Quiz 1

- PBFT: compute the quorum sizes necessary in the system of $n=3f+2c+1 > 3f+1$ processes, where up to f can be Byzantine
- If we add a fast phase: what is the minimal fast quorum size?
- What is the minimal recovery quorum size: the minimal number of processes the new primary should contact to recover all previously committed values?

Quiz 2

- The Byzantine generals setting assumes a synchronous system
- BFT assumes asynchronous system and digital signatures
- Both protocol assume >2/3 correct servers

Can you devise a synchronous state machine replication protocol with signatures that tolerates any number of faulty servers?

Quiz 3

- What are the liveness guarantees of PBFT?
  - Under which conditions a client's operation is committed and executed?
- What are the liveness guarantees of Hyperledger Fabric?
  - Is it possible that a correct client does not make progess (even in the synchronous fault-free case)?