Course Number and Title: CS 5433: Blockchains, Cryptocurrencies, and Smart Contracts

Instructor (Author of Syllabus): Prof. Ari Juels

Credits and Credit Hour Options: 3 credits, Letter Grade

Time and Location: Monday/Wednesday 10:10 - 11:25 a.m. Bloomberg Center Auditorium (131)

Course Description:

Viewed variously as a niche currency for online criminals and a technological threat to the financial industry, Bitcoin has fueled mythmaking, financial speculation, and real technological innovation. We will study both Bitcoin and the technological landscape it has inspired and catalyzed. Topics will include: the mechanics of consensus algorithms, such as Proof of Work and Byzantine consensus, and their role in blockchains and cryptocurrencies; cryptographic tools employed in cryptocurrencies, including digital signatures algorithm and zero-knowledge proofs; the evolution and mechanics of Bitcoin and its ecosystem; smart contracts; and special topics, such as artificial intelligence and blockchain systems, trusted hardware in blockchain-based systems, smart contracts and real-world contract law, and cryptocurrencies and crime.

Prerequisites:

A good level of programming experience—specifically, the ability to deal with challenging programming tasks—familiarity with common algorithms and data structures, and an understanding of basic concepts in discrete mathematics.

Corequisites:

None.

Textbook(s) and/or Other Required Materials:

- Narayanan, A., Bonneau, J., Felten, E., Miller, A., & Goldfeder, S. (2016). *Bitcoin and cryptocurrency technologies: a comprehensive introduction*. Princeton University Press.
- Shi, E. (2020). *Foundations of Distributed Consensus and Blockchains*. Available at http://elaineshi.com/docs/blockchain-book.pdf.
- Slides and selected readings will be distributed via the course website

Class and Laboratory Schedule:

Lectures: 2.5 hrs/wk

Recitations: None required

Labs: None

Assignments, Exams and Projects:

Activity	**Overview**	**Point Values**
Homework 1	This homework consists of a series of programming exercises presented in a text document and accompanied by code scaffolding and test vectors for select	5%

	problems. Students are to submit code solutions to the exercises in the assignment. The topic is cryptographic hash functions and their applications to cryptocurrency.	
Homework 2	This homework consists of a series of programming exercises presented in a text document and accompanied by code scaffolding and test vectors for select problems. Students are to submit code solutions to the exercises in the assignment. The topics are proof-of-work and proof-of-authority blockchain protocols, coin management in cryptocurrency wallets, and peer-to-peer networks in blockchain systems.	5%
Homework 3	This homework consists of a series of programming exercises presented in a text document and accompanied by code scaffolding and test vectors for select problems. Students are to submit code solutions to the exercises in the assignment. The topics are smart contracts, digital tokens, and anonymizing services for cryptocurrency.	5%
Homework 4	This homework consists of a series of programming exercises presented in a text document accompanied by a text tutorial, code scaffolding, and test vectors for select problems. Students are to submit code solutions to the exercises in the assignment. The topic is smart-contract security: students will hack vulnerable smart contracts.	5%
Class Participation	Attend all in-person lectures and demonstrate respect for other students, TAs, and the instructor.	5%

Midterm Exam	In-person, closed-book exam with five to ten detailed problems requiring written answers consisting of short text or mathematical solutions and ten to twenty multiple-choice questions. Potential exam coverage includes all topics discussed in the first half of course.	35%
Comprehensive Final Exam	In-person, closed-book exam with five to ten detailed problems requiring written answers consisting of short text or mathematical solutions and ten to twenty multiple-choice questions. Potential exam coverage includes all topics discussed in the course.	40%
Total Points		100%

Method of assessing student achievement: Students' code submissions will be autograded, with the grade for a given piece of code determined according to the fraction of correct outputs it yields. Graders *will not directly inspect students' submitted code*. The midterm and final exams will be graded according to rubrics, with partial credit admitted.

Basis of grade determination:
Grading: [options: letter]

Grade	**Percent**
A+	98-100
A	93-97
A-	90-92
B+	87-89
B	83-86
B-	80-82
C+	77-79
C	73-76
C-	70-72

F	<70

Typical Topics Covered:

- Technical and social goals of cryptocurrencies
- Cryptographic hash functions, their modeling by means of random oracles, and applications to blockchain systems
- Public-key cryptographic primitives, including identification schemes, digital signatures, and encryption
- The unspent-transaction-output (UTXO) model of Bitcoin representation
- Bitcoin transaction mechanics, including script execution
- Foundations of Byzantine agreement, protocols and impossibility results
- Bitcoin block structure and Bitcoin mining protocol, a.k.a. Nakamoto consensus
- Proof-of-stake in consensus protocols
- Cryptocurrency wallets and key management challenges and approaches
- Privacy in cryptocurrencies, including vulnerabilities in Bitcoin and privacy enhancement approaches including mixers and privacy coins
- Introduction to smart contracts; Ethereum transaction format and state-tree format
- Blockchain oracles, architecture and applications
- Decentralized Finance (DeFi), including lending protocols and decentralized exchanges
- Miner-extractable value (MEV) and ways to mitigate it
- Non-fungible tokens (NFTs)
- Decentralized identity
- Special topics, potentially including artificial intelligence and blockchain systems, trusted hardware in blockchain-based systems, smart contracts and real-world contract law, and cryptocurrencies and crime.

Course Outcomes:

1. Demonstrate an understanding of basic cryptographic primitives used in blockchains
2. Demonstrate fundamental understanding of the functionality provided by cryptocurrencies as well as their security and privacy properties
3. Demonstrate understanding of basic technical underpinnings of blockchains, including consensus protocols, cryptographic primitives, and key-management techniques
4. Demonstrate a basic ability to write smart contracts and identify flaws in their code
5. Demonstrate knowledge of popular applications of smart contracts, such as Decentralized Finance (DeFi), including functional goals, design components, and limitations

Academic Integrity:
Each student in this course is expected to abide by the Cornell University Code of Academic Integrity. Any work submitted by a student in this course for academic credit will be the student's own work. The policy can be found on the university's website here: https://theuniversityfaculty.cornell.edu/academic-integrity/.

Academic Integrity
You are encouraged to study together and to discuss information and concepts covered in lecture and the sections with other students. You can give "consulting" help to or receive "consulting" help from such students. However, this permissible cooperation should never involve one student having possession of a copy of all or part of work done by someone else, in *any* form. Additionally, you must be able to explain solutions submitted on your homework assignment to TAs or the instructor.

Should copying occur, both the student who copied work from another student and the student who gave material to be copied will both automatically receive a zero for the assignment. Penalty for violation of this Code can also be extended to include failure of the course and University disciplinary action.

During examinations, you must do your own work. Talking or discussion is not permitted during the examinations, nor may you compare papers, copy from others, or collaborate in any way. Any collaborative behavior during the examinations will result in failure of the exam, and may lead to failure of the course and University disciplinary action.

Optional statement about Academic Misconduct:

- **Academic Misconduct.** A faculty member may impose a grade penalty for any misconduct in the classroom or examination room. Examples of academic misconduct include, but are not limited to, talking during an exam, bringing unauthorized materials into the exam room, and disruptive behavior in the classroom.

Students with Disabilities

Your access in this course is important. Please give the instructor your Student Disability Services (SDS) accommodation letter early in the semester so that we have adequate time to arrange your approved academic accommodations. If you need an immediate accommodation for equal access, please speak with me after class or send an email message to me and/or SDS at sds_cu@cornell.edu. If the need arises for additional accommodations during the semester, please contact SDS. You may also feel free to speak with Student & Academic Affairs at Cornell Tech who will connect you with the university SDS office.

Religious Observances

Cornell University is committed to supporting students who wish to practice their religious beliefs. Students are advised to discuss religious absences with their instructors well in advance of the religious holiday so that arrangements for making up work can be resolved before the absence.

Options Statement about our supportive community:

- **Cornell Tech Cares**: The Cornell Tech community is a diverse and vibrant group of students, faculty, and staff. We take our responsibility to look out for one another seriously. As members of this community, your openness and proactive communication will allow us all to better care for students and respond to their needs, whether they be interpersonal or academic. Please help us continue to build and strengthen our community by reaching out if you are having an issue or are concerned about a fellow student. Contact studentwellness@tech.cornell.edu with concerns and we will make sure to care for one another. In the event of an emergency, please call 911 and Cornell Tech Safety & Security at 646-971-3611 (This number is also located on the back of your Cornell ID), when safe to do so.