Assignment 1

What is your understanding of BlockChain?
According to me BlockChain is a combination Of Distributed DataSystems and Cryptocurrency.It is a concept where data is verifiable ,Immutable, Tamper Proof and unchangeable.

Here a signature or fingerprint of the data is being created then in the second block of data there is a signature of the previous block and the data of the current block and a new signature is created .This thus leads to unchangeable and tamperproof data. The data benign created is immutable and thus verifiable.

Previous Key + Current Data = New Key

Ex: SHA (Secure Hash Algorithm) is used to create a fingerprint or a Hash.
The concept of blockchain could be understood with Anderson BlockChain.

What is the core problem blockchain is trying to solve?
After the 2008 crisis of leeman roose bank there was a great recession. To eliminate the middleman and make the data verifiable ,Immutable, Tamper Proof and unchangeable. Thus to solve these issues blockchain came into existence.

Question 3

What are the few features which Blockchain will give you?

A blockchain provides the following features:

- The data cannot be corrupted. This is because of the immutablefeature of the blockchain which prevents any individual from changing the data on the chain.
- There is a Decentralized Authority in Blockchain. This means that there is no single authority preceding over the functioning of the blockchain.
- Blockchain provides added security. This is because of the cryptography that is introduced at each stage of the chain calculation.
- Blockchain is a distributed ledger, which means that all information is publicly available for the participants to see. This makes sure that there

is nothing to hide. And since there s nothing to hide, there would not be any sort of cheating.

- It follows the consensus protocol which makes sure that no single party to append to the block without having approval from the other members of the network, added to the security of the chain.

Question 4

What all things does a block contain?

A block in the blockchain usually contains the following data:

- Block header
    - The hash of the previous block
    - The time of block creation
    - The difficulty and the nonce
    - The Merkle tree root
- The transaction details

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.