Syllabus

Meetings: Mondays and Wednesdays, 2:00-3:15pm in Rice Hall 032.

Teacher: David Evans.

Office Hours: After class today. Regular office hours to be scheduled and posted on the course calendar.

Course Site: All course materials will be posted at http://bitcoin-class.org/.

Textbook: We will not follow a textbook closely, but will have several readings from 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). If you are not sure if you should prefer reading things on paper, you should read *The Reading Brain in the Digital Age: The Science of Paper versus Screens*, Scientific American, 11 April 2013.)

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 study the technical aspects of cryptocurrencies, as well as the political, legal, and economic issues they raise.

Format. The class will be mostly lectures for the first half of the semester, with about three problem sets that will involve a mix of math, programming, reading, and writing (and of course, thinking). For most assignments, students will be expected to work individually or in small teams. The second half of the class will be more like a research seminar, focused around student projects (done individually or in small teams), and with presentations focused on research papers and other interesting materials.

Enrollment. Because of limited space available in the class, instructor permission is required to register. The course is open to students in all majors, and I hope to have students with a variety of backgrounds in the course, including some students with strong backgrounds in economics, politics, and law. There will be some assignments that require significant programming work and computer science background, but students who can contribute substantially to the course may be allowed to enroll without that background (and assignments will be adjusted in ways that make sense for these students).

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 new programming language features and APIs by reading their documentation (or source code when no documentation is available), and not be surprised when solving programming assignments requires you 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 I 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 me know about it at the beginning of the semester.

Honor and Expectations

As a student at Mr. Jefferson's University, you are trusted to be honorable.

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.

Other Expectations. 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.

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, so 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 frequent short assignments (Problem Sets), 3 major projects, and one open-ended project.

Problem Sets. The problem sets generally will be assigned at class on Monday or Wednesday, and due shortly after (sometimes as early as by midnight the following day). This will typically involve a short reading assignment and some questions to answer, but may also involve short technical problems.

Projects. The three major projects will involve writing programs and solving problems to understand a bitcoin wallet (Project 1), bitcoin mining (Project 2), and blockchain analysis (Project 3). 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.

Exams. I do not anticipate having any traditional exams in this course, but may schedule exams in the unfortunate even that they seem necessary for students to participate fully in the course.

The registrar has scheduled an exam for this course on Thursday, 3 May (2-5pm). I do not anticipate using this time for a traditional exam, but will use it for presenting final projects.

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 11:59pm on the due date.

Grading

I prefer to spend my 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, I 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. Grades will be determined based on your performance on the problem sets, projects, and class contributions (including postings on the course site). You should not be surprised or upset if assignments are 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 I hope out of the class then you'll receive an A grade.

