Q5. How is the verifiability of blockchain has be attained??

The Blockchain contains a data. Each block is connected to other block and also they generates their own key if any changes happen in data the key will change automatically and the rest of the block also tells changes made in data by verifying the previous block key. And these blocks are stored on different servers if one of them gets deleted then it is easy to recover from other.

Verifiability of Blockchain is achieved with the help of distributed database system. In this system every user has a same record of all the transactions taken. In this process all the users have the same data with

similar hash at the end. Hash is simply a fingerprint(code/key) which is used to check whether everyone has the correct chronological order of the data.
Block 1 = A+B = C
Block 2 = B+D = F
Where,
A is Genesis Block,
B&D are data to be stored.

The copy of the data which is stored in one block is distributed to all other blocks, if the data is changed in any of the block the data can be made proper from the remaining blocks. So, the verifiability of the blockchain is achieved.
A blockchain uses distributed databases. The data is distributed to various users. It

also uses cryptography to generate a unique fingerprint key for each data.
By checking this key among various users data can be verified.

It is similar to the WhatsApp concept. Like If anyone reports different fingerprint, we all will ask that one guy to replace the data entirely from his nearest friend as he is fully wrong. If, Similar any invalid sign is provided by a block all other blocks will be notified of the mistake.