Announcement

- Final Exam on Monday, May 8 at 9-11am -- cumulative test that covers all lectures (through April 25), recitation labs, homework assignments, and assigned reading

Please submit your course evaluation at https://bu.campuslabs.com/courseeval/

Review questions:

1. How is Lightning Network different from Bitcoin's traditional transaction model?
2. What are the benefits of using Lightning Network for Bitcoin transactions?
3. What is common randomness generation, and why is it important for distributed systems?
4. What are some of the drawbacks associated with using the commit and reveal paradigm for generating common randomness in distributed systems?
5. What is verifiable secret sharing?
6. Using zero-knoweldge proofs, describe how you can build verifiable secret sharing.
7. Using verifiable secret sharing describe a protocol for computing common randomness.
8. How to build a t-out-of-n secret sharing scheme from an n-out-of-n secret sharing scheme?
9. What are the advangtages of using shamir secret over replicated secret sharing?
10. What is a smart contract, and how is it implemented on the Ethereum network?
11. What is gas in the context of Ethereum, and why is it important for transaction processing?
12. What are some of the scaling solutions being developed for Ethereum, and how do they work?
13. What is a verifiable random function (VRF)?
14. Describle how you can you can solve the common randomness problem using a VRF?
15. What is an oracle, and how does it relate to blockchain technology?