Day 1 Assignment By : Hari Krishna

1. What is your understanding of BlockChain?

A**.** Blockchain is a data structure that holds any type of data by ensuring security,transparency & decentralization.

OR

It is a chain of records stored in the forms of blocks which are controlled by no single authority.Blockchain mainly works on P2P (peer to peer) computing , the same on which torrent works

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

A. Data loss due to hardware issues is the core problem which is being solved by blockchain by using a decentralised system.

3. What are the few features which blockchain will give you ?

A. Its

1. Immutable ,
2. Secure,
3. Decentralized ,
4. Peer to peer network ,

4. What are all the things a block contains ?

A.Block has following parameters

1. Index of the block
2. Time stamp
3. Data
4. Hash of this block
5. Previous block hash

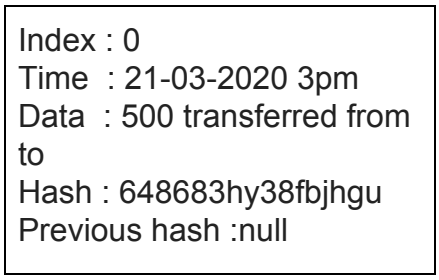
5. How is the verifiability of blockchain attained ?

A. Verifiability of blockchain is attained by using the Hash concept. Whenever a data is feeded into a block it is hashed and a hash value is generated.So if someone changes the date in the block the hash value of the block will change.

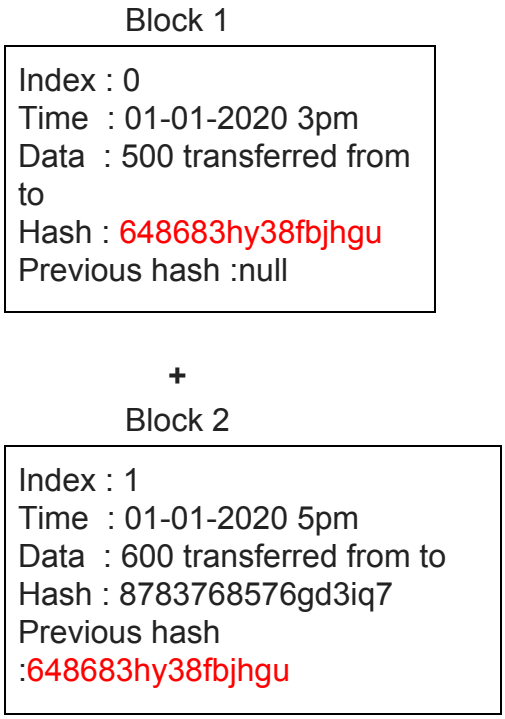
Let's consider an example for better understanding

Let's consider “A” is transfering an amount 5000 to “B”. This transaction is stored in a block as follows :

Block 1



Here a block (block 1) is created , so when another transaction is done it is stored in another block (ex:Block 2) , and after validation block 2 gets attached to block 1 as follows



From the above example we can see that the **Hash of Block 1** and **Previous Hash of Block 2** are the same .

If the block1 is opened or **modified by a hacker** , then the **hash of the block 1 will change.**

So when the next transaction happens a block 3 is created with data and a hash of block 2 is attached to the previous hash of block3. Then its goes for validation , when user(miner in case of bitcoin) validates it , he will be start validating from block 3 and go on to block 2 (by using previous hash of block 3) and when he successfully validates block 2 he will go to validate block 1 (by using previous hash of block 2). This fails as block 1 hash is changed due to modification done by the hacker . By this the user (miner in case of bitcoin) will know that the blockchain has been hacked.

Note : Blockchain can only be hacked by doing a 51% attack