BLOCKCHAIN (UE20CS335)

OPEN BOOK ASSIGNMENT 1

1. Can blockchain be applied to any application? Give an example to support your answer.
2. Why do we say that public blockchain is prone to 51% attack?
3. What is the disadvantage of Consortium blockchain? In what type of systems, would you prefer consortium blockchain over private or hybrid blockchain?
4. How much time would it require for a miner to mine a block?
5. Why DES is not a good idea to be used in blockchain setup?
6. What are the different fields present in a block header of bitcoin and Ethereum?
7. Consider two friends Alice and Bob. Bob wants to send a message m that is digitally signed to Alice. Let the pair of private and public keys for Alice and Bob be denoted represent the operation of encrypting m with a key Kx and H(m) represent the message digest. How the message will be transmitted from Bob to Alice.
8. How does blockchain contribute to the development of digital identity and personal data management?
9. Compare and contrast blockchain with other emerging technologies such as artificial intelligence and the Internet of Things.
10. Given a message of 748 bits. How many padded bits are required for SHA 256?
11. What is the future of blockchain-based finance?
12. How has the evolution of mining hardware and software impacted the competitiveness and efficiency of blockchain mining, and what are some of the latest trends and innovations in this field?
13. How is difficulty playing an important role in mining process?
14. What is the difference between gas fee, gas price, transaction fee, block fee, uncle fee, burnt fee in Ethereum? Out of these, which are not present in bitcoin?
15. It is said that the contents on blockchain are immutable. If any change is made at a node X, everyone in the network sees it and X's ledger is updated to its previous state to maintain the consistency. Now consider that Digilocker application is launched on a blockchain platform. In this application, if a person's address has to be updated on his Aadhaar document. Does the blockchain allow this change? Ideally No because of the immutable property. But in a situation like this, it should be allowed as the address of a person can change. In a scenario like, how blockchain will perform such a change?