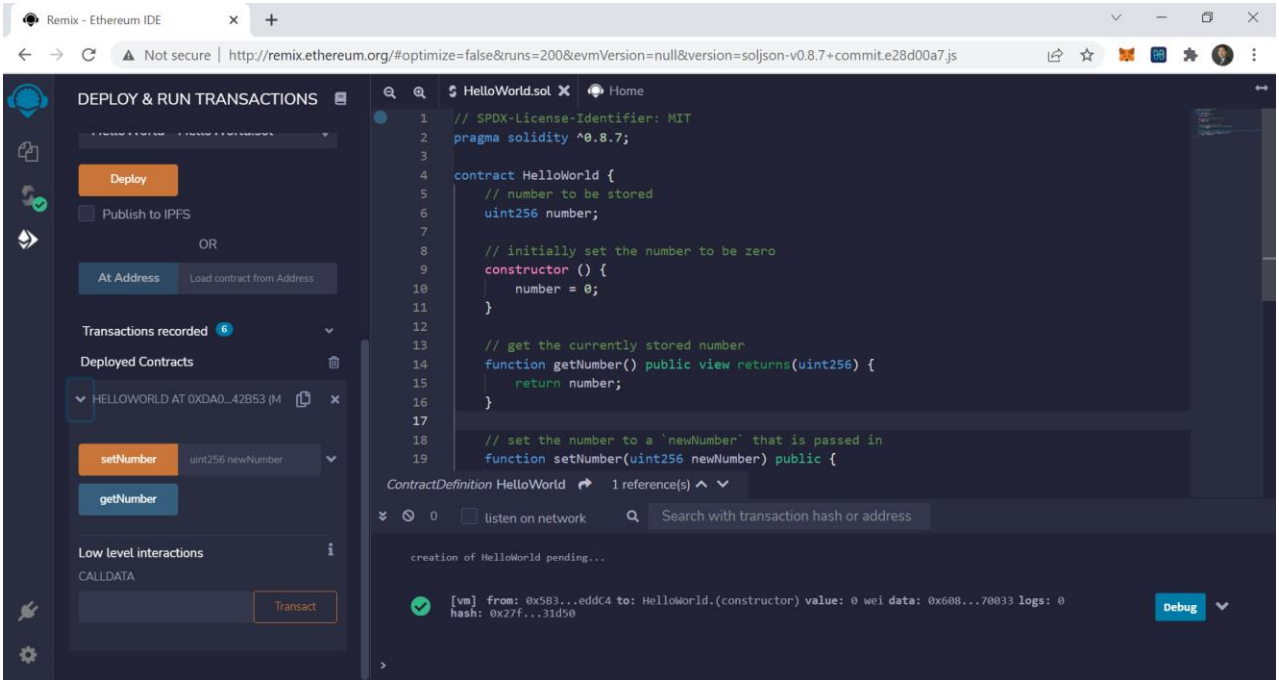
Zero Knowledge University March-April 2022 Cohort

Background Assignment

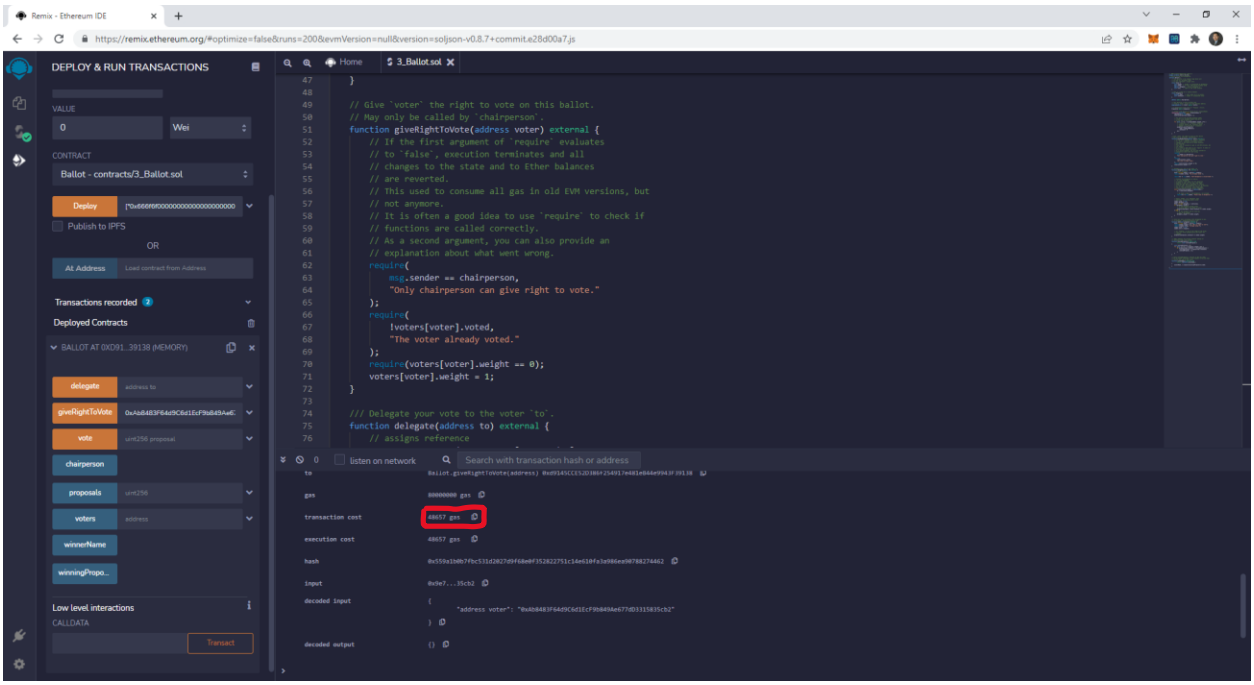
Course Registration Email: zhang.jeremy.2001@gmail.com

Discord Username: xyz5368#1102

1. Hello World Smart Contract
    a. Solidity file: https://github.com/jeremyzhang1/zku-submissions/blob/main/background/HelloWorld.sol
    b. Screenshot of Remix UI once deployed:

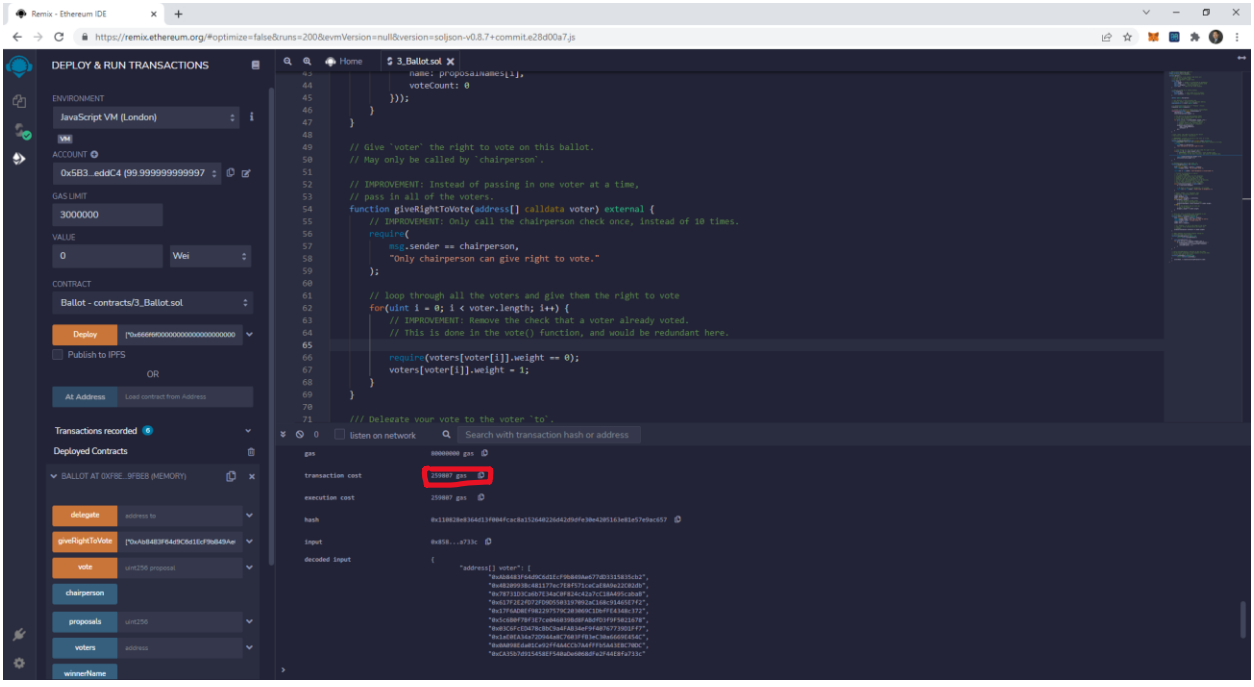


2. Optimizing the Ballot Contract
    a. To give the right to vote to 10 users, the method must be called 10 times. Moreover, the assertion that it is called by the chairperson needs to be checked 10 times. Rather than calling the method 10 times, we can save lots of gas by passing in an array of the all the voters, and looping over the array after checking the assertion only once.
    b. Another optimization is getting rid of the assertion checking that the user already voted. This is done already in the vote() method, so checking again here would be redundant.
3. Implementing the Optimized Ballot Contract
    a. Solidity file: https://github.com/jeremyzhang1/zku-submissions/blob/main/background/NewBallot.sol
    b. Screenshot of gas fees before:



Note that this is for each voter. Since each voter requires 48657 gas, 10 voters would require 486570 gas.

c. Screenshot of gas fees after:



Note that this is the total gas for all 10 voters. The total gas used here is 259807, which is only 53% of the gas used in the old code!