CS 856 Advanced Topics in Distributed Computing

Blockchain: Foundations and Applications

Tuesdays and Thursdays, 1:00 – 2:20 PM, DC 2568. First class is on Jan. 8, 2019

Instructor: S. Keshav; keshav@uwaterloo.ca; DC 3621; http://cs.uwaterloo.ca/~keshav

1. Overview

This seminar course examines foundations and current research into distributed ledger (blockchain) technologies and their applications. Students will read, review, and present research papers. There will also be a term-long research project. 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, such as CS 454 (basic concepts of computer networking and operating systems, distributed systems, concurrency, cryptography, security, and performance analysis).

3. Learning objectives

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

Students will learn about:

Blockchains

1. Blockchain basics
2. Bitcoin and its variants
3. Ethereum and smart contracts
4. Other permissionless blockchain technologies
5. Permissioned blockchains
6. Blockchain scalability

Foundations

7. Crash fault-tolerant consensus
8. Byzantine fault-tolerant consensus
9. Scalable consensus protocols

Applications

10. Applications to the Internet, mobility, genomics, and energy systems

We will study four papers in each topic area; two papers per class. The paper list is at the end of this document.

Students will also learn the following research skills (please note these are hyperlinked to online resources):

1. How to read a paper
2. How to review a paper
3. How to analyze a paper's strengths and weaknesses
4. Formulating a research problem
5. Choosing a research path
6. Written and oral presentation skills

The first three will be based on in-class guidance by the instructor, the latter three by means of a course project.

4. Class mechanics

Students are expected to carefully read the assigned papers and come to class prepared to take part in classroom discussions. To ensure this, they must submit an online review for both papers *before class*. The review should summarize the paper and the issues the student plans to discuss in class. Students need to submit a review even for the paper they are themselves presenting.

Each paper will be presented by a student in a 10-minute oral presentation. Presenters should take an adversarial position by pointing out weak and controversial positions in the paper. They should highlight the paper's contributions, any surprises, and other possible applications of the techniques proposed in the paper, while placing the work in the context of other papers covered in the course (and especially the papers covered in that particular week). Presenters are encouraged begin discussion by posing some open-ended questions and controversial statements. This will be followed by an in-class instructor-led discussion, using Socratic questioning.

Attendance alone is not enough for the participation mark (10%). Students must participate: each student is expected to contribute to class discussion at least once or twice each class by asking a question, commenting on a topic, or clarifying a point. The instructor will keep track of participation by each student, which will be taken into account in computing the final grade.

Auditing the class is permitted. Auditors must read all papers and submit reviews online. However, they need not do a project, and will not be expected to participate in class discussions.

5. Project

Students will work in **pairs** on an original research project on a topic related to blockchain technologies. Each pair will obtain approval for their draft proposal from the instructor; proposals must be refined in a second draft. Towards the end of the term, they will present their work to the class in a 30-minute conference-style presentation including five minutes for questions. In addition, by the end of term, they will produce a potentially-publishable workshop-quality paper, 10–12 pages in length, in ACM single-spaced double-column format, describing their project.

Project deadlines are as follows:

Submission of first draft: February 10th

Submission of second draft: March 24th

Final report due: April 14th

6. Grading

Grades will be assigned as follows:

10% Paper presentations (5% for each of 2 paper presentations)
22% Reviews of papers (0.5% per paper)
10% Class participation (based on overall participation in class)
58% Project (10% for first draft; 10% for second draft, 30% for final report; 8% presentation)

Grades will be available after the end of term through LEARN.

Paper list

These papers can be found online in the paper review system. Reading materials may be augmented by reading related articles from: https://a16z.com/2018/02/10/crypto-readings-resources/

Week 1	Jan 8,10	Introduction

Two lectures on an introduction to blockchains and research skills based on the tutorial on "Fundamentals of Blockchains" by Maiyya, Zakhary, Agrawal, and El Abbadi, UC Santa Barbara.

Week 2	Jan 15, 17	Blockchain basics

[2.1] Bitcoin, Beyond. "BlockChain Technology." (2015).
[2.2] Narayanan, Arvind, et al., "Preface" in *Bitcoin and cryptocurrency technologies: a comprehensive introduction*. Princeton University Press, 2016.
[2.3] Narayanan, Arvind, et al., Introduction to Cryptography & Cryptocurrencies, Chapter 1 in *Bitcoin and cryptocurrency technologies: a comprehensive introduction* *Princeton University Press*, 2016.
[2.4] Narayanan, Arvind, et al., How Bitcoin Achieves Decentralization, Chapter 2 in *Bitcoin and cryptocurrency technologies: a comprehensive introduction*, ibid.

Week 3	Jan 22,34	Bitcoin and its variants

[3.1] Nakamoto, Satoshi. "Bitcoin: A peer-to-peer electronic cash system." (2008).
[3.2] Narayanan, Arvind, et al., "Mechanics of Bitcoin," Chapter 3 in *Bitcoin and cryptocurrency technologies: a comprehensive introduction*, ibid.
[3.3] Tschorsch, Florian, and Björn Scheuermann. "Bitcoin and beyond: A technical survey on decentralized digital currencies." *IEEE Communications Surveys & Tutorials* 18.3 (2016): 2084-2123.
[3.4] Narayanan, Arvind, et al. "Bitcoin as a platform," Chapter 9 in *Bitcoin and cryptocurrency technologies: a comprehensive introduction*, ibid.

Week 4	Jan 29,31	Ethereum and smart contracts

[4.1] Buterin, Vitalik, "Ethereum: A next-generation smart contract and decentralized application platform," Online 2014. Also see the online documents here.
[4.2] Wood, Gavin. "Ethereum: A secure decentralised generalised transaction ledger." Ethereum project yellow paper 151 (2014): 1-32. (Skip the appendix).
[4.3] Szabo, Nick, "Formalizing and securing relationships on public networks," *First Monday*, https://ojphi.org/ojs/index.php/fm/article/view/548 (online only).
[4.4] Delmolino, Kevin, et al. "Step by step towards creating a safe smart contract: Lessons and insights from a cryptocurrency lab." *International Conference on Financial Cryptography and Data Security*. Springer, Berlin, Heidelberg, 2016.

Week 5	Feb 5,7	Other permissionless blockchain technologies

[5.1] Gilad, Yossi, et al. "Algorand: Scaling byzantine agreements for cryptocurrencies." *Proceedings of the 26th Symposium on Operating Systems Principles*. ACM, 2017.
[5.2] Kogias, Eleftherios Kokoris, et al. "Enhancing bitcoin security and performance with strong consistency via collective signing." 25th USENIX Security Symposium (USENIX Security 16). 2016.
[5.3] EOS.IO Technical Whitepaper v2
[5.4] Popov, Sergeui, "The Tangle", http://untangled.world/iota-whitepaper-tangle/

Week 6	Feb 12,14	Permissioned blockchains

[6.1] Monax tutorial on permissioned blockchains at https://monax.io/learn/permissioned_blockchains/
[6.2] Androulaki, Elli, et al. "Hyperledger fabric: a distributed operating system for permissioned blockchains." *Proceedings of the Thirteenth EuroSys Conference*. ACM, 2018.
[6.3] Brown, Richard Gendal, et al. "Corda: An introduction." *R3 CEV, August* (2016).
For more details, refer to Hearn, Mike, "Corda: A distributed ledger", Technical White paper, Version 0.5, November 29, 2016 and https://arxiv.org/pdf/1809.03421
[6.4] Quorum Technical Whitepaper Version 0.2, https://github.com/jpmorganchase/quorum-docs/blob/master/Quorum%20Whitepaper%20v0.2.pdf

Week 7: Break for reading week

Week 8	Feb 26,28	Blockchain scalability

[8.1] Vukolić, Marko. "The quest for scalable blockchain fabric: Proof-of-work vs. BFT replication." International Workshop on Open Problems in Network Security. Springer, 2015.
[8.2] Back, Adam, et al. "Enabling blockchain innovations with pegged sidechains." (2014).
[8.3] Klarman, Uri, et al., bloXroute: A Scalable Trustless Blockchain Distribution Network Technical whitepaper, Version 1.0, March 2018.
[8.4] Poon, Joseph, and Thaddeus Dryja. "The bitcoin lightning network: Scalable off-chain instant payments." *Draft version 0.5*.9.2, January 2014.

Week 9	Mar 5, 7	Crash fault-tolerant consensus

[9.1] Lampson, Butler W. "How to build a highly available system using consensus." *International Workshop on Distributed Algorithms*. Springer, Berlin, Heidelberg, 1996.
[9.2] Lamport, Leslie. "Paxos made simple." *ACM Sigact News* 32.4 (2001): 18-25.
[9.3] Van Renesse, Robbert, and Deniz Altinbuken. "Paxos made moderately complex." *ACM Computing Surveys (CSUR)* 47.3 (2015): 42.
[9.4] 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.

Week 10	Mar 12, 14	Byzantine fault tolerant consensus

[10.1] Castro, Miguel, and Barbara Liskov. "Practical Byzantine fault tolerance." *Proc. OSDI*. Vol. 99. 1999.
[10.2] Kotla, Ramakrishna, et al. "Zyzzyva: speculative byzantine fault tolerance." *ACM SIGOPS Operating Systems Review* 41.6 (2007): 45-58.
[10.3] Van Renesse, Robbert, Chi Ho, and Nicolas Schiper. "Byzantine chain replication." *Proc. PODS*, 2012.
[10.4] Miller, Andrew, et al. "The honey badger of BFT protocols." *Proc. CCS, 2016.*

Week 11	Mar 19, 21	Scalable consensus protocols

[11.1] Moraru, Iulian, David G. Andersen, and Michael Kaminsky. "Egalitarian paxos." *ACM Symposium on Operating Systems Principles*. 2012.
[11.2] 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.
[11.3] Gilad, Yossi, et al. "Algorand: Scaling byzantine agreements for cryptocurrencies." *Proceedings of the 26th Symposium on Operating Systems Principles*. ACM, 2017.
[11.4] Gueta, Guy Golan, et al. "SBFT: a Scalable Decentralized Trust Infrastructure for Blockchains." *arXiv preprint arXiv:1804.01626* (2018).

Week 12	Mar 26, 28	Applications 1

[12.1] 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.
[12.2] Wilkinson, Shawn, et al. "Storj a peer-to-peer cloud storage network." (2014).
[12.3] Ripple Inc., "Product Overview: A technical overview of xCurrent", October 2017.
[12.4] 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.

Week 13	Apr 2, 4	Applications 2

[13.1] Mengelkamp, Esther, et al. "A blockchain-based smart grid: towards sustainable local energy markets." *Computer Science-Research and Development* 33.1-2 (2018): 207-214.
[13.2] 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).
[13.3] Ozercan, Halil Ibrahim, et al. "Realizing the potential of blockchain technologies in genomics." *Genome research* 28.9 (2018): 1255-1263.
[13.4] Werbach, Kevin, Trust, But Verify: Why the Blockchain Needs the Law. 33 *Berkeley Tech. L.J.* 489 (2018). Available at SSRN: https://ssrn.com/abstract=2844409 or http://dx.doi.org/10.2139/ssrn.2844409