

For Graduate Students

In addition to the 4010 class syllabus the following is required for graduate students:

Date	Topics
Wed Jan 29, 2021	Reading Papers
Fri Jan 31, 2021	Individual times to meet with graduate students on papers/concepts.
	Plan on getting tougher with me for 3 hours across the semester.
	We will do this on a per-person basis.
Fri May 01, 2021	Paper due.

Please read all of the following:

Honey Badger Byzantine Fault Tolerance

<https://eprint.iacr.org/2016/199.pdf>

zk-SNARK

<https://blog.goodaudience.com/understanding-zero-knowledge-proofs-through-simple-examples-df673f796d99>

Byzantine Fault Tolerance

<https://lamport.azurewebsites.net/pubs/lamport-paxos.pdf>

https://www.usenix.org/legacy/events/osdi99/full_papers/castro/castro_html/castro.html

<https://bitcoin.org/bitcoin.pdf>

The zero-knowledge (zk-SNARK) is a user level for understanding - the math is deep and I don't know of a good paper to read that will give a understanding of the math in it.

Consider z-Cash and Ripple. Ripple is using a Honey Badger based consensus system. z-Cash is using zero-knowledge proofs. Both of these are 3rd generation systems.

There are a number of projects around the state government and UW that are Blockchain related.

1. Environmental Credits

2. Co2 Sequestration Credits
3. Supply Chain Tracking (SheepChain)
4. Document Tracking
5. Registration of Companies

Pick one of these and write an outline of how it can be implemented on a Blockchain.