RPI

Decentralized AI

Course Introduction

Class 01

Jan 13, 2026

Oshani Seneviratne

Assistant Professor

Department of Computer Science

Rensselaer Polytechnic Institute, Troy NY USA

RPI

Course Team

INSTRUCTOR

Name: Oshani Seneviratne

Email: senevo@rpi.edu

Office Hour: Fri 12 pm – 1 pm ET

Office Location: Lally 306

TEACHING ASSISTANT

Name: Jui Chien Lin

Email: 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: carrc4@rpi.edu

Office Hour: Wed 4 pm – 5 pm ET

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

RPI

Class Logistics

- **Prerequisites:**
  - 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
  - Lecture material are posted here
- **Submitty:** https://submitty.cs.rpi.edu/courses/s26/csci4190
- **WebEx Space:** "Decentralized AI - Spring 2026"
  - https://eurl.io/#x1aS4tMMB (please use your rpi.edu email address to join)

Class Logistics

- **Textbooks:** None, but please refer to the reading list at the end of each lecture.

- **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 GitHub repository under the following GitHub organization: https://github.com/RPI-DecentralizedAI

RPI

Course Goals & Objectives

1. **Identify and explain relevant tools and techniques**

   Students will identify and explain relevant tools and techniques in decentralized AI.

2. **Demonstrate critical thinking skills**

   Students will demonstrate critical thinking skills and a solid technical foundation in decentralized AI model-driven decision-making.

3. **Apply and design novel solutions**

   Students will apply and design novel solutions using decentralized AI techniques to formulate and solve real-world problems.

4. **[6000 level]: Critique existing research**

   [6000 level]: Critique the existing research at the intersection of decentralized AI and blockchain/web3 technologies.

5. **[6000 level]: Develop research communication skills**

   [6000 level]: Develop and demonstrate advanced academic research communication skills by preparing and formatting a final project report suitable for submission to suitable for submission to a relevant conference or journal.

RPI

Learning Outcomes and Assessment Measures

Learning Outcomes

1. Understand the **fundamental concepts and principles** of decentralized decentralized AI systems.
2. Analyze the **differences between centralized and decentralized AI decentralized AI** approaches.
3. Design **federated learning systems** for **distributed data** scenarios.
4. Implement **privacy-preserving A**I 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 **developments** in the field.

Assessment Measures

1. Students will be assessed on, **written assignments, programming labs**, **in-class quizzes**, 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**.

RPI

Course Assessment & Grading

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%

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.

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 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.

RPI

Course Policies

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 should not take more than 15 minutes to complete. These quizzes will be will be based on the assigned readings for the class that day and the previous the previous class content. No other resources as well as generative AI tools generative AI tools will be allowed. The **top 80% of the scores** from these from these quizzes will be counted in the final course grade on quizzes, quizzes, which means that the students must attend at least 80% of the in- of the in-person lectures and answer the quiz correctly to obtain the full 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) above courses) define various forms of Academic Dishonesty, and you should make yourself familiar with these. In this class, all assignments that 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 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 their unique contributions in their project notebooks and team breakouts. Students should fairly represent their own work, and misrepresenting and misrepresenting others' work as your own could be a violation of academic integrity. Team members found to not be contributing their fair 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 grade for the work segment or segments involved.

- **Penalties:** 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.

RPI

Other Course-Specific Information

Laptops & Devices

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 and applications for the final group project. Each project will have its own public GitHub GitHub repository under the following GitHub organization: **https://github.com/RPI-https://github.com/RPI-DecentralizedAI**. If, for some reason, you prefer not to be part of a be part of a public GitHub repository for the group project, please communicate that to the that to the instructor before the group projects commence.

Ethics Statement

- This course touches on several aspects of cybersecurity.
  - It is unethical to use techniques that we will be discussing in class to compromise the security of others.
- This course is has lectures and a lab on digital cryptocurrencies.
  - This is a rapidly evolving area where laws, regulations, and policies apply.
- 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, such as the public Sepolia or Goreli 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).

Software we will be using

- WebEx
  - Install the WebEx app and join the course WebEx space (please use your rpi.edu email address to join)
  - We will be using this space for general class chatter, to debug things, discuss research, and coordinate class projects.
- Metamask Wallet
  - Please have Chrome (or another developer-friendly browser) installed on your computer.
  - We will be installing a Chrome extension called MetaMask.
- Machine Learning Computational Cluster
  - The IDEA computational cluster will be available for the final class projects.
- Git
  - We will be using GitHub for the project work.

RPI

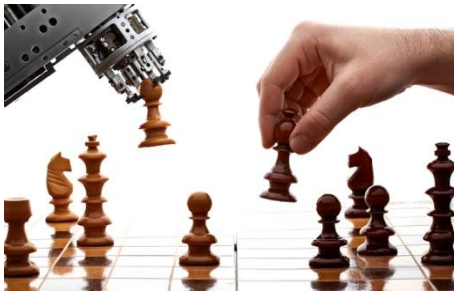
Attendance Policy

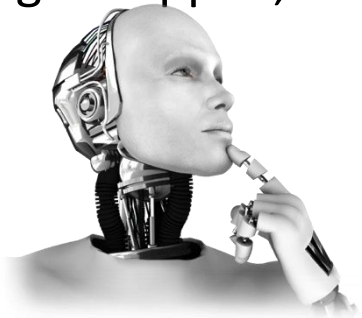
- In-person participation is **mandatory** during both lectures, lab, and project sessions.
- Students are responsible for completing the quiz which doubles as the ”attendance sheet” before the end of the class.
- The in-class quiz score accounts for 40% of your grade!
  - We will only count the top 80% of the scores you receive throughout the course.

RPI

What is artificial intelligence (AI)?

- Simulation of intelligence properties in machines
- The science of making intelligent machines through intelligent software
- The study and making of machines that mimic human thinking and goes beyond what humans are capable of doing
- Ability to use massive computing power to address certain situations, predict what might happen, and proactively do something about it





RPI

Why Decentralization?

To understand our motivation, we must first examine why decentralization matters in the context of modern AI.

Data Locality

Keep data with its rightful owners to prevent mass surveillance and unauthorized leakage.

Transparent Provenance

Immutable audit trails ensure we know exactly where data comes from and how models are trained.

Auditable Collaboration

Trust is established through open code and cryptographic verification rather than brand reputation.

Incentive Alignment

Create fair reward mechanisms that properly compensate data contributors and model builders.

RPI

Privacy: From Data Hoarding to Local Compute

Data Minimization & Federated Compute

Instead of hoarding raw data in central servers, we push computation to where data resides. This ensures sensitive information never leaves the local device, significantly reducing the attack surface.

Differential Privacy & Governance

Mathematical noise is added to updates to prevent reverse-engineering of individual records. Consent is managed via smart contracts, giving users granular, programmable control over who accesses their data.

Can you give an example where decentralized learning is useful?

RPI

Bias & Fairness: Transparent Provenance

Diverse Data Contribution

Decentralized networks incentivize a wider range of data providers, reducing demographic blind spots. This helps mitigate the bias often inherent in centralized, homogenous datasets.

On-Chain Audit Trails

Every model update is cryptographically signed and logged on-chain. This creates an immutable history of who contributed what and when, ensuring full accountability for the model's evolution.

Community-Driven Evaluation

Models are evaluated by a distributed network of peers rather than a single authority. This crowdsourced benchmarking helps identify bias earlier and more effectively.

Can you give an example where transparent provenance in AI is useful?

RPI

Decentralized AI Technology Overview

Blockchain Layer
Trust
Provenance, Incentives, and Governance

Federated Learning
Privacy
Distributed Training without data sharing

ZKML
Verification
Verifiable Inference and Proofs

RPI

Tentative Course Calendar (1)

- 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

RPI

Tentative Course Calendar (2)

- 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

RPI

Tentative Course Calendar (3)

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

RPI

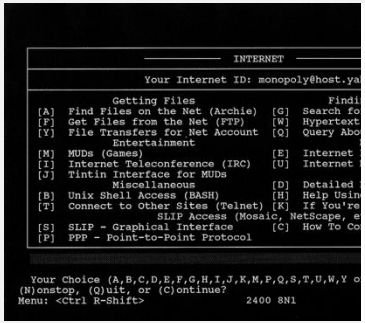
Quick Introductions

- Name
- Major
- Level (4000/6000)
- Why are you interested in this course?

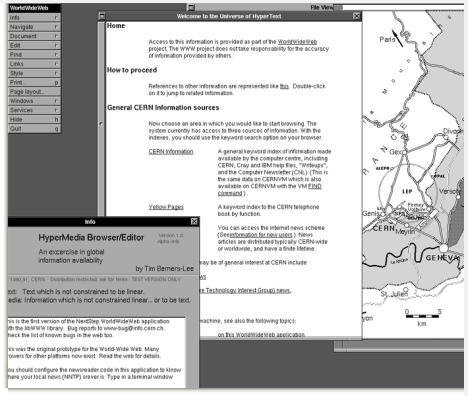
Two Successful "Projects"

Web (1989)

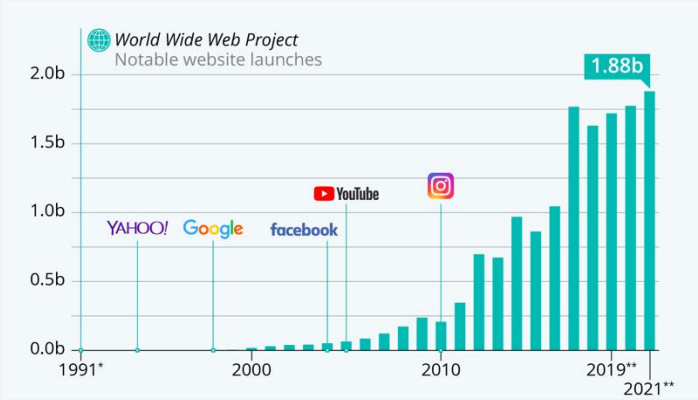
Early Browsers



Web Applications

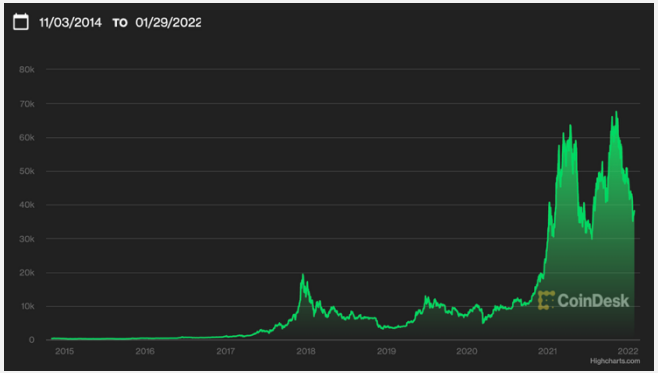


Website Registrations



Blockchain (2008)

Bitcoin Valuation



Blockchain Applications

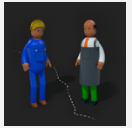

Banking


Supply chain

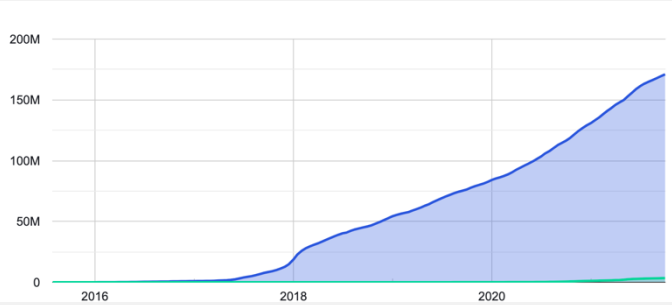

Health care


Voting


Insurance


Property records

Ethereum Addresses

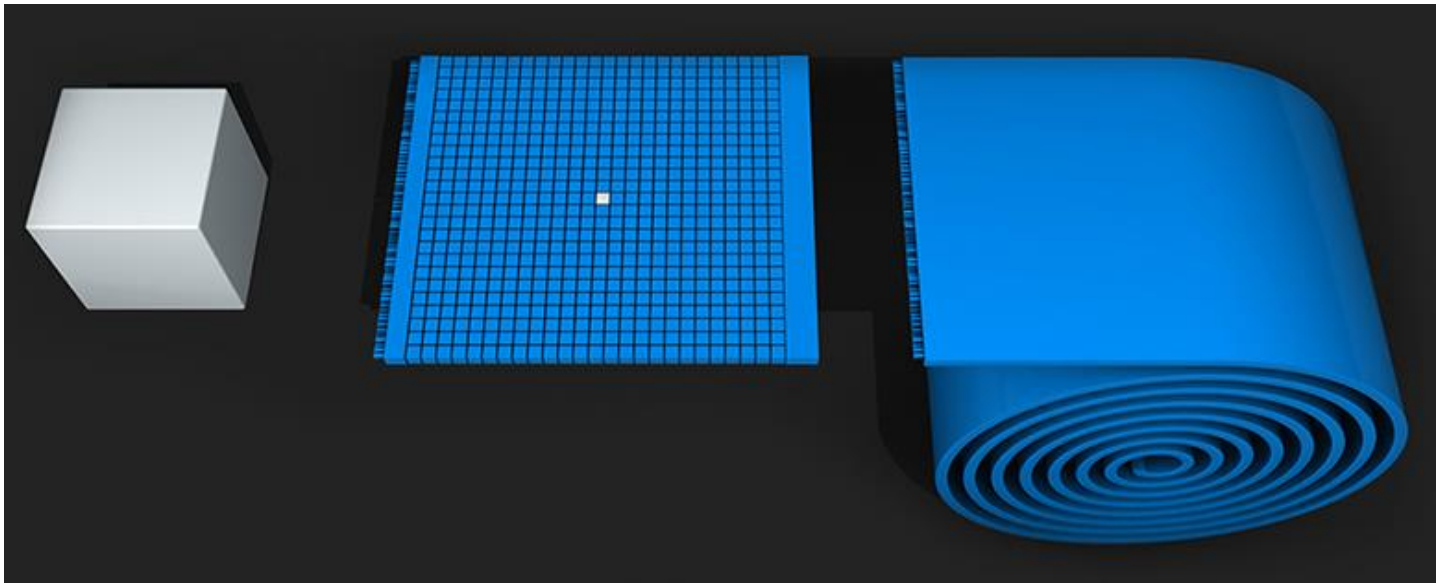


RPI

Blockchain Building Blocks

RPI

The Parts



THE RECORD
Can contain anything

THE BLOCK
A bundle of records

THE CHAIN
All the blocks linked together

Source: http://graphics.reuters.com/TECHNOLOGY-BLOCKCHAIN/010070P11GN/index.html

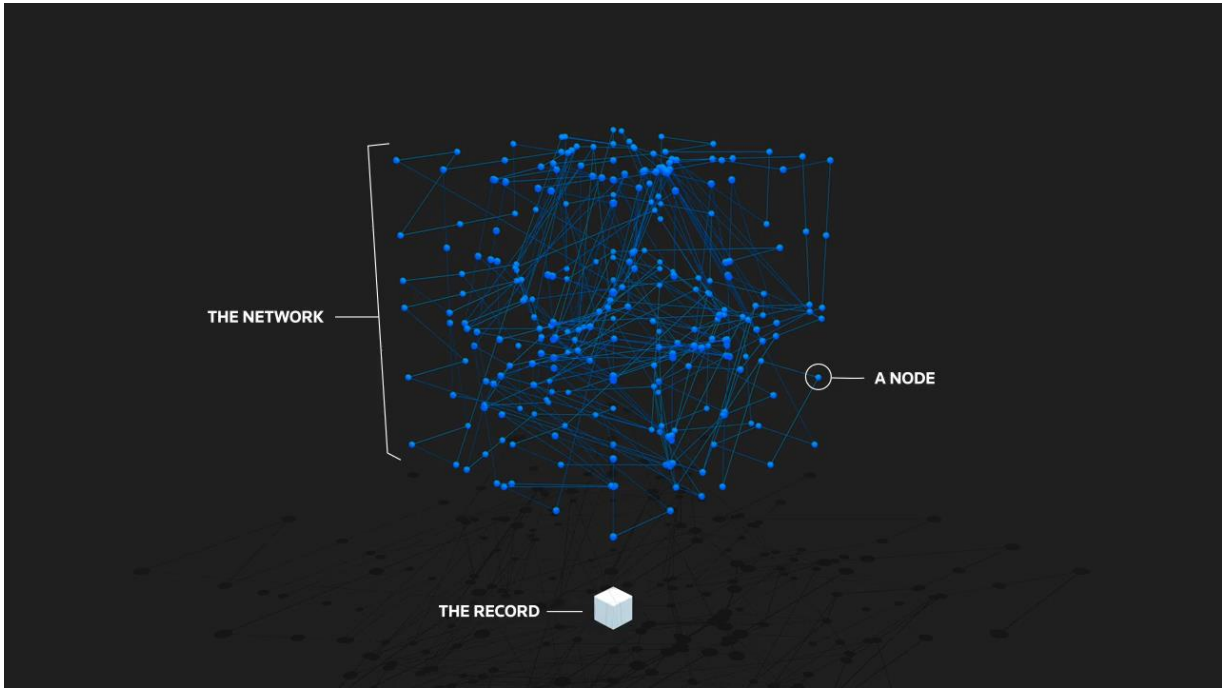
RPI

Step 1: Transaction

Source: http://graphics.reuters.com/TECHNOLOGY-BLOCKCHAIN/010070P11GN/index.html

RPI

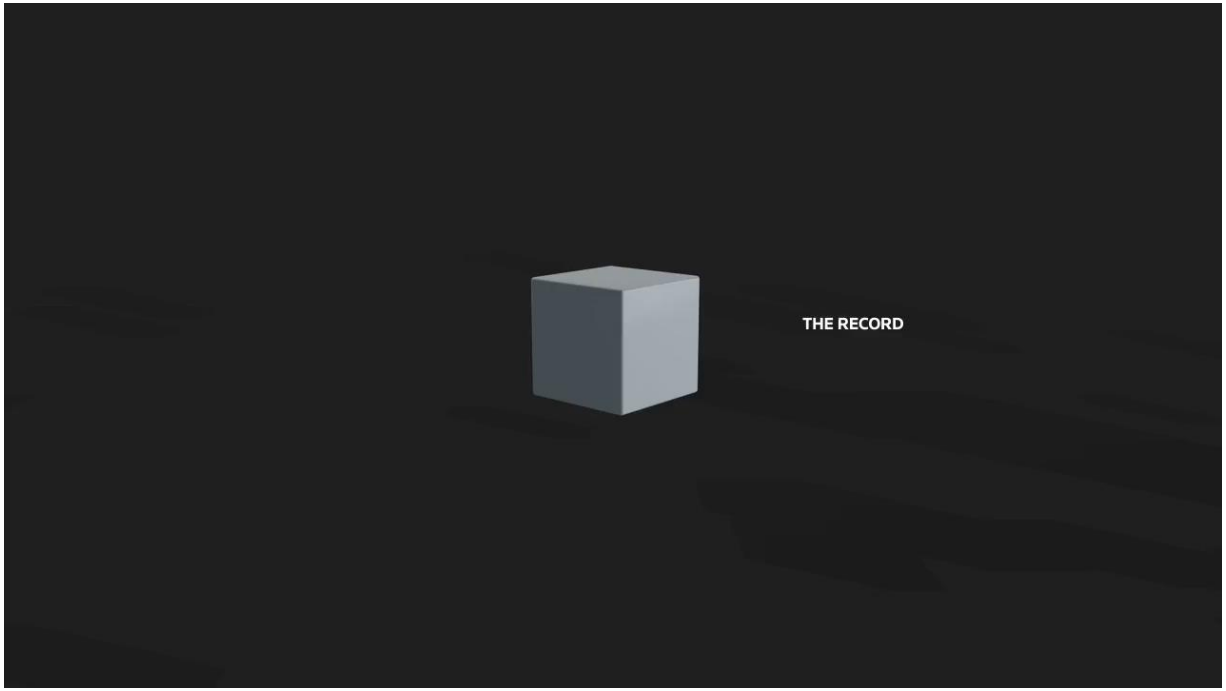
Step 2: Distributed Consensus



Source: http://graphics.reuters.com/TECHNOLOGY-BLOCKCHAIN/010070P11GN/index.html

RPI

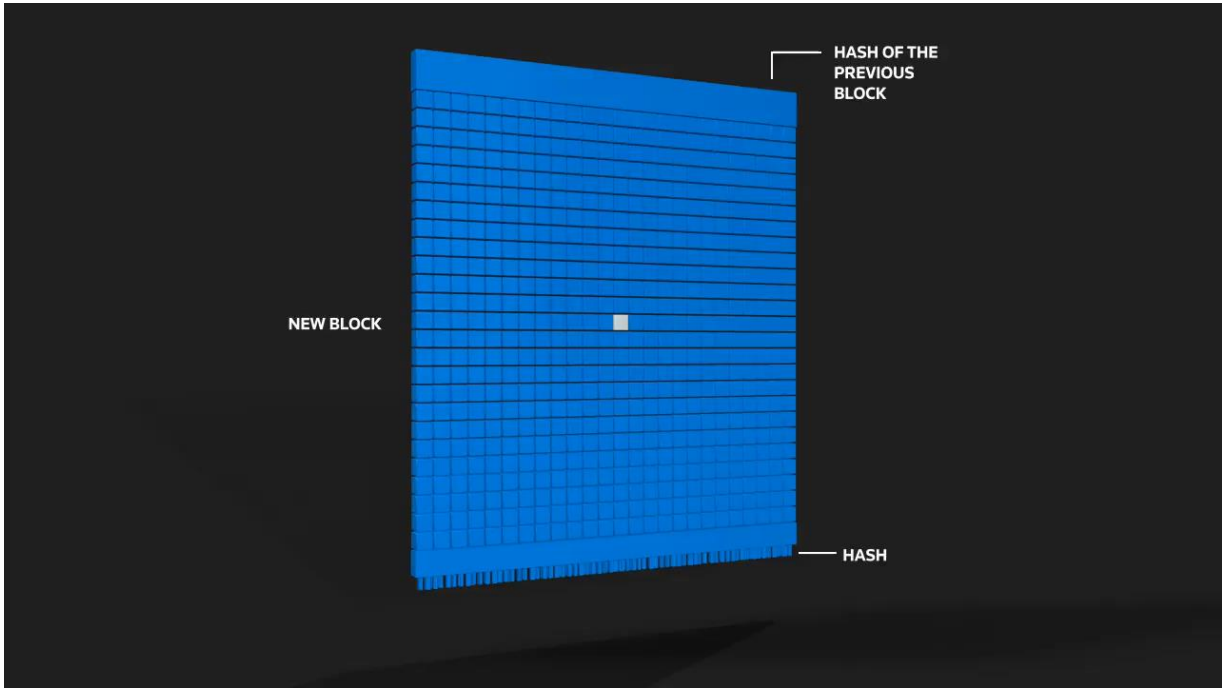
Step 3: Block Creation



Source: http://graphics.reuters.com/TECHNOLOGY-BLOCKCHAIN/010070P11GN/index.html

RPI

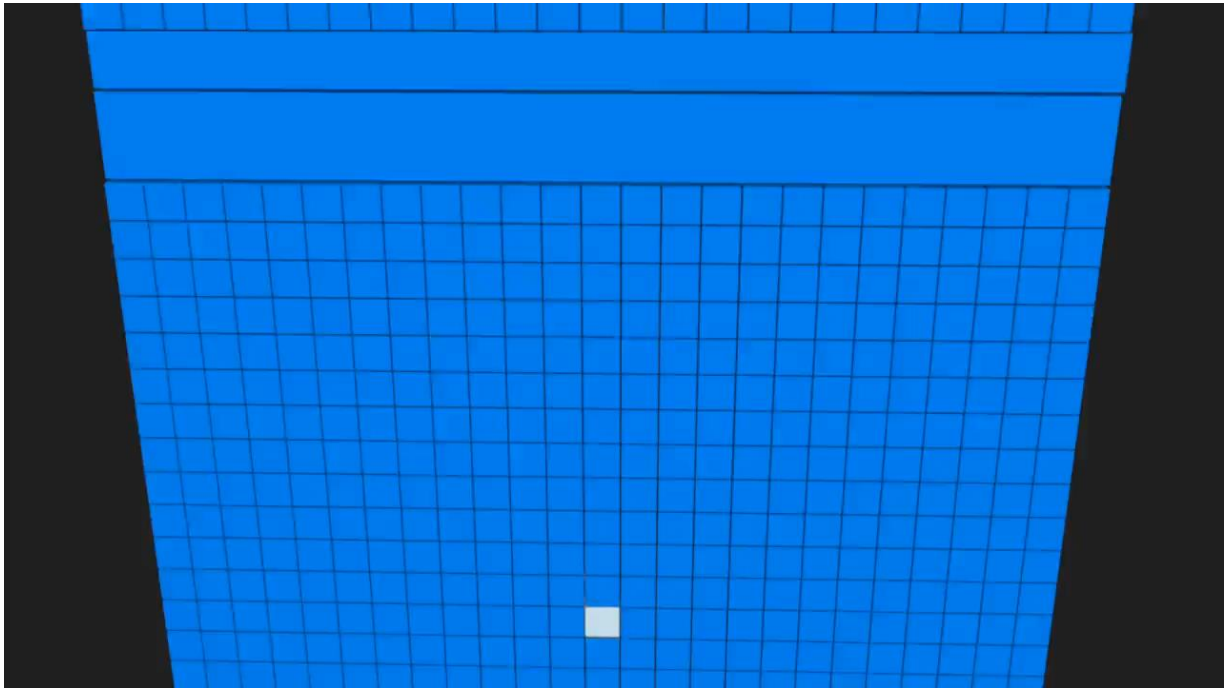
Step 4: Adding the block to the blockchain



Source: http://graphics.reuters.com/TECHNOLOGY-BLOCKCHAIN/010070P11GN/index.html

RPI

A Transaction in a committed block is difficult to change

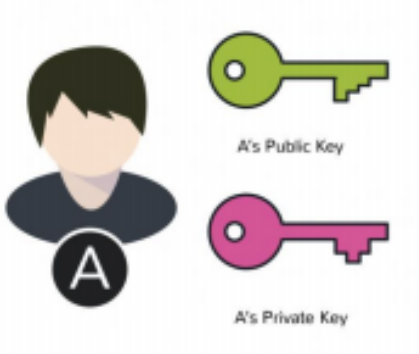


Source: http://graphics.reuters.com/TECHNOLOGY-BLOCKCHAIN/010070P11GN/index.html

RPI

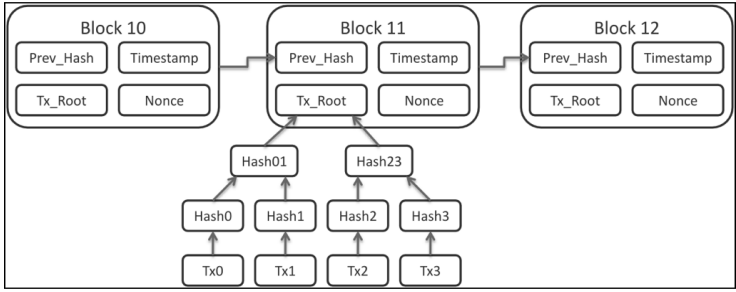
Blockchain != Cryptocurrency

- Cryptocurrency is an application that sits on top of a blockchain.
- **This course is not about cryptocurrencies!**
- We analyze technologies like the following and how they interface with AI.
- However, we should learn from the success of the most prominent (and successful blockchain application, i.e., cryptocurrencies.



Cryptographic Hashes and Identities

Consensus Protocol



Ledger aka “Chain”

RPI

Blockchain Pillars

- **Authenticity (cryptographic)**: creates transactions that are impervious to fraud through the use of digital signatures, establishing a shared truth
- **Shared**: the more entities participating in the blockchain, the more value it brings
- **Distributed**: many replicas of the blockchain database, making it more fault-tolerant
- **Ledger**: read/write once database maintaining an immutable record of every transaction

RPI

Blockchain Hype?

- Blockchains are largely based on **well-established** and **understood** technologies:
  - cryptography,
  - distributed databases and networks,
  - peer-to-peer,
  - discovery and network protocols, etc.
- It's the **composite** of these technologies that creates a big impact and disruption across all industries (starting in financial services)
- Initial designs (**bitcoin**) proved to be **resilient**.
- **Smart contracts** showed the real potential for blockchain in **securely transferring value** and creating future **binding contracts** in a **trustless environment.**

RPI

Disruptive Effect of Blockchain

- Removing middleman processes makes things more efficient and cost-effective
- Peer-to-peer value exchange reduces centralized control
- One ledger instead of comparing multiple ledgers
- More collaborative economy – shared costs, risks, etc.
- Dramatic changes in how identity is defined and controlled

RPI

Why study blockchain? Why now?

- Blockchain technology has:
  - created an industry worth trillions of dollars
  - launched a wave of innovation in distributed systems, cryptography, privacy, security, and economics
- Two views:
  - Some believe that blockchains will be **integral to the future of money**, **governments, and the Internet**.
  - Others claim that this is a **transient bubble** and cryptocurrencies will be relegated to a footnote in history.

Minting money out of thin air?

- To create a free-floating digital currency that is likely to acquire real value, you need to have something that's **scarce by design** (gold or diamonds)
- In the digital realm, one way to achieve scarcity is to design the system so that minting money requires **solving a computational problem** (or "puzzle") that takes a while to crack
- This idea has been around since the early 90's: first to solve email spam (**Hashcash**)
  - To enforce this requirement, the recipient's email program would simply ignore your email if you didn't attach the solution to the computational puzzle.
  - For the average user, it wouldn't be that much of a barrier to sending emails because you're not sending emails very frequently.
  - But if you're a spammer, you're trying to send out thousands or millions of emails all at once, and solving those computational puzzles could become prohibitive!

RPI

What is Money? An Artist's Make and Take

https://www.wsj.com/video/what-is-money-an-artists-make-and-take/DAC445B2-B01C-42ED-B928-91E5E7FC3BA3.html

RPI

Exchanging Goods and Services: Bartering

Is it possible for both you and your friend to get what you want by bartering?

A. No, it's not possible to give up your apple to receive the cookie.
B. Only if your friend is willing to compromise.
C. Yes, but it requires a third person with different snacks and preferences.

RPI

What is the role of money?

If your friend thinks that trading you her cookie in exchange for one dollar is a good deal for her, what is she assuming?

A. The cookie is worth exactly one dollar to her — no more, no less.

B. She'll be able to use the dollar to buy something else she wants later.

C. The paper bill can directly meet her wants and needs.

D. All of the above

RPI

Precious Metals (or “Gold 1.0”) as Money

- They don’t degrade over time.
- They’re rare enough that it takes a lot of work to find more.
- They’re common enough that it's possible to find more.
- The amounts that most people would have are easy to carry around.
- Precious metals don’t meet a basic need.

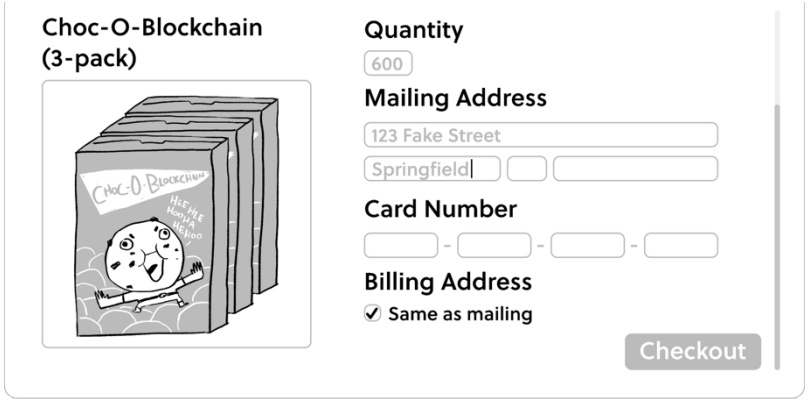
Source: https://spectrum.ieee.org/at-work/innovation/a-brief-history-of-money

RPI

Credit

- You don't even need to trade gold coins or pieces of fancy paper (i.e., cash) for goods, you also have the option to trade a **promise** that you'll pay the person back later.
- Why might someone be hesitant to accept credit as payment rather than cash?

- What is one downside to using credit cards when shopping online?
  - A. You need to have a lot of cash on hand to use a credit card
  - B. You have to share your credit card number.
  - C. It takes a long time for your payment info to go through.
  - D. There are no downsides



Reading Assignment for Next Class

Bitcoin and Cryptocurrency Technologies by Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller, Steven Goldfeder

https://d28rh4a8wq0iu5.cloudfront.net/bitcointech/readings/princeton_bitcoin_book.pdf (pre-print version of the book)

Please read the **Preface – The Long Road to Bitcoin (pages 3-21)**

The next class's quiz will be based on these contents.

RPI

Any Questions?