Blockchain QuestionBank

1. What is the difference between hashing and encryption?
2. Write a short note on distributed consensus.
3. Explain symmetric and asymmetric algorithm.
4. Which are the Properties of Interactive Zero-Knowledge Proofs of Knowledge.
5. Explain ECDSA signature generation algorithm.
6. What is nothing at the stake problem?
7. Which of the following does PoW consensus guarantee (or guarantee with all but negligible probability)?
    a) agreement
    b) validity
    c) termination
8. Compare PoW and PoS consensus mechanisms.
9. What are the strength and weaknesses of the PoW.
10. Explain steps of the PoB and list advantages and disadvantages of PoB.
11. Explain the steps of the PoW and comment on the energy efficiency of the PoW.
12. List the advantages of the permissioned blockchain.
13. List the advantages of the permissionless blockchain.
14. List the disadvantages of the permissioned blockchain.
15. List the disadvantages of the permissioned blockchain.
16. How blockchain is different than the distributed databases.
17. How PoW guarantees ledger consistency?
18. How PoW guarantees participants' privacy?
19. How PoW guarantees ledger anonymity?
20. How PoW guarantees ledger transparency?
21. What are the different types of the blockchains?
22. What is Hash function? Write down the properties of good hash functions.
23. Write short note on Cybil attack.
24. Write short note on eclipse attack.
25. Write short note on majority attack.
26. Write short note on blockchain difficulty.
27. Write short note on PoW energy utilization.
28. Write short note on bitcoin incentive mechanism.
29. PoS is more energy efficient than PoW, Justify.
30. What are the limitations of the blockchain?
31. Explain the working of the GHOST mechanism.
32. Explain hard forking and soft forking in terms of bitcoin blockchain.
33. How bitcoin blockchain handles temporary forking?
34. How blockchain provides immutability, transparency, and privacy?
35. Explain practical byzantine fault tolerance mechanism.
36. Write short note on double spending in bitcoin.
37. How to decide that 1KKhtG8XygZM7ioyWFWUzSwGZTjFcs8nR4 bitcoin address has suspicious activities.

Ans.

i. first visit to **bitcoinabuse** portal to verify that address belongs to bitcoin blockchain.

ii. Verify that the address is reported by someone as a malicious or not if yes then the address is malicious otherwise we need to check financial transactions of that account.
iii. Visit **bitref** and insert suspected bitcoin address in the search box and hit enter. This will give us details about list of transactions are done by that address.
iv. Search number of transactions and intended source and recipient for those transaction on blockchain.com
v. If after six or more hopes bitcoin is again resend to this address it indicates that address is suspicious.
vi. Search current address and all other suspicious address on **bitcoinwhoswho** portal to get its IP.
vii. Search that IP on the **passivedns** to get URL for that IP address.
viii. After getting URL finally search who owns that URL on the **whois.domaintolls.com**

38. Explain bitcoin transaction flow. How miner solves bitcoin block cryptopuzzle.
39. Differentiate between permissioned and permissionless blockchain?
40. Write short note on the forking and its variations in the bitcoin blockchain.
41. Write short note on blockchain identity management?
42. Explain overall working of the bitcoin blockchain.
43. How blockchain can handle real time day to day challenges?
44. What are the challenges in the blockchain regulation in the india?
45. Define blockchain.
46. Explain DAO and DAO attack.
47. What is Smart Contract? Explain it with example
48. Explain the concept of digital signature in Blockchain in detail
49. What is Gas and Gas limit? Explain all the cases
50. Explain the role of Merkle tree in Blockchain
51. Explain role of Blockchain in Medical Record Management System

Ans: We face a lot of issues, such as doctor's appointments, report organization in one spot, and report follow-ups. People now bring a large number of papers to the doctor's chamber. They carry prescriptions, reports, and X-ray files, among other things. It complicates everyone's life as a result. All of the reports must be reviewed by doctors on a regular basis. It is difficult to read old reports on a regular basis, and patients do not receive the correct medications or treatment. Doctors also find it extremely difficult to comprehend handwritten prescriptions. Data security, authenticity, time management, and other areas of data administration are dramatically improved when blockchain (smart contract) technology is linked with standard database management solutions. Blockchain is a groundbreaking, decentralized technology that protects data from unauthorized access. After smart contracts are implemented, the management will be satisfied with the patients. As a result, maintaining data privacy and accountability in the system is tough. It signifies that the information is only accessible to those who have been authenticated. Blockchain focuses on limiting third-party engagement in medical health data and improving data security. ,throughout the process, this will improve accessibility and time efficiency. People will feel safer during the payment procedure, which is the most significant benefit. A smart contract and a peer-to-peer encrypted technology were used. ,The hacker will not be able to gain access to this system since this document uses an immutable ledger. ,They will not be able to change any of the data if they gain access to the system. If the items are found to be defective, the transaction will be halted. Transaction security will be a viable option for recasting these problems using cryptographic methodologies.

52. What is Quantum Computing? Explain its need in Blockchain

Ans: Quantum computing is a method of solving problems that are too large or complex for traditional computers by employing the laws of quantum mechanics. This branch of computer

science employs quantum theory principles. Quantum theory explains how energy and matter behave at the atomic and subatomic levels. Qubits, or quantum bits, are the fundamental unit of information in quantum computing. In traditional computing, this is analogous to a binary bit. Whereas traditional computers use bits with either 0s or 1s to store information, quantum computers use qubits. Qubits carry information in a multidimensional quantum state.

Quantum Key Distribution (QKD) uses quantum mechanics laws to allow two parties to exchange secure data for detecting whether a third party is attempting to eavesdrop on their exchange. Using quantum keys in conjunction with a blockchain network could help protect against attacks from both classical and quantum computers.