USC Viterbi
School of Engineering

CSCI 599: Introduction to Blockchain Ecosystems

Units: 4.0
Fall 2024 — Wednesday — 4:00-7:20PM

Location: TBD

Instructor: Srivatsan Ravi
Office: ISI 1149
Office Hours: TBD
Contact Info: srivatsr@usc.edu

Catalogue Description

Introduction to Blockchain Ecosystems: Basics of Blockchains and Smart Contracts, Blockchain Consensus and State-Machine Replication, Blockchain Performance Analysis and Evaluation, Adversary Models, Payment-Channel Networks, Case studies of popular cryptocurrency blockchains: Solana, Bitcoin, Ethereum, Aptos, Stellar.

Course Description

The goal of this course is to introduce students to the modern blockchain and smart contract payment platforms with a focus on the core cryptographic and distributed computing algorithms underlying the functioning of these ecosystems.
This course will introduce students to the myraid of algorithms and technologies underlying modern blockchain ecosystems and how to implement them and understand their vulnerabilities.
The class projects will play a central role in the course to provide hands-on experience in building blockchains and understand how they are vulnerable to security attacks.

Learning Objectives

Course outcome: The course will enable students to

- Evaluate the different distributed computing and cryptographic technologies employed in blockchain smart contracts
- Analyse how to reason about the safety and scalability of modern blockchain systems

After completing the course, the graduates of this course will be able to do the following:

Design and Execute Blockchain Algorithms and Experiments

- specify and verify the correctness of a blockchain protocol
- analyze the different adversary models for blockchain protocols
- analyze the dimensions that affect the scalability of a distributed protocols like blockchains
- quantify how to compare two implementations of different blockchain protocols
- demonstrate about how the correctness of blockchain protocols might be subverted resulting in “double-spending attacks”

Evaluate the functioning of modern a smart contract ecosystem with blockchain and associated security vulnerabilities

- demonstrate how blockchain protocols are used in widely used technologies like Bitcoin, Ethereum, Aptos, Solana, etc
- describe Smart Contract ecosystems and topics like Non-fungible Tokens (NFT) and Payment-Channel Networks
- develop an understanding of the adversary models within the smart contract ecosystems and blockchains

Course Notes

Readings, Chapters from Online Textbooks, Lectures, and Discussion Charts will be posted regularly on our course website. A list of reference texts and publications all available freely online will also be posted on the same site.

Technological Proficiency and Hardware/Software Required

Familiarity with Computer Networking and Python/Rust programming will be required. Other learning material on algorithms and cryptography will be provided during the course.

Description of Assessment and Assignments

Each assignment in this course serves to measure the students understanding of the correctness of a particular blockchain or smart contract protocol and the programming assignments will seek to demonstrate the scalability or lack there-of of the particular smart contract implementation.

Assignment 1 will be evaluation of distributed consensus protocols
Assignment 2 will be on the correctness of state-machine replication protocols
Assignment 3 will be on the verification of smart contract protocols
Assignment 4 will be evaluating the security vulnerabilities of blockchain protocols
Assignment 5 will evaluate the vulnerabilities of payment-channel networks

Assignments Weights

This course has five assignments each of which is graded equally for 12% of the grade each.

Participation

Credit for participation is acquired by showing up and contributing to the in-class quizzes and discussion.

Grading Breakdown

Assessment Tool	**% of Grade**
Algorithms and Programming Assignments (5)	60
Midterm exam (90 minute exam) with combination of multiple choice questions and long answers for algorithm and security analysis	15
Final exam (90 minute exam) with combination of multiple choice questions and long answers for algorithm and security analysis	15
In class written quizzes with two questions (2) on select days+participation	10
TOTAL	100

Academic Integrity

Unless otherwise noted, this course will follow the expectations for academic integrity as stated in the USC Student Handbook. The general USC guidelines on Academic Integrity and Course Content Distribution are provided in the subsequent "Statement on Academic Conduct and Support Systems" section.

Collaboration: In this class, you are expected to submit work that demonstrates your individual mastery of the course concepts. You may work with at most another student, but are expected to write up your own answers. Please clearly specify with whom you discussed the assignment with.

If found responsible for an academic violation, students may be assigned university outcomes, such as suspension or expulsion from the university, and grade penalties, such as an "F" grade on the assignment, exam, and/or in the course.

Please ask the instructor [and/or TA(s)] if you are unsure about what constitutes unauthorized assistance on an exam or assignment, or what information requires citation and/or attribution.

You may not record this class without the express permission of the instructor and all other students in the class. Distribution of any notes, recordings, exams, or other materials from a university class or lectures — other than for individual or class group study — is prohibited without the express permission of the instructor.

Use of Generative AI in this Course

Generative AI is not permitted: Since creating, analytical, and critical thinking skills are part of the learning outcomes of this course, all assignments should be prepared by the student working individually or in groups as described on each assignment. Students may not have another person or entity complete any portion of the assignment. Developing strong competencies in these areas will prepare you for a competitive workplace. Therefore, using AI-generated tools is prohibited in this course, will be identified as plagiarism, and will be reported to the Office of Academic Integrity.

Course Schedule

	Topics/Daily Activities	**Assignments**
Week 1	Introduction to Course Logistics and background of Networking and Distributed Algorithm Analysis	**Assigned: Assignment 0 (not graded)**
Week 2	Discussion of Assignment 0 and overview of Distributed Computing Models	
Week 3	Distributed Consensus for Blockchains	Assigned: Assignment 1
Week 4	Byzantine State-machine replication	
Week 5	Blockchain Adversary models	*Assigned: Assignment 2*
Week 6	Empirical evaluation of Blockchain Algorithms	
Week 7	Introduction to Smart Contracts and review material for mid term exam	
Week 8	**Review and Mid term Exam**	
Week 9	Smart contract Blockchains: Case studies with Aptos/Solana	Assigned: Assignment 3
Week 10	Smart contract Blockchains: Case studies with Bitcoin	
Week 11	Smart Contracts and Blockchains: Case studies with Ethereum	Assigned: Assignment 4
Week 12	Taxonomy of Smart contract blockchain attacks	
Week 13	Blockchain storage	Assigned: Assignment 5
Week 14	Payment-Channel Networks	
Week 15	**Review material for Final Exam**	
FINAL	**Final Exam**	Due on the university-scheduled date of the final exam. Refer to the final exam schedule on the USC *Schedule of Classes* at classes.usc.edu.

Statement on Academic Conduct and Support Systems

Academic Integrity:
The University of Southern California is a learning community committed to developing successful scholars and researchers dedicated to the pursuit of knowledge and the dissemination of ideas. Academic misconduct, which includes any act of dishonesty in the production or submission of academic work, comprises the integrity of the person who commits the act and can impugn the perceived integrity of the entire university community. It stands in opposition to the university's mission to research, educate, and contribute productively to our community and the world.

All students are expected to submit assignments that represent their own original work, and that have been prepared specifically for the course or section for which they have been submitted. You may not submit work written by others or "recycle" work prepared for other courses without obtaining written permission from the instructor(s).

Other violations of academic integrity include, but are not limited to, cheating, plagiarism, fabrication (e.g., falsifying data), collusion, knowingly assisting others in acts of academic dishonesty, and any act that gains or is intended to gain an unfair academic advantage.

The impact of academic dishonesty is far-reaching and is considered a serious offense against the university. All incidences of academic misconduct will be reported to the Office of Academic Integrity and could result in outcomes such as failure on the assignment, failure in the course, suspension, or even expulsion from the university.

For more information about academic integrity see the student handbook or the Office of Academic Integrity's website, and university policies on Research and Scholarship Misconduct.

Please ask your instructor if you are unsure what constitutes unauthorized assistance on an exam or assignment, or what information requires citation and/or attribution.

Course Content Distribution and Synchronous Session Recordings Policies
USC has policies that prohibit recording and distribution of any synchronous and asynchronous course content outside of the learning environment.

Recording a university class without the express permission of the instructor and announcement to the class, or unless conducted pursuant to an Office of Student Accessibility Services (OSAS) accommodation. Recording can inhibit free discussion in the future, and thus infringe on the academic freedom of other students as well as the instructor. (Living our Unifying Values: The USC Student Handbook, page 13).

Distribution or use of notes, recordings, exams, or other intellectual property, based on university classes or lectures without the express permission of the instructor for purposes other than individual or group study. This includes but is not limited to providing materials for distribution by services publishing course materials. This restriction on unauthorized use also applies to all information, which had been distributed to students or in any way had been displayed for use in relationship to the class, whether obtained in class, via email, on the internet, or via any other media. (Living our Unifying Values: The USC Student Handbook, page 13).

Students and Disability Accommodations:
USC welcomes students with disabilities into all of the University's educational programs. The Office of Student Accessibility Services (OSAS) is responsible for the determination of appropriate accommodations for students who encounter disability-related barriers. Once a student has completed the OSAS process (registration, initial appointment, and submitted documentation) and accommodations are determined to be reasonable and appropriate, a Letter of Accommodation (LOA) will be available to generate for each

course. The LOA must be given to each course instructor by the student and followed up with a discussion. This should be done as early in the semester as possible as accommodations are not retroactive. More information can be found at osas.usc.edu. You may contact OSAS at (213) 740-0776 or via email at osasfrontdesk@usc.edu.

Support Systems:

Counseling and Mental Health - (213) 740-9355 – 24/7 on call
Free and confidential mental health treatment for students, including short-term psychotherapy, group counseling, stress fitness workshops, and crisis intervention.

988 Suicide and Crisis Lifeline - 988 for both calls and text messages – 24/7 on call
The 988 Suicide and Crisis Lifeline (formerly known as the National Suicide Prevention Lifeline) provides free and confidential emotional support to people in suicidal crisis or emotional distress 24 hours a day, 7 days a week, across the United States. The Lifeline is comprised of a national network of over 200 local crisis centers, combining custom local care and resources with national standards and best practices. The new, shorter phone number makes it easier for people to remember and access mental health crisis services (though the previous 1 (800) 273-8255 number will continue to function indefinitely) and represents a continued commitment to those in crisis.

Relationship and Sexual Violence Prevention Services (RSVP) - (213) 740-9355(WELL) – 24/7 on call
Free and confidential therapy services, workshops, and training for situations related to gender- and power-based harm (including sexual assault, intimate partner violence, and stalking).

Office for Equity, Equal Opportunity, and Title IX (EEO-TIX) - (213) 740-5086
Information about how to get help or help someone affected by harassment or discrimination, rights of protected classes, reporting options, and additional resources for students, faculty, staff, visitors, and applicants.

Reporting Incidents of Bias or Harassment - (213) 740-5086 or (213) 821-8298
Avenue to report incidents of bias, hate crimes, and microaggressions to the Office for Equity, Equal Opportunity, and Title for appropriate investigation, supportive measures, and response.

The Office of Student Accessibility Services (OSAS) - (213) 740-0776
OSAS ensures equal access for students with disabilities through providing academic accommodations and auxiliary aids in accordance with federal laws and university policy.

USC Campus Support and Intervention - (213) 740-0411
Assists students and families in resolving complex personal, financial, and academic issues adversely affecting their success as a student.

Diversity, Equity and Inclusion - (213) 740-2101
Information on events, programs and training, the Provost's Diversity and Inclusion Council, Diversity Liaisons for each academic school, chronology, participation, and various resources for students.

USC Emergency - UPC: (213) 740-4321, HSC: (323) 442-1000 – 24/7 on call
Emergency assistance and avenue to report a crime. Latest updates regarding safety, including ways in which instruction will be continued if an officially declared emergency makes travel to campus infeasible.

USC Department of Public Safety - UPC: (213) 740-6000, HSC: (323) 442-1200 – 24/7 on call
Non-emergency assistance or information.

Office of the Ombuds - (213) 821-9556 (UPC) / (323-442-0382 (HSC)

A safe and confidential place to share your USC-related issues with a University Ombuds who will work with you to explore options or paths to manage your concern.

Occupational Therapy Faculty Practice - (323) 442-2850 or otfp@med.usc.edu
Confidential Lifestyle Redesign services for USC students to support health promoting habits and routines that enhance quality of life and academic performance.