1dc6188e788251A0A794f0d45 to: FeeCollector.balance() data: 0xb69...ef8a8
```

<step 4> Make a smart contract

After pressing deploy, you will need to pay some gas, and the money in my wallet (0x5616d8...794f0d45) will decrease.

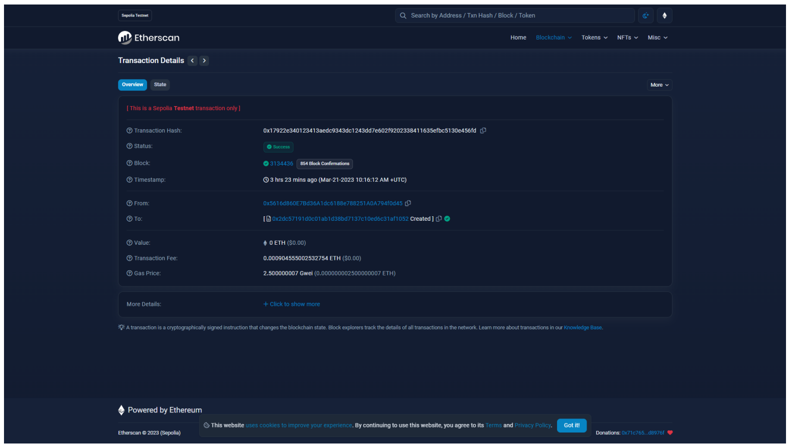


https://remix.ethereum.org
部署合約
0

Gas (estimated) 0.00064254
0.00064254 SepoliaETH
Max fee: 0.00064254 SepoliaETH

總量 0.00064254
0.00064254 SepoliaETH
Amount + gas fee Max amount: 0.00064254 SepoliaETH

Transaction Details from etherscan



[This is a Sepolia Testnet transaction only]

Transaction Hash: 0x17922e340123413aedc9343dc1243dd7e602f9202338411635efbc5130e456fd
Status: Success
Block: 3134436 854 Block Confirmations
Timestamp: 3 hrs 23 mins ago (Mar-21-2023 10:16:12 AM +UTC)

From: 0x5616d860E7Bd36A1dc6188e788251A0A794f0d45
To: [0x2dc57191d0c01ab1d38bd7137c10ed6c31af1052 Created]

Value: 0 ETH ($0.00)
Transaction Fee: 0.000904555002532754 ETH ($0.00)
Gas Price: 2.500000007 Gwei (0.000000002500000007 ETH)

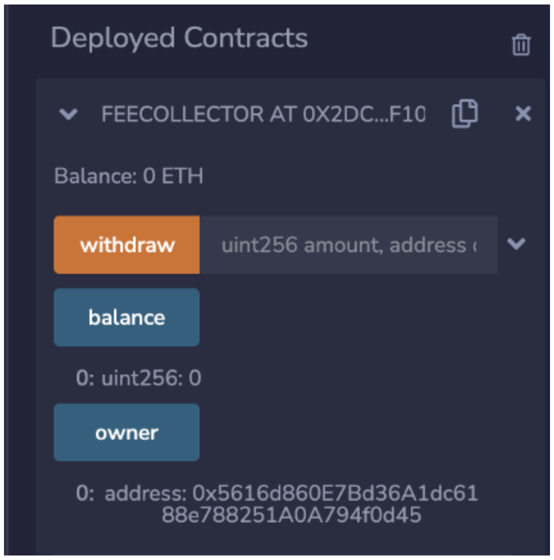
More Details: + Click to show more

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.

This website uses cookies to improve your experience. By continuing to use this website, you agree to its Terms and Privacy Policy.
Etherscan © 2023 (Sepolia)
Donations: 0x71c765...d8976f

<step 5>The details of the smart contract

About Our new smart contract (0x2Dc571...31aF1052), we can check who the owner is and how much money is in the smart contract.



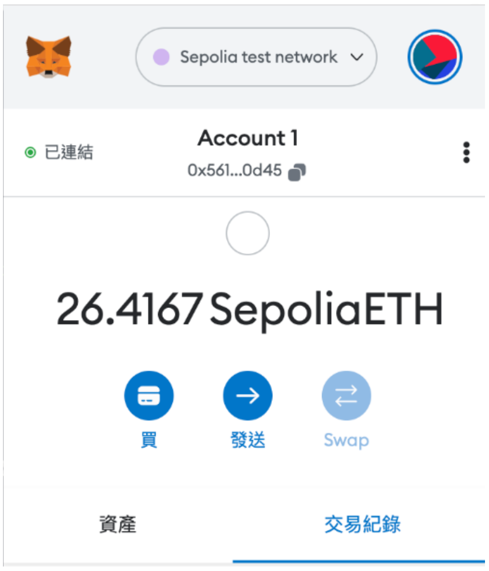
Balance: 0 ETH

0: uint256: 0

0: address: 0x5616d860E7Bd36A1dc6188e788251A0A794f0d45

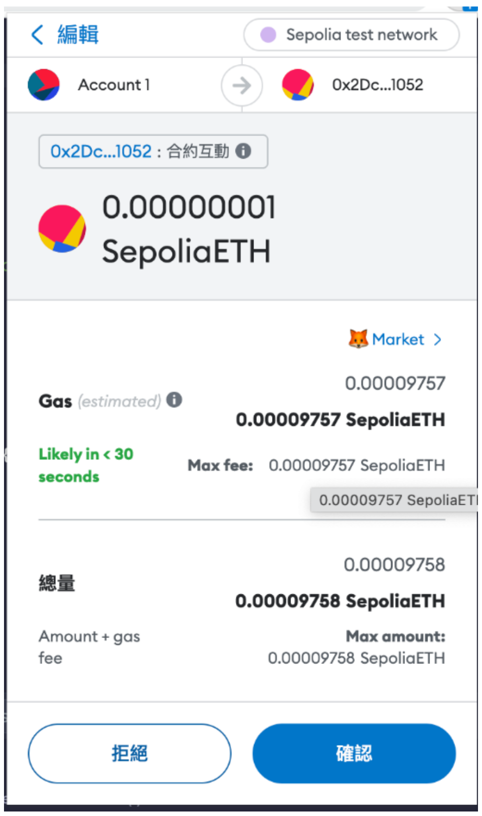
<step 6>Sending

Send money from my wallet (0x5616d8...794f0d45) to the smart contract (0x2Dc571...31aF1052)



26.4167 SepoliaETH

The details of the transaction: Amount+gas free = 0.00009757+0.00000001 = 0.00009758



< 編輯 Sepolia test network

Account 1 → 0x2Dc...1052

0x2Dc...1052 : 合約互動

0.00000001 SepoliaETH

Market >

Gas (estimated) 0.00009757

0.00009757 SepoliaETH

Likely in < 30 seconds

Max fee: 0.00009757 SepoliaETH

0.00009757 SepoliaET

總量 0.00009758

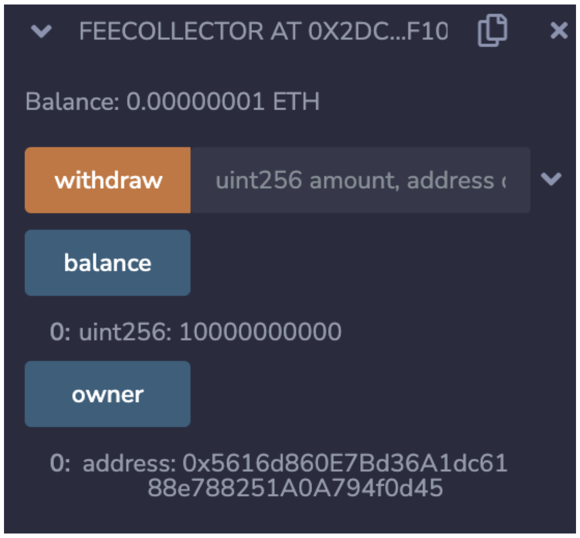
0.00009758 SepoliaETH

Amount + gas fee

Max amount: 0.00009758 SepoliaETH

拒絕 確認

Confirm that the smart contract has 0.00000001 ETH



FEECOLLECTOR AT 0X2DC...F10

Balance: 0.00000001 ETH

withdraw uint256 amount, address

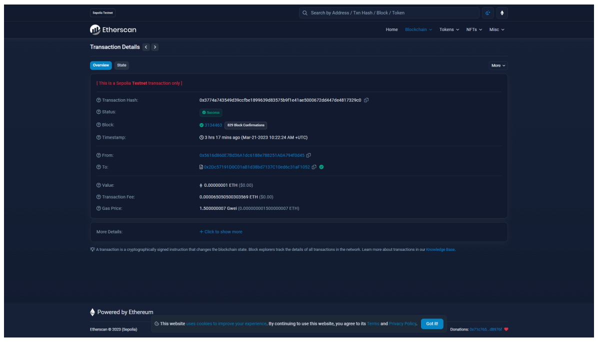
balance

0: uint256: 10000000000

owner

0: address: 0x5616d860E7Bd36A1dc61
88e788251A0A794f0d45

Transaction Details from etherscan


Sepolia Testnet

Search by Address / Txn Hash / Block / Token

Etherscan

Home | Blockchain | Tokens | NFTs | Misc

Transaction Details

Overview | State | More

[This is a Sepolia Testnet transaction only]

Transaction Hash:	0x3774a743549d39ccfbe1899639d83575b9f1e41ae5000672dd447de4817329c0
Status:	Success
Block:	3134463 829 Block Confirmations
Timestamp:	3 hrs 17 mins ago (Mar-21-2023 10:22:24 AM +UTC)
From:	0x5616d860E7Bd36A1dc6188e788251A0A794f0d45
To:	0x2Dc57191D0C01aB1d38bd7137C10ed6c31aF1052
Value:	0.00000001 ETH ($0.00)
Transaction Fee:	0.000065050500303569 ETH ($0.00)
Gas Price:	1.500000007 Gwei (0.000000001500000007 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.

Powered by Ethereum

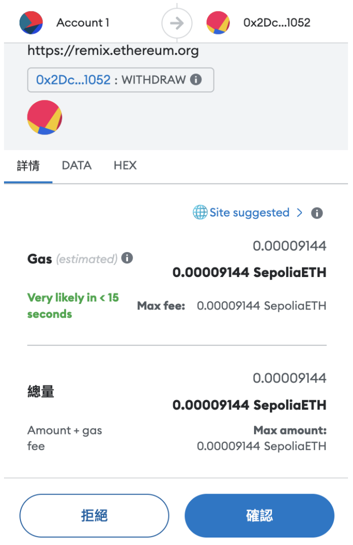
This website uses cookies to improve your experience. By continuing to use this website, you agree to its Terms and Privacy Policy. Got it!

Etherscan © 2023 (Sepolia)

Donations: 0x71c765...d8976f

<step 9>Widrawing

After pressing the transaction in withdraw, the gas fee will be charged, and the money will be withdrawn


Account 1 → 0x2Dc...1052

https://remix.ethereum.org

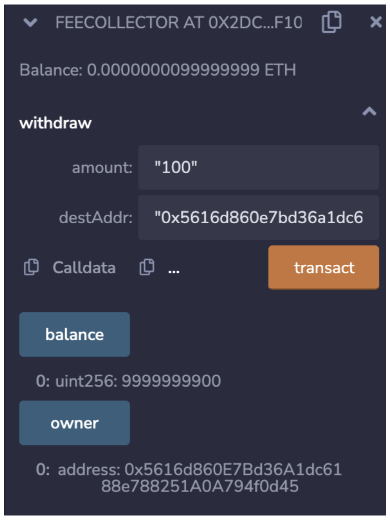
0x2Dc...1052 : WITHDRAW

詳情 | DATA | HEX

Site suggested

Gas (estimated)	0.00009144 **0.00009144 SepoliaETH**
Very likely in < 15 seconds	**Max fee:** 0.00009144 SepoliaETH
總量	0.00009144 **0.00009144 SepoliaETH**
Amount + gas fee	**Max amount:** 0.00009144 SepoliaETH

拒絕 | 確認


FEECOLLECTOR AT 0X2DC...F10

Balance: 0.0000000099999999 ETH

withdraw

amount: "100"

destAddr: "0x5616d860e7bd36a1dc6

Calldata ... transact

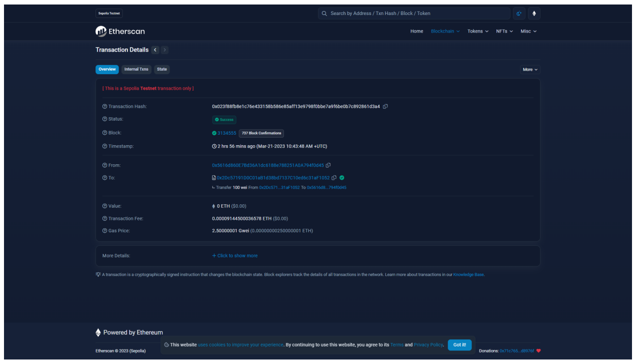
balance

0: uint256: 9999999900

owner

0: address: 0x5616d860E7Bd36A1dc6188e788251A0A794f0d45

Transaction Details from etherscan


Sepolia Testnet

Search by Address / Txn Hash / Block / Token

Etherscan

Home | Blockchain | Tokens | NFTs | Misc

Transaction Details

Overview | Internal Txns | State | More

[This is a Sepolia Testnet transaction only]

Transaction Hash:	0x023f88fb8e1c76e433158b586e85aff13e9798f0bbe7a9f6be0b7c892861d3a4
Status:	Success
Block:	3134555 737 Block Confirmations
Timestamp:	2 hrs 56 mins ago (Mar-21-2023 10:43:48 AM +UTC)
From:	0x5616d860E7Bd36A1dc6188e788251A0A794f0d45
To:	0x2Dc57191D0C01aB1d38bd7137C10ed6c31aF1052 └ Transfer 100 wei From 0x2Dc571...31aF1052 To 0x5616d8...794f0d45
Value:	0 ETH ($0.00)
Transaction Fee:	0.00009144500036578 ETH ($0.00)
Gas Price:	2.50000001 Gwei (0.00000000250000001 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.

Powered by Ethereum

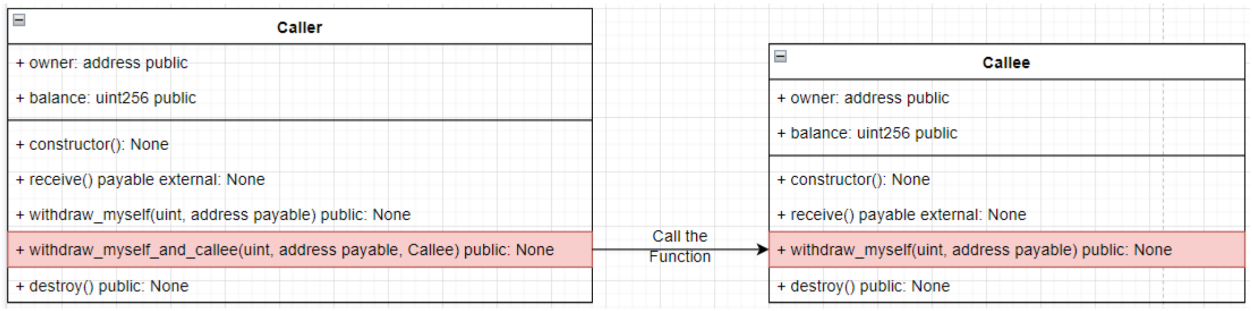
This website uses cookies to improve your experience. By continuing to use this website, you agree to its Terms and Privacy Policy. Got it!

Etherscan © 2023 (Sepolia)

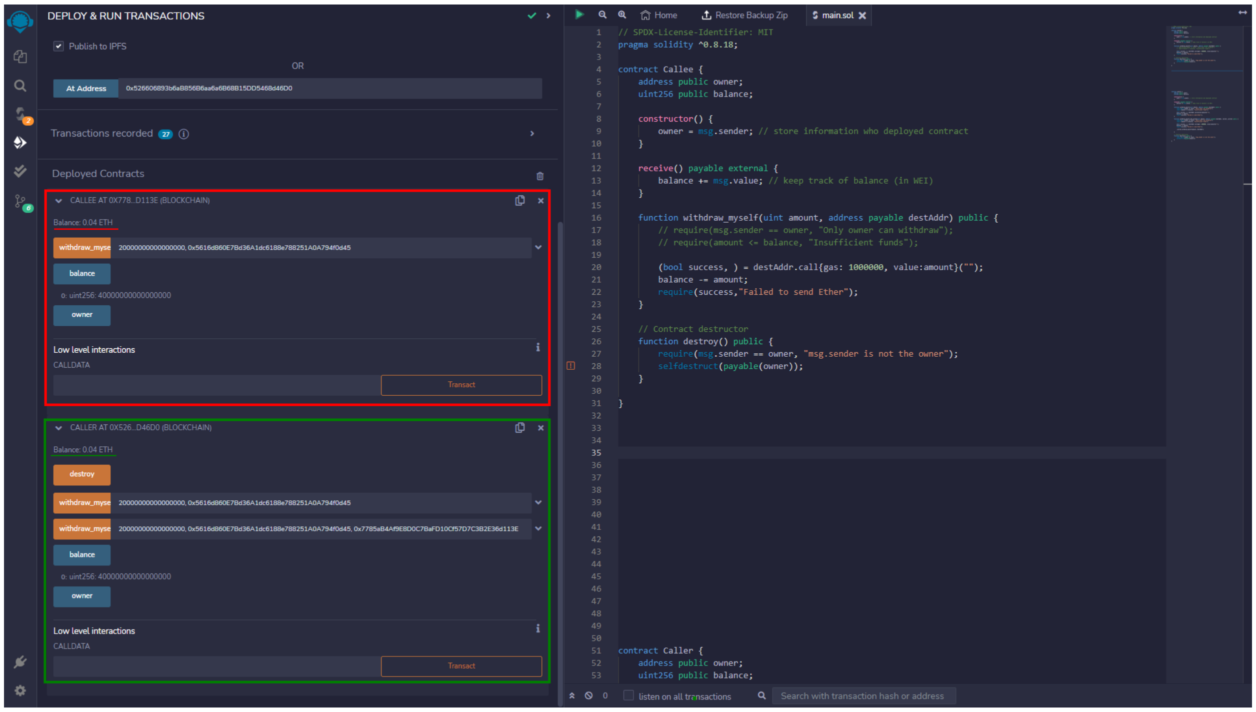
Donations: 0x71c765...d8976f

Call Other Contracts

Introduction: we want to try to check the problem: Who pays gas when a contract function that creates/calls another contract is called? In the Below diagram, we design two smart contracts Caller and callee. The function withdraw_myself of both smart contracts can withdraw money from the smart contract to our wallet. The Caller's withdraw_myself_and_callee of can ont only withdraw money, but call the Callee's function withdraw_myself. Our source code on GitHub.


Caller
+ owner: address public
+ balance: uint256 public
+ constructor(): None
+ receive() payable external: None
+ withdraw_myself(uint, address payable) public: None
+ withdraw_myself_and_callee(uint, address payable, Callee) public: None
+ destroy() public: None
Call the Function
Callee
+ owner: address public
+ balance: uint256 public
+ constructor(): None
+ receive() payable external: None
+ withdraw_myself(uint, address payable) public: None
+ destroy() public: None

<step 1>Check the wallet and smart contracts: We have a wallet (0x5616d8...794f0d45) and two smart contracts callee (0x7785aB...E36d113E) and caller (0x526606...468d46D0) with a balance 0.04 ETH.



0x526606893b6aB856B6aa6a6B68B15DD5468d46D0

CALLEE AT 0X778...D113E (BLOCKCHAIN)

Balance: 0.04 ETH

withdraw_myse 20000000000000000, 0x5616d860E7Bd36A1dc6188e788251A0A794f0d45

balance

0: uint256: 40000000000000000

owner

Low level interactions

CALLDATA

Transact

CALLER AT 0X526...D46D0 (BLOCKCHAIN)

Balance: 0.04 ETH

destroy

withdraw_myse 20000000000000000, 0x5616d860E7Bd36A1dc6188e788251A0A794f0d45

withdraw_myse 20000000000000000, 0x5616d860E7Bd36A1dc6188e788251A0A794f0d45, 0x7785aB4Af9E8D0C7BaFD10Cf57D7C3B2E36d113E

balance

0: uint256: 40000000000000000

owner

Low level interactions

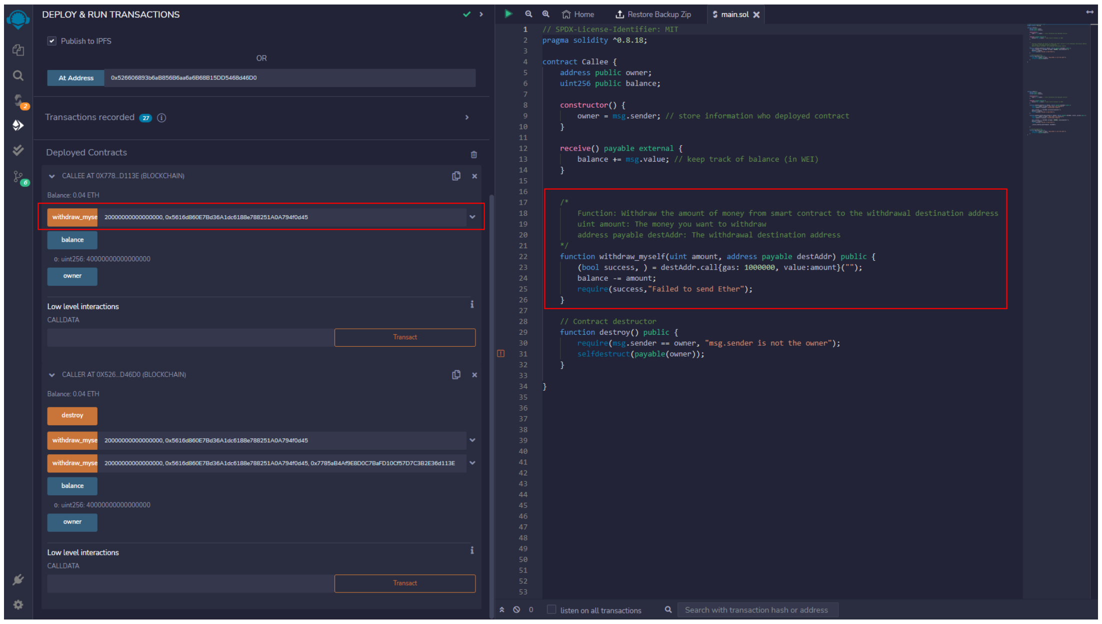
CALLDATA

Transact

```
// SPDX-License-Identifier: MIT
pragma solidity ^0.8.18;

contract Callee {
    address public owner;
    uint256 public balance;

    constructor() {
        owner = msg.sender; // store information who deployed contract
    }

    receive() payable external {
        balance += msg.value; // keep track of balance (in WEI)
    }

    function withdraw_myself(uint amount, address payable destAddr) public {
        // require(msg.sender == owner, "Only owner can withdraw");
        // require(amount <= balance, "Insufficient funds");

        (bool success, ) = destAddr.call{gas: 1000000, value:amount}("");
        balance -= amount;
        require(success,"Failed to send Ether");
    }

    // Contract destructor
    function destroy() public {
        require(msg.sender == owner, "msg.sender is not the owner");
        selfdestruct(payable(owner));
    }

}



















contract Caller {
    address public owner;
    uint256 public balance;
```

0
listen on all transactions
Search with transaction hash or address

<step 2> General Transfer money (Transaction Details): We call the function withdraw_myself to withdraw the amount of money from smart contract callee (0x7785aB...E36d113E) to my wallet (0x5616d8...794f0d45).
Transfer 0.02 ETH From 0x7785aB...E36d113E(callee) To 0x5616d8...794f0d45 (wallet)
Transaction Fee: 0.000086507500276824 ETH = 86507.500276824 Gwei



0x526606893b6aB856B6aa6a6B68B15DD5468d46D0

Transactions recorded 27

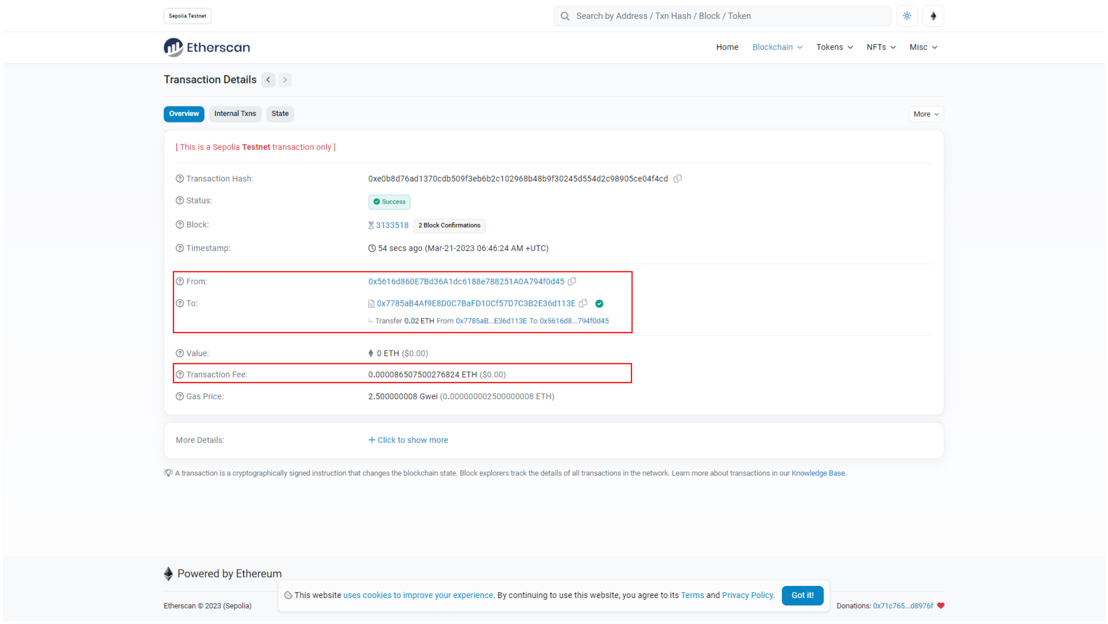
Deployed Contracts

CALLEE AT 0X778...D113E (BLOCKCHAIN)
Balance: 0.04 ETH
withdraw_myse 20000000000000000, 0x5616d860E7Bd36A1dc6188e788251A0A794f0d45
balance
0: uint256: 40000000000000000
owner
Low level interactions
CALLDATA
Transact

CALLER AT 0X526...D46D0 (BLOCKCHAIN)
Balance: 0.04 ETH
destroy
withdraw_myse 20000000000000000, 0x5616d860E7Bd36A1dc6188e788251A0A794f0d45
withdraw_myse 20000000000000000, 0x5616d860E7Bd36A1dc6188e788251A0A794f0d45, 0x7785aB4Af9E8D0C7BaFD10Cf57D7C3B2E36d113E
balance
0: uint256: 40000000000000000
owner
Low level interactions
CALLDATA
Transact

listen on all transactions
Search with transaction hash or address

```
// SPDX-License-Identifier: MIT
pragma solidity ^0.8.18;

contract Callee {
    address public owner;
    uint256 public balance;

    constructor() {
        owner = msg.sender; // store information who deployed contract
    }

    receive() payable external {
        balance += msg.value; // keep track of balance (in WEI)
    }


    /*
        Function: Withdraw the amount of money from smart contract to the withdrawal destination address
        uint amount: The money you want to withdraw
        address payable destAddr: The withdrawal destination address
    */
    function withdraw_myself(uint amount, address payable destAddr) public {
        (bool success, ) = destAddr.call{gas: 1000000, value:amount}("");
        balance -= amount;
        require(success,"Failed to send Ether");
    }

    // Contract destructor
    function destroy() public {
        require(msg.sender == owner, "msg.sender is not the owner");
        selfdestruct(payable(owner));
    }

}
```



Transaction Details

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

Transaction Hash:	0xe0b8d76ad1370cdb509f3eb6b2c102968b48b9f30245d554d2c98905ce04f4cd
Status:	Success
Block:	3133518 2 Block Confirmations
Timestamp:	54 secs ago (Mar-21-2023 06:46:24 AM +UTC)
From:	0x5616d860E7Bd36A1dc6188e788251A0A794f0d45
To:	0x7785aB4Af9E8D0C7BaFD10Cf57D7C3B2E36d113E └ Transfer 0.02 ETH From 0x7785aB...E36d113E To 0x5616d8...794f0d45
Value:	0 ETH ($0.00)
Transaction Fee:	0.000086507500276824 ETH ($0.00)
Gas Price:	2.500000008 Gwei (0.000000002500000008 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.

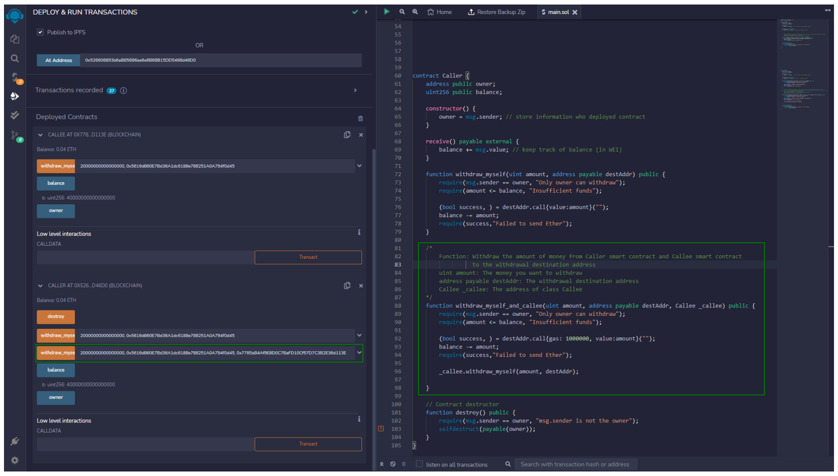
Powered by Ethereum

This website uses cookies to improve your experience. By continuing to use this website, you agree to its Terms and Privacy Policy. Got it!

Etherscan © 2023 (Sepolia)

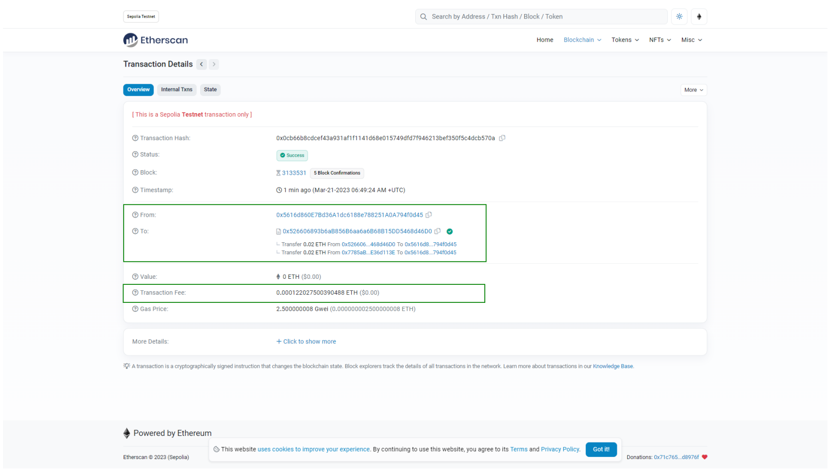
Donations: 0x71c765...d8976f

<step 3> Transfer money two times(Transaction Details): a contract function that creates/calls another contract is called.
Transfer 0.02 ETH From 0x526606...468d46D0 (caller) To 0x5616d8...794f0d45 (wallet)
Transfer 0.02 ETH From 0x7785aB...E36d113E (callee)To 0x5616d8...794f0d45 (wallet)
Transaction Fee: 0.000122027500390488 ETH = 122027.500390488 Gwei



```
At Address 0x526606893b6aB856B6aa6a6B68B15DD5468d46D0

CALLEE AT 0X778...D113E (BLOCKCHAIN)
Balance: 0.04 ETH
withdraw_myse 20000000000000000, 0x5616d860E7Bd36A1dc6188e788251A0A794f0d45
balance
0: uint256: 40000000000000000

CALLER AT 0X526...D46D0 (BLOCKCHAIN)
Balance: 0.04 ETH
withdraw_myse 20000000000000000, 0x5616d860E7Bd36A1dc6188e788251A0A794f0d45
withdraw_myse 20000000000000000, 0x5616d860E7Bd36A1dc6188e788251A0A794f0d45, 0x7785aB4Af9E8D0C7BaFD10Cf57D7C3B2E36d113E
balance
0: uint256: 40000000000000000
```

```
contract Caller {
    address public owner;
    uint256 public balance;

    constructor() {
        owner = msg.sender; // store information who deployed contract
    }

    receive() payable external {
        balance += msg.value; // keep track of balance (in WEI)
    }

    function withdraw_myself(uint amount, address payable destAddr) public {
        require(msg.sender == owner, "Only owner can withdraw");
        require(amount <= balance, "Insufficient funds");

        (bool success, ) = destAddr.call{value:amount}("");
        balance -= amount;
        require(success,"Failed to send Ether");
    }

    /*
        Function: Withdraw the amount of money from Caller smart contract and Callee smart contract
                    to the withdrawal destination address
        uint amount: The money you want to withdraw
        address payable destAddr: The withdrawal destination address
        Callee _callee: The address of class Callee
    */
    function withdraw_myself_and_callee(uint amount, address payable destAddr, Callee _callee) public {
        require(msg.sender == owner, "Only owner can withdraw");
        require(amount <= balance, "Insufficient funds");

        (bool success, ) = destAddr.call{gas: 1000000, value:amount}("");
        balance -= amount;
        require(success,"Failed to send Ether");

        _callee.withdraw_myself(amount, destAddr);

    }

    // Contract destructor
    function destroy() public {
        require(msg.sender == owner, "msg.sender is not the owner");
        selfdestruct(payable(owner));
    }
}
```



Transaction Details

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

Transaction Hash:	0x0cb66b8cdcef43a931af1f1141d68e015749dfd7f946213bef350f5c4dcb570a
Status:	Success
Block:	3133531 5 Block Confirmations
Timestamp:	1 min ago (Mar-21-2023 06:49:24 AM +UTC)
From:	0x5616d860E7Bd36A1dc6188e788251A0A794f0d45
To:	0x526606893b6aB856B6aa6a6B68B15DD5468d46D0 └ Transfer 0.02 ETH From 0x526606...468d46D0 To 0x5616d8...794f0d45 └ Transfer 0.02 ETH From 0x7785aB...E36d113E To 0x5616d8...794f0d45
Value:	0 ETH ($0.00)
Transaction Fee:	0.000122027500390488 ETH ($0.00)
Gas Price:	2.500000008 Gwei (0.000000002500000008 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.

Powered by Ethereum

This website uses cookies to improve your experience. By continuing to use this website, you agree to its Terms and Privacy Policy. Got it!

Etherscan © 2023 (Sepolia)

Donations: 0x71c765...d8976f

Conclusion:
On step 3, we can find that our wallet has to pay the gas used by the smart contract caller and callee.

The problems we meet

a. Warning message:

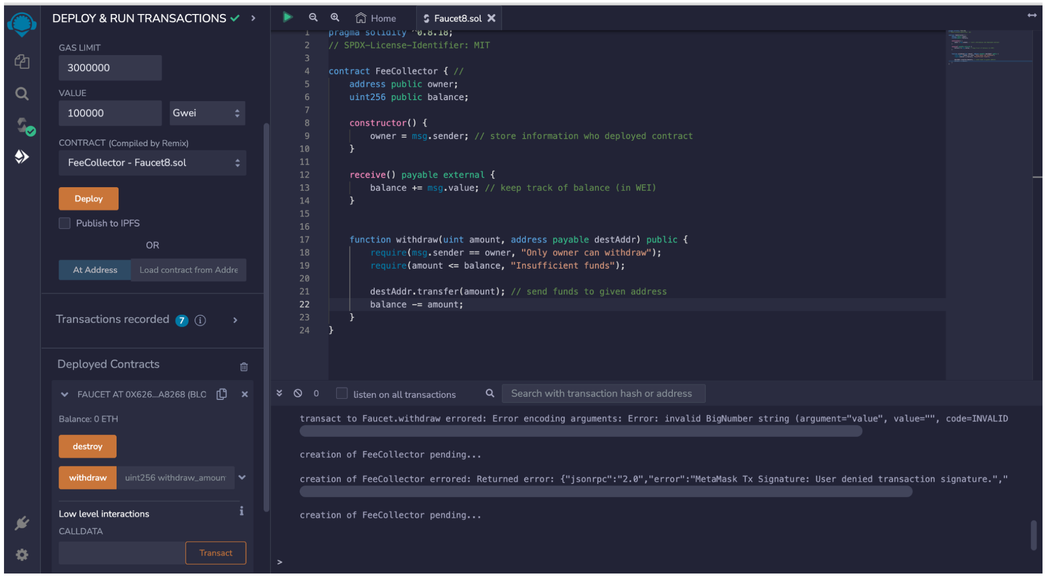
```
Warning: SPDX license identifier not provided in source file. Before publishing, consider adding a comment containing "SPDX-License-Identifier: <SPDX-License>" to each source file. Use "SPDX-License-Identifier: UNLICENSED" for non-open-source code. Please see https://spdx.org for more information.
```

can add the '// SPDX-License-Identifier: MIT' on the first line of code to fix the problem.

b. In the beginning, our previous version code have an error message:

```
Gas estimation errored with the following message (see below). The transaction execution will likely fail. Do you want to force sending?
```

The reason may be that the money will not be sent until the smart contract is deployed, so you must set this value to 0.



GAS LIMIT: 3000000

VALUE: 100000 Gwei

CONTRACT (Compiled by Remix): FeeCollector - Faucet8.sol

FAUCET AT 0X626...A8268 (BLC

Balance: 0 ETH

```
pragma solidity ^0.8.18;
// SPDX-License-Identifier: MIT

contract FeeCollector { //
    address public owner;
    uint256 public balance;

    constructor() {
        owner = msg.sender; // store information who deployed contract
    }

    receive() payable external {
        balance += msg.value; // keep track of balance (in WEI)
    }


    function withdraw(uint amount, address payable destAddr) public {
        require(msg.sender == owner, "Only owner can withdraw");
        require(amount <= balance, "Insufficient funds");

        destAddr.transfer(amount); // send funds to given address
        balance -= amount;
    }
}
```

```
transact to Faucet.withdraw errored: Error encoding arguments: Error: invalid BigNumber string (argument="value", value="", code=INVALID

creation of FeeCollector pending...

creation of FeeCollector errored: Returned error: {"jsonrpc":"2.0","error":"MetaMask Tx Signature: User denied transaction signature.","

creation of FeeCollector pending...

>
```

So we replaced a new version of original.sol.