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:

1. Blockchain basics
2. Bitcoin and its variants
3. Ethereum and smart contracts
4. Other permissionless blockchain technologies
5. Permissioned blockchains
6. Consensus
7. Byzantine fault tolerant consensus
8. Scalability proposals
9. Scalable consensus protocols
10. Blockchain applications
11. Blockchain in the world

We will study four papers in each topic area; two papers per class. A preliminary paper list can be found 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.

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.

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.

Preliminary paper list

I plan to cover the papers in this list. Most of the papers listed below can be accessed on-line from UW servers. Papers published in ACM journals and proceedings can be accessed through the ACM Digital Library while those published in IEEE sources can be obtained from IEEE Xplore. Springer publications (e.g., Lecture Notes in Computer Science - LNCS) can be obtained from Springer LINK.

Reading materials will be augmented by related articles from:
https://a16z.com/2018/02/10/crypto-readings-resources/

All papers can be found online in the review system.

Week 1 Jan 8,10: Two lectures on an introduction to blockchains and research skills

Week 2 Jan 15, 17: Blockchain basics

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

Week 3 Jan 22, 24: Bitcoin and its variants

[1] Nakamoto, Satoshi. "Bitcoin: A peer-to-peer electronic cash system." (2008).
[2] Narayanan, Arvind, et al., "Mechanics of Bitcoin," Chapter 3 in *Bitcoin and cryptocurrency technologies: a comprehensive introduction, Princeton University Press*, 2016.
[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.
[4] Narayanan, Arvind, et al. "Bitcoin as a platform," Chapter 9 in *Bitcoin and cryptocurrency technologies: a comprehensive introduction,* Princeton University Press, 2016.

Week 4 Jan 29, 31: Ethereum and smart contracts

[1] Buterin, Vitalik, "Ethereum: A next-generation smart contract and decentralized application platform," Online 2014. Also see the online documents here.
[2] Wood, Gavin. "Ethereum: A secure decentralised generalised transaction ledger." Ethereum project yellow paper 151 (2014): 1-32. (Skip the appendix).
[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] 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

[1] Gilad, Yossi, et al. "Algorand: Scaling byzantine agreements for cryptocurrencies." *Proceedings of the 26th Symposium on Operating Systems Principles*. ACM, 2017.
[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.
[3] EOS.IO Technical Whitepaper v2
[4] Popov, Sergeui, "The Tangle", http://untangled.world/iota-whitepaper-tangle/

Papers are finalized up to here, preliminary after this.

Week 6 Feb 12, 14: Permissioned blockchains

[1] Androulaki, Elli, et al. "Hyperledger fabric: a distributed operating system for permissioned blockchains." *Proceedings of the Thirteenth EuroSys Conference*. ACM, 2018.
[2] Sousa, Joao, Alysson Bessani, and Marko Vukolić. "A byzantine fault-tolerant ordering service for the hyperledger fabric blockchain platform." *arXiv preprint arXiv:1709.06921* (2017).
[3] Vukolić, Marko. *Hyperledger fabric: towards scalable blockchain for business*. Tech. rep. Trust in Digital Life 2016. IBM Research, 2016. URl: https://www. zurich. ibm. com/dccl/papers/cachin_dccl. pdf, 2016.
[4] Androulaki, Elli, et al. "Cryptography and protocols in hyperledger fabric." *Real-World Cryptography Conference*. 2017.

Week 7: Break for reading week

Week 8 Feb 26, 28: Consensus

[1] Lamport, Leslie. "Paxos made simple." *ACM Sigact News* 32.4 (2001): 18-25.
[2] Ongaro, Diego, and John K. Ousterhout. "In search of an understandable consensus algorithm." *USENIX Annual Technical Conference*. 2014.
[3] Howard, Heidi, Dahlia Malkhi, and Alexander Spiegelman. "Flexible paxos: Quorum intersection revisited." *arXiv preprint arXiv:1608.06696* (2016).
[4] Van Renesse, Robbert, Nicolas Schiper, and Fred B. Schneider. "Vive la différence: Paxos vs. viewstamped replication vs. ZAB." *IEEE Transactions on Dependable and Secure Computing* 12.4 (2015): 472-484.

Week 9 March 5, 7: Byzantine fault tolerant consensus: PBFT, Zyzzyva, Tendermint

[1] Castro, Miguel, and Barbara Liskov. "Practical Byzantine fault tolerance." *OSDI*. Vol. 99. 1999.
[2] Kotla, Ramakrishna, et al. "Zyzzyva: speculative byzantine fault tolerance." *ACM SIGOPS Operating Systems Review* 41.6 (2007): 45-58.
[3] Y. Gilad, R. Hemo, S. Micali, G. Vlachos, and N. Zeldovich, "Algorand: Scaling byzantine agreements for cryptocurrencies," 2017.
[4] Tendermint

Week 10 March 12, 14: Scalability proposals: sharding, sidechains, payment channels, Bloxroute

[1] Vukolić, Marko. "The quest for scalable blockchain fabric: Proof-of-work vs. BFT replication." International Workshop on Open Problems in Network Security. Springer, Cham, 2015.
[2] Sidechains
[3] Poon, Joseph, and Thaddeus Dryja. "The bitcoin lightning network: Scalable off-chain instant payments." *Draft version 0.5* 9 (2016): 14.
[4] Buterin, Vitalik, and Virgil Griffith. "Casper the friendly finality gadget." arXiv preprint arXiv:1710.09437 (2017).

Week 11 March 19, 21: Scalable consensus protocols

[1] Li, Jialin, et al. "Just Say NO to Paxos Overhead: Replacing Consensus with Network Ordering." *OSDI*. 2016.
[2] Jin, Xin, et al. "NetChain: Scale-Free Sub-RTT Coordination." *15th {USENIX} Symposium on Networked Systems Design and Implementation ({NSDI} 18)*. USENIX} Association}, 2018.
[3] 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.
[4] Keshav, Srinivasan, et al. "RCanopus: Making Canopus Resilient to Failures and Byzantine Faults." (2018).

Week 12 March 26, 28: Applications: BigChainDB, Storj, Bitcoin Covenants

[1] McConaghy, Trent, et al. "BigchainDB: a scalable blockchain database." *white paper, BigChainDB* (2016).
[2] Wilkinson, Shawn, et al. "Storj a peer-to-peer cloud storage network." (2014).
[3] O'Connor, Russell, and Marta Piekarska. "Enhancing Bitcoin transactions with covenants." *International Conference on Financial Cryptography and Data Security*. Springer, Cham, 2017.
[4] https://www.cybermiles.io/wp-content/uploads/2018/03/Technical-Whitepaper_en-US.pdf

Week 13 April 2, 4: Blockchain in the world

[1] Korpela, Kari, Jukka Hallikas, and Tomi Dahlberg. "Digital supply chain transformation toward blockchain integration." *Proceedings of the 50th Hawaii international conference on system sciences*. 2017.
[2] Basden, James, and Michael Cottrell. "How utilities are using blockchain to modernize the grid." *Harvard Business Review* (2017).
[3] Liang, Xueping, et al. "Provchain: A blockchain-based data provenance architecture in cloud environment with enhanced privacy and availability." *Proceedings of the 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing*. IEEE Press, 2017.
[4] 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.