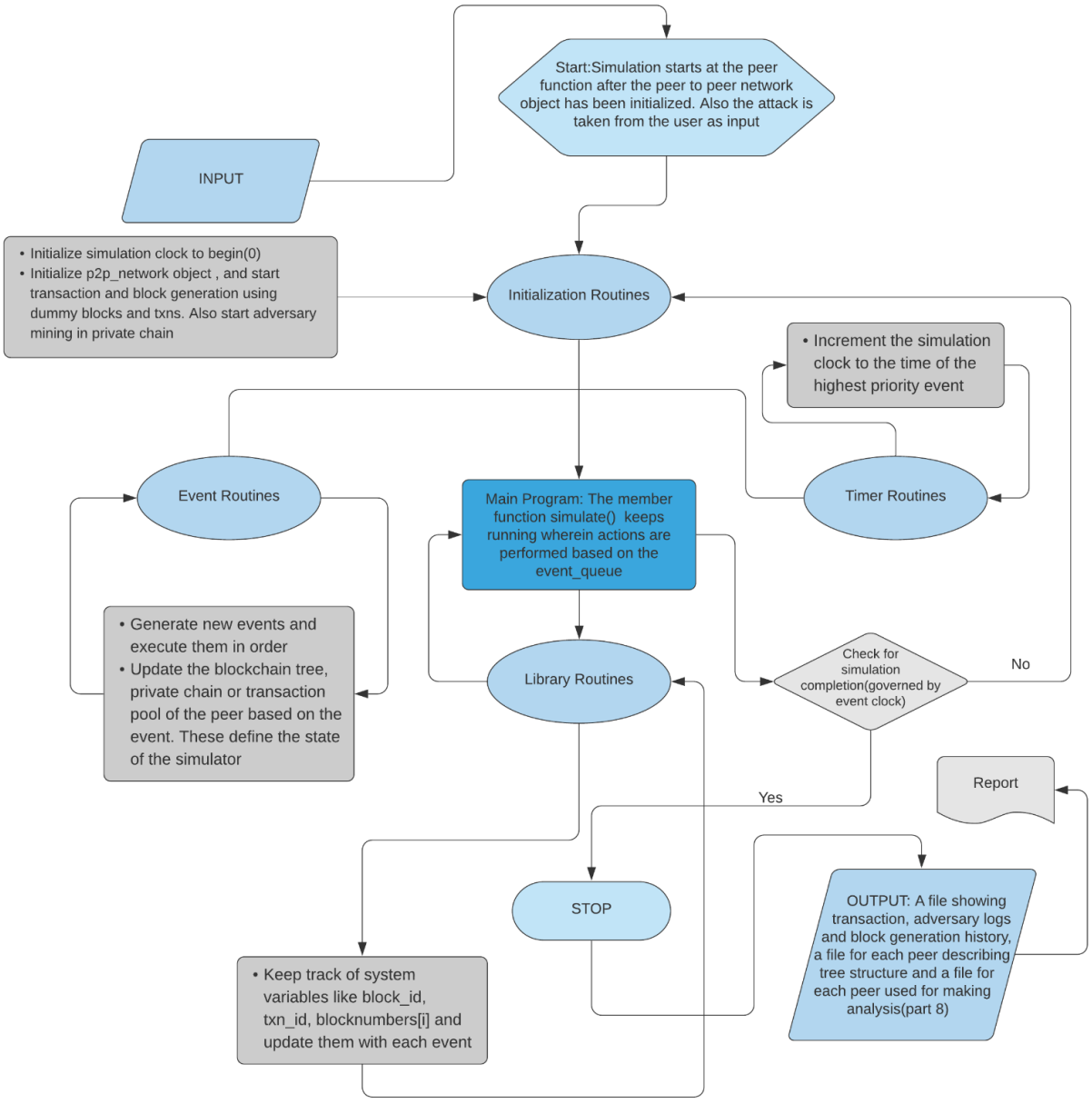
DESIGN DOCUMENT

180050054
180050025
180050020

Modular flow of code



SUMMARY OF BOTH THE ATTACKS

In the below diagram the lead of the attacker is the number of blocks by which he is ahead of the honest chain before receiving an honest block. The code can be found in recieve_block event
E.g if lead = 1, it means that before receiving and validating an honest block the adversary was one block ahead. If this block turns out to be valid then both chains would be equal in length and we'd be in state 0'.