A Brief Review of IS6200

# Money

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

# Cryptographic Techniques

## Encryption:

## What are symmetric and asymmetric encryptions?

1. How are these two different from each other?

## Hash functions

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

## Digital signatures

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

# Bitcoin

## 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.

## Why is Bitcoin so energy intensive?

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

## What is 51% attack in Bitcoin?

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

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

## 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?

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

## What is “ordinals”? How does it change the Bitcoin ecosystem?

# Ethereum

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

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

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

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

## What does it mean by “nothing at stake” in a PoS blockchain network like Ethereum?

## 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?

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

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

# Decentralized Autonomous Organization

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

## How do DAOs mitigate this agency conflict?

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

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

# Hyperledger Fabric

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

## What is a channel in a Fabric network?

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

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

## Can Raft solve the Byzantine Generals Problem?

# Cryptotokens

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

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

## What are stablecoins? What are the different types? What’s its benefit (recall the examples?)

## 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.

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