zku.ONE background assignment

Darshana, vdcrw7@gmail.com, darz#2944

All answers,code snippets and screenshots can be found at
https://github.com/darshana-v/zku.one

A. Conceptual Knowledge

1. Smart contract is a code that gets executed automatically when predetermined terms and conditions are met. It is essentially a set of self-executing instructions that let all participants be immediately certain of the outcome, without any 3rd party intermediary's involvement. They can also automate a workflow, triggering the next action when conditions are met.

Prerequisite for smart contract deployment:

- Code compiler and hasher
- Some tokens for gas fees
- Deployment script
- Node access to mainnet

Deployment steps:

- Setup mainnet node access
- Install tools
- Test your smart contract, ideally in testnet
- Connect to the wallet, and some tokens for deployment using tools
- Verify your smart contract using any tracker app

2. Gas refers to the cost necessary to perform a transaction on the network. Miners set the price of gas based on supply and demand for the computational power of the network needed to process smart contracts and other transactions.

It is important to optimize gas because it leads to affordable and efficient transactions which in turn leads to the simplicity of transactions, making it more scalable. Furthermore, by decreasing the number of transactions, the network is less prone to malicious attacks and is hence more secure.

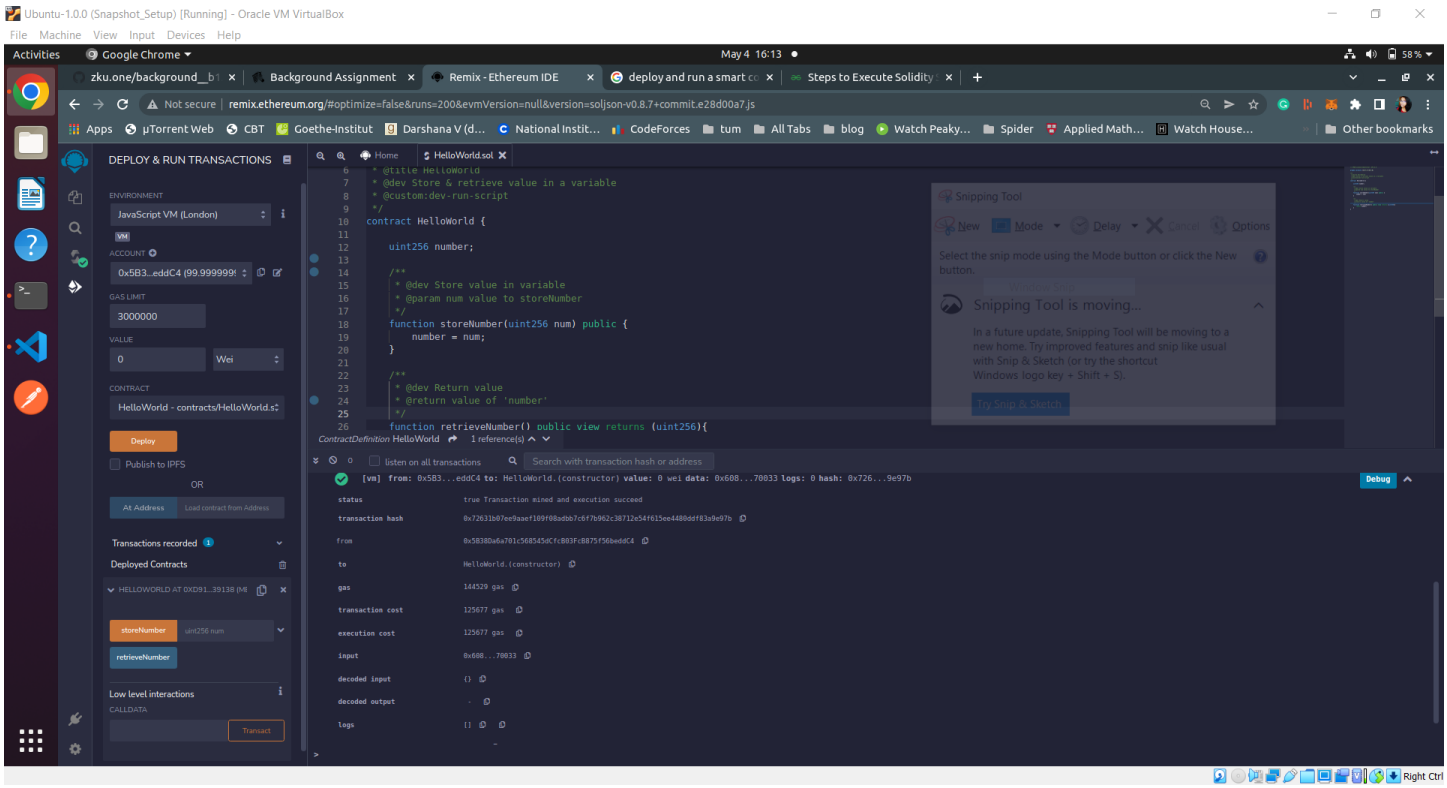
3. Hash refers to a unique fixed length of bits produced by a hash function after a piece of data is submitted through it. Hash functions are mathematical algorithms that convert an input value of any size to an output (hash) of fixed size.

It is used to hide information because it is a one-way process and information cannot be easily retrieved with just the hash digest without heavy brute force to solve for all possibilities(impossible with the computing power we have today).

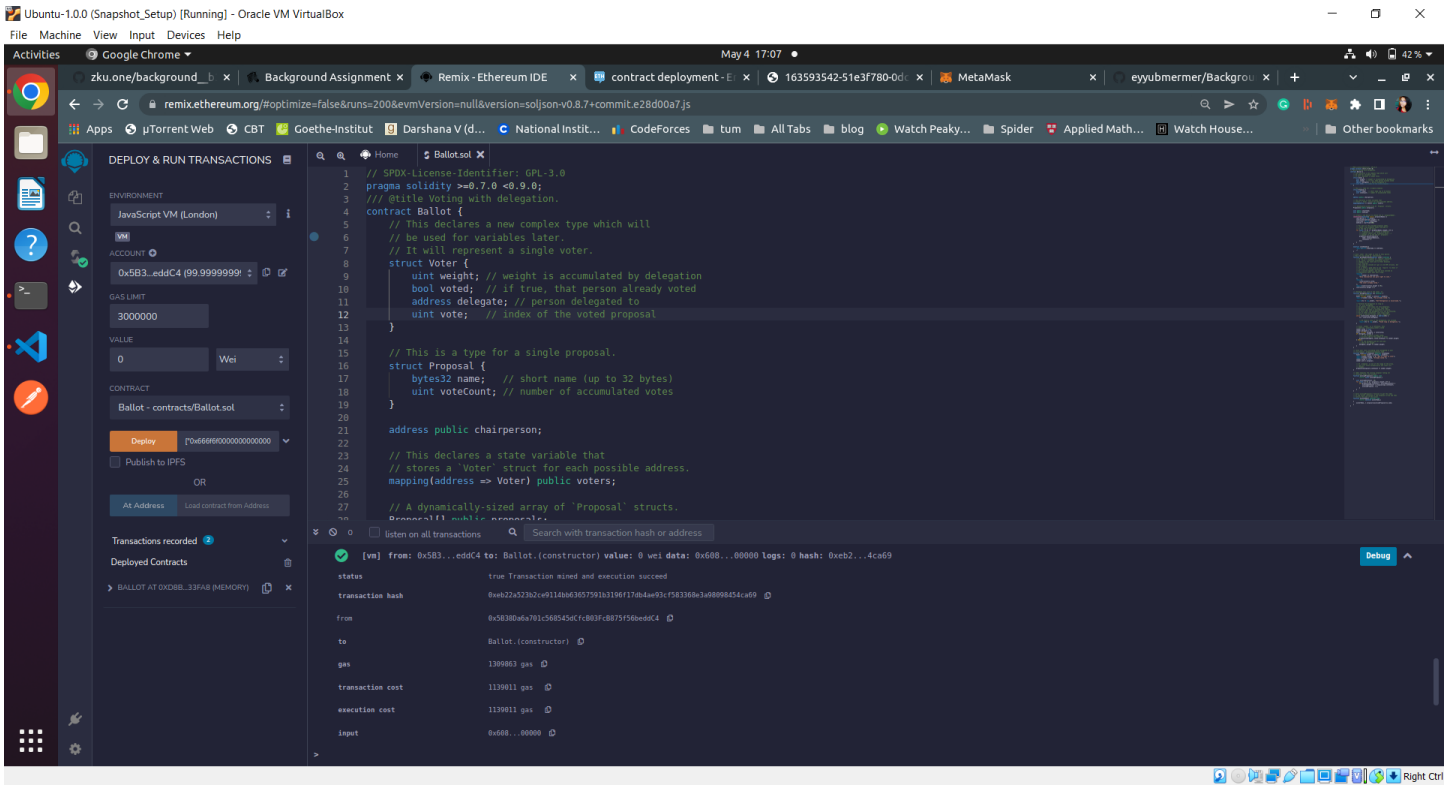
4. I would ask the color blind person to choose one object that I would identify after swapping (secretly) as many ever times as needed by him to prove that they are of different colors.

B. Solidity basics

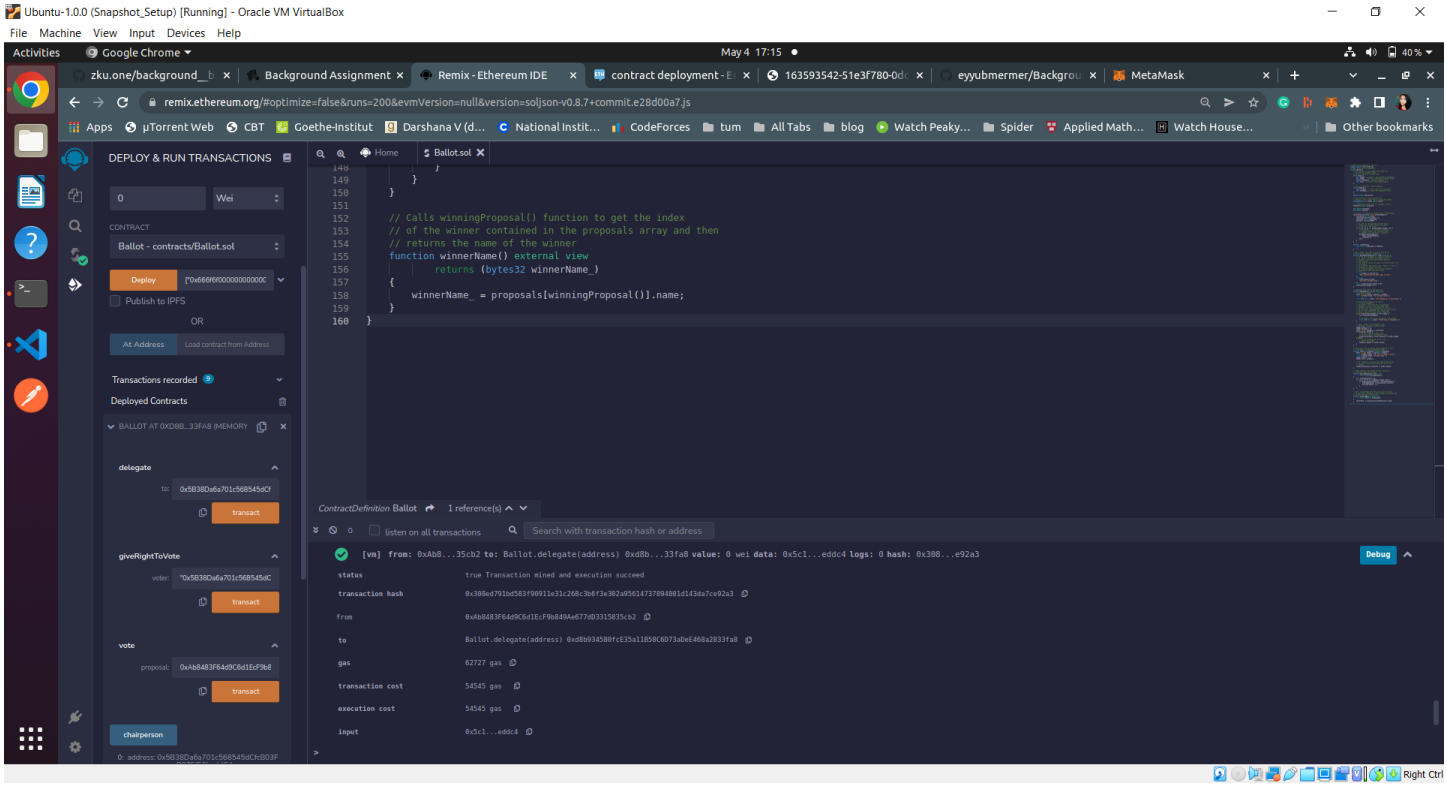
1. Deployed “Helloworld” smart contract



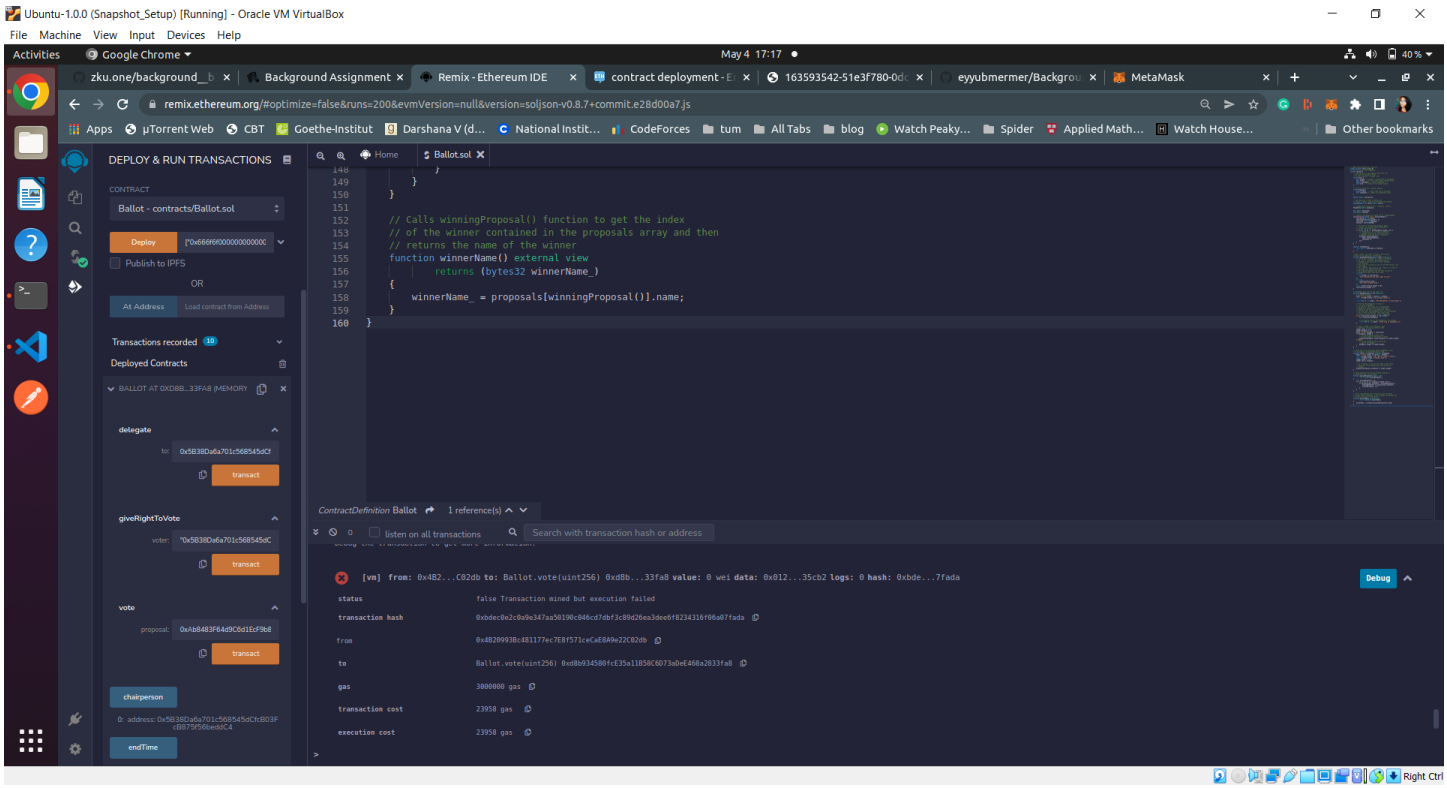
2. Went through and implemented the Ballot script
3. Updated the Ballot script to revert transactions after the 5-minute deadline
    - Successful transactions after deploying



- Successful voting after deploying



- Unsuccessful voting after the 5-minute deadline



- Reverting transaction if the voter has already voted