Practice Problems on Streamlet

June-2-2022

1. In the safety argument for Streamlet, we considered a scenario that 3 blocks B_5, B_6, B_7 in epochs $5, 6, 7$ respectively are notarized and hence blocks B_5 and B_6 are confirmed. We argue that if the number of adversary nodes $f < n/3$, then there cannot be another block from epoch $4, 5, 6$ or 7 notarized at the same height as B_6. Here we will complete the safety argument by showing that there cannot be any block from any epoch that is notarized at the same height as B_6.

   a) Argue that there cannot be any block from any epoch less than 4 notarized at the same height as B_6.

   b) Argue that there cannot be any block from any epoch greater than 7 notarized at the same height as B_6.

2. In Streamlet, the quorum size for notarization is chosen to be $2n/3$, where n is the number of nodes. With that quorum size, we showed that the protocol can tolerate up to $n/3$ adversary nodes. In this question, we explore whether the quorum size can be optimized to increase the resilience of the protocol, i.e., the number of adversary nodes it can tolerate.

   a) Suppose we set the quorum size to be q. Let t be the number of adversary nodes. What condition must q and t satisfy for Streamlet to be safe? Explain.

   b) What condition must q and t satisfy for Streamlet to be live? Explain.

   c) Using the constraints in parts (a) and (b), optimize q to maximize the resilience of Streamlet. What is the resulting resilience?