CSCI 1951L: Blockchains and Cryptocurrencies

Course Information and Syllabus
Summer Semester 2022

Lectures	Remote
Room	None
Lecture Notes	http://cs.brown.edu/courses/cs1951l/ A recording of each lecture will be available soon after it is given.
Text	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. All course materials can be found on the course website. 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.
Prerequisite	*CS0150 or CS0170 or CS0190*.
Instructor	Maurice Herlihy (mph@cs.brown.edu)
Office	CIT 341
Professor's Office Hours	By appointment
Head TAs	TBD
UTAs	TBD
TA Office Hours	TBD
Time Requirements	The course will require at least 180 hours over the course of the semester (including class time).In addition to three hours per week in class, you will spend 10-18 hours per week on projects. The project times will vary — less time will be required for earlier assignments than for later ones.
Goals	The primary goal is for you to understand how blockchain technology works, and how to separate myth and hype from the reality. Topics covered include consensus and distributed computing, example cryptocurrencies, programming smart contracts, privacy and secrecy, transfer networks, atomic swaps and transactions, non-currency applications of blockchains, and legal and social

	implications. Students will do a programming project and a term project.
Diversity: All are Welcome	Our intent is that this course provide a welcoming environment for all students who satisfy the prerequisites. Our TAs have undergone training in diversity and inclusion; all members of the CS community, including faculty and staff, are expected to treat one another in a professional manner. If you feel you have not been treated in a professional manner by any of the course staff, please contact either Prof. Herlihy (the instructor), Prof. Cetintemel (the department chair), or Laura Dobler (the department's coordinator for diversity and inclusion initiatives). We take all complaints about unprofessional behavior seriously.
Grading	Your grade in this course will be based solely on your performance on the homeworks and projects. • 70% Projects • 30% Homework If you have a question about the grading of an assignment, please bring it up first with the TA who graded it. If your question is not resolved to your satisfaction, then bring it up with Prof. Herlihy.
Incomplete Policy	We expect everyone to complete the course on time. However, we certainly understand that there may be factors beyond your control, such as health problems and family crises, that prevent you from finishing the course on time. If you feel you cannot complete the course on time, please discuss with Prof. Herlihy the possibility of being given a grade of Incomplete for the course and setting a schedule for completing the course in the upcoming year.
Due Dates	Projects and homeworks must be handed in by 11:59 pm on their due dates. Labs are due during the last lab hours before the next lab is released (NOT at 11:59pm!).
Late Policy	You have a total of 2 Late Days that can be used towards any assignment. 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. If you must miss class or a project deadline because of a religious holiday, you may also get an extension without using late days, please contact Prof. Herlihy.
More Information	For more in-depth information about the course, refer to the Course Missive and Collaboration Policy linked from the course website.
Accommodations	If you feel you have physical, psychological, or learning disabilities that could affect your performance in the course, we urge you to contact SEAS (https://www.brown.edu/campus-life/support/accessibility-services/). We will do whatever we can to support accommodations recommended by SEAS.
Mental Health	Being a student can be very stressful. If you feel you are under too much pressure or there are psychological issues that are keeping you from performing well at

	Brown, we encourage you to contact Brown's Counseling and Psychological Services (CAPS: https://www.brown.edu/campus-life/support/counseling-and-psychological-services/). They provide confidential counseling.
Coping with Unforeseen or Difficult Circumstances	If there are events that are upsetting to you, whether political, family-related, weather-related, etc., that affect your ability to do well in class, we are happy to take them into account with respect to our late and incomplete policies. Please feel free to talk to Prof. Herlihy about this. Additionally, Student Support Services Deans (https://www.brown.edu/offices/student-support/student-support-services) can be a helpful resource for discussing current concerns and academic and personal plans. They are available for both same-day consults and scheduled appointments.

Lectures (subject to change)

Date	Topic
13 May	Course Introduction
18 May	Bitcoin Introduction
20 May	Bitcoin Mining and Attacks
25 May	Bitcoin Data Structures
27 May	Ethereum Virtual Machine
3 June	Ethereum Data Structures
8 June	Solidity Language
10 June	Solidity Pitfalls and Hazards Part 1
15 June	Solidity Pitfalls and Hazards Part 2
17 June	Solidity Pitfalls and Hazards Part 3
22 June	Solidity Pitfalls and Hazards Part 4
24 June	Concurrency in smart contracts
29 June	Cross-chain transactions (part 1)
1 July	Cross-chain transactions (part 2)
6 July	NO CLASS

8 July	Off-chain payment channels
13 July	Automated Market Makers and DEFI
15 July	Wallets and custody
20 July	Privacy and Zero Knowledge
22 July	Byzantine Consensus Protocols
27 July	Proof of Stake
29 July	Conclusion

Due Dates

What	Out	Due
Project 1	16 May	05 June
Homework 1	13 May	20 May
Project 2	5 June	25 June
Homework 2	5 June	12 June
Project 3	25 June	15 July
Homework 3	25 June	3 July
Project 4	15 July	6 August
Homework 5	15 July	22 July