CCMP 606 – Orchestration of Cloud Resources

Assignment 2 Report

Instructor: **Yongchang He**

Student: **Hai Nam Nguyen – 000520322 – nguyen0465@saskpolytech.ca**

2023/2024 Winter Semester

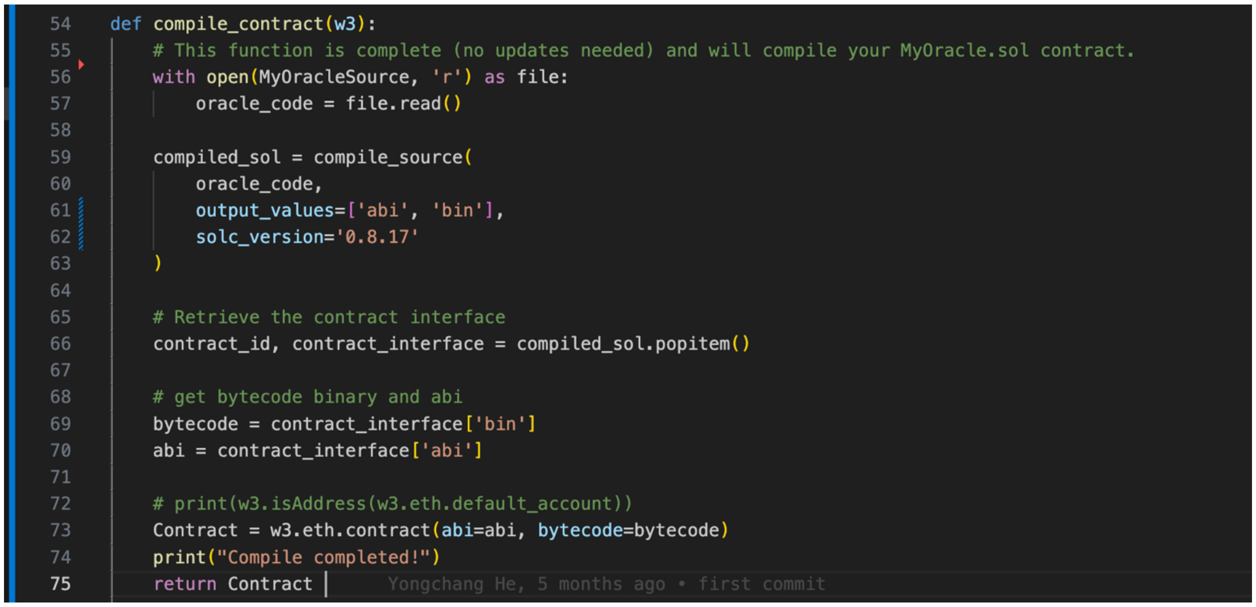
Saskatchewan Polytechnic

Submitted:

January 29th, 2024

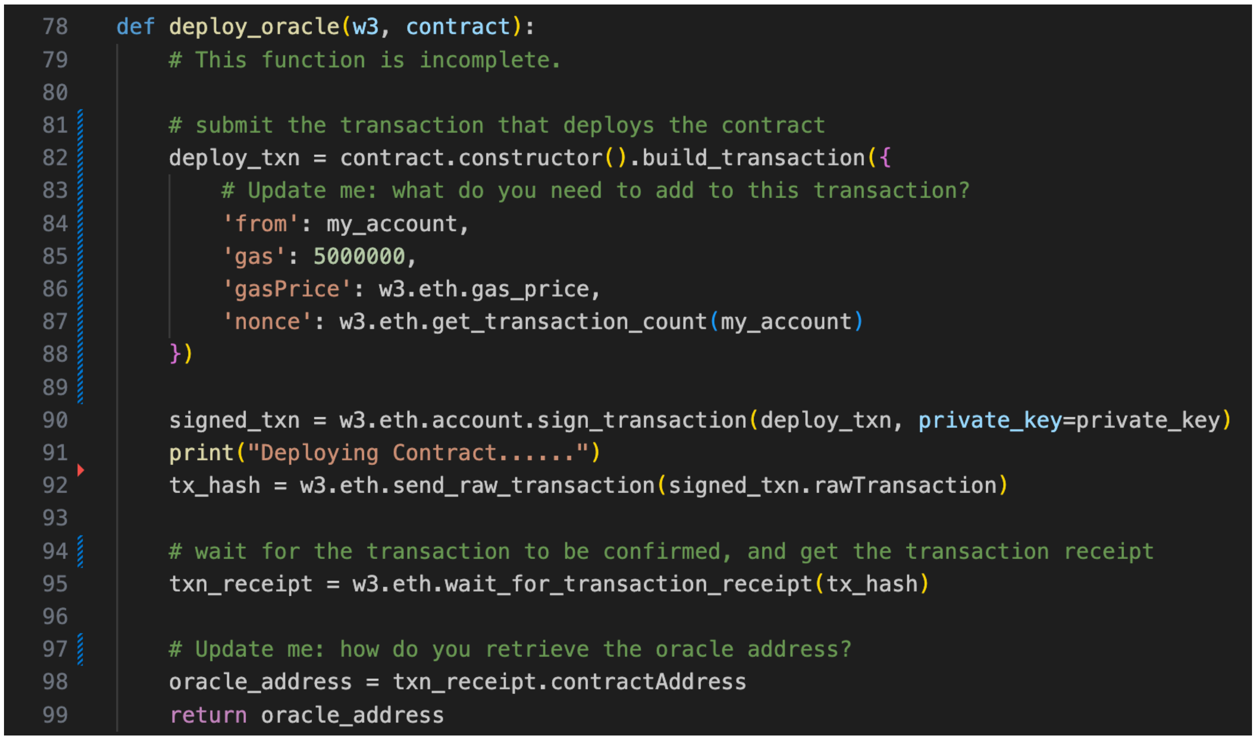
1. Smart Contract Compiled and Deployed

In the code, file **oracle-node.py**, line 54-75 is a function compile this contract. On line **62**, I have added **solc_version='0.8.17'** to matched with the version in the **main** function.



```
54  def compile_contract(w3):
55      # This function is complete (no updates needed) and will compile your MyOracle.sol contract.
56      with open(MyOracleSource, 'r') as file:
57          oracle_code = file.read()
58
59      compiled_sol = compile_source(
60          oracle_code,
61          output_values=['abi', 'bin'],
62          solc_version='0.8.17'
63      )
64
65      # Retrieve the contract interface
66      contract_id, contract_interface = compiled_sol.popitem()
67
68      # get bytecode binary and abi
69      bytecode = contract_interface['bin']
70      abi = contract_interface['abi']
71
72      # print(w3.isAddress(w3.eth.default_account))
73      Contract = w3.eth.contract(abi=abi, bytecode=bytecode)
74      print("Compile completed!")
75      return Contract        Yongchang He, 5 months ago • first commit
```

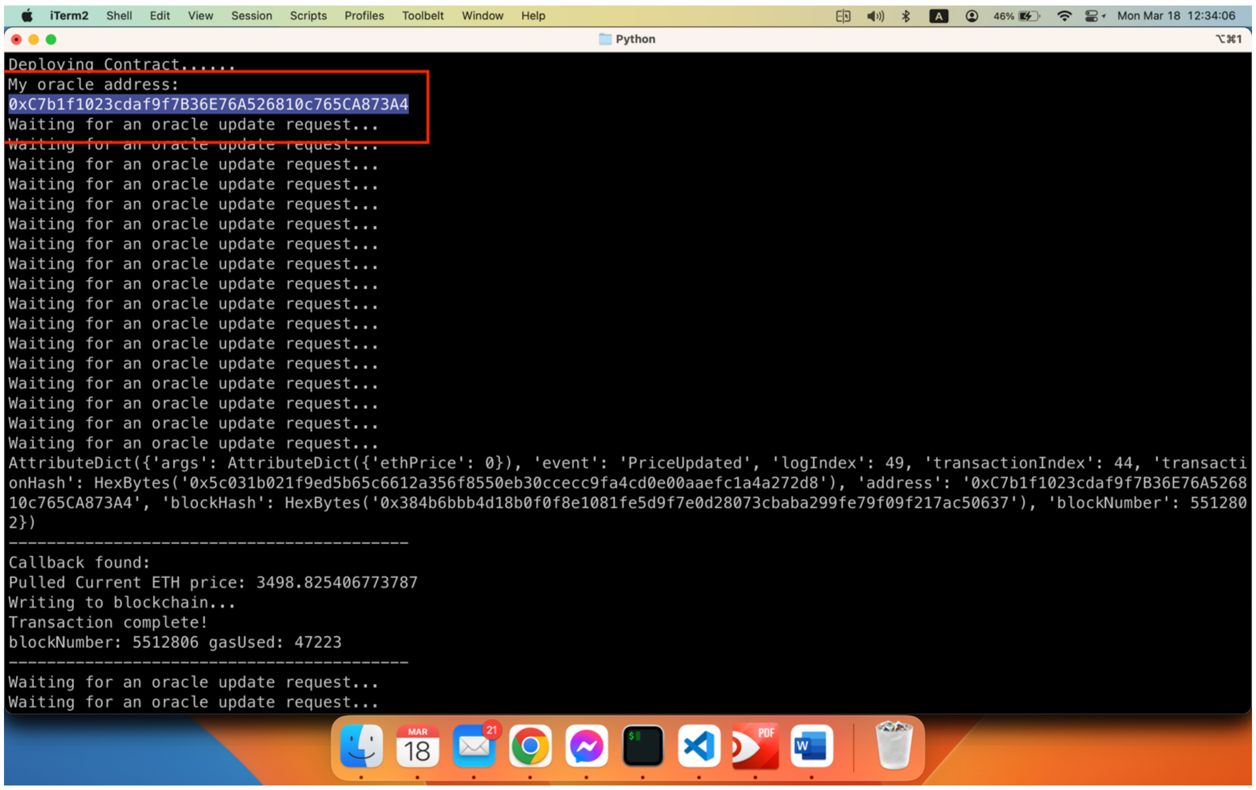
Line **78-99** is the one that use to deploy the contract, I have made some changes to make it work, such as added **'nonce'**.


```python
def deploy_oracle(w3, contract):
    # This function is incomplete.

    # submit the transaction that deploys the contract
    deploy_txn = contract.constructor().build_transaction({
        # Update me: what do you need to add to this transaction?
        'from': my_account,
        'gas': 5000000,
        'gasPrice': w3.eth.gas_price,
        'nonce': w3.eth.get_transaction_count(my_account)
    })

    signed_txn = w3.eth.account.sign_transaction(deploy_txn, private_key=private_key)
    print("Deploying Contract......")
    tx_hash = w3.eth.send_raw_transaction(signed_txn.rawTransaction)

    # wait for the transaction to be confirmed, and get the transaction receipt
    txn_receipt = w3.eth.wait_for_transaction_receipt(tx_hash)

    # Update me: how do you retrieve the oracle address?
    oracle_address = txn_receipt.contractAddress
    return oracle_address
```

The image below showed that my Smart Contract has been copiled after running `**python oracle-node.py**`, and deployed to Sepolia test network using my own credentials.

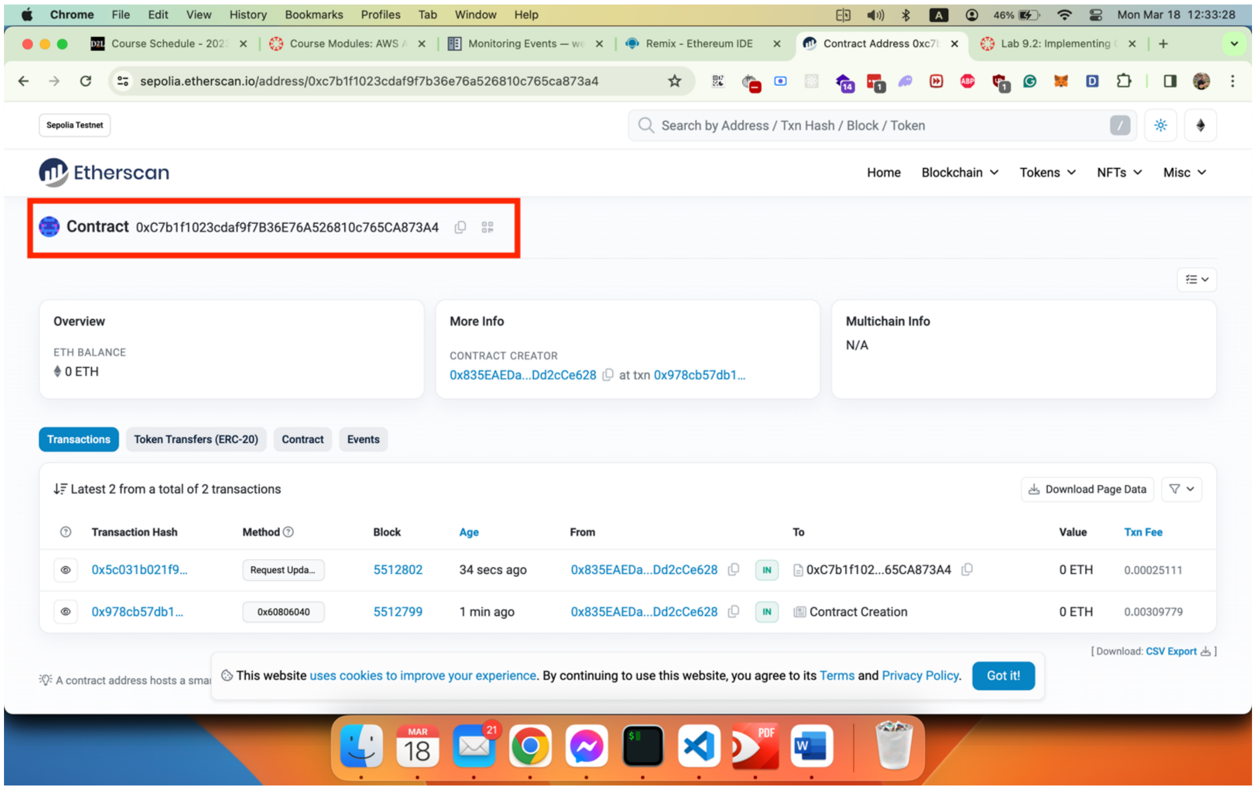
The address of this smart:

https://sepolia.etherscan.io/address/0xc7b1f1023cdaf9f7b36e76a526810c765ca873a4



```
Deploying Contract......
My oracle address:
0xC7b1f1023cdaf9f7B36E76A526810c765CA873A4
Waiting for an oracle update request...
Waiting for an oracle update request...
Waiting for an oracle update request...
Waiting for an oracle update request...
Waiting for an oracle update request...
Waiting for an oracle update request...
Waiting for an oracle update request...
Waiting for an oracle update request...
Waiting for an oracle update request...
Waiting for an oracle update request...
Waiting for an oracle update request...
Waiting for an oracle update request...
Waiting for an oracle update request...
Waiting for an oracle update request...
Waiting for an oracle update request...
Waiting for an oracle update request...
Waiting for an oracle update request...
AttributeDict({'args': AttributeDict({'ethPrice': 0}), 'event': 'PriceUpdated', 'logIndex': 49, 'transactionIndex': 44, 'transacti
onHash': HexBytes('0x5c031b021f9ed5b65c6612a356f8550eb30ccecc9fa4cd0e00aaefc1a4a272d8'), 'address': '0xC7b1f1023cdaf9f7B36E76A5268
10c765CA873A4', 'blockHash': HexBytes('0x384b6bbb4d18b0f0f8e1081fe5d9f7e0d28073cbaba299fe79f09f217ac50637'), 'blockNumber': 551280
2})
------------------------------------------
Callback found:
Pulled Current ETH price: 3498.825406773787
Writing to blockchain...
Transaction complete!
blockNumber: 5512806 gasUsed: 47223
------------------------------------------
Waiting for an oracle update request...
Waiting for an oracle update request...
```

Figure 1: Smart Contract compiled & deployed



sepolia.etherscan.io/address/0xC7b1f1023cdaf9f7b36e76a526810c765ca873a4

Contract 0xC7b1f1023cdaf9f7B36E76A526810c765CA873A4

Overview
ETH BALANCE
0 ETH

More Info
CONTRACT CREATOR
0x835EAEDa...Dd2cCe628 at txn 0x978cb57db1...

Multichain Info
N/A

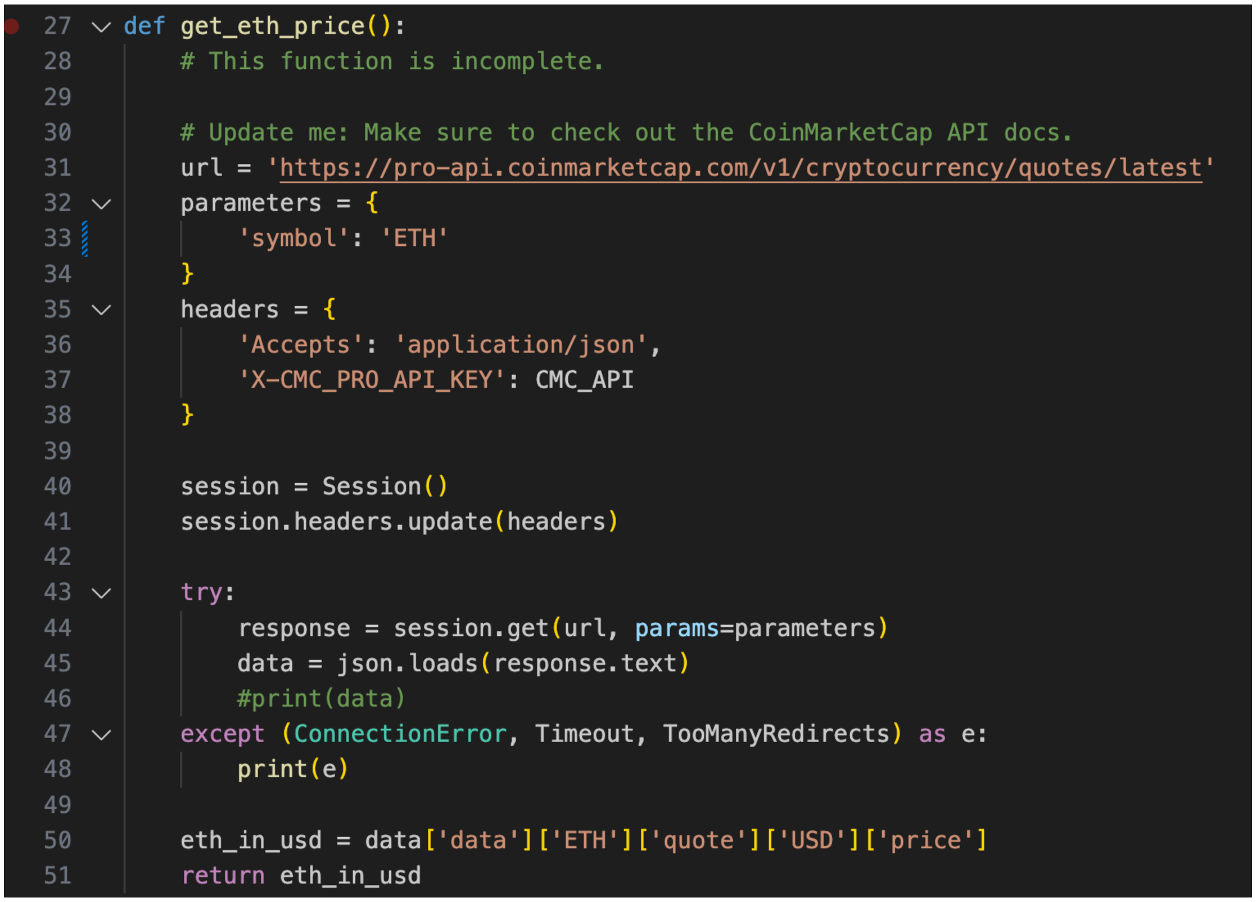
Latest 2 from a total of 2 transactions

Transaction Hash	Method	Block	Age	From		To	Value	Txn Fee
0x5c031b021f9...	Request Upda...	5512802	34 secs ago	0x835EAEDa...Dd2cCe628	IN	0xC7b1f102...65CA873A4	0 ETH	0.00025111
0x978cb57db1...	0x60806040	5512799	1 min ago	0x835EAEDa...Dd2cCe628	IN	Contract Creation	0 ETH	0.00309779

Figure 2: Smart contract information on Sepolia Test Network

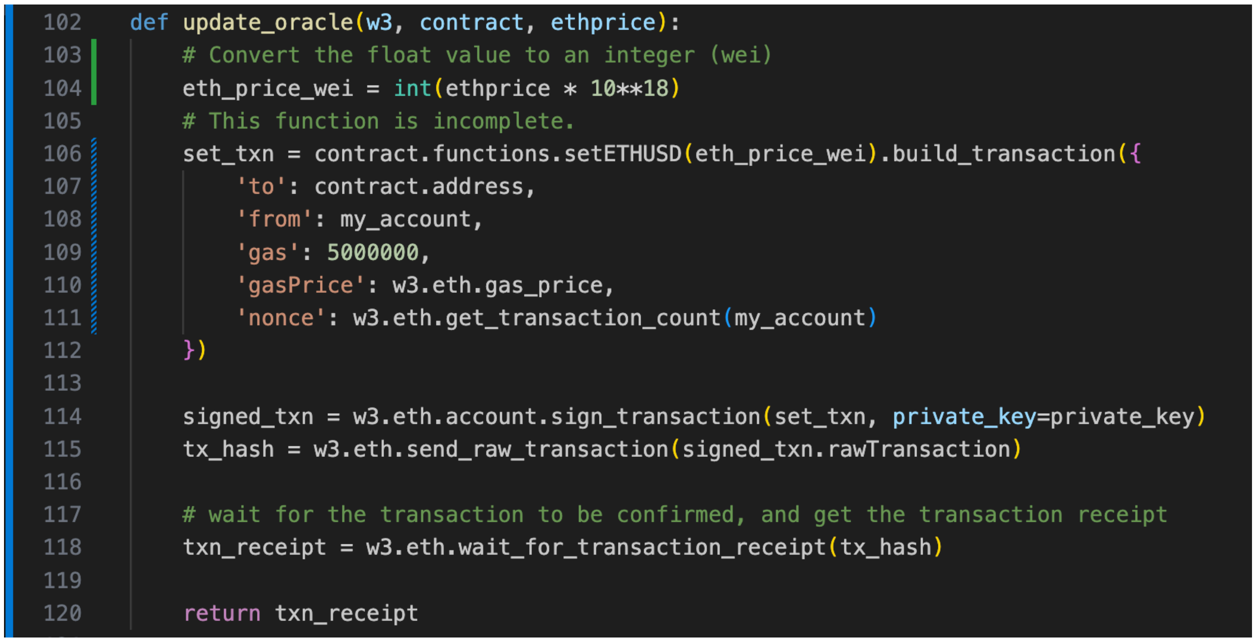
2. Oracle pulled new ETH price in USD and written it to the blockchain

The code in file **oracle-node.py** from line 27-51 is using to getting price of ETH in USD via CoinMarketcap API.



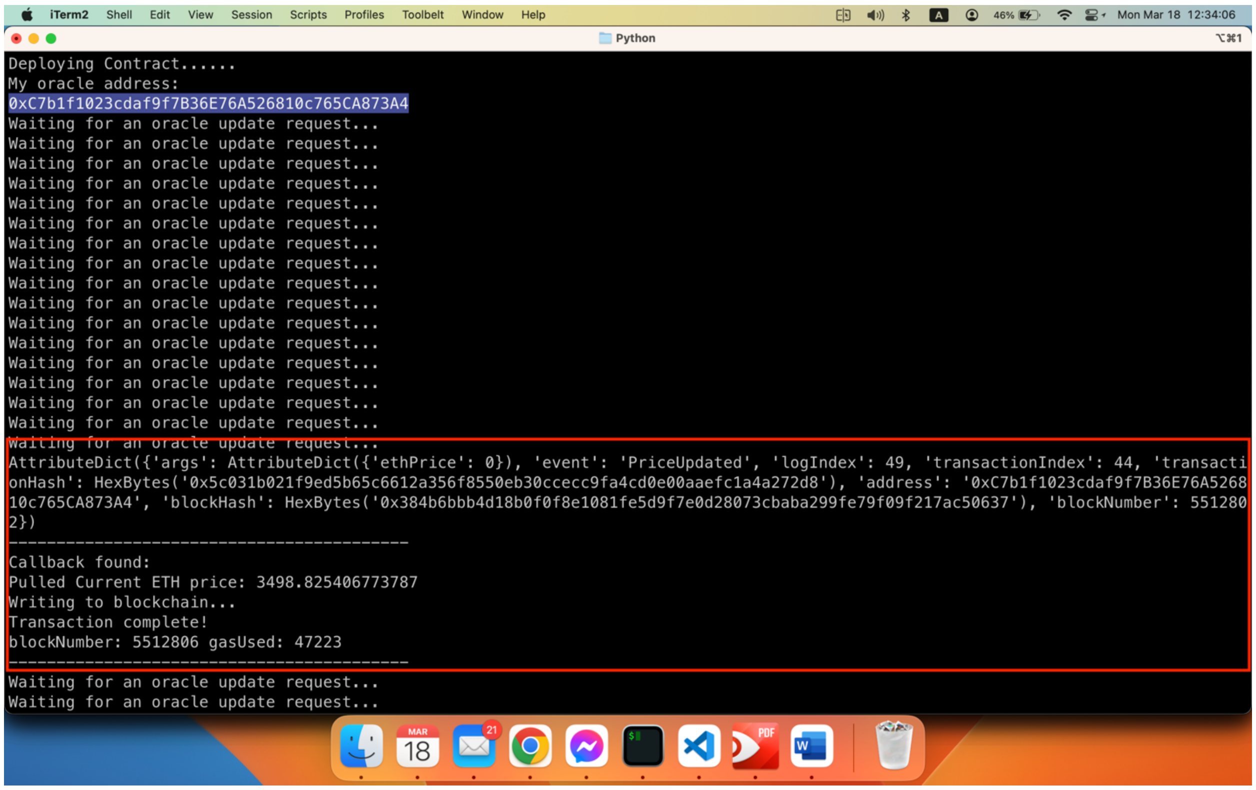
```
27  def get_eth_price():
28      # This function is incomplete.
29
30      # Update me: Make sure to check out the CoinMarketCap API docs.
31      url = 'https://pro-api.coinmarketcap.com/v1/cryptocurrency/quotes/latest'
32      parameters = {
33          'symbol': 'ETH'
34      }
35      headers = {
36          'Accepts': 'application/json',
37          'X-CMC_PRO_API_KEY': CMC_API
38      }
39
40      session = Session()
41      session.headers.update(headers)
42
43      try:
44          response = session.get(url, params=parameters)
45          data = json.loads(response.text)
46          #print(data)
47      except (ConnectionError, Timeout, TooManyRedirects) as e:
48          print(e)
49
50      eth_in_usd = data['data']['ETH']['quote']['USD']['price']
51      return eth_in_usd
```

Line **102-120** is using to write it to the blockchain.



```python
def update_oracle(w3, contract, ethprice):
    # Convert the float value to an integer (wei)
    eth_price_wei = int(ethprice * 10**18)
    # This function is incomplete.
    set_txn = contract.functions.setETHUSD(eth_price_wei).build_transaction({
        'to': contract.address,
        'from': my_account,
        'gas': 5000000,
        'gasPrice': w3.eth.gas_price,
        'nonce': w3.eth.get_transaction_count(my_account)
    })

    signed_txn = w3.eth.account.sign_transaction(set_txn, private_key=private_key)
    tx_hash = w3.eth.send_raw_transaction(signed_txn.rawTransaction)

    # wait for the transaction to be confirmed, and get the transaction receipt
    txn_receipt = w3.eth.wait_for_transaction_receipt(tx_hash)

    return txn_receipt
```

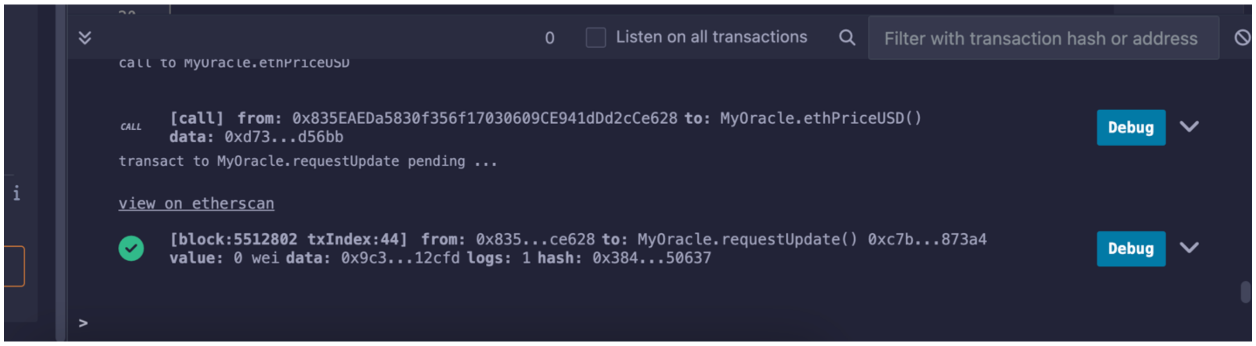
The image below showed that my function is working to receive the event on blockchain:



iTerm2 Shell Edit View Session Scripts Profiles Toolbelt Window Help
46% Mon Mar 18 12:34:06
Python
⌥⌘1

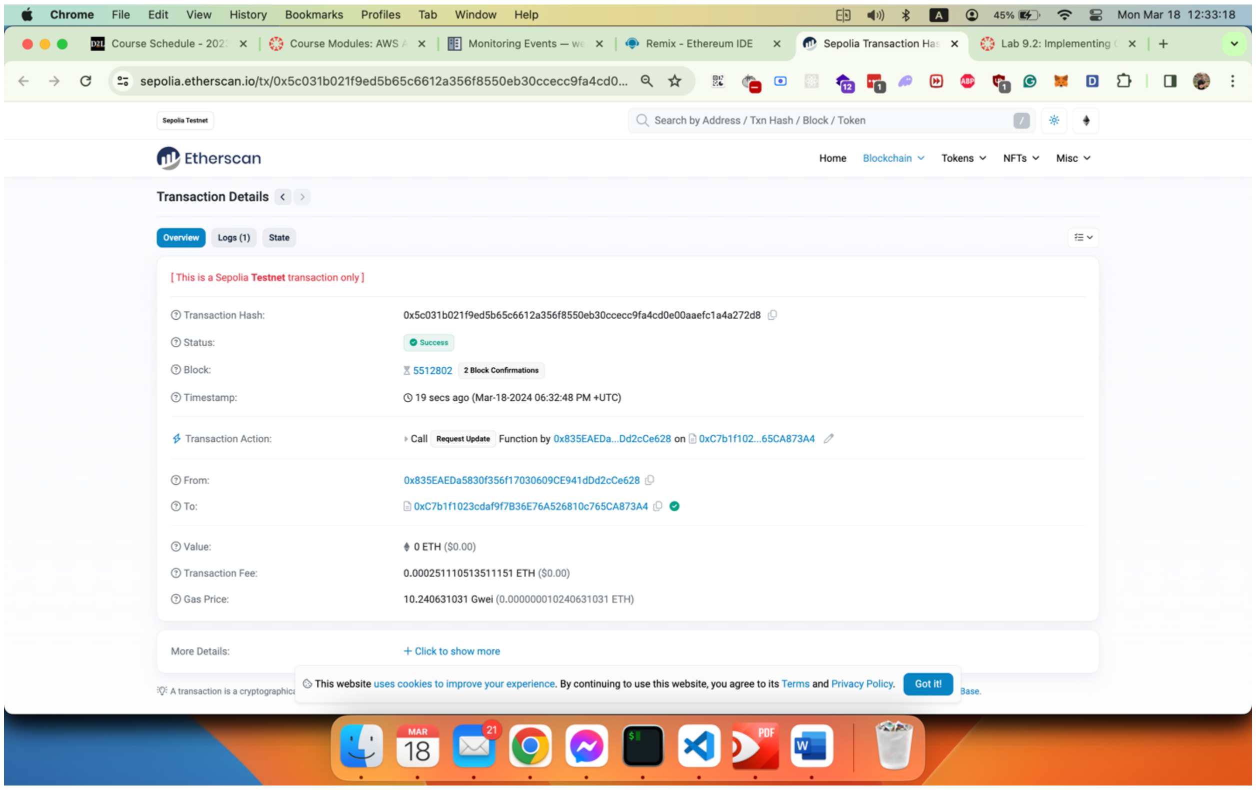
```
Deploying Contract......
My oracle address:
0xC7b1f1023cdaf9f7B36E76A526810c765CA873A4
Waiting for an oracle update request...
Waiting for an oracle update request...
Waiting for an oracle update request...
Waiting for an oracle update request...
Waiting for an oracle update request...
Waiting for an oracle update request...
Waiting for an oracle update request...
Waiting for an oracle update request...
Waiting for an oracle update request...
Waiting for an oracle update request...
Waiting for an oracle update request...
Waiting for an oracle update request...
Waiting for an oracle update request...
Waiting for an oracle update request...
Waiting for an oracle update request...
Waiting for an oracle update request...
Waiting for an oracle update request...
AttributeDict({'args': AttributeDict({'ethPrice': 0}), 'event': 'PriceUpdated', 'logIndex': 49, 'transactionIndex': 44, 'transacti
onHash': HexBytes('0x5c031b021f9ed5b65c6612a356f8550eb30ccecc9fa4cd0e00aaefc1a4a272d8'), 'address': '0xC7b1f1023cdaf9f7B36E76A5268
10c765CA873A4', 'blockHash': HexBytes('0x384b6bbb4d18b0f0f8e1081fe5d9f7e0d28073cbaba299fe79f09f217ac50637'), 'blockNumber': 551280
2})
------------------------------------------
Callback found:
Pulled Current ETH price: 3498.825406773787
Writing to blockchain...
Transaction complete!
blockNumber: 5512806 gasUsed: 47223
------------------------------------------
Waiting for an oracle update request...
Waiting for an oracle update request...
```

The images below are evidence of the **requestUpdate** requested:



```
call to MyOracle.ethPriceUSD

CALL   [call] from: 0x835EAEDa5830f356f17030609CE941dDd2cCe628 to: MyOracle.ethPriceUSD()
       data: 0xd73...d56bb
transact to MyOracle.requestUpdate pending ...

view on etherscan

✓      [block:5512802 txIndex:44] from: 0x835...ce628 to: MyOracle.requestUpdate() 0xc7b...873a4
       value: 0 wei data: 0x9c3...12cfd logs: 1 hash: 0x384...50637
```

Listen on all transactions
Filter with transaction hash or address
Debug
Debug



sepolia.etherscan.io/tx/0x5c031b021f9ed5b65c6612a356f8550eb30ccecc9fa4cd0...

Transaction Details

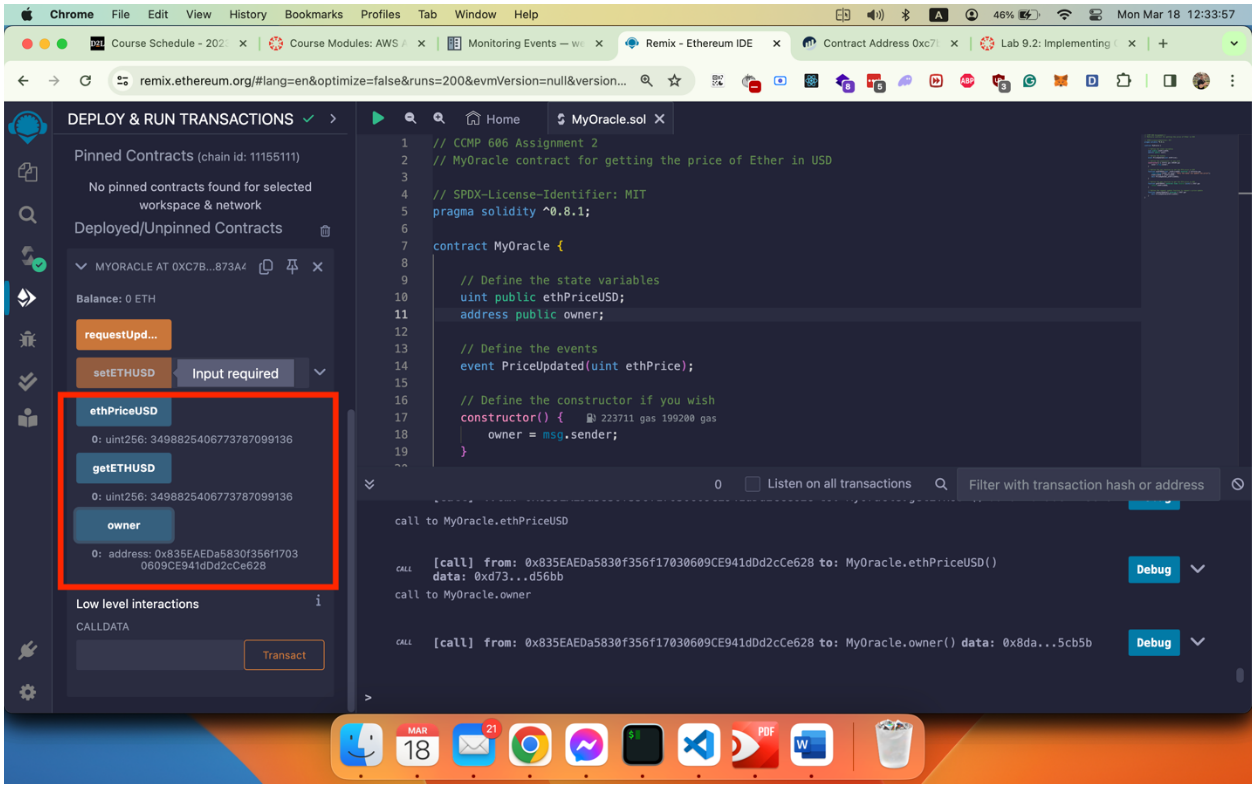
[This is a Sepolia **Testnet** transaction only]

Transaction Hash:	0x5c031b021f9ed5b65c6612a356f8550eb30ccecc9fa4cd0e00aaefc1a4a272d8
Status:	Success
Block:	5512802 2 Block Confirmations
Timestamp:	19 secs ago (Mar-18-2024 06:32:48 PM +UTC)
Transaction Action:	Call Request Update Function by 0x835EAEDa...Dd2cCe628 on 0xC7b1f102...65CA873A4
From:	0x835EAEDa5830f356f17030609CE941dDd2cCe628
To:	0xC7b1f1023cdaf9f7B36E76A526810c765CA873A4
Value:	0 ETH ($0.00)
Transaction Fee:	0.000251110513511151 ETH ($0.00)
Gas Price:	10.240631031 Gwei (0.000000010240631031 ETH)
More Details:	+ Click to show more

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

3. ETH Price in USD using the state variable

The image below shows that the price in USD using state variable which invoked after the Smart Contract compiled, deployed, and updated the price:



Pinned Contracts (chain id: 11155111)

No pinned contracts found for selected workspace & network

Deployed/Unpinned Contracts

MYORACLE AT 0XC7B...873A4

Balance: 0 ETH

requestUpd...

setETHUSD — Input required

ethPriceUSD

0: uint256: 3498825406773787099136

getETHUSD

0: uint256: 3498825406773787099136

owner

0: address: 0x835EAEDa5830f356f17030609CE941dDd2cCe628

Low level interactions

CALLDATA

Transact

```solidity
// CCMP 606 Assignment 2
// MyOracle contract for getting the price of Ether in USD

// SPDX-License-Identifier: MIT
pragma solidity ^0.8.1;

contract MyOracle {

    // Define the state variables
    uint public ethPriceUSD;
    address public owner;

    // Define the events
    event PriceUpdated(uint ethPrice);

    // Define the constructor if you wish
    constructor() {     223711 gas 199200 gas
        owner = msg.sender;
    }
```

```
call to MyOracle.ethPriceUSD

CALL  [call] from: 0x835EAEDa5830f356f17030609CE941dDd2cCe628 to: MyOracle.ethPriceUSD()
      data: 0xd73...d56bb
call to MyOracle.owner

CALL  [call] from: 0x835EAEDa5830f356f17030609CE941dDd2cCe628 to: MyOracle.owner() data: 0x8da...5cb5b

>
```