

Problem 1:

Two suggested protocols to increase transaction rate to 70/second are:

1. Increase size of block from 1MB to 10MB.
2. Decrease the block interval time to 1 min.

Issues with increasing block size: This would require a lot more storage, and would make the full nodes more expensive to operate. And eventually fully operating nodes will decrease, and the system will become more centralized. There might be more double spending attacks due to slower propagation speeds. Achieving consensus would be difficult since validating a block would require lot more efforts.

Issues with decreasing block interval time: Propagation of the block in the network, takes some time. If we reduce the block interval time, block might not be propagated fully in the network till that time. We might not be able to achieve consensus in due time. Block propagation and latency would also lead to more orphan nodes, since they might be delayed in propagating. It would also have an environmental effect, since power would be used more since block rate is high.

Question 1

Question 2

He is wrong. We can have a double spending attack if there are 51

Question 3

Question 4

Question 5

Question 6

Question 7

Question 8