SI 486I: Randomized and Blockchain Technology

Course Policy, Spring AY2022

Instructors:

- Assoc. Prof. Daniel S. Roche, 438 Hopper Hall, x36814, roche@usna.edu (Coordinator).
- Assoc. Prof. Jacek A. Rothert, 370 Michelson Hall, x36889, rothert@usna.edu (Frequent guest lecturer on economics topics).

Course Description: This course will provide an overview of the technical foundations and economic implications of distributed cryptographic blockchains, including distributed ledgers, cryptocurrencies, non-fungible tokens, smart contracts, and decentralized applications. Students will gain an understanding of underlying cryptographic tools such as random nonces, cryptographic hashes, Merkle trees, signature schemes, zero-knowledge proofs, and consensus mechanisms including proof of work and proof of stake. A keen understanding of computational randomness will be developed to both construct these primitives and to analyze the probability that their guarantees can be violated. This technical knowledge will be integrated with economic understanding of the context in which blockchains are used and the basics of decentralized finance, as well as the societal and ethical implications of how cryptocurrencies and decentralized applications can disrupt markets and circumvent government regulations. Course projects and labs will involve both programming and research, and will include tasks such as creating a simple cryptocurrency, writing a smart contract for the Ethereum network, and investigating the features and implications of emerging coins, tokens, or networks.

Credits: 2-2-3

Learning Objectives:

1. Apply knowledge of cryptographic hashing, digital signatures, and concensus mechanisms to build and operate a node on a mock decentralized currency network.
2. Write simple smart contracts to extend the functionality of a distributed ledger.
3. Understand the role of digital and fiat currency in the economy and the potential applications for decentralized finance.

Student Outcomes: Graduates of the program will have an ability to:

1. **Analysis.** Analyze a complex computing problem and to apply principles of computing and other relevant disciplines to identify solutions.
2. **Implementation.** Design, implement, and evaluate a computing-based solution to meet a given set of computing requirements in the context of the program's discipline.
3. **Communication.** Communicate effectively in a variety of professional contexts.
4. **Ethics.** Recognize professional responsibilities and make informed judgments in computing practice based on legal and ethical principles.
5. **Teamwork.** Function effectively as a member or leader of a team engaged in activities appropriate to the program's discipline.

CS-6. Theory. Apply computer science theory and software development fundamentals to produce computing-based solutions.

Syllabus:

1. **Money as a medium of exchange**
   The purpose of currency in economic markets
2. **Bitcoin overview**
   High-level picture of how Bitcoin works from the Satoshi Nakamoto whitepaper
3. **Cryptographic hashing**
   Required security properties and most common constructions
4. **Cryptographic puzzles and mining**
   Proof-of-work consensus mechanisms based on the HashCash protocol
5. **Digital signatures and transactions**
   Transactions structure, addresses, UTXOs, and verification
6. **Crypto assets as money**
   The model of money as a permanent, imperfect memory of past transactions in a market
7. **Bitcoin in the real world**
   How Bitcoin assets are actually acquired and spent in the current market; ethical implications and cybersecurity risks
8. **Long-run value of crypto assets**
   Quantity theory of money (QTM) as applied to digital currencies
9. **Bitcoin standard in monetary policy**
   Fixed supply, halving of mining reward, inflation
10. **Etherium network**
    Differences from Bitcoin, introduction to smart contracts, Eth and Gas
11. **Contract enforcement in economics**
    Lending, collateral, and defaults
12. **Smart contracts in Etherium with Solidity**
    How code interacts with a blockchain ledger; storing values and triggering updates
13. **Central bank digital coins**
    The role of central banks with fiat money; case studies on experiments with government interaction into digital currencies
14. **Non-fungible tokens (NFTs)**
    Smart contract structure, most common use cases
15. **Proof of stake**
    Negative externalities for proof of work consensus; advantages and challenges of alternatives

Updates to the course policy: In case this course policy needs to be changed during the semester, students will be notified by email and verbally during class. The current version will always be posted on the course website.

Textbooks:

- Narayanan, Bonneau, Felten, Miller, and Goldfeder. *Bitcoin and Cryptocurrency Technologies*. Princeton University Press, 2016.

Course Website: https://www.usna.edu/Users/CS/roche/courses/s22si486i/

Extra Instruction: Extra instruction (EI) is strongly encouraged and should be scheduled by email. (For Dr. Roche, first go here to check available times.) EI is not a substitute lecture; students should come prepared with specific questions or problems.

Collaboration: The guidance in the Honor Concept of the Brigade of Midshipmen and the Computer Science Department Honor Policy must be followed at all times. See https://www.usna.edu/CS/resources/honor.php. Specific instructions for this course:

- Collaboration or assistance from any human other than the instructors and those enrolled in SI486I this semester is not permitted. This includes any written or electronic materials from previous semesters.
- Homework: Students may collaborate on homework with others in the same class, but must cite this collaboration clearly. Every student must actually complete their own assignment and understand anything they turn in.
- Labs: Labs represent the main work of this class. Students may discuss and help each other in debugging and conceptual understanding, but may never share or copy code directly beyond small one-line snippets or specific error message debugging. Everyone is expected to completely understand their completed work.
- Projects: As project topics will be different, classmates may discuss and share resources with each other, but all submitted work must be original and all sources used must be clearly and specifically cited.
- Exams: No collaboration is allowed. Each student may prepare and bring a single study sheet to the midterm and final exams, but these must be prepared individually (no photocopies). Any group study guides should be shared with the instructor.

All collaboration and outside sources should always be cited. The same rules apply for giving and receiving assistance. If you are unsure whether a certain kind of assistance or collaboration is permitted, you should assume it is not, work individually, and seek clarification from your instructor.

Classroom Conduct:

Everyone in the classroom will show appropriate respect to each other at all times.

The section leader is responsible for recording attendance, bringing the class to attention, notifying the CS department office if the instructor is more than 5 minutes late, and directing the class in useful work in the instructor's absence.

Drinks are permitted, but they must be in closable containers. Food, alcohol, and tobacco (of all kinds) are prohibited. Electronic devices must be silent during class and should never serve as a distraction to other students.

Absences:

Students are responsible for all class material. Notes will be posted for each lecture, along with recommended readings. However, this material is not exhaustive and students missing class should arrange to copy notes from a classmate.

Any absences for scheduled in-class exams — even if excused according to USNA — must be discussed with your instructor at least 1 week in advance (preferably sooner), except under extenuating circumstances.

Late Policy: In most cases, deadlines correspond to an in-class discussion of homework problems, an in-lab network demo of working solutions, or project presentations. Therefore **late work will not receive credit** except under exceptional circumstances, at the discretion of the instructor.

Grading:

The final grading weight is as follows:

- 40%: Labs and homeworks
- 20%: Course projects
- 40%: Written exams (midterm and final)

Labs, homeworks, and projects will follow provided rubrics, and students will be asked to self-assess their own performance after each assignment. This self-assessment is a crucial and required part of the learning process and will help develop a consensus on fair grade assignment.

Plus/minus grades will be assigned based on the following numerical cutoffs:

	-		+
A	90–92	93–100	
B	80–82	83–86	87–89
C	70–72	73–76	77–79
D		60–66	67–69
F		0–59	

Submitted:

Assoc. Prof. Daniel S. Roche
Course Coordinator