Student: Fengning (Fred) Luo 1004687029 freddy.luo@mail.utoronto.ca

Question 1:

If block propagation is slow, attackers might outpace honest nodes in creating blocks, leading to forks in the blockchain. On the other hand, it could lead to network centralization by giving miners with faster access to block information a competitive advantage. Both can harm and disadvantage individual miners.

Question 2:

One major assumption is that the majority of Computational Power (>50%) is controlled by honest nodes. This is the fundamental assumption that ensures the longest blockchain is the one that reflects the true and correct record of transactions. Without it, the attacker can create a chain that is longer enough that other nodes will begin to work off this invalid chain as the legitimate one.

Question 3:

Without the proof-of-work puzzle, it will no longer be computationally impractical to perform malicious actions. On the other hand, the individual or group nodes that can most quickly spam transactions will dominate the ecosystem, and will likely lead to centralization, defeating the purpose of Bitcoin.

Question 4:

This broadcast process is likely implemented through a peer-to-peer (P2P) network model. Within the network, each node has a list of other nodes that they are connected to. When a new transaction or block is created, this information is quickly propagated throughout the network without the need for a central server or authority organization.

Question 5:

If the attacker controls up to 20% of computation power, with 0.1% tolerance, this person needs to wait for 11 blocks.

If the attacker controls up to 30% of computation power, with 0.01% tolerance, this person needs to wait for 32 blocks.