**Question Bank of Blockchain**

1. How can you identify a block?
2. List and explain the type of nodes in blockchain.
3. Differentiate between the token and cryptocurrency.
4. Explain the types of blockchain models.
5. What are the types of keys important in cryptography and how it is used?
6. Define hash function. Explain the properties of it.
7. List and explain the data structures used in blockchain.
8. Define consensus. What is the need of it?
9. Define smart contract. How it works?
10. **What is a Dapp and how is it different from a normal application?**
11. Define Blockchain with Key features.
12. Suppose john wants to encrypt email messages before sending them to friends. The RSA Encryption Scheme is often used to encrypt and then decrypt electronic communications. John wants to set up his own public and private keys. He chooses p = 23 and q = 19 with e = 283. Find d so that ed has a remainder of 1 when divided by (p − 1)(q − 1).
13. Assume that, A hospital XYZ is planning to replace the tradition systems with blockchain. So, analyze and tell how effective it will be with some advantageous?
14. Explain a real-life use-case where Blockchain is being used.
15. Differentiate between Proof of Work vs Proof of Stake.
16. What is a 51% attack?
17. What do you mean by blocks in Blockchain technology?
18. In a company, they want to replace current system with blockchain. To be part of this network, certain nodes don’t have the more computational requirement and storage capacity. So, how can they take part in blockchain? What is your suggestion?
19. Define the immutable property of the blockchain. How the transactions in a block will be organized?
20. Explain blockchain construction and the structure of a block.
21. What is cryptography? What is its role in Blockchain?
22. What are the different types of Blockchain?
23. What is a Genesis Block?
24. How is the hash (Block signature) generated?
25. What is a smart contract and list some of its applications?
26. Assume the blockchain with SHA256 bits hash function, M is the input message and H(M) is the output message digest. Explain three important properties of this hash function with by considering given input and output.
27. What is the Ethereum network and how many Ethereum networks are you familiar with?
28. What is the very first thing you must specify in a solidity file?
29. What is the difference between Bitcoin and Ethereum?
30. What is the nonce and how is it used in mining?
31. Name the steps that are involved in the Blockchain project implementation.
32. Callie wants to send the message M = 13 to Alice. Using Alice’s public and private keys, calculate the ciphertext C, and the value for Remainder when Alice recovers the message.
33. Dexter wants to set up his own public and private keys. He chooses p = 23 and q = 19 with e = 283. Find d so that e has a remainder of 1 when divided by (p − 1)(q − 1).
34. Write and execute python code to recover the cipher message from the original message for the following problem: Alice wants to send the message M = 20 to Bob. Using Bob’s public and private keys, calculate the ciphertext C, and check for the integrity of the message when Alice recovers it.
35. What happens if the execution of a smart contract costs more than the specified gas?
36. In a blockchain, there exist 10 peers. Among 10 peers Alice and Bob acting as miners. Both collected same set of transactions and mined separate blocks. If both attached their blocks to blockchain, how these two blocks uniquely identified?
37. How to reduce the signature size? Explain the mechanism.
38. Suppose john wants to encrypt email messages before sending them to friends. The RSA Encryption Scheme is often used to encrypt and then decrypt electronic communications. John wants to set up his own public and private keys. He chooses p = 23 and q = 19 with e = 283. Find d so that ed has a remainder of 1 when divided by (p − 1)(q − 1).
39. Alice perform asset transfer from bank A to Bank D, He would like to track his asset transfer path between Bank A to Bank D. His application is using blockchain to perform this. Which blockchain model will help Alice to track his asset transfer.

### **What is the nonce and how is it used in mining?**

1. Write any three difference between Proof of Work and Proof of Elapsed time.
2. Analyze Proof of Stake, Proof of Burn and Proof of capacity and justify which is efficient consensus.
3. Consider there exist blockchain network with 10 number of nodes. This system using RAFT consensus algorithm. While electing leader node, two nodes A and B send Request vote message with term 25 at the same time. So which mechanism will be used to elect leader? Following shows the state of the node logs:
   1. A: 1.1, 2.1
   2. B: 1.1, 3.1, 3.2
   3. B: 1.1, 1.2
   4. D: 1.1
   5. E: 1.1, 3.1
   6. F: 1.1,2.1,3.1

Here 2.1 represents the 6nd log from the 1st term. If the system is searching for a new leader. Then is there any chance of committing the transaction of 2.1 in future?

Among these nodes 4 nodes get failed. How the system will manage this failure?

if your system identifies that the leader is Byzantine, then what will the system do now?

1. In a system, A client sends a request to invoke a service operation to the primary, The primary multicasts the request to the backups, The backups execute the request and send a reply to the client, The client waits for replies from different backups with the same result. N this scenario the system is using which consensus?

* If the primary node is byzantine, how the system will work?
* How it differs from BF?

1. How can you identify a block in blockchain?
2. How is Blockchain distributed ledger different from a traditional ledger?
3. Differentiate between private and public blockchain solutions.
4. What will be ensured through the blockchain implementation in the KYC process?
5. Assume the implementation of blockchain for GST collection and write any three advantageous and one disadvantage.
6. In the blockchain network, Ram wants to transfer 500 bitcoins to shin. How Ram initiates the transaction and sign the transaction? How the transaction will be verified?
7. Suppose john wants to encrypt email messages before receiving from his friends. He started using RSA Encryption Scheme to encrypt and then decrypt electronic communications. John set up his own public and private keys and broadcasted them to his friends. He had message of 50 and chosen p = 7 and q = 11 with e = 7 and d=11. Illustrate e-mail exchange with plain text and cipher text conversion.

### **What is Merkel Tree? What is the need of Markle tree in blockchain? How hash code will be processed?**

### **How the digital signature is created and verified?**

1. Consider there exist blockchain network with 6 number of nodes. This system using RAFT consensus algorithm. While electing leader node, two nodes A and B send Request vote message with term 25 at the same time. So which mechanism will be used to elect leader? Following shows the state of the node logs:

* A: 1.1, 4.1
* B: 1.1, 3.1, 3.2
* B: 1.1, 1.2
* D: 1.1,3.1
* E: 1.1, 4.1
* F: 1.1,2.1,4.1

Here 1.2 represents the 3nd log from the 1st term. If the system is searching for a new leader. Then is there any chance of committing the transaction of 1.2 in future?

* Among these nodes 4 nodes behaving maliciously. How the system will manage this failure?
* if your system identifies that the leader is Byzantine, then what will the system do now?

1. In a system, A client sends a request to invoke a service operation to the primary, The primary multicasts the request to the backups, The backups execute the request and send a reply to the client, The client waits for replies from different backups with the same result. N this scenario the system is using which consensus?
2. If the primary node is byzantine, how the system will work?
3. How it differs from BFT?
4. Considering the Proof of Elapsed Time (PoET) adapted in Hyperledger Sawtooth framework, what mechanism is used to ensure that the miner (or block leader) is a legitimate participant and not an attacker and has waited for the random amount of time assigned by the network?
5. Suppose in a distributed network, running Paxos as the underlying consensus algorithm, has 6 proposers and 10 acceptors and 2 learners. Say, 6 of the acceptors have failed, how the network will work? Explain with reason.
6. Alice wants to develop a secure distributed system where she wants to keep track of the node identity. Additionally, she wants fixed message content representation although any node in the system can transfer the message of any size. You as a system consultant, suggest a consensus protocol to Alice which is extremely suitable for her system and Justify the reason. Suppose if they want to change the consensus to RAFT protocol and your system identifies that the leader is Byzantine. What will the system do now?
7. In a PAXOS consensus mechanism, how a new value will be proposed and accepted in the blockchain network? Explain each step.
8. Explain the practical byzantine fault tolerant model with three lieutenants, one commander and one client scenario.
9. List and explain any four important components of blockchain solution for any real time applications.