Question Bank – Blockchain Technology (CO4118T)

Sample Short Questions:

1. Define Transaction, Block and Blockchain.
2. List Blockchain design properties and give their technical implications.
3. Define Consensus, Immutability and Proof.
4. With respect to Blockchain, define following properties: Integrity, Authenticity, Availability, Confidentiality, Anonymity
5. Differentiate Symmetric Key and Asymmetric Key Cryptography.
6. Explain - how ECDSA is used in Bitcoin?
7. What are the key differences between database and blockchain?
8. Explain Byzentine General Problem and how it is resolved?
9. Explain key properties of currency: Fungibility, Durability, Portability, Cognizability
10. Explain Merkle Tree and its use in Blockchain
11. Explain Bitcoin block verification.
12. Explain significance of Synchronization problem in Distributed Consensus.
13. What is double spending? How will you solve it?
14. Define Miner and types of Fork
15. Explain - how Wallet address is derived? Also discuss generation of private and public key.
16. Write a short note on Smart contract.
17. Explain Etherum Virtual Machine and how changes are made in it?
18. Explain structs and arrays in Solidity. How they are created?
19. How identity management can be done using Blockchain?
20. Explain location based addressing and content based addressing in IPFS.
21. What are the corrective measures to store or process sensitive data on Blockchain?
22. Differentiate Proof of Work (PoW) v/s Proof of Stake (PoS).
23. Explain Zero Knowledge Proof and its use in Blockchain.
24. Explain Supply Chain Management use case of Blockchain.
25. Explain Energy Management use case of Blockchain.
26. List 5 smart contract use cases.
27. List different blockchains and their consensus mechanisms
28. In solidity programming, explain purpose of Mapper function
29. How smart contract communicates about event to front-end?
30. Write a note on function modifier
31. List four problems that Blockchain cannot solve
32. Discuss any three attacks on the Blockchain
33. Post-test questionnaire

Sample Design Questions

1. Explain Hyperledger Fabric Architecture and Workflow with suitable diagram.
2. Explain VJTI Blockchain with UML diagrams and Architectural insights.
3. How bitcoin is used in money laundering? Explain gaps in existing anti-money-laundering (AML) system for cryptocurrency.

4. What is Reconciliation problem? What are the issues of centralized database for this problem? How Corda solves it?
5. Explain Bitcoin UTXO model and Ethereum account balance model. Highlight differences between them.
6. Explain problems with http and how does IPFS solves them?
7. Design Student Result Record Verification system as dApp (give Solidity code).
8. Provide analysis of Bitcoin Backbone Protocol.
9. What is Lamport Clock? How does it apply to Blockchain?
10. Design a coin with the following properties and provide structure along with function signature:
    a. I should be able to generate
    b. Anyone should be able to verify
    c. Onwer should be able to spend
11. List and explain 4 potential use cases of Blockchain

Sample Long questions

1. Why is Corda said to be a Distributed Ledger and not a Blockchain? How does Corda platform provide privacy of information across parties in the network? What are the two types of consensus that the peers use in the Corda Ecosystem? Draw the architecture of a typical Corda Node.

2. Explain working of Bitcoin Blockchain. How mining is done and how the difficulty level is set?

3. Describe the approach taken by you to solve assignment#2. Mention and justify the logic, pseudo code/algorithm, and the complete working of program.

4. You are a part of the bitcoin foundation. Due to the increasing size of the bitcoin blockchain you want to start anew, this time with less memory.
   Design a way to stop and restart the bitcoin blockchain using less memory. Assume all nodes will agree to doing this.
   Your solution must have the following 2 properties.
   a. All the coins in circulation must still belong to the original wallets.
   b. After restart, your blockchain must consume less memory than before.

   Your design must describe how the data will be stored when the blockchain is offline, what processing will be done on the data, and what changes need to be made, if any, when the blockchain comes back online. Assume all nodes will restart together with the new version of software you release.

   You can provide pseudocode to explain your idea if you wish. Based on your solution answer the following questions:
   i. What if some nodes refuse to participate when the blockchain is restarted? Is a solution possible in this case? If yes, how will their state be updated assuming they are running when everyone else is shutdown?
   ii. If after the restart the blockchain consumes less memory, is it still possible to track the utxo back to its original block where it was mined? If yes, describe how this will work in your solution.

iii. Is there a way to ensure all pending unmined transactions are not lost when the blockchain restarts?

5. A paper wallet is the name given to an obsolete and unsafe method of storing bitcoin which was popular between 2011 and 2016.
   It works by having a single private key and bitcoin address, being printed out onto paper.
   For the bitcoin blockchain any 256-bit number from 0x1 to 0xFFFF FFFF FFFF FFFF FFFF FFFF FFFF FFFE BAAE DCE6 AF48 A03B BFD2 5E8C D036 4140 is a valid private key.
   Assume you have found the paper wallet of Satoshi Nakamoto. However some of the paper is torn, specifically the last 72 bits are missing.
   Satoshi's wallet is known to have around 600000 btc, with a value of $4 billion.
   Design an algorithm to find Satoshi's private key. Assume you know his public key.
   i. Can you do better than brute force?
   ii. Will your algorithm finish execution before your grandchildren die? How much computation will you need to do this in your lifetime?
   iii. If you get access to his wallet, how will you transfer money from his wallet to yours without raising suspicion?

6. Consider the "proof of burn consensus algorithm": The idea is that miners should show proof that they burned some coins - that is, sent them to a verifiably unspendable address. This is expensive from their individual point of view, just like proof of work; but it consumes no resources other than the burned underlying asset.

   To date, all proof of burn cryptocurrencies work by burning proof-of-work-mined cryptocurrencies, so the ultimate source of scarcity remains the proof-of-work-mined "fuel".
   Answer the following questions:
   i. A miner should not be able to burn some coins immediately and claim transaction fees. There must be a block delay of around 8 to 10 blocks when the coins were burnt. Why is this so?
   ii. On average, to maintain economic stability how much bitcoin should a miner burn. Give your answer in terms of transaction fees and real hardware resource costs. Is this cost greater than simply mining a block?
   iii. Can a blockchain be created using only proof of burn, without using any other consensus?

7. Design and describe an alert system which would allow all nodes to receive an alert notification