SYLLABUS

Decentralized AI CSCI 4190/ CSCI 6190

4 Credit Hours | Spring 2026

Prerequisites or Other Requirements:

- CSCI 2300 (Introduction to Algorithms)
- CSCI 2600 (Principles of Software)

Other Preferred Requirements:

- CSCI 4100 (Machine Learning from Data) or CSCI 4150 (Introduction to Artificial Intelligence) or familiarity with basic machine learning algorithms
- CSCI 4230 (Cryptography and Network Security I) or familiarity with basic cryptography

Room Location: Lally 104

Time: Tue/Fri 10:00am - 11:50am ET

Course Website: https://cs.rpi.edu/academics/courses/spring26/csci4190

Submitty: https://submitty.cs.rpi.edu/courses/s26/csci4190

WebEx Space: Please go to https://eurl.io/#x1aS4tMMB join the "Decentralized AI - Spring 2026" WebEx Space

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:

This course explores the design, implementation, and governance of Decentralized Artificial Intelligence (AI) systems that operate without centralized control over data, compute, or decision-making. As modern AI increasingly relies on centralized data monopolies and opaque infrastructures, this course examines alternative architectures that emphasize data sovereignty, privacy preservation, verifiable computation, and permissionless innovation.

Students will study the technical foundations of decentralization, including blockchain systems, smart contracts, decentralized storage, oracles, and zero-knowledge proofs, alongside core AI paradigms such as federated learning, privacy-preserving machine learning, decentralized inference, and autonomous agents. The course integrates blockchain programming with Solidity, smart contract security, and incentive design with advanced topics like zero-knowledge machine learning (ZKML), decentralized knowledge graphs, and agent-to-agent economies.

Through lectures and a substantial group project, students will design and evaluate decentralized AI applications spanning Decentralized Finance, Decentralized Science, content provenance, and AI governance via DAOs. By the end of the course, students will be equipped to critically assess decentralization claims, reason about trade-offs in performance and trust, and architect AI systems that align technical rigor with ethical and societal considerations.

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

REQUIRED TEXT(S):

Refer to the Reading/ Assignment/ Reference list for each week in the course material.

COURSE GOALS/OBJECTIVES

1. Students will identify and explain relevant tools and techniques in decentralized AI.
2. Students will demonstrate critical thinking skills and a solid technical foundation in decentralized AI model-driven decision-making.
3. Students will apply and design novel solutions using decentralized AI techniques to formulate and solve real-world problems.
4. [6000 level]: Critique the existing research at the intersection of decentralized AI and blockchain/web3 technologies.
5. [6000 level]: Develop and demonstrate advanced academic research communication skills by preparing and formatting a final project report suitable for submission to a relevant conference or journal. This includes effectively presenting research findings, adhering to academic standards, and utilizing proper citation and formatting techniques.

STUDENT LEARNING OUTCOMES

1. **Understand** the fundamental concepts and principles of decentralized AI systems.
2. **Analyze** the differences between centralized and decentralized AI approaches.
3. **Design** federated learning systems for distributed data scenarios.
4. **Implement** privacy-preserving AI techniques and algorithms.
5. **Evaluate** the trade-offs between performance, privacy, and decentralization.
6. **Apply** blockchain technologies to AI applications.
7. [6000 level]: **Critically** assess current research and developments in the field.

Course (Student) Learning Outcomes Assessment Measures:

1. Students will be assessed on written assignments, programming labs, and the group project.
2. The programming assignments will equip the students with the foundation to build robust applications that leverage decentralized AI technologies.
3. The group project will utilize decentralized AI techniques to solve a real-world problem and advance the state-of-the-art.

COURSE CALENDAR

This is a tentative calendar, and it is subject to change. Students should consult the online course materials for the latest course calendar.

- Week 1: **Motivation & the Centralization Problem**
  - (01) Jan 13: Course Introduction and Decentralized AI Stack
  - (02) Jan 16: Blockchain History
- Week 2: **Blockchain Foundations & History**
  - (03) Jan 20: Blockchain Technology Overview
  - (04) Jan 23: Blockchain Applications and Limitations
- Week 3: **Blockchain Technical Deep Dive**
  - (05) Jan 27: Blockchain Programming
  - (06) Jan 30: Solidity Introduction

- Week 4: **Smart Contracts & Solidity**
  - (07) Feb 03: Solidity Deep Dive
  - (08) Feb 06: Securing Smart Contracts
- Week 5: **External Knowledge for Decentralized AI**
  - (09) Feb 10: Decentralized Knowledge Graphs
  - (10) Feb 13: Oracles
- Week 6: **Decentralized Compute & Storage**
  - Feb 17: *No class (Monday Schedule)*
  - (11) Feb 20: DePIN and IPFS
- Week 7: **Secure and Private AI**
  - (12) Feb 24: Federated Learning
  - (13) Feb 27: Differential Privacy
- Week 8
  - (14) Mar 03: *No Class (Spring Break)*
  - (15) Mar 06: *No Class (Spring Break)*
- Week 9: **Zero-Knowledge Proofs & ZKML**
  - Mar 10: Zero-Knowledge Proofs
  - Mar 13: Zero-Knowledge Machine Learning (ZKML)
- Week 10: **Agentic Web, Federated LLMs, DeFi & DeSci**
  - Mar 17: Autonomous Agents & Federated LLMs
  - Mar 20: DAOs for AI Governance, DeFi and DeSci

Group Project Work

- Week 11
  - Mar 24: Project Idea Presentation and Group Selection
  - (16) Mar 27: Initial Project Pitches
- Week 12
  - Mar 31: Project Check-in #1 + Group Work
  - (17) Apr 03: **Incentives & Tokenomics** + Group Work
- Week 13
  - Apr 07: Project Check-in #2 + Group Work
  - (18) Apr 10: **Provenance & Authenticity** + Group Work
- Week 14
  - Apr 14: Project Check-in #3 + Group Work
  - (19) Apr 17: **Scaling, Ethics, Governance & Regulation** + Group Work
- Week 15
  - Apr 21: Project Check-in #4 + Group Work
  - Apr 24: Group Work + Report/Publication Preparation
- Week 16
  - (20) Apr 28: Final Project Presentations

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:
Homeworks: 10%
Labs: 10%
In-Class Quizzes: 40%
Project Check-ins: 15%
Project Deliverables: 25%

6000 Level:
Homeworks (includes additional advanced questions): 15%
Labs: 10%
In-Class Quizzes: 30%
Project Check-ins: 15%
Project Deliverables (includes literature review): 30%

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.

LATE SUBMISSION POLICY

We will deduct 20% per day for late submissions on all the individual assignment submissions. Final project-related deliverables will need to be submitted on the specified due date/time, given the dynamic and group nature of the deliverable. Answers to the in-class quizzes must be submitted during class time, and the instructor will allow 10-15 mins for everyone in the class to complete the quiz. Please see the attendance policy below for more information about the class quizzes.

ATTENDANCE POLICY

In-person participation is mandatory during both lectures, lab, and project sessions. Attendance will be taken each day/session. Students are responsible for submitting an electronic form provided by the instructor before the end of the class.

Each day the class is in session, there will be a short quiz, which should not take more than 15 minutes to complete. These quizzes will be based on the assigned readings for the class that day and the previous class content. **No other resources as well as generative AI tools will be allowed.** The top 80% of the scores from these quizzes will be counted in the final course grade on quizzes, which means that the students must attend at least 80% of the in-person lectures and answer the quiz correctly to obtain the full score for quizzes (worth 40% of the final 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 final group project. Each project will have its own public GitHub repository under the following GitHub organization: https://github.com/RPI-DecentralizedAI. If, for some reason, you prefer not to be part of a public GitHub repository for the group project, please communicate that to the instructor before the group projects commence.

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.