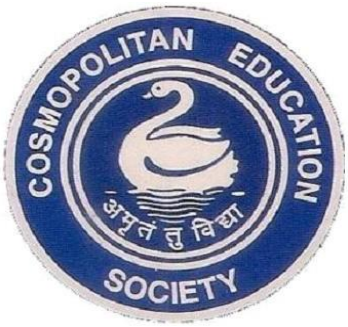
VALIA C.I. COLLEGE OF COMMERCE & VALIA LC COLLEGE OF ARTS
CES ROAD D.N NAGAR

(Affiliated to University Of Mumbai)

Mumbai-Maharashtra-400053

DEPARTMENT OF INFORMATION TECHNOLOGY



CERTIFICATE

This is to certify that the Journal entitled **BlockChain** is bonafied work of **GOVIND SAINI** bearing Roll No: **07** submitted in partial fulfillment of the requirements for the award of degree of **MASTER OF SCIENCE in INFORMATION TECHNOLOGY** from University of Mumbai.

Date: **Internal Guide**

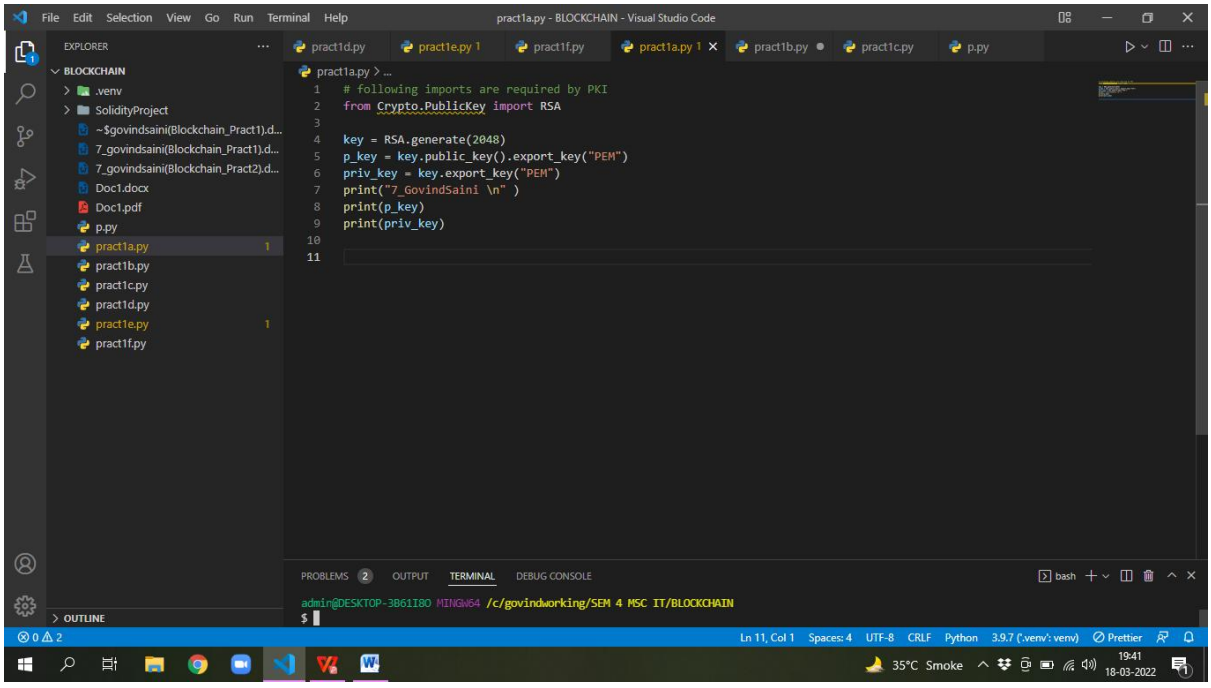
INDEX

Practical No : 1

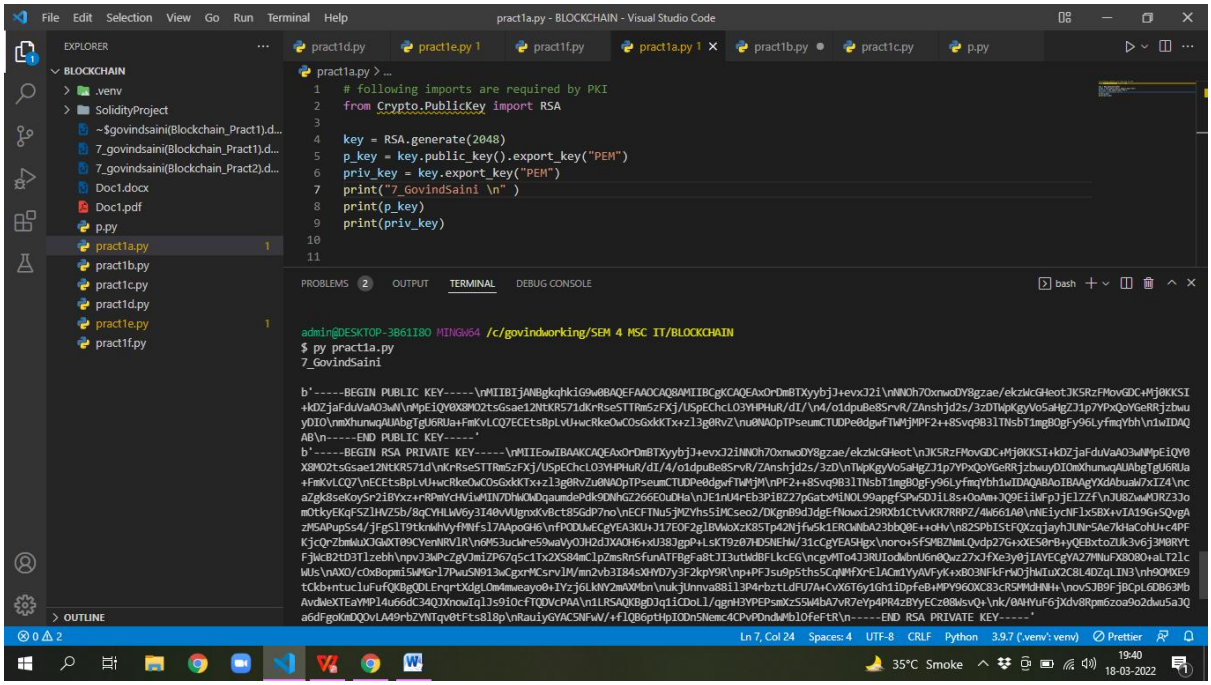
Aim : Write the following programs for Blockchain in Python.

1a) A simple client class that generates the private and public keys by using the built in Python RSA algorithm and test it.

Code:

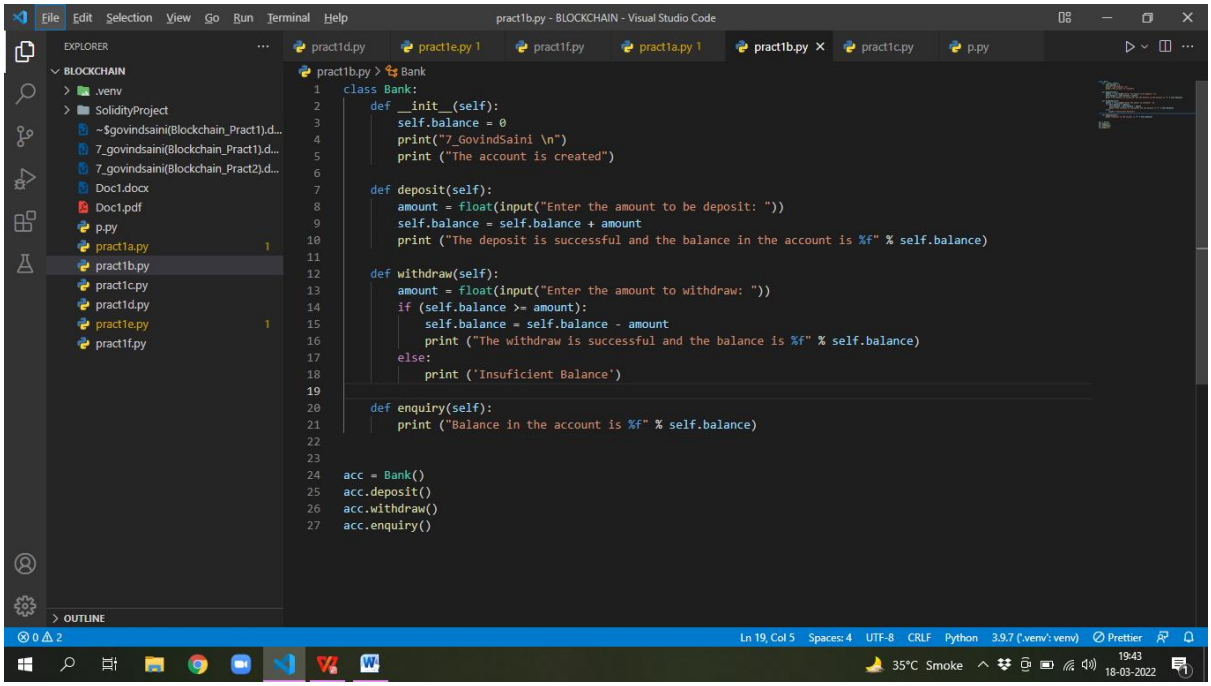


Output :



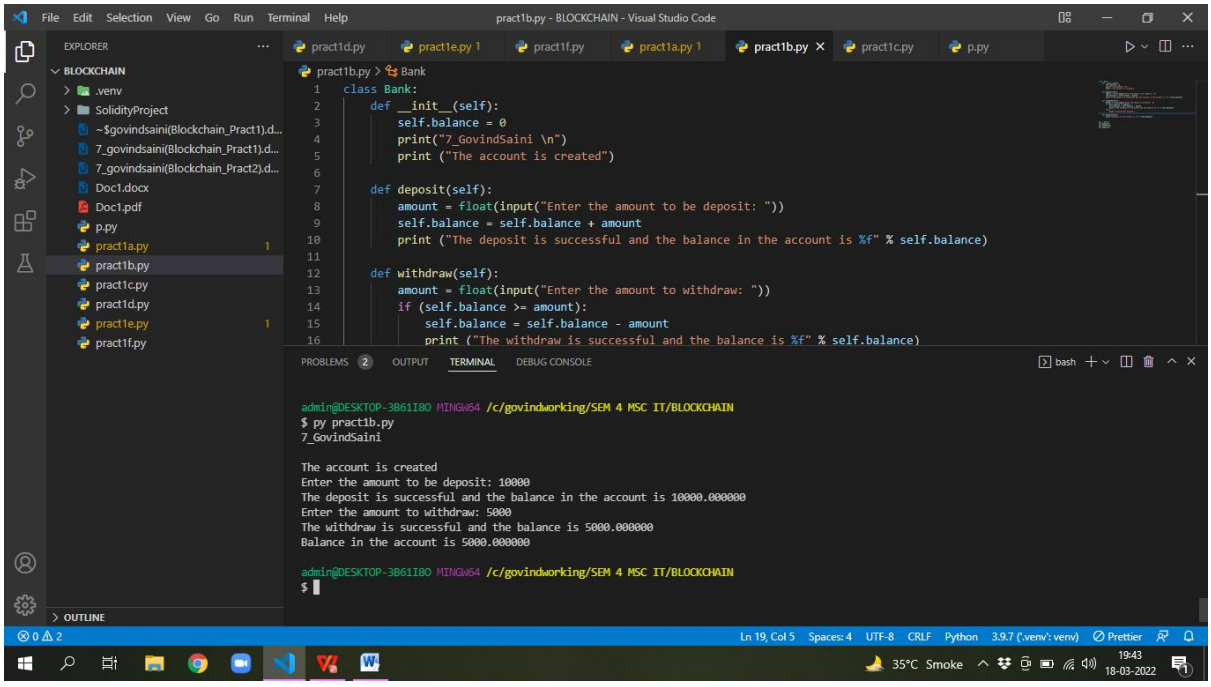
1b) A transaction class to send and receive money and test it.

Code:



```
class Bank:
    def __init__(self):
        self.balance = 0
        print("7_GovindSaini \n")
        print ("The account is created")

    def deposit(self):
        amount = float(input("Enter the amount to be deposit: "))
        self.balance = self.balance + amount
        print ("The deposit is successful and the balance in the account is %f" % self.balance)

    def withdraw(self):
        amount = float(input("Enter the amount to withdraw: "))
        if (self.balance >= amount):
            self.balance = self.balance - amount
            print ("The withdraw is successful and the balance is %f" % self.balance)
        else:
            print ('Insuficient Balance')

    def enquiry(self):
        print ("Balance in the account is %f" % self.balance)


acc = Bank()
acc.deposit()
acc.withdraw()
acc.enquiry()
```

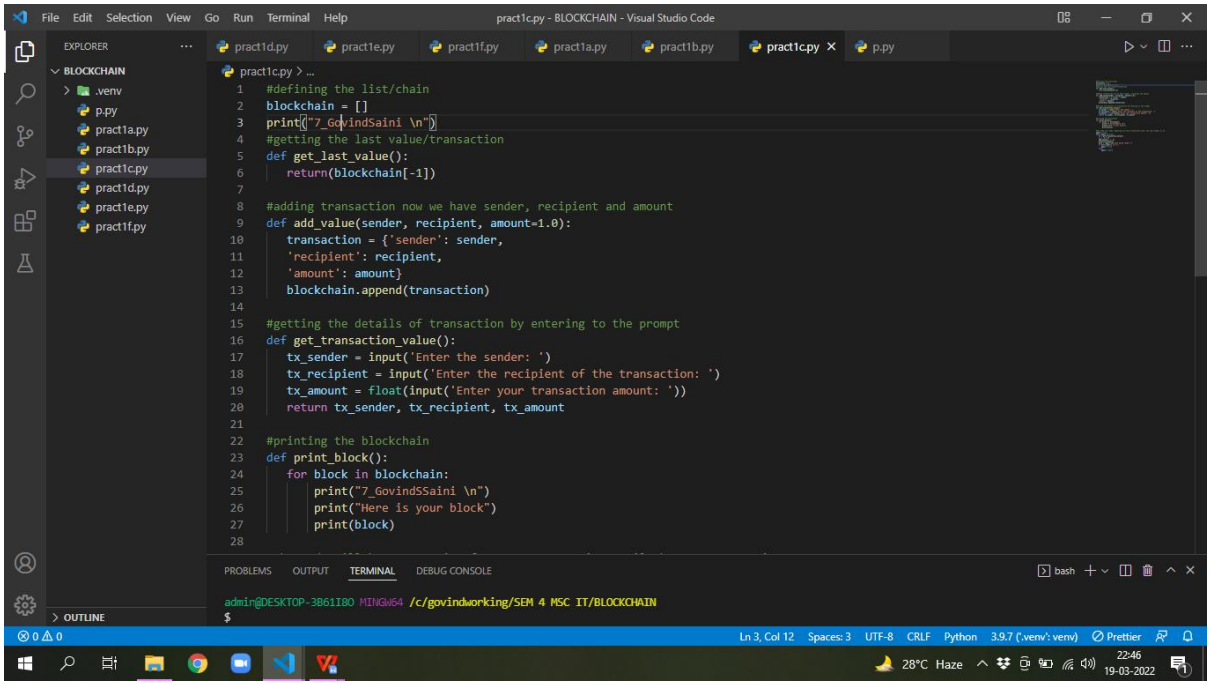
Output:

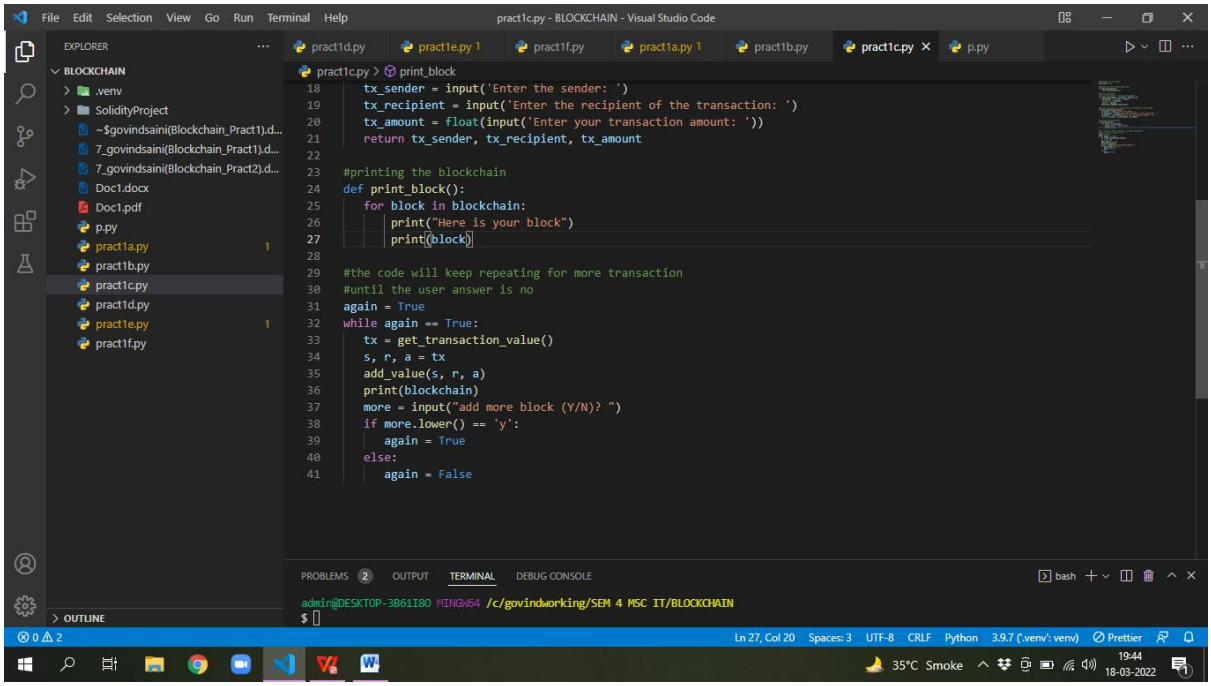


```
admin@DESKTOP-3B61I8O MINGW64 /c/govindworking/SEM 4 MSC IT/BLOCKCHAIN
$ py pract1b.py
7_GovindSaini

The account is created
Enter the amount to be deposit: 10000
The deposit is successful and the balance in the account is 10000.000000
Enter the amount to withdraw: 5000
The withdraw is successful and the balance is 5000.000000
Balance in the account is 5000.000000

admin@DESKTOP-3B61I8O MINGW64 /c/govindworking/SEM 4 MSC IT/BLOCKCHAIN
$
```

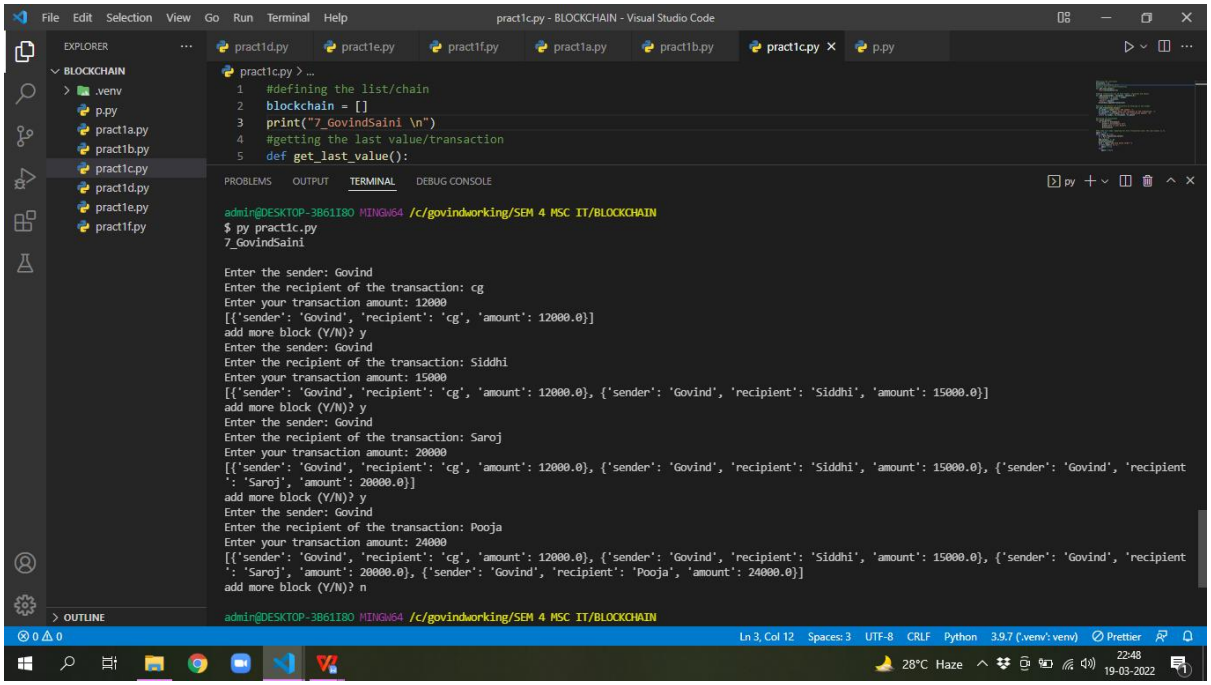
1c) Create Multiple Transaction and display them.

Code :


File Edit Selection View Go Run Terminal Help
pract1c.py - BLOCKCHAIN - Visual Studio Code
EXPLORER
BLOCKCHAIN
.venv
p.py
pract1a.py
pract1b.py
pract1c.py
pract1d.py
pract1e.py
pract1f.py
pract1d.py pract1e.py pract1f.py pract1a.py pract1b.py pract1c.py p.py
pract1c.py > ...
#defining the list/chain
blockchain = []
print("7_GovindSaini \n")
#getting the last value/transaction
def get_last_value():
return(blockchain[-1])
#adding transaction now we have sender, recipient and amount
def add_value(sender, recipient, amount=1.0):
transaction = {'sender': sender,
'recipient': recipient,
'amount': amount}
blockchain.append(transaction)
#getting the details of transaction by entering to the prompt
def get_transaction_value():
tx_sender = input('Enter the sender: ')
tx_recipient = input('Enter the recipient of the transaction: ')
tx_amount = float(input('Enter your transaction amount: '))
return tx_sender, tx_recipient, tx_amount
#printing the blockchain
def print_block():
for block in blockchain:
print("7_GovindSSaini \n")
print("Here is your block")
print(block)
PROBLEMS OUTPUT TERMINAL DEBUG CONSOLE
bash
admin@DESKTOP-3B61I8O MINGW64 /c/govindworking/SEM 4 MSC IT/BLOCKCHAIN
$
OUTLINE
Ln 3, Col 12 Spaces: 3 UTF-8 CRLF Python 3.9.7 ('.venv': venv) Prettier
28°C Haze
22:46
19-03-2022

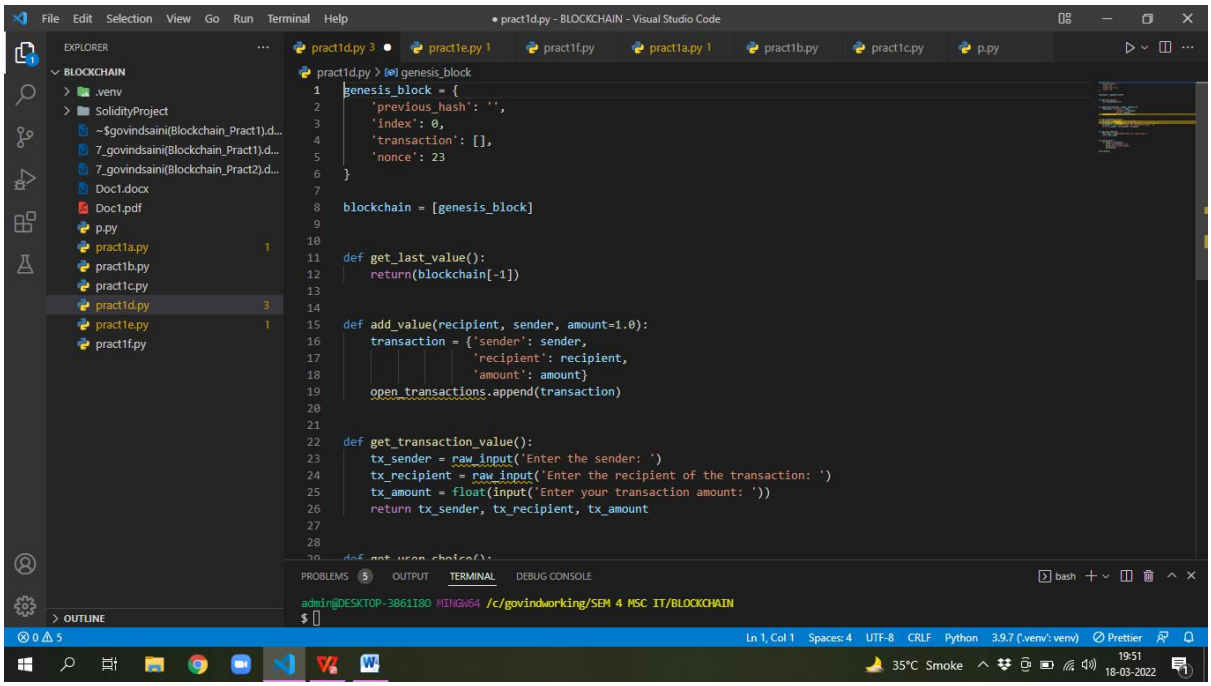

File Edit Selection View Go Run Terminal Help
pract1c.py - BLOCKCHAIN - Visual Studio Code
EXPLORER
BLOCKCHAIN
.venv
SolidityProject
~$govindsaini(Blockchain_Pract1).d...
7_govindsaini(Blockchain_Pract1).d...
7_govindsaini(Blockchain_Pract2).d...
Doc1.docx
Doc1.pdf
p.py
pract1a.py
pract1b.py
pract1c.py
pract1d.py
pract1e.py
pract1f.py
pract1d.py pract1e.py 1 pract1f.py pract1a.py 1 pract1b.py pract1c.py p.py
pract1c.py > print_block
tx_sender = input('Enter the sender: ')
tx_recipient = input('Enter the recipient of the transaction: ')
tx_amount = float(input('Enter your transaction amount: '))
return tx_sender, tx_recipient, tx_amount
#printing the blockchain
def print_block():
for block in blockchain:
print("Here is your block")
print(block)
#the code will keep repeating for more transaction
#until the user answer is no
again = True
while again == True:
tx = get_transaction_value()
s, r, a = tx
add_value(s, r, a)
print(blockchain)
more = input("add more block (Y/N)? ")
if more.lower() == 'y':
again = True
else:
again = False
PROBLEMS 2 OUTPUT TERMINAL DEBUG CONSOLE
bash
admin@DESKTOP-3B61I8O MINGW64 /c/govindworking/SEM 4 MSC IT/BLOCKCHAIN
$
OUTLINE
Ln 27, Col 20 Spaces: 3 UTF-8 CRLF Python 3.9.7 ('.venv': venv) Prettier
35°C Smoke
19:44
18-03-2022

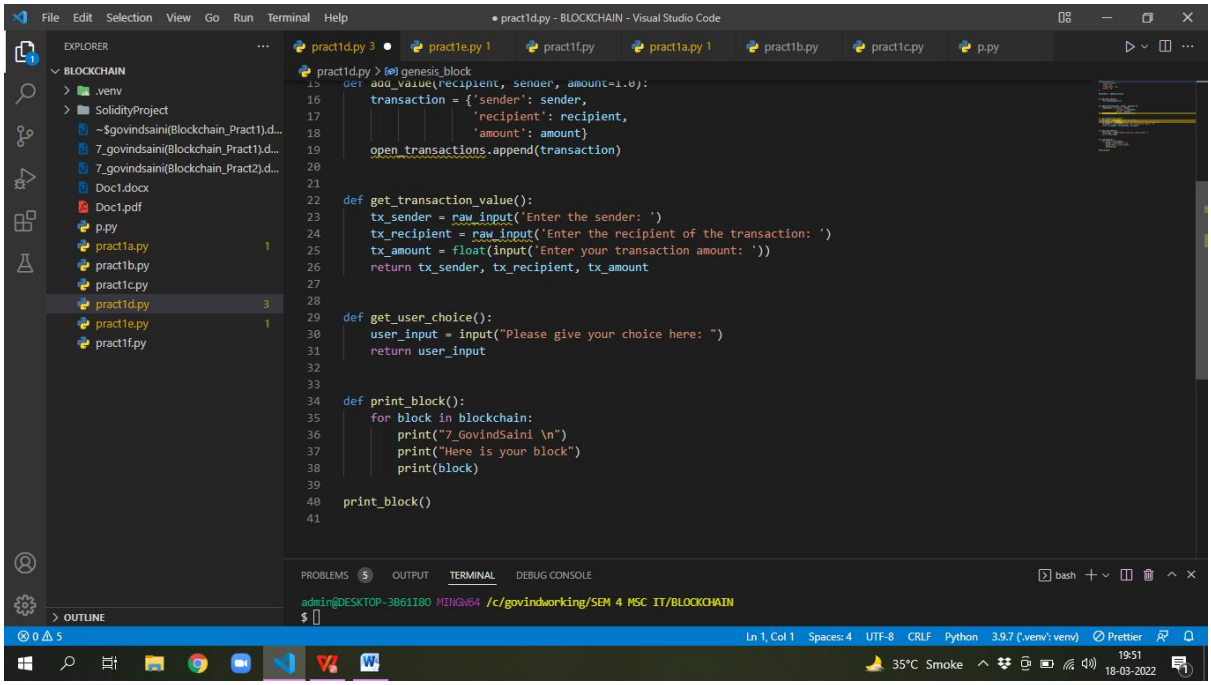
Output :



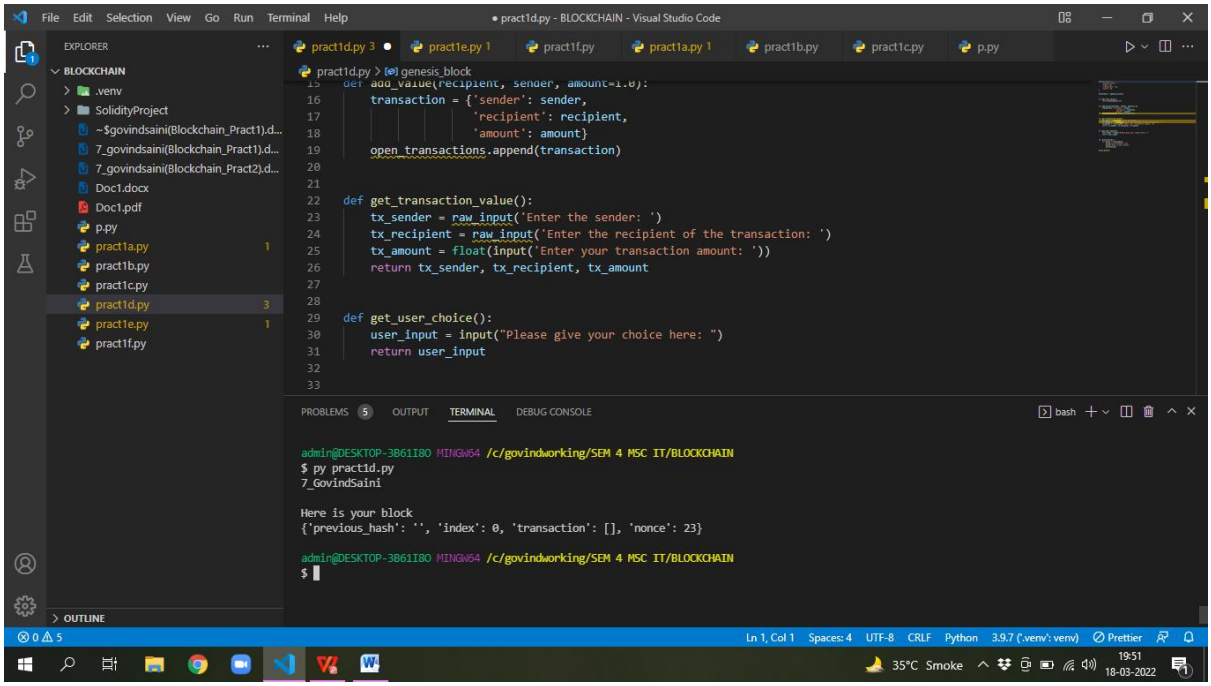
1d) Create a blockchain, a genesis block and execute it.

Code :



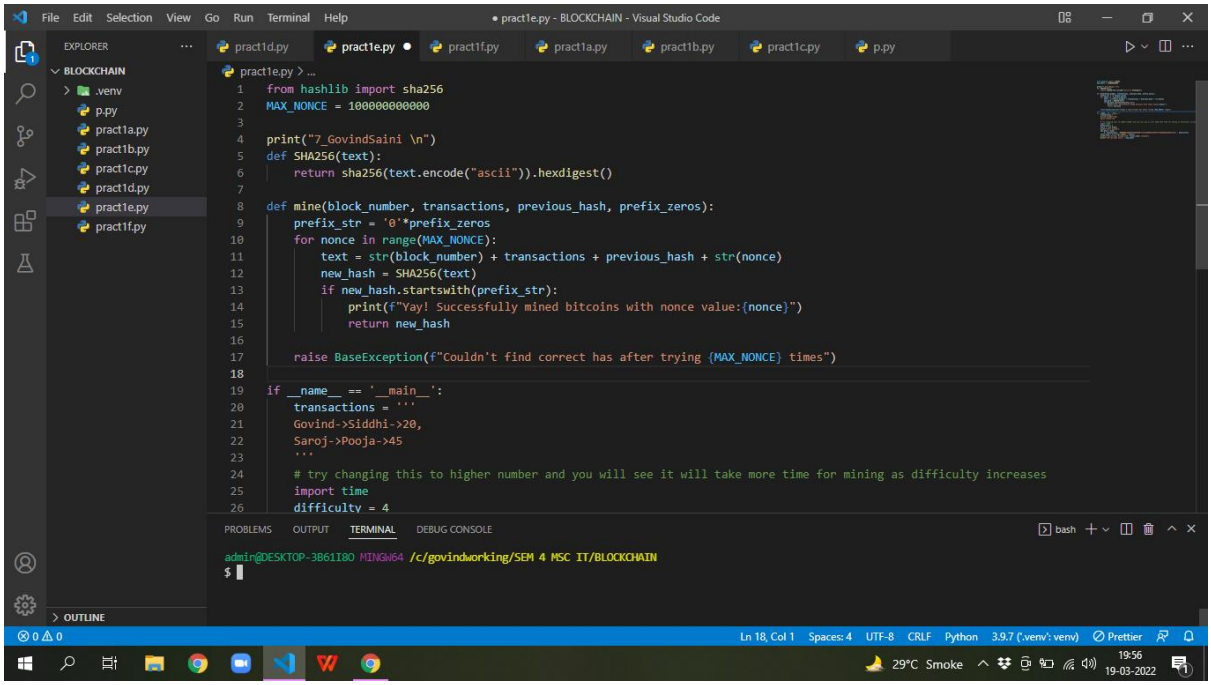


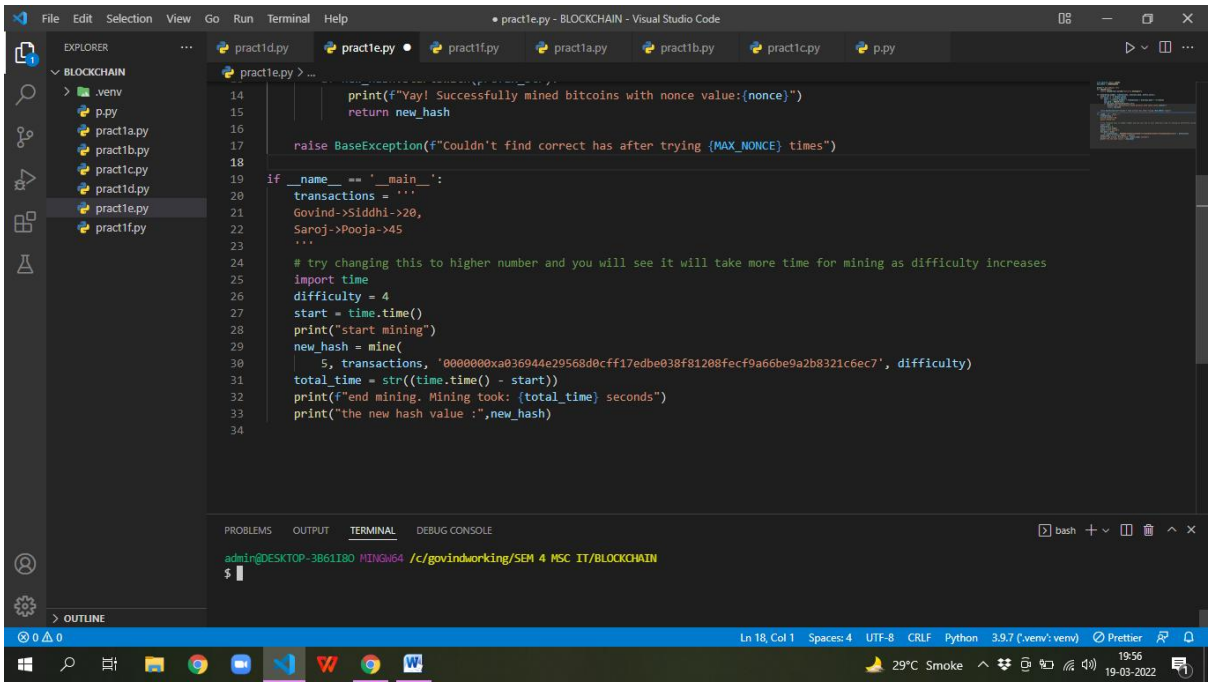
Output :



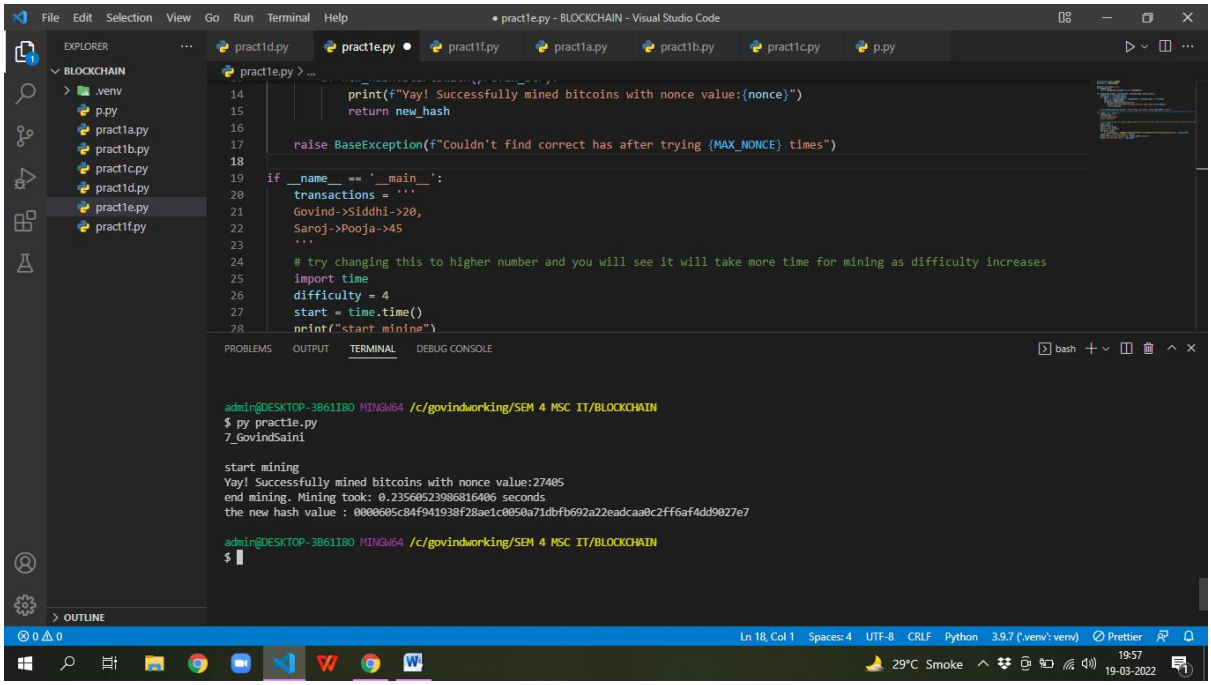
1e) Create a mining function and test it.

Code :


File Edit Selection View Go Run Terminal Help
• pract1e.py - BLOCKCHAIN - Visual Studio Code
EXPLORER
BLOCKCHAIN
.venv
p.py
pract1a.py
pract1b.py
pract1c.py
pract1d.py
pract1e.py
pract1f.py
pract1d.py
pract1e.py
pract1f.py
pract1a.py
pract1b.py
pract1c.py
p.py
pract1e.py > ...
from hashlib import sha256
MAX_NONCE = 100000000000
print("7_GovindSaini \n")
def SHA256(text):
return sha256(text.encode("ascii")).hexdigest()
def mine(block_number, transactions, previous_hash, prefix_zeros):
prefix_str = '0'*prefix_zeros
for nonce in range(MAX_NONCE):
text = str(block_number) + transactions + previous_hash + str(nonce)
new_hash = SHA256(text)
if new_hash.startswith(prefix_str):
print(f"Yay! Successfully mined bitcoins with nonce value:{nonce}")
return new_hash
raise BaseException(f"Couldn't find correct has after trying {MAX_NONCE} times")
if __name__ == '__main__':
transactions = '''
Govind->Siddhi->20,
Saroj->Pooja->45
'''
# try changing this to higher number and you will see it will take more time for mining as difficulty increases
import time
difficulty = 4
PROBLEMS OUTPUT TERMINAL DEBUG CONSOLE
bash
admin@DESKTOP-3B61I8O MINGW64 /c/govindworking/SEM 4 MSC IT/BLOCKCHAIN
$
OUTLINE
Ln 18, Col 1 Spaces: 4 UTF-8 CRLF Python 3.9.7 ('.venv': venv) Prettier
29°C Smoke
19:56
19-03-2022

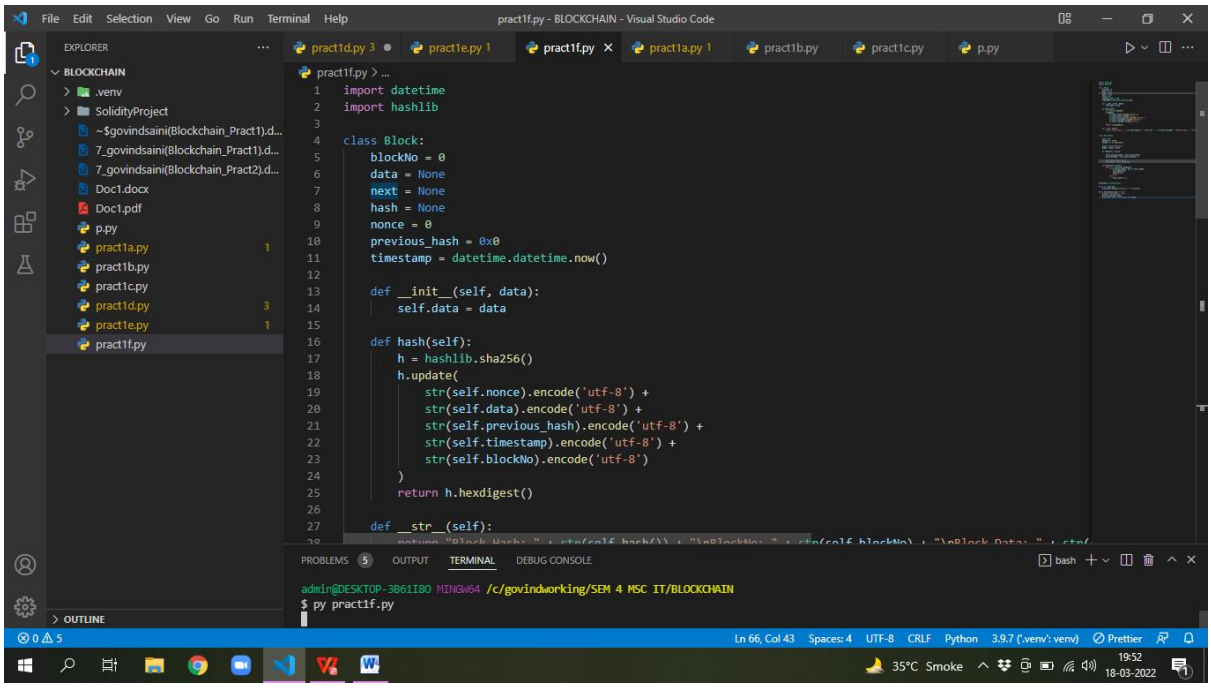

File Edit Selection View Go Run Terminal Help
• pract1e.py - BLOCKCHAIN - Visual Studio Code
EXPLORER
BLOCKCHAIN
.venv
p.py
pract1a.py
pract1b.py
pract1c.py
pract1d.py
pract1e.py
pract1f.py
pract1d.py
pract1e.py
pract1f.py
pract1a.py
pract1b.py
pract1c.py
p.py
pract1e.py > ...
print(f"Yay! Successfully mined bitcoins with nonce value:{nonce}")
return new_hash
raise BaseException(f"Couldn't find correct has after trying {MAX_NONCE} times")
if __name__ == '__main__':
transactions = '''
Govind->Siddhi->20,
Saroj->Pooja->45
'''
# try changing this to higher number and you will see it will take more time for mining as difficulty increases
import time
difficulty = 4
start = time.time()
print("start mining")
new_hash = mine(
5, transactions, '0000000xa036944e29568d0cff17edbe038f81208fecf9a66be9a2b8321c6ec7', difficulty)
total_time = str((time.time() - start))
print(f"end mining. Mining took: {total_time} seconds")
print("the new hash value :",new_hash)
PROBLEMS OUTPUT TERMINAL DEBUG CONSOLE
bash
admin@DESKTOP-3B61I8O MINGW64 /c/govindworking/SEM 4 MSC IT/BLOCKCHAIN
$
OUTLINE
Ln 18, Col 1 Spaces: 4 UTF-8 CRLF Python 3.9.7 ('.venv': venv) Prettier
29°C Smoke
19:56
19-03-2022

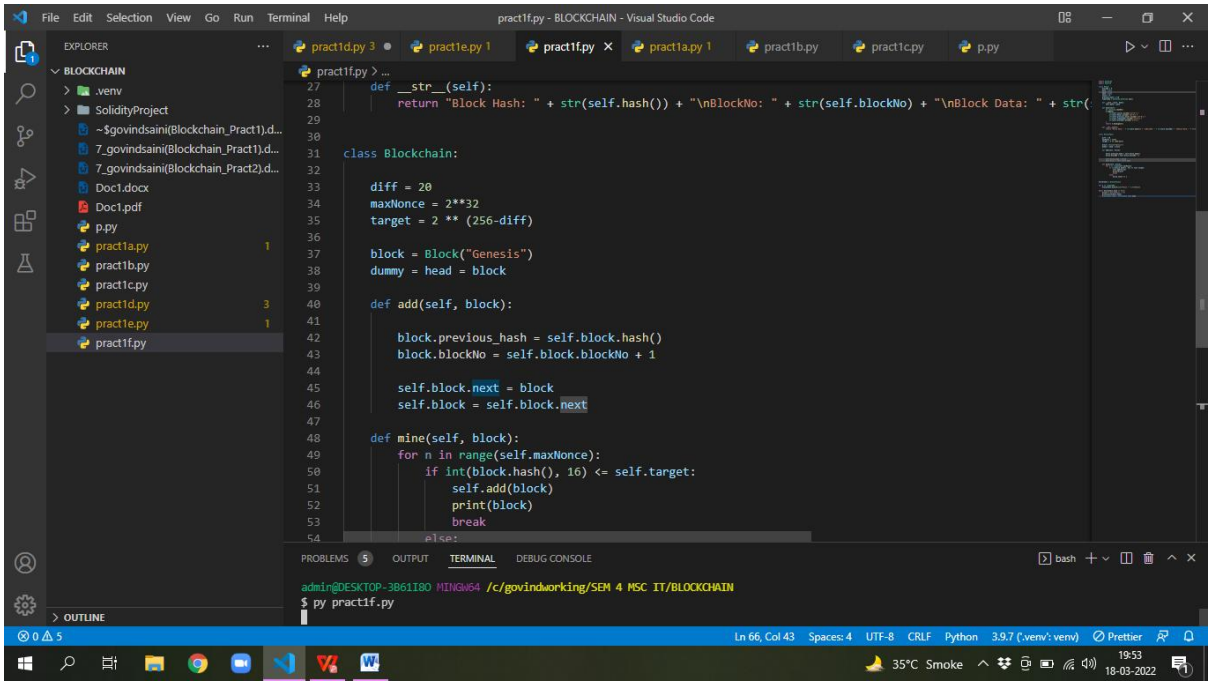
Output :

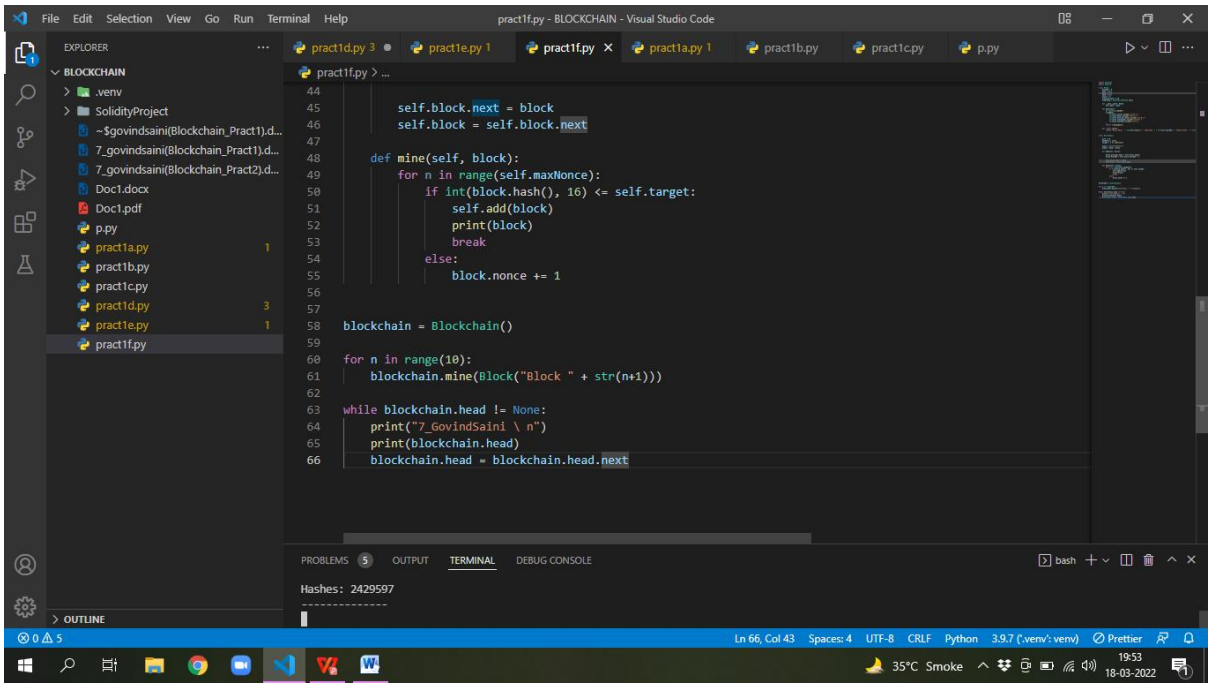


1f) Add blocks to the miner and dump the blockchain

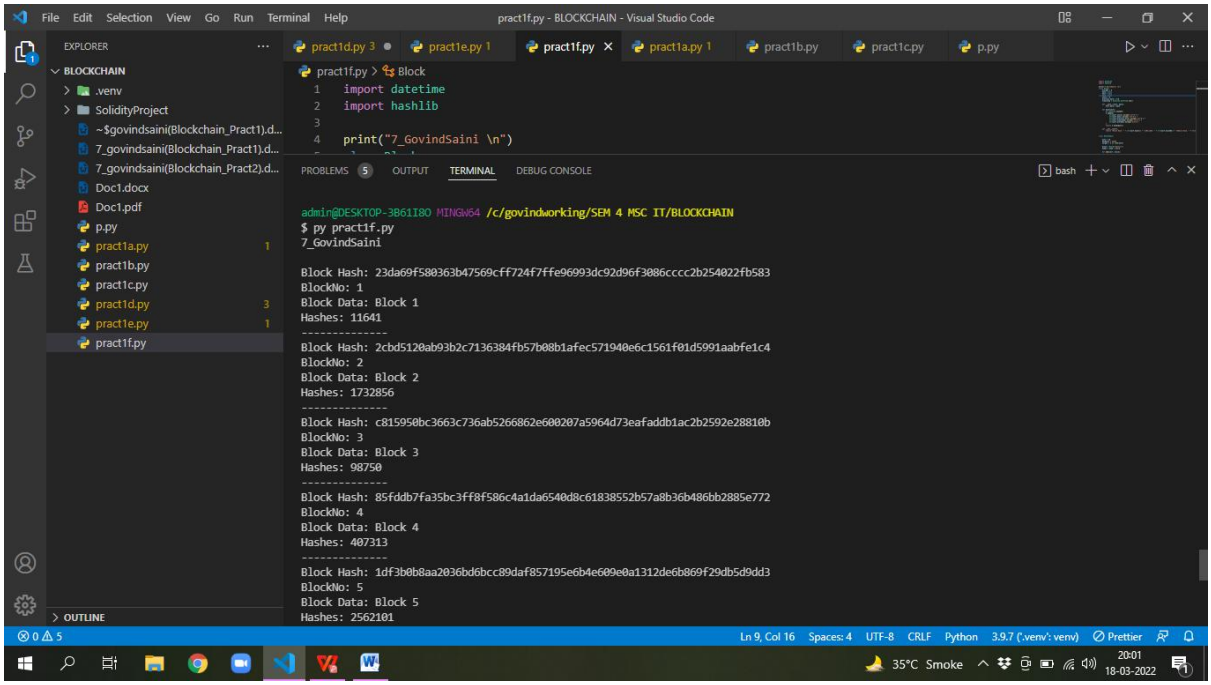
Code :

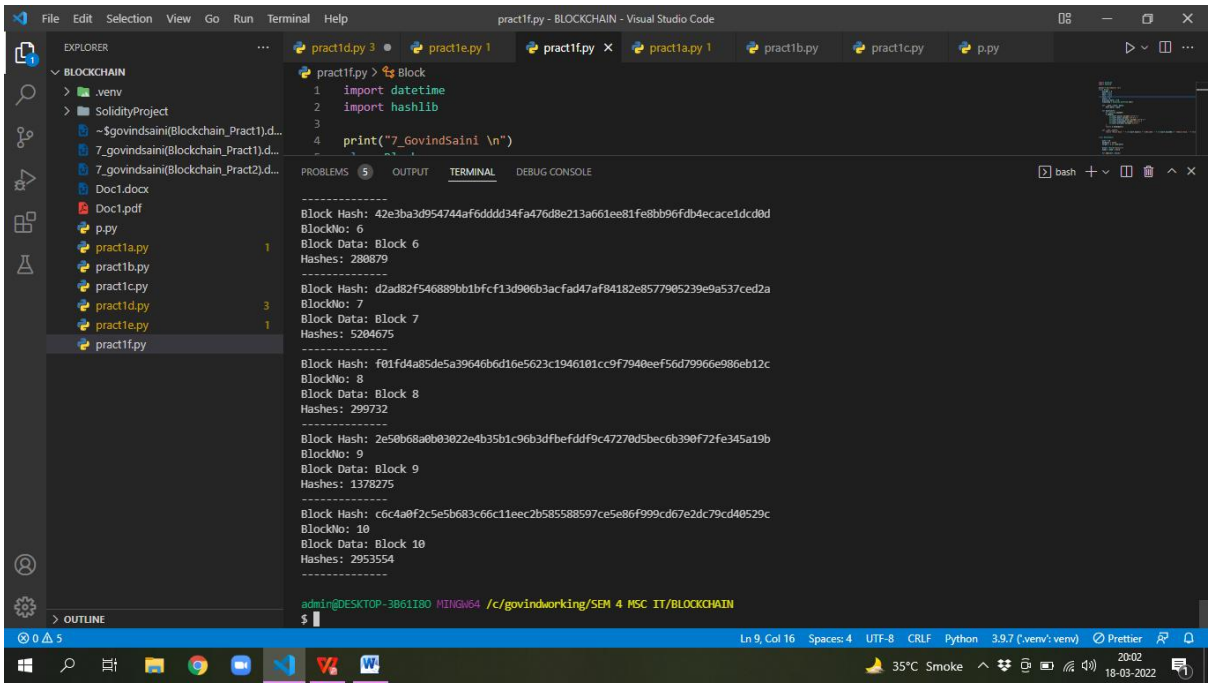



File Edit Selection View Go Run Terminal Help
pract1f.py - BLOCKCHAIN - Visual Studio Code
EXPLORER
BLOCKCHAIN
.venv
SolidityProject
~$govindsaini(Blockchain_Pract1).d...
7_govindsaini(Blockchain_Pract1).d...
7_govindsaini(Blockchain_Pract2).d...
Doc1.docx
Doc1.pdf
p.py
pract1a.py
pract1b.py
pract1c.py
pract1d.py
pract1e.py
pract1f.py
OUTLINE
pract1d.py 3
pract1e.py 1
pract1f.py
pract1a.py 1
pract1b.py
pract1c.py
p.py
pract1f.py > ...
def __str__(self):
return "Block Hash: " + str(self.hash()) + "\nBlockNo: " + str(self.blockNo) + "\nBlock Data: " + str(
class Blockchain:
diff = 20
maxNonce = 2**32
target = 2 ** (256-diff)
block = Block("Genesis")
dummy = head = block
def add(self, block):
block.previous_hash = self.block.hash()
block.blockNo = self.block.blockNo + 1
self.block.next = block
self.block = self.block.next
def mine(self, block):
for n in range(self.maxNonce):
if int(block.hash(), 16) <= self.target:
self.add(block)
print(block)
break
else:
PROBLEMS 5
OUTPUT
TERMINAL
DEBUG CONSOLE
bash
admin@DESKTOP-3B61I8O MINGW64 /c/govindworking/SEM 4 MSC IT/BLOCKCHAIN
$ py pract1f.py
Ln 66, Col 43
Spaces: 4
UTF-8
CRLF
Python
3.9.7 ('.venv': venv)
Prettier
35°C Smoke
19:53
18-03-2022


File Edit Selection View Go Run Terminal Help
pract1f.py - BLOCKCHAIN - Visual Studio Code
EXPLORER
BLOCKCHAIN
.venv
SolidityProject
~$govindsaini(Blockchain_Pract1).d...
7_govindsaini(Blockchain_Pract1).d...
7_govindsaini(Blockchain_Pract2).d...
Doc1.docx
Doc1.pdf
p.py
pract1a.py
pract1b.py
pract1c.py
pract1d.py
pract1e.py
pract1f.py
OUTLINE
pract1d.py 3
pract1e.py 1
pract1f.py
pract1a.py 1
pract1b.py
pract1c.py
p.py
pract1f.py > ...
self.block.next = block
self.block = self.block.next
def mine(self, block):
for n in range(self.maxNonce):
if int(block.hash(), 16) <= self.target:
self.add(block)
print(block)
break
else:
block.nonce += 1
blockchain = Blockchain()
for n in range(10):
blockchain.mine(Block("Block " + str(n+1)))
while blockchain.head != None:
print("7_GovindSaini \ n")
print(blockchain.head)
blockchain.head = blockchain.head.next
PROBLEMS 5
OUTPUT
TERMINAL
DEBUG CONSOLE
bash
Hashes: 2429597
Ln 66, Col 43
Spaces: 4
UTF-8
CRLF
Python
3.9.7 ('.venv': venv)
Prettier
35°C Smoke
19:53
18-03-2022

Output :


File Edit Selection View Go Run Terminal Help
pract1f.py - BLOCKCHAIN - Visual Studio Code
EXPLORER
BLOCKCHAIN
.venv
SolidityProject
~$govindsaini(Blockchain_Pract1).d...
7_govindsaini(Blockchain_Pract1).d...
7_govindsaini(Blockchain_Pract2).d...
Doc1.docx
Doc1.pdf
p.py
pract1a.py
pract1b.py
pract1c.py
pract1d.py
pract1e.py
pract1f.py
OUTLINE
pract1d.py 3
pract1e.py 1
pract1f.py
pract1a.py 1
pract1b.py
pract1c.py
p.py
pract1f.py > Block
1 import datetime
2 import hashlib
3
4 print("7_GovindSaini \n")
PROBLEMS 5
OUTPUT
TERMINAL
DEBUG CONSOLE
bash
admin@DESKTOP-3B61I8O MINGW64 /c/govindworking/SEM 4 MSC IT/BLOCKCHAIN
$ py pract1f.py
7_GovindSaini
Block Hash: 23da69f580363b47569cff724f7ffe96993dc92d96f3086cccc2b254022fb583
BlockNo: 1
Block Data: Block 1
Hashes: 11641
Block Hash: 2cbd5120ab93b2c7136384fb57b08b1afec571940e6c1561f01d5991aabfe1c4
BlockNo: 2
Block Data: Block 2
Hashes: 1732856
Block Hash: c815950bc3663c736ab5266862e600207a5964d73eafaddb1ac2b2592e28810b
BlockNo: 3
Block Data: Block 3
Hashes: 98750
Block Hash: 85fddb7fa35bc3ff8f586c4a1da6540d8c61838552b57a8b36b486bb2885e772
BlockNo: 4
Block Data: Block 4
Hashes: 407313
Block Hash: 1df3b0b8aa2036bd6bcc89daf857195e6b4e609e0a1312de6b869f29db5d9dd3
BlockNo: 5
Block Data: Block 5
Hashes: 2562101
Ln 9, Col 16 Spaces: 4 UTF-8 CRLF Python 3.9.7 ('.venv': venv) Prettier
35°C Smoke
20:01
18-03-2022


File Edit Selection View Go Run Terminal Help
pract1f.py - BLOCKCHAIN - Visual Studio Code
EXPLORER
BLOCKCHAIN
.venv
SolidityProject
~$govindsaini(Blockchain_Pract1).d...
7_govindsaini(Blockchain_Pract1).d...
7_govindsaini(Blockchain_Pract2).d...
Doc1.docx
Doc1.pdf
p.py
pract1a.py
pract1b.py
pract1c.py
pract1d.py
pract1e.py
pract1f.py
OUTLINE
pract1d.py 3
pract1e.py 1
pract1f.py
pract1a.py 1
pract1b.py
pract1c.py
p.py
pract1f.py > Block
1 import datetime
2 import hashlib
3
4 print("7_GovindSaini \n")
PROBLEMS 5
OUTPUT
TERMINAL
DEBUG CONSOLE
bash
Block Hash: 42e3ba3d954744af6dddd34fa476d8e213a661ee81fe8bb96fdb4ecace1dcd0d
BlockNo: 6
Block Data: Block 6
Hashes: 280879
Block Hash: d2ad82f546889bb1bfcf13d906b3acfad47af84182e857905239e9a537ced2a
BlockNo: 7
Block Data: Block 7
Hashes: 5204675
Block Hash: f01fd4a85de5a39646b6d16e5623c1946101cc9f7940eef56d79966e986eb12c
BlockNo: 8
Block Data: Block 8
Hashes: 299732
Block Hash: 2e50b68a0b03022e4b35b1c96b3dfbefddf9c47270d5bec6b390f72fe345a19b
BlockNo: 9
Block Data: Block 9
Hashes: 1378275
Block Hash: c6c4a0f2c5e5b683c66c11eec2b585588597ce5e86f999cd67e2dc79cd40529c
BlockNo: 10
Block Data: Block 10
Hashes: 2953554
admin@DESKTOP-3B61I8O MINGW64 /c/govindworking/SEM 4 MSC IT/BLOCKCHAIN
$
Ln 9, Col 16 Spaces: 4 UTF-8 CRLF Python 3.9.7 ('.venv': venv) Prettier
35°C Smoke
20:02
18-03-2022

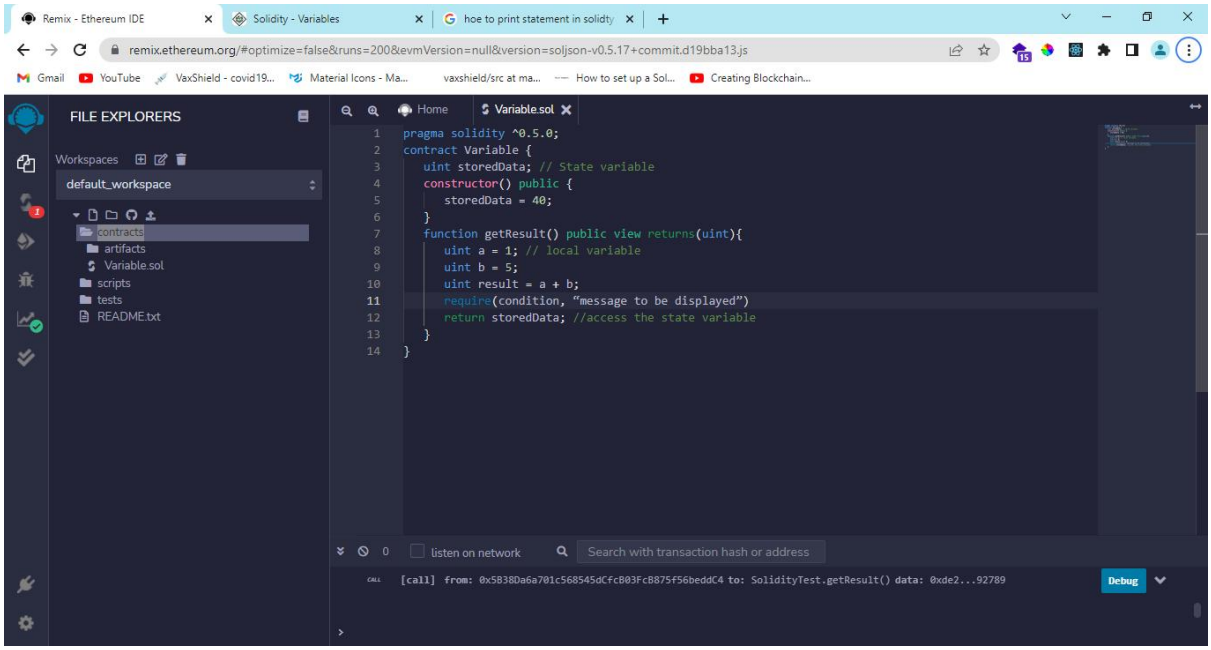
Practical No : 3

Aim : Implement and demonstrate the use of the following in Solidity

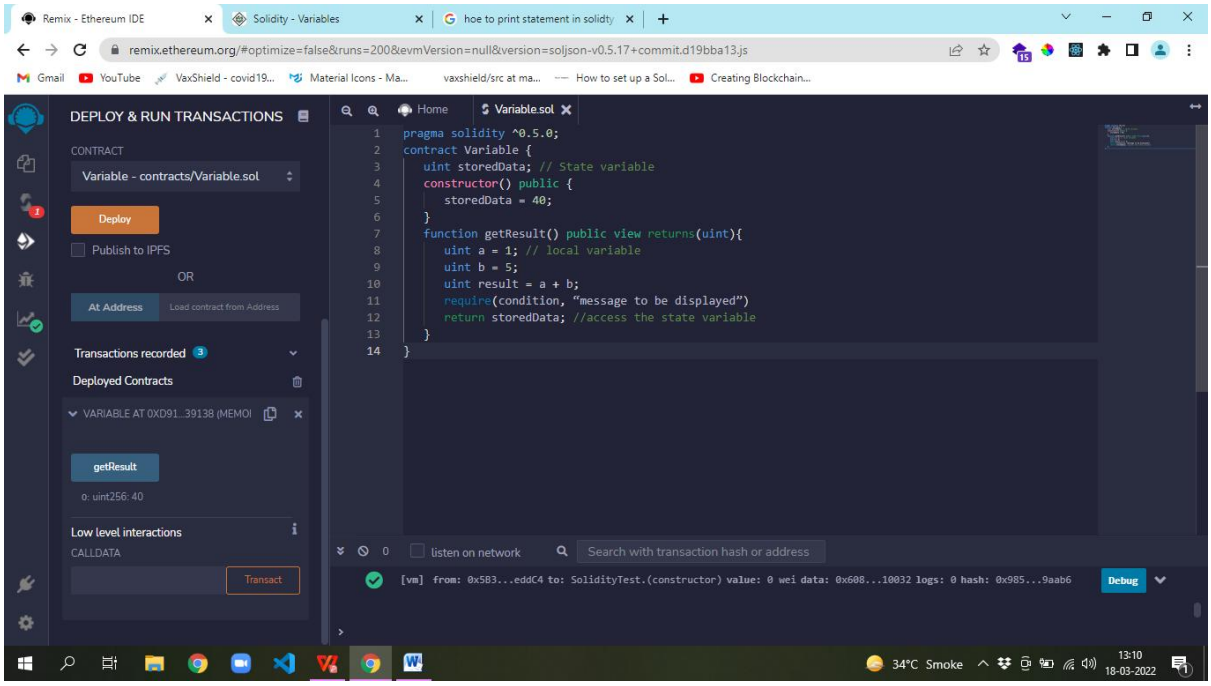
3a) Variable, Operators, Loops, Decision Making, Strings, Arrays, Enums, Structs, Mappings, Conversions, Ether Units, Special Variables.

Variable

Code :



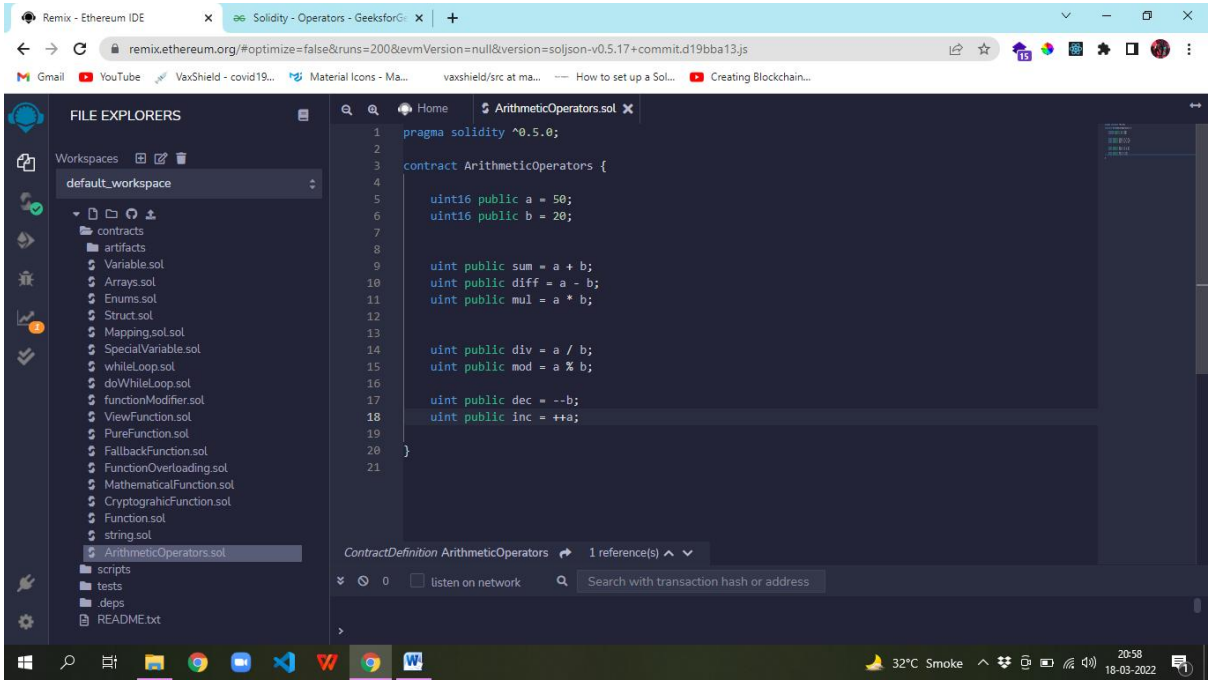
Output :



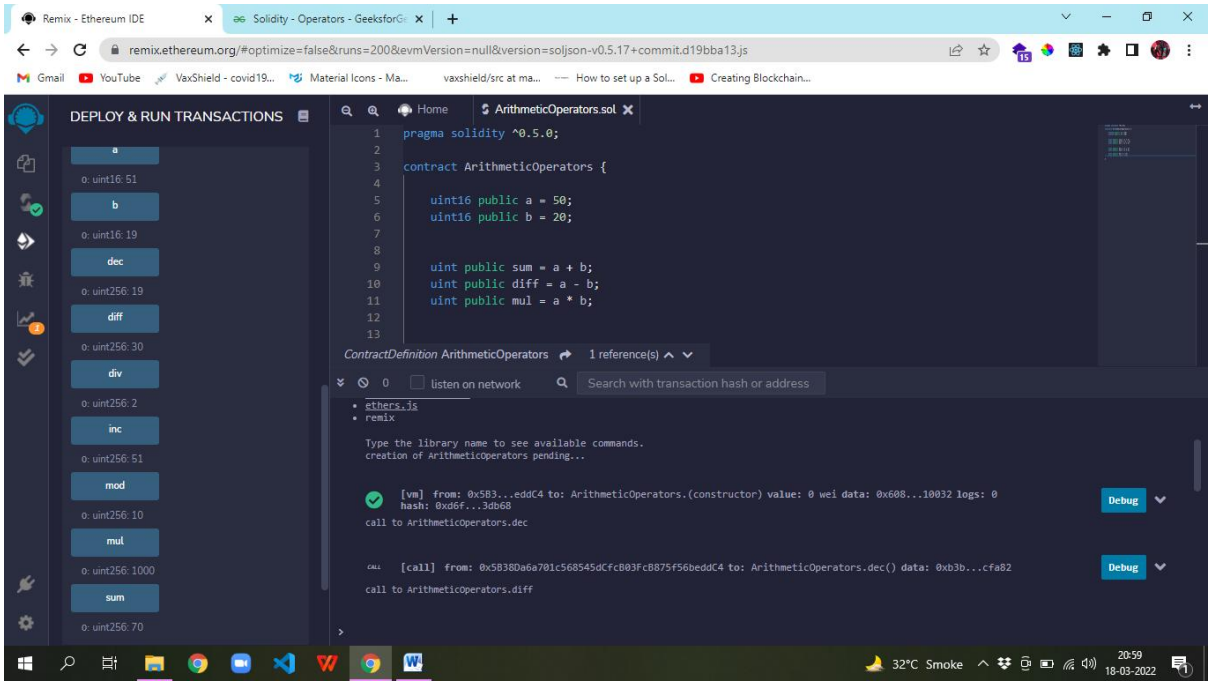
Operators :

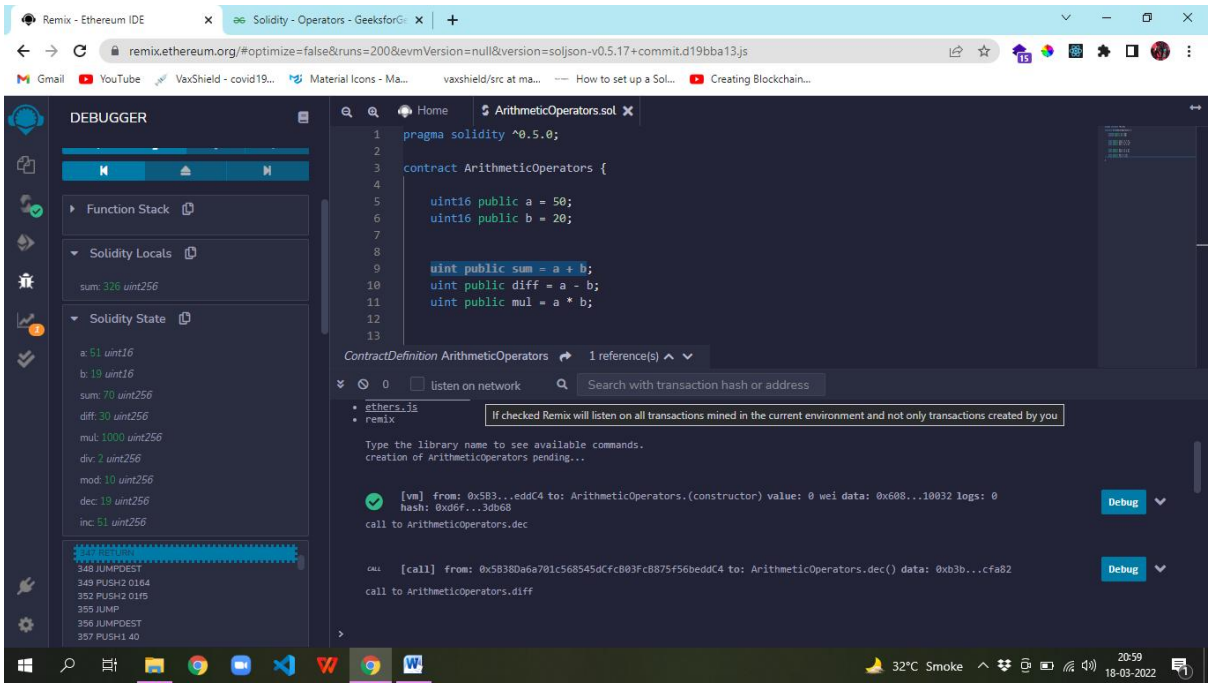
Arthmetic Operator

Code:



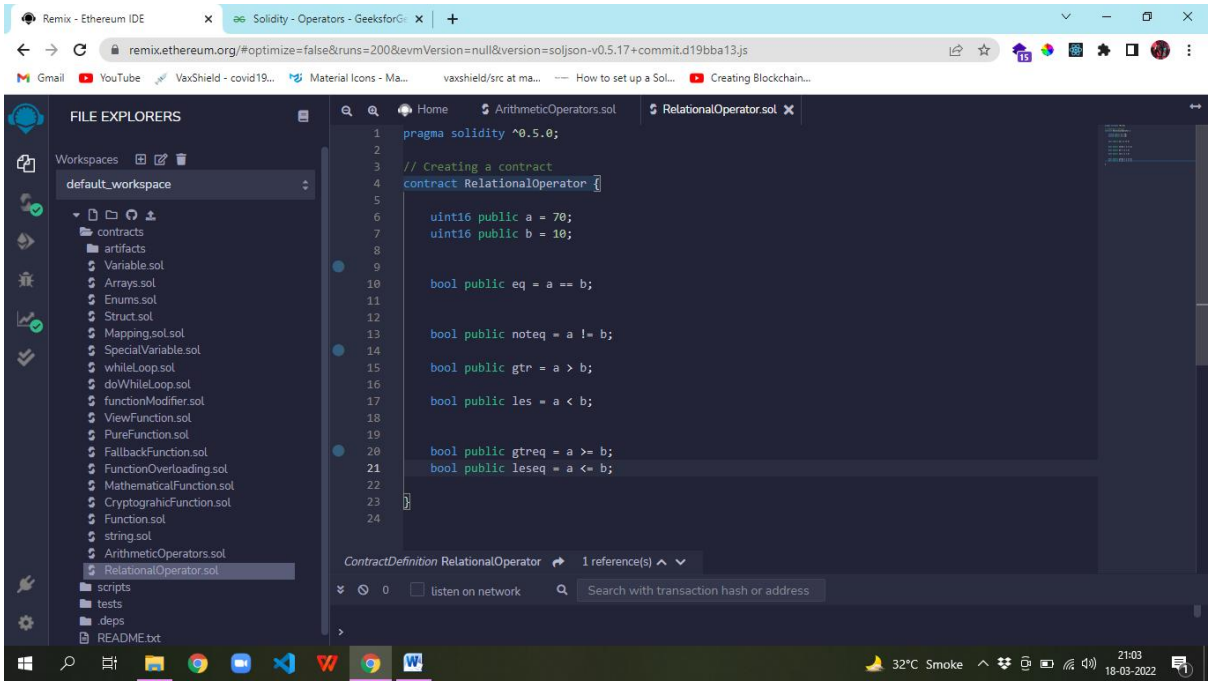
Output:



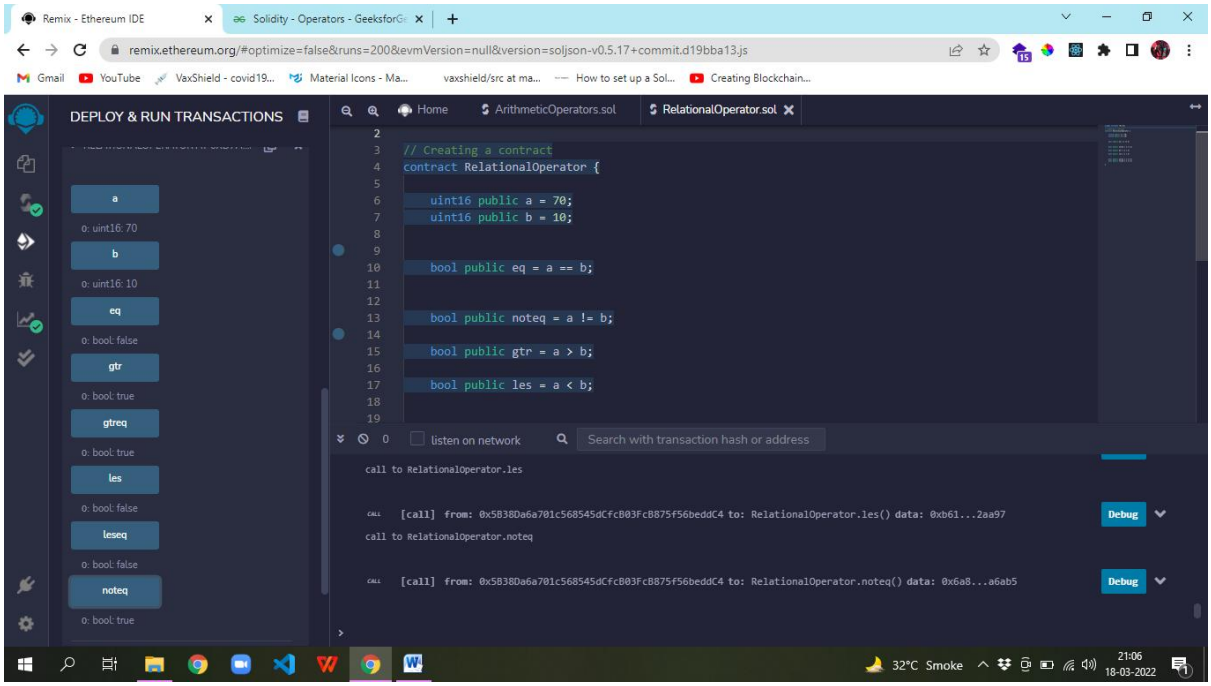


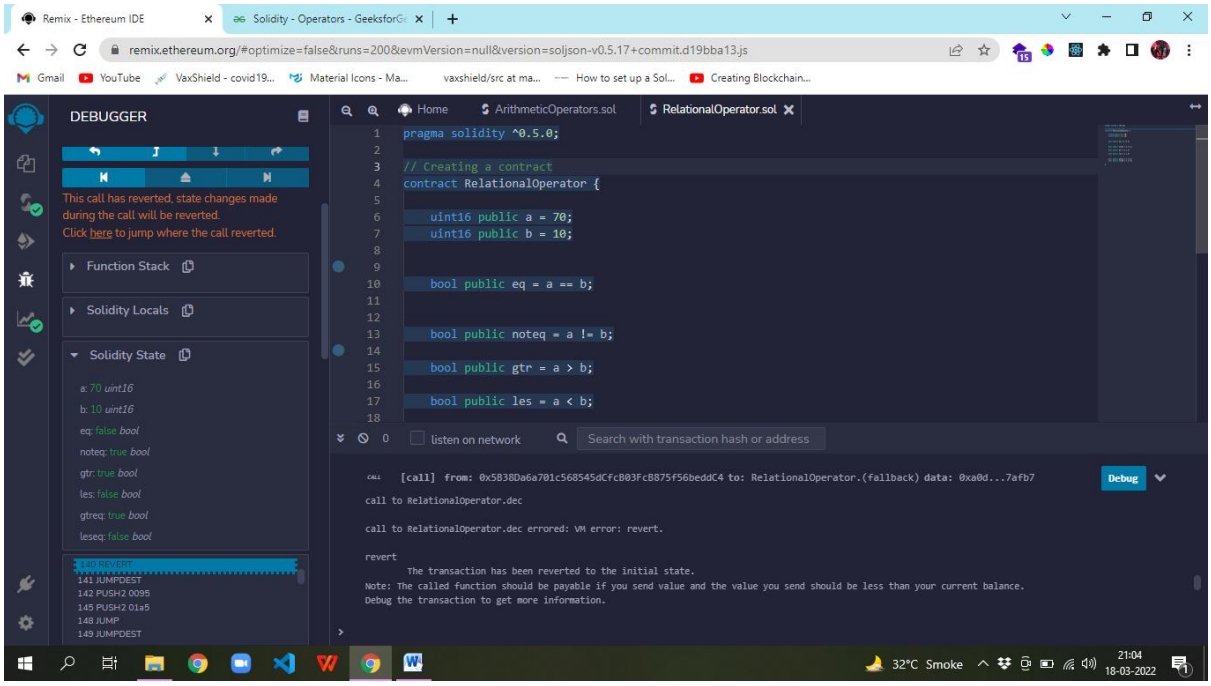
Relational Operator

Code:


Remix - Ethereum IDE
Solidity - Operators - GeeksforGe
remix.ethereum.org/#optimize=false&runs=200&evmVersion=null&version=soljson-v0.5.17+commit.d19bba13.js
FILE EXPLORERS
Workspaces
default_workspace
contracts
artifacts
Variable.sol
Arrays.sol
Enums.sol
Struct.sol
Mapping.sol.sol
SpecialVariable.sol
whileLoop.sol
doWhileLoop.sol
functionModifier.sol
ViewFunction.sol
PureFunction.sol
FallbackFunction.sol
FunctionOverloading.sol
MathematicalFunction.sol
CryptograhicFunction.sol
Function.sol
string.sol
ArithmeticOperators.sol
RelationalOperator.sol
scripts
tests
.deps
README.txt
Home
ArithmeticOperators.sol
RelationalOperator.sol
pragma solidity ^0.5.0;
// Creating a contract
contract RelationalOperator {
uint16 public a = 70;
uint16 public b = 10;
bool public eq = a == b;
bool public noteq = a != b;
bool public gtr = a > b;
bool public les = a < b;
bool public gtreq = a >= b;
bool public leseq = a <= b;
}
ContractDefinition RelationalOperator
1 reference(s)
listen on network
Search with transaction hash or address
32°C Smoke
21:03
18-03-2022

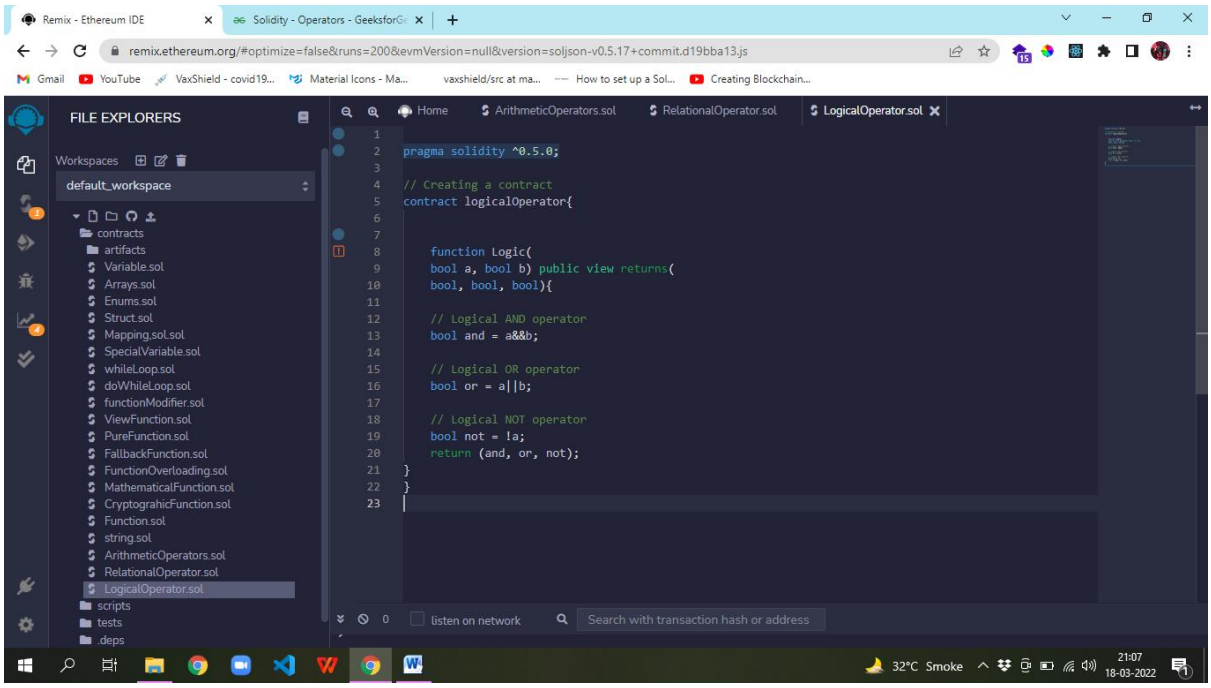
Output :


Remix - Ethereum IDE
Solidity - Operators - GeeksforGe
remix.ethereum.org/#optimize=false&runs=200&evmVersion=null&version=soljson-v0.5.17+commit.d19bba13.js
DEPLOY & RUN TRANSACTIONS
a
0: uint16: 70
b
0: uint16: 10
eq
0: bool: false
gtr
0: bool: true
gtreq
0: bool: true
les
0: bool: false
leseq
0: bool: false
noteq
0: bool: true
Home
ArithmeticOperators.sol
RelationalOperator.sol
// Creating a contract
contract RelationalOperator {
uint16 public a = 70;
uint16 public b = 10;
bool public eq = a == b;
bool public noteq = a != b;
bool public gtr = a > b;
bool public les = a < b;
listen on network
Search with transaction hash or address
call to RelationalOperator.les
[call] from: 0x5B38Da6a701c568545dCfcB03FcB875f56beddC4 to: RelationalOperator.les() data: 0xb61...2aa97
Debug
call to RelationalOperator.noteq
[call] from: 0x5B38Da6a701c568545dCfcB03FcB875f56beddC4 to: RelationalOperator.noteq() data: 0x6a8...a6ab5
Debug
32°C Smoke
21:06
18-03-2022

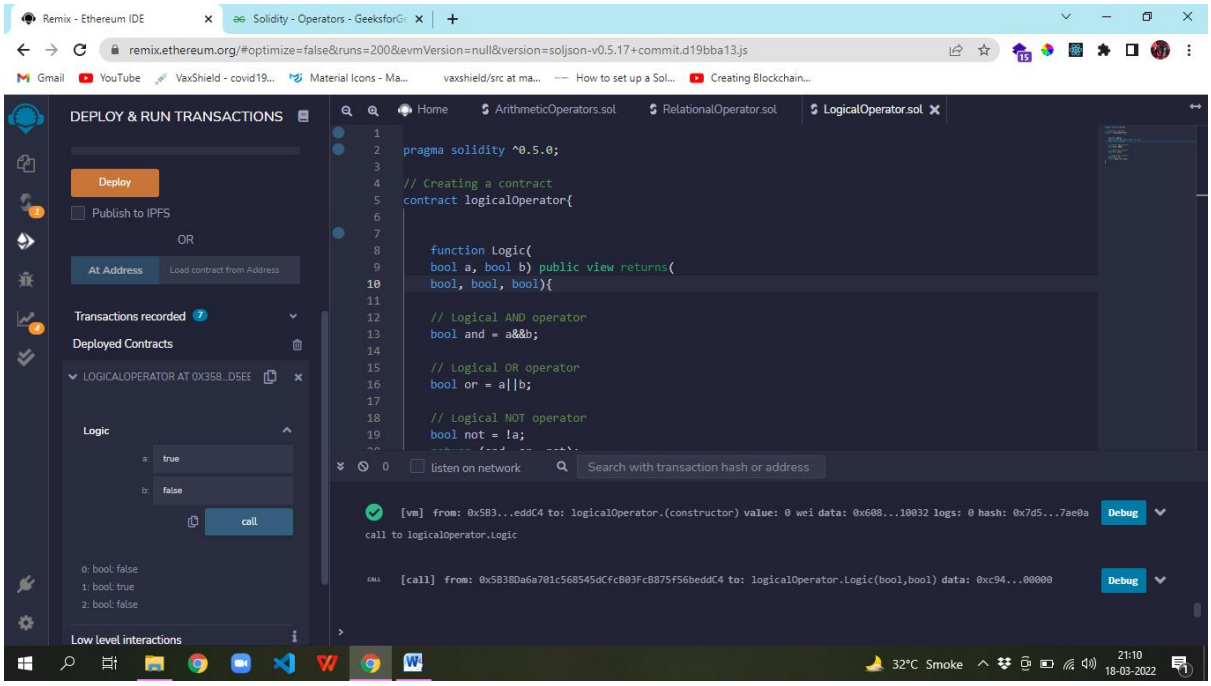


Logical Operator

Code :

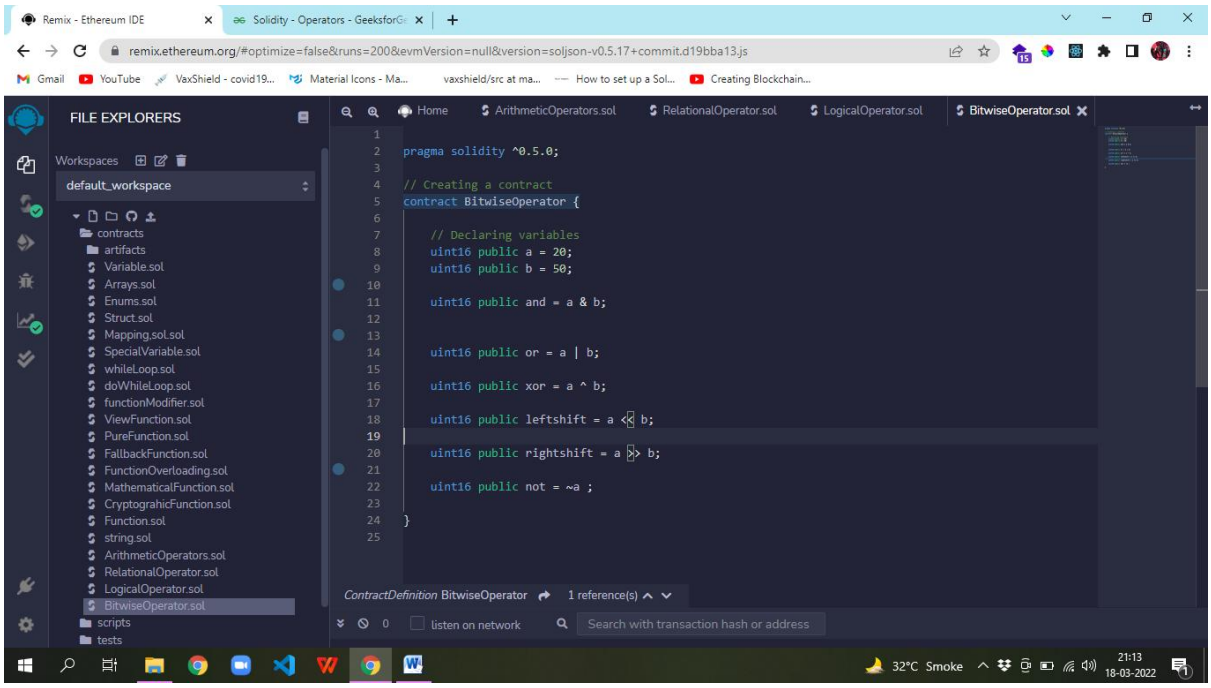


Output:

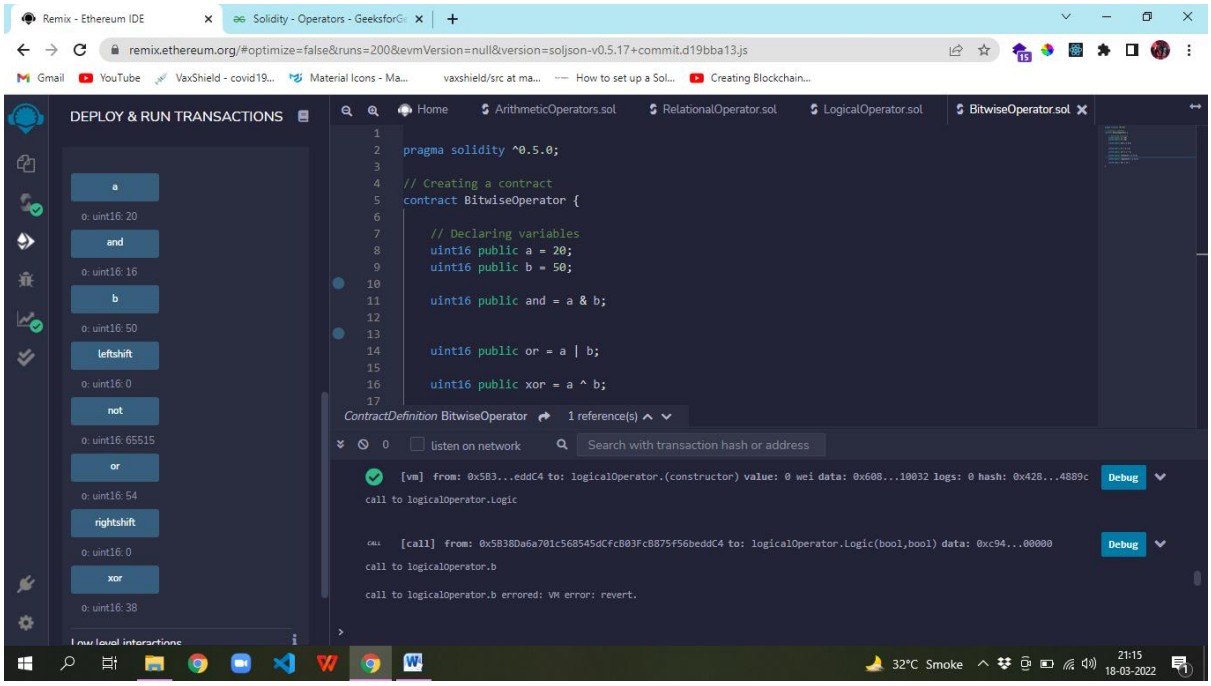


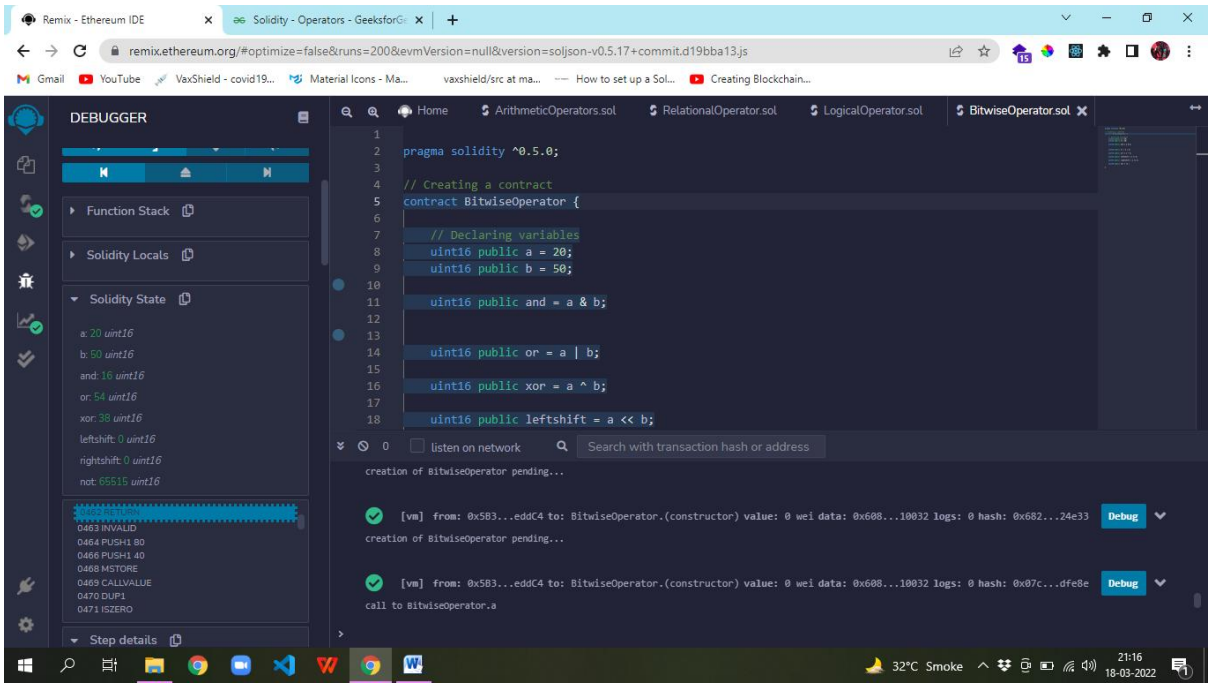
Bitwise Operator

Code:



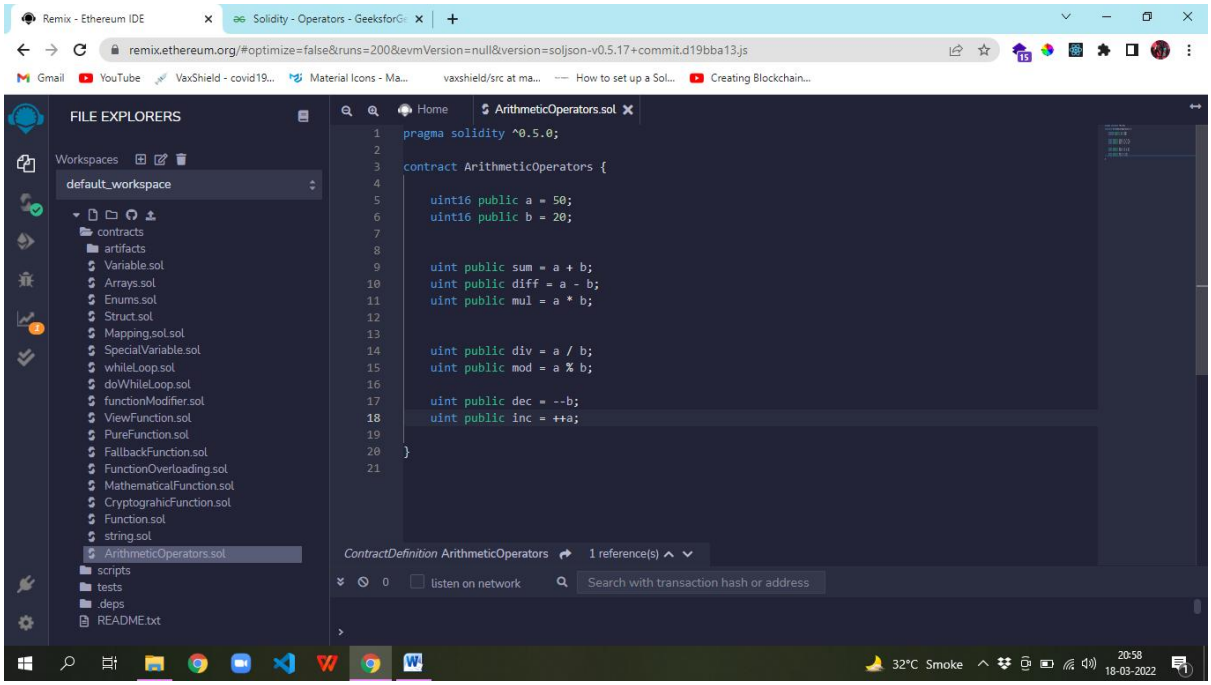
Output :



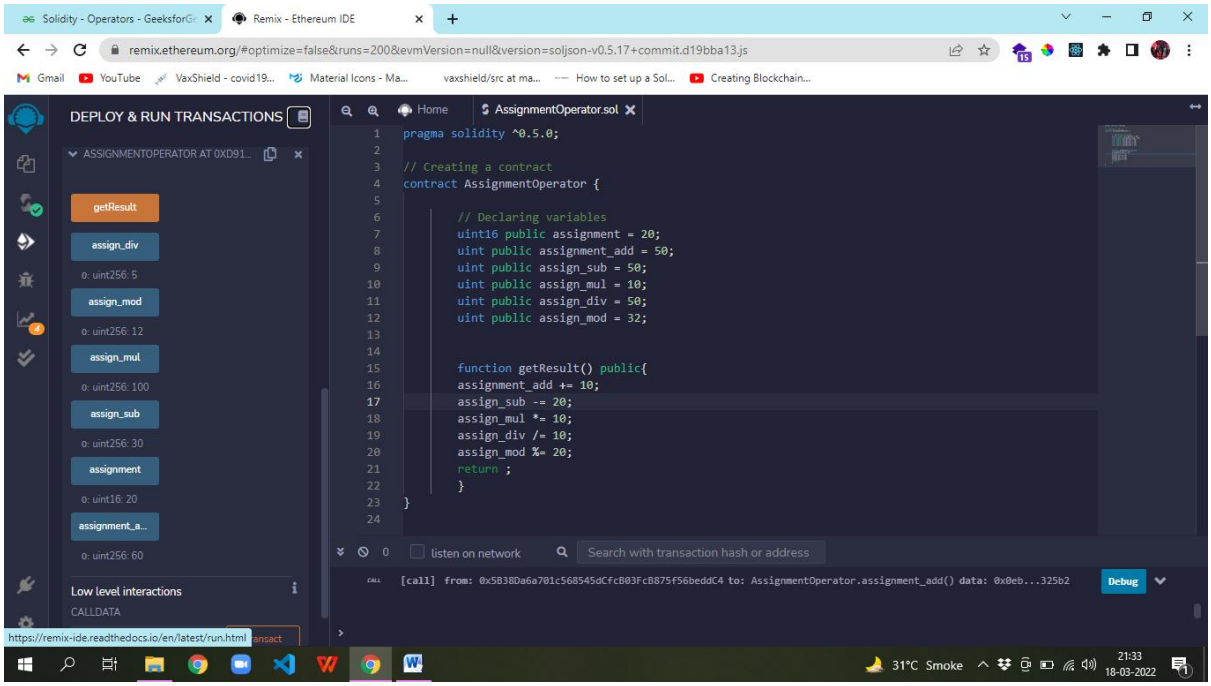


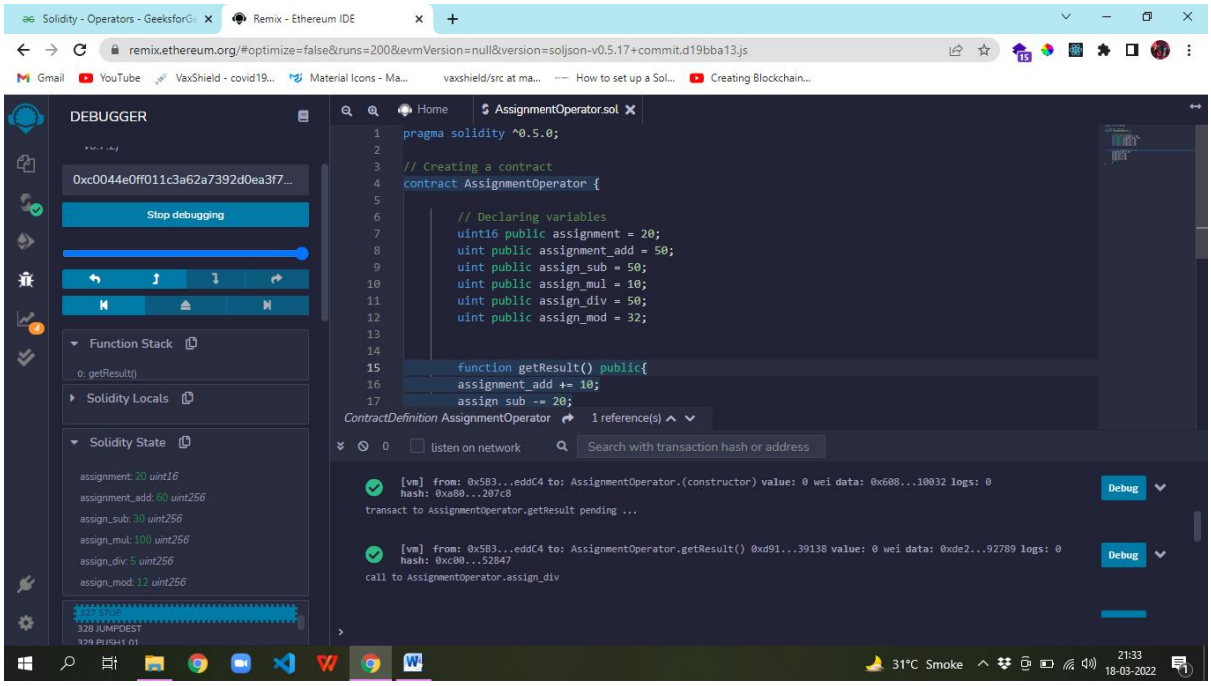
Assignment Operator

Code :


Remix - Ethereum IDE
Solidity - Operators - GeeksforGe
remix.ethereum.org/#optimize=false&runs=200&evmVersion=null&version=soljson-v0.5.17+commit.d19bba13.js
FILE EXPLORERS
Workspaces
default_workspace
contracts
artifacts
Variable.sol
Arrays.sol
Enums.sol
Struct.sol
Mapping.sol.sol
SpecialVariable.sol
whileLoop.sol
doWhileLoop.sol
functionModifier.sol
ViewFunction.sol
PureFunction.sol
FallbackFunction.sol
FunctionOverloading.sol
MathematicalFunction.sol
CryptograhicFunction.sol
Function.sol
string.sol
ArithmeticOperators.sol
scripts
tests
.deps
README.txt
Home
ArithmeticOperators.sol
pragma solidity ^0.5.0;
contract ArithmeticOperators {
uint16 public a = 50;
uint16 public b = 20;
uint public sum = a + b;
uint public diff = a - b;
uint public mul = a * b;
uint public div = a / b;
uint public mod = a % b;
uint public dec = --b;
uint public inc = ++a;
}
ContractDefinition ArithmeticOperators
1 reference(s)
listen on network
Search with transaction hash or address
32°C Smoke
20:58
18-03-2022

Ouput :

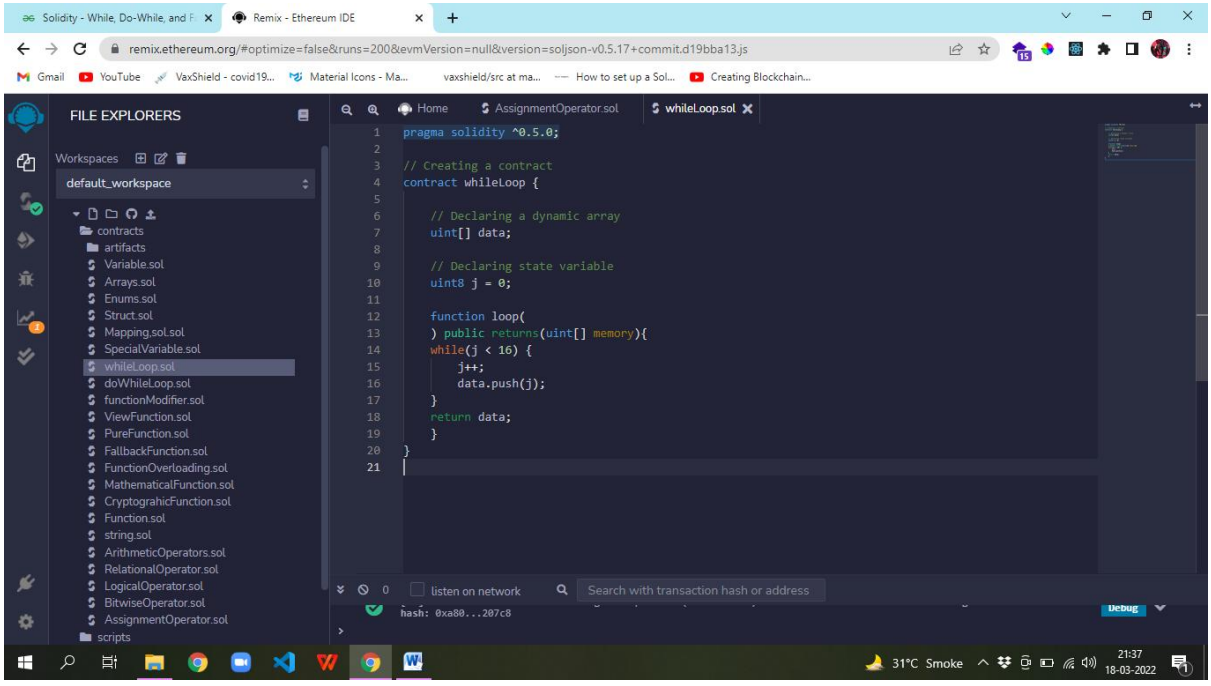

Solidity - Operators - GeeksforGe
Remix - Ethereum IDE
remix.ethereum.org/#optimize=false&runs=200&evmVersion=null&version=soljson-v0.5.17+commit.d19bba13.js
DEPLOY & RUN TRANSACTIONS
ASSIGNMENTOPERATOR AT 0XD91...
getResult
assign_div
o: uint256: 5
assign_mod
o: uint256: 12
assign_mul
o: uint256: 100
assign_sub
o: uint256: 30
assignment
o: uint16: 20
assignment_a...
o: uint256: 60
Low level interactions
CALLDATA
Home
AssignmentOperator.sol
pragma solidity ^0.5.0;
// Creating a contract
contract AssignmentOperator {
// Declaring variables
uint16 public assignment = 20;
uint public assignment_add = 50;
uint public assign_sub = 50;
uint public assign_mul = 10;
uint public assign_div = 50;
uint public assign_mod = 32;
function getResult() public{
assignment_add += 10;
assign_sub -= 20;
assign_mul *= 10;
assign_div /= 10;
assign_mod %= 20;
return ;
}
}
listen on network
Search with transaction hash or address
[call] from: 0x5B38Da6a701c568545dCFcB03FcB875f56beddC4 to: AssignmentOperator.assignment_add() data: 0x0eb...325b2
Debug
https://remix-ide.readthedocs.io/en/latest/run.html
31°C Smoke
21:33
18-03-2022



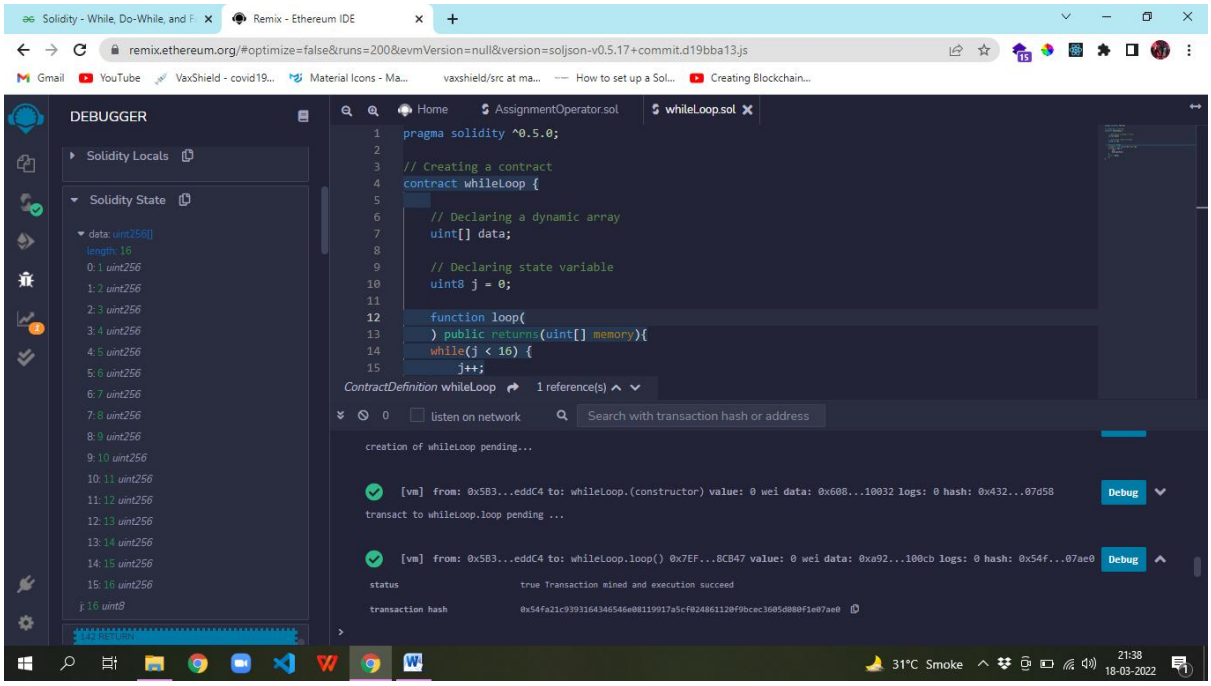
Loops

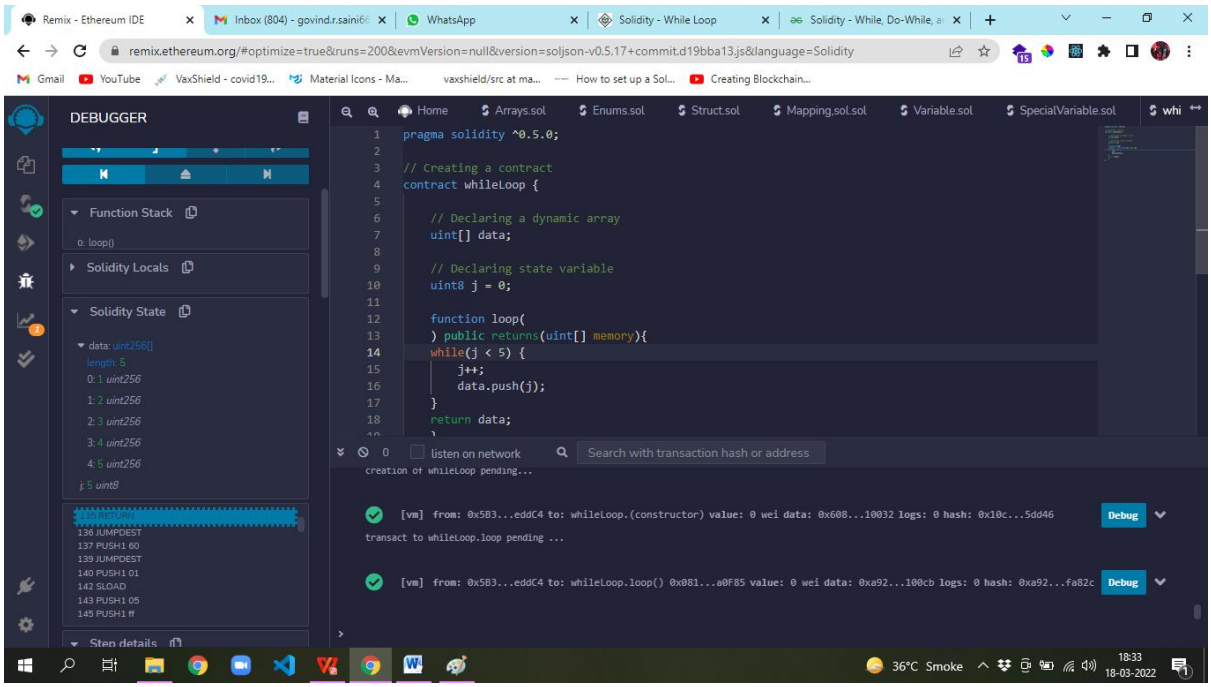
whileLoop

code:



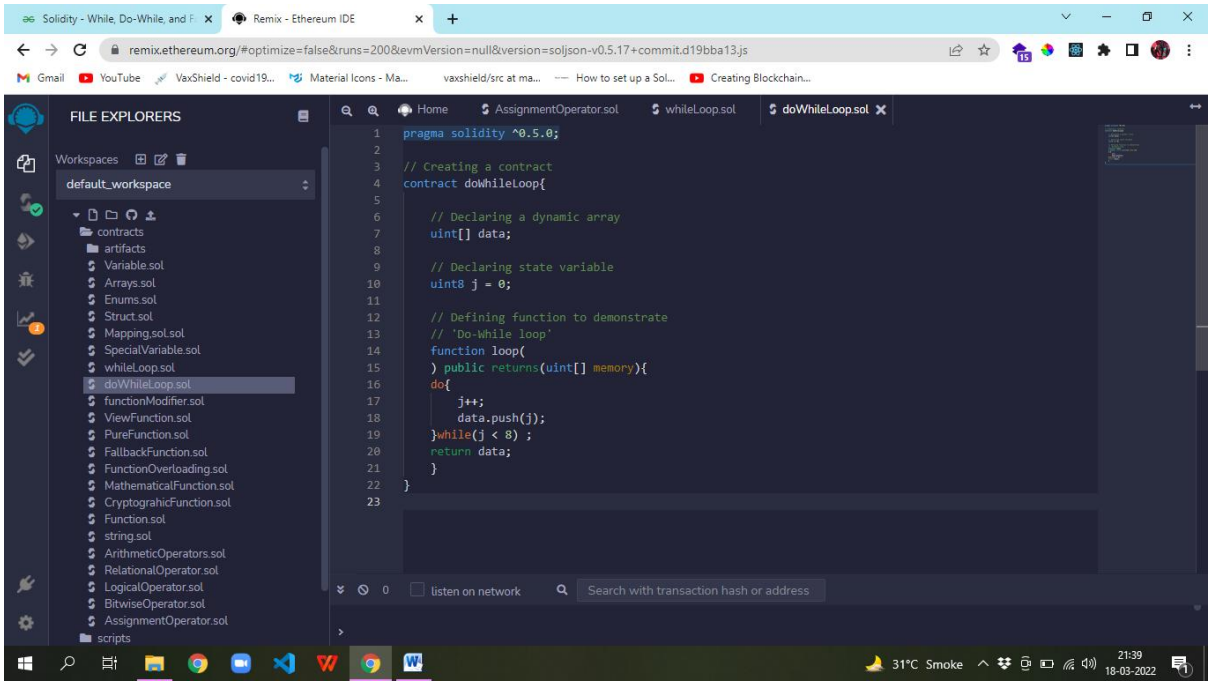
Output



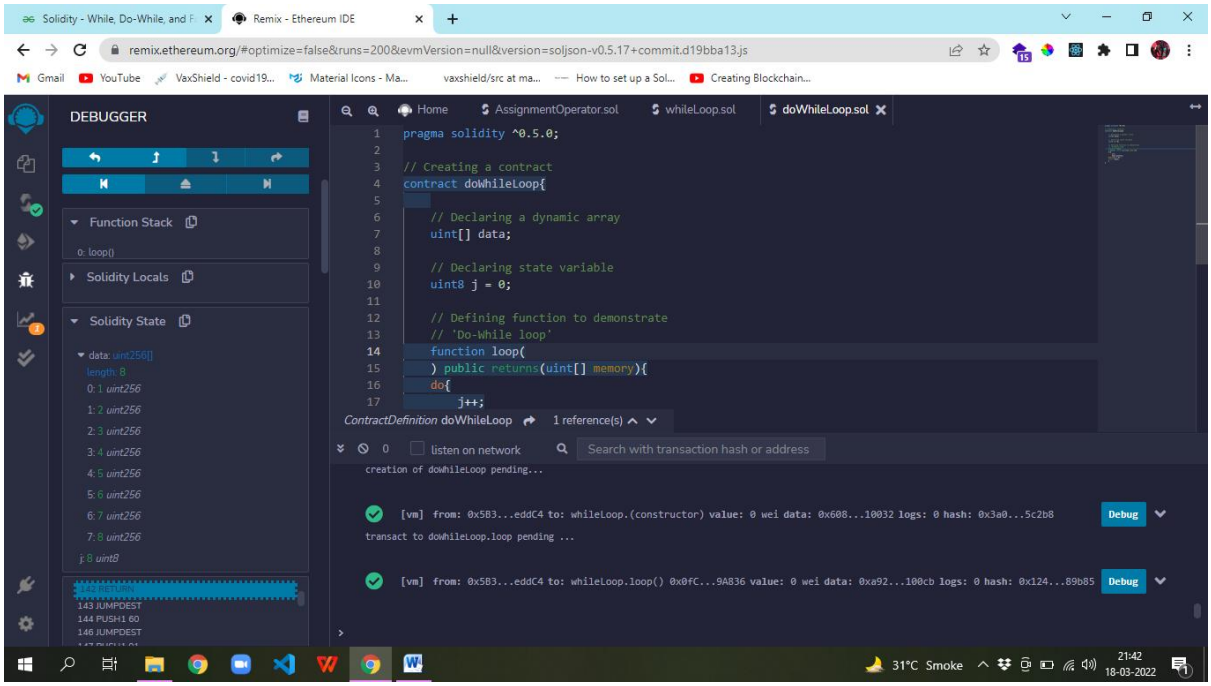


Dowhile loop

Code:

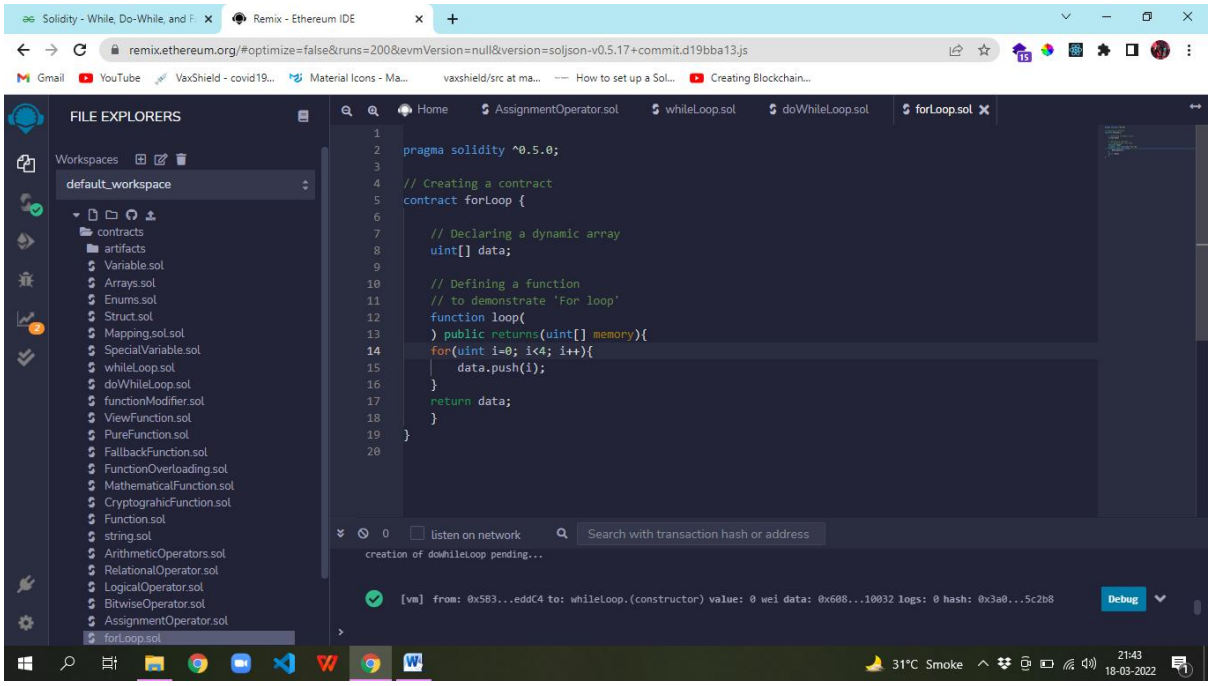


Output :

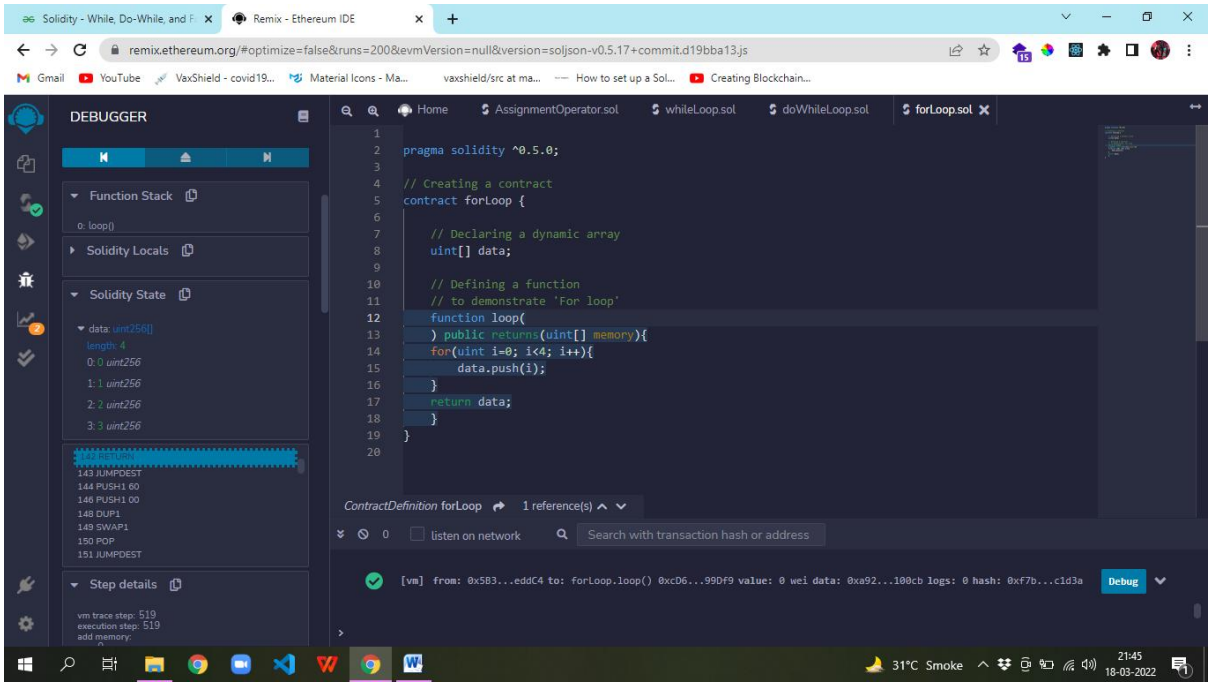


Forloop

Code :



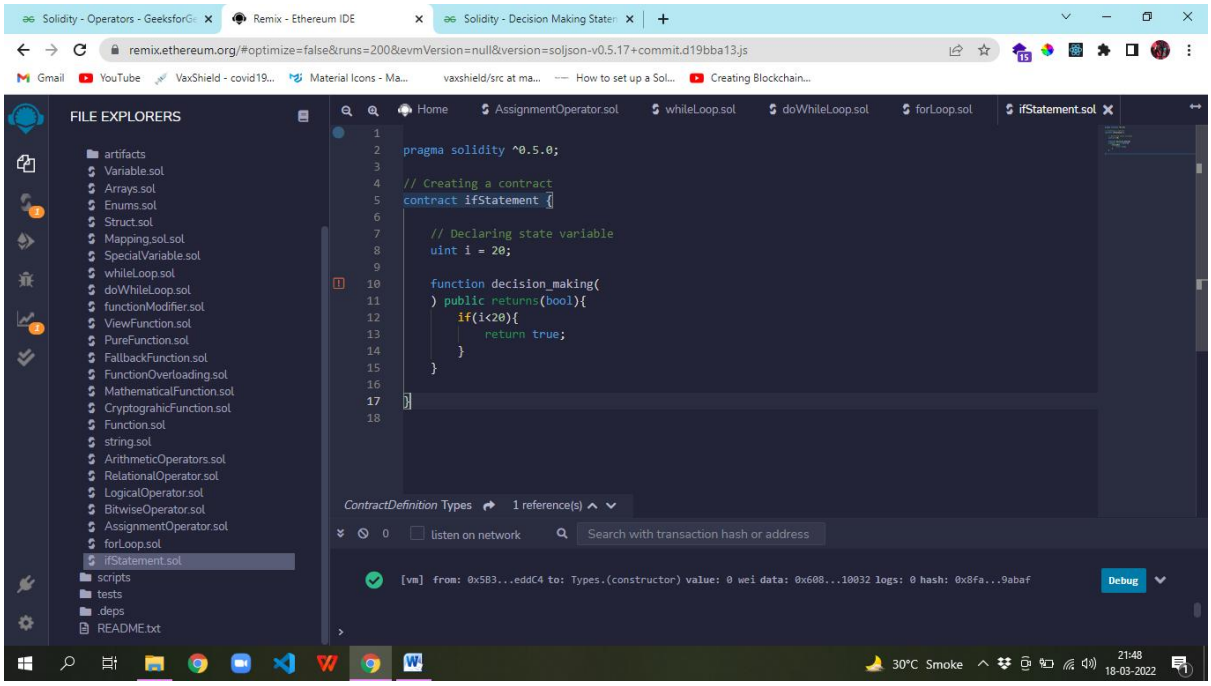
Output :



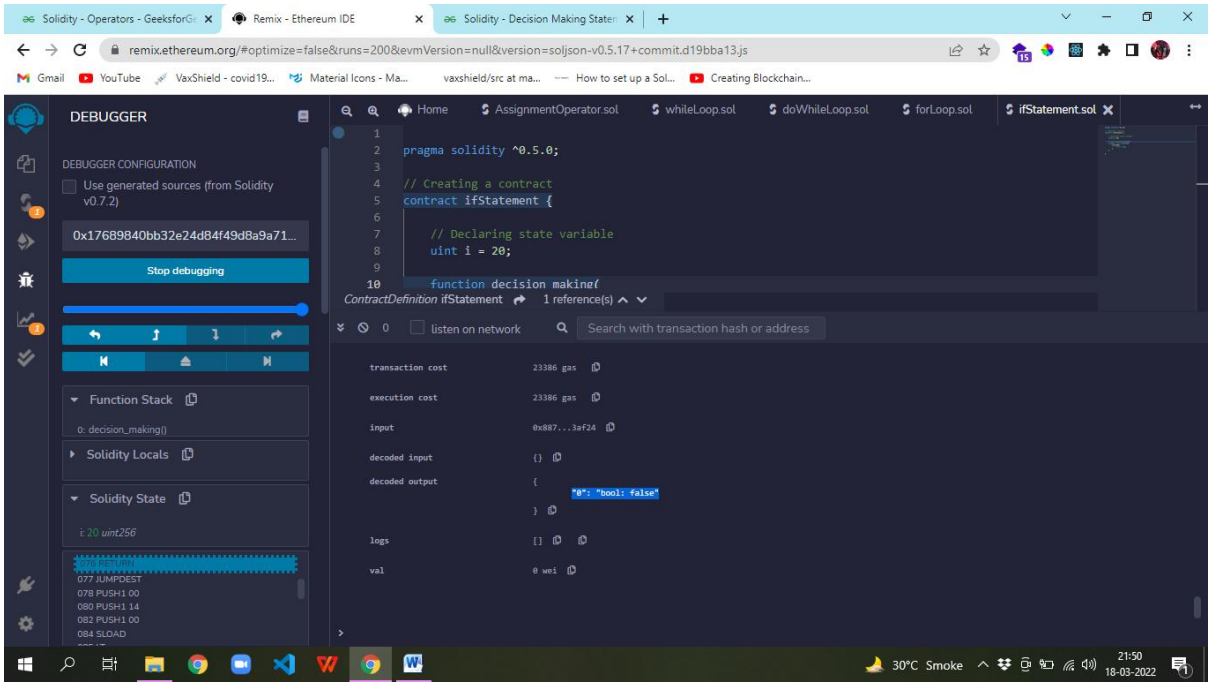
<u>Decision making</u>

If statement

Code:

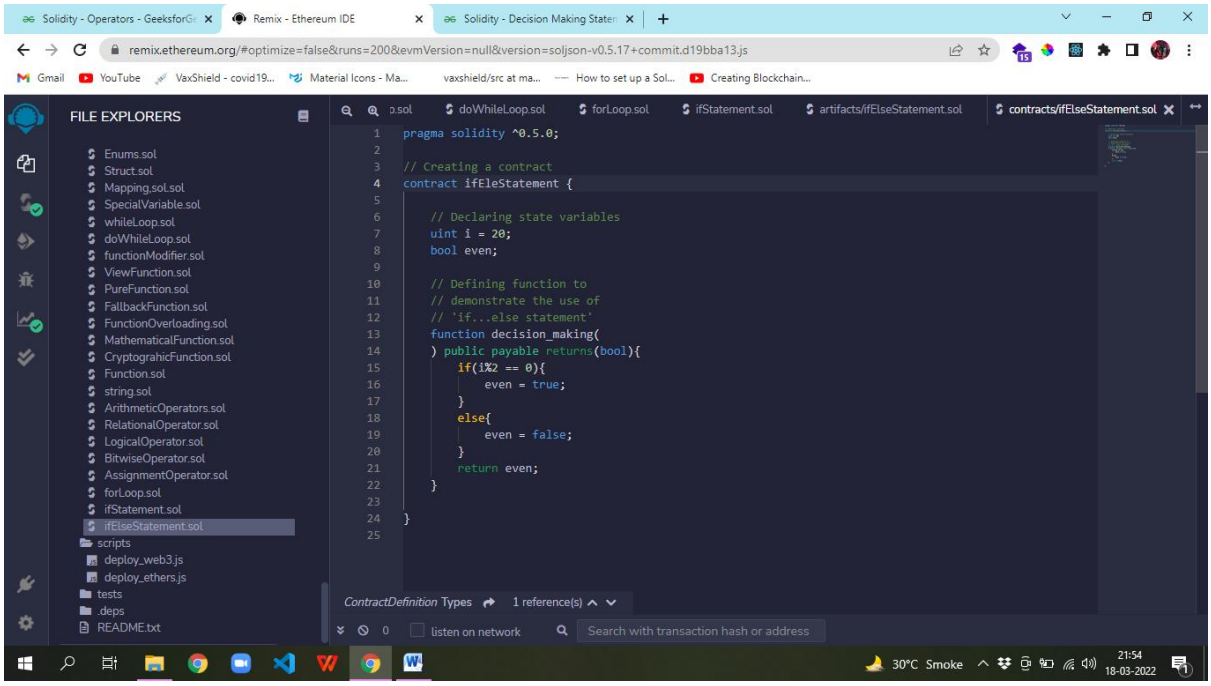


Code :

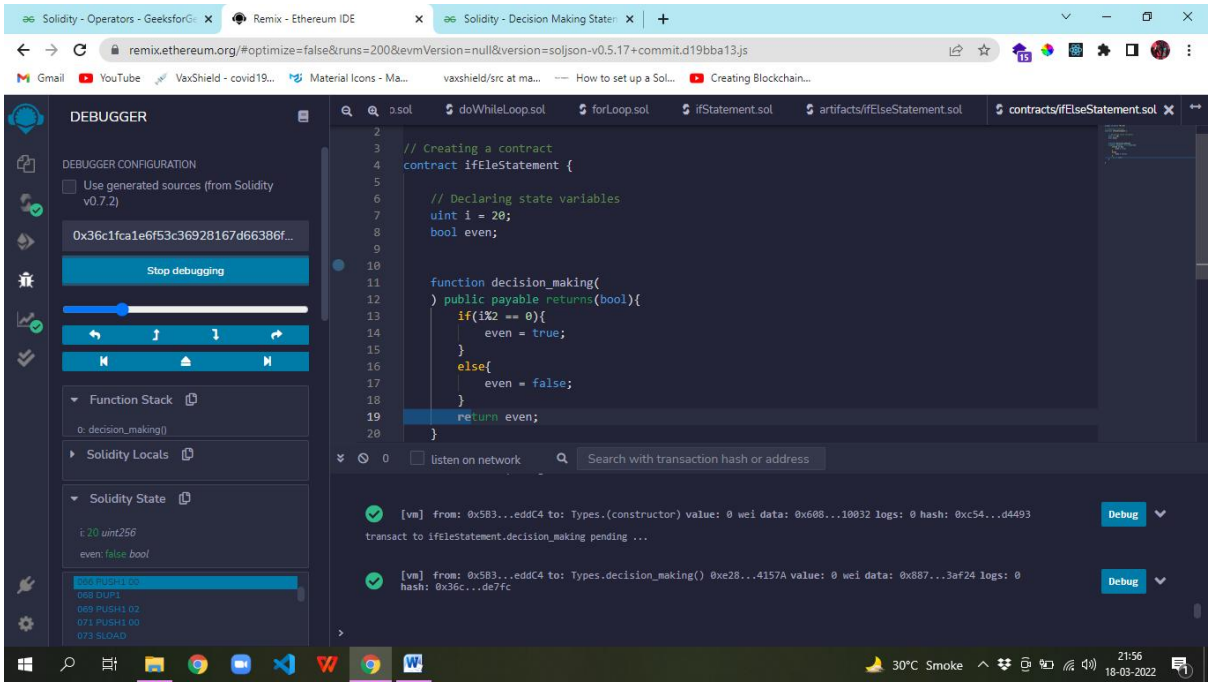


If…else statement

Code :

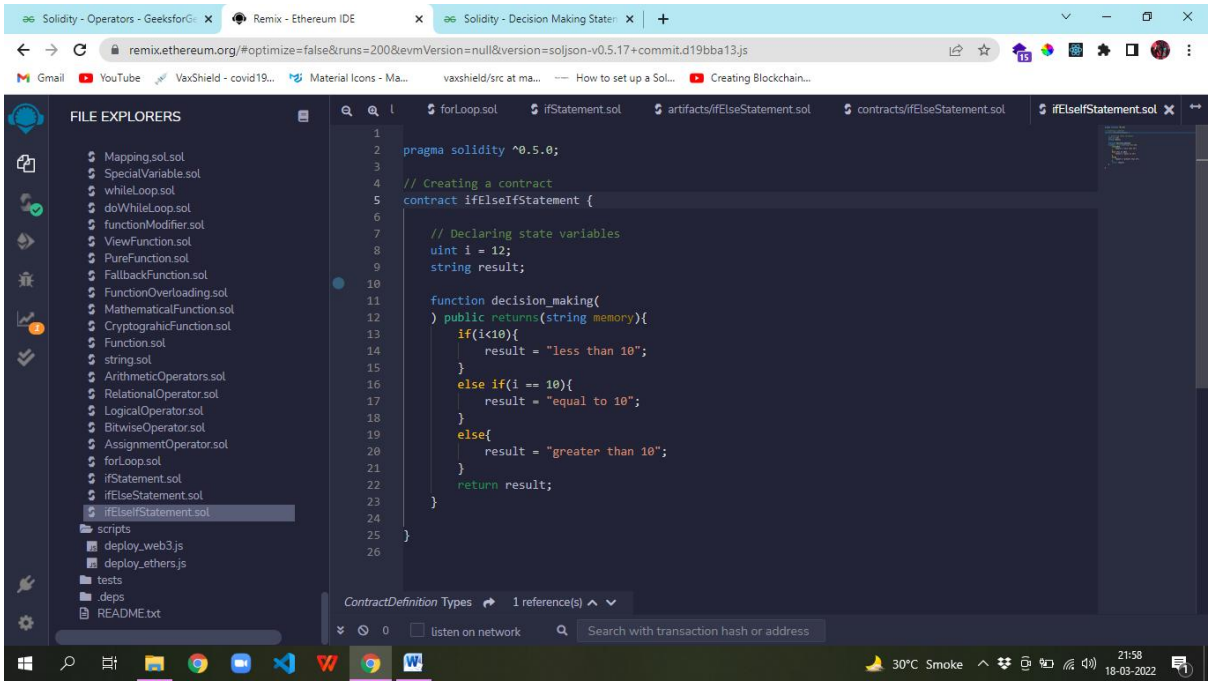


Output :

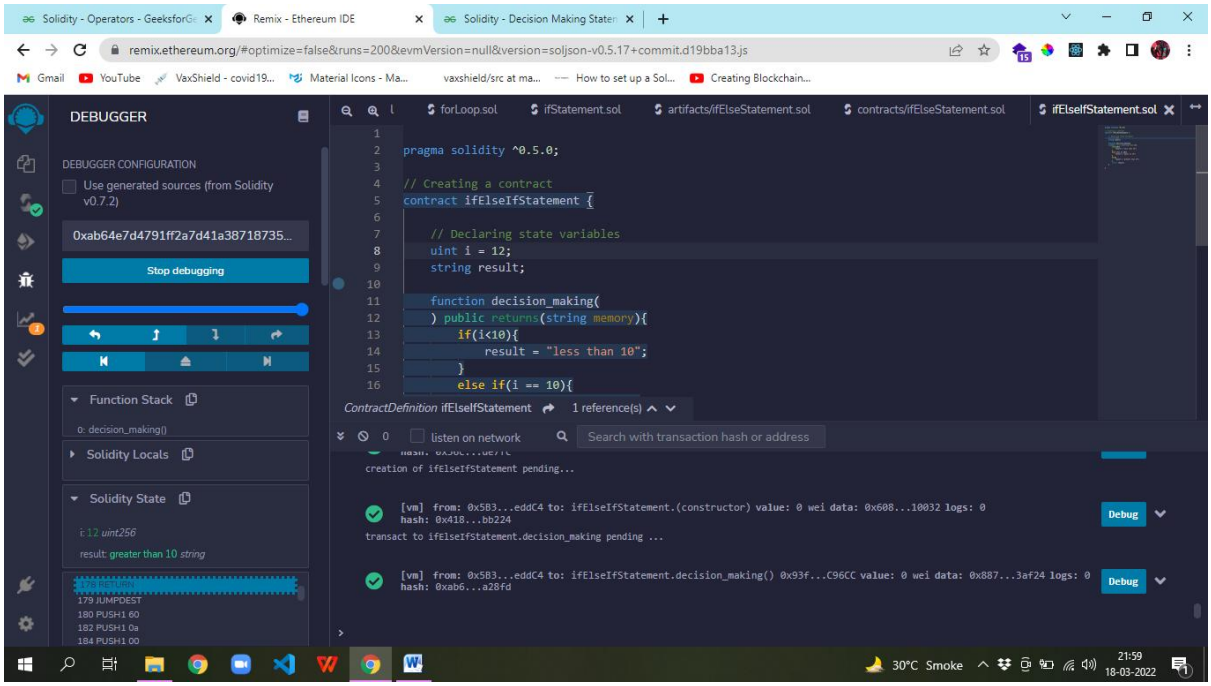


If…else if…else statement

Code :

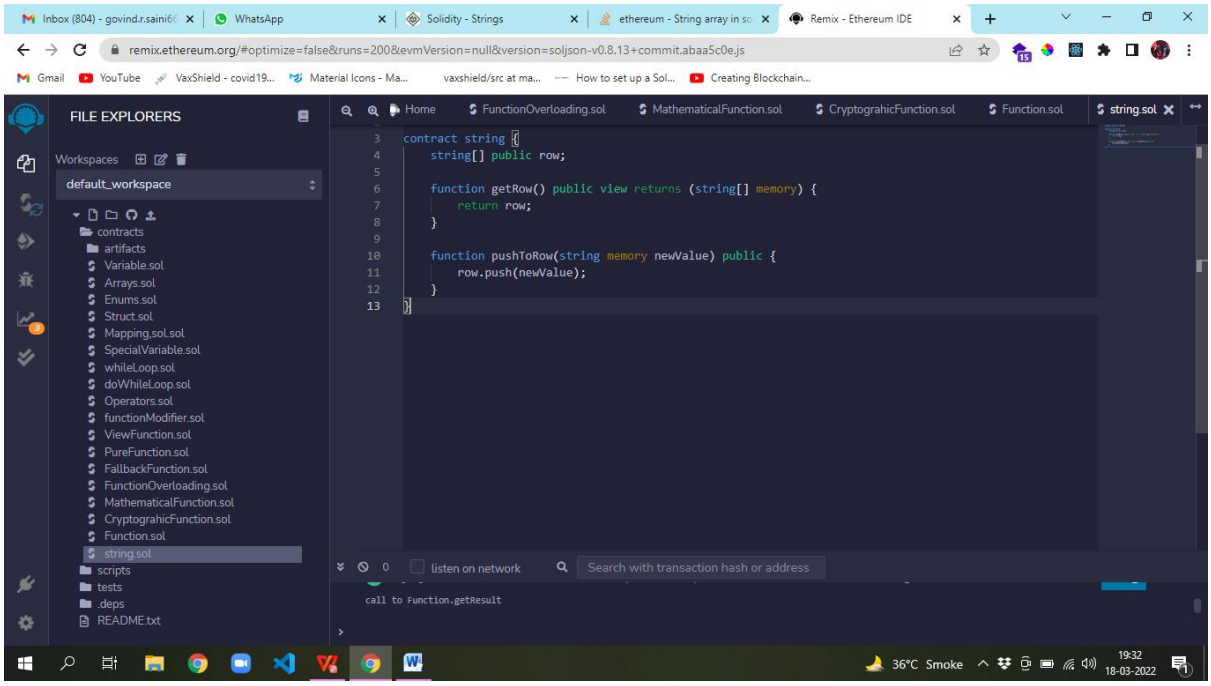


Output:

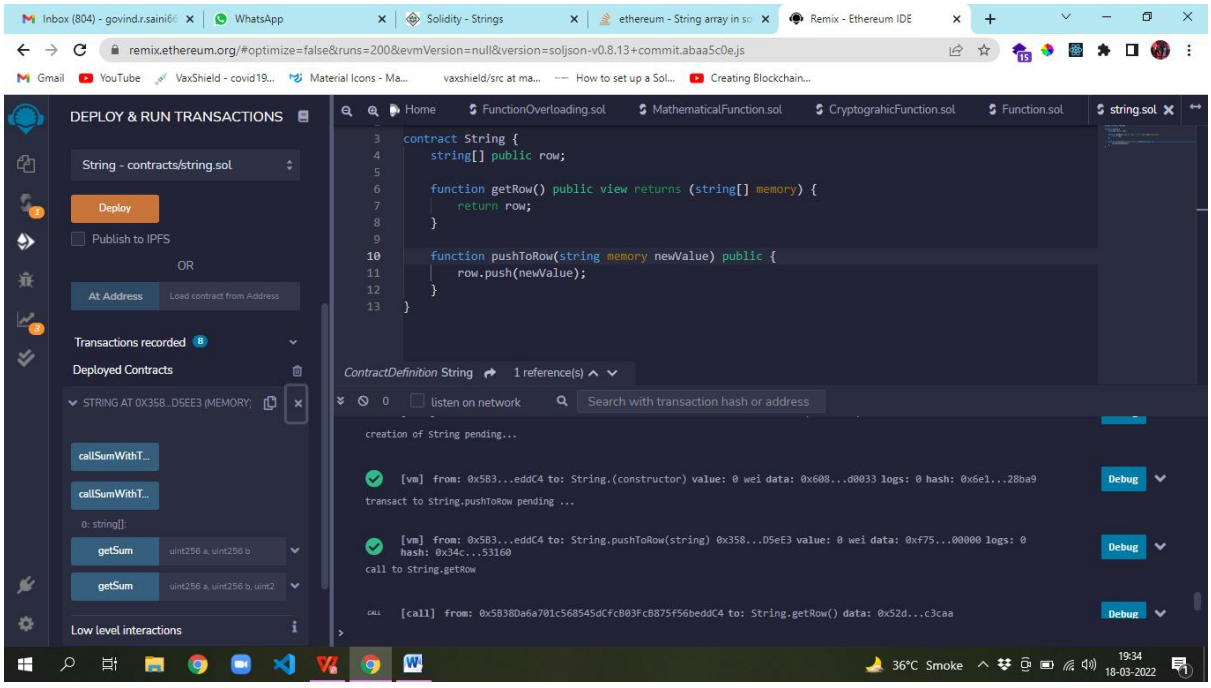


String

Code:

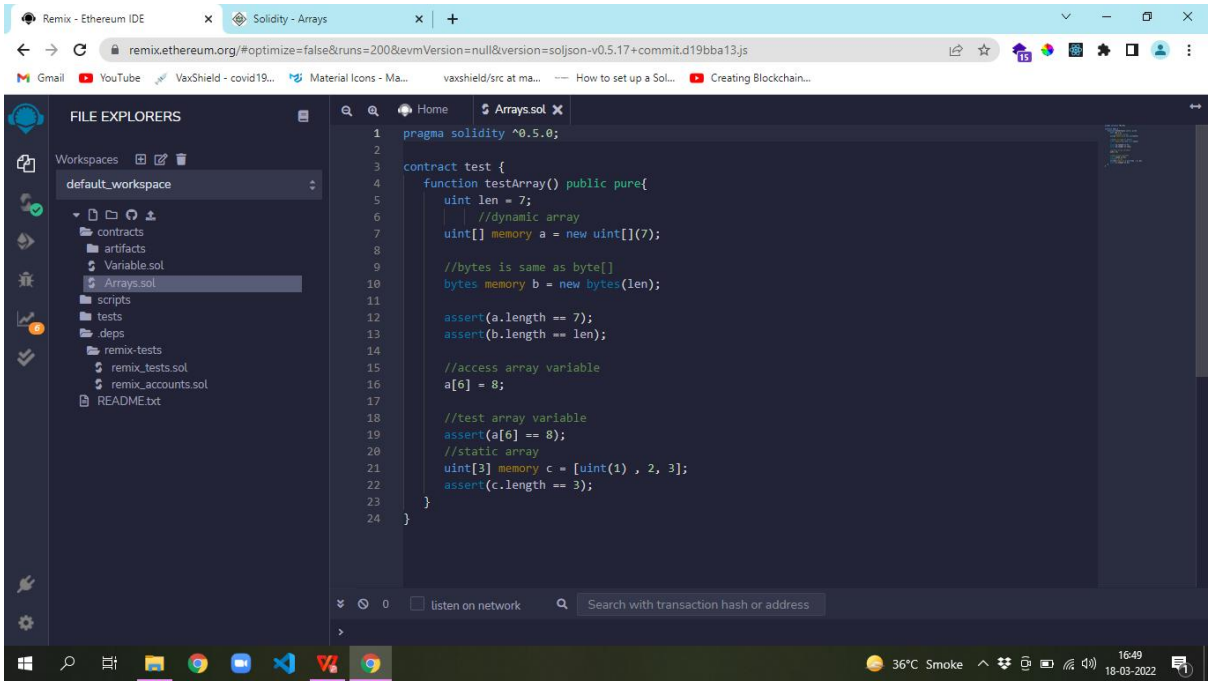


Output :

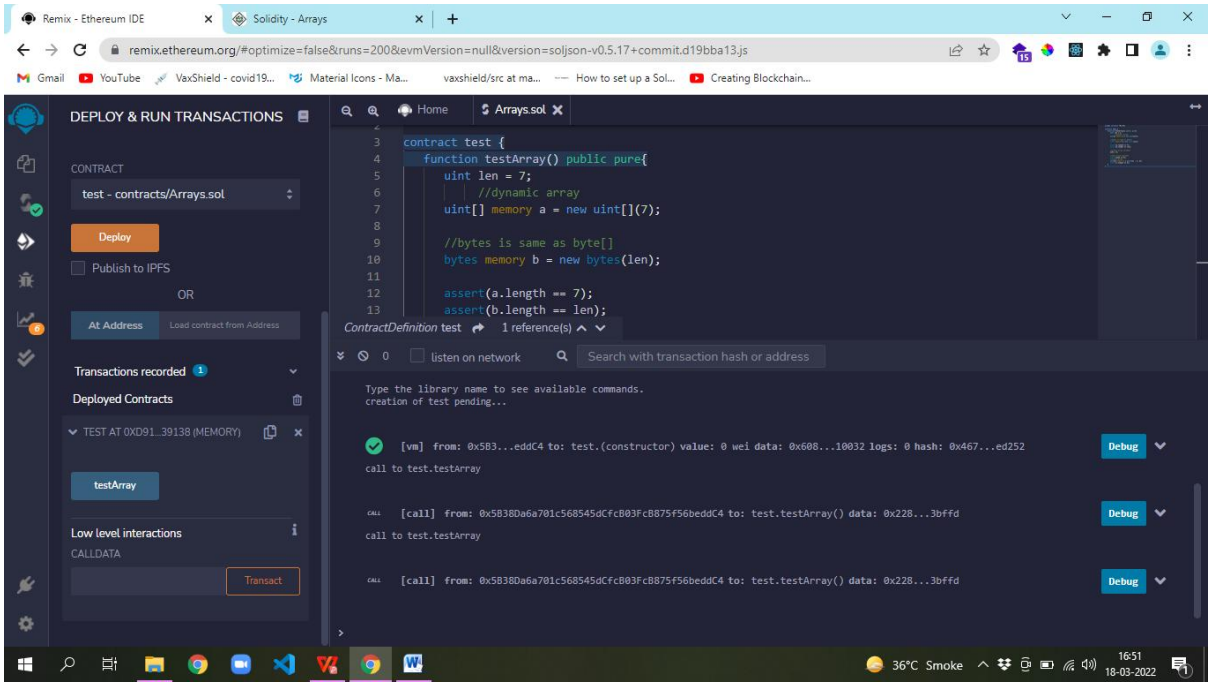


Array

Code :

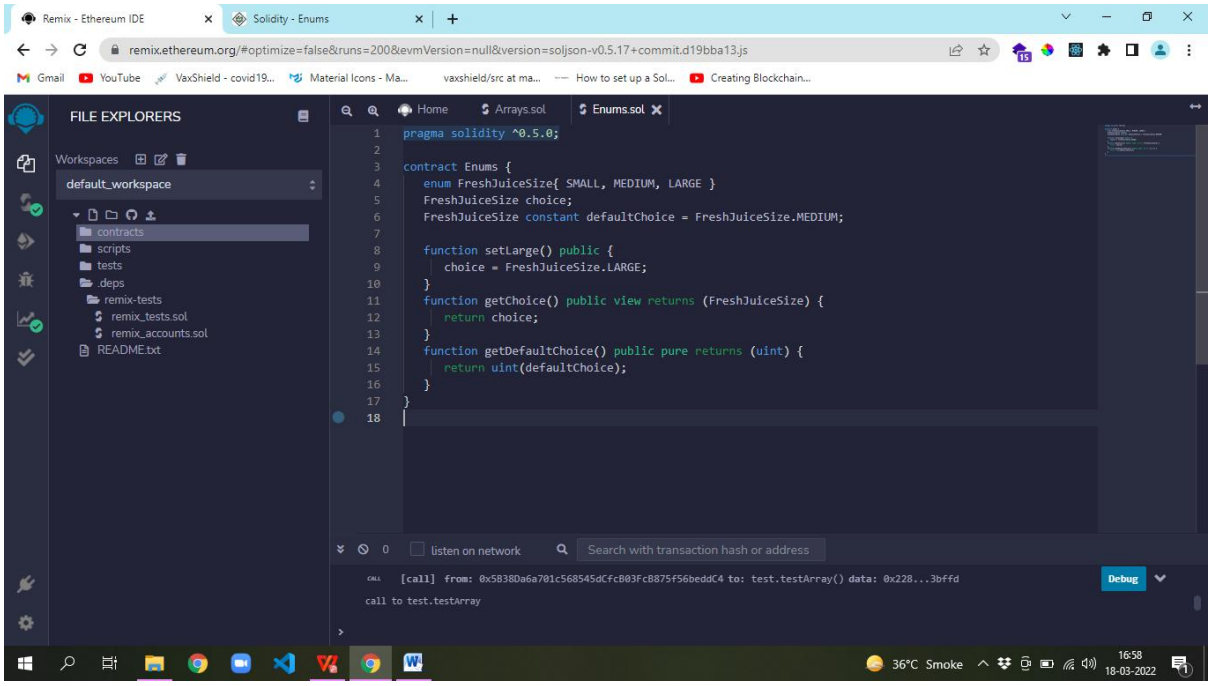


Output:

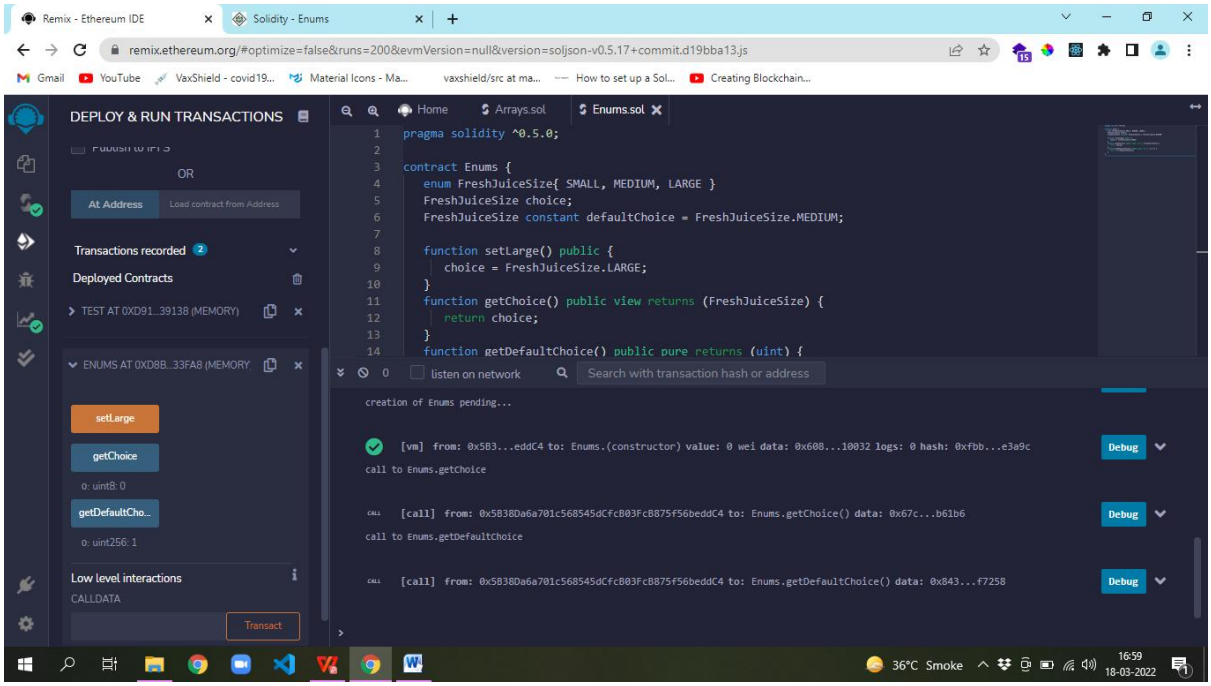


Enums

Code :

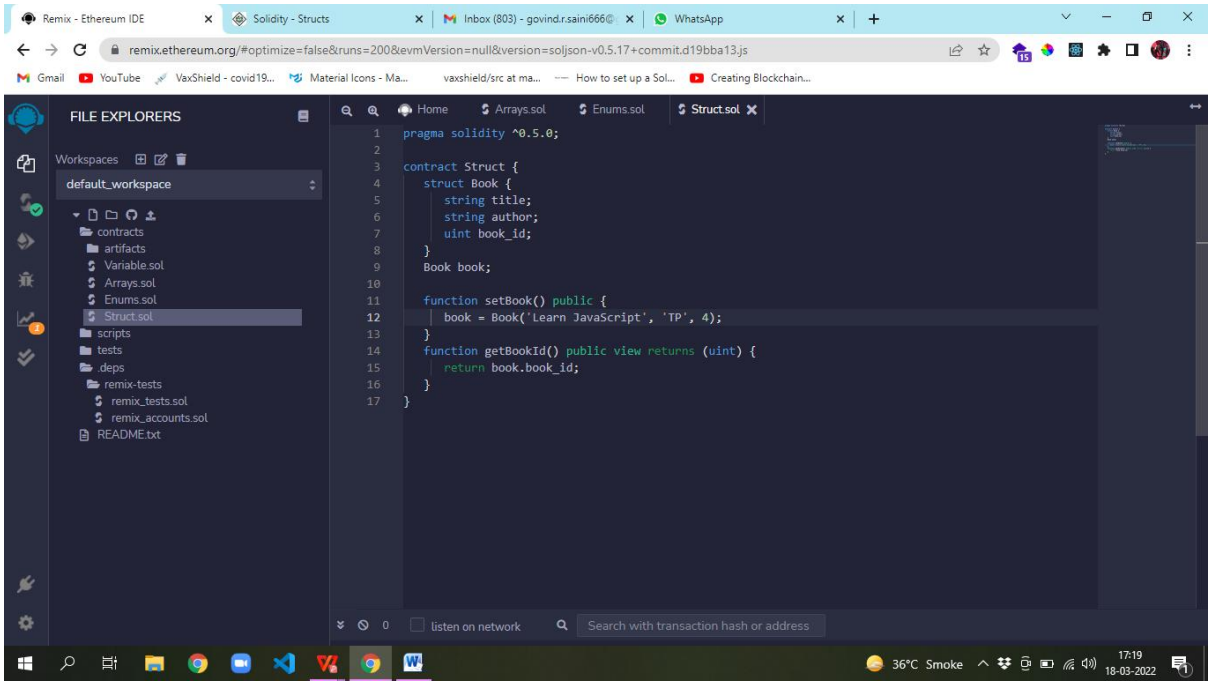


Output :

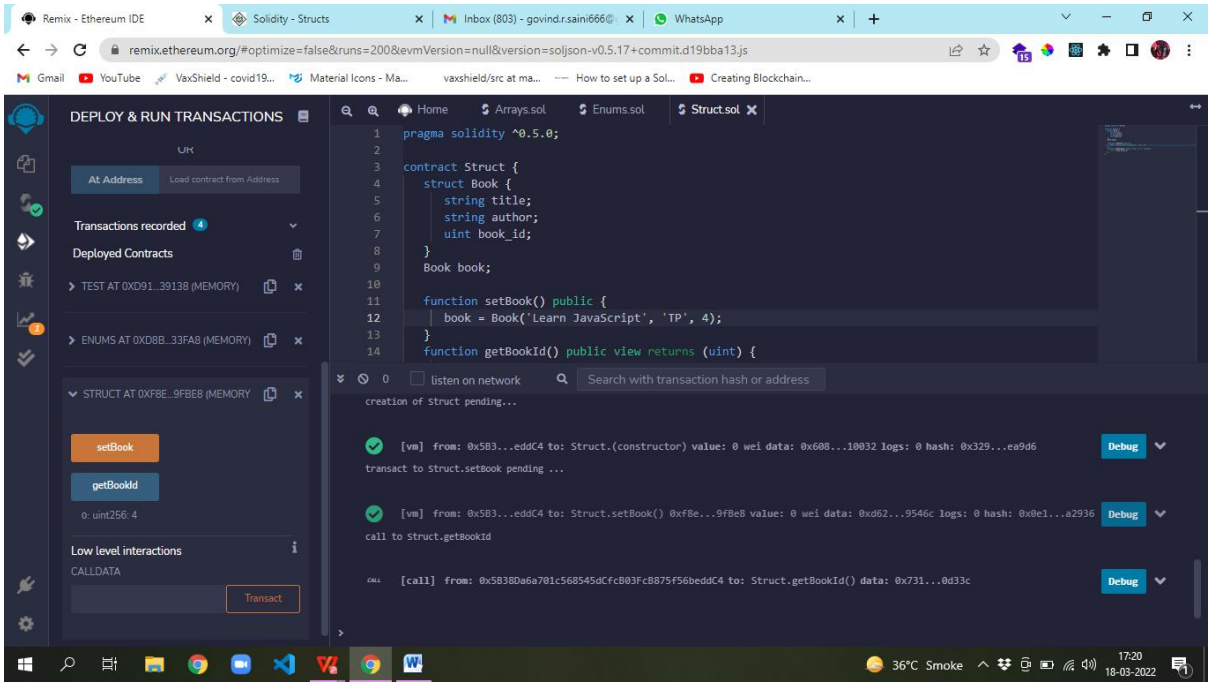


Struct

Code:

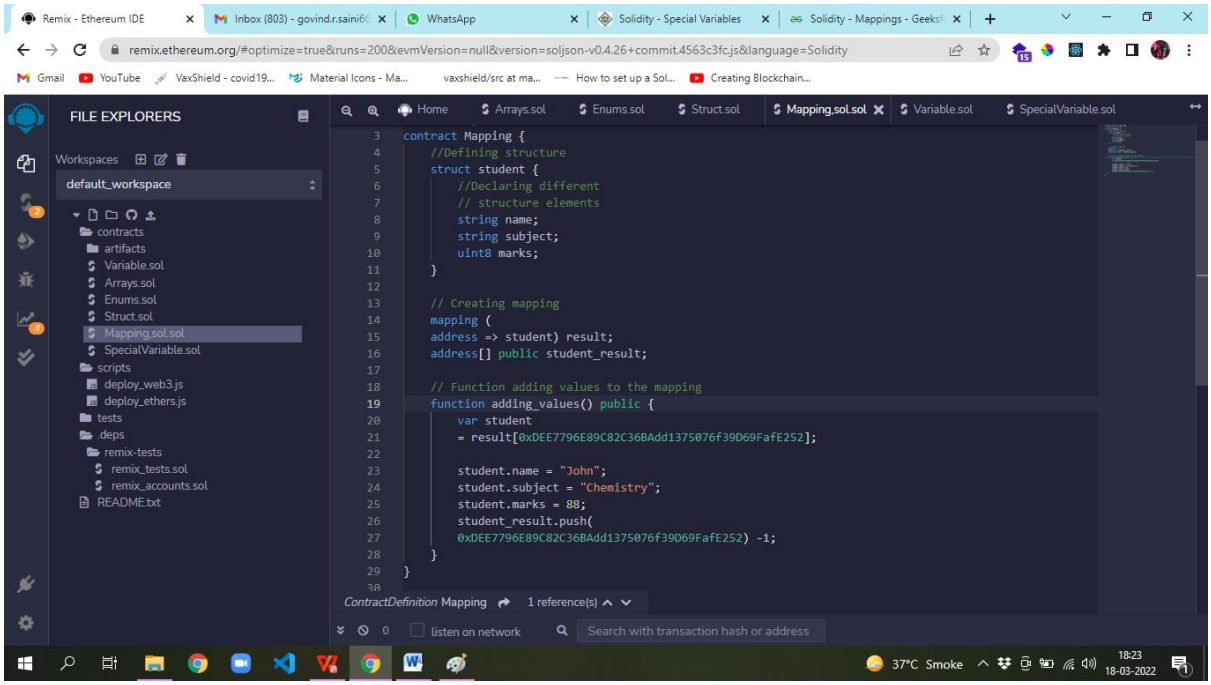


Output:

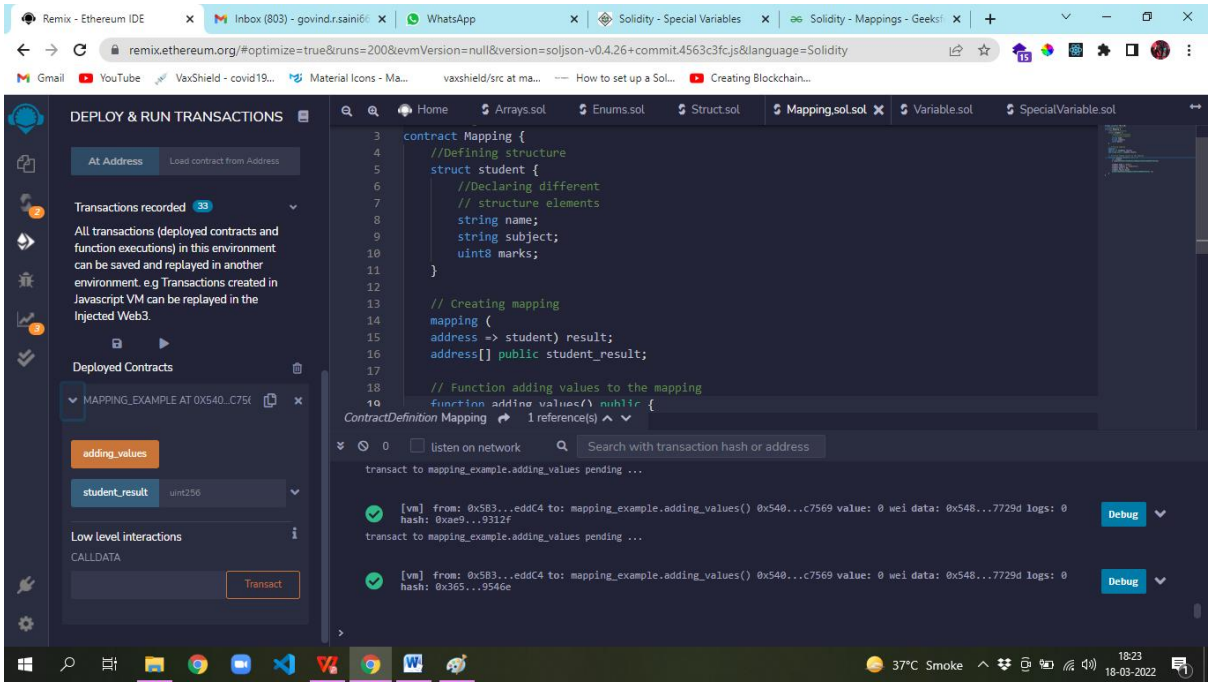


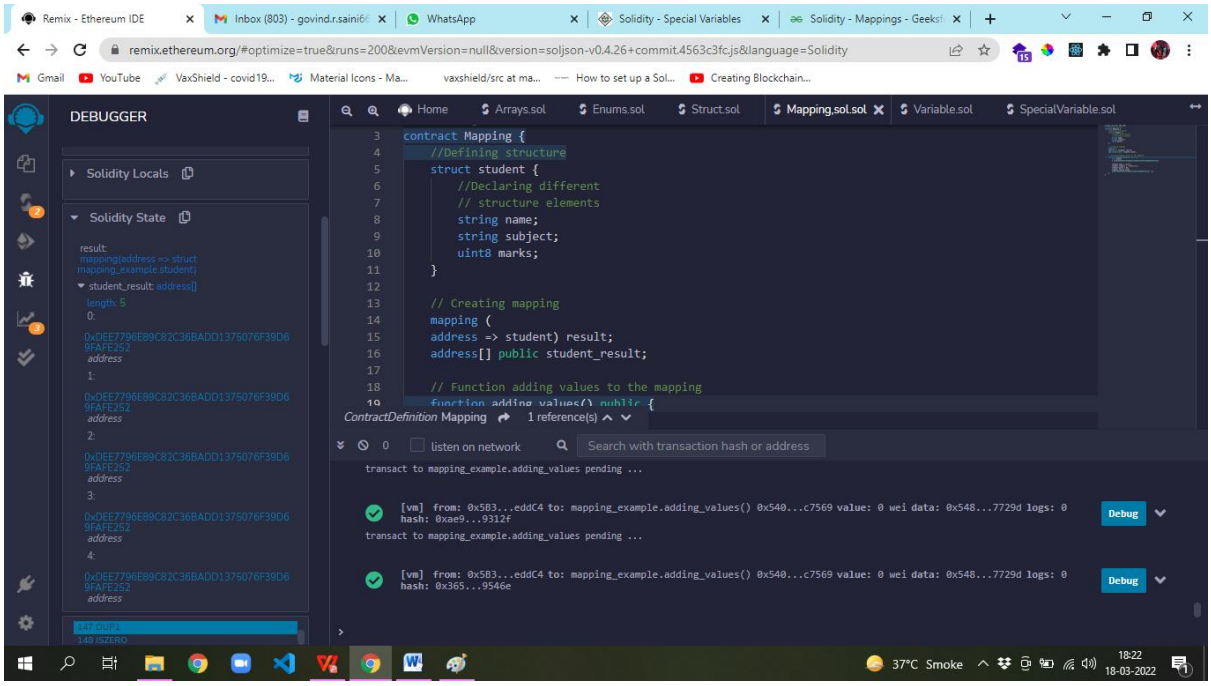
Mapping

Code:


Remix - Ethereum IDE
remix.ethereum.org/#optimize=true&runs=200&evmVersion=null&version=soljson-v0.4.26+commit.4563c3fc.js&language=Solidity
FILE EXPLORERS
Workspaces
default_workspace
contracts
artifacts
Variable.sol
Arrays.sol
Enums.sol
Struct.sol
Mapping.sol.sol
SpecialVariable.sol
scripts
deploy_web3.js
deploy_ethers.js
tests
.deps
remix-tests
remix_tests.sol
remix_accounts.sol
README.txt
Home
Arrays.sol
Enums.sol
Struct.sol
Mapping.sol.sol
Variable.sol
SpecialVariable.sol
contract Mapping {
//Defining structure
struct student {
//Declaring different
// structure elements
string name;
string subject;
uint8 marks;
}
// Creating mapping
mapping (
address => student) result;
address[] public student_result;
// Function adding values to the mapping
function adding_values() public {
var student
= result[0xDEE7796E89C82C36BAdd1375076f39D69FafE252];
student.name = "John";
student.subject = "Chemistry";
student.marks = 88;
student_result.push(
0xDEE7796E89C82C36BAdd1375076f39D69FafE252) -1;
}
}
ContractDefinition Mapping
1 reference(s)
listen on network
Search with transaction hash or address
37°C Smoke
18:23
18-03-2022

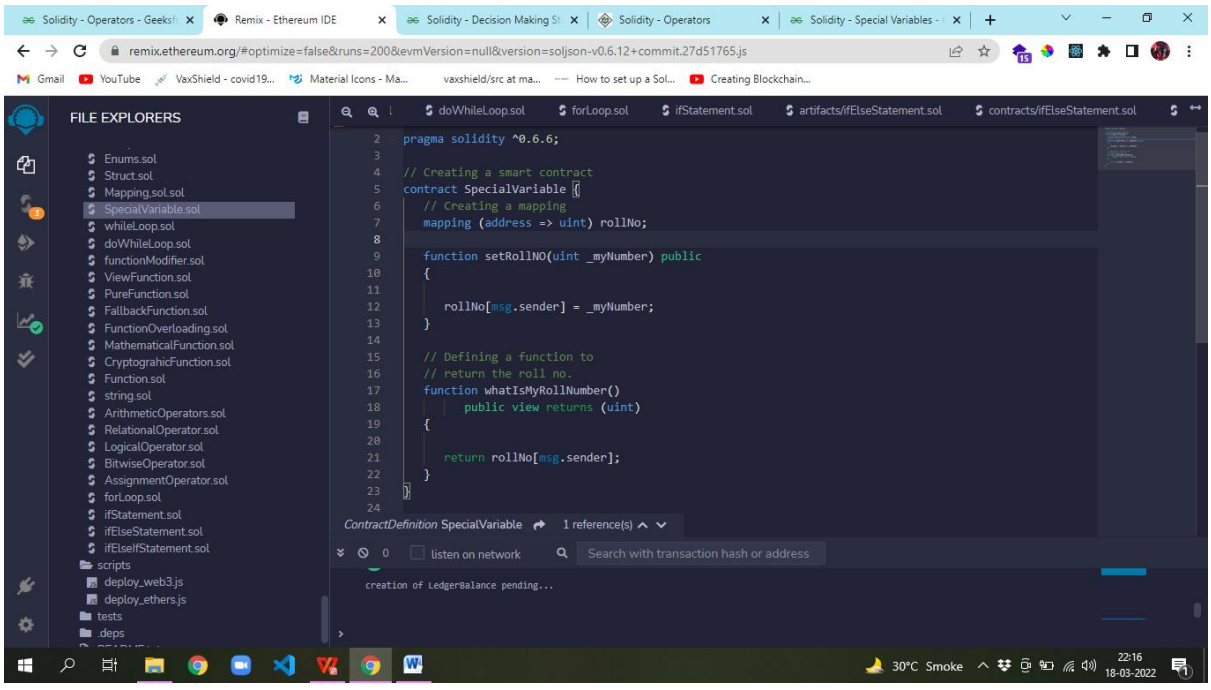
Output :


Remix - Ethereum IDE
remix.ethereum.org/#optimize=true&runs=200&evmVersion=null&version=soljson-v0.4.26+commit.4563c3fc.js&language=Solidity
DEPLOY & RUN TRANSACTIONS
At Address
Load contract from Address
Transactions recorded 33
All transactions (deployed contracts and function executions) in this environment can be saved and replayed in another environment. e.g Transactions created in Javascript VM can be replayed in the Injected Web3.
Deployed Contracts
MAPPING_EXAMPLE AT 0X540...C756
adding_values
student_result
uint256
Low level interactions
CALLDATA
Transact
Home
Arrays.sol
Enums.sol
Struct.sol
Mapping.sol.sol
Variable.sol
SpecialVariable.sol
contract Mapping {
//Defining structure
struct student {
//Declaring different
// structure elements
string name;
string subject;
uint8 marks;
}
// Creating mapping
mapping (
address => student) result;
address[] public student_result;
// Function adding values to the mapping
ContractDefinition Mapping
1 reference(s)
listen on network
Search with transaction hash or address
transact to mapping_example.adding_values pending ...
[vm] from: 0x5B3...eddC4 to: mapping_example.adding_values() 0x540...c7569 value: 0 wei data: 0x548...7729d logs: 0 hash: 0xae9...9312f
Debug
transact to mapping_example.adding_values pending ...
[vm] from: 0x5B3...eddC4 to: mapping_example.adding_values() 0x540...c7569 value: 0 wei data: 0x548...7729d logs: 0 hash: 0x365...9546e
Debug
37°C Smoke
18:23
18-03-2022

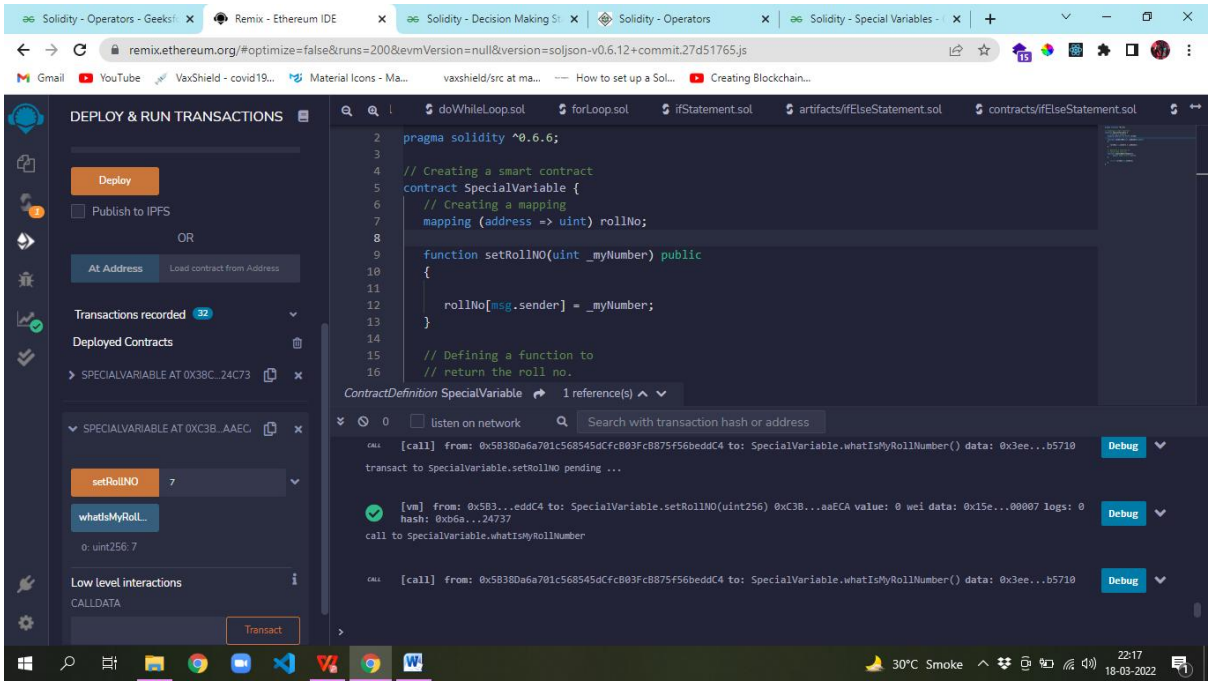


Special Variable

Code:



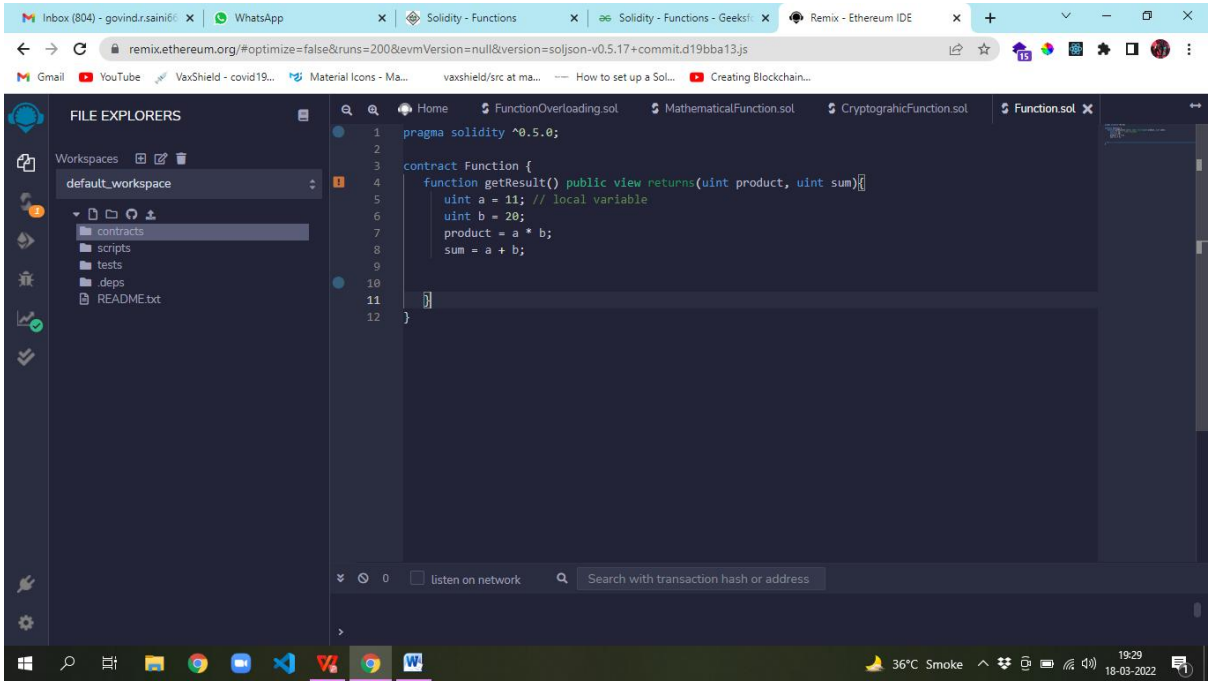
Output


Solidity - Operators - Geeks
Remix - Ethereum IDE
Solidity - Decision Making St
Solidity - Operators
Solidity - Special Variables -
remix.ethereum.org/#optimize=false&runs=200&evmVersion=null&version=soljson-v0.6.12+commit.27d51765.js
Gmail
YouTube
VaxShield - covid19...
Material Icons - Ma...
vaxshield/src at ma...
How to set up a Sol...
Creating Blockchain...
DEPLOY & RUN TRANSACTIONS
Deploy
Publish to IPFS
OR
At Address
Load contract from Address
Transactions recorded 32
Deployed Contracts
SPECIALVARIABLE AT 0X38C...24C73
SPECIALVARIABLE AT 0XC3B...AAEC
setRollNO
7
whatIsMyRoll...
0: uint256: 7
Low level interactions
CALLDATA
Transact
doWhileLoop.sol
forLoop.sol
ifStatement.sol
artifacts/ifElseStatement.sol
contracts/ifElseStatement.sol
pragma solidity ^0.6.6;
// Creating a smart contract
contract SpecialVariable {
// Creating a mapping
mapping (address => uint) rollNo;
function setRollNO(uint _myNumber) public
{
rollNo[msg.sender] = _myNumber;
}
// Defining a function to
// return the roll no.
ContractDefinition SpecialVariable
1 reference(s)
listen on network
Search with transaction hash or address
[call] from: 0x5B38Da6a701c568545dCfcB03FcB875f56beddC4 to: SpecialVariable.whatIsMyRollNumber() data: 0x3ee...b5710
Debug
transact to SpecialVariable.setRollNO pending ...
[vm] from: 0x5B3...eddC4 to: SpecialVariable.setRollNO(uint256) 0xC3B...aaECA value: 0 wei data: 0x15e...00007 logs: 0 hash: 0xb6a...24737
Debug
call to SpecialVariable.whatIsMyRollNumber
[call] from: 0x5B38Da6a701c568545dCfcB03FcB875f56beddC4 to: SpecialVariable.whatIsMyRollNumber() data: 0x3ee...b5710
Debug
30°C Smoke
22:17
18-03-2022

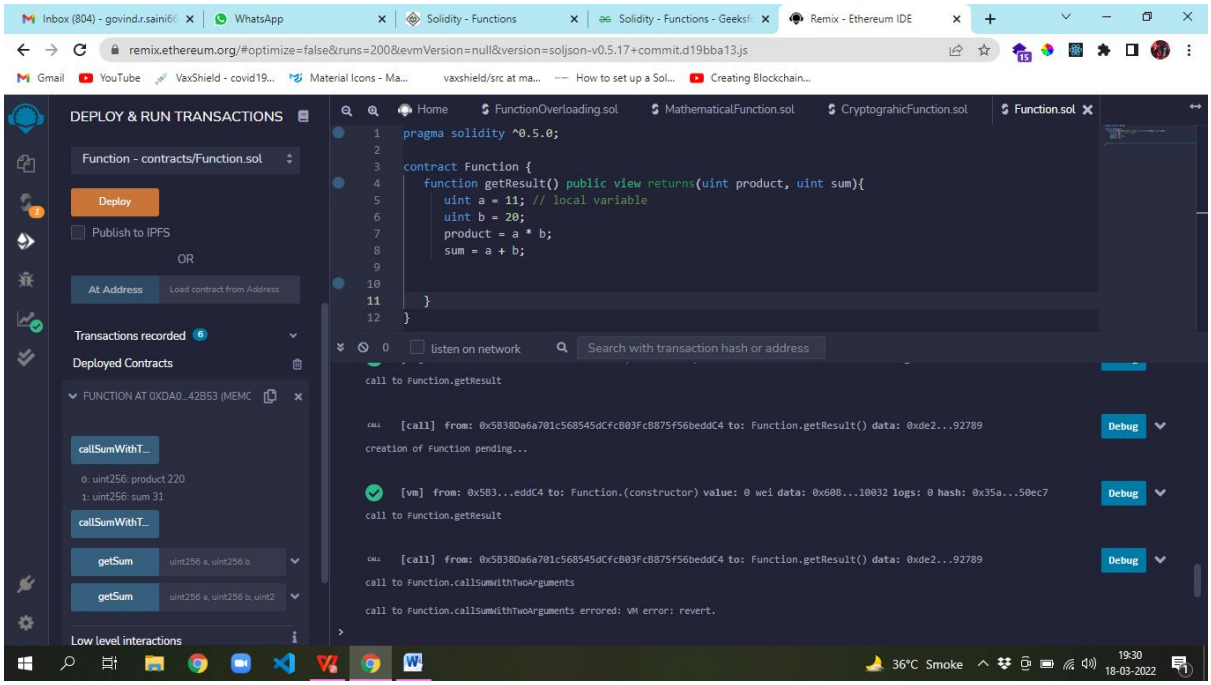
3b) Functions, Function Modifiers, View functions, Pure Functions, Fallback Function, Function Overloading, Mathematical functions, Cryptographic functions.

Function

Code:

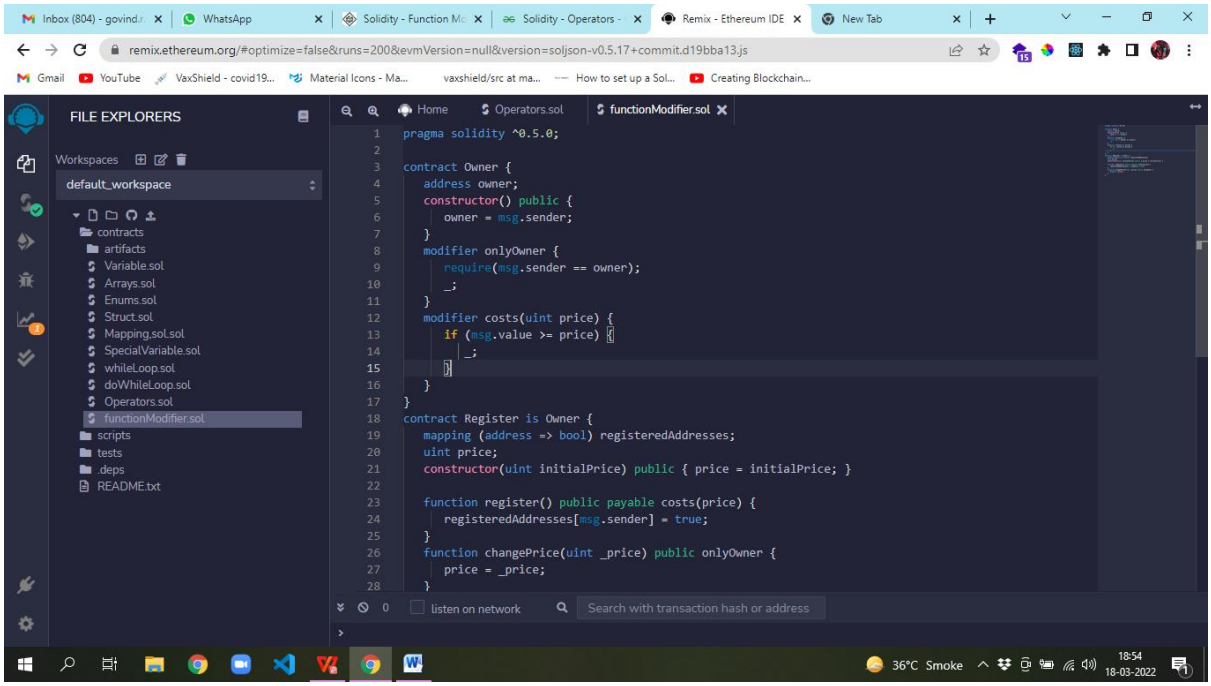


Output:

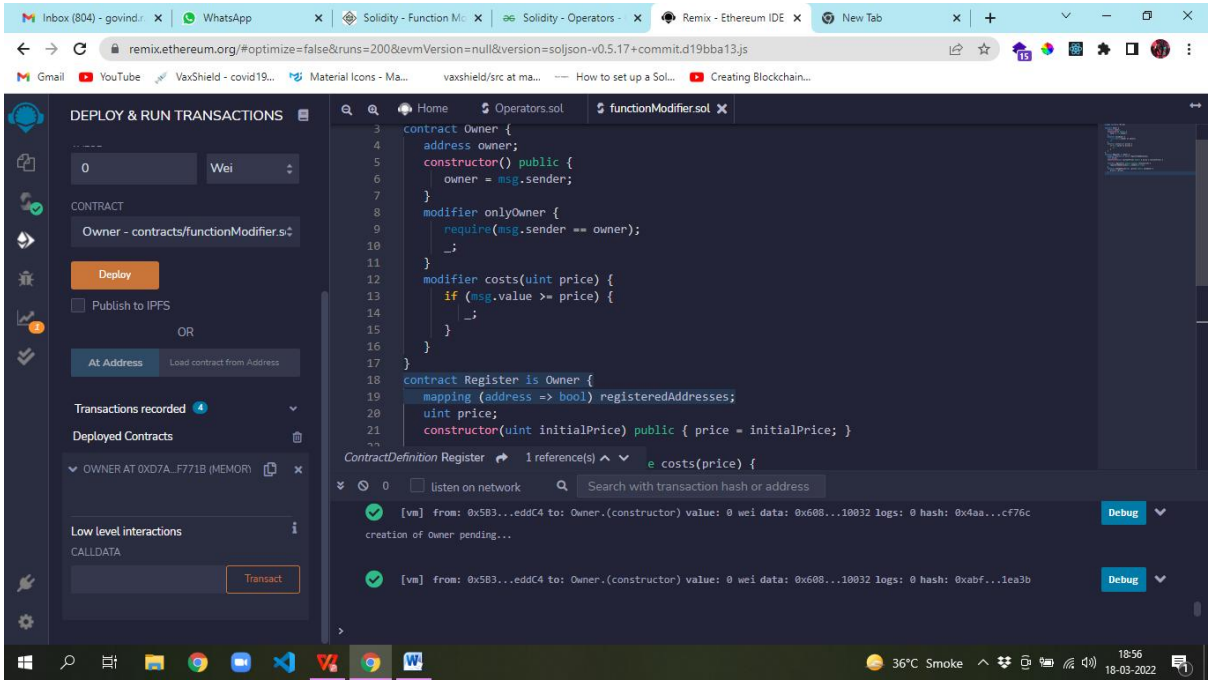


Functions Modifiers

Code :

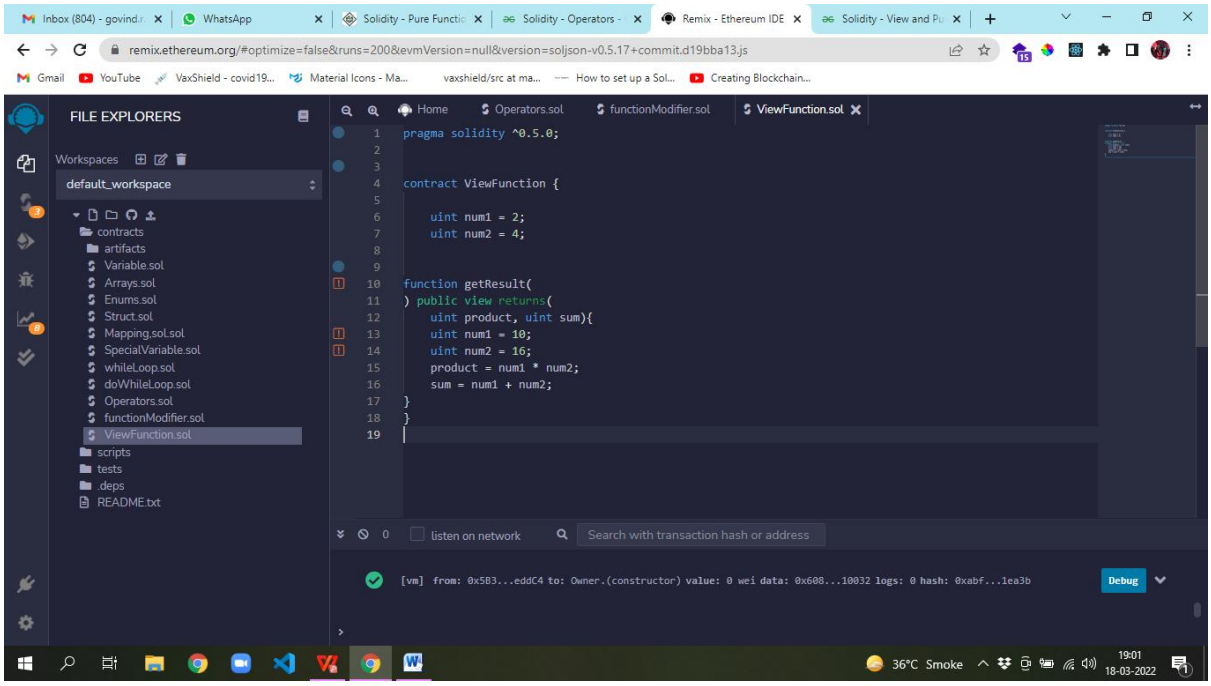


Output :

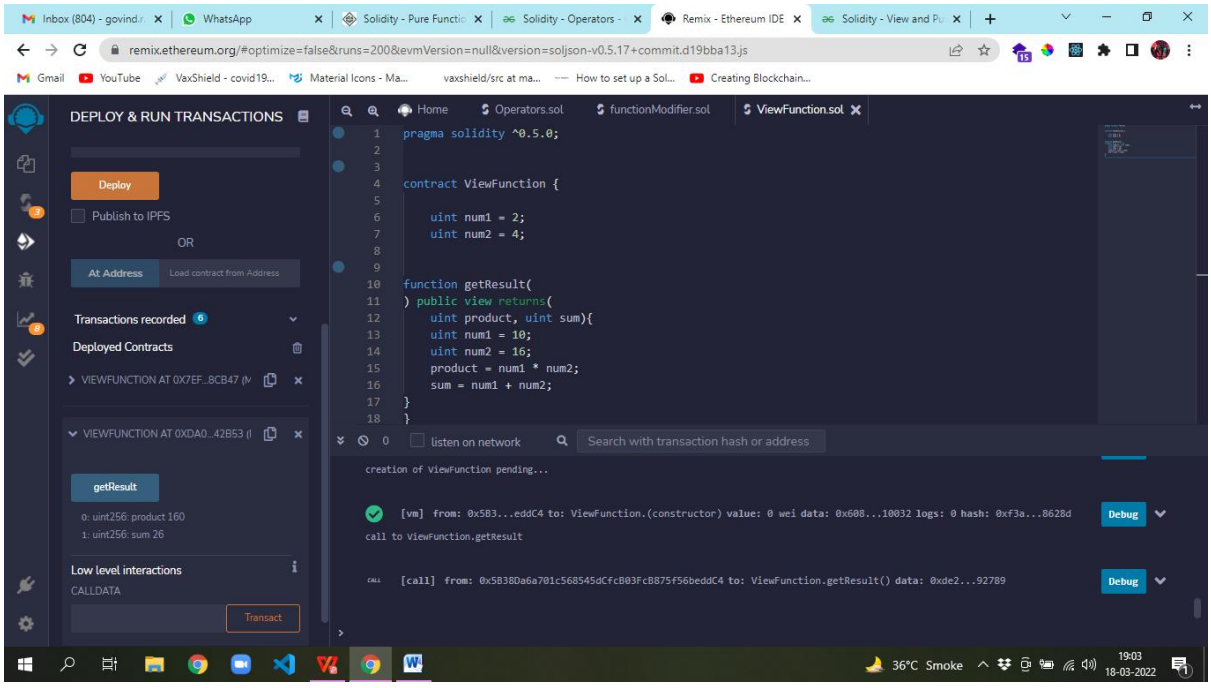


View function

Code:

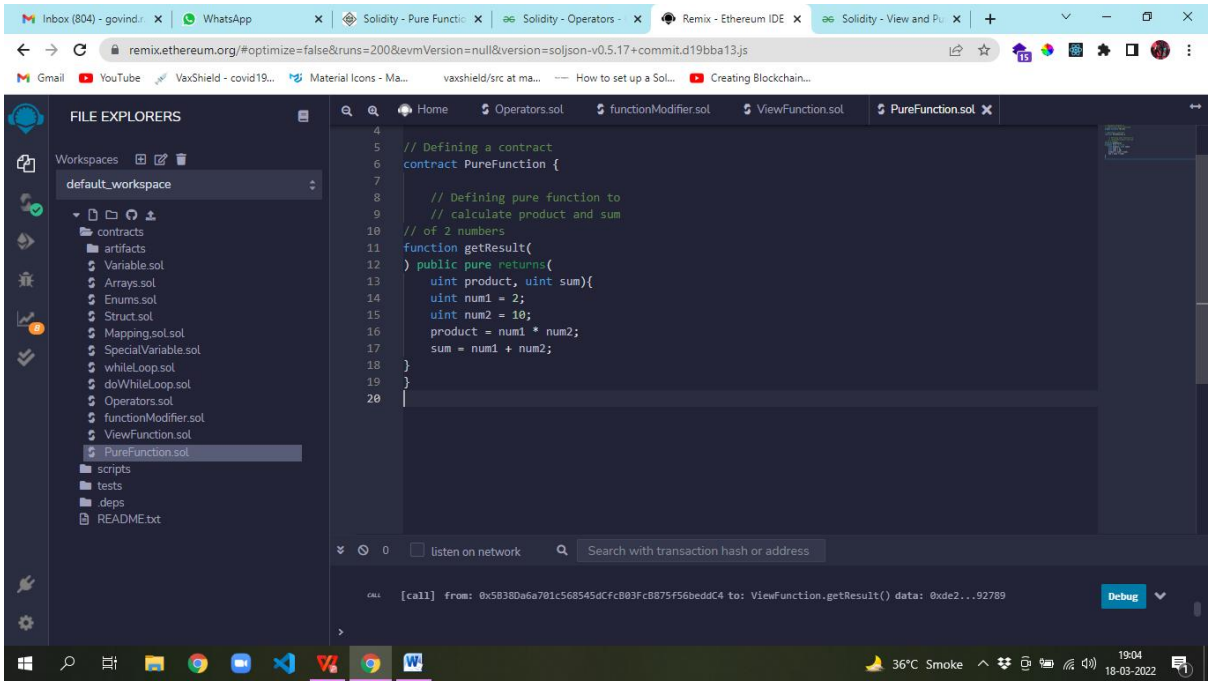


Output :

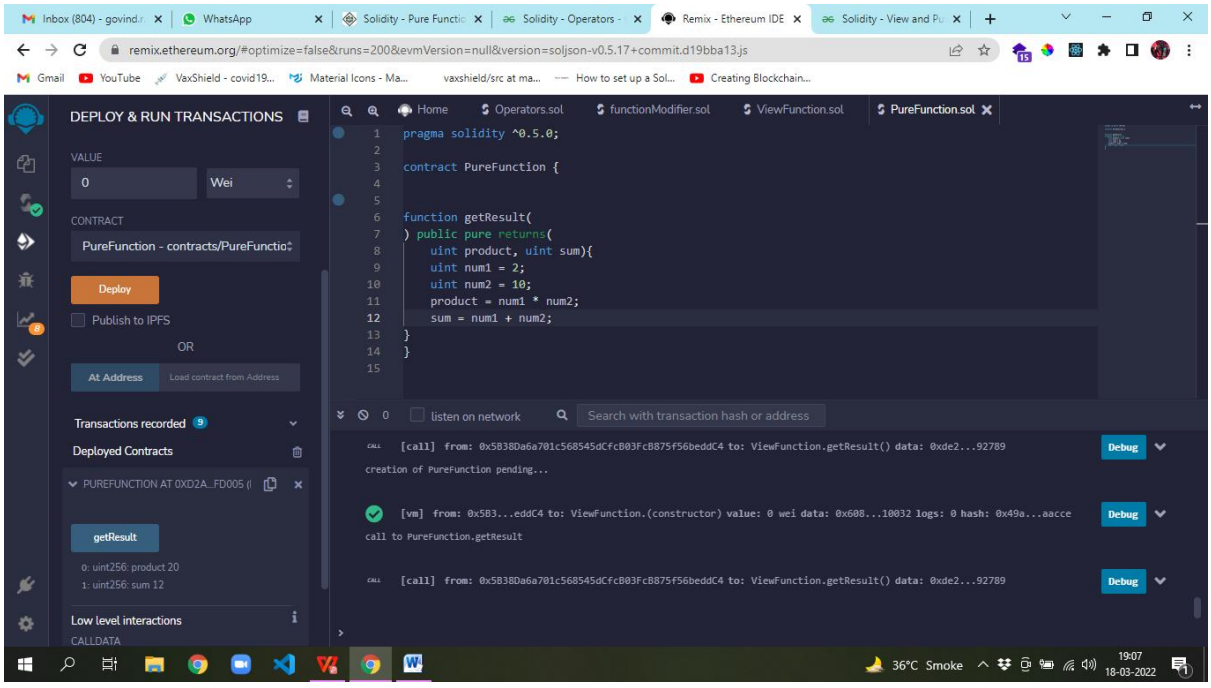


Pure function

Code :

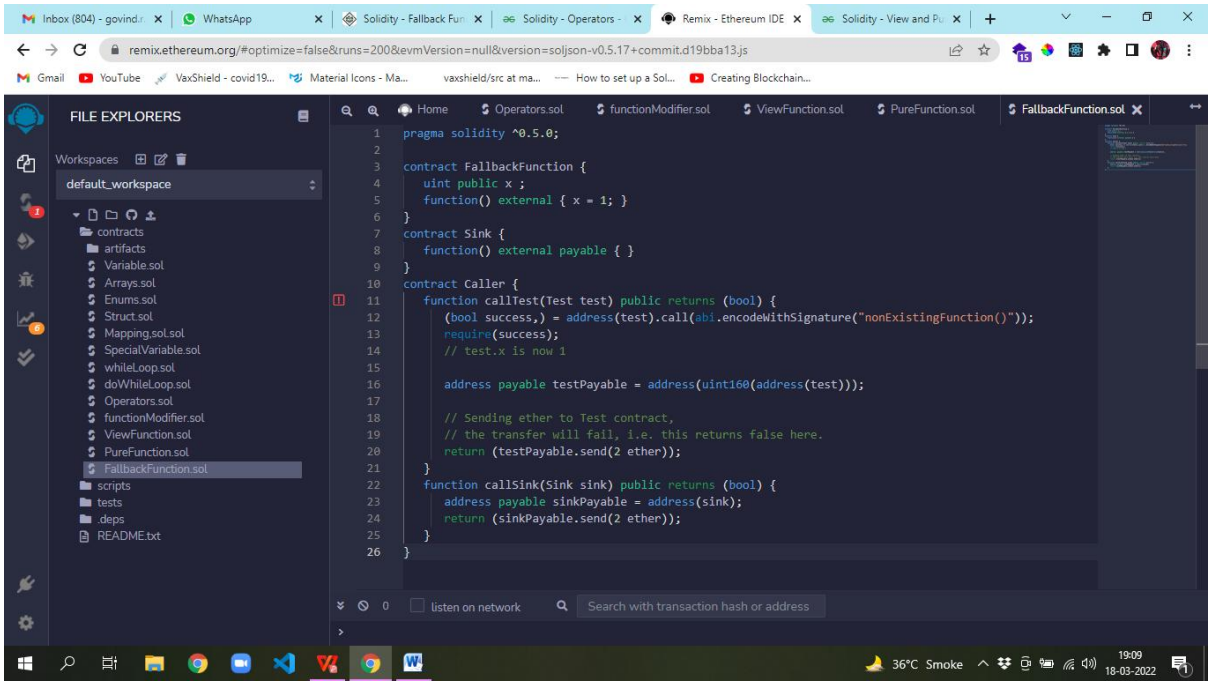


Output:

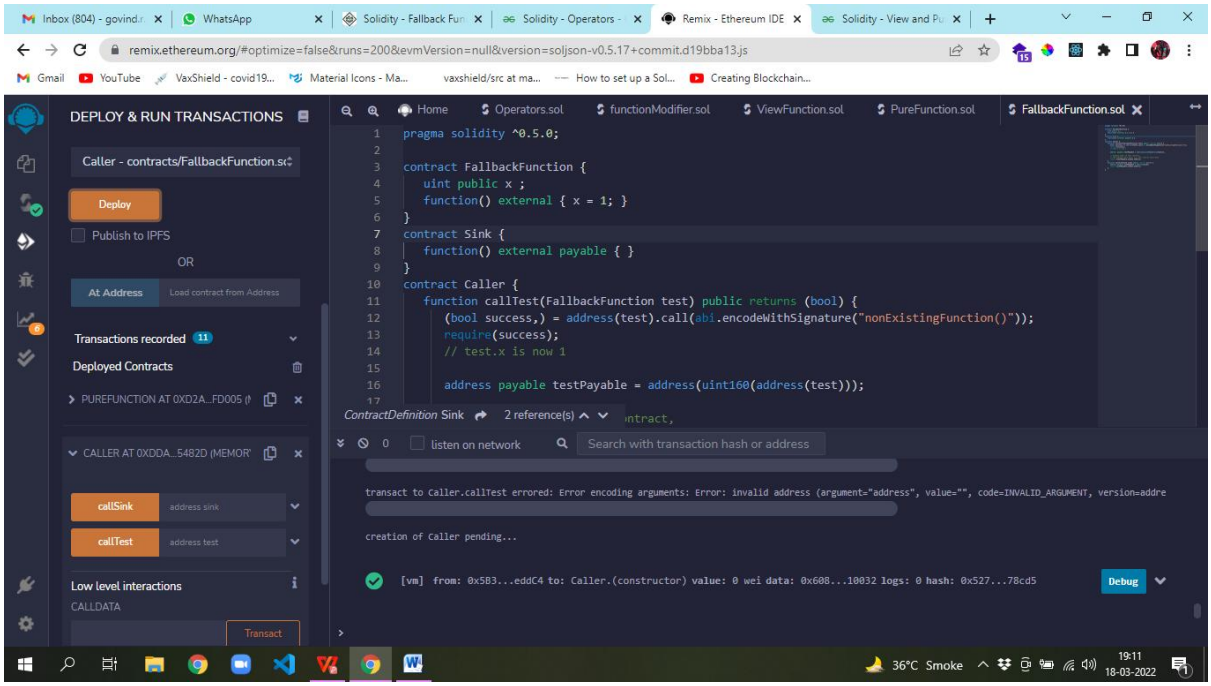


Fallback function

Code:

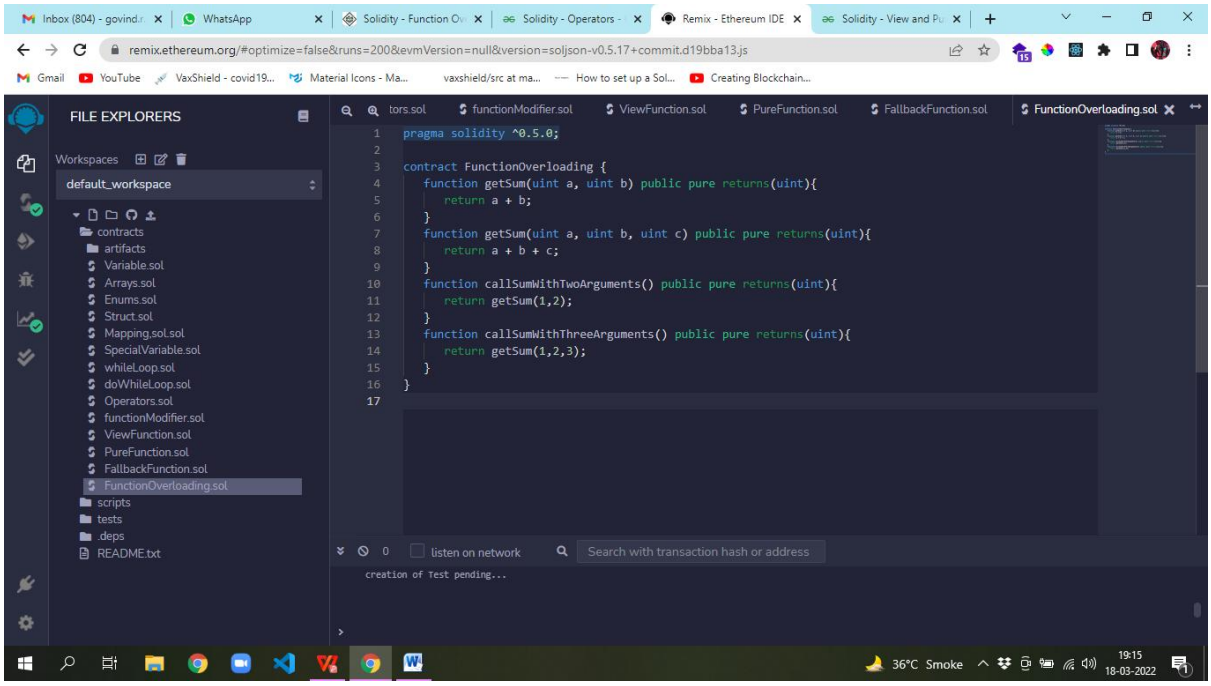


Output :

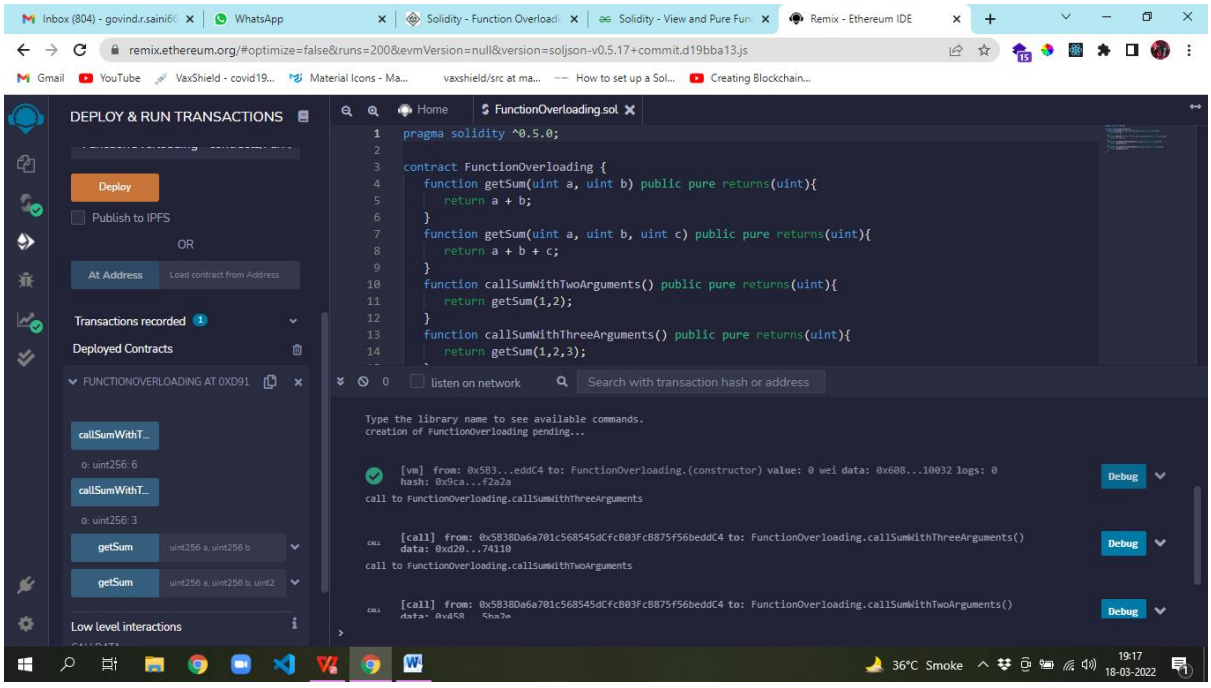


Function Overloading

Code:

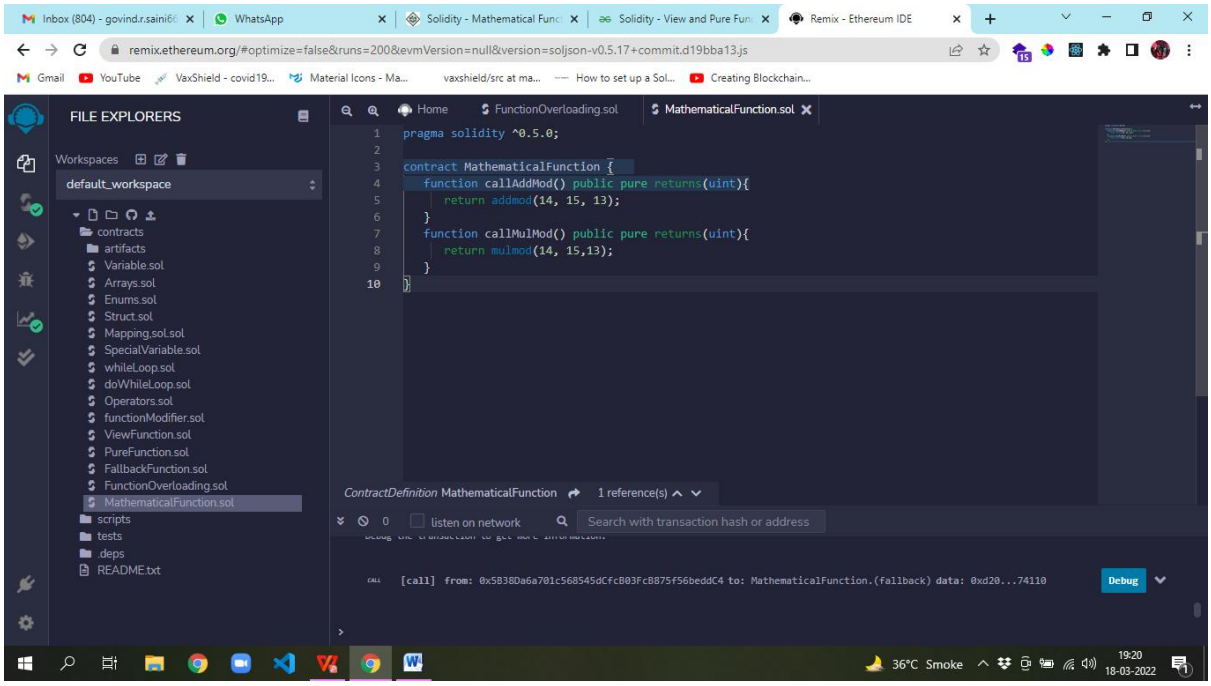


Output :

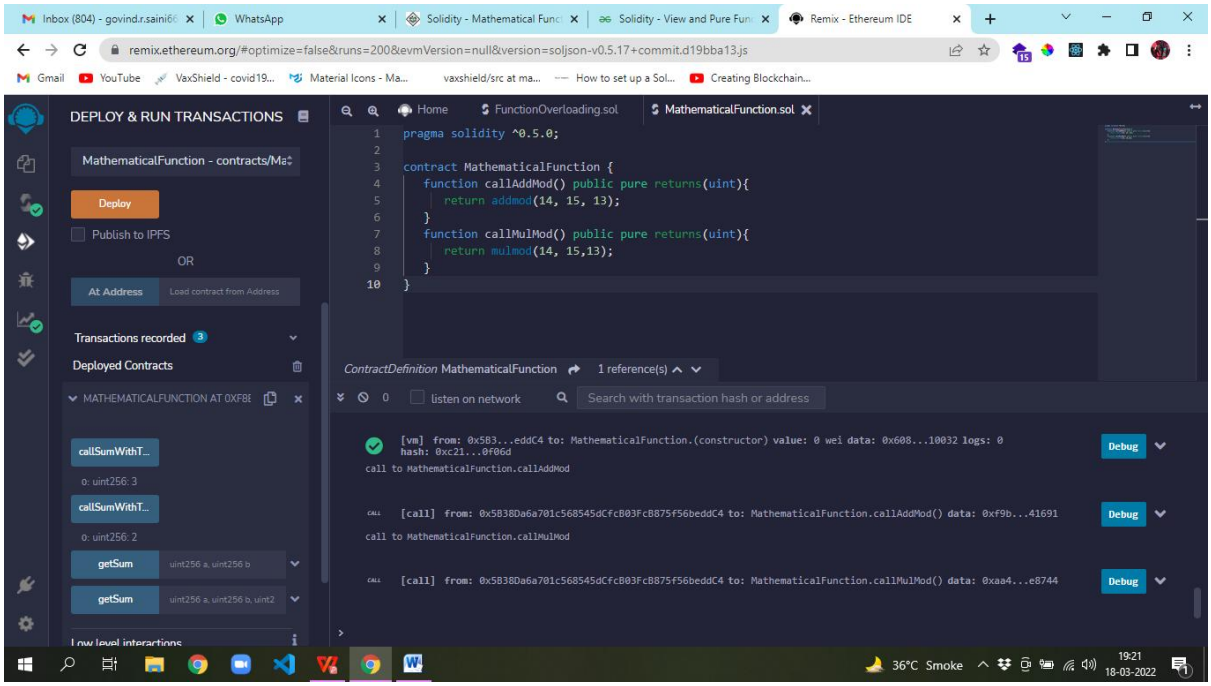


Mathematical Function

Code:

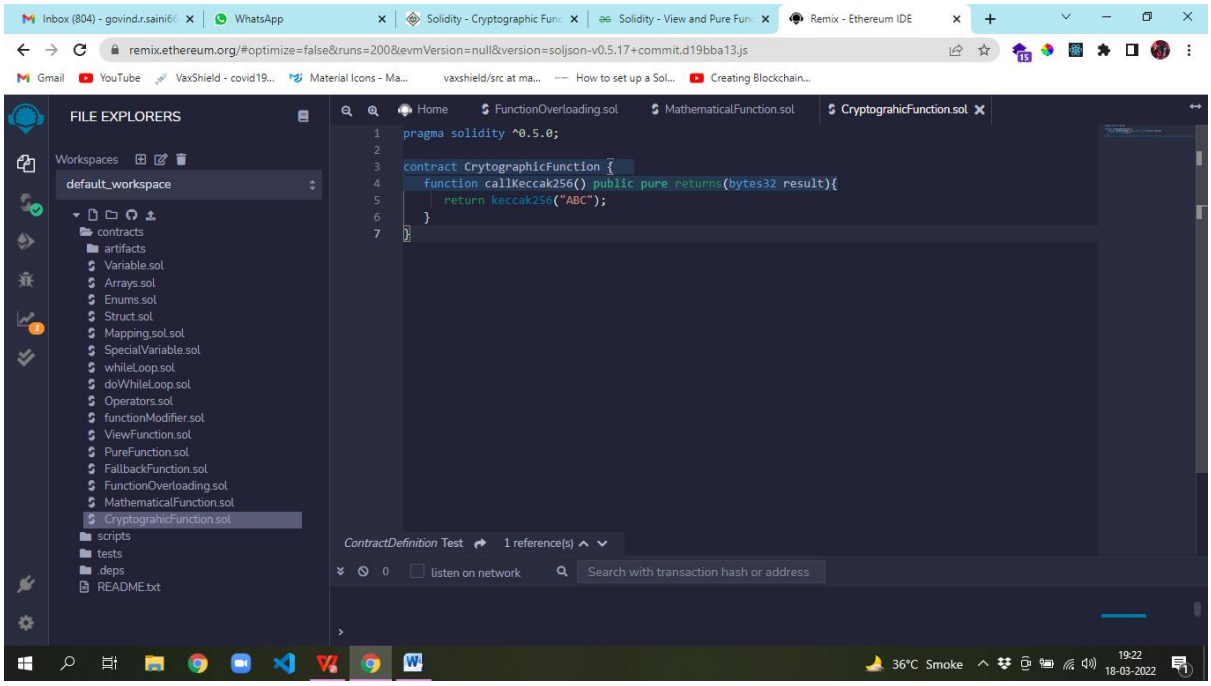


Output :

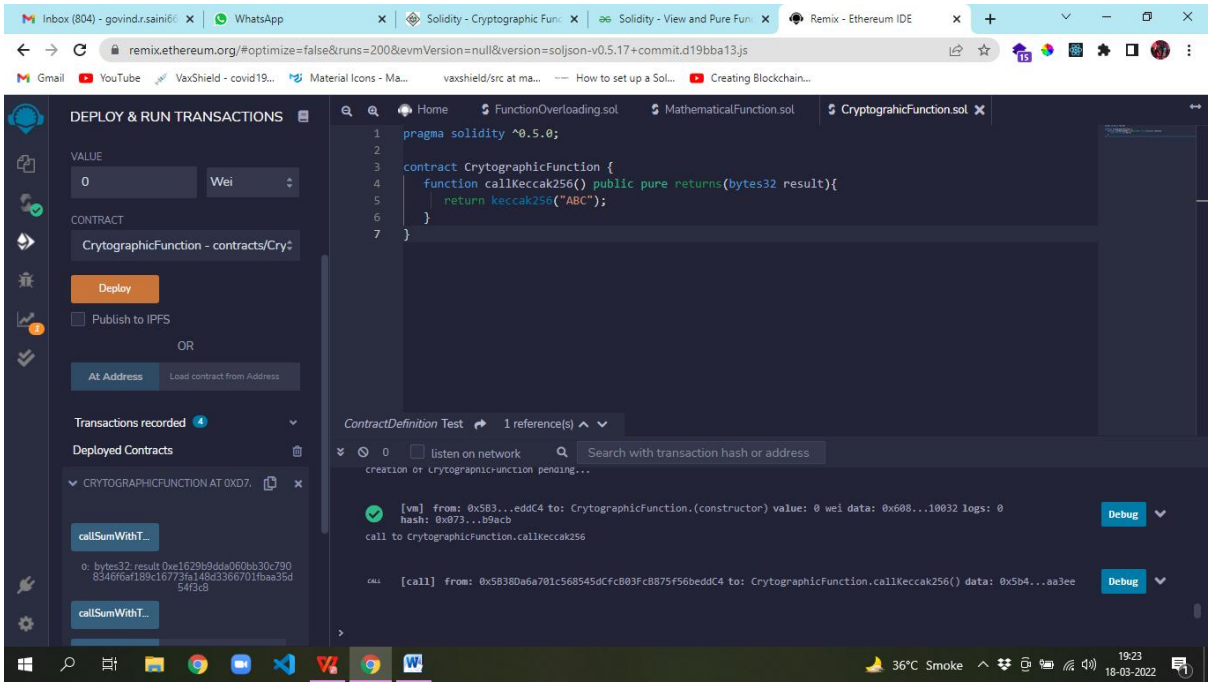


Cryptographic function

Code:


FILE EXPLORERS
Workspaces
default_workspace
contracts
artifacts
Variable.sol
Arrays.sol
Enums.sol
Struct.sol
Mapping.sol.sol
SpecialVariable.sol
whileLoop.sol
doWhileLoop.sol
Operators.sol
functionModifier.sol
ViewFunction.sol
PureFunction.sol
FallbackFunction.sol
FunctionOverloading.sol
MathematicalFunction.sol
CryptograhicFunction.sol
scripts
tests
.deps
README.txt
Home
FunctionOverloading.sol
MathematicalFunction.sol
CryptograhicFunction.sol
pragma solidity ^0.5.0;
contract CrytographicFunction {
function callKeccak256() public pure returns(bytes32 result){
return keccak256("ABC");
}
}
ContractDefinition Test
1 reference(s)
listen on network
Search with transaction hash or address

Output :


DEPLOY & RUN TRANSACTIONS
VALUE
0
Wei
CONTRACT
CrytographicFunction - contracts/Cry
Deploy
Publish to IPFS
OR
At Address
Load contract from Address
Transactions recorded
Deployed Contracts
CRYTOGRAPHICFUNCTION AT 0XD7...
callSumWithT...
callSumWithT...
Home
FunctionOverloading.sol
MathematicalFunction.sol
CryptograhicFunction.sol
pragma solidity ^0.5.0;
contract CrytographicFunction {
function callKeccak256() public pure returns(bytes32 result){
return keccak256("ABC");
}
}
ContractDefinition Test
1 reference(s)
listen on network
Search with transaction hash or address
creation of CrytographicFunction pending...
[vm] from: 0x5B3...eddC4 to: CrytographicFunction.(constructor) value: 0 wei data: 0x608...10032 logs: 0
hash: 0x073...b9acb
Debug
call to CrytographicFunction.callKeccak256
[call] from: 0x5B38Da6a701c568545dCFcB03FcB875f56beddC4 to: CrytographicFunction.callKeccak256() data: 0x5b4...aa3ee
Debug

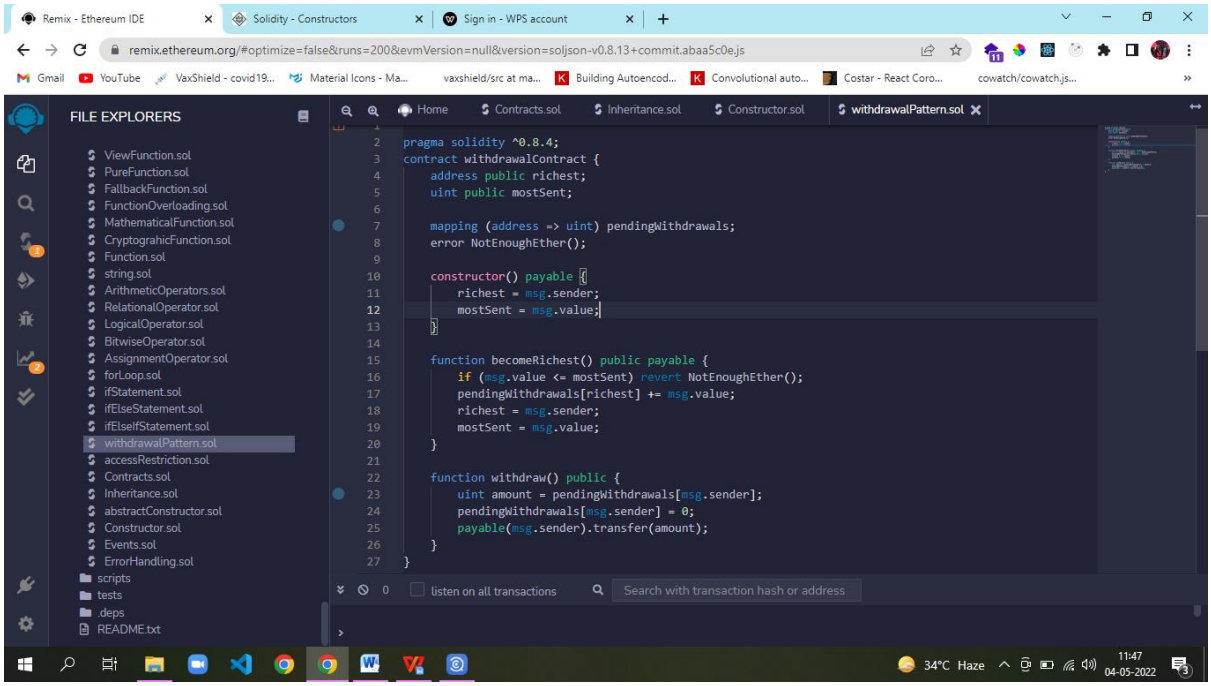
Practical No : 4

Aim : Implement and demonstrate the use of the following in Solidity :

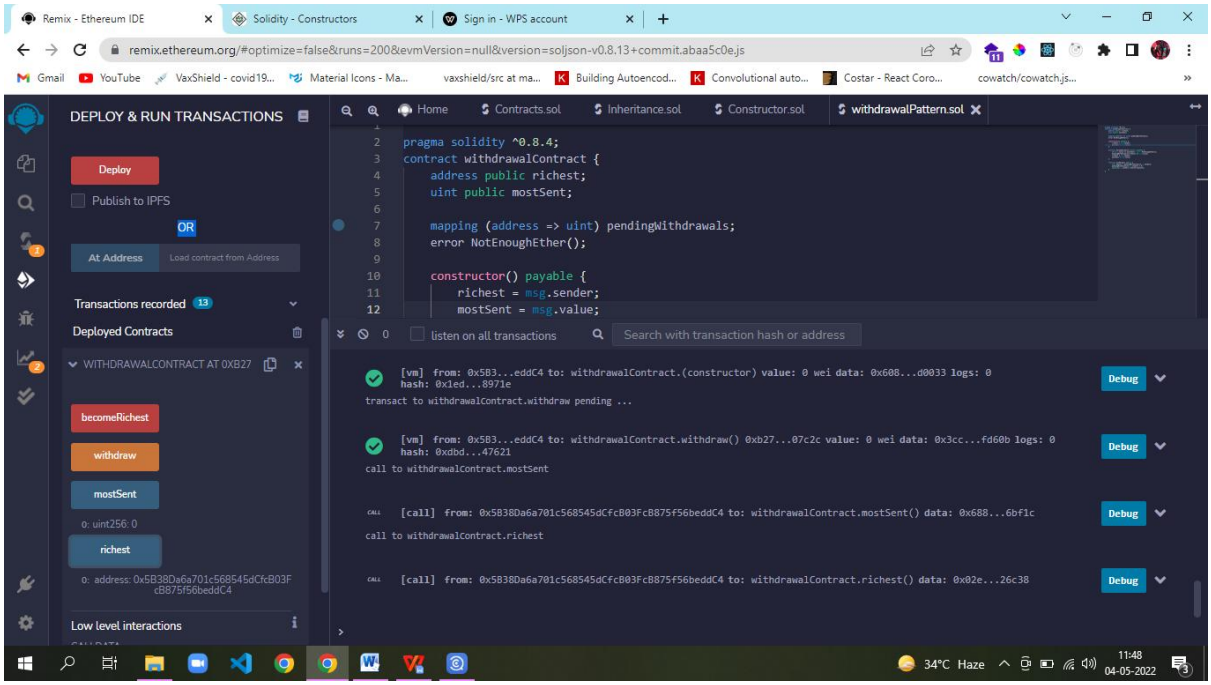
4a) Withdrawal Pattern, Restricted Access.

Withdrawal Pattern :

Code :

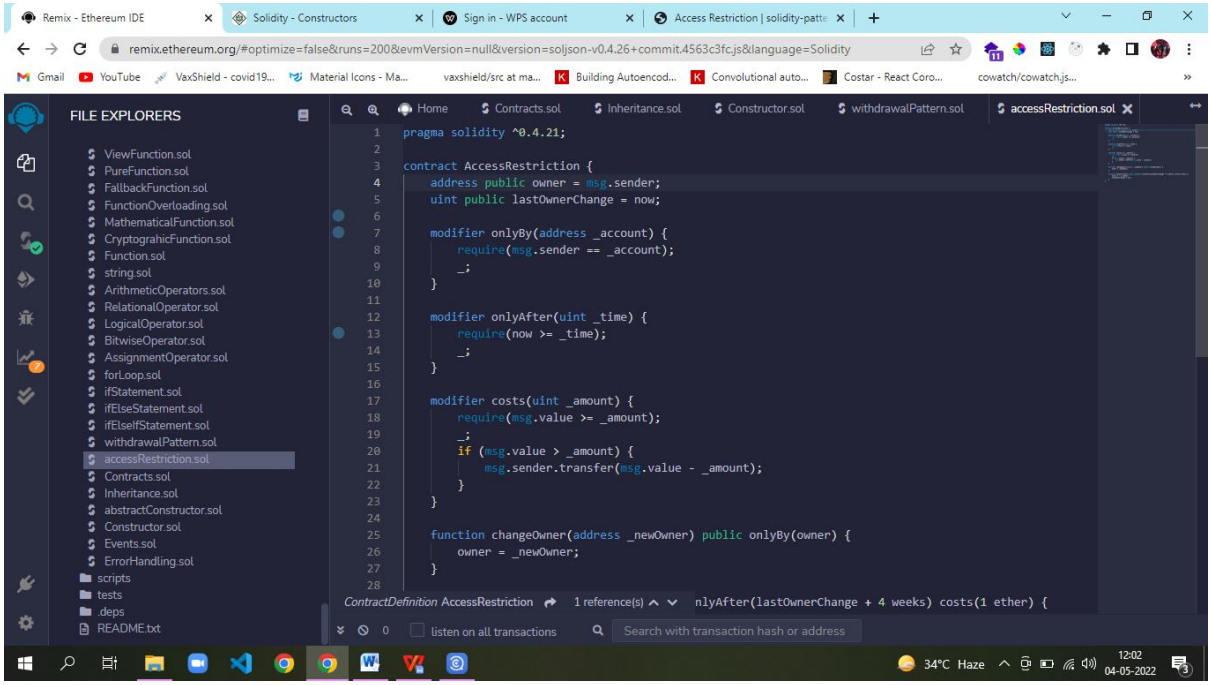


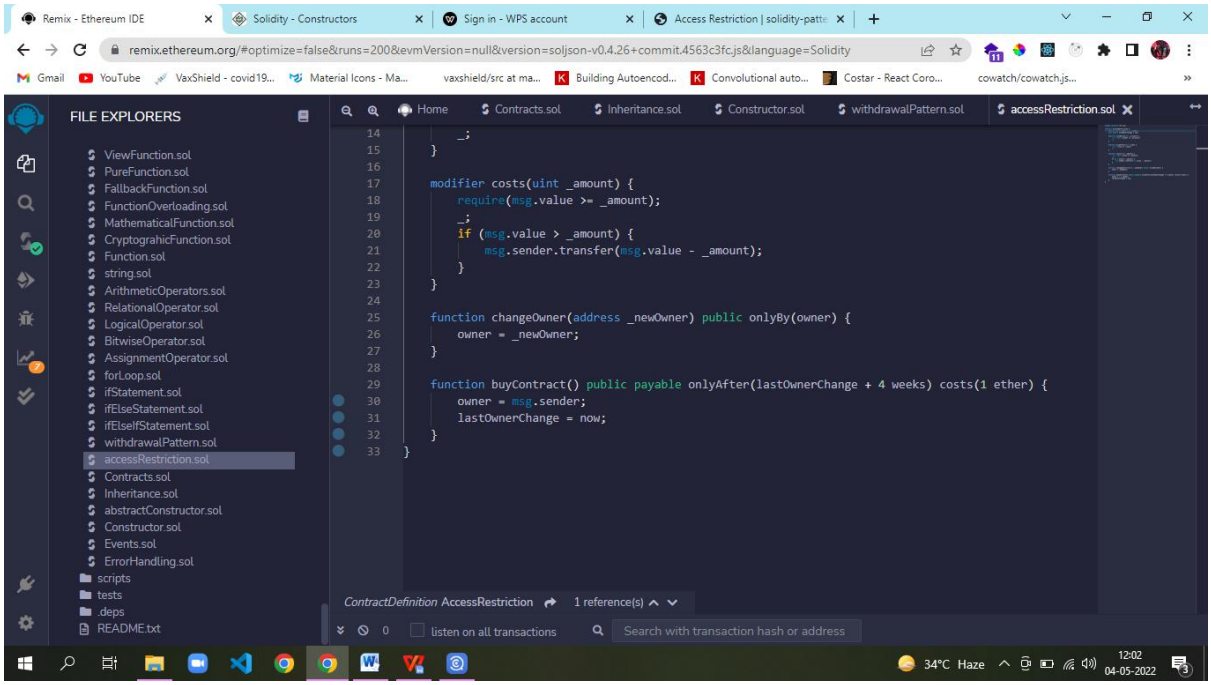
Ouput :



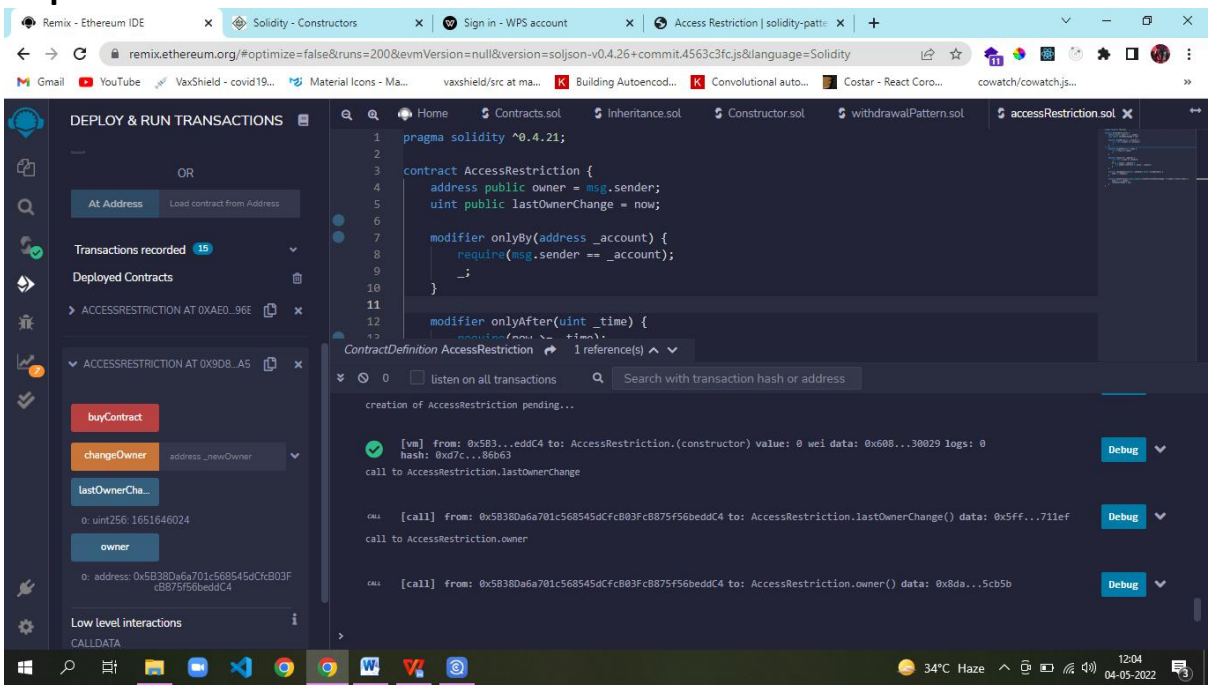
Restricted Access :

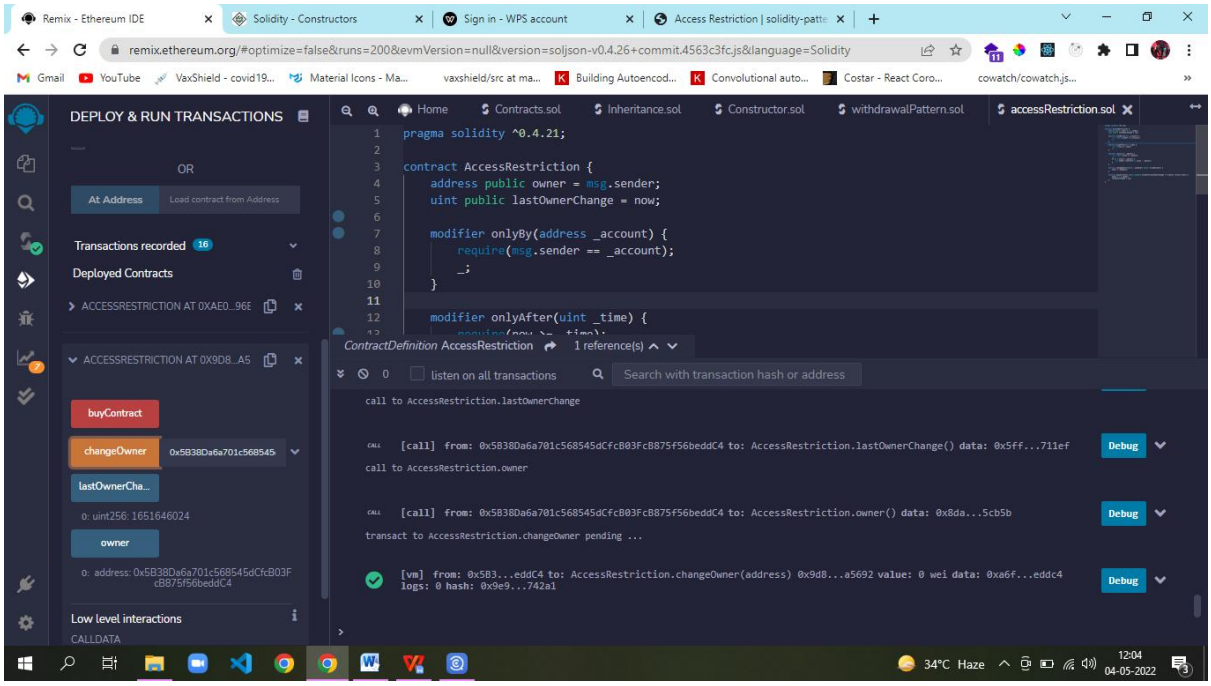
Code :




Remix - Ethereum IDE
Solidity - Constructors
Sign in - WPS account
Access Restriction | solidity-patte
remix.ethereum.org/#optimize=false&runs=200&evmVersion=null&version=soljson-v0.4.26+commit.4563c3fc.js&language=Solidity
FILE EXPLORERS
ViewFunction.sol
PureFunction.sol
FallbackFunction.sol
FunctionOverloading.sol
MathematicalFunction.sol
CryptograhicFunction.sol
Function.sol
string.sol
ArithmeticOperators.sol
RelationalOperator.sol
LogicalOperator.sol
BitwiseOperator.sol
AssignmentOperator.sol
forLoop.sol
ifStatement.sol
ifElseStatement.sol
ifElselfStatement.sol
withdrawalPattern.sol
accessRestriction.sol
Contracts.sol
Inheritance.sol
abstractConstructor.sol
Constructor.sol
Events.sol
ErrorHandling.sol
scripts
tests
.deps
README.txt
Home
Contracts.sol
Inheritance.sol
Constructor.sol
withdrawalPattern.sol
accessRestriction.sol
_;
}
modifier costs(uint _amount) {
require(msg.value >= _amount);
_;
if (msg.value > _amount) {
msg.sender.transfer(msg.value - _amount);
}
}
function changeOwner(address _newOwner) public onlyBy(owner) {
owner = _newOwner;
}
function buyContract() public payable onlyAfter(lastOwnerChange + 4 weeks) costs(1 ether) {
owner = msg.sender;
lastOwnerChange = now;
}
}
ContractDefinition AccessRestriction
1 reference(s)
listen on all transactions
Search with transaction hash or address
34°C Haze
12:02
04-05-2022

Ouput :

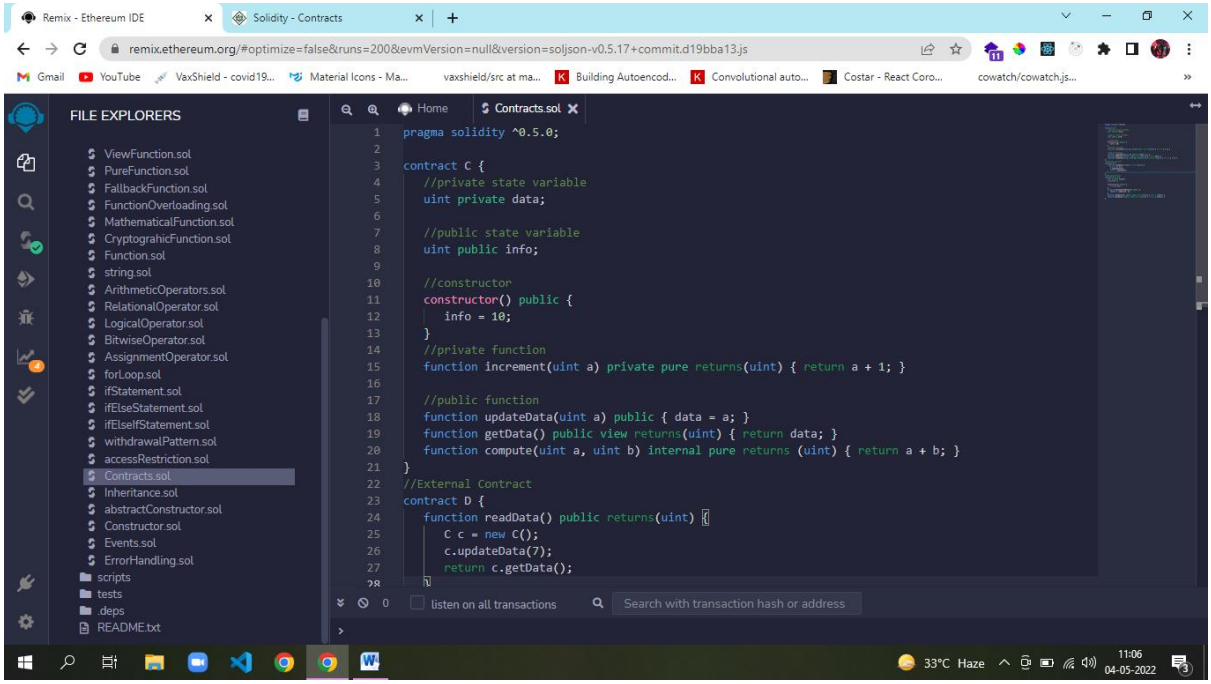

Remix - Ethereum IDE
Solidity - Constructors
Sign in - WPS account
Access Restriction | solidity-patte
remix.ethereum.org/#optimize=false&runs=200&evmVersion=null&version=soljson-v0.4.26+commit.4563c3fc.js&language=Solidity
DEPLOY & RUN TRANSACTIONS
OR
At Address
Load contract from Address
Transactions recorded 15
Deployed Contracts
ACCESSRESTRICTION AT 0XAE0...96E
ACCESSRESTRICTION AT 0X9D8...A5
buyContract
changeOwner
address _newOwner
lastOwnerCha...
0: uint256: 1651646024
owner
0: address: 0x5B38Da6a701c568545dCfcB03FcB875f56beddC4
Low level interactions
CALLDATA
Home
Contracts.sol
Inheritance.sol
Constructor.sol
withdrawalPattern.sol
accessRestriction.sol
pragma solidity ^0.4.21;
contract AccessRestriction {
address public owner = msg.sender;
uint public lastOwnerChange = now;
modifier onlyBy(address _account) {
require(msg.sender == _account);
_;
}
modifier onlyAfter(uint _time) {
ContractDefinition AccessRestriction
1 reference(s)
listen on all transactions
Search with transaction hash or address
creation of AccessRestriction pending...
[vm] from: 0x5B3...eddC4 to: AccessRestriction.(constructor) value: 0 wei data: 0x608...30029 logs: 0
hash: 0xd7c...86b63
Debug
call to AccessRestriction.lastOwnerChange
[call] from: 0x5B38Da6a701c568545dCfcB03FcB875f56beddC4 to: AccessRestriction.lastOwnerChange() data: 0x5ff...711ef
Debug
call to AccessRestriction.owner
[call] from: 0x5B38Da6a701c568545dCfcB03FcB875f56beddC4 to: AccessRestriction.owner() data: 0x8da...5cb5b
Debug
34°C Haze
12:04
04-05-2022

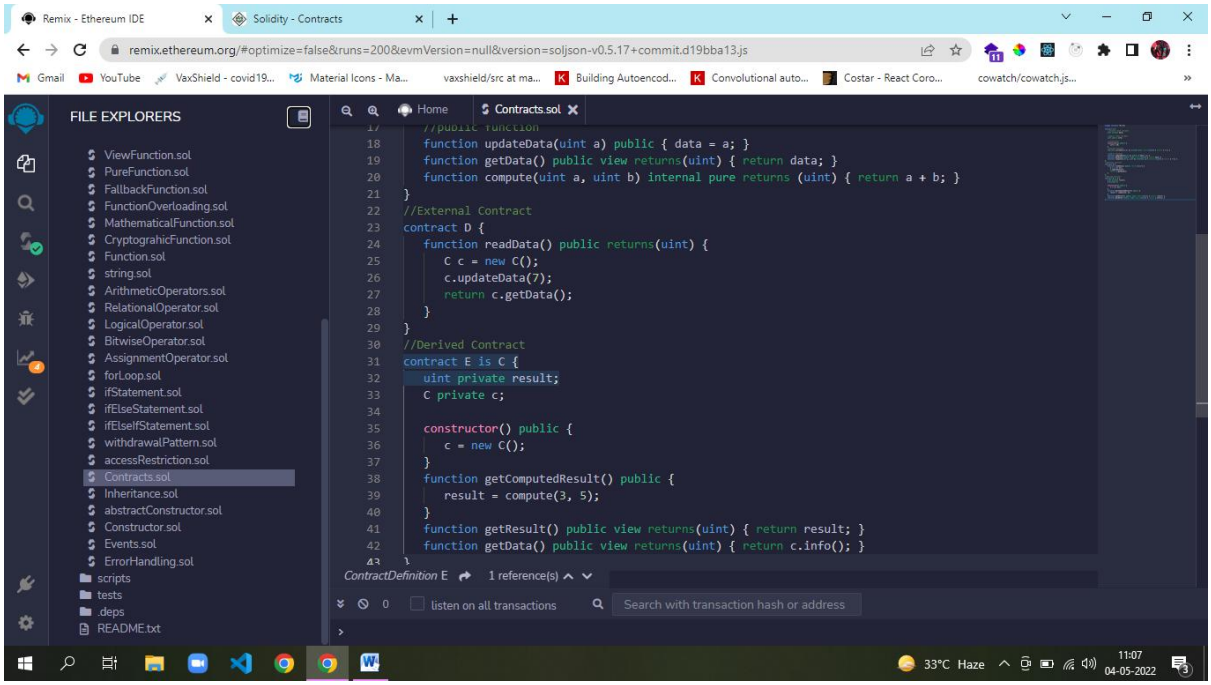


4b) Contracts, Inheritance, Constructors, Abstract Contracts, Interfaces.

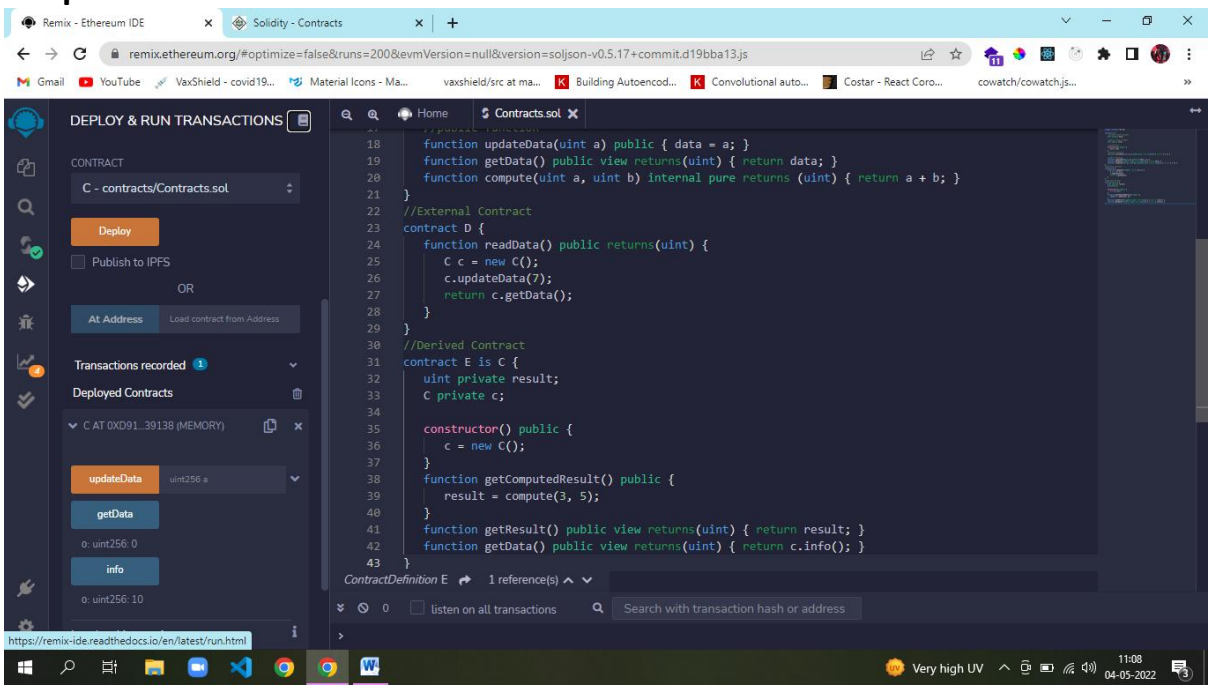
Contracts:

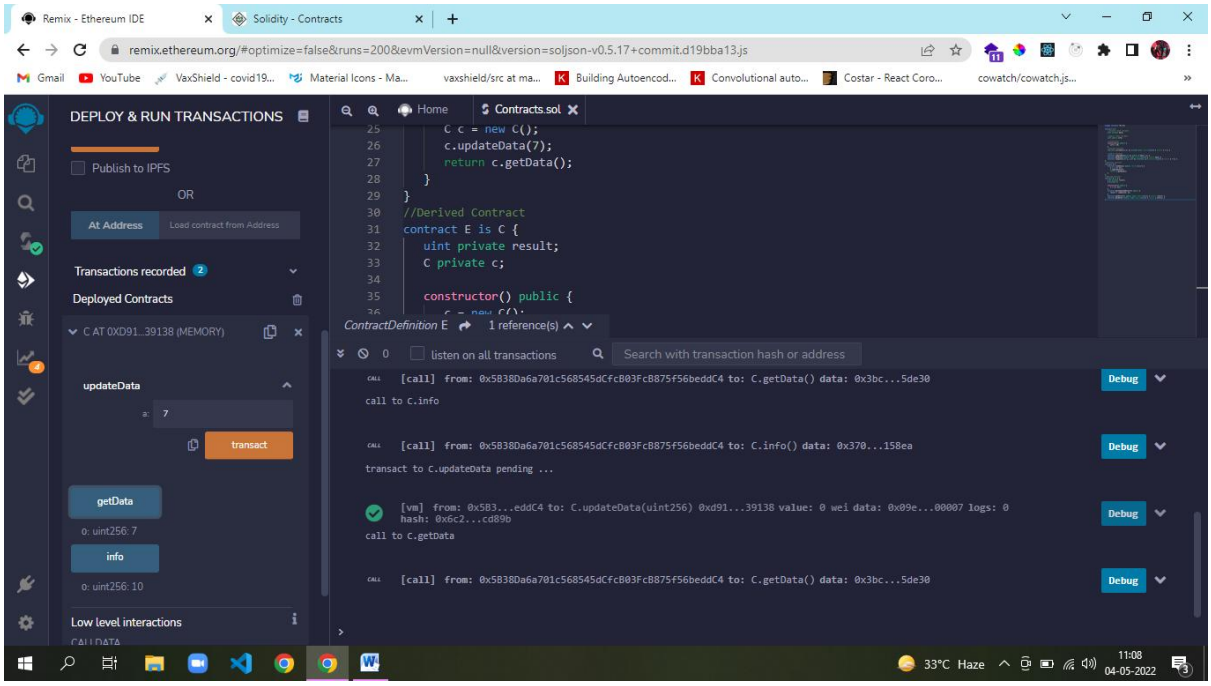
Code :




Remix - Ethereum IDE
Solidity - Contracts
remix.ethereum.org/#optimize=false&runs=200&evmVersion=null&version=soljson-v0.5.17+commit.d19bba13.js
FILE EXPLORERS
ViewFunction.sol
PureFunction.sol
FallbackFunction.sol
FunctionOverloading.sol
MathematicalFunction.sol
CryptograhicFunction.sol
Function.sol
string.sol
ArithmeticOperators.sol
RelationalOperator.sol
LogicalOperator.sol
BitwiseOperator.sol
AssignmentOperator.sol
forLoop.sol
ifStatement.sol
ifElseStatement.sol
ifElseIfStatement.sol
withdrawalPattern.sol
accessRestriction.sol
Contracts.sol
Inheritance.sol
abstractConstructor.sol
Constructor.sol
Events.sol
ErrorHandling.sol
scripts
tests
.deps
README.txt
Home
Contracts.sol
function updateData(uint a) public { data = a; }
function getData() public view returns(uint) { return data; }
function compute(uint a, uint b) internal pure returns (uint) { return a + b; }
}
//External Contract
contract D {
function readData() public returns(uint) {
C c = new C();
c.updateData(7);
return c.getData();
}
}
//Derived Contract
contract E is C {
uint private result;
C private c;
constructor() public {
c = new C();
}
function getComputedResult() public {
result = compute(3, 5);
}
function getResult() public view returns(uint) { return result; }
function getData() public view returns(uint) { return c.info(); }
}
ContractDefinition E
1 reference(s)
listen on all transactions
Search with transaction hash or address
33°C Haze
11:07
04-05-2022

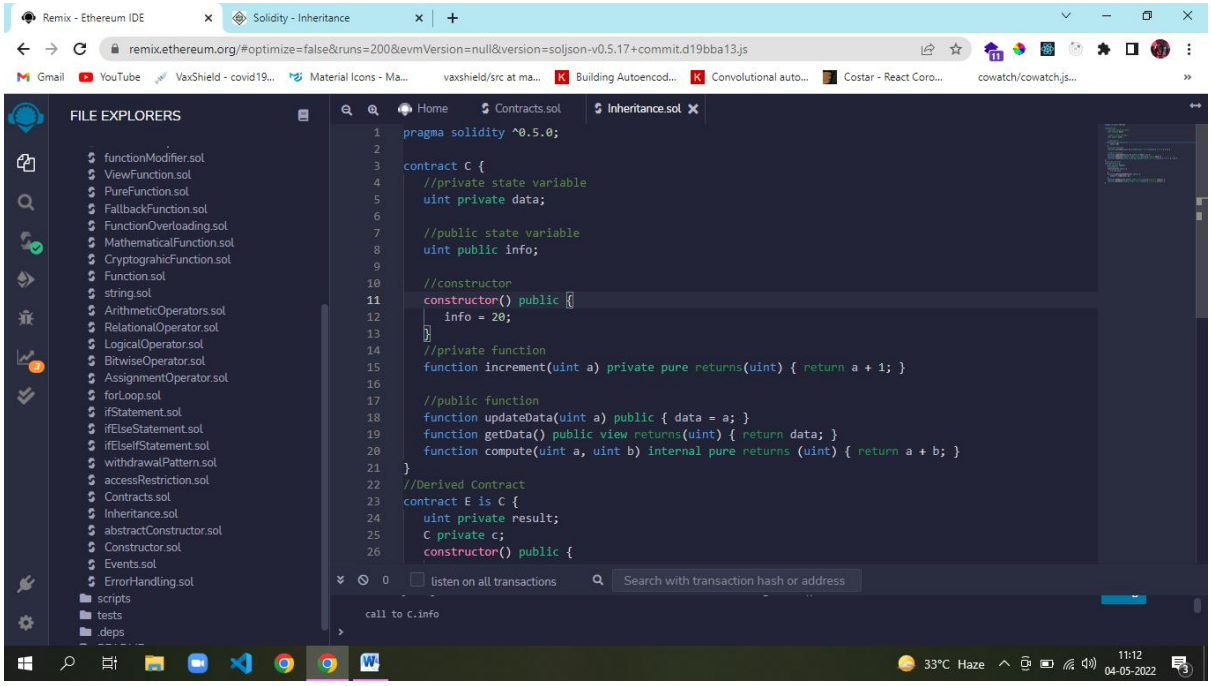
Output :

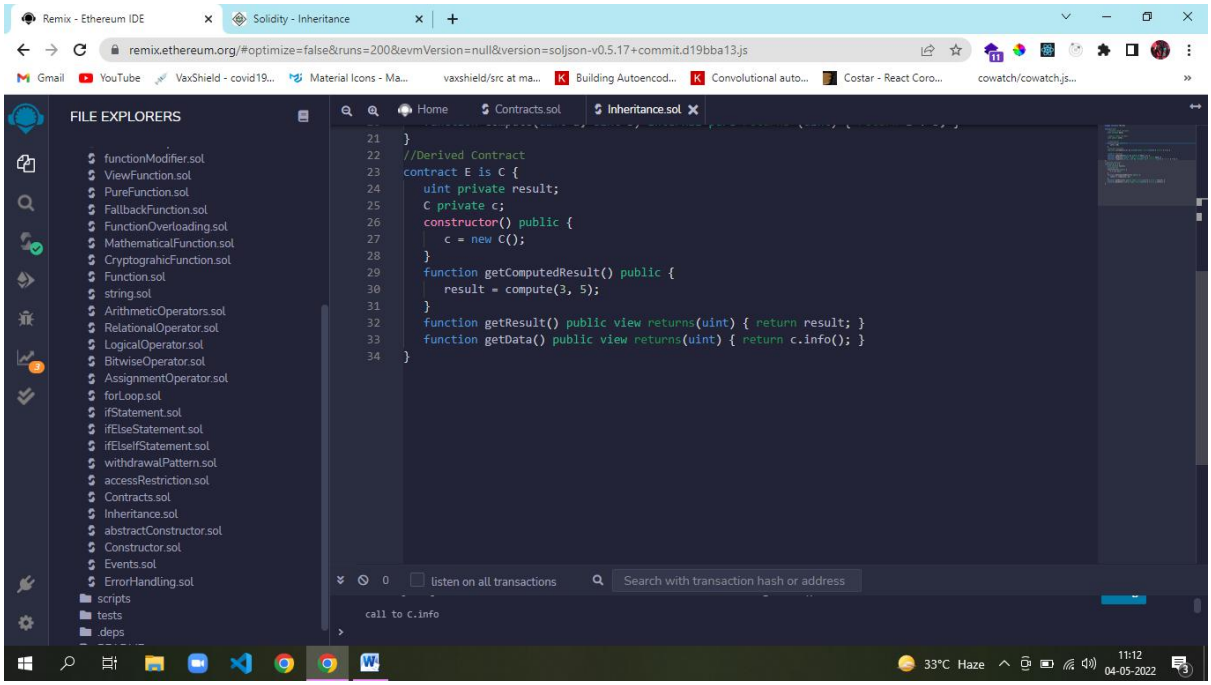

Remix - Ethereum IDE
Solidity - Contracts
remix.ethereum.org/#optimize=false&runs=200&evmVersion=null&version=soljson-v0.5.17+commit.d19bba13.js
DEPLOY & RUN TRANSACTIONS
CONTRACT
C - contracts/Contracts.sol
Deploy
Publish to IPFS
OR
At Address
Load contract from Address
Transactions recorded 1
Deployed Contracts
C AT 0XD91...39138 (MEMORY)
updateData
uint256 a
getData
0: uint256: 0
info
0: uint256: 10
https://remix-ide.readthedocs.io/en/latest/run.html
Home
Contracts.sol
function updateData(uint a) public { data = a; }
function getData() public view returns(uint) { return data; }
function compute(uint a, uint b) internal pure returns (uint) { return a + b; }
}
//External Contract
contract D {
function readData() public returns(uint) {
C c = new C();
c.updateData(7);
return c.getData();
}
}
//Derived Contract
contract E is C {
uint private result;
C private c;
constructor() public {
c = new C();
}
function getComputedResult() public {
result = compute(3, 5);
}
function getResult() public view returns(uint) { return result; }
function getData() public view returns(uint) { return c.info(); }
}
ContractDefinition E
1 reference(s)
listen on all transactions
Search with transaction hash or address
Very high UV
11:08
04-05-2022



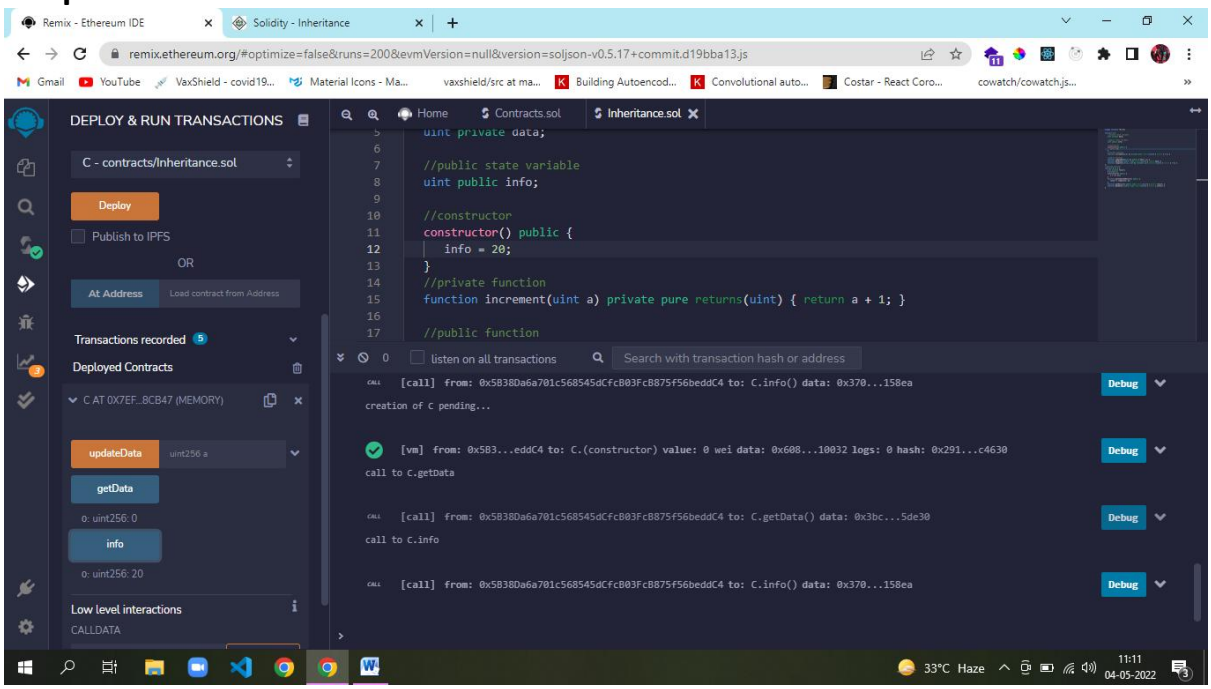
Inheritance

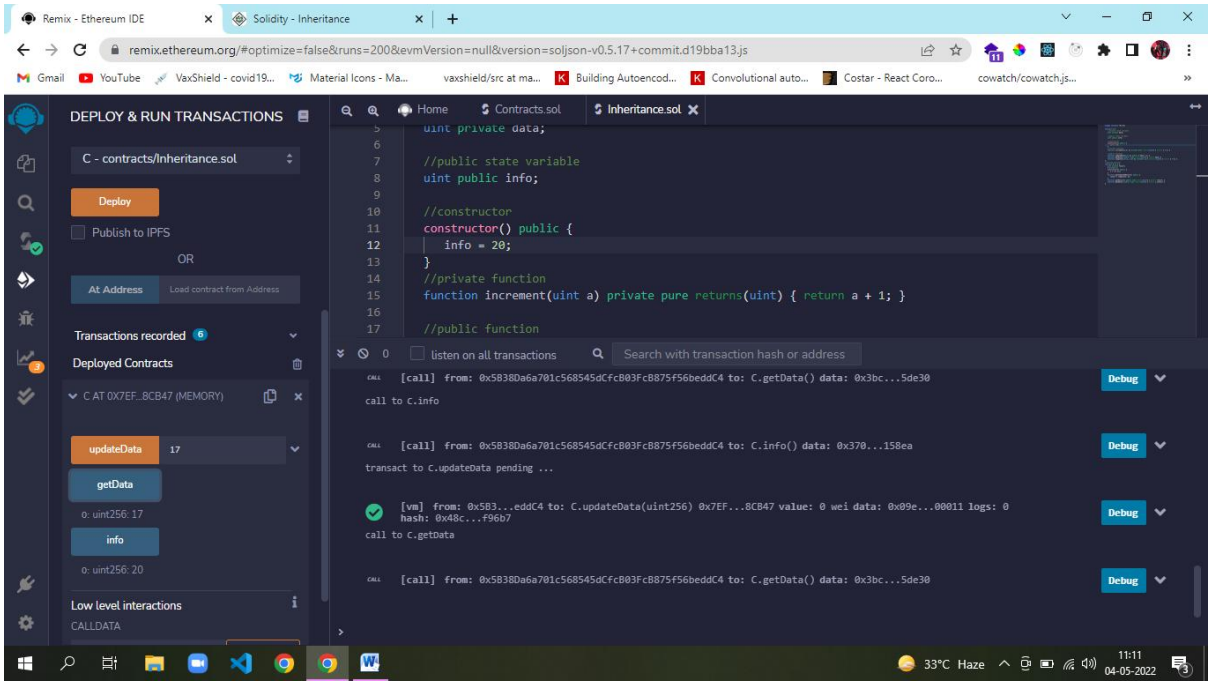
Code :




Remix - Ethereum IDE
Solidity - Inheritance
remix.ethereum.org/#optimize=false&runs=200&evmVersion=null&version=soljson-v0.5.17+commit.d19bba13.js
FILE EXPLORERS
functionModifier.sol
ViewFunction.sol
PureFunction.sol
FallbackFunction.sol
FunctionOverloading.sol
MathematicalFunction.sol
CryptograhicFunction.sol
Function.sol
string.sol
ArithmeticOperators.sol
RelationalOperator.sol
LogicalOperator.sol
BitwiseOperator.sol
AssignmentOperator.sol
forLoop.sol
ifStatement.sol
ifElseStatement.sol
ifElseIfStatement.sol
withdrawalPattern.sol
accessRestriction.sol
Contracts.sol
Inheritance.sol
abstractConstructor.sol
Constructor.sol
Events.sol
ErrorHandling.sol
scripts
tests
.deps
Home
Contracts.sol
Inheritance.sol
21 }
22 //Derived Contract
23 contract E is C {
24 uint private result;
25 C private c;
26 constructor() public {
27 c = new C();
28 }
29 function getComputedResult() public {
30 result = compute(3, 5);
31 }
32 function getResult() public view returns(uint) { return result; }
33 function getData() public view returns(uint) { return c.info(); }
34 }
listen on all transactions
Search with transaction hash or address
call to C.info
33°C Haze
11:12
04-05-2022

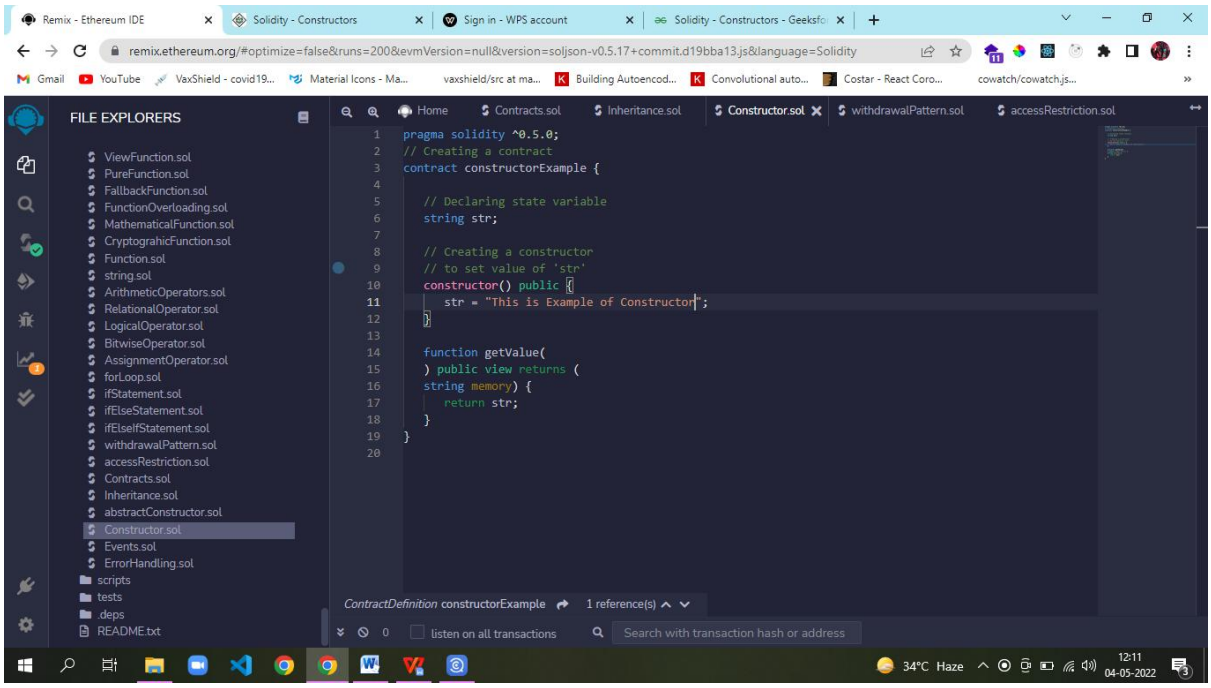
Output :


Remix - Ethereum IDE
Solidity - Inheritance
remix.ethereum.org/#optimize=false&runs=200&evmVersion=null&version=soljson-v0.5.17+commit.d19bba13.js
DEPLOY & RUN TRANSACTIONS
C - contracts/Inheritance.sol
Deploy
Publish to IPFS
OR
At Address
Load contract from Address
Transactions recorded 5
Deployed Contracts
C AT 0X7EF...8CB47 (MEMORY)
updateData
uint256 a
getData
0: uint256: 0
info
0: uint256: 20
Low level interactions
CALLDATA
Home
Contracts.sol
Inheritance.sol
uint private data;
//public state variable
uint public info;
//constructor
constructor() public {
info = 20;
}
//private function
function increment(uint a) private pure returns(uint) { return a + 1; }
//public function
listen on all transactions
Search with transaction hash or address
[call] from: 0x5B38Da6a701c568545dCfcB03FcB875f56beddC4 to: C.info() data: 0x370...158ea
creation of C pending...
[vm] from: 0x583...eddC4 to: C.(constructor) value: 0 wei data: 0x608...10032 logs: 0 hash: 0x291...c4630
call to C.getData
[call] from: 0x5B38Da6a701c568545dCfcB03FcB875f56beddC4 to: C.getData() data: 0x3bc...5de30
call to C.info
[call] from: 0x5B38Da6a701c568545dCfcB03FcB875f56beddC4 to: C.info() data: 0x370...158ea
Debug
33°C Haze
11:11
04-05-2022

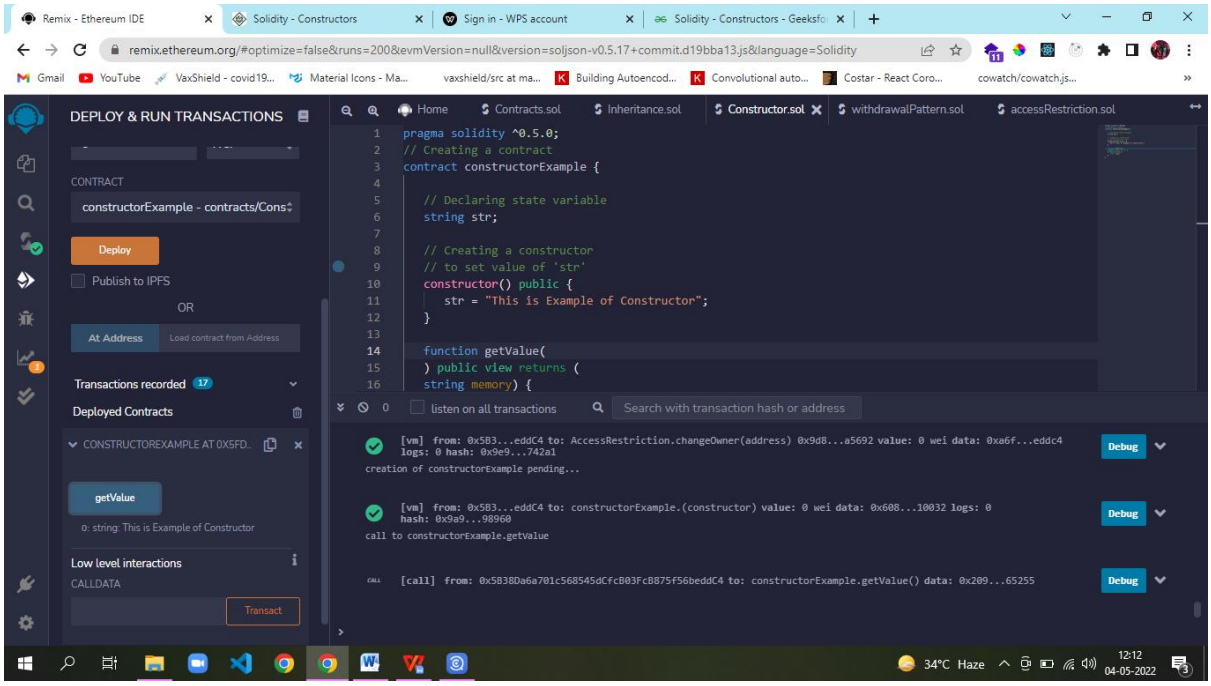


Constructors :

Code :

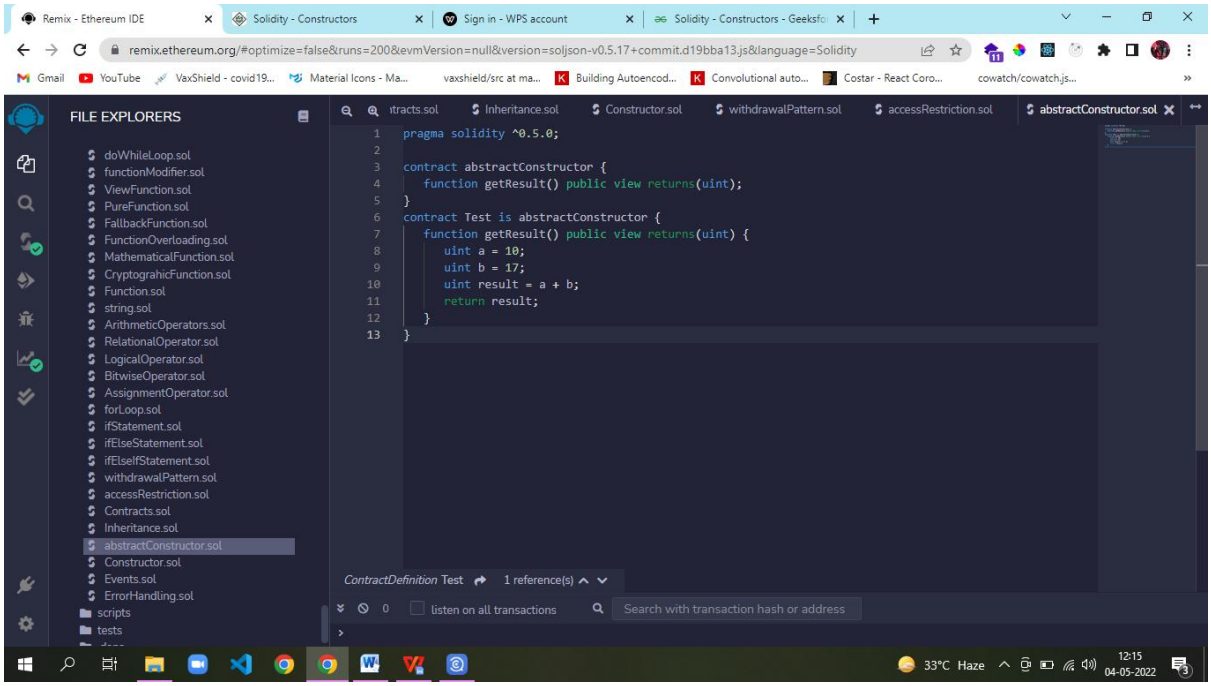


Output :

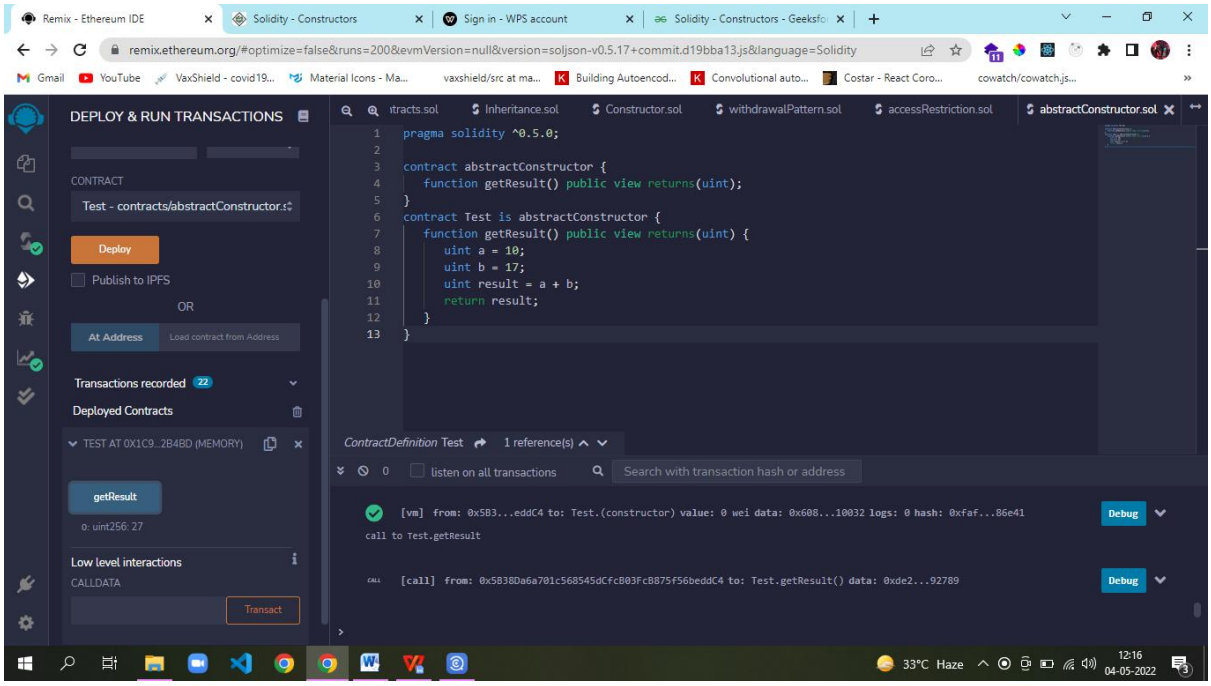


Abstract Contracts :

Code :

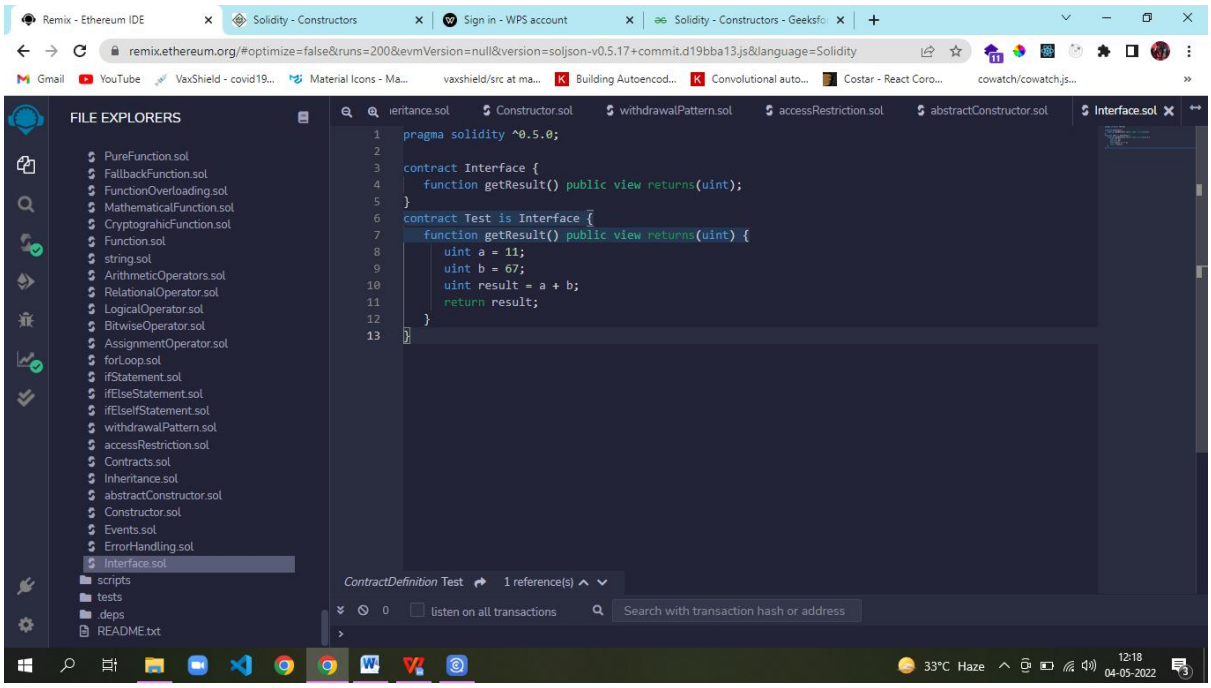


Output :

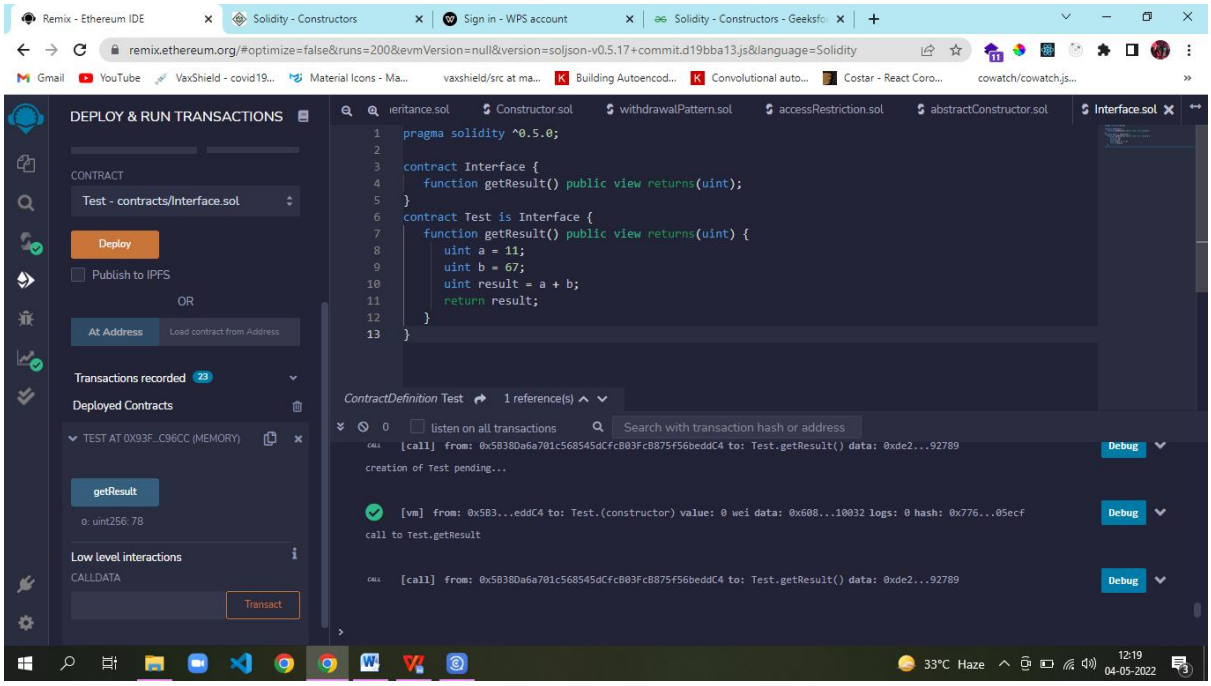


Interfaces :

Code :



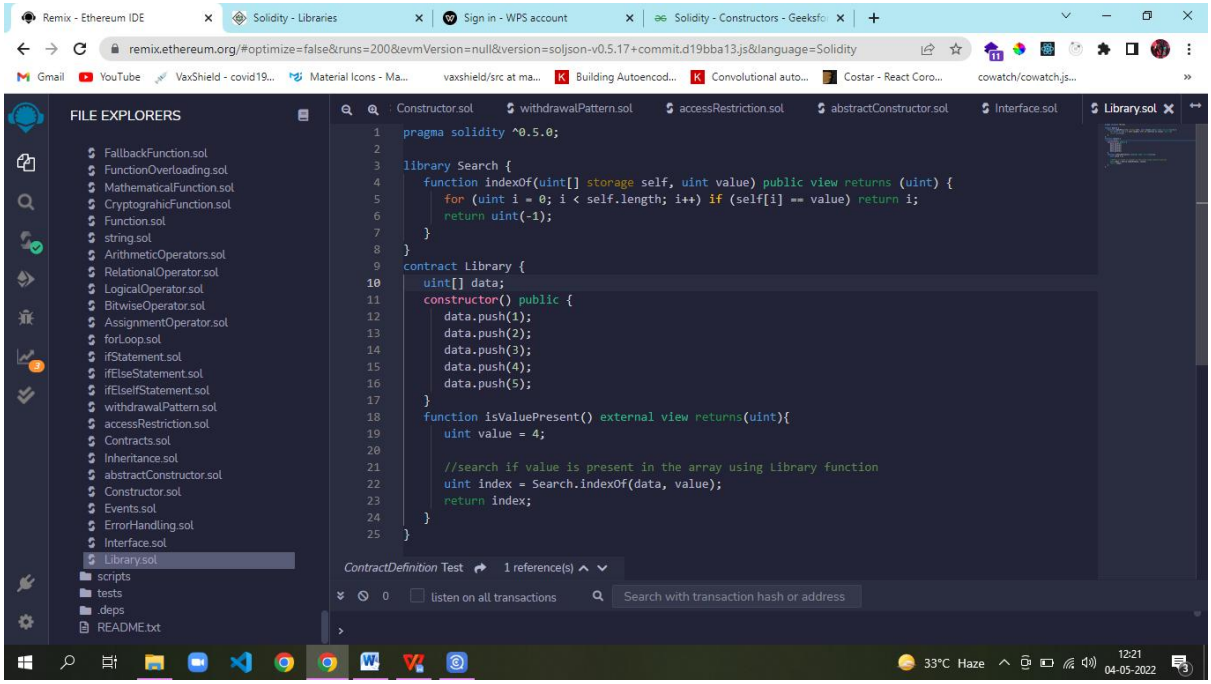
Output :



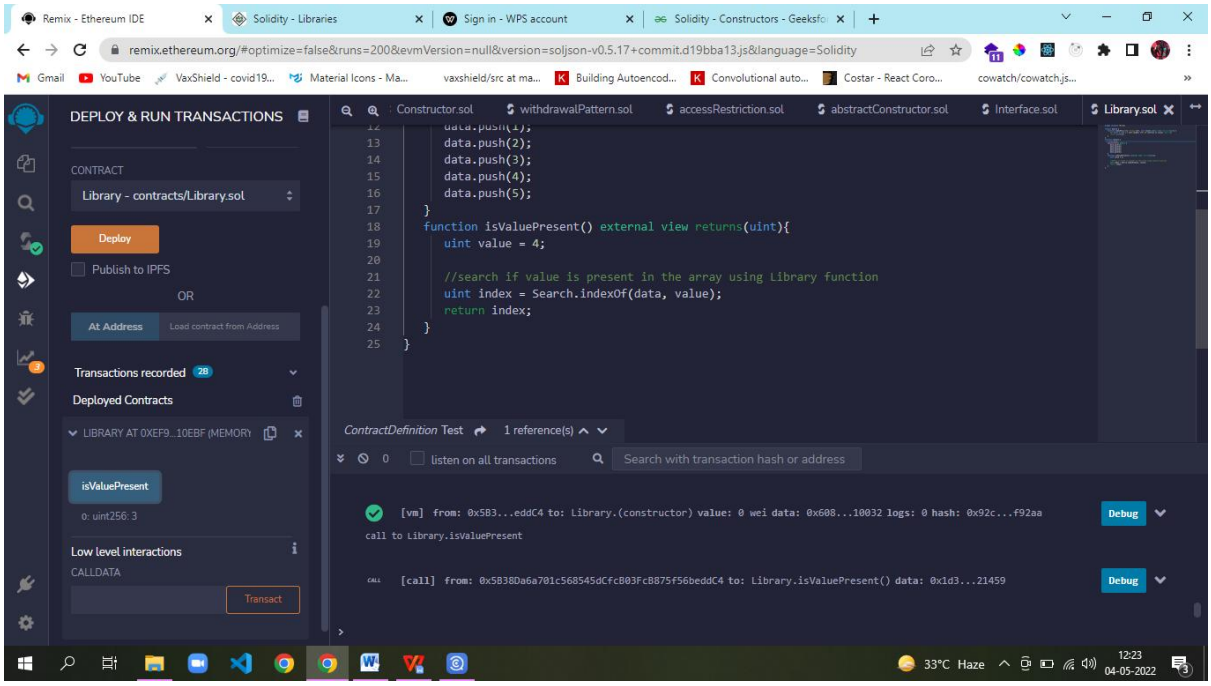
4c) Libraries, Assembly, Events, Error handling.

Libraries :

Code :

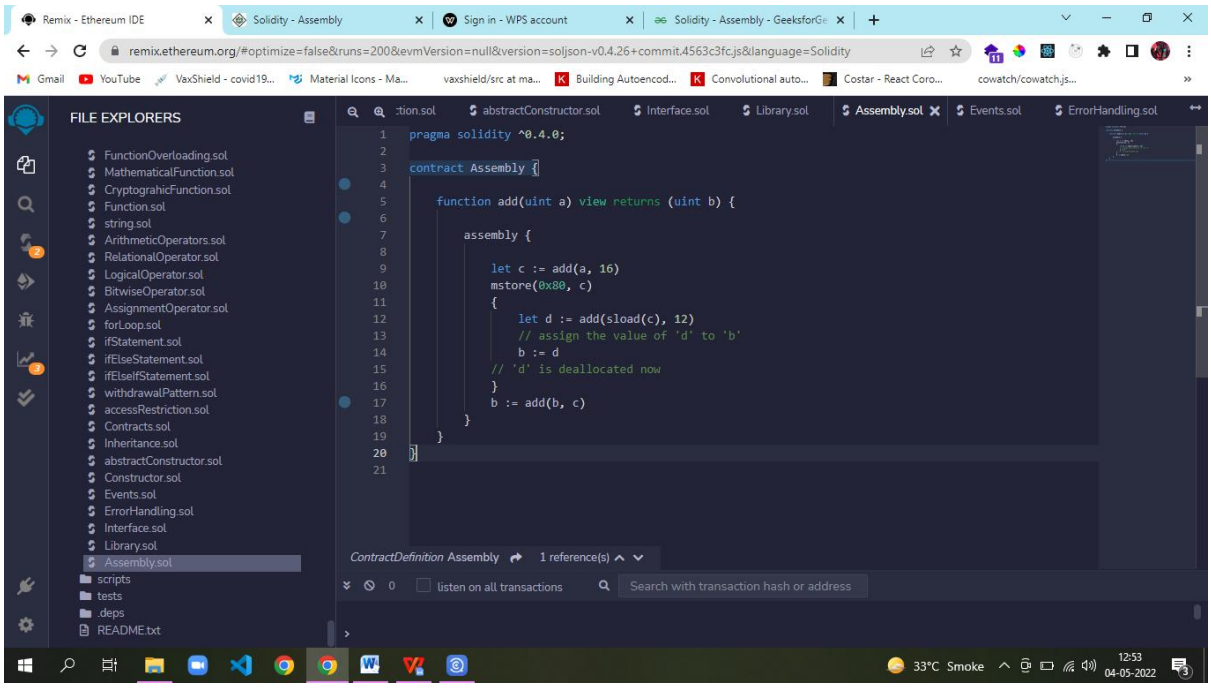


Output :

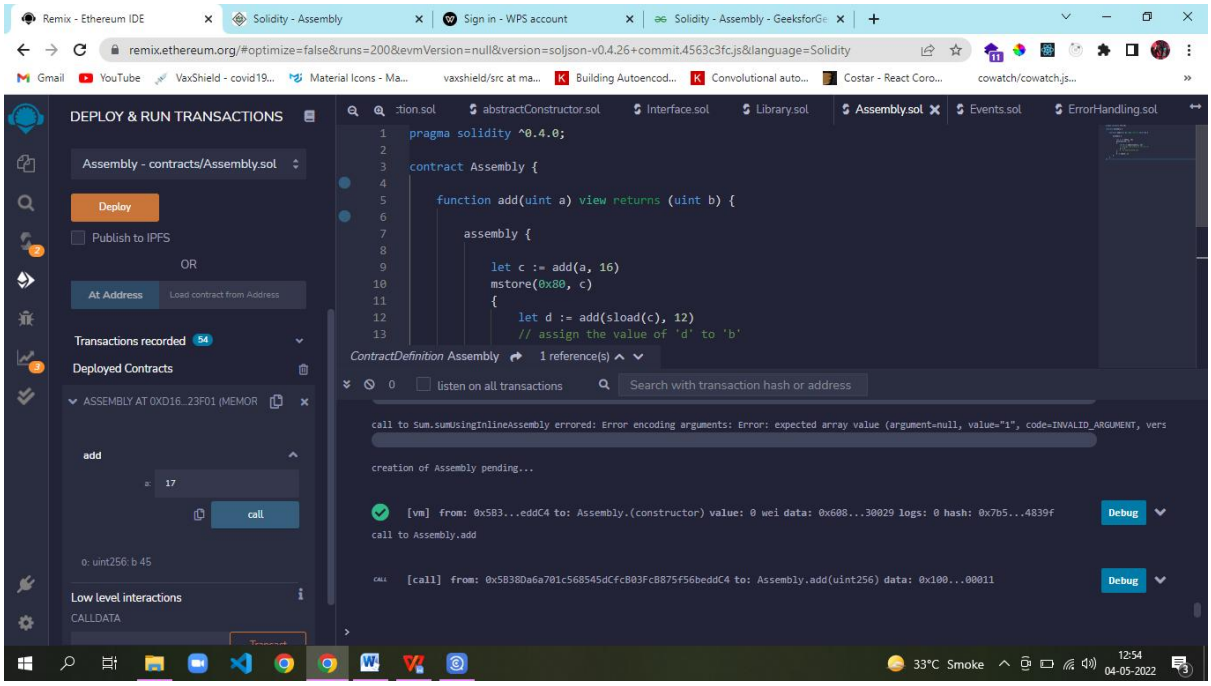


Assembly :

Code :

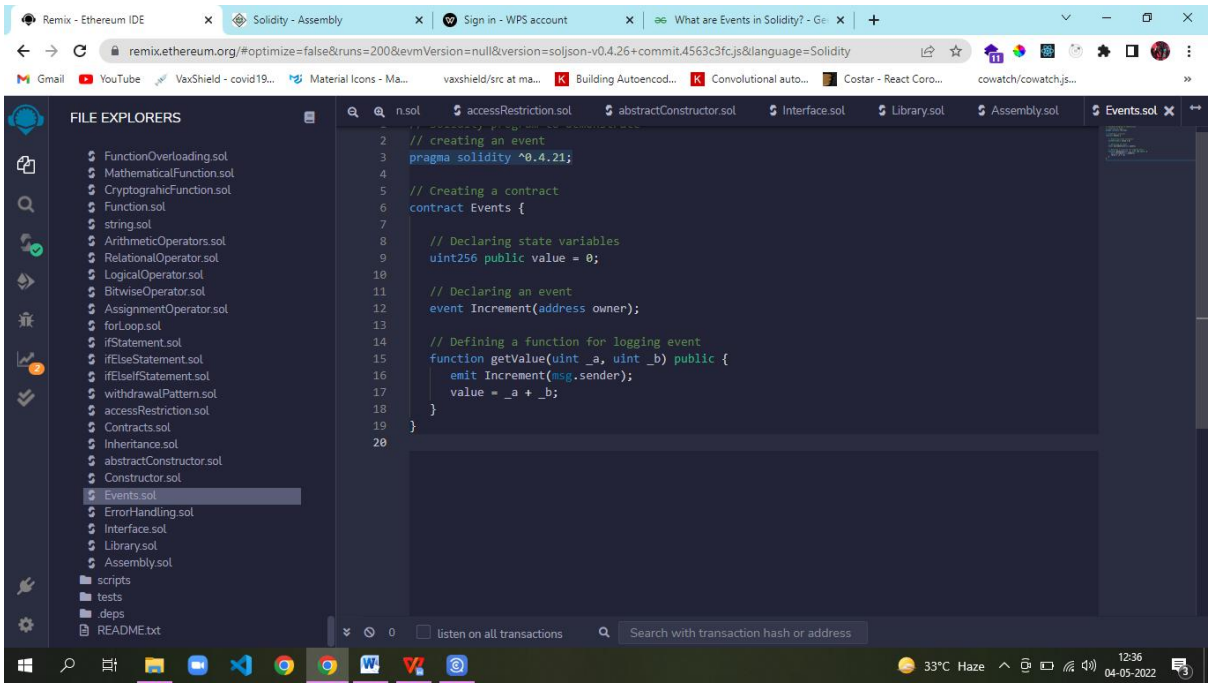


Output :

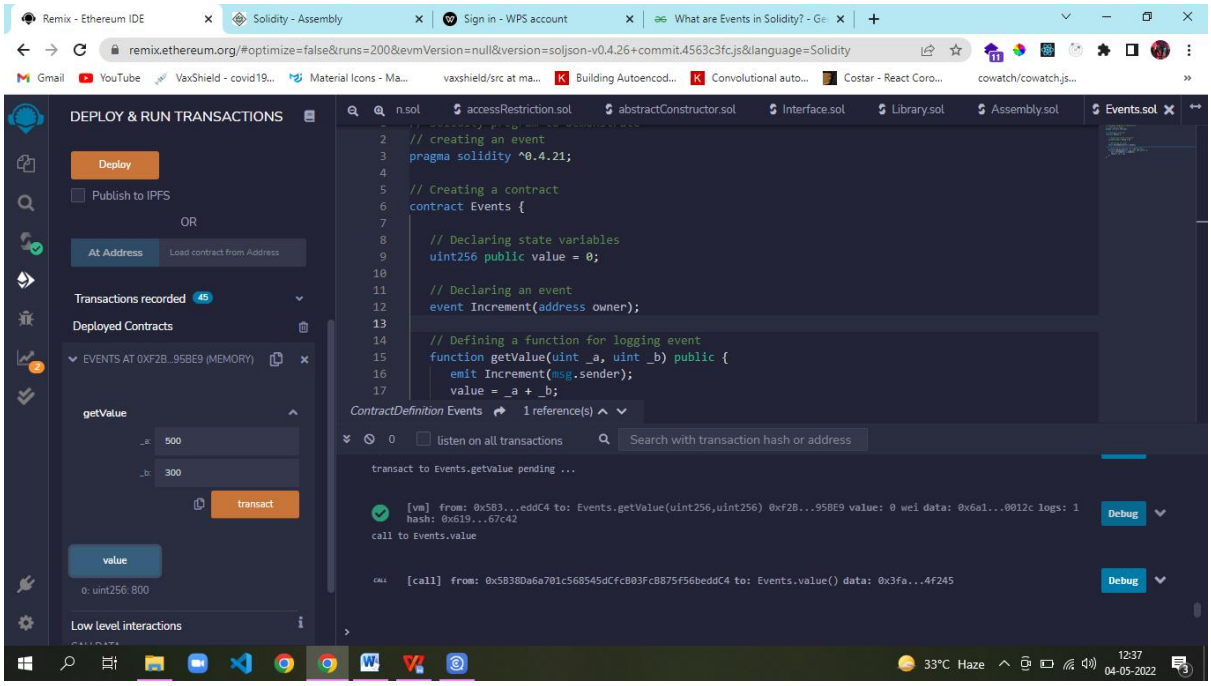


Events:

Code :

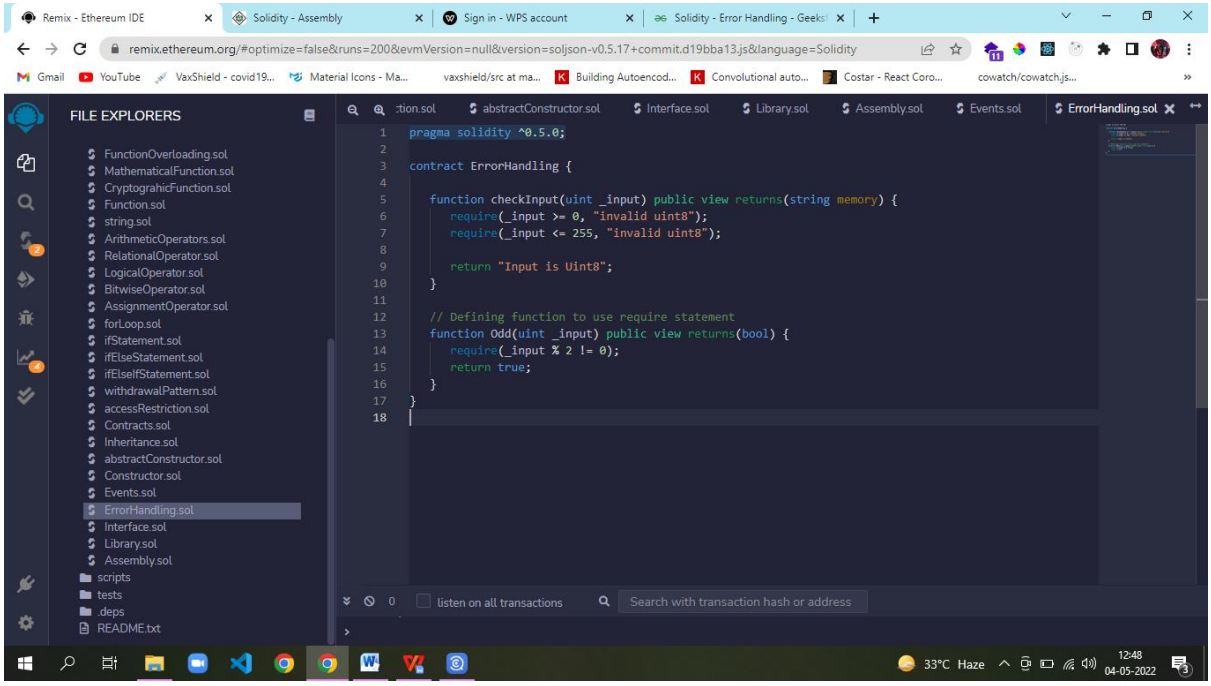


Outut :

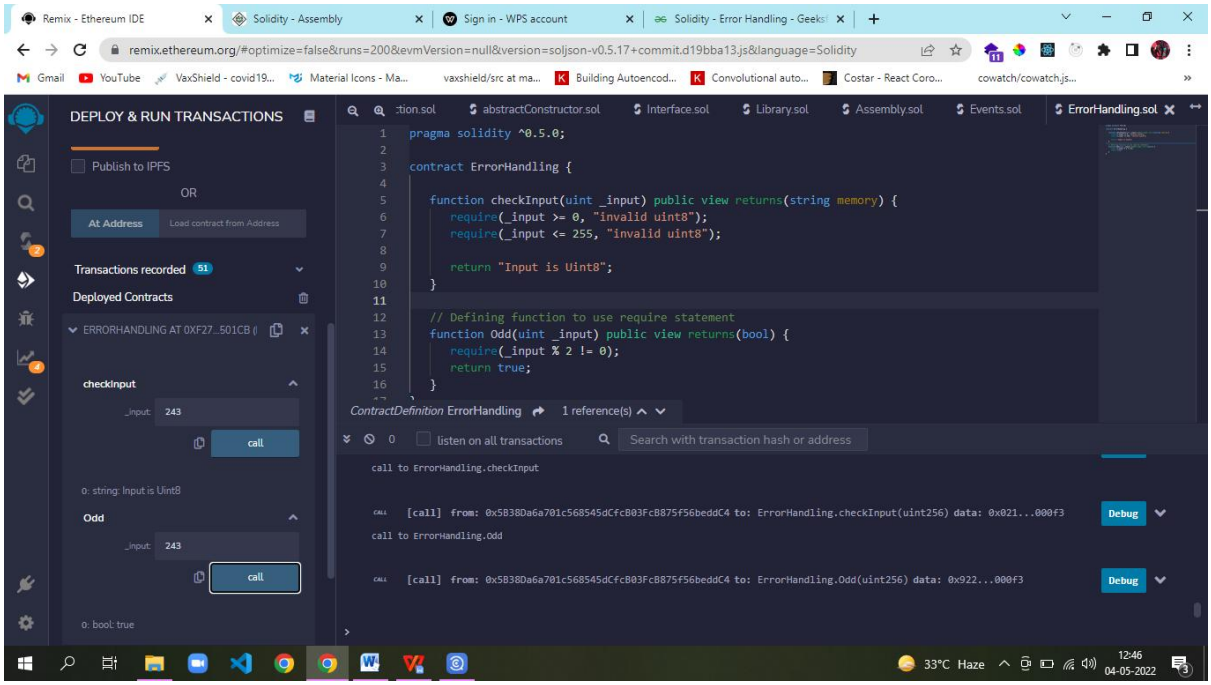


Error handling :

Code :



Output :


Remix - Ethereum IDE
Solidity - Assembly
Sign in - WPS account
Solidity - Error Handling - Geeks
remix.ethereum.org/#optimize=false&runs=200&evmVersion=null&version=soljson-v0.5.17+commit.d19bba13.js&language=Solidity
DEPLOY & RUN TRANSACTIONS
Publish to IPFS
OR
At Address
Load contract from Address
Transactions recorded 51
Deployed Contracts
checkInput
_input: 243
call
0: string: Input is Uint8
Odd
_input: 243
call
0: bool: true
abstractConstructor.sol
Interface.sol
Library.sol
Assembly.sol
Events.sol
ErrorHandling.sol
pragma solidity ^0.5.0;
contract ErrorHandling {
function checkInput(uint _input) public view returns(string memory) {
require(_input >= 0, "invalid uint8");
require(_input <= 255, "invalid uint8");
return "Input is Uint8";
}
// Defining function to use require statement
function Odd(uint _input) public view returns(bool) {
require(_input % 2 != 0);
return true;
}
ContractDefinition ErrorHandling
1 reference(s)
listen on all transactions
Search with transaction hash or address
call to ErrorHandling.checkInput
[call] from: 0x5B38Da6a701c568545dCfcB03FcB875f56beddC4 to: ErrorHandling.checkInput(uint256) data: 0x021...000f3
Debug
call to ErrorHandling.Odd
[call] from: 0x5B38Da6a701c568545dCfcB03FcB875f56beddC4 to: ErrorHandling.Odd(uint256) data: 0x922...000f3
Debug
33°C Haze
12:46
04-05-2022