جامعة الملك عبدالله
للعلوم والتقنية
King Abdullah University of
Science and Technology

Course Syllabus: Contemporary Topics in Computing Network - CS 394B

Division	Computer, Electrical and Mathematical Sciences & Engineering
Course Number	CS 394B
Course Title	Contemporary Topics in Computing Network
Academic Semester	Spring
Academic Year	2017/2018
Semester Start Date	01/28/2018
Semester End Date	05/24/2018
Class Schedule (Days & Time)	04:00 PM - 05:30 PM | Sun Wed

Instructor(s)

Name	Email	Phone	Office Location	Office Hours
Marco Canini	marco@kaust.edu.sa	+966128080489	0144, 1, Al-Khawarizmi (bldg. 1)	On request

Teaching Assistant(s)

Name	Email

Course Information

Comprehensive Course Description	This course will cover the technical aspects of blockchain technologies and distributed consensus. Students will learn how these systems work and how to engineer secure software that interacts with the Bitcoin network and other cryptocurrencies. The introductory material will cover the following areas: - basics of cryptography; Merkle tree - blockchain; distributed consensus - mining; incentives - proof of work; proof of stake - economics - security - smart contracts; applications The advanced material will delve into active research problems in the area, including attacks, network scalability, alternatives to proof of work/stake.
Course Description from Program Guide	
Goals and Objectives	By the end of the course, students will: - Have the conceptual foundations to engineer secure software that interacts with the blockchain. - Be able to integrate ideas from the blockchain in their own projects. - Comprehend and critique relevant research papers in the area of blockchain systems. - Present research ideas both orally in a concise way and within the allotted time as well as in writing. - Defend the research approach, design decisions, and the evaluation methods in a discussion. - Moderate a discussion after a research presentation.

Required Knowledge	Basic Computer Science and basic computer programming skills are essential. Knowledge of Computing Systems and Concurrency (CS 240), or an equivalent course, or instructor consent, is required. Background in cryptography is helpful but not necessary; we will introduce concepts from cryptography as needed during class but students with no background in cryptography may wish to do extra reading. A basic understanding of probability theory and modular arithmetic will be helpful.
Reference Texts	The main textbook reference is: Bitcoin and Cryptocurrency Technologies, by Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller, Steven Goldfeder, Princeton University Press, 2016 Additional material consists of video lectures on Youtube and papers. We will read the papers in the schedule, which are available electronically through the course website.
Method of evaluation	**5.00**% - Active participation **15.00**% - Scientific review article presentation **15.00**% - Presentation **25.00**% - Homework /Assignments **40.00**% - Course Project(s)
Nature of the assignments	This course will consist of a combination of classes taught using a flipped classroom style and paper presentations and discussions. Each student will be individually responsible for writing up a short summary of every paper. Programming assignments and group projects are the other critical aspect of the course. Projects should tackle a relevant and motivated problem related to using the blockchain technology or improving an existing blockchain system. Students will be encouraged to work within existing open source projects. Projects must be written up in a term paper. There are no exams in the course.
Course Policies	We will have zero tolerance for academic misconduct. Cheating, plagiarism, and any form of dishonesty will be handled with maximum severity, according to university regulations. If you are ever in doubt about whether an action on your part may constitute unacceptable behavior, please ask the instructor before proceeding—doing so afterward is too late. **Your work.** Apart from the group project, any work you turn in must be your own and is to be done individually, and the usual code of conduct applies. You must acknowledge any sources of your words, ideas, and software when they are not your own, and you must disclose in advance, without any specific request, any sources you used. Do not use code from a student who took the course in a previous semester. **Late work.** There is no policy on late work. If you cannot submit your work by the deadline, it will not be accepted. **Attendance and participation.** It is expected that you will attend and participate actively to all lectures. If you have any concerns about not being able to regularly attend class (e.g., you will have to miss several classes during the quarter) please discuss this as soon as possible with the course staff. Attendance is a necessary but not sufficient condition for good class participation. In particular, we expect papers to have been read thoroughly prior to lecture and that you should prepare questions or opinions about the reading, and I may call upon you to speak in class. We evaluate class participation by observing how prepared you are to discuss the covered papers.
Additional Information	Disclaimer: This course focuses exclusively on the technical aspects of Bitcoin. The monetary and legal aspects of Bitcoin and other cryptocurrencies are not a subject of this course. For a more up to date version of this syllabus and the actual lecture schedule, you are required to see the version of the syllabus on the class website. The class website will be announced on the first lecture. An online discussion forum will be offered on the Piazza system. This instructor does not use Blackboard.

Tentative Course Schedule *(Time, topic/emphasis & resources)*		
Week	**Lectures**	**Topic**
1	Sun 01/28/2018 Wed 01/31/2018	Introduction to Blockchain and Cryptocurrencies Basics of cryptography
2	Sun 02/04/2018 Wed 02/07/2018	How Bitcoin Achieves Decentralization
3	Sun 02/11/2018 Wed 02/14/2018	Mechanics of Bitcoin
4	Sun 02/18/2018 Wed 02/21/2018	How to Store and Use Bitcoins
5	Sun 02/25/2018 Wed 02/28/2018	Mining
6	Sun 03/04/2018 Wed 03/07/2018	Anonymity
7	Sun 03/11/2018 Wed 03/14/2018	Governance
8	Sun 03/18/2018 Wed 03/21/2018	Alternative Mining Puzzles
9	Sun 03/25/2018 Wed 03/28/2018	Blockchain as a Platform
10	Sun 04/01/2018 Wed 04/04/2018	Beyond Bitcoin
11	Sun 04/08/2018 Wed 04/11/2018	Smart Contracts
12	Sun 04/15/2018 Wed 04/18/2018	Scalability
13	Sun 04/22/2018 Wed 04/25/2018	Alternatives to PoW / PoS Tangle
14	Sun 04/29/2018 Wed 05/02/2018	Attacks and Verification Improving Anonimity
15	Sun 05/06/2018 Wed 05/09/2018	Project presentations
16	Sun 05/13/2018 Wed 05/16/2018	
17	Sun 05/20/2018 Wed 05/23/2018	
18		

Note

The instructor reserves the right to make changes to this syllabus as necessary.