7610 Distributed Systems **Spring 2018**

HOMEWORK 3
DUE Thursday Nov. 15 2018, 10:00pm EST

1 Submission

Papers you need to read to answer this homework:

- Paxos for System Builders, Jonathan Kirsch and Yair Amir, http://www.cnds.jhu.edu/pub/papers/cnds-2008-2.pdf
- In Search of an Understandable Consensus Algorithm (Extended Version), Diego Ongaro and John Ousterhout, https://raft.github.io/raft.pdf
- Bitcoin: A Peer-to-Peer Electronic Cash System Satoshi Nakamoto, https://bitcoin.org/bitcoin.pdf.

2 Description

Problem 1 (50 points) Consider the Technical Report "Paxos for Systems Builders". Consider the setup where the algorithm is ran by 5 servers named a, b, c, d, e, with ids 1, 2, 3, 4, 5.

Part 1 (25 points): Consider that the current view has view_id 1 and the leader, server a, crashed. Server b detects the failure and initiates the view change by sending a $VIEW\_CHANGE$ message to the other servers. Describe how the algorithm proceeds from this point till all servers install the new view. Note: no other server detects the failure of the leader and no other server crashes. Describe all the information from the messages by following the format from the technical report.

Part 2 (25 points): Same setup as before, but after the leader a crashes, two servers, b and c detect the crash and send $VIEW\_CHANGES$ messages. Describe all the steps of the algorithm till all servers install the new view. As before describe all the details of the messages, following the format from the technical report.

Problem 2 RAFT, PAXOS (20 points) Consider the RAFT algorithm as described in class and in the paper "In Search of an Understandable Consensus Algorithm (Extended Version)". Why do entry logs in the RAFT

algorithms are identified only by entry id and they do not need a view id like in Paxos?

Problem 3 Blockchains (30 points) Consider the Bitcoin system as described in class and in "Bitcoin: A Peer-to-Peer Electronic Cash System" https://bitcoin.org/bitcoin.pdf.

- What is the proof of work component of Bitcoin and what is its role?
- When can a transaction be considered committed and why?
- What is the incentive system used by Bitcoin and why it is needed?

3 Submission

Information about submission is in post @11 in piaza. Name of the project in the submission command is hw3. Submission is in *PDF* format. Please do not submit by email.