Class Syllabus

Course Web Page

Contact Info for Instructor, office hours, assignments, tests, and general information is all on the course web page.

Course Description

This course is an introduction to the foundations of Cryptocurrencies and Blockchains

Text:

Our text is **Bitcoin and Cryptocurrency Technologies** by Narayanan et al.

Prereqs

CS362, CS561 or Equivalents

Assignments:

- Assignments are due at the **beginning** of class on the due date. Assignment deadlines are strict: late homeworks will automatically receive a grade of zero, without *prior* approval. Prior approval is generally given only in the case of a medical problem or family emergency.
- Group collaboration is encouraged on the homeworks, provided that you write at the top of your homework the names of all the other students that you collaborated with. Note that although collaboration is encouraged, **the *solutions* must always be written up individually**. You should not look at or copy another student's solution **and should not copy solutions from the Internet**. In particular, when *writing up* your solutions, you should not be looking at any other solution. A rule of thumb here is the "Star Trek" Rule. After working with your group, go watch a half hour of Star Trek on TV, or your favorite mindless (sorry Trekkies) but fun TV show, before you write up the solutions. You may consult other textbooks or the Internet as you would another student (i.e. cite your source and use the ``Star Trek'' rule).
- **Copying solutions from another student or from the Internet is cheating**. In case a student presents a solution that is essentially identical in whole or in part to solutions from another student or other source, that student will receive a 0 on the assignment, will be reported to the University Administration, and may not be permitted to continue in the class.
- Put pages of hw **in order**. We don't care what order you solve the hw in, but before you turn it in, you must put the problems in order (this makes grading much easier)
- **Staple** hws, do not use paper clips, folding, tape, putty, gum, etc. Prof Saia and the TA do not bring staplers to class, so make sure you staple the hw before class (stapling helps us keep together all pages of your hw)
- Regrades: if you feel a mistake was made grading your hw, please let the TA know about it (if you still feel there is a problem, then please talk to Prof. Saia). Please ask for a regrade within one week of receiving the graded assignment.

Notes on Grading Hws

Your hws and test answers should have the following properties. We will be looking for these when we grade:

- **Clarity**: Make sure all of your work and answers are clearly legible and well separated from other problems. If we can't read it, then we can't grade it. Likewise, if we can't immediately find all of the relevant work for a problem, then we will be more likely to grade only what we see at first.

- **Completeness**: Full credit for all problems is based on both sufficient intermediate work (the lack of which often produces a 'justify' comment) and the final answer. There are many ways of doing most problems, and we need to understand exactly how YOU chose to solve each problem. Here is a good rule of thumb for deciding how much detail is sufficient: if you were to present your solution to the class and everyone understood the steps, then you can assume it is sufficient.
- **Succinctness**: The work and solutions which you hand-in should be long enough to convey exactly why the answer you get is correct, yet short enough to be easily digestible by someone with a basic knowledge of this material. If you find yourself doing more than half a page of dense algebra, generating more than a dozen numeric values or using more than a page or two of paper per problem for your solution, you're probably doing too much work. Don't turn in pages with scratch work or multiple answers - if you need to do scratch work, do it on separate scratch paper. Clearly indicate your final answer (circle, box, underline, etc.). Note: It's usually best to rewrite your solution to a problem before you hand it in. If you do this, you'll find you can usually make the solution much more succinct.

Topics

Please read the material in the textbook **before** we cover it in class. The class material will be challenging and the class pace will be fast - you will get lost very quickly if you come into the classes unprepared. Topics will likely include (total weeks in the semester is roughly 15)

- Cryptographic primitives and Centralized Blockchains
- Achieving decentralization: Byzantine Consensus
- Storing and Using Bitcoins
- Anonymity and Sybil attacks
- Smart contracts and Secure Multiparty Computation

Course Assessment

Approximate weighting:

- 30%: Class Participation
  - 10%: Questions on Papers: Post 3 discussion questions (on Piazza) for each paper covered in class
  - 10%: Responses: Answer or respond to at least one question (in class or on Piazza) for each paper
  - 10%: Presentation: Present and Lead discussion for at least one paper
- 50%: Final Project
  - 10%: Project Proposal
  - 10%: Project Checkpoint (7 minute presentation + 2 page report)
  - 30%: Final Project (15 minute presentation + 10 page paper)
- 20%: Homeworks

Grading Policies

"No deals, Mr. Bond.": Grades assigned at the end of the semester are final. You will not be able to do any additional projects, papers, etc. to change your grade.