ZKU ONE

SHREYAS VIVEK

shreyasvivek01@gmail.com

+91 9741002164

Q A.1

What is a smart contract? How are they deployed? You should be able to describe how a smart contract is deployed and the necessary steps.

Ans:

Smart contracts is basically a bunch of code written to perform a specific task, it could be vaguely considered as a written contract, for example, say you want to trade chocolates with your friend, but you want some kind of proof for that, so you would take it in writing, smart contracts are similar to that, they are just written in code, and basically agrees to do something.

***for someone who is over 5 yrs**

Smart contracts could be deployed in a similar way as transacting between 2 accounts, but the catch is, you just send the contract, without specifying the recipient address. This is a very basic idea of deployment of smart contacts.

You would need ETH for gas fees for deployment.

Main things needed are the contracts bytecode which can be generated after compiling the contracts on IDEs

The next thing that you would need is a deployment plugin or script, there's no specific deployment plugin, but we could use the hardhat plugin as it quite simple to use and execute

Hardhat deploy plugin would be to have a scripts/deploy.js

Code below:

```
async function main() {
  // We get the contract to deploy
  const          = await        .getContractFactory("Greeter");
  const          = await         .deploy("Hello, Hardhat!");

  await         .deployed();
```

```
        .log("Greeter deployed to:",         .       );
}

main()
  .then(() =>         .exit(0))
  .catch((      ) => {
           .error(      );
           .exit(1);
  });
```

A sample code to deploy using hardhat greeter

Deploying on a local host would be

1)staring the local node

npx hardhat node

2) on a new in the terminal deploy the contact on localhost

npx hardhat run --network localhost scripts/deploy.js

Q A.2

What is gas? Why is gas optimization such a big focus when building smart contracts?

Say you need to eat a burger, you would go to shop and pay some money and get your order made for you, and then you would eat it.

The money that you pay for the food is for the ingredients, facilities, equipment used, miscellaneous, and then skills, time of the person preparing it. In a similar way, while transacting on the blockchain you must pay a certain amount of money to the person/miner who completes your transaction. This is called gas fees. And it has to be paid to the miners for their work.

***for someone who is over 5 yrs**

Gas is basically a small fraction of fee that has to be paid in order for transactions to be successful.

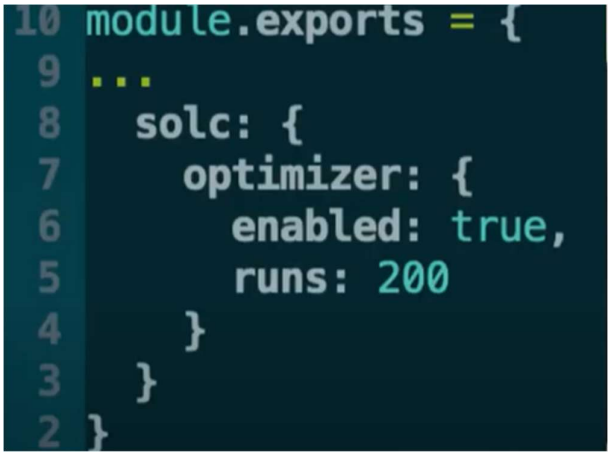
This gas fee is usually a small fraction in of the ETH it is used to allocate resources of the Ethereum virtual machine(EVM) and it is variable, for the same contract at different times, because it is basically a supply demand chain,

ie, if there are many requests, gas fees would be higher on average when compared to the fees when the request is not that much.

Gas optimization is quite essential when considering the overall smart contract because, higher gas fees would mean that fewer users would be utilizing the contract once deployed. But if we consider the overall cost for transaction.

One thing to note would be that if gas is optimized in one part of the contract, it would be increased in another part. So it would be quite crucial to decide when and where you have to optimize the gas.

Gas optimization would refer to minimizing the gas fees for smart contracts. And this could be optimized by an inbuilt solidity function



Q A.3 Q B.1

What is a hash? Why do people use hashing to hide information?

Lets say you're in the middle of a very boring class. And you want to share a secret with your best friend who is sitting far away. You could write your message in a piece of paper and pass it on through your friends. But in doing so, everyone who passes your paper, would be able to know your secret. But you don't want anyone else to know your secret.

So what you could do is make a secret language with your best friend and then write the message In the secret language. Similarly in the world of computer science, the process of "making a secret language is called *ENCRYPTION* and the study of it is called *CRYPTOGRAPHY. HASHING* is one such type of

encryption and it is basically a mathematical function used to make this secret language and it no one could be able to decode or understand it. That's why many people tend to use hashing for protecting their secrets.

***for someone who is over 5 yrs**

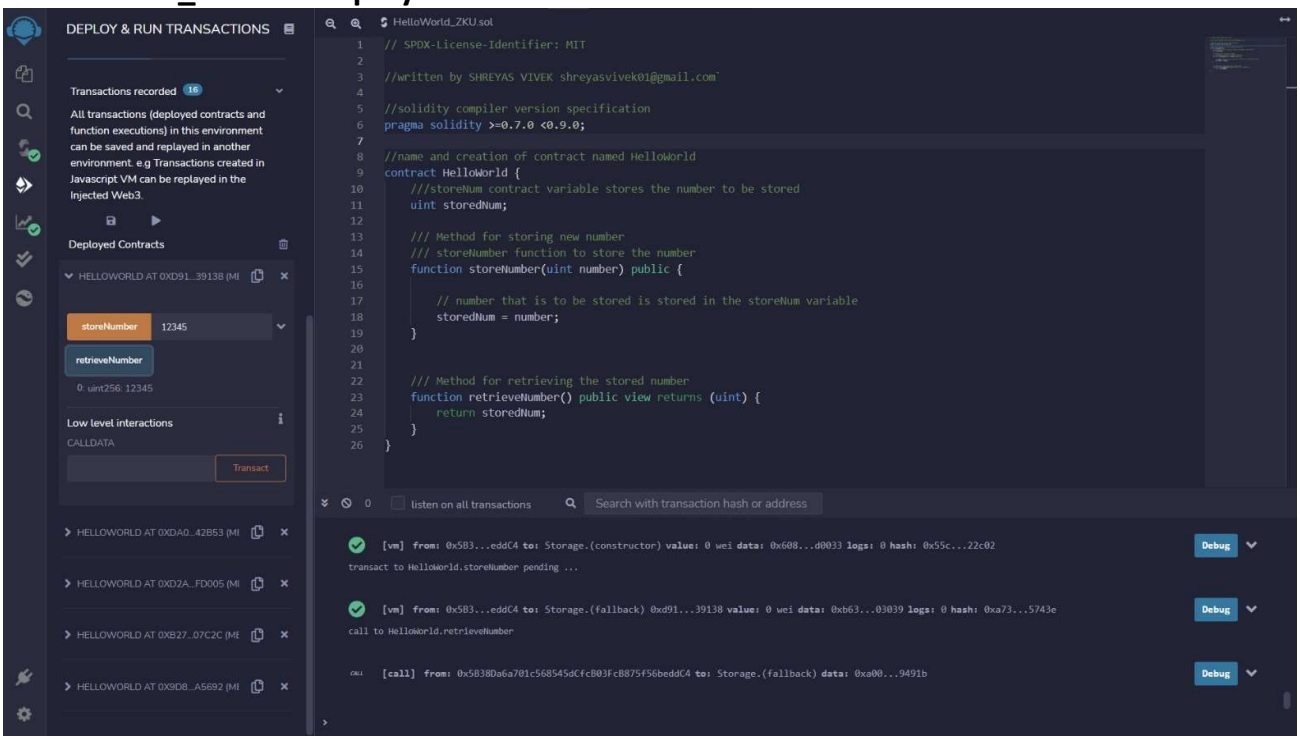
Hash is basically a mathematical function that is used to convert any arbitrary input of variable length to an output of fixed length. This output is highly encrypted and is used mainly for its security/ encryption feature. Every hash value is unique, and only one hash value is generated for an input.

Many people use hashing to hide information is because, It can't be reverse engineered to get the input from the hashed value similar to a cyclic redundancy check or a checksum, it can be used to validate the authenticity or originality of the information. Because, for a given input there will be just one hash value generated, and if at all the data was tampered, it would lead to a change in the hash. When compared with the original data, the difference would indicate the data was tampered.

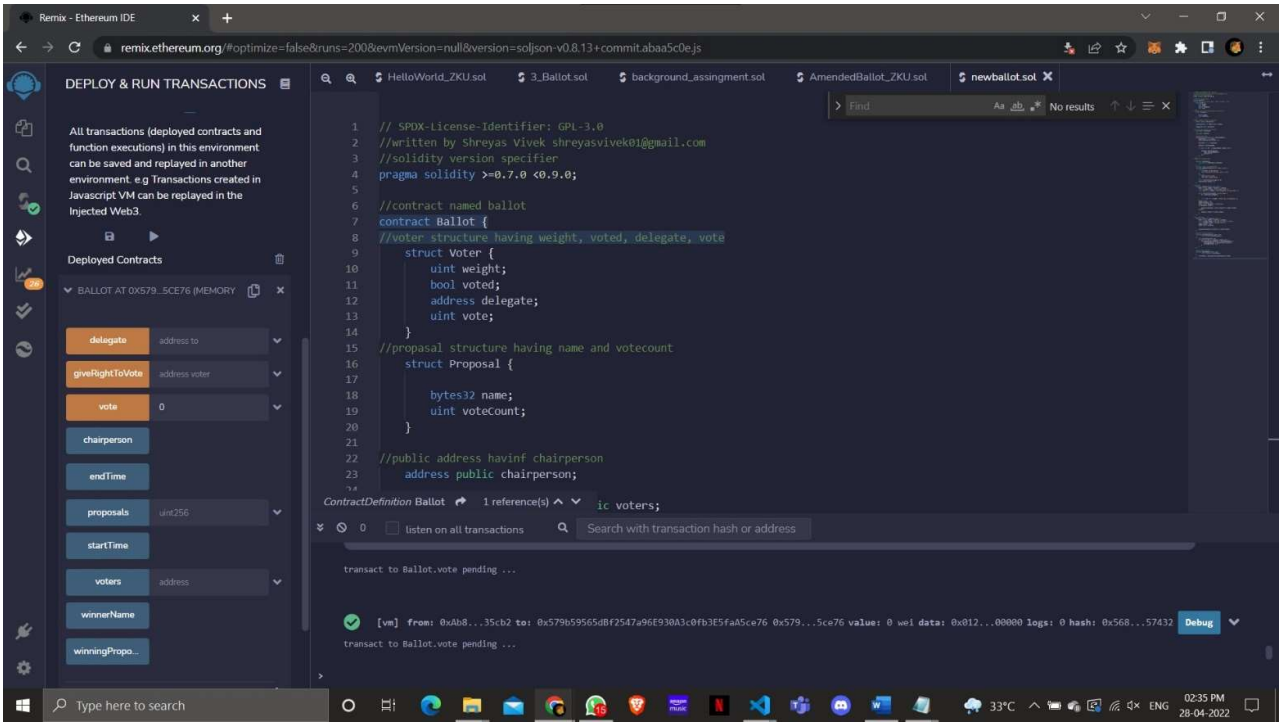
Q B.1

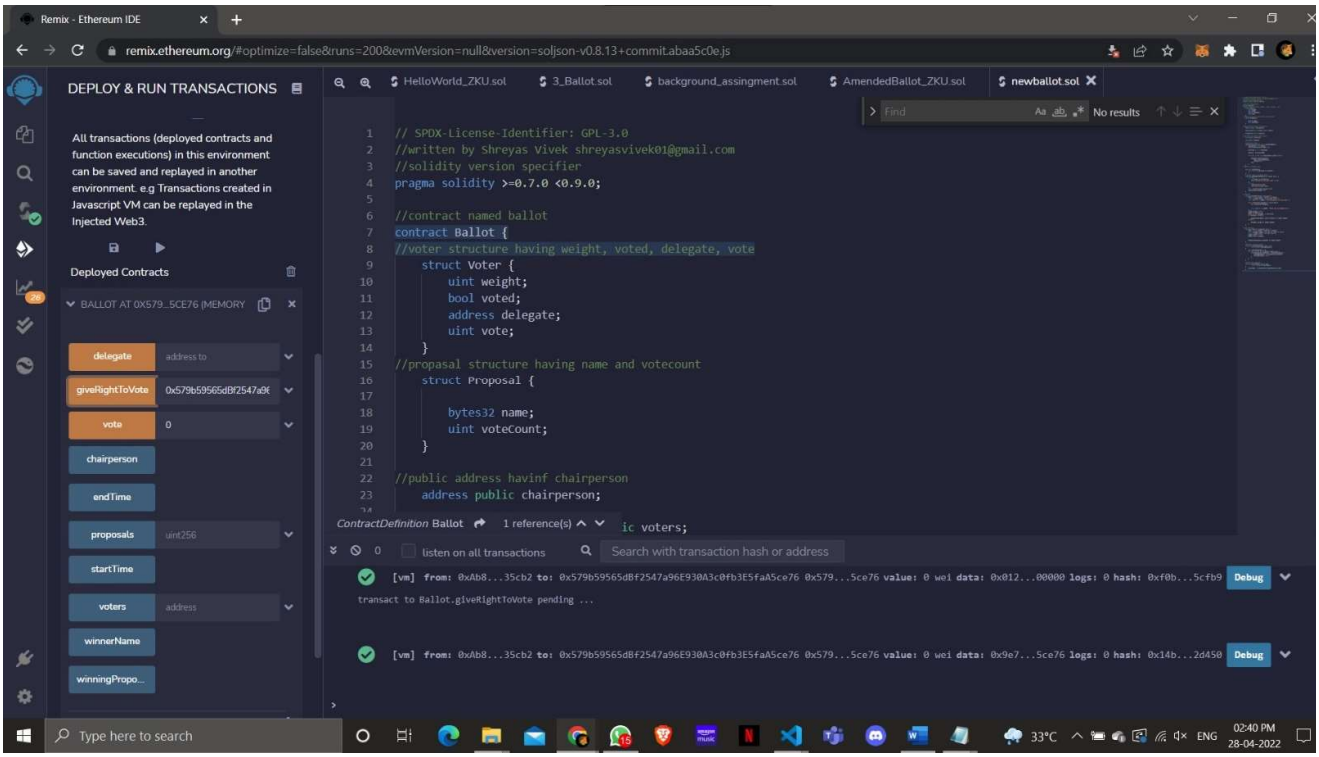
Program a super simple "Hello World" smart contract: write a storeNumber function to store an unsigned integer and then a retrieveNumber function to retrieve it. Clearly comment your code. Once completed, deploy the smart contract on remix. Push the .sol file to Github or Gist and include a screenshot of the Remix UI once deployed in your final submission pdf.

HelloWorld_ZKU.sol Deployment



AmendBallot_ZKU.sol Deployment





GITHUB REPO LINK:

https://github.com/shreyas-vivek/ZKU_BACKGROUND_ASSIGNMENT