Question 5

How is the verifiability of Blockchain attained?

Verifiability of a blockchain is made possible by something called the Merkle Tree. In this method, the data are paired and their hash is calculated, and this pairing keeps on happening till a single hash is obtained, called the Merkle Root. This single hash represents the entire hash of the chain, and when two different copies of the chain have to be compared, this Root is what is compared. Any single variation in the chain completely changes the Merkle Root, thus, it makes sure that the two copies are a match, and that one of the two is not corrupted.