BlockChain Assignment 1

1. Explain the concept of hash with respect to bitcoin blockchain.
Ans.
A hash is a digital fingerprint, made by hashing the block header twice through the SHA256 algorithm. In the Bitcoin blockchain hashes are of 256 bits, or 64 characters.
A hash is developed based on the information present in the block header which includes (block number, the time and difficulty when the block was mined, the Merkle root of the included transactions, and the nonce)
During mining, a block header is hashed repeatedly by miners by altering the nonce value. Through this exercise, they attempt to create a proof of work, which helps miners get rewarded for their contributions by finding the correct nonce value to a block, which in the end gives us the hash of the block.
Hashes are of a fixed length regardless of the original amount of data or file size involved, its unique hash will always be the same size which makes it impossible to guess the length of the hash if someone was trying to crack the blockchain.

2. What is one way mapping? How is it different from 2 way mapping?
Ans.
One way Mapping is the process of conversion of data of any length into its hash value of fixed size.
Original data can't be produced back from its hash value in one way mapping.

Two way Mapping is the process of first conversion of the data into encrypted form using any encryption and then using any decryption method decrypting the encrypted text to get back the original data.
Original data can be obtained back once encrypted in Two way mapping.

3. What is the public key and private key in blockchain? Explain with the help of a suitable example.
Ans.
A public key is a cryptographic code that allows users to receive cryptocurrencies into their accounts. A bitcoin wallet address is a hashed version of your public key. Every public key is 256 bits long and wallet addresses are 160 bits long.
A private key is a secret number that is used in cryptography, similar to a password. In cryptocurrency, private keys are also used to sign transactions and prove ownership of a blockchain address.
Example:
In Bitcoin when we are performing a transaction to another person there private key is used to generate a digital signature, which can be used by another person whom the amount is sent to verify the transaction. Public can be referred to as a wallet address of the other person to whom the transaction was sent.

4. What web 2.0 problems does web 3.0 solve?

Ans.

Problems of web 2.0

There is centralized database storage in web 2.0 due to which 2 main problem arises:
Privacy Concern
Single Point Failure
Easy Hackable System due to centralized storage.
If for some reason the central storage system gets down then access to all other nodes gets down too.

Problem solved by Web 3.0

Decentralized Storage which resolves the concern of centralized storage.
User have complete control over data, data is not exposed to the 3rd parties which were there in Web 2.0
User can even monetize their data

5. What are the different technologies in web 3.0?

Ans.

Blockchain
AI
Augmented Reality / Virtual Reality
Metaverse
Big data