CSCI 1951L: Course Syllabus

1 Introduction

Welcome to CS1951L: Blockchains and Cryptocurrencies! This course is an introduction to modern blockchain-based systems. Topics covered include: consensus and distributed computing, cryptocurrencies, programming smart contracts, privacy and secrecy, transfer networks, atomic swaps and transactions, non-currency applications of blockchains, and legal and social implications. CS1951L meets in Tuesdays and Thursdays from 1 to 2:20 in CIT 477.

2 The Staff

2.1 The Professor

Professor Maurice Herlihy has his office in CIT 341. He will host office hours by appointment for general course feedback (not for coursework).

2.2 The TAs

Visit the staff page on the website to see this year’s TAs. They have two main functions:

- They evaluate and give critical feedback on your assignments.
- They hold hours (and maintain a Piazza forum) to answer your questions.

All TAs grade programs, hold TA hours, and have other assorted duties. The HTA are responsible for the organization and administration of the course, and work closely with Professor Herlihy on all aspects of the course. They also supervise the TAs in grading programming assignments to ensure consistent grading, which is aided by detailed rubrics for each assignment that discuss common mistakes as well as if and how to deduct points for them.

3 Course Materials

All course materials can be found on the course website (cs.brown.edu/courses/cs1951l). Slides for the lectures are released the day before, and recordings of the lectures are posted the following class. Assignments are also posted on the site when they are released. Piazza, our online QA forum, will also be updated regularly with assignment clarifications and pinned posts relating to frequently-asked questions.
4 Topics

1. Introduction

2. Fundamentals of Crypto, Hashing, Consensus

3. Bitcoin
   - Blockchain Data Structure
   - UTXO
   - Blocks
   - PoW
   - P2P network

4. Bitcoin Mining
   - Incentives
   - Consortiums
   - Selfish mining
   - Bitcoin with no CoinBase

5. Bitcoin Data Structures
   - Merkle Trees
   - LPV nodes

6. Retrospective on Nakamoto Paper

7. Ethereum
   - EVM
   - EVEM Data Structures
   - Alternative Data Structures

8. Smart Contracts
   - Solidity
   - Solidity pitfalls and disasters

9. Example Smart Contracts
   - ICO token
   - Cryptokitties

10. Wallets, storage, custody

11. Permissioned Blockchains
    - Hyperledger Fabric
    - Concurrent Contract Execution
4.1 Lectures

CS1951L lectures are Tuesday and Thursday, 1:00pm - 2:20pm. You are expected to attend all class hours. A copy of the lecture slides will also be accessible online, from the CS1951L homepage. You are responsible for everything said in class.

Here is a tentative list of the lectures:

1. 1/24 - Course Introduction
2. 1/29 - Bitcoin Introduction
3. 2/5 - Bitcoin Mining & Attacks
4. 2/7 - Bitcoin Data Structures
5. 2/12 - Ethereum Virtual Machine
6. 2/14 - Solidity Language
7. 2/19 - TBD
8. 2/21 - Solidity Pitfalls Part 1
9. 2/26 - Solidity Pitfalls Part 2
10. 2/28 - Solidity Pitfalls Part 3
11. 3/5 - Solidity Pitfalls Part 4
12. 3/7 - Ethereum Data Structures
13. 3/14 - Off-chain payments
14. 3/19 - Atomicity in Blockchain
15. 3/21 - Cross-Chain swaps
16. 4/2 - Privacy and Zero Knowledge Part 1
17. 4/4 - Privacy and Zero Knowledge Part 2
18. 4/11 - Byzantine Fault-tolerance
19. 4/16 - Hashgraph
20. 4/18 - Avalanche
21. 4/23 - Algorand
22. 4/25 - TBD
23. 4/30 - TBD
24. 5/2 - TBD
4.2 Handouts & Emails

We post most of the handouts and course materials on the website and the TAs will also send out emails containing useful administrative information and assignment clarifications to the class email list.

Just as you are expected to keep up with course readings in literature courses, so too are you expected to keep up with course materials and communications in this course. Please read everything thoroughly because much of it is essential to your success in this course.

4.3 Projects

There will be 2 projects that will be released throughout the semester, leading to a final project. More details will be available on the course website.

4.4 Homework

There will be 5 homework assignments used to help your understandings of the course material. They must be typed and handed in as a PDF on Gradescope. Please refer to section 4 to learn more about the late policy.

4.5 Quizzes

There will be 3 “Quizzes” during the semester. Here is a tentative date for the Quizzes:

1. 3/12 - Quiz 1
2. 4/9 - Quiz 2
3. 5/7 Quiz 3

The times and locations will be updated on the course website.

5 Late Policy

You have a total of 2 Late Days that can be used towards any assignment except the final exam. You may turn in an assignment late even if you have used your 2 late days but a letter grade will be dropped per additional day you take. These late days are generally reserved for job interviews, emergencies, etc. If you find yourself in more extreme circumstances please let us know.
6 Grading

Your grade in this course will be based solely on your performance on the homework, quizzes, and projects.

- 45% Quizzes
- 35% Projects
- 20% Homework

6.1 Grade Complaints

Any questions or complaints regarding grading must first be addressed to the TA who graded your particular assignment, by email or at their hours. No other TA can answer questions pertaining to your specific grade. If you are unable to resolve an issue with a TA, you may take your concerns to the HTAs, and then to Professor Herlihy.

7 Recommended Textbook

The textbook is by no means required but it may serve you as a nice resource to help you better understand the course material. The textbook is called *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction* by Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller, and Steven Goldfeder. It can be found on Amazon for around 31$ or you may find it elsewhere...

8 Feedback

Since this is a new course we will take feedback seriously. We will email out several surveys throughout the semester, and we really appreciate your constructive criticism on any topic. In short, if you don’t tell us, we will assume everything is just fine, which may not be an accurate impression - so if you have any problems, please speak up!