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

Date	No	Topics
Wed Jan 29, 2020	02	Reading Papers
Fri Jan 31, 2020	03	Individual times to meat 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, 2020	39	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 Tollerance

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.

Write up a 1 to 2 page informal proposal paper on how you would make blockchain faster and more secure. Would you combine these?