Syllabus

Syllabus

Meetings: Mondays and Wednesdays, 2:00-3:15pm in Olsson 120.

Teachers: David Evans and Samee Zahur
Assistant: Ori Shimony

Office Hours: Mondays 4-5:30pm (Ori, Rice 442); Wednesdays 3:15-4:30pm (Samee, Rice 442); Thursdays 2:30-3:30pm (Dave, Rice 507). Office hours will be updated on the course calendar.

Course Site: http://bitcoin-class.org/

Readings: We will not follow a textbook closely, but will have several readings from two books (both of which are freely available):

- Andreas M. Antonopoulos, *Mastering Bitcoin: Unlocking Digital Cryptocurrencies*. (You can use the free version of the book available at https://github.com/aantonop/bitcoinbook, but would probably benefit from buying the printed version).
- Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller, Steven Goldfeder. *Bitcoin and Cryptocurrency Technologies*. This is a new book under development by a team at Princeton University. (There are also lecture videos and slides that correspond to the book.)

In addition to those books, we will have several readings from both general audience publications, technical documents, and research papers.

Overview

For the past 10,000 years, humans have been seeking better ways to store and transfer value. *Cryptocurrencies* (most notably bitcoin), provide a way to do this using bits alone without any centralized authority. In this course, we will learn about the cryptographic foundations for cryptocurrencies; networking, software, hardware, and security issues relevant to designing and implementing a cryptocurrency, and consider the economic, legal, and political issues raised by cryptocurrencies.

Expected Background

Students entering this course are expected to be comfortable reading, designing, and writing complex programs that involve thousands of lines of code distributed over many modules. You should be fairly comfortable with math, at least enough to analyze probabilities.

You should be comfortable learning how to use a new programming language features and APIs by reading their documentation (or source code when no documentation is available), and not be surprised when you are expected to learn a new language on your own or to seek documentation beyond what was provided in class.

Students are **not expected** to have significant previous experience with cryptography (although such background will certainly be helpful).

Some specific things we expect of students entering this course:

- You should have some experience programming in at least one programming language, and not be afraid of needing to learn new languages.
- You have written at least one program with over 1000 lines of code.
- You should understand basic probability and be able to figure out things like the probability that 100 tosses of a fair coin do not result in any tails.
- You should understand at least as much about complexity and computability as is covered in *Dori-Mic and the Universal Machine*.
- You should find computing exciting and delighting, and believe you can use computing to make the world a better place.

If you do not satisfy any of these expectations, that doesn't mean you cannot take the class, but you need to let one of the course teachers know about it at the beginning of the semester.

Honor Pledge

This course focuses on how to establish trust among distrusting people using mathematics, computing, and networking. As a student at Mr. Jefferson's University, you are intrinsically trusted.

We take advantage of this trust to provide a better learning environment for everyone. In particular, students in this class are expected to follow these rules:

- I will not lie, cheat or steal. If I am unsure whether something would be considered lying, cheating or stealing, I will ask before doing it.
- I will carefully read and follow the collaboration policy on each assignment. I will not abuse resources, including any submissions or solutions for assignments from last semester's version of this course, that would be clearly detrimental to my own learning.

In addition to the honor rules, students in this class are also expected to follow these behaviors:

- I will do what I can to help my fellow classmates learn. *Except when specifically instructed not to*, this means when other students ask me for help, I will attempt to provide it. I will look at their answers and discuss what I think is good or bad about their answers. I will help others improve their work, but will not give them my answers directly. I will try to teach them what they need to know to discover solutions themselves.

- I will ask for help. I will make a reasonable effort to do things on my own first (or with my partners for group assignment), but will ask my classmates or the course staff for help before getting overly frustrated. There are many ways to ask for help including the course website and office hours.
- I grant the course staff permission to reproduce and distribute excerpts from my submissions for teaching purposes. If may opt-out of this by adding a comment to your code, but without an explicit opt-out comment we assume you agree to it. Excerpts will be used anonymously when illustrating a misunderstanding or common problem, and with credit when showing an interesting or exemplary answer.
- I will not invest money I cannot afford to lose in cryptocurrencies. The main topic of this course is cryptocurrencies, and students will be encouraged to gain experience using bitcoin to conduct real transactions (but will not be expected to spend any personal money on bitcoin). Please be aware that bitcoin is very volatile, and that you could lose all the money in your bitcoin wallet if you make a programming error or lose your key. It would be foolish and reckless to convert any money you would be upset about losing into a cryptocurrency.
- I will provide useful feedback. I realize that this is a new and experimental course, and it is important that I let the course staff know what they need to improve the course. I will not wait until the end of the course to make the course staff aware of any problems. I will provide feedback either anonymously or by contacting the course staff directly. I will fill out all requested surveys honestly and thoroughly.

Assignments

The course will have one midterm, four problem sets, one final project, and a (discretionary) final exam. In addition, there will be several check-ups (short tests in class, with opportunities to revise and improve answers after discussion) and short assignments that may involve reading assignments and posting answers and questions on the course website.

Exams. The midterm is Monday, 19 October. The final exam is scheduled for Friday, 11 December (2-5pm). This time will be used to schedule short oral exams for students who have not already demonstrated strong understanding of the course topics.

Problem Sets. The problem sets will involve writing programs and solving problems to understand transactions in bitcoin (Problem Set 1), bitcoin nodes and mining (Problem Set 2), blockchain analysis (Problem Set 3), and alternate cryptocurrencies (Problem Set 4). For most of these assignments, you will be encouraged to work with one or two other people in a small team.

Final Project. For the final project, you are free to work on anything relevant to cryptocurrencies. Some suggestions for project ideas will be posted on the course website. Students who have ambitious ideas for a project may be able to arrange with the course staff to expand the project to substitute for other assignments (such as Problem Set 4).

Schedule

A tenative and (continually) updated schedule is available as a Google calendar. (You can view this calendar on the course site, or incorporate in as iCal calendar into your own calendar using this link. Except when noted otherwise, assignments are due at 8:29pm on the due date.

The main expected due dates:

- Saturday, 29 August: **Registration**
- Monday, 7 September: **Checkup 1** (in class)
- Tuesday, 15 September: **Problem Set 1: Bitcoin Transactions**
- Monday, 21 September: **Checkup 2** (in class)
- Friday, 2 October: **Problem Set 2: Nodes and Mining**
- Monday, 19 October: **Midterm Exam**
- Tuesday, 27 October: **Problem Set 3: Blockchain Analysis**
- Tuesday, 17 November: **Problem Set 4: Alternate Cryptocurrencies**
- Sunday, 22 November: **Project Proposal**
- Monday, 7 December: Last class
- Friday, 11 December: **Final Exam** (discretionary)

Dates shown here are subject to change based on how the semester progresses, but with ample warning.

Grading

We prefer to spend our time focused as much as possible on *teaching*, and as little as possible on *grading*. The assignments in this class are designed to maximize *learning*, rather than primarily for *assessment*.

That said, we understand that students do need to be assigned grades at the end of the semester, and sometimes grades can be a powerful and effective motivator as well as a useful way to measure progress and understanding.

Grades will be determined based on your performance on all the class assignments and class contributions (including postings on the course site). Some assignments may be graded by randomly looking at selected answers, rather than reading everything submitted.

There is no set weighting among these things, and in general, if there is some combination of the above that demonstrates that you have gotten what we hope out of the class then you will receive an A grade.