CS690P: Secure Distributed Systems
3 credits

SYLLABUS

Prof. Brian Levine

Last revised: December 30, 2017

1 Important Details

When: M 2:30pm–3:45pm

Where: Integrated Learning Center N101

Readings: There is no textbook for this class. Instead, we will be reading research papers on blockchains, as well as several prepared notes authored by myself.

Office Hours: Tuesdays 11–Noon and by appointment. Always held in my office, 306 of the CS Building. My email is `bnl@umass.edu`.

2 Introduction

This is a class devoted to the study of securing distributed systems, with decentralized digital currencies serving as our real platform of interest. Examples of such decentralized systems include Bitcoin and Ethereum, which are both open source, the subject of great academic interest, and supporting an enormous user base — not to mention holding hundreds of millions of dollars in value. We'll start with the fundamentals of Lamport's, Fischer's, and Douceur's results that fence-in consensus systems, including blockchains. We'll also look at the efficiency of the network architectures for peer-to-peer communication and attacks on their security (e.g., eclipse and other denial of service attacks). And we'll review applied crypto such as elliptical curves (used to validate transactions). Other topics include privacy and attribution, economics and finance, and crime.

In many ways, our goal is to explore this broad collection of topics in security, network, and distributed systems with blockchains being the common thread that allows a cohesive structure. You'll learn a lot in this class that is applicable well beyond bitcoin and blockchains.

Assignments will include advanced programming projects and reading research papers. Students will complete these readings, several take-home assignments based on the readings, and participate in a lively class discussion. In addition, there will be a midterm and final exam. Students will be asked to express an opinion on many topics and challenge the instructor's views and analyses.

The specific objectives for the course are as follows:

- To gain a deep understanding of secure distributed systems, with attention paid to underlying theory as well as the practical blockchain technologies that are in wide use today.
- To gain an understanding of the broader implications of this technology in terms of finance and economics.
- To gain experience in making well-reasoned arguments during class discussion.

Because of the programming assignments, students will need prior experience programming. You must use Python for these assignments. Later in the semester, we'll write Ethereum software contracts in a language called Solidity that I don't expect you to have used before (it's similar to java/python/C), and partially in javascript, which I also don't expect you to have used.

2.1 Flipped Classes and Relationship to 490P

This course will be making use of a "flipped classroom" model. Lectures will be pre-recorded and available online. We meet once a week for discussion. Discussions will be carried out assuming that students have not only completed readings and assignments, but that the pre-recorded lectures have been viewed. There will be some work assigned and completed during discussions (included in "written assignments" portion of the grade). Students that do not attend discussion will lose points towards their final grade.

This class will be offered somewhat concurrently with cs490P. The pre-recorded lectures will be the same. The discussion sections for 490P will focus on practical topics, whereas the 690P sections will focus on additional details and some additional research papers. The assignments will be shared at their core, but the tasks may be slightly different.

2.2 List of Topics

Below are an overview of topics covered in this course. The blackboard site has more specifics and last minute changes.

1. Applied cryptography
    - definition of security
    - hash functions
    - Merkle trees
    - public/private key crypto using elliptical curves
2. Blockchains
    - Nakamoto consensus
    - Details of Bitcoin: transactions, blocks, p2p networking
    - Ethics
    - Doublespend attacks (including Gambler's Ruin)
    - Selfish mining attacks
    - Eclipse attacks
3. Distributed Systems
    - Doucer's Sybil attack impossibility result
    - Clocks: NTP and Lamport clocks
    - Lamport's byzantine general's result
    - Fischer, Lynch, and Paterson's(FLP) impossibility result
4. More Bitcoin Details
    - Bitcoin's scripting language
    - Difficulty adjustment algorithms and hashrate estimation
    - Transaction malleability
    - Lightning networks
    - Segwit
5. Ethereum
    - Ghost
    - ETHASH
    - OP codes
    - Patricia Merkle Trees
    - DAPPS
    - Programming Ethereum with Solidity
6. Finance
    - basic overview of economic metrics
    - basic overview of financial instruments (derivatives, etc)
    - Initial Coin Offerings
    - Using futures contracts to insure DAPPs
7. Improving Blockchain performance
    - Bloom filters
    - Invertible Bloom Lookup Tables (IBLTs)
    - Compact Blocks
    - Graphene
    - Low variance mining with Bobtail
    - Proof of stake based blockchains
    - DAG-based blockchains

3 Inclusive Discussion

In this course, each voice in the classroom has something of value to contribute. Please take care to respect the different experiences, beliefs and values expressed by students and staff involved in this course. I support the commitment of the UMass Amherst College of Information and Computer Sciences to diversity, and welcome individuals of all ages, backgrounds, citizenships, disability, sex, education, ethnicities, family statuses, genders, gender identities, geographical locations, languages, military experience, political views, races, religions, sexual orientations, socioeconomic statuses, and work experiences.

4 Grading

Your overall grade for the course will be derived from three components. At a high-level grading is based on the following formula:

- 50% Written Assignments (including assignments completed during discussion)
- 20% Midterm Exam (evening exam, 7pm–9pm during the week of March 5)
- 20% Final Exam (during finals week)
- 10% Class participation (including attendance in discussion and online participation)

Additionally, without a passing grade on each of the two exams, students cannot pass the class.

Each assignment will have a slightly different number of points. Your score will be the total number of points earned over total number of points available for the assignments you completed. Late homeworks are NOT accepted. Final letter grades will be based on the class curve. I typically pick a B to be the midpoint of the curve but I reserve the right to pick that midpoint at the end of the semester based on class performance. Because I use a curve, that means that if the entire class does very, very well and you just do well, you might receive a C or B grade.

Don't underestimate the *Class Participation* component — full credit versus none can move your final grade by quite a bit.

4.1 Homeworks

I will use Blackboard exclusively to accept assignments, which must be in the form of a PDF (no word, text, or other formats), with your name clearly visible. In the case that an assignment involves code, please submit a tar-ball or zip file. I will not accept assignments late, and I will assign a score of zero for work that is not submitted on time (or at all).

If class participation is generally low, or if I get the sense that students aren't reading, or if it seems like good preparation for the midterm or final exams, I will give in-class quizzes. These quizzes will be pre-announced. They will become part of the homework component of your grade.

Assignments that do not compile will receive no credit.

4.2 Exams

There will be a midterm exam and a final exam. The midterm will be given in class. The final is not cumulative. It will cover material presented after the midterm, though some references to pre-midterm material are inevitable and are to be expected.

You cannot pass this class without passing grades on the exams, even with full marks otherwise.

4.3 Class Participation

I will assign this portion of your grade on the basis of your presence and participation in class. Obviously, I expect you to always attend class. Further, I expect you to participate in class discussion, posing and answering questions as appropriate. Also, I expect that you'll leave room for others to speak their minds as well. I will provide feedback about halfway through the semester as to the status of this portion of your grade.

I intend to have a series of experts from other disciplines come join us in class. Not attending on these days will weigh more heavily against your participation grade.

I will to assign grades of only none (0/3), some (1/3), some more (2/3), or highest level (3/3) for class participation.

5 Policies

All official material for the class can be found on the UMass Blackboard site. Any external course web page is more of an advertisement for the class and won't be kept up to date.

All assignments must be handed in through the Blackboard interface. See the note below about our use of *Turn It In.*

Cell phones, laptops, and similar devices may not be used during class.

5.1 Collaboration and Plagiarism

Please come see me if you are unable to keep up with the work for this class, for any reason, and I will work something out. Obviously, there isn't anything I can do when the semester has already ended. I want to see you succeed and will do everything I can to help you out. The earlier you let me help, the more help I can offer. I've been here since last millennium and I've seen it all; please come by.

Please be cognizant of the University's policies on cheating. You may discuss material with others, but your writing must be your own. When in doubt, contact me about whether a potential action would be considered plagiarism. When discussing problems with others, do not show any of your written solutions. When asking others for help, do not take notes about the solution other than to jot down publicly available references. Use only verbal communication.

If you do discuss material with anyone besides the instructors, acknowledge your collaborators in each write-up. If you obtain a key insight with help (e.g., through library work or a friend), acknowledge your source, briefly state the insight, and write up the solution on your own. I expect to see citations if you use an outside source (other than Kerr or assigned articles) to complete an assignment. You may directly quote from a decision in order to complete a brief — provided you surround the text by quotation marks — without citation.

Never misrepresent someone's work as your own. It must be absolutely clear what material is your original work. You must remove any possibility of someone else's work from being misconstrued as yours. I consider the facilitation of plagiarism (giving your work to someone else) as plagiarism as well.

As a condition of continued enrollment in this course, you agree to submit all assignments to the Turnitin and/or My Drop Box services for textual comparison or originality review for the detection of possible plagiarism. All submitted assignments will be included in the UMass Amherst dedicated databases of assignments at Turnitin and/or My Drop Box. These databases of assignments will be used solely for the purpose of detecting possible plagiarism during the grading process and during this term and in the future. Students who do not submit their papers electronically to the selected service will be required to submit copies of the cover page and first cited page of each source listed in the bibliography with the final paper in order to receive a grade on the assignment.

You can and should read the University's policies on cheating as well at http://www.umass.edu/ombuds/honesty.php/. In short, intellectual honesty requires that students demonstrate their own learning during examinations and other academic exercises, and that other sources of information or knowledge be appropriately credited. Scholarship depends upon the reliability of information and reference in the work of others. Student work at the University may be analyzed for originality of content. Such analysis may be done electronically or by other means. Student work may also be included in a database for the purpose of checking for possible plagiarized content in future student submissions. No form of cheating, plagiarism, fabrication, or facilitating dishonesty will be condoned in the University community. (Some portions of the above plagiarized from http://www.umass.edu/academichonesty/AddressingPlagiarism.html!)

6 UMass Policies

Accommodation Statement. The University of Massachusetts Amherst is committed to providing an equal educational opportunity for all students. If you have a documented physical, psychological, or learning disability on file with Disability Services (DS), you may be eligible for reasonable academic accommodations to help you succeed in this course. If you have a documented disability that requires an accommodation, please notify me within the first two weeks of the semester so that we may make appropriate arrangements.

Academic Honesty Statement. Since the integrity of the academic enterprise of any institution of higher education requires honesty in scholarship and research, academic honesty is required of all students at the University of Massachusetts Amherst. Academic dishonesty is prohibited in all programs of the University. Academic dishonesty includes but is not limited to: cheating, fabrication, plagiarism, and facilitating dishonesty. Appropriate sanctions may be imposed on any student who has committed an act of academic dishonesty. Instructors should take reasonable steps to address academic misconduct. Any person who has reason to believe that a student has committed academic dishonesty should bring such information to the attention of the appropriate course instructor as soon as possible. Instances of academic dishonesty not related to a specific course should be brought to the attention of the appropriate department Head or Chair. Since students are expected to be familiar with this policy and the commonly accepted standards of academic integrity, ignorance of such standards is not normally sufficient evidence of lack of intent (http://www.umass.edu/dean_students/codeofconduct/acadhonesty/).