Visvesvaraya Technological University
Belagavi, Karnataka-590 018

TASK-2 REPORT

ON

BLOCKCHAIN TECHNOLOGY
20CC621

By

Meghana Bhat P	4nm20ai025
Shubhambari K Shetty	4nm20cm040

NITTE EDUCATION TRUST | N.M.A.M. INSTITUTE OF TECHNOLOGY
(An Autonomous Institution affiliated to Visvesvaraya Technological University, Belagavi)
Nitte – 574 110, Karnataka, India

Department of Computer and Communication Engineering/Artificial Intelligence and Machine Learning

2022-2023

Library

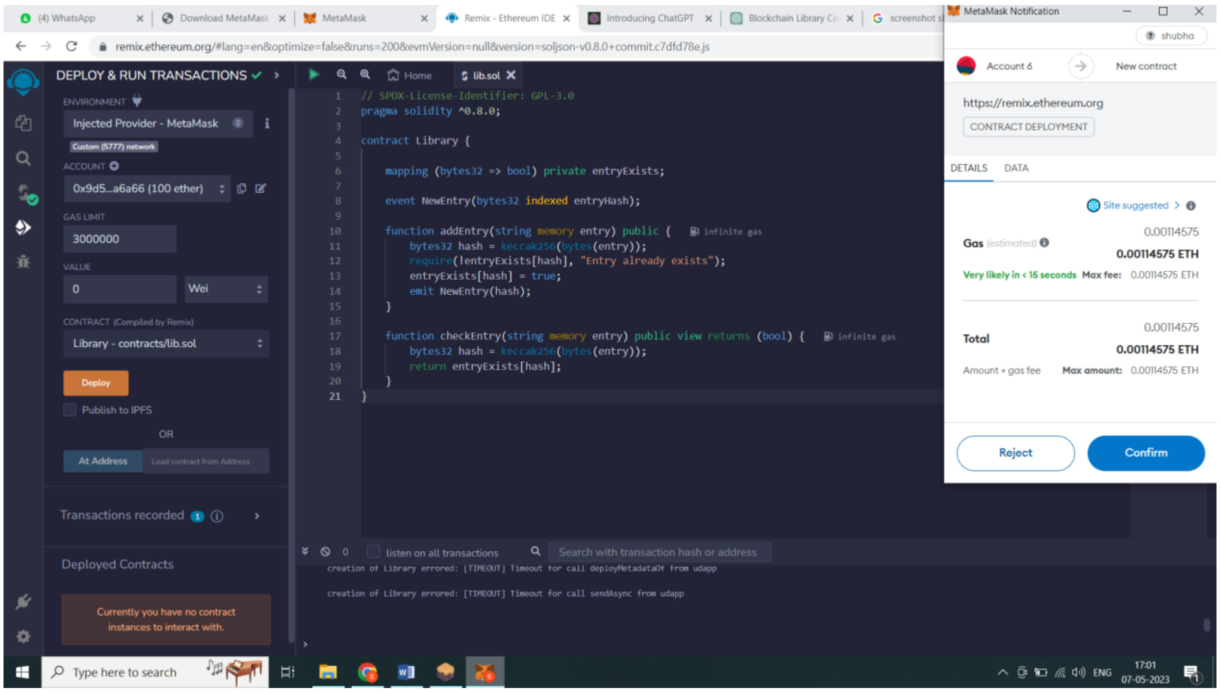
This is a simple smart contract written in Solidity, a programming language used for creating smart contracts on the Ethereum blockchain.The contract is named "Library" and has two functions: "addEntry" and "checkEntry". The "addEntry" function takes a string argument "entry" and adds it to the contract's mapping data structure called "entryExists”. The "checkEntry" function takes a string argument "entry" and returns a Boolean value indicating whether the entry exists in the mapping or not. The contract also includes a SPDX-License-Identifier statement at the top to indicate the license under which the contract code is released. In this case, it is released under the GPL-3.0 license.

Smart Contract Code:

```
// SPDX-License-Identifier: GPL-3.0

pragma solidity ^0.8.0;

contract Library {

    mapping (bytes32 => bool) private entryExists;

    event NewEntry(bytes32 indexed entryHash);

    function addEntry(string memory entry) public {

        bytes32 hash = keccak256(bytes(entry));

        require(!entryExists[hash], "Entry already exists");

        entryExists[hash] = true;

        emit NewEntry(hash);

    }

    function checkEntry(string memory entry) public view returns (bool) {

        bytes32 hash = keccak256(bytes(entry));

        return entryExists[hash];

    }

}
```

Snapshots of Output:

While deploying:



remix.ethereum.org/#lang=en&optimize=false&runs=200&evmVersion=null&version=soljson-v0.8.0+commit.c7dfd78e.js

DEPLOY & RUN TRANSACTIONS

ENVIRONMENT: Injected Provider - MetaMask (Custom (5777) network)

ACCOUNT: 0x9d5...a6a66 (100 ether)

GAS LIMIT: 3000000

VALUE: 0 Wei

CONTRACT (Compiled by Remix): Library - contracts/lib.sol

Currently you have no contract instances to interact with.

```solidity
// SPDX-License-Identifier: GPL-3.0
pragma solidity ^0.8.0;

contract Library {

    mapping (bytes32 => bool) private entryExists;

    event NewEntry(bytes32 indexed entryHash);

    function addEntry(string memory entry) public {
        bytes32 hash = keccak256(bytes(entry));
        require(!entryExists[hash], "Entry already exists");
        entryExists[hash] = true;
        emit NewEntry(hash);
    }

    function checkEntry(string memory entry) public view returns (bool) {
        bytes32 hash = keccak256(bytes(entry));
        return entryExists[hash];
    }
}
```

```
creation of Library errored: [TIMEOUT] Timeout for call deployMetadataOf from udapp

creation of Library errored: [TIMEOUT] Timeout for call sendAsync from udapp
```

MetaMask Notification

Account 6 → New contract

https://remix.ethereum.org

CONTRACT DEPLOYMENT

Gas (estimated): 0.00114575 — 0.00114575 ETH

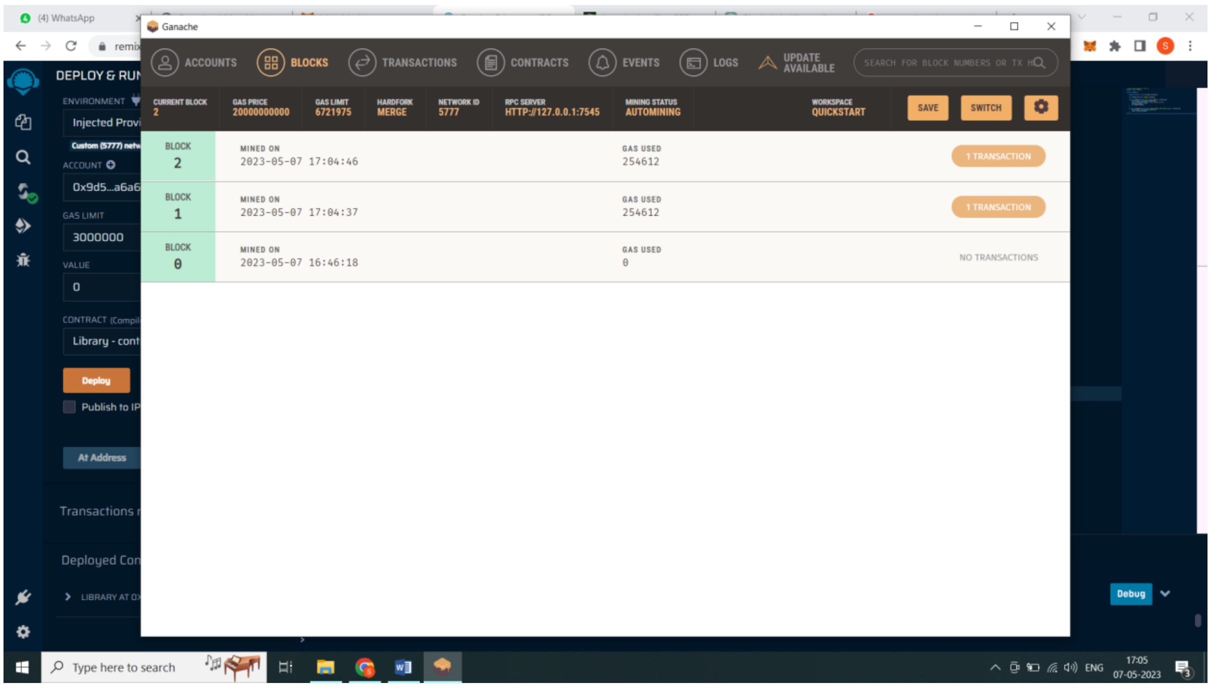
Very likely in < 15 seconds Max fee: 0.00114575 ETH

Total: 0.00114575 — 0.00114575 ETH

Amount + gas fee Max amount: 0.00114575 ETH

Reject Confirm

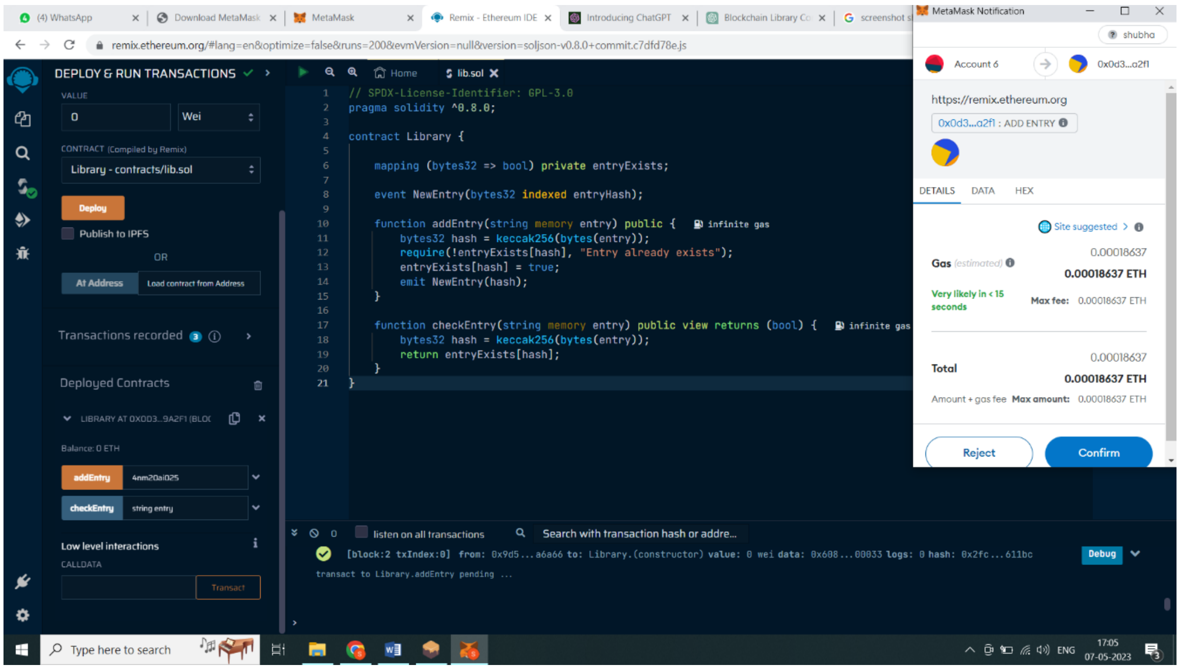
Gas used for deploying:



Ganache

```
CURRENT BLOCK  GAS PRICE    GAS LIMIT  HARDFORK  NETWORK ID  RPC SERVER             MINING STATUS  WORKSPACE
2              20000000000  6721975    MERGE     5777        HTTP://127.0.0.1:7545  AUTOMINING     QUICKSTART

BLOCK 2   MINED ON 2023-05-07 17:04:46   GAS USED 254612   1 TRANSACTION
BLOCK 1   MINED ON 2023-05-07 17:04:37   GAS USED 254612   1 TRANSACTION
BLOCK 0   MINED ON 2023-05-07 16:46:18   GAS USED 0        NO TRANSACTIONS
```

Add Entry:



```
// SPDX-License-Identifier: GPL-3.0
pragma solidity ^0.8.0;

contract Library {

    mapping (bytes32 => bool) private entryExists;

    event NewEntry(bytes32 indexed entryHash);

    function addEntry(string memory entry) public {
        bytes32 hash = keccak256(bytes(entry));
        require(!entryExists[hash], "Entry already exists");
        entryExists[hash] = true;
        emit NewEntry(hash);
    }

    function checkEntry(string memory entry) public view returns (bool) {
        bytes32 hash = keccak256(bytes(entry));
        return entryExists[hash];
    }
}
```

```
[block:2 txIndex:0] from: 0x9d5...a6a66 to: Library.(constructor) value: 0 wei data: 0x608...00033 logs: 0 hash: 0x2fc...611bc
transact to Library.addEntry pending ...
```

MetaMask Notification

Account 6 → 0x0d3...a2f1

https://remix.ethereum.org

0x0d3...a2f1 : ADD ENTRY

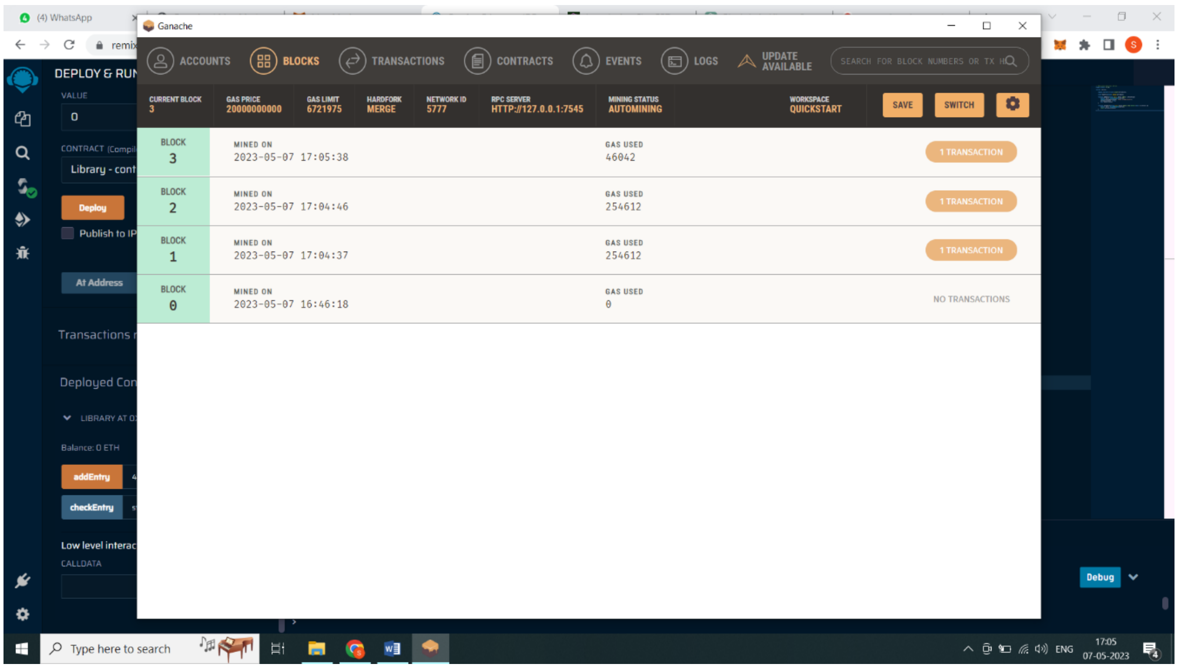
Gas (estimated) 0.00018637 — 0.00018637 ETH

Very likely in < 15 seconds — Max fee: 0.00018637 ETH

Total 0.00018637 — 0.00018637 ETH

Amount + gas fee — Max amount: 0.00018637 ETH

Gas used for AddEntry:

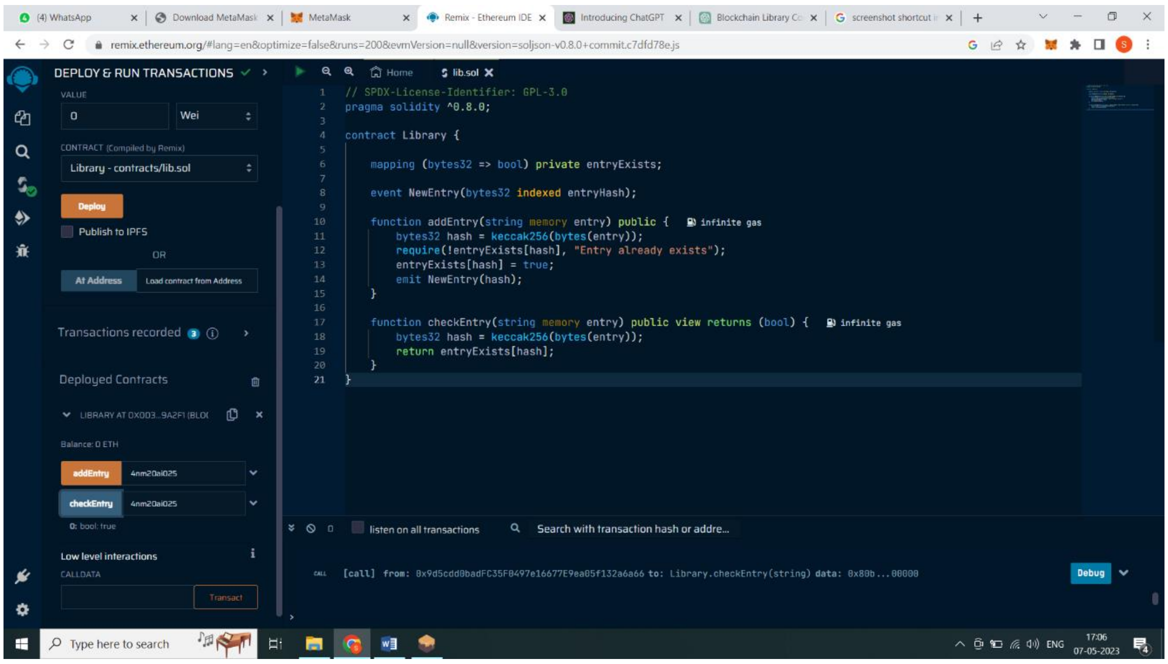


Ganache

CURRENT BLOCK	GAS PRICE	GAS LIMIT	HARDFORK	NETWORK ID	RPC SERVER	MINING STATUS	WORKSPACE
3	20000000000	6721975	MERGE	5777	HTTP://127.0.0.1:7545	AUTOMINING	QUICKSTART

BLOCK	MINED ON	GAS USED	
3	2023-05-07 17:05:38	46042	1 TRANSACTION
2	2023-05-07 17:04:46	254612	1 TRANSACTION
1	2023-05-07 17:04:37	254612	1 TRANSACTION
0	2023-05-07 16:46:18	0	NO TRANSACTIONS

CheckEntry for true case:



remix.ethereum.org/#lang=en&optimize=false&runs=200&evmVersion=null&version=soljson-v0.8.0+commit.c7dfd78e.js

DEPLOY & RUN TRANSACTIONS

VALUE: 0 Wei

CONTRACT (Compiled by Remix): Library - contracts/lib.sol

Transactions recorded 3

Deployed Contracts

LIBRARY AT 0X0D3...9A2F1 (BLOC

Balance: 0 ETH

addEntry: 4nm20ai025

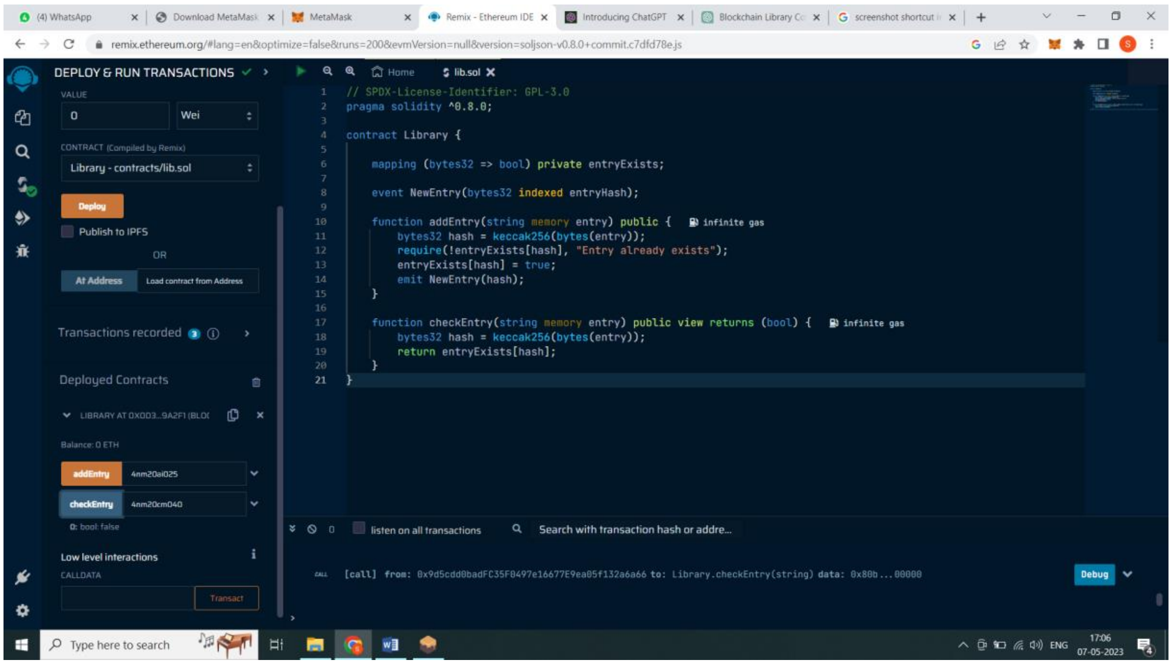
checkEntry: 4nm20ai025

0: bool: true

```
// SPDX-License-Identifier: GPL-3.0
pragma solidity ^0.8.0;

contract Library {

    mapping (bytes32 => bool) private entryExists;

    event NewEntry(bytes32 indexed entryHash);

    function addEntry(string memory entry) public {
        bytes32 hash = keccak256(bytes(entry));
        require(!entryExists[hash], "Entry already exists");
        entryExists[hash] = true;
        emit NewEntry(hash);
    }

    function checkEntry(string memory entry) public view returns (bool) {
        bytes32 hash = keccak256(bytes(entry));
        return entryExists[hash];
    }
}
```

```
[call] from: 0x9d5cdd0badFC35F0497e16677E9ea05f132a6a66 to: Library.checkEntry(string) data: 0x80b...00000
```

CheckEntry for false case:



remix.ethereum.org/#lang=en&optimize=false&runs=200&evmVersion=null&version=soljson-v0.8.0+commit.c7dfd78e.js

DEPLOY & RUN TRANSACTIONS

VALUE: 0 Wei

CONTRACT (Compiled by Remix): Library - contracts/lib.sol

Transactions recorded 3

Deployed Contracts

LIBRARY AT 0X0D3...9A2F1 (BLOC

Balance: 0 ETH

addEntry: 4nm20ai025

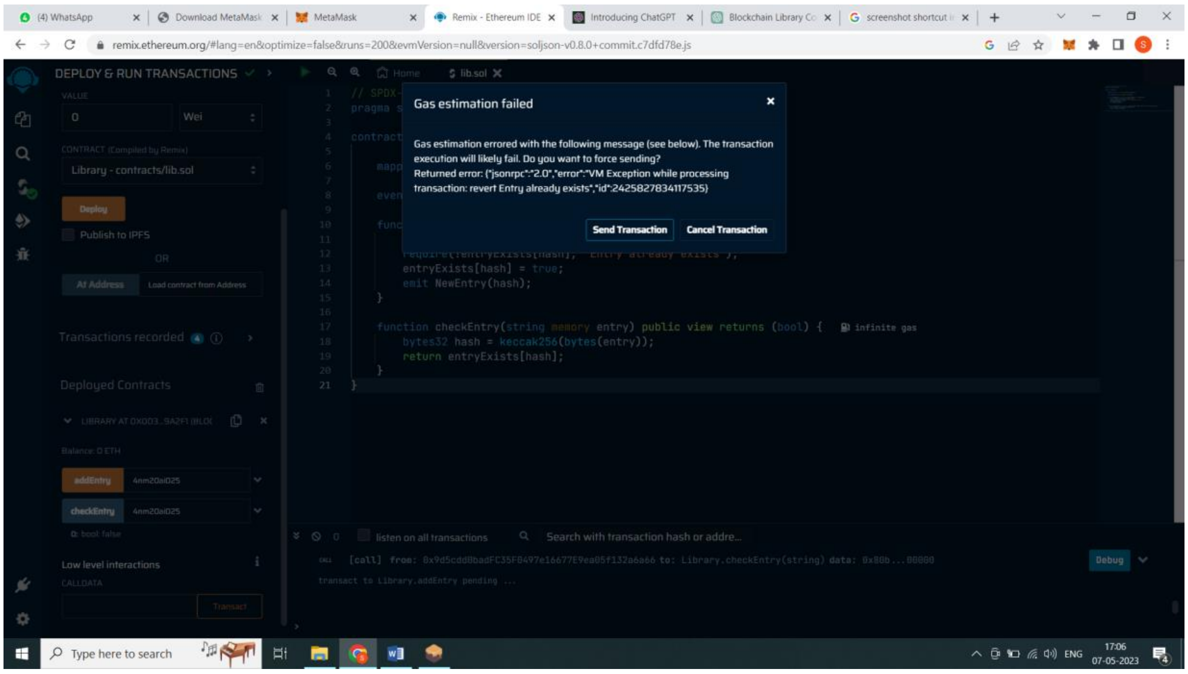
checkEntry: 4nm20cm040

0: bool: false

```
// SPDX-License-Identifier: GPL-3.0
pragma solidity ^0.8.0;

contract Library {

    mapping (bytes32 => bool) private entryExists;

    event NewEntry(bytes32 indexed entryHash);

    function addEntry(string memory entry) public {
        bytes32 hash = keccak256(bytes(entry));
        require(!entryExists[hash], "Entry already exists");
        entryExists[hash] = true;
        emit NewEntry(hash);
    }

    function checkEntry(string memory entry) public view returns (bool) {
        bytes32 hash = keccak256(bytes(entry));
        return entryExists[hash];
    }
}
```

```
[call] from: 0x9d5cdd0badFC35F0497e16677E9ea05f132a6a66 to: Library.checkEntry(string) data: 0x80b...00000
```

Popup for Entry already exists:



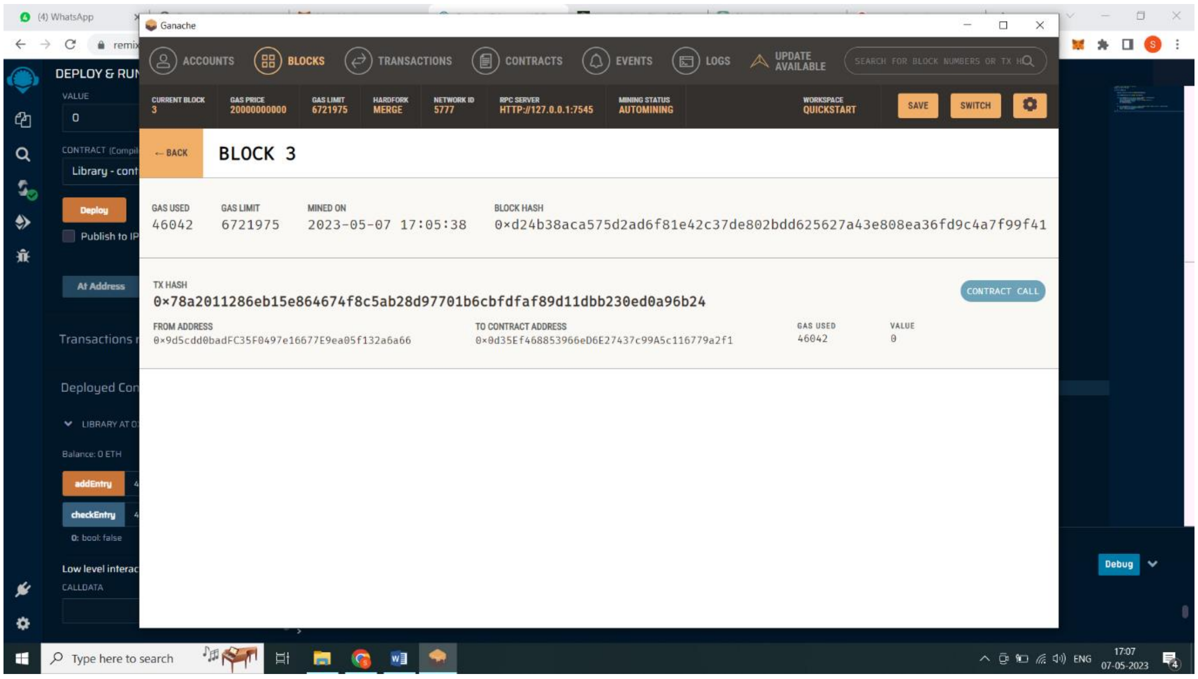
Gas estimation failed

Gas estimation errored with the following message (see below). The transaction execution will likely fail. Do you want to force sending?
Returned error: {"jsonrpc":"2.0","error":"VM Exception while processing transaction: revert Entry already exists","id":2425827834117535}

```
        entryExists[hash] = true;
        emit NewEntry(hash);
    }

    function checkEntry(string memory entry) public view returns (bool) {
        bytes32 hash = keccak256(bytes(entry));
        return entryExists[hash];
    }
}
```

```
[call] from: 0x9d5cdd0badFC35F0497e16677E9ea05f132a6a66 to: Library.checkEntry(string) data: 0x80b...00000
transact to Library.addEntry pending ...
```

Ganache block 3 status:



CURRENT BLOCK 3 · GAS PRICE 20000000000 · GAS LIMIT 6721975 · HARDFORK MERGE · NETWORK ID 5777 · RPC SERVER HTTP://127.0.0.1:7545 · MINING STATUS AUTOMINING · WORKSPACE QUICKSTART

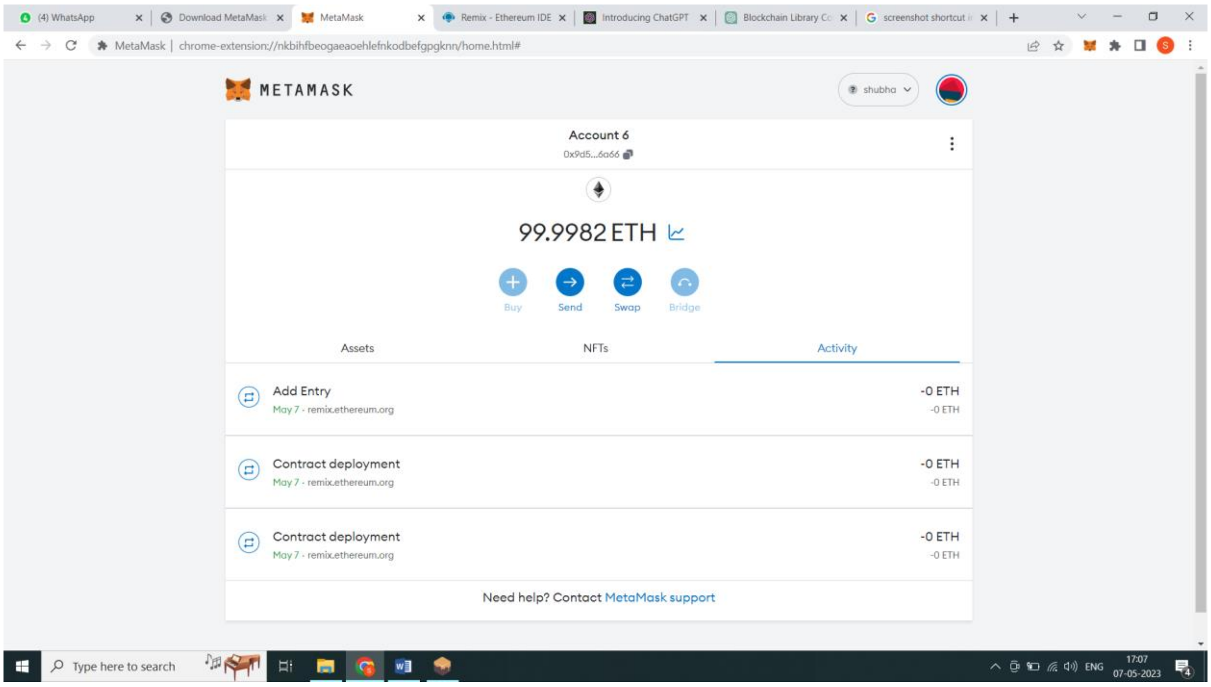
BLOCK 3

GAS USED	GAS LIMIT	MINED ON	BLOCK HASH
46042	6721975	2023-05-07 17:05:38	0×d24b38aca575d2ad6f81e42c37de802bdd625627a43e808ea36fd9c4a7f99f41

TX HASH
0×78a2011286eb15e864674f8c5ab28d97701b6cbfdfaf89d11dbb230ed0a96b24

FROM ADDRESS	TO CONTRACT ADDRESS	GAS USED	VALUE
0×9d5cdd0badFC35F0497e16677E9ea05f132a6a66	0×0d35Ef468853966eD6E27437c99A5c116779a2f1	46042	0

Final Metamask Activity:


METAMASK

Account 6
0x9d5...6a66

99.9982 ETH

Add Entry
May 7 · remix.ethereum.org
-0 ETH
-0 ETH

Contract deployment
May 7 · remix.ethereum.org
-0 ETH
-0 ETH

Contract deployment
May 7 · remix.ethereum.org
-0 ETH
-0 ETH

Need help? Contact MetaMask support