**Problem 1**

In this problem, we will consider the Streamlet protocol run by $n$ permissioned nodes, with a tunable quorum size $q$ for notarization.

1. Suppose we want to maximize the resilience of the protocol, i.e., maximize the number of adversarial nodes $f$ that can be tolerated such that the protocol is both safe and live. Derive the optimal quorum size $q$ and show that the resulting optimal resilience is $f = n/3$.

2. Suppose you believe that an attack against safety is more likely than an attack against liveness (since a double-spend can provide significant rewards to the attacker). Hence, you want to tune Streamlet to increase the resilience against safety attacks, even at the expense of decreasing the resilience against a liveness attack. Can this be done? If so, exhibit and plot the tradeoff between the two resilience. If not, explain why not.

**Problem 2**

A consensus protocol is said to be $t$-safe if whenever the number of adversary parties is less than $t$, the protocol is safe. A consensus protocol is said to be $t$-accountable-safe if whenever safety is violated, at least $t$ parties can be irrefutably proven to have violated the protocol.


2. In Lecture 18, we claimed that Streamlet (with quorum size $2n/3$) is $n/3$-accountable, where $n$ is the total number of parties. But we have only gone through one possible safety violation scenario, not all. Complete the analysis by considering all safety violation scenarios.

**Problem 3**

Does the safety of the Streamlet protocol depends on the $\Delta$-synchrony assumption? Explain.

**Problem 4**

Suppose all $n$ parties running the Streamlet protocols are honest. Compute the average confirmation latency in terms of protocol parameters. Contrast this with the confirmation latency of the PoS longest chain protocol.