



SYLLABUS

Frontiers in Blockchain Research CSCI 4962 / CSCI 6962

4 Credit Hours | Spring 2026

Prerequisites or Other Requirements:

- None

Other Preferred Requirements:

- CSCI 2300 (Introduction to Algorithms)
- CSCI 2600 (Principles of Software)
- CSCI 4230 (Cryptography and Network Security I) or familiarity with basic cryptography
- CSCI 4510 - Distributed Systems and Algorithms

Room Location: LOW 4034

Time: Tue/Fri 2:00pm - 3:50pm ET

Course Website: <https://cs.rpi.edu/academics/courses/spring26/csci4962>

Submitty: <https://submitty.cs.rpi.edu/courses/s26/csci4962>

WebEx Space: "Frontiers in Blockchain Research - Spring 2026"
<https://eurl.io/#-gJShBLpd> (please use your rpi.edu email address to join)

INSTRUCTOR

Name: Oshani Seneviratne

Email Address: senevo@rpi.edu

Office Hour: Fri 12 pm – 1 pm ET

Office Location: Lally 306

TEACHING ASSISTANT

Name: Jui Chien Lin

Email Address: linj26@rpi.edu

Office Hour: Mon 12 pm – 1 pm ET

Office Location: Library (exact location announced via WebEx space)

MENTOR

Name: Caleb Carr

Email Address: carrc4@rpi.edu

Office Hour: Wed 4 pm – 5 pm ET

Office Location: Library (exact location announced via WebEx space)

COURSE DESCRIPTION:

Frontiers in Blockchain Research is an advanced seminar course that explores the theoretical foundations, system architectures, and emerging research directions of blockchain and decentralized ledger technologies. The course examines seminal and influential works on consensus protocols, cryptography, smart contracts, and decentralized governance, alongside cutting-edge research on scalability, privacy-preserving computation, interoperability, decentralized finance (DeFi), and Web3 ecosystems. Through critical reading, student-led discussions, and research presentations, participants will analyze open challenges at the intersection of distributed systems, cryptography, economics, and socio-technical systems, and engage with current debates shaping the future of decentralized infrastructures.

Students may not receive credit for both the 4000 level and 6000 level versions of this course.

COURSE GOALS/OBJECTIVES

By the end of this course, students will be able to:

- 1. Understand foundational blockchain principles**
 - Analyze the core concepts underlying blockchain systems, including distributed consensus, cryptographic primitives, immutability, and trust minimization, as established by seminal research.
- 2. Critically evaluate blockchain protocols and architectures**
 - Compare and critique major blockchain designs (e.g., Proof-of-Work, Proof-of-Stake, BFT-style consensus, Layer-2 systems) with respect to security, scalability, decentralization, and real-world deployment constraints.
- 3. Assess security, privacy, and cryptographic guarantees**
 - Evaluate formal security models, attack vectors, and privacy-preserving techniques such as zero-knowledge proofs, secure multiparty computation, and cryptoeconomic incentives.
- 4. Examine programmability and smart contract systems**
 - Understand smart contract execution models, formal verification approaches, and common sources of vulnerabilities, and assess their implications for decentralized applications.
- 5. Analyze economic, governance, and socio-technical dimensions**
 - Investigate how incentives, governance mechanisms, regulatory pressures, and human behavior shape the stability and evolution of blockchain ecosystems.
- 6. Engage with cutting-edge research and open problems**
 - Read, present, and critique recent blockchain research papers, identifying limitations, open challenges, and promising future research directions.
- 7. [6000 level] Develop independent research skills**
 - Formulate research questions, synthesize insights across multiple papers, and communicate technical arguments clearly through written critiques and oral presentations.

STUDENT LEARNING OUTCOMES

- 1. Foundations:** Explain the core principles of blockchain systems and how they relate to seminal research.
- 2. Protocol Analysis:** Compare and evaluate major blockchain architectures (PoW, PoS, BFT-style consensus, Layer-2 scaling) using clear criteria such as security, scalability, decentralization, and real-world constraints.
- 3. Security & Privacy Reasoning:** Assess security threats and privacy mechanisms in blockchain systems (e.g., smart contract vulnerabilities, incentive attacks, ZK proofs/formal methods) and argue about trade-offs and mitigations.
- 4. Research Literacy & Communication:** Critically read and synthesize blockchain research papers, leading scholarly discussions and communicating technical insights effectively in presentations and written critiques.
- 5. [6000 level] Research Paper Writing:** Develop a publication-style research artifact (e.g., a workshop-ready paper, short research paper, or structured research

proposal) that identifies a gap in the literature, motivates a contribution, and presents a coherent methodology and evaluation plan grounded in prior work.

Course (Student) Learning Outcomes Assessment Measures:

1. Students will be assessed on in-class presentations, class participation, and a small research project.
2. [6000 level] Graduate students are expected to compile a research paper by the end of the course.

COURSE ASSESSMENT MEASURES & GRADING CRITERIA

Students taking a 6000-level course, regardless of student status (i.e., Undergraduate or Graduate), must satisfy the learning outcomes at the 6000 level if they expect to receive graduate credit for the course.

4000 Level:

Paper Presentations: 30%
In-class Participation: 20%
Project: 50%

6000 Level:

Paper Presentations: 20%
In-class Participation: 20%
Project: 40%
Paper: 20%

Grade – letter scale:

93% + is an A;
90%-92% is an A-
87%-89% is a B+
83%-86% is a B
80%-82% is a B-
77%-79% is a C+
73%-76% is a C
70%-72% is a C-
65%-69% is a *D+
60%-64% is a *D
0%-59% is an F.

*Note: Students taking the course at the 6000 level cannot receive a D+/D grade.

ACADEMIC INTEGRITY

Student-teacher relationships are built on trust. For example, students must trust that teachers have made appropriate decisions about the structure and content of the courses they teach, and teachers must trust that the assignments that students turn in are their own. Acts that violate this trust undermine the educational process.

The Rensselaer Handbook of Student Rights and Responsibilities and the Graduate Student Supplement (For 4000 level and above courses) define various forms of Academic Dishonesty, and you should make yourself familiar with these. In this class, all assignments that are turned in for a grade must represent the student's own work. In cases where help was received or teamwork was allowed, a notation on the assignment should indicate your collaboration.

Every student will be doing different work in this class. Teams can and should work together. Students will be asked to present their unique contributions in their project notebooks and team breakouts. Students should fairly represent their own work, and misrepresenting others' work as your own could be a violation of academic integrity. Team members found to not be contributing their fair share of the workload will be counseled, and if the problem persists, they will be given a low or failing grade for the work segment or segments involved.

Submission of any assignment that is in violation of this policy will result in (1) an academic (grade) penalty and (2) reporting to the Associate Dean of Academic Affairs and either the Dean of Students (for Undergraduates) or the Dean of Graduate Education (for Graduate students).

In this course, the academic penalty for a first offense is zero grade for the relevant portion of the grade. A second offense will result in failure of the course.

If you have any questions concerning this policy before submitting an assignment, please ask for clarification.

ETHICS STATEMENT

This course touches on some aspects of cybersecurity. As such, we will discuss several attack techniques and scenarios from the point of view of an attacker. It is unethical to use such techniques to compromise the security of others. This course is also partially about privacy techniques and cryptocurrencies. This is a rapidly evolving area where laws, regulations, U.S. export restrictions, and policies apply.

Furthermore, the assignments in this course only require you to use test blockchain networks, and no "real" money is involved. Do not intentionally create smart contracts that harm other users. It is your responsibility not to run afoul of laws, regulations, or ethical standards. If in doubt, please get in touch with the instructor.

Some guidelines:

- Only use test networks for your blockchain code experimentation. Nothing required from you in class involves real money.
- Do not interfere with the operation of existing computer networks. Read the Computer Fraud and Abuse Act (<https://www.law.cornell.edu/uscode/text/18/1030>).

OTHER COURSE-SPECIFIC INFORMATION

You should bring your laptop or mobile device to class (but it must be on silent). We use real-world collaboration, coding, and project management tools essential for highly effective group work. When laptops are required, the only programs and tabs that should be open are the ones relevant to the class (e.g., Outlook, Slack, Discord, various games etc., should not be open).

WebEx: Through experience with projects and classes, we have found that online chats are a highly effective way to get answers quickly and collaborate with team members across different locations and times. Online communication for this course will be done primarily on WebEx. You should install the WebEx app. Please use the link above in the course description to join the team.

Metamask Wallet: Please have a developer-friendly web browser, such as Chrome, installed on your computer. We will be installing a web browser extension called MetaMask. Please do not install it until you get detailed instructions from me.

GitHub: We will use GitHub to capture teamwork to enable the development of research and applications for the project. Each project will have its own GitHub repository.

ACADEMIC ACCOMMODATIONS

Rensselaer Polytechnic Institute strives to make all learning experiences as accessible as possible. If you anticipate or experience academic barriers based on a disability, please let me know immediately so that we can discuss your options.

To establish reasonable accommodations, please register with The Office of Disability Services for Students (<mailto:dss@rpi.edu>; 518-276-8197; 4226 Academy Hall). After registration, make arrangements with me as soon as possible to discuss your accommodations so that they may be implemented in a timely fashion.