**Assignment 1**

Ali Mohammed Taresh Ali

[Ali713626792@gmail.com](mailto:Ali713626792@gmail.com)

-------------------------------------------------------------------------------------------------------------------------------------------

**1-What is your understanding IN Block chain?**

Blockchain is a form of recording transactions in a secure way in a public or private mode without the intervention of governing authority. It is a digital ledger of transactions encrypted and distrubuted accross the computer systems in the network. One of the applications of Blockchain is Bitcoin, Eherium etc. In simple words, it can be explained as a data structure that holds the transaction records while ensuring security, transparency and decentralization.

Block chain mainly consist of two technology Distributed database and Cryptography Distributed database means all data are share and save in different locations

Cryptography is method of protecting information and communicate using codes.

**2-what are the core problem blockchain try to solve.**

Blockchain solves data loss, data corruption, transparency / trust issues which can arise due to hardware or connection issues by making the ledger public. In simple words, the transactions carried out by the users are flooded to the network so that all the nodes records the transactions by every user.

Authenticity

Security

Third-party dependant

**3-What are the new features blockchain gives you.**

Transparency,

Immutability,

verifiability,

highly secure network,

Decentralized,  
Tamper proof  
Unchangeable-

**4-What all things block chain contains?**

A Block number,

Transaction records,

Hash or signature of the previous block,

mining key.

In addition, the transactions are formed as per Merkel Tree, a target value or nounce.

**5. How is verifiable of blockchain has been attained?**

Verifiability is achieved by using the digital signature, comparing Hash. For Example, The transactions are added to the blockchain network when A performs or send some information to B.

The transaction are flooded to the network and all the nodes record the transactions between A and B. For a node to build or mine a Block, the hash of the previous block is verified. Since hashing is a one-way method of encrypting data, hashing concept protects the transaction data even if a malicious user tries to intercept the network. Even, if a transaction is intercepted, the copies of the transaction stored in the other nodes does not accept the change as per the consensus achieved in the network.