ZKU Background Assignment

Youssef Agiza

Conceptual Knowledge

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.**

   Smart contracts are contracts deployed on the Ethereum blockchain network that execute specific tasks when predetermined conditions are met. They usually follow simple if/then statements inside the code which controls the workflow. In simple words, smart contracts are code that is deployed on a blockchain network that performs some actions when some conditions are met.

   To deploy smart contracts:

   a. We first write the contract that will be deployed.
   b. Compile the contract into its bytecode format.
   c. Then, we choose the environment in which the contract will be deployed (e.g. local node, main Ethereum network, etc.)
   d. We can perform some configurations such as the gas limit and
   e. Some specific details related to the deployment depend on the tool being used such as truffle or hardhat.

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

   Gas is the cost necessary to perform a transaction on the Ethereum network. For example, one transaction may require 10k gas and each gas has a cost in ether(the currency in the Ethereum network). To calculate the cost of a transaction in Ether, we multiply the cost of the transaction by the cost of the gas to get how much ether it cost. Then, we multiply that we the result with the value of ether in dollars for example to get the cost in dollars. Gas optimization is important to reduce the cost of the transaction being performed and for deploying the contract itself.

3. **What is a hash? Why do people use hashing to hide**

information?

It is a function that takes an input of any length and transforms it using some operations into a string of fixed length. For example, we can give a hash function the word hello and it will output a string like “2cf24dba5fb0a30e26e83b2ac5b9e29e1b161e5c1fa7425e73043362938b9824”. People use hashing to hide information since it is very difficult to reverse the hash output to its original input.

4. **How would you prove to a colorblind person that two different colored objects are actually of different colors? You could check out Avi Wigderson talk about a similar problem here.**

   Give the two objects to the person and make him put each one of them in a different hand. I will take note of which hand had which color. He then puts the object behind his back and decided to switch them as he pleases. After that, he shows me the objects again and I will tell him whether or not the object changed hands. I can know if he switched them by knowing their colors which is enough to show him that they are different.

Links for part 2:

https://github.com/Youssef-Agiza/ZKU-course/tree/master/background assignment