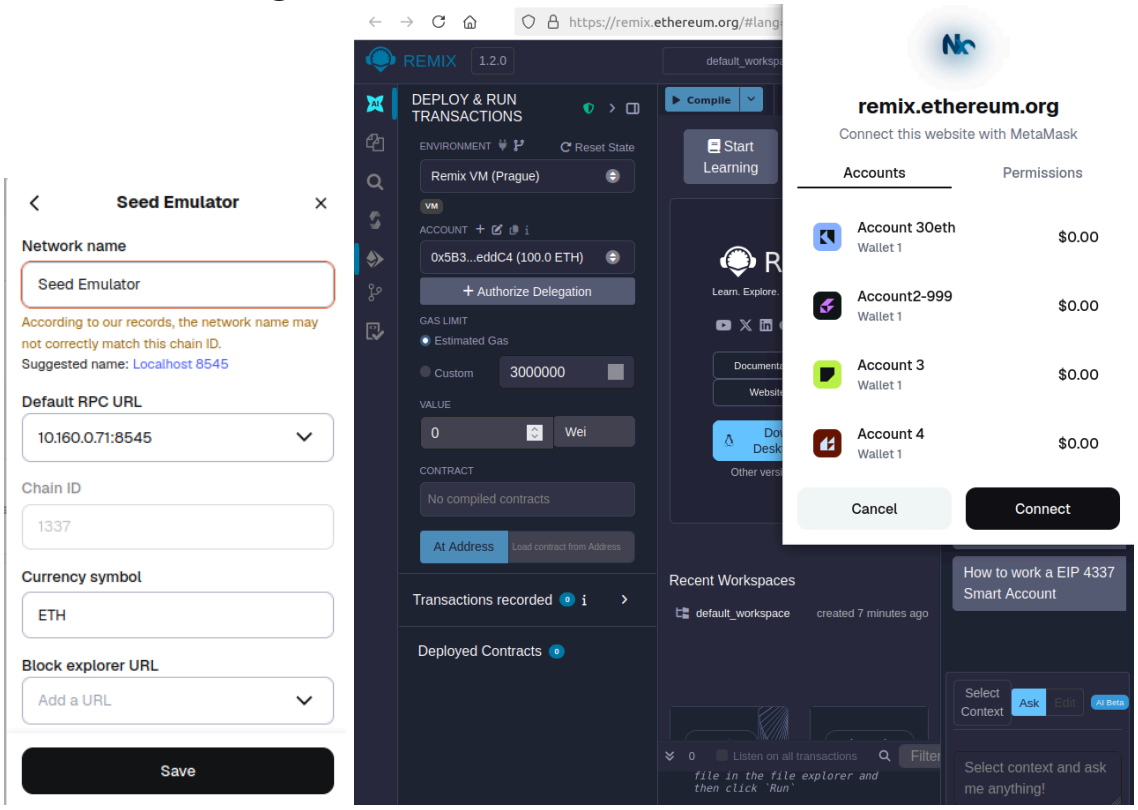
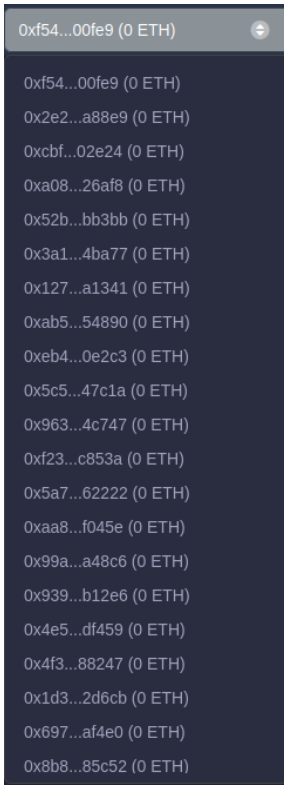
Smart Contract Lab

Task 1.a: Connecting Remix to the SEED Emulator

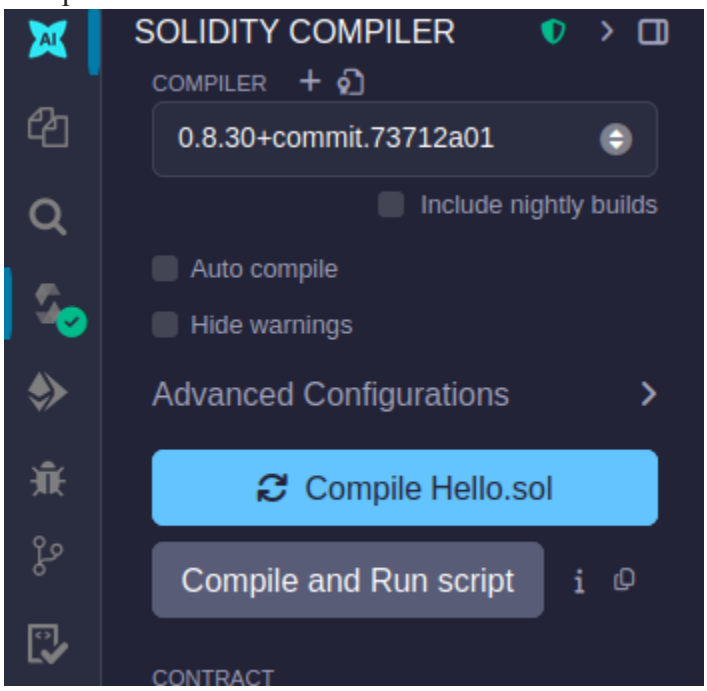


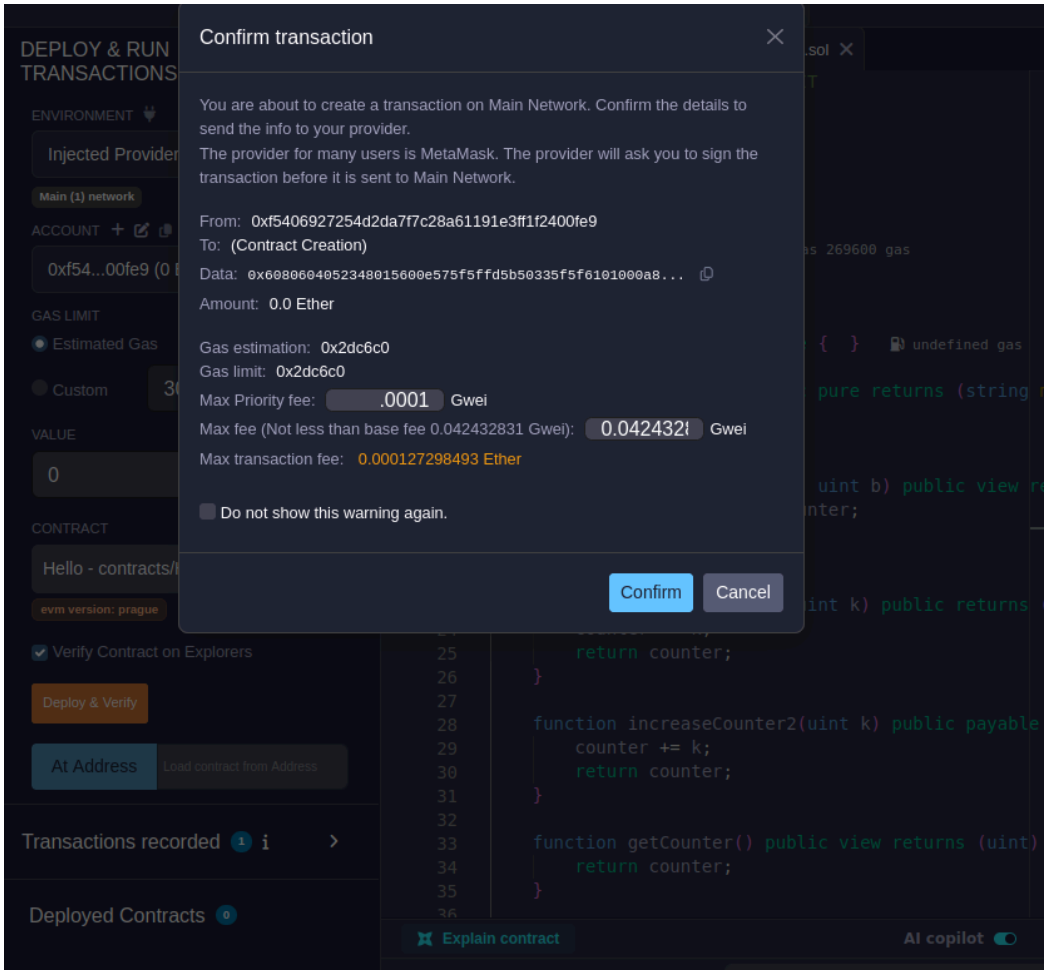


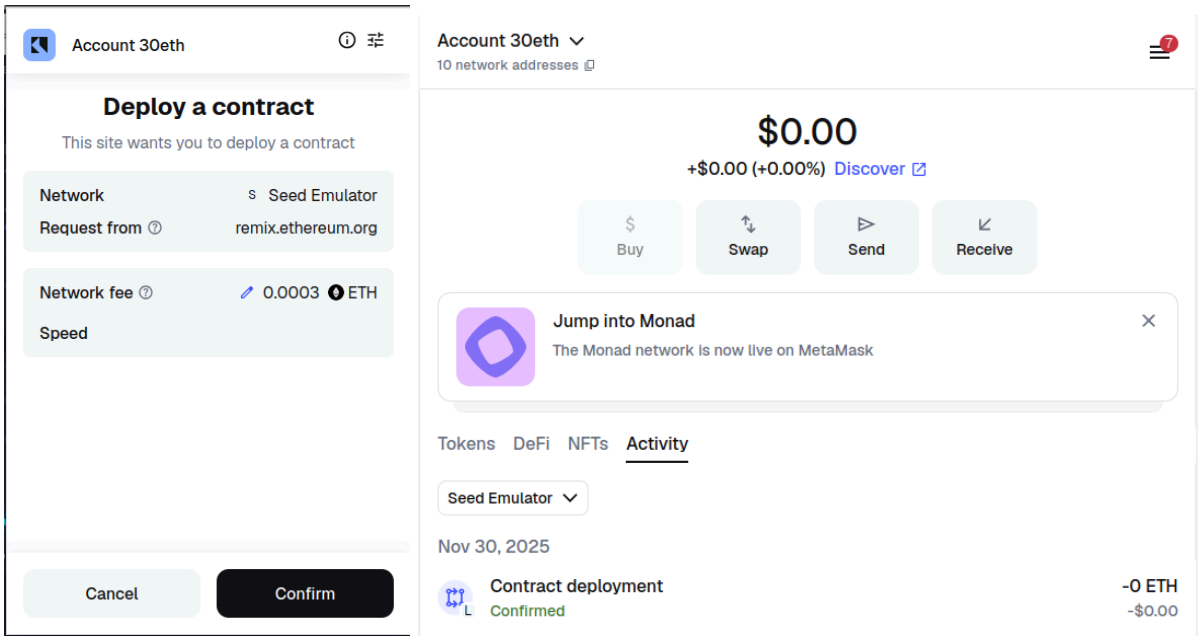
Task 1.b: Write, Compile, and Deploy Smart Contract

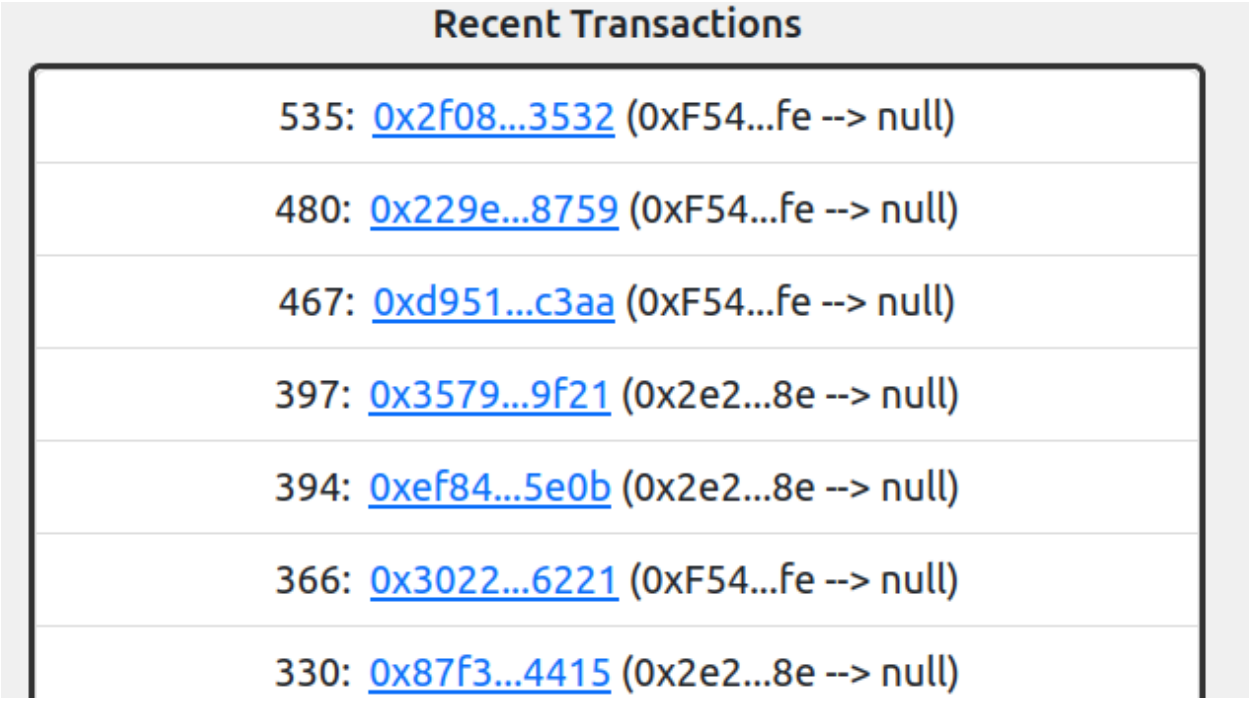
```
Compile   Home   Hello.sol
1  // SPDX-License-Identifier: MIT
2  pragma solidity ^0.8.15;
3
4  contract Hello{
5      address public owner;
6      uint256 counter;
7
8      constructor(){    294174 gas 269600 gas
9          owner = msg.sender;
10     }
11
12     receive() external payable {  }    undefined gas
13
14     function sayHello() public pure returns (string memory) {    infinite gas
15         return "Hello World";
16     }
17
18     function getResult(uint a, uint b) public view returns (uint) {    infinite gas
19         uint sum = a + b + counter;
20         return sum;
21     }
22
23     function increaseCounter(uint k) public returns (uint) {    infinite gas
24         counter += k;
25         return counter;
26     }
27
28     function increaseCounter2(uint k) public payable returns (uint) {    infinite gas
29         counter += k;
30         return counter;
31     }
32
33     function getCounter() public view returns (uint) {    2455 gas
34         return counter;
35     }
```

Compile Hello.sol




DEPLOY & RUN TRANSACTIONS
ENVIRONMENT
Injected Provider
Main (1) network
ACCOUNT
0xf54...00fe9 (0
GAS LIMIT
Estimated Gas
Custom
VALUE
0
CONTRACT
Hello - contracts/
evm version: prague
Verify Contract on Explorers
Deploy & Verify
At Address
Load contract from Address
Transactions recorded 1
Deployed Contracts 0
Confirm transaction
You are about to create a transaction on Main Network. Confirm the details to send the info to your provider.
The provider for many users is MetaMask. The provider will ask you to sign the transaction before it is sent to Main Network.
From: 0xf5406927254d2da7f7c28a61191e3ff1f2400fe9
To: (Contract Creation)
Data: 0x608060405234801560e575f5ffd5b50335f5f6101000a8...
Amount: 0.0 Ether
Gas estimation: 0x2dc6c0
Gas limit: 0x2dc6c0
Max Priority fee: .0001 Gwei
Max fee (Not less than base fee 0.042432831 Gwei): 0.042432 Gwei
Max transaction fee: 0.000127298493 Ether
Do not show this warning again.
Confirm
Cancel
269600 gas
undefined gas
pure returns (string
uint b) public view
int k) public returns
return counter;
function increaseCounter2(uint k) public payable
counter += k;
return counter;
function getCounter() public view returns (uint)
return counter;
Explain contract
AI copilot


Account 30eth
Deploy a contract
This site wants you to deploy a contract
Network
Seed Emulator
Request from
remix.ethereum.org
Network fee
0.0003 ETH
Speed
Cancel
Confirm
Account 30eth
10 network addresses
$0.00
+$0.00 (+0.00%) Discover
Buy
Swap
Send
Receive
Jump into Monad
The Monad network is now live on MetaMask
Tokens
DeFi
NFTs
Activity
Seed Emulator
Nov 30, 2025
Contract deployment
Confirmed
-0 ETH
-$0.00



Task 1.c: Under the Hood

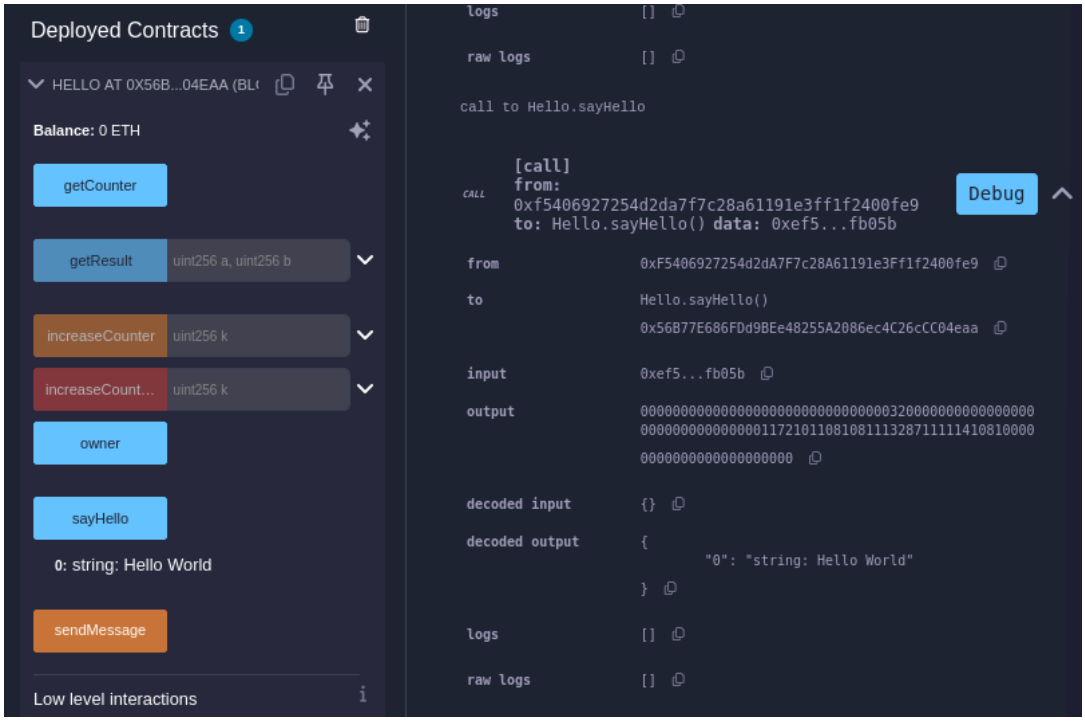
Transaction | Receipt

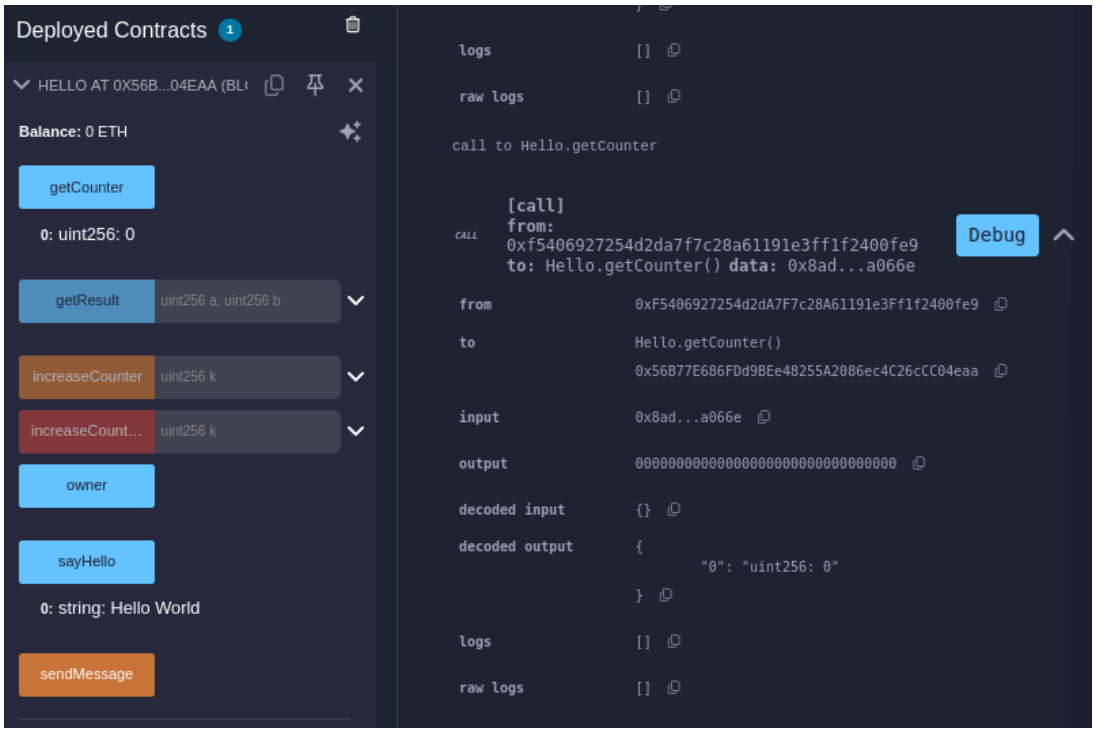
hash	0x2f083af1a033f2bff689d44b3b2710cf87293ebe3fb48a0eebc67efd25a35321
type	2
accessList	
blockHash	0x1753480bed3708006e0731cc3084679229a37ab653e9909e084f5328ffb593f9
blockNumber	535
transactionIndex	0
confirmations	24
from	0xF5406927254d2dA7F7c28A61191e3Ff1f2400fe9
gasPrice	1000000007
maxPriorityFeePerGas	1000000007
maxFeePerGas	1000000007
gasLimit	290883
to	null
value	0
nonce	5
data	0x6080604052348015610010576000080fd5b50336000806101000a81548173ffffffffffffffff
r	0x564e01345905f71363f07d7972fd942d978c8138af28348eb49611cf5d535e81
s	0x63c03e04a6bf69f50afbc7c5d2d47126f4341697e8ed4eea43cdf2dac2152cd5
v	1
creates	0x4e6A5dbdf46270331aC1618F1497BEFbFee00b47
chainId	1337
wait	(omitted)

We can see that the main differences between contract deployment transaction and normal fund transfer is that deployment has no “to” address, deployment stores bytecode in the data field and gas usage is higher

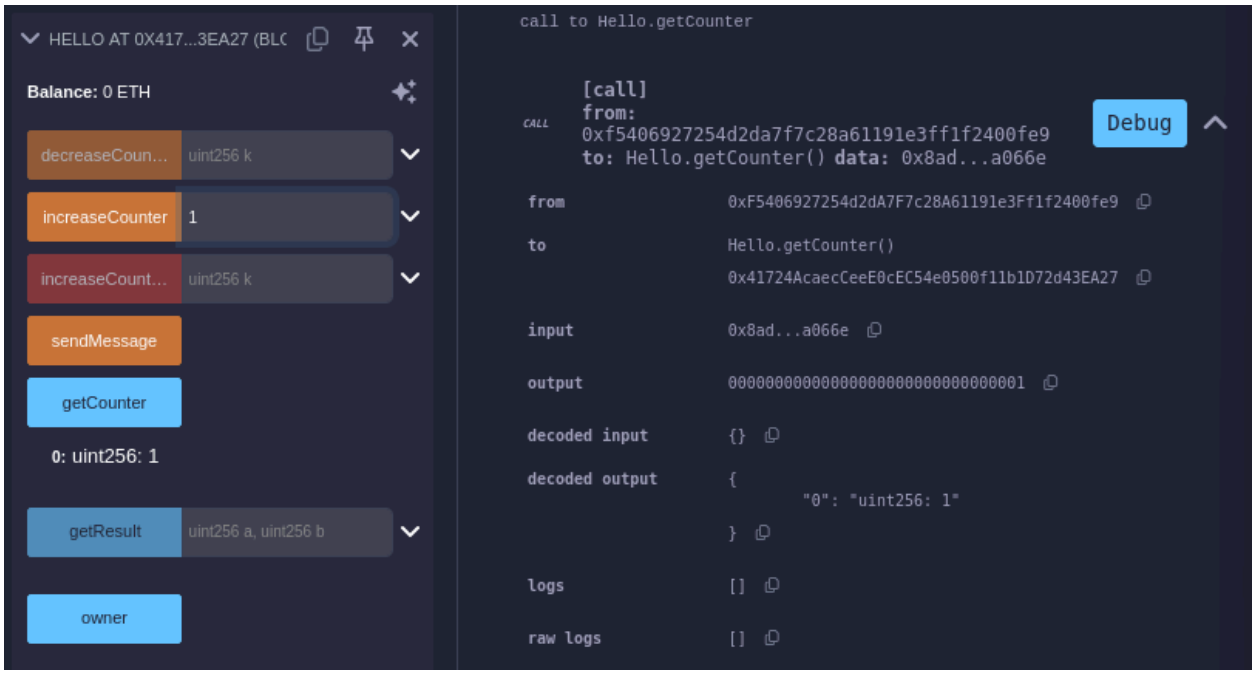
Task 2: Invoke Contract Functions

Task 2.a: Invoke a function via local call



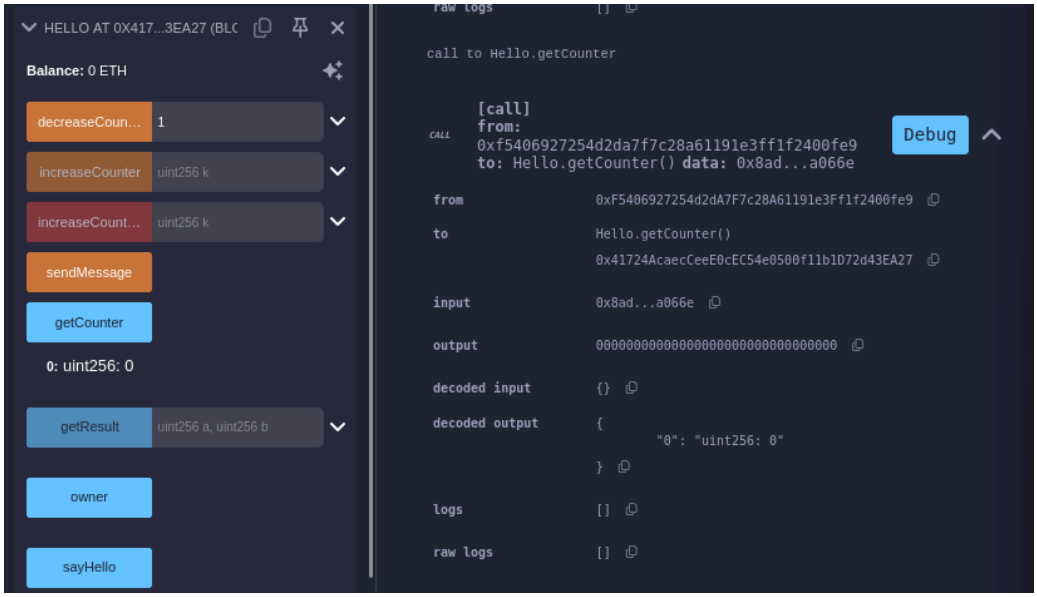


Task 2.b: Invoke a function via transaction



From this we can see that the counter indeed go up by 1, Now we implement decreaseCounter

```
function decreaseCounter(uint k) public returns (uint) {    21955 gas
    counter -= k;
    return counter;
}
```



From this we can see that counter gets decreased after calling decreaseCounter

Task 2.c: Under the hood

Transaction | Receipt

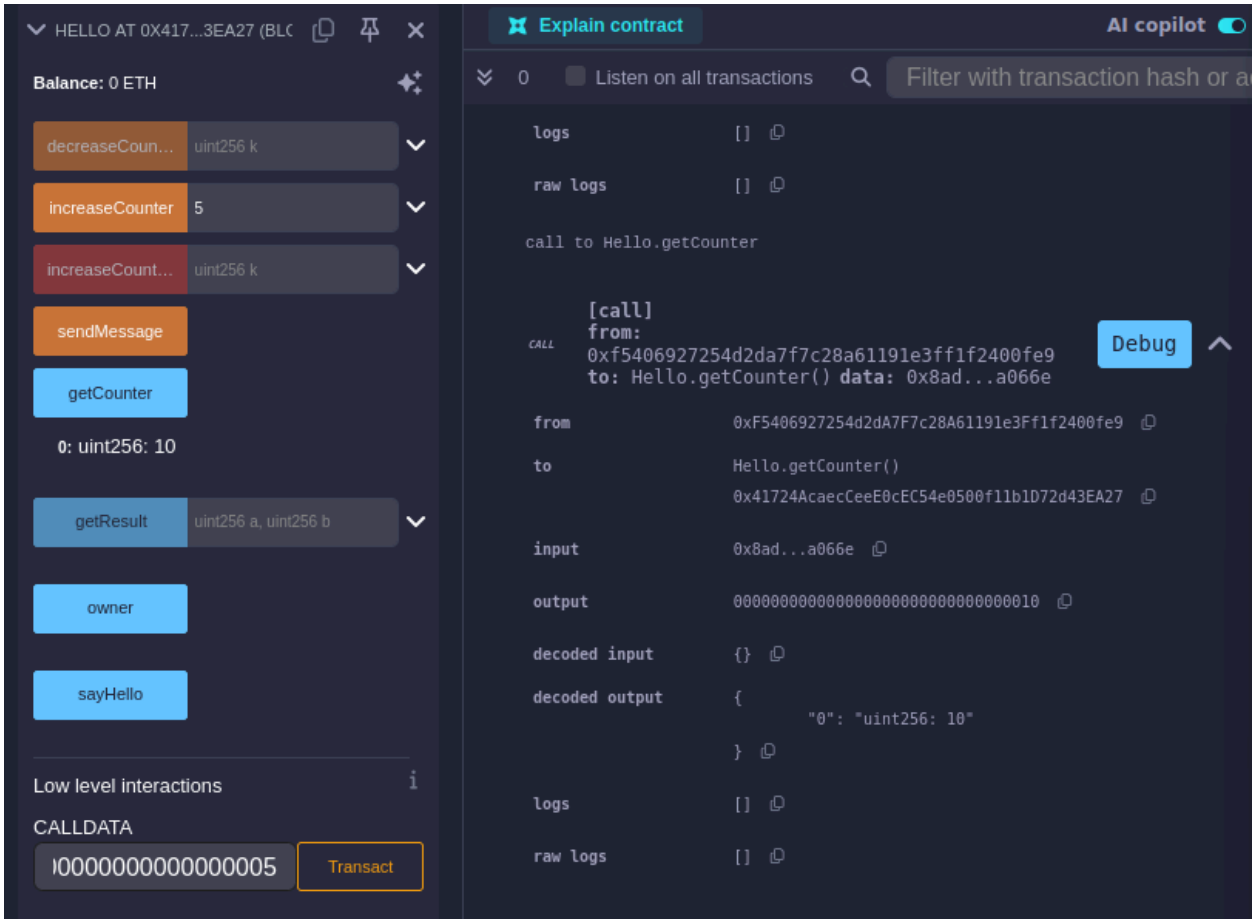
hash	0xfc11015fda8da0dffabbf3a954e30ba1fd0622ec3bbed113a332c21e410a64c7
type	2
accessList	
blockHash	0x58dddc3686891c0f7c93c6211e020ac700280e1fde8af2172d7ba184c699d35e
blockNumber	878
transactionIndex	0
confirmations	2
from	0xF5406927254d2dA7F7c28A61191e3Ff1f2400fe9
gasPrice	1000000007
maxPriorityFeePerGas	1000000007
maxFeePerGas	1000000007
gasLimit	43737
to	0x41724AcaecCeeE0cEC54e0500f11b1D72d43EA27
value	0
nonce	22
data	0x9e80c0740000000000000000000000000000000000000000000000000000000000000000
r	0x713634bd244f56ce29f71b8dc6d093cf0b7026027a5af19d50710cbc6e288152
s	0x086b63136b66227dea33b0d555d042f2773884a6e552f974a9da958a838550e2
v	0
creates	null
chainId	1337
wait	(omitted)

```
  GNU nano 4.8                    script.py
from web3 import Web3
hash = Web3.sha3(text="increaseCounter(uint256)")
print(hash.hex())
```

```
[11/30/25]seed@VM:~/.../contract$ nano script.py
[11/30/25]seed@VM:~/.../contract$ python3 script.py
/usr/lib/python3/dist-packages/requests/__init__.py:89: RequestsDep
endencyWarning: urllib3 (2.2.3) or chardet (3.0.4) doesn't match a
supported version!
  warnings.warn("urllib3 ({}) or chardet ({}) doesn't match a suppo
rted "
0x9e80c074933ed616d86c79d926a1dfd97afbe0ba20c42d692de450d20df14d77
```

As we can see 0x9e80c matches with the data field from EtherView

Now we try with low level instructions using 0x9e80c07400000000000000000000000000000000000000000000000000000000000000000000000000000005 as input



From this, we were able to successfully send a transaction to increase the counter by 5.

Task 2.d: Emit events

logs

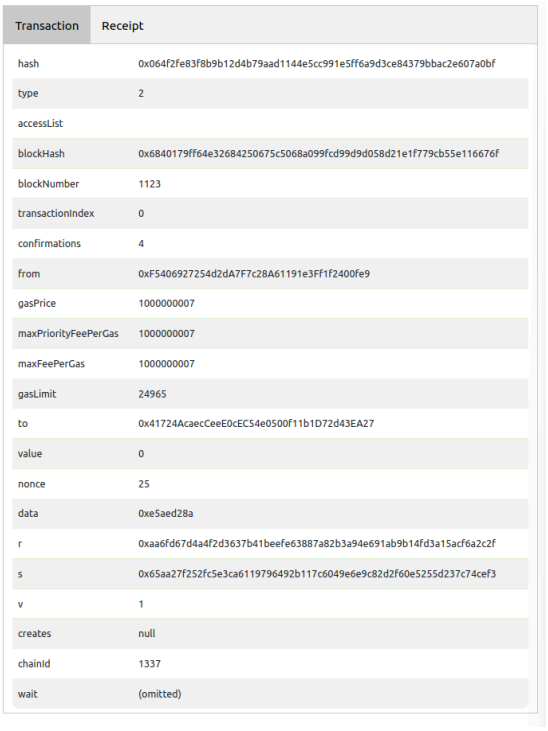

```
[
        {
                "from":
"0x41724AcaecCeeE0cEC54e0500f11b1D72d43EA27",
                "topic":
"0x8ff41ca1815f7eac6985bf4ba03a8cf43ca7fcd5354be9
797190a614f56b106c",
                "event": "MyMessage",
                "args": {
                        "0":
"0xF5406927254d2dA7F7c28A61191e3Ff1f2400fe9",
                        "1": "10"
                }
        }
]
```


raw logs


```
[
  {
    "_type": "log",
    "address":
"0x41724AcaecCeeE0cEC54e0500f11b1D72d43EA27",
    "blockHash":
"0x6840179ff64e32684250675c5068a099fcd99d9d058d21
e1f779cb55e116676f",
    "blockNumber": 1123,
    "data":
"0x0000000000000000000000000000000000000000000000
0000000000000000a",
    "index": 0,
    "topics": [

"0x8ff41ca1815f7eac6985bf4ba03a8cf43ca7fcd5354be9
797190a614f56b106c",

"0x000000000000000000000000f5406927254d2da7f7c28a
61191e3ff1f2400fe9"
    ],
    "transactionHash":
"0x064f2fe83f8b9b12d4b79aad1144e5cc991e5ff6a9d3ce
84379bbac2e607a0bf",
    "transactionIndex": 0
  }
]
```

Transaction | Receipt

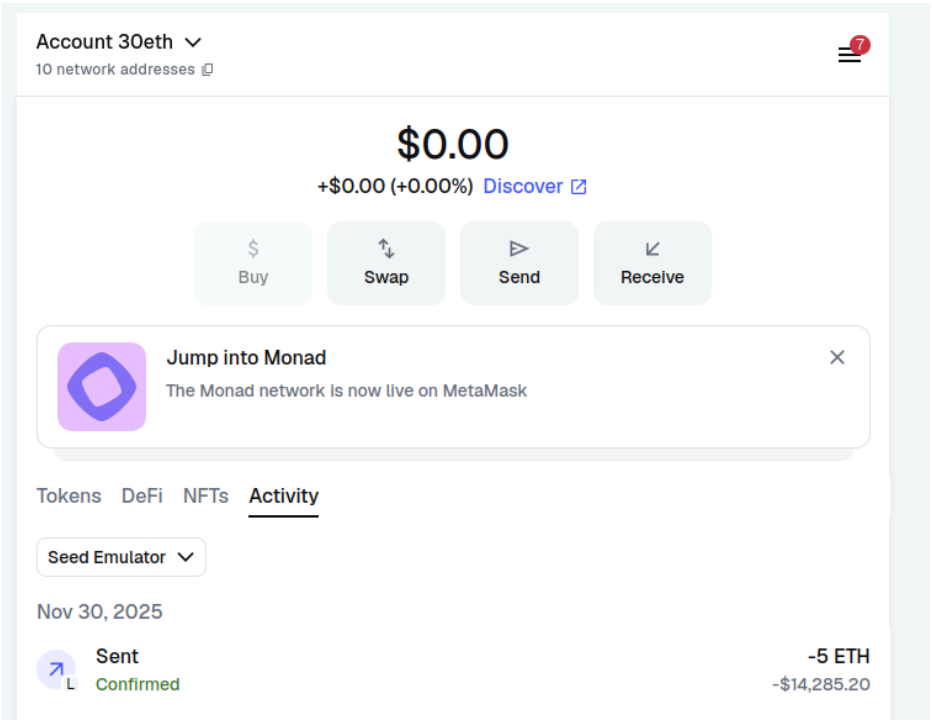
hash	0x064f2fe83f8b9b12d4b79aad1144e5cc991e5ff6a9d3ce84379bbac2e607a0bf
type	2
accessList	
blockHash	0x6840179ff64e32684250675c5068a099fcd99d9d058d21e1f779cb55e116676f
blockNumber	1123
transactionIndex	0
confirmations	4
from	0xF5406927254d2dA7F7c28A61191e3Ff1f2400fe9
gasPrice	1000000007
maxPriorityFeePerGas	1000000007
maxFeePerGas	1000000007
gasLimit	24965
to	0x41724AcaecCeeE0cEC54e0500f11b1D72d43EA27
value	0
nonce	25
data	0xe5aed28a
r	0xaa6fd67d4a4f2d3637b41beefe63887a82b3a94e691ab9b14fd3a15acf6a2c2f
s	0x65aa27f252fc5e3ca6119796492b117c6049e6e9c82d2f60e5255d237c74cef3
v	1
creates	null
chainId	1337
wait	(omitted)

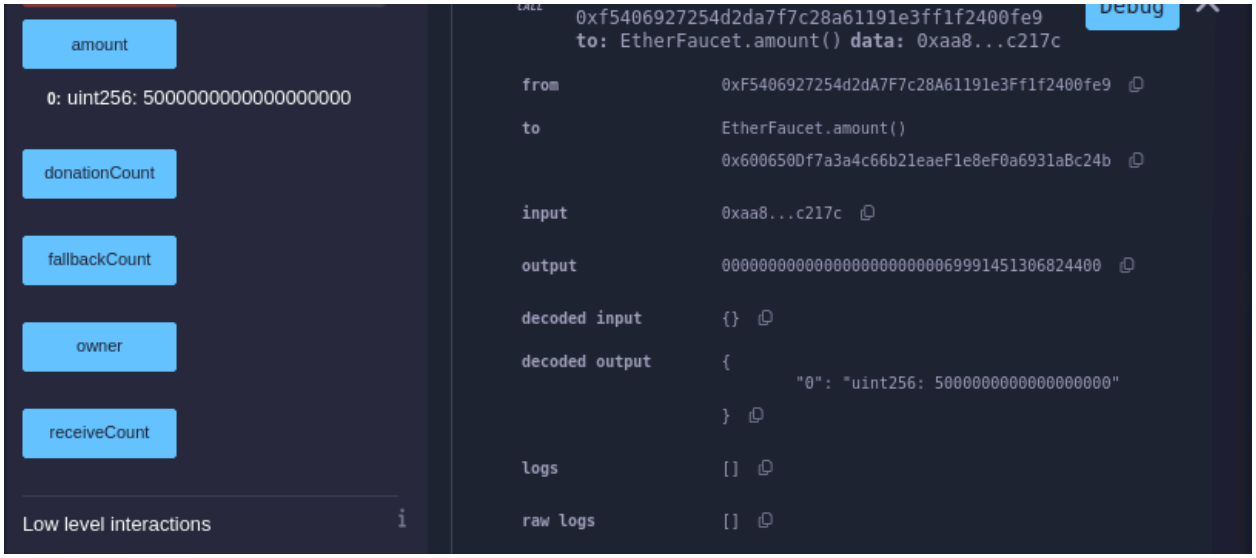
From this we can see the message logs and raw logs that remix produced.

Task 3: Send Fund to Contract

Task 3.a: Send fund directly to a contract address

Use EtherFaucet.sol, recompile and create a new contract





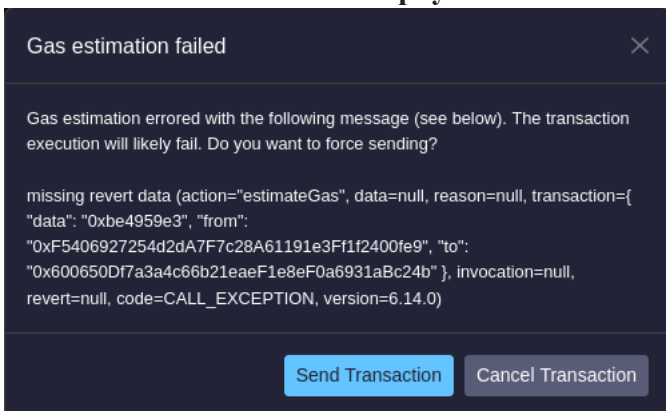
Transaction	Receipt
hash	0x1247cb2bf9207b6dc1823fd03c6c59d2baae46fa39ffd2c2fb7fef0f4498e1a3
type	2
accessList	
blockHash	0x4abd9e3dab9d24963ab3f448b9bb73a8c467dee877fbdbe21f38b7478b394e05
blockNumber	1227
transactionIndex	0
confirmations	17
from	0xF5406927254d2dA7F7c28A61191e3Ff1f2400fe9
gasPrice	1000000007
maxPriorityFeePerGas	1000000007
maxFeePerGas	1000000007
gasLimit	65305
to	0x600650Df7a3a4c66b21eaeF1e8eF0a6931aBc24b
value	5000000000000000000
nonce	27
data	0x
r	0x54886e5159423b0e9bc062caa45b0e540c003c80eb8554609d76490ef5147a1c
s	0x5f969df083076500859c68a90532c933f8689446e9e2eda98dd212a9eb72fdaa
v	0
creates	null
chainId	1337
wait	(omitted)

When removing receive(), we can see that Remix will say that it cannot receive any funds and cause an error. Since the smart contract can't receive outside funds.

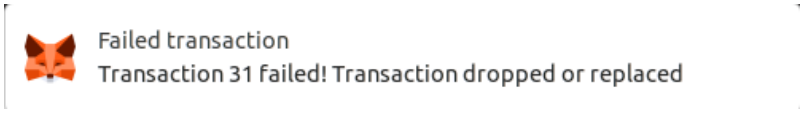
Task 3.b: Send fund to a payable function

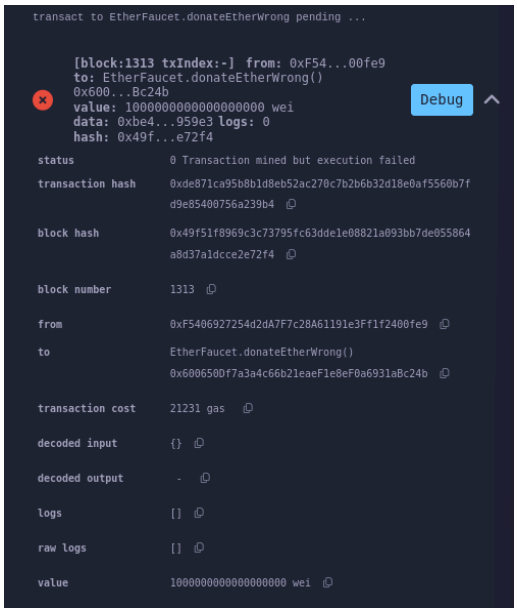
We can see that donationCount and amount have increased

Task 3.c: Send fund to a non-payable function



We get this error, but if we continue to still send the transaction, we can see that the transaction failed





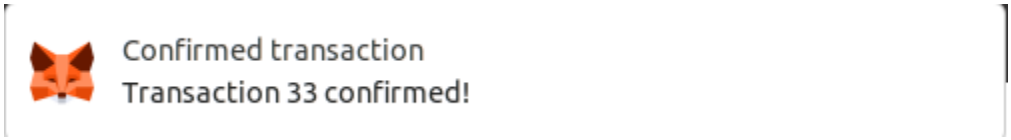
And that the transaction simply just got dropped and ignored.

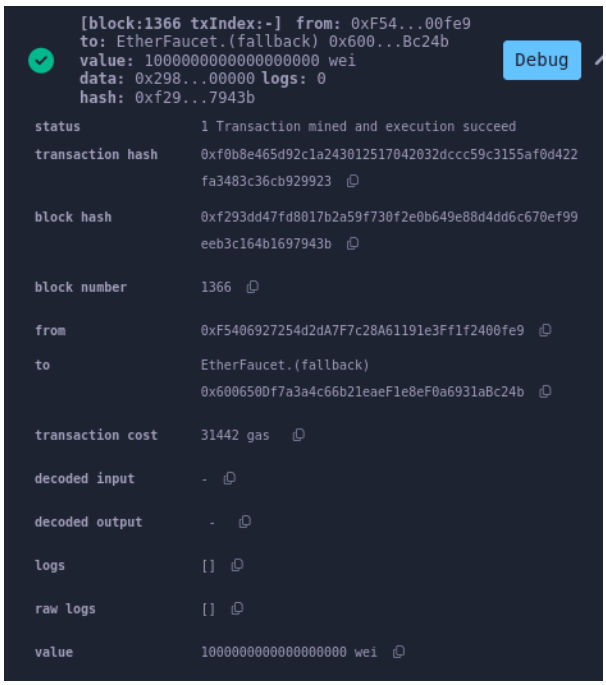
Task 3.d: Send fund to a non-existing function

```
  GNU nano 4.8                          script.py
from web3 import Web3
hash = Web3.sha3(text="foo()")
print(hash.hex())
```

```
[11/30/25]seed@VM:~/.../contract$ nano script.py
[11/30/25]seed@VM:~/.../contract$ python3 script.py
/usr/lib/python3/dist-packages/requests/__init__.py:89: RequestsDep
endencyWarning: urllib3 (2.2.3) or chardet (3.0.4) doesn't match a
supported version!
  warnings.warn("urllib3 ({}) or chardet ({}) doesn't match a suppo
rted "
0xc2985578b8f3b75f7dc66a767be2a4ef7d7c2224896a1c86e92ccf30bae678b7
```

Take the first 8 and rest with 0s
0x2985578b0000000000000000000000000000000000000000000000000000000000000000 as input
We can see that the transaction succeeded as it went to fallback





Task 4: Send Fund from Contract

First with getEtherViaCall

Where the balance went from 23 ETH to 24 ETH and the balance on the contract went from 7 ETH to 6 ETH

Next with getEtherViaSend

Similarly, the balance went from 24 ETH to 25 ETH and the balance on the contract went from 6 ETH to 5 ETH

Finally getEtherViaTransfer

Similarly, the balance went from 25 ETH to 26 ETH and the balance on the contract went from 5 ETH to 4 ETH

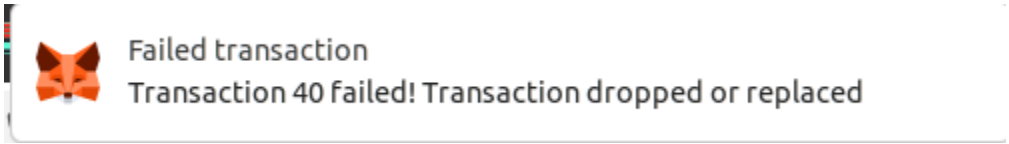
Task 5: Invoke Another Contract

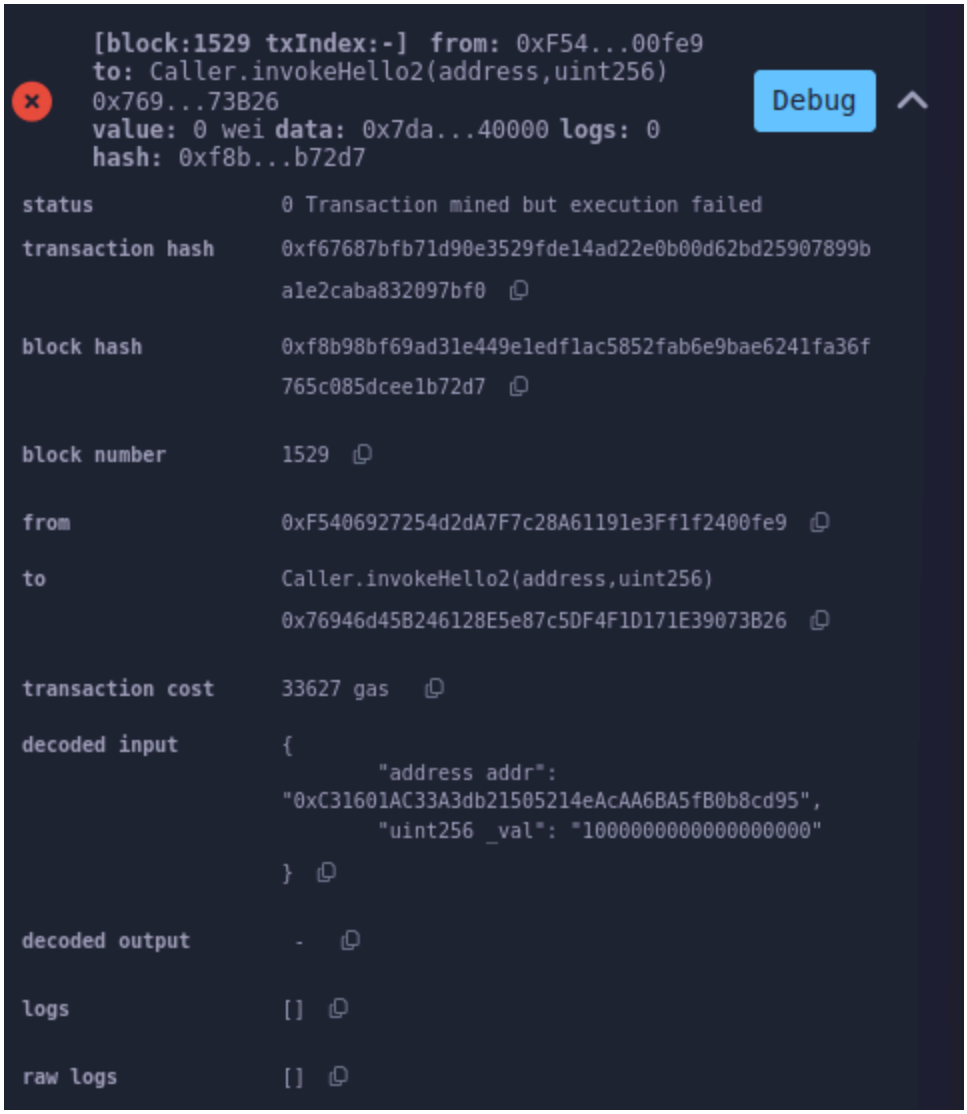
Use Caller.sol, recompile and create a new contract

First with invokeHello

We can see that the transaction succeeded and we were able to receive this output

Next with invokeHello2





We can see that it failed with invokeHello2