A Brief Review of IS6200

1 Money

a. What are the three functions of money?
b. How do you rate cryptocurrencies (i.e., digital currencies issued in a blockchain network) as money?

2 Cryptographic Techniques

2.1 Encryption:

a. What are symmetric and asymmetric encryptions?
b. How are these two different from each other?

2.2 Hash functions

a. What is the definition of a hash function?
b. For a hash function to be a cryptographic hash function, what are the expected properties?
c. What are the distinctions between encryption and hash functions? Or, can we use these two interchangeably?

2.3 Digital signatures

a. What is its usage/application?
b. Is it better than wet-ink signatures? Why or why not?
c. How is it used in Bitcoin?

3 Bitcoin

3.1 Using one sentence, define the Bitcoin network. Note that "Bitcoin" is used to refer to the blockchain network, while "bitcoin" refers to the cryptocurrency on the network.

3.2 Why is Bitcoin so energy intensive?

3.3 If it costs so much to help maintain the network, why are there still so many miners?

3.4 What is 51% attack in Bitcoin?

3.5 The number of miners has been growing exponentially. How can Bitcoin maintain a 10-min average block time?

3.6 Is Bitcoin ready to handle global transactions? Why or why not?

3.7 People have come up with scaling solutions. They often use layer 1 and layer 2 to distinguish the different types of such solutions. What are these two types?

3.8 There have been heated discussions on SegWit, Taproot, and the lightning network. What are them?

3.9 What is "ordinals"? How does it change the Bitcoin ecosystem?

4 Ethereum

4.1 It is just another public blockchain network. What makes it special, given that we already have Bitcoin?

4.2 What is Gas in Ethereum? Why is it needed? (What is the halting problem?)

4.3 What happened in the 2016 DAO hack? What was the bug? What did the developers do to fix the bug?

4.4 Ethereum shifted from PoW to PoS. What is PoS (in Ethereum)? Is it better than PoW?

4.5 What does it mean by "nothing at stake" in a PoS blockchain network like Ethereum?

4.6 In addition to 51% attack, it seems like one with 34% stake might launch attacks as well. How may these attacks happen and how could we counteract such attacks?

4.7 Is the shift from PoW to PoS a layer 1 or layer 2 scaling solution?

4.8 What is "optimistic rollup"? How many honest nodes do we need to ensure that the batched transactions are valid?

5 Decentralized Autonomous Organization

5.1 What is the principal–agent problem? What are the agency costs?

5.2 How do DAOs mitigate this agency conflict?

5.3 Do DAOs introduce new agency costs? If so, what are such costs?

5.4 Voting is important in DAO governance. What are the common voting approaches?

6 Hyperledger Fabric

6.1 How does frameworks like Fabric facilitate the adoption of blockchain into businesses?

6.2 What is a channel in a Fabric network?

6.3 In Fabric, certificate authority is needed for identity management. Why is it important? Recall what's man-in-the-middle attack?

6.4 How does Raft ordering service work? At most how many failed node can it withstand?

6.5 Can Raft solve the Byzantine Generals Problem?

7 Cryptotokens

7.1 We can categories the tokens issued through blockchain networks into different types. What are they?

7.2 How does Zcash differ from Bitcoin? What's the novel technology that makes it unique?

7.3 What are stablecoins? What are the different types? What's its benefit (recall the examples?)

7.4 What are NFTs? How are they special? A couple of innovations based on ERC -1155 and ERC 4907 were implemented to improve NFTs. Describe these innovations.

7.5 Metaverse: the role of blockchain – data continuity; transaction.