1. What is your understanding of Blockchain?

A blockchain is a database that is shared across a network of computers. Once a record has been added to the chaon it is very difficult to change. To ensure all the copies of the database are the same, the network makes constant checks. Blockchains have been used to underpin cyber-currencies like bitcoin, but many other possible uses are emerging.

2. What is the core problem blockchain is trying to solve?

Security, Data transparency, Verifiability.

3. What are the few features that Blockkchain will give you?

Verifiable, unchangeable, tamper-proof, immutable.

4. What all things does a Block contain?

A block contains block number, transaction records, previous block signatures, mining key.

A block represents the ‘present’ and contains information about its past and future. Each time a block is completed it becomes part of the past and gives way to a new block in the blockchain. The completed block is a permanent record of transactions in the past and the new transactions are recorded in the current one.

5. How is the verifiability of a Blockchain attained?

Every time a transaction is conducted on a blockchain, the transaction data will be stored in a new block. This new block will then be added to the blockchain.

But before the block can be added to the chain, the information contained in it must be verified by the network. This happens by creating a so-called “hash”.

A hash is a 256-bit number that uniquely identifies the data in the block. In order to create this hash, nodes on the network need to solve a complex “mathematical puzzle.” Once the puzzle is solved, all other nodes on the network check if the calculations are correct.

The process of solving this puzzle and as a result creating a new hash is called “mining”.Mining requires great computational power, as it relies on complex mathematical operations.

Example:

Take two blocks, block A and block B. Block A is the first block in the blockchain. In order to verify block A, miners collect the transaction data and give it a hash – call it “hash A”.

To verify the next block in the chain, block B, miners will have to collect another set of transactions and find a new hash – “hash B”. Hash B consists of hash A plus a new hash based on the new transaction data.

Now, if a malicious hacker would want to change any data in block A, hash A would change, as it is based on the data contained in block A. As a result, hash B would change as well, and also all other hashes that follow hash B.

That said, a malicious actor would have to alter the entire blockchain to change any of the stored data. That, however, is practically impossible, because it requires too much computing power.