ZKU Background Assignement

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

- A hash is a fixed length code (usually a string of characters) that identifies a piece of data, and this process of encrypting data using hashes is done by a hashing function, which gets data as its input, and produces the equivalent hash as its output.
- People use hashing to hide information because it's a very secure process and prevent hackers from accessing the information, and also it makes the process of information manipulating and retrieving easier, faster, and more efficient.

2) What is a smart contract?

- A smart contract is a self-executed set of instructions (implement real world agreements) that is executed when certain preconditions are satisfied and without a third-party intermediary. Smart contracts run on a blockchain network.

3) What are gas fees? Why is gas optimization a big focus when building smart contracts?

- Gas fees are payments paid by users in blockchain native token as a compensate for the energy required to perform the computations of their transactions in the blockchain network.
- Gas optimization is a big focus when building smart contracts because it allows us to reduce the fees required for executing our contract, and make the interactions with our contract cheaper and affordable.

4) You have the ability to quickly count the number of leaves in a tree. How can you prove this to a friend, without revealing the exact number of leaves?

Before proving the following statement, I would like to define Zero Knowledge Proof first,

- Zero Knowledge Proof is a proof that proves and verifies the truth of an information without revealing the information itself or any other data, and it can be interactive or non-interactive.
- Now by dropping this definition on our example, I can prove to my friend that I have the ability to quickly count the number of leaves in a tree, without revealing the exact number of leaves by turning around or closing my eyes and letting my friend to choose whether he/she wants to pull off a leaf from the tree or not without telling me, then I will open my eyes and use my ability to quickly count the number of leaves in the tree and tell my friend whether he/she has pulled off a leaf or not, hence by repeating the process many times and in each time I give the right answer I will then prove to him/her that I have this ability and I'm telling the truth.

  This kind of Zero Knowledge Proof belongs to the Interactive type because it required the prover (me) and the verifier (my friend) to interact several times before proving and verifying the truth of the statement.

5) How are smart contracts deployed? List the necessary steps.

- Make sure that the code of the smart contract compiled successfully.
- Choose a blockchain network along with selecting its type (Test or Main).
- Include enough corresponding blockchain native token in our wallet that is being used for the process.
- Push the smart contract to the network.
- Pay the Gas fees needed for the execution and deployment of the smart contract.
- Finally, our smart contract is live…

7) Is the new design better than having separate `confirmReceived` and `refundSeller`? Why or why not?

The new design is better than having separate `confirmReceived` and `refundSeller` because of the following,

- The new design reduces the lines of code; hence it includes less computations than the old one, which means that it decreases the amount of Gas fees required to execute and interact with the smart contract (Gas optimization).
- The new design also makes the process of refunding the seller be automatic, and this is much better since that the seller wants his money back eventually, and as long as the buyer has confirmed the purchase and has received his item, refunding the seller then would be an obvious and inevitable matter and should be done directly.