Background Assignment:

Hello, this is my submission for the background assignment of ZKU.

Section A:

Part 1 Answer:

A smart contract is a program that defines a set of rules or conditions that automatically executes the encoded rules when called by a user on the blockchain. Smart contracts always act identically. In particular, once they are deployed on the blockchain, they cannot be modified or controlled by a bad actor. They are like agreements on a specific set of instructions.

To deploy a smart contract, we send an ethereum transaction with the compiled bytecode of the smart contract without the recipient's address. This compiled code is deployed on VM, having a specific address to interact with

Necessary Steps to deploy and smart contract

- Generate the byteCode of your contract by compiling it
- Deployment plugin or a script
- Access to the ethereum node. connecting to a public node or via an API key using a node service like Infura or Alchemy
- Eth funds to pay gas for deployment

Part 2 Answer:

Gas in Ethereum refers to the additional fee required to execute a smart contract or transaction on the blockchain network. Users pay gas fees to compensate for the computing energy required to process and validate transactions on the Ethereum blockchain.

Gas optimization is necessary while developing the smart contract because a user has to pay for the amount of gas used by the function call on the ethereum blockchain. Therefore, contracts should be gas efficient to use less gas.

Part 3 Answer:

Hash is like packing everything in a plain single-sized box. People will not be able to know what is inside the box. The hash function converts everything into a unique fixed-length hexadecimal string. It is practically impossible to find the convert hash back to its original form as every input has a different hash.

Hashing technique is widely used in encrypting private data and passwords to secure and validate the source of input and data. It is also highly used for finding and storing in large databases. It is also used to solve blockchain computation and security.

Part 4 Answer:

Here's how you prove the two balls are different in color to a colorblind person.

Two balls are given to the colorblind person, which he will put behind his back. Next, he will reveal one ball to the prover. Then he will again put it behind his back and show it again, asking. "Did I switch the ball?" if the prover tells/guesses the correct answer colorblind person will agree that two balls are not identical. This whole procedure is then repeated as often as necessary.

The probability of this process a single time is 50%, but if you repeat the process 128 times, the probability of guessing it correct drops close to 0% resulting in the colorblind person getting convinced.

Section B:

Part 1:

Here is the verified deployed link of the commit added Hello World smart contract. In addition, here is the screenshot of the contract deployed and the source code [Gist].

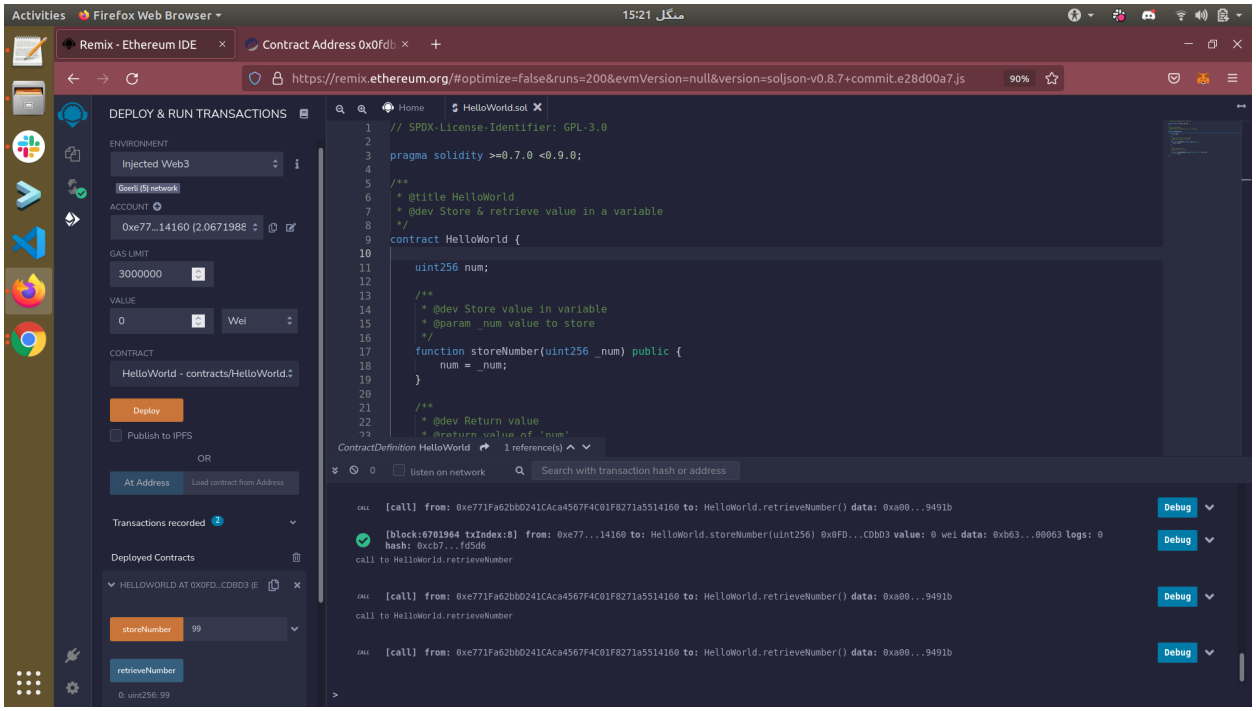

Fig 1.0: Hello World smart contract

Part 2:

1. The commit adding the improved Ballot contract with an additional feature of adding 5 minutes deadline for submitting the vote is deployed here, and here is the contract source file [Gist].

2. Screenshots are attached below.

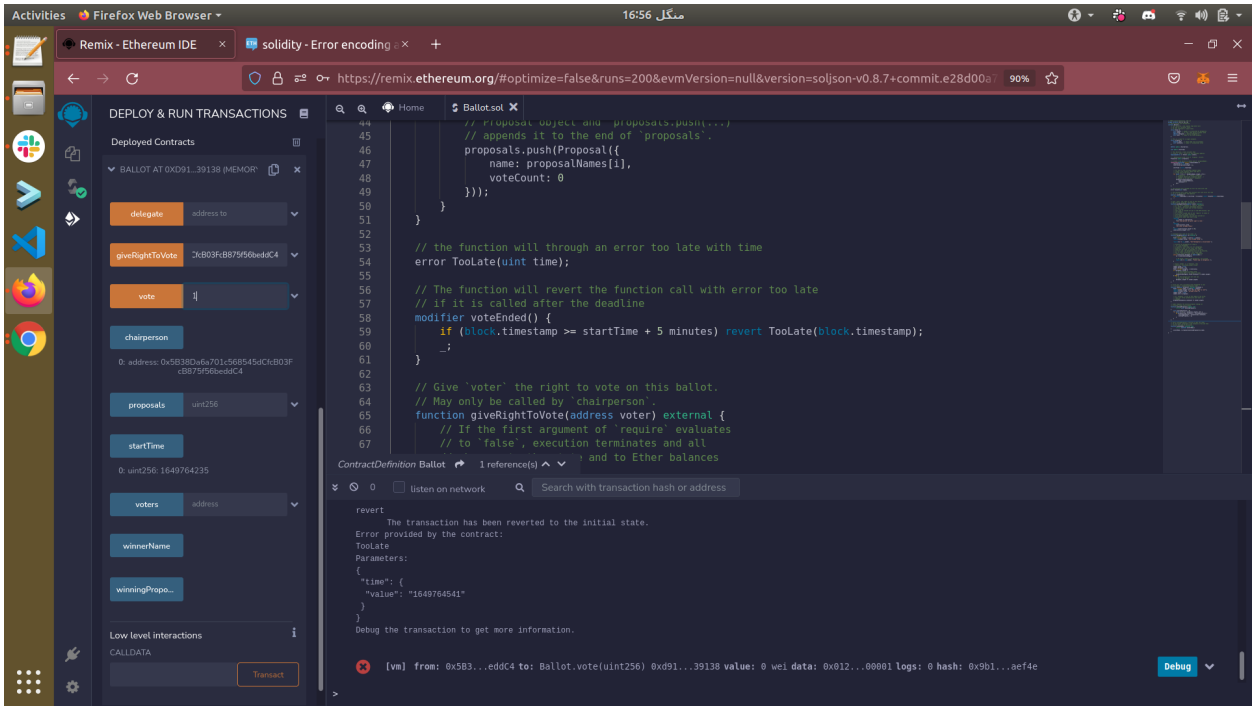

Fig 2.0: Ballot contract interaction

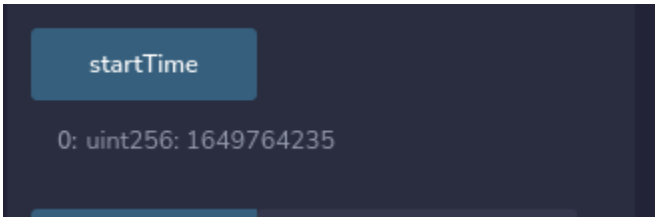

Fig 2.1: startTime of Ballot contract

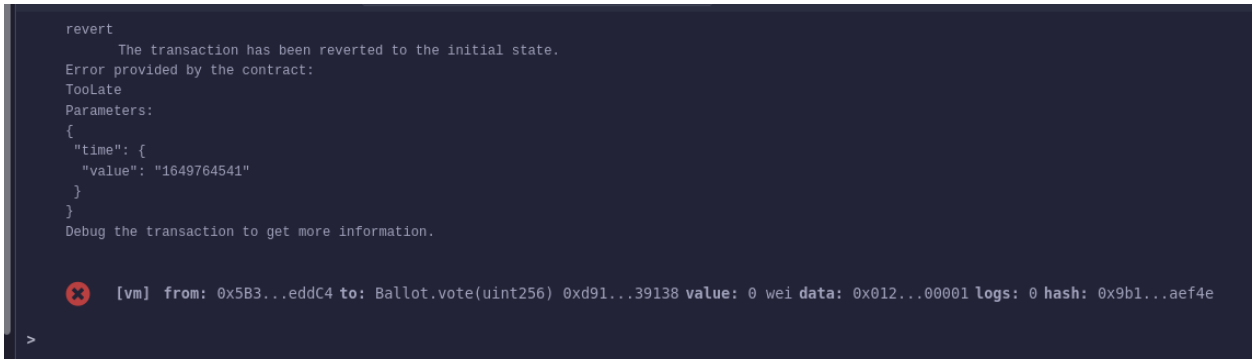

Fig 2.2: revert transaction after the deadline in Ballot contract