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 10\textsuperscript{th}
   Submission of second draft: March 24\textsuperscript{th}
   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/

<table>
<thead>
<tr>
<th>Week</th>
<th>Jan 8,10</th>
<th>Introduction</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>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.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Week</th>
<th>Jan 15, 17</th>
<th>Blockchain basics</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Week</th>
<th>Jan 22,34</th>
<th>Bitcoin and its variants</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Week</th>
<th>Jan 29,31</th>
<th>Ethereum and smart contracts</th>
</tr>
</thead>
</table>
**Week 5**  
Feb 5,7  
Other permissionless blockchain technologies

[5.3] EOS.IO Technical Whitepaper v2

**Week 6**  
Feb 12,14  
Permissioned blockchains


**Week 7: Break for reading week**

**Week 8**  
Feb 26,28  
Blockchain scalability


**Week 9**  
Mar 5, 7  
Crash fault-tolerant consensus

Week 10  Mar 12, 14  Byzantine fault tolerant consensus


Week 11  Mar 19, 21  Scalable consensus protocols


Week 12  Mar 26, 28  Applications 1


Week 13  Apr 2, 4  Applications 2

Mental Health: If you or anyone you know experiences any academic stress, difficult life events, or feelings like anxiety or depression, we strongly encourage you to seek support.

On-campus Resources

- Campus Wellness [https://uwaterloo.ca/campus-wellness/](https://uwaterloo.ca/campus-wellness/)
- Counselling Services: counselling.services@uwaterloo.ca / 519-888-4567 ext 32655 / Needles Hall North 2nd floor, (NH 2401)
- MATES: one-to-one peer support program offered by Federation of Students (FEDS) and Counselling Services: mates@uwaterloo.ca
- Health Services service: located across the creek from Student Life Centre, 519-888-4096.

Off-campus Resources

- Good2Talk (24/7): Free confidential help line for post-secondary students. Phone: 1-866-925-5454
- Here 24/7: Mental Health and Crisis Service Team. Phone: 1-844-437-3247
- OK2BME: set of support services for lesbian, gay, bisexual, transgender or questioning teens in Waterloo. Phone: 519-884-0000 extension 213

Diversity: It is our intent that students from all diverse backgrounds and perspectives be well served by this course, and that students’ learning needs be addressed both in and out of class. We recognize the immense 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. In particular:

- We will gladly honour your request to address you by an alternate/preferred name or gender pronoun. Please advise us of this preference early in the semester so we may make appropriate changes to our records.
- We will honour your religious holidays and celebrations. Please inform of us these at the start of the course.
- We will follow AccessAbility Services guidelines and protocols on how to best support students with different learning needs.