ZKU Background Assignment

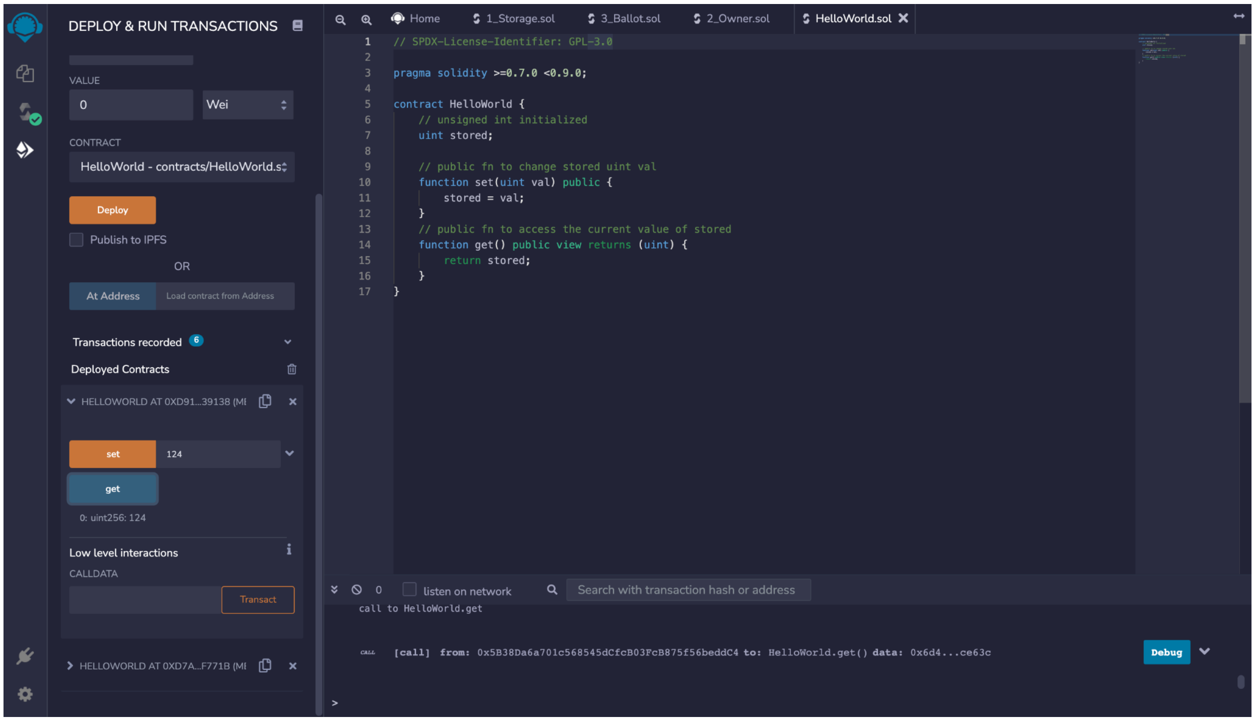
Ashlan Ahmed

course registration email: ashlanahmed@gmail.com

discord username: Ash3156#3173

github with .sol files: https://github.com/Ash3156/zku/tree/master/Background

HelloWorld.sol screenshot:



VALUE: 0 Wei

CONTRACT: HelloWorld - contracts/HelloWorld.s

set 124

0: uint256: 124

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

pragma solidity >=0.7.0 <0.9.0;

contract HelloWorld {
    // unsigned int initialized
    uint stored;

    // public fn to change stored uint val
    function set(uint val) public {
        stored = val;
    }
    // public fn to access the current value of stored
    function get() public view returns (uint) {
        return stored;
    }
}
```

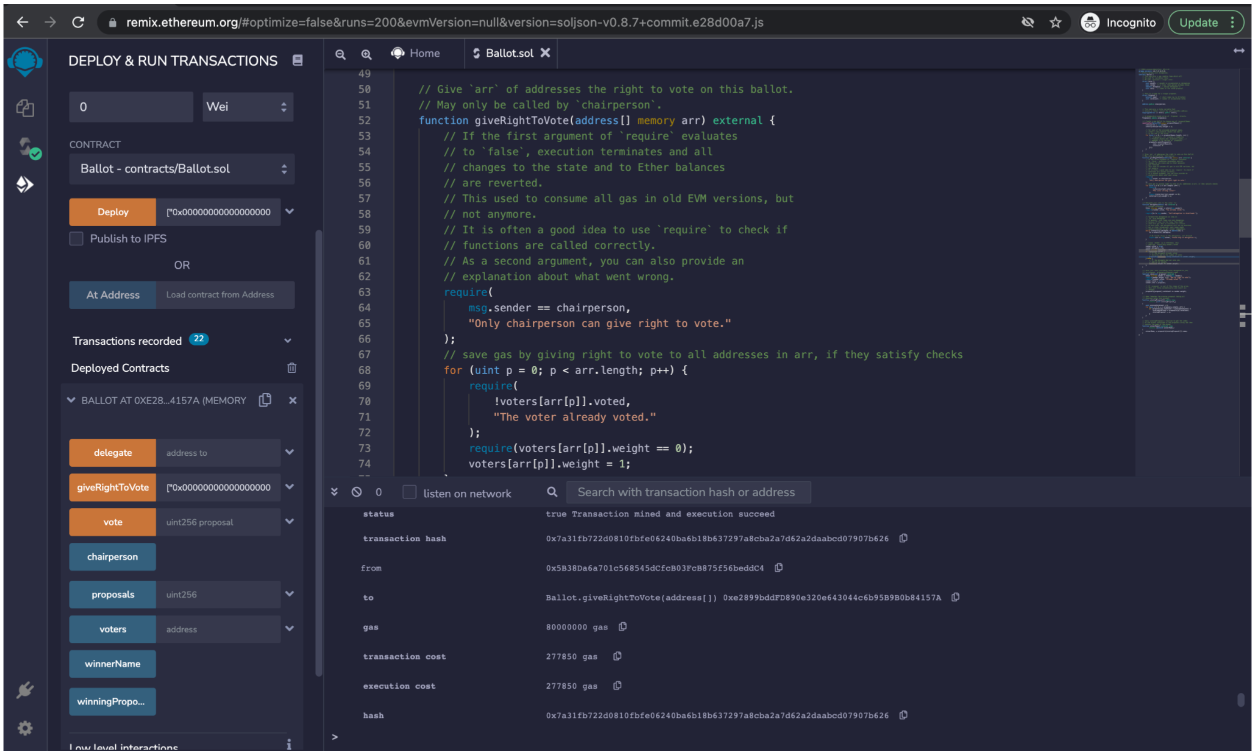
```
call to HelloWorld.get

CALL  [call] from: 0x5B38Da6a701c568545dCfcB03FcB875f56beddC4 to: HelloWorld.get() data: 0x6d4...ce63c

>
```

I optimized the giveRightToVote() function by changing it to accept an array of addresses rather than only one address at a time (reduces function calls to give rights to many addresses, thereby reducing gas fees).

Array of 10 addresses for optimized giveRightToVote() function:
["0x0000000000000000000000000000000000000001",
"0x0000000000000000000000000000000000000002",
"0x0000000000000000000000000000000000000003",
"0x0000000000000000000000000000000000000004",
"0x0000000000000000000000000000000000000005",
"0x0000000000000000000000000000000000000006",
"0x0000000000000000000000000000000000000007",

"0x0000000000000000000000000000000000000008",
"0x0000000000000000000000000000000000000009",
"0x000000000000000000000000000000000000000a"]

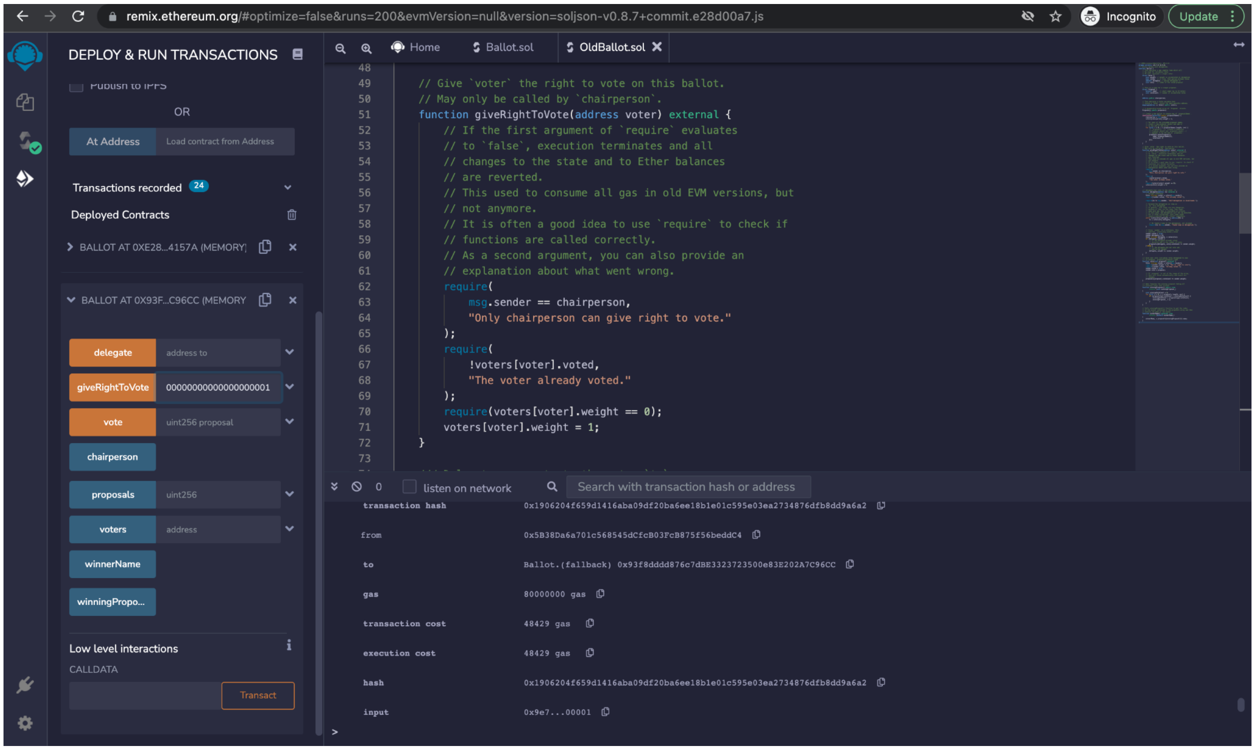
Total gas for optimized: 277850 gas



```
    // Give `arr` of addresses the right to vote on this ballot.
    // May only be called by `chairperson`.
    function giveRightToVote(address[] memory arr) 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."
        );
        // save gas by giving right to vote to all addresses in arr, if they satisfy checks
        for (uint p = 0; p < arr.length; p++) {
            require(
                !voters[arr[p]].voted,
                "The voter already voted."
            );
            require(voters[arr[p]].weight == 0);
            voters[arr[p]].weight = 1;
```

```
status              true Transaction mined and execution succeed
transaction hash    0x7a31fb722d0810fbfe06240ba6b18b637297a8cba2a7d62a2daabcd07907b626
from                0x5B38Da6a701c568545dCfcB03FcB875f56beddC4
to                  Ballot.giveRightToVote(address[]) 0xe2899bddFD890e320e643044c6b95B9B0b84157A
gas                 80000000 gas
transaction cost    277850 gas
execution cost      277850 gas
hash                0x7a31fb722d0810fbfe06240ba6b18b637297a8cba2a7d62a2daabcd07907b626
>
```

48429 for 1 tx on original, so for 10 tx, 484290



giveRightToVote 00000000000000000001

```
    // Give `voter` the right to vote on this ballot.
    // May only be called by `chairperson`.
    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,
            "The voter already voted."
        );
        require(voters[voter].weight == 0);
        voters[voter].weight = 1;
    }
```

```
transaction hash     0x1906204f659d1416aba09df20ba6ee18b1e01c595e03ea2734876dfb8dd9a6a2
from                 0x5B38Da6a701c568545dCfcB03FcB875f56beddC4
to                   Ballot.(fallback) 0x93f8dddd876c7dBE3323723500e83E202A7C96CC
gas                  80000000 gas
transaction cost     48429 gas
execution cost       48429 gas
hash                 0x1906204f659d1416aba09df20ba6ee18b1e01c595e03ea2734876dfb8dd9a6a2
input                0x9e7...00001
>
```

We clearly see that there is less gas for the optimized version; by using a for loop to giveRightToVote for 10 addresses in one function call, rather than 10 individual function calls and permission checks, we have reduced gas costs.