R 47 Distributed Ledger Technologies: Foundations and Applications

Wednesdays, 11:00 – 13:00 PM, in person in Room FW26. First class is on Oct. 13, 2021

Instructor: S. Keshav; sk818
https://svr-sk818-web.cl.cam.ac.uk/keshav/wiki/index.php/Main_Page

Principal lecturer: Prof. Srinivasan Keshav
Taken by: MPhil ACS, Part III
Course Code: R47
Hours: 16 (One two-hour introductory lecture followed by seven two-hour sessions with student presentations and discussion)
Class limit: 21 students

1. Aims

This reading group course examines foundations and current research into distributed ledger (blockchain) technologies and their applications. Students will read, review, and present research papers in this area. Once completed, students should be able to integrate blockchain technologies into their own research and gain familiarity with a range of research skills.

2. Prerequisites

Students are expected to be familiar with the material in typical undergraduate distributed systems courses, i.e., basic concepts of computer networking and operating systems, distributed systems, concurrency, cryptography, security, and performance analysis. Specific University of Cambridge courses are:

Computer Networking
Concurrent and Distributed Systems
Operating Systems

3. Topics

1. Introduction to DLTs
2. Bitcoin
3. Ethereum and smart contracts
4. Other DLTs: Algorand and Hyperledger Fabric
5. Crash- and Byzantine-fault tolerant consensus protocols
6. Applications

We will cover 14 Major and 14 Minor papers in this course; the full list of papers and the schedule of discussion is in the Appendix. The papers themselves are available from the course Moodle.

4. **Learning objectives**

There are two broad objectives: to acquire familiarity with a body of work in the area of distributed ledgers and to learn some specific research skills:

1. How to read a paper
2. How to review a paper
3. How to analyze a paper's strengths and weaknesses
4. Written and oral presentation skills

5. Assessment

All participants are expected to attend and participate in every class; the instructor must be notified of any absences in advance.

You are expected to carefully read and critique the 14 assigned Major papers and review seven of them (either one of the two Major papers for each week). Reading the Minor papers is encouraged but optional. Reviews must either follow the review form linked here: [PDF] [Latex source] or may be a PDF copy of your presentation slide deck for those papers you are asked to present (in this case, you will be marked 10% for the content of the slide deck which represents your review and 5% for the presentation).

Each review is worth 10% of your total mark. Marks will be awarded and penalties for late submission applied according to ACS Assessment Guidelines. Please submit your review (max 1200 words) using the Moodle.

You will give **two** presentations that should critically introduce one Major and its associated Minor paper in a 20-minute conference-style presentation (15 minutes for the Major paper and 5 minutes for the Minor paper). Each presentation will be followed by a guided discussion in class. Slides should be used for presentation. 10% of the course mark are for the two presentations (5% each). Students will be assigned to presentation papers at random.

20% of the grade will be for a summative essay that explores one aspect of blockchain technology in detail (max 2500 words). Potential topics for essays include:

1. Design NFT art and put it up for sale. Write an essay on your experience.
2. Critique a blockchain such as Cardano, Tezos, or Avalanche.
3. Survey recent work on fast and scalable consensus algorithms.
4. Identify an innovative application where the use of blockchains is justified.
5. Create a wallet to buy a small amount of cryptocurrency and then sell it. Write an essay on your experience.

6. Diversity

We recognize the value of the diversity in identities, perspectives, and contributions that students bring, and the benefit it has on our educational environment. Your suggestions are encouraged and appreciated. Please let us know ways to improve the effectiveness of the course for you personally or for other students or student groups.

Appendix

These papers can be found on the Moodle. Additional articles can be found here: https://a16z.com/2018/02/10/crypto-readings-resources/

Note: Minor papers are indented, Major papers are not.

Week 1 October 13 Introduction

The first class will be an introduction to blockchains based on the tutorial on "Fundamentals of Blockchains" by Maiyya, Zakhary, Agrawal, and El Abbadi, UC Santa Barbara.

Supplementary reading:

- Clark, Jeremy "Preface" in Bitcoin and cryptocurrency technologies: a comprehensive introduction. Princeton University Press, 2016.
- Narayanan, Arvind, et al., Introduction to Cryptography & Cryptocurrencies, Chapter 1 in Bitcoin and cryptocurrency technologies: A Comprehensive Introduction, ibid.

Week 2 October 20 Bitcoin

Narayanan, Arvind, et al., How Bitcoin Achieves Decentralization, Chapter 2 in *Bitcoin and cryptocurrency technologies: a comprehensive introduction,* ibid.

> Narayanan, Arvind, et al., "Mechanics of Bitcoin," Chapter 3 in *Bitcoin and cryptocurrency technologies: a comprehensive introduction,* ibid.

Nakamoto, Satoshi. "Bitcoin: A peer-to-peer electronic cash system." (2008).

> Narayanan, Arvind, et al. "Bitcoin as a platform," Chapter 9 in *Bitcoin and cryptocurrency technologies: a comprehensive introduction,* ibid.

Week 3 October 27 Ethereum and smart contracts

Buterin, Vitalik, "Ethereum: A next-generation smart contract and decentralized application platform," Online 2014. Also see the online documents here.

> Wood, Gavin. "Ethereum: A secure decentralised generalised transaction ledger." Ethereum project yellow paper Petersberg Version, Accessed, 2020-12-28. (Skip the appendix, starting page 17).

Luu, Loi, et al. "Making smart contracts smarter." *Proceedings of the 2016 ACM SIGSAC conference on computer and communications security*. 2016.

> Szabo, Nick, "Formalizing and securing relationships on public networks," *First Monday*, https://firstmonday.org/ojs/index.php/fm/article/view/548 (online only).

Week 4 November 3 Other blockchains

Gilad, Yossi, et al. "Algorand: Scaling byzantine agreements for cryptocurrencies." *Proceedings of the 26th Symposium on Operating Systems Principles*. ACM, 2017.

Chen, Jing, and Silvio Micali. "Algorand: A secure and efficient distributed ledger." *Theoretical Computer Science* 777 (2019): 155-183.

Androulaki, Elli, et al. "Hyperledger fabric: a distributed operating system for permissioned blockchains." *Proceedings of the Thirteenth EuroSys Conference*. ACM, 2018.

Gorenflo, Christian, et al. "Fastfabric: Scaling hyperledger fabric to 20,000 transactions per second." *2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*. IEEE, 2019.

Week 5 November 10 Crash fault-tolerant consensus

Lampson, Butler W. "How to build a highly available system using consensus." *International Workshop on Distributed Algorithms*. Springer, Berlin, Heidelberg, 1996.

Van Renesse, Robbert, and Deniz Altinbuken. "Paxos made moderately complex." *ACM Computing Surveys (CSUR)* 47.3 (2015): 42.

Ongaro, Diego, and John K. Ousterhout. "In search of an understandable consensus algorithm." *USENIX Annual Technical Conference*. 2014. Also see Howard, Heidi, et al. "Raft refloated: do we have consensus?." *ACM SIGOPS Operating Systems Review* 49.1 (2015): 12-21.

Hunt, Patrick, et al. "ZooKeeper: Wait-free Coordination for Internet-scale Systems." *USENIX annual technical conference*. Vol. 8. No. 9. 2010.

Week 6 November 17 Byzantine fault tolerant consensus

Castro, Miguel, and Barbara Liskov. "Practical Byzantine fault tolerance and proactive recovery." *ACM Transactions on Computer Systems (TOCS)* 20.4 (2002): 398-461.

Van Renesse, Robbert, Chi Ho, and Nicolas Schiper. "Byzantine chain replication." *Proc. PODS*, 2012.

Yin, Maofan, et al. "Hotstuff: Bft consensus with linearity and responsiveness." *Proceedings of the 2019 ACM Symposium on Principles of Distributed Computing*. 2019.

Gueta, Guy Golan, et al. "SBFT: a scalable and decentralized trust infrastructure." *2019 49th Annual IEEE/IFIP international conference on dependable systems and networks (DSN)*. IEEE, 2019.

Week 7 November 24 Scalable consensus protocols/Applications 1

Rizvi, Sajjad, Bernard Wong, and Srinivasan Keshav. "Canopus: A Scalable and Massively Parallel Consensus Protocol." *Proceedings of the 13th International Conference on emerging Networking EXperiments and Technologies*. ACM, 2017.

Moraru, Iulian, David G. Andersen, and Michael Kaminsky. "There is more consensus in egalitarian parliaments." *Proceedings of the Twenty-Fourth ACM Symposium on Operating Systems Principles*. 2013.

Casino, Fran, Thomas K. Dasaklis, and Constantinos Patsakis. "A systematic literature review of blockchain-based applications: current status, classification and open issues." *Telematics and Informatics* 36 (2019): 55-81.

Hari, Adiseshu, and T. V. Lakshman. "The internet blockchain: A distributed, tamper-resistant transaction framework for the internet." *Proceedings of the 15th ACM Workshop on Hot Topics in Networks*. ACM, 2016.

Week 8 December 1 Applications 2

Gosele, Martin and Philipp Sandner, "Analysis of Blockchain Technology in the Mobility Sector," *Working Paper, Frankfurt School Blockchain Sector*, Frankfurt School of Finance and Management, April 2018.

Ozercan, Halil Ibrahim, et al. "Realizing the potential of blockchain technologies in genomics." *Genome research* 28.9 (2018): 1255-1263.

Downes, Lauren, and Chris Reed. "Blockchain for Governance of Sustainability Transparency in the Global Energy Value Chain." *Queen Mary School of Law Legal Studies Research Paper* 283 (2018).

Mengelkamp, Esther, et al. "Designing microgrid energy markets: A case study: The Brooklyn Microgrid." Applied Energy 210 (2018): 870-880.