1. Explain briefly how digital signatures work.
2. Assume that Alice wants to send a message to Bob and she wants to ensure that the message cannot be altered during transmission. How can Alice use digital signatures to achieve this goal?
3. Explain the concept of proof of work and how it is used in Bitcoin mining.
4. Assume that the Bitcoin network undergoes a hard fork, and that two separate chains are created. Explain how this affects the network, and how miners and other nodes can decide which chain to follow.
5. Explain how hash functions are used in blockchain technology to ensure the integrity of the ledger.
6. In a bitcoin transaction, the hash of the transaction is signed. Explain the concept of hash function collision, and how it can affect the security of a digital signature.
7. A modified Base 58 binary-to-text encoding known as Base58Check is used for encoding Bitcoin addresses instead of the standard base64. Why is that?
8. Assume that a miner wants to add a new block to the blockchain. Explain the steps that the miner needs to follow to create a valid block, and how the miner can earn a block reward.
9. Assume that you have a large set of data items that you want to verify for integrity. Explain how you can use a Merkle tree to efficiently verify the integrity of a specific data item.
10. Assume we already know exactly which subset of nodes are corrupt. Describe a 1-round protocol that achieves Byzantine Broadcast.
11. Explain what is a PKI, and why Dolev-Strong Byzantine Broadcast requires it to work.
12. Why would someone use Phase-King Byzantine Broadcast instead of Dolev-Strong protcol?
13. Why would someone use Dolev-Strong protcol instead of Phase-King Byzantine Broadcast.

Colab paid products - Cancel contracts here