# CMPT 431: Distributed Systems

## Assignment 5, Spring 2019

This assignment is to be done in groups of 2!

In this assignment we become familiar with blockchain and with distributed consensus protocols.

References

- **Sawtooth**
  - Introduction
  - App Developer Guide
  - Event Subscription
  - Sawtooth's default consensus algorithm
- **Raft**
  - Introduction
  - Hyperledger Sawtooth Raft Documentation
  - Useful video
- **Byzantine fault**

**Q1. Blockchain (65 marks)**

Use Hyperledger Sawtooth to implement a smart contract for a notary in which users can record property sale agreements. A sale agreement consists of the following fields:

A. Buyer name: e.g John Doe
B. Seller Name e.g Jim Carrey
C. House ID: 123 Main Dr., Vancouver, BC, Canada, A1B 2C3

You don't need to model any notion of currency. Simply assume that sale agreements are documents which will be recorded on the blockchain. Use the Sawtooth SDK (in the programming language of your choice) to create a smart contract and run it on a Sawtooth network. Then, create an event for the sale agreement and use ZeroMQ to subscribe to the sale agreement events.

Submit your application code and screenshots.

**Q2. Consensus Protocol (15 marks)**

Replace the default consensus algorithm of Hyperledger Sawtooth with Raft. Raft is equivalent to the Paxos algorithm for distributed consensus but is easier to understand and implement. Run your application with the new consensus protocol.

Submit all the configuration files and Screenshots

**Q3.**

A. **(8 marks)** Compare the pros and cons of using Blockchain vs a centralized database server for Q1.
B. **(12 marks)** Is Sawtooth's default consensus algorithm able to reach consensus in the case of Byzantine fault? What about Raft? Explain each separately.