2. The talk introduced the "replication" problem, which can be solved by consistency and fault tolerance among serves. The talk also talked about some models used in this problem and their protocols. These models include bitcoins, PBFT and Paxos. My favorite topic is the bitcoin and block chain, because I have heard these terms a lot, but never actually learned them. Now, I was able to understand them and also the motivation behind. I think the talk is very interesting. Even though the topics does not align much with what we learned, I was able to understand most part of the talk.

3. PBFT model is in partial synchrony, so there could be a message delay upper bound. It can tolerate $\frac{1}{3}$ faults, so the number of servers is $n = 3f + 1$ where f is the maximum number of faulty servers. All messages are encrypted using public key encryption and digitally signed.
In PBFT, one leader server propose a value v, and the replica servers vote. Upon receiving $n-f$ votes, vote again. Upon receiving second round $n-f$ votes, commit value v.

4 The hash function takes two inputs: the puzzle and the nonce and produce a value. The correct nonce will give an output below some threshold. The correct nonce is called proof-of-work
This the same as the random oracle model, so the probability of finding a POW is $O(\frac{q^2}{q^{l_{out}}})$ where q is number of queries, l_{out} is the length of output. The probability is negligible.