Homework1

Read Bitcoin whitepaper (https://bitcoin.org/bitcoin.pdf) and answer the following questions. A comprehensive answer to each question would be around ~50 words. You may want to search additional materials on web for answering these questions.

Section 4 argues that the longest chain rule represents the majority vote of the transaction history. This argument relies on the assumption that block propagation is fast enough, so that blocks generated by honest participants will form a chain. What would happen if this assumption is violated?

Can you think of any other assumption the above claim relies on? Write down these assumptions and discuss them.

What would happen if Bitcoin removes the Proof-of-Work puzzle from block generation? Imagine a hypothetical system in which all transactions form a chain directly instead of being packed into blocks first. Anyone who wants to submit a transaction can append to the end of the transaction chain without PoW. In this hypothetical system, the longest transaction chain is considered the correct transaction history. What could go wrong for the system?

Section 5 mentions that each transaction and each block are broadcasted to everyone else in the network. How is this actually implemented in Bitcoin? You may want to search additional materials on the web to answer this question.

Based on the discussion in Section 11, how many blocks does the recipient of a transaction need to wait if 1) he or she assumes that the attacker controls up to 20% of computation powers and 2) he or she can only tolerate 0.1% of double-spending risk? How many blocks to wait, if the attacker controls 30% of power and he or she can only tolerate 0.01% of double-spending risk?