Advanced Distributed Algorithms and Data Structures SS 2019 Homework Assignment 7

Problem 1:

Prove Lemma 5.12 on slide 66 of the updated Chapter 5.

Hint: Suppose that v is the process that currently has the smallest round counter t(v). How many processes w would contact it in round t(v) + 1 (and therefore would get stuck)? How many processes w' would contact any of these processes in round t(v) + 2 (and therefore would get stuck as well)? Continue with this argument. Compute expected values and, if possible, also values that hold w.h.p. by making use of the Chernoff bounds.

Problem 2:

Implement the extended median algorithm in the NetSimLan environment and test it with bit sequences that are continuously extended by the processes. (You may ignore the issue of appending missing keys at the end of the median sequence.)

Problem 3:

Are there any adversarial attacks on blockchains that come to your mind and which haven't been addressed in the slides? Do you have an idea of how to counter these?