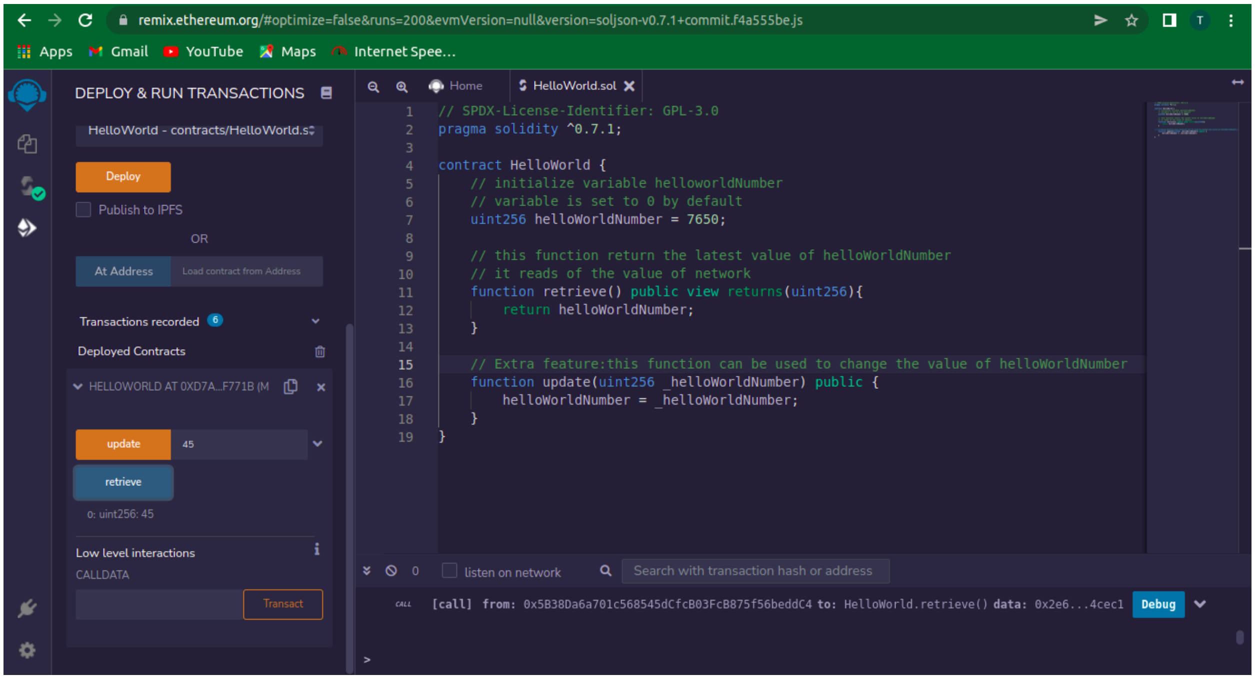
Name: Oluwatobi Akintunlese
Discord Name: Tobi Akin#0304

Background Assignment Solution

Link to github repo solution:
https://github.com/oluwatobi1/ZKU-solidity-et.al/tree/main/background%20Assignment

Q 1: Hello World snippet


remix.ethereum.org/#optimize=false&runs=200&evmVersion=null&version=soljson-v0.7.1+commit.f4a555be.js
Apps
Gmail
YouTube
Maps
Internet Spee...
DEPLOY & RUN TRANSACTIONS
HelloWorld - contracts/HelloWorld.s
Deploy
Publish to IPFS
OR
At Address
Load contract from Address
Transactions recorded 6
Deployed Contracts
HELLOWORLD AT 0XD7A...F771B (M
update
retrieve
Low level interactions
CALLDATA
Transact
Home
HelloWorld.sol
listen on network
Search with transaction hash or address
Debug

update 45

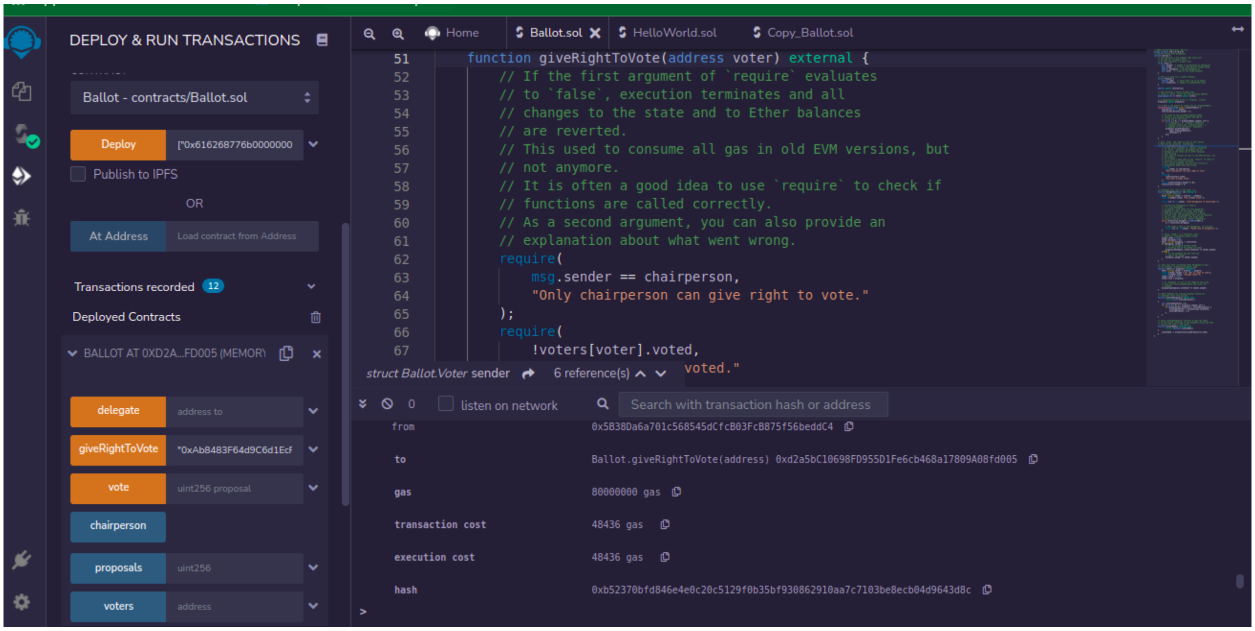
0: uint256: 45

```
// SPDX-License-Identifier: GPL-3.0
pragma solidity ^0.7.1;

contract HelloWorld {
    // initialize variable helloworldNumber
    // variable is set to 0 by default
    uint256 helloWorldNumber = 7650;

    // this function return the latest value of helloWorldNumber
    // it reads of the value of network
    function retrieve() public view returns(uint256){
        return helloWorldNumber;
    }

    // Extra feature:this function can be used to change the value of helloWorldNumber
    function update(uint256 _helloWorldNumber) public {
        helloWorldNumber = _helloWorldNumber;
    }
}
```

```
CALL  [call] from: 0x5B38Da6a701c568545dCfcB03FcB875f56beddC4 to: HelloWorld.retrieve() data: 0x2e6...4cec1
```

Q2 &Q 3

Before improvement



Deploy ["0x616268776b0000000

delegate address to

giveRightToVote "0xAb8483F64d9C6d1EcF

vote uint256 proposal

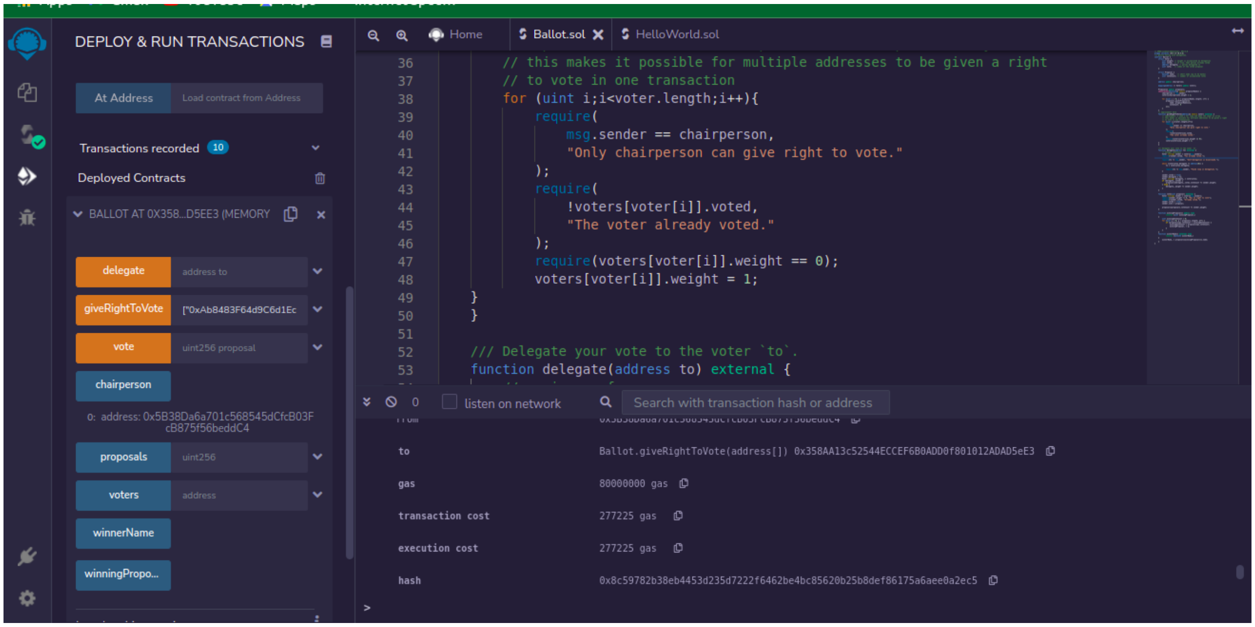
proposals uint256

voters address

```
    function giveRightToVote(address voter) external {
        // If the first argument of `require` evaluates
        // to `false`, execution terminates and all
        // changes to the state and to Ether balances
        // are reverted.
        // This used to consume all gas in old EVM versions, but
        // not anymore.
        // It is often a good idea to use `require` to check if
        // functions are called correctly.
        // As a second argument, you can also provide an
        // explanation about what went wrong.
        require(
            msg.sender == chairperson,
            "Only chairperson can give right to vote."
        );
        require(
            !voters[voter].voted,
                                      voted."
```

```
from              0x5B38Da6a701c568545dCfcB03FcB875f56beddC4

to                Ballot.giveRightToVote(address) 0xd2a5bC10698FD955D1Fe6cb468a17809A08fd005

gas               80000000 gas

transaction cost  48436 gas

execution cost    48436 gas

hash              0xb52370bfd846e4e0c20c5129f0b35bf930862910aa7c7103be8ecb04d9643d8c
```

After improvement



giveRightToVote: ["0xAb8483F64d9C6d1Ec

0: address: 0x5B38Da6a701c568545dCfcB03FcB875f56beddC4

```
        // this makes it possible for multiple addresses to be given a right
        // to vote in one transaction
        for (uint i;i<voter.length;i++){
            require(
                msg.sender == chairperson,
                "Only chairperson can give right to vote."
            );
            require(
                !voters[voter[i]].voted,
                "The voter already voted."
            );
            require(voters[voter[i]].weight == 0);
            voters[voter[i]].weight = 1;
    }
    }

    /// Delegate your vote to the voter `to`.
    function delegate(address to) external {
```

```
to                  Ballot.giveRightToVote(address[]) 0x358AA13c52544ECCEF6B0ADD0f801012ADAD5eE3

gas                 80000000 gas

transaction cost    277225 gas

execution cost      277225 gas

hash                0x8c59782b38eb4453d235d7222f6462be4bc85620b25b8def86175a6aee0a2ec5

>
```