**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 revolutionary. They are the solid steps into decentralization and removing mediatorial structures, which makes the whole system more transparent and fairer. Basically, a smart contract is a piece of code that is implemented on the blockchain itself. Therefore, they are open to the public. And once deployed, there is no going back, they’ll stay on the blockchain forever. They also execute themselves automatically, which is also a crucial quality.

Let’s take Ethereum, for instance. First of all, an Ethereum wallet is required to deploy our smart contract, which is commonly written in Solidity language. Wallets are the way to interact with the blockchain. For Ethereum, there is an online IDE called Remix. It allows you to write, demonstrate and deploy our contract to the Ethereum blockchain. On the other hand, Remix is not a must. There are other solutions such as Hardhat, Truffle and Ganache, which are more solid solutions than Remix and are used more frequently among non-beginner developers.

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

Ethereum is a Turing-complete World Computer. So, it is open to everyone who wants to deploy smart contracts. The problem is that anyone can run an infinite loop or malicious code on the blockchain and, therefore, block the whole system. To prevent this from happening, the term “gas” has coined. Every transaction, deploying a smart contract also counts as a transaction and requires a gas amount, which depends on the complexity of the transaction. Therefore, the person who wants to block the system forever will need an infinite amount of money, which is practically impossible to block the system.

Gas consumption also incentives developers to write more efficient codes than ever before since every transaction will require “real” money. That’s why every transaction, in other words, smart contract codes must be optimized and, therefore the projects can cost as low as possible.

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

Hashing is an essential concept in blockchain technologies. There are various hashing algorithms. For instance, Ethereum uses Keccak-256 and Bitcoin SHA-256. Simply, the hash is a series of characters in the hexadecimal system and it is derived from any length of text. There are some vital principles. For instance, the same text will always result with the same hash. When you do minor changes in the text, even changing one single character, it will cause an “Avalanche effect” and the hash changes unpredictably and with no connection with the previous hash. Another vital quality is that it is not practically possible to decrypt a hash and see the text it is derived from. Even in a scenario, where the fastest computers are used, it will take millions of years to decrypt. These are the powers of hash algorithms and that’s why they are used widely in hiding information.

1. **How would you prove to a colorblind person that two different colored objects are actually of different colors?**

We can create a spectrum of colors that includes nearly every possible color that our eyes can see and distinguish. Then we can check if both of the objects are at the same point in our spectrum. So, my suggestion is pretty similar to what a litmus paper does (some basic chemistry here ☺). A litmus paper cannot tell us what the solution consists of, or cannot give us any clue what color is it, or is it dangerous to drink. However, we can use a litmus paper to check the pH level of the given solution. And then we can use pH levels to check if the two solutions are the same, without knowing any other information about the solutions themselves. Hash algorithms also have a similar methodology to a litmus paper, or a color spectrum, that I have talked about earlier.