UCONN
UNIVERSITY OF CONNECTICUT

CSE5095-007
Blockchain Technology
Computer Science and Engineering Dept.

Syllabus -- Fall 2022

Course Info

Title. Special Topics in Computer Science and Engineering - Blockchain Technology
Credits. 3.00 credits
Format. In person
Prerequisites. CSE3400 and CSE2050
Meeting time. Tue/Thu 9:30 - 10:45 am
Meeting location. OAK 441

Course Description

This course is a research oriented one targeting a topic that gained wide interest lately—blockchain technology. This technology is an emerging economic force with a large variety of potential applications. Although early systems focused only on providing a virtual currency exchange medium, i.e., building cryptocurrencies, nowadays there is increasing interest in providing various distributed services on top of this medium. Furthermore, blockchains have found new applications beyond supporting public verifiability in a cryptocurrency system, with influencing impact on issues such as privacy, regulation, social and environmental aspects. This course provides an extensive treatment of this new technology. The course will be viewed through the lens of secure systems design and applied cryptography.

Course goals. By the end of this course, you will be able to:

- Understand and track the rapid technical development in the fields of blockchains and cryptocurrencies.
- Analyze the security of blockchain-based systems.
- Identify and build use cases of blockchains and cryptocurrencies.
- Assess the impact of these systems on other fields and sectors.

Instructor and Contact Info

Ghada Almashaqbeh
ghada@uconn.edu

Office Hours. Tuesday at 11 am - 12 pm at my office ITE 255 (any changes will be announced on HuskyCT), or by appointment (if you have questions and cannot make it please email me to arrange another time).

Communication

The lecture slides and reading material will be posted on the course website (usually the night before the class): https://ghadaalmashaqbeh.github.io/teaching/ . Syllabus, announcements, problem sets, solutions, homework submission, project description and submission will be done on HuskyCT. We will have a discord

server to ease communication. Please post any questions there, especially those that may benefit multiple students.

I will be answering questions on discord once a day (usually around the end of the day). For emails, I will answer in 24 - 48 hours once I receive your email, if for some reason you do not hear back from me within this timeframe, please feel free to send me a reminder. I will not answer emails or view discord over the weekend (Friday 5 pm until Monday 8 am).

Suggested Textbooks

- *Mastering Bitcoin: Programming the Open Blockchain*, by Andreas M. Antonopoulos (2nd edition, 2017).
    - Available on github: https://github.com/bitcoinbook/bitcoinbook/blob/develop/book.asciidoc
- *Mastering Ethereum: Building Smart Contracts and DApps*, by Andreas M. Antonopoulos and Gavin Wood (1st edition, 2018).
    - Available on github: https://github.com/ethereumbook/ethereumbook/blob/develop/book.asciidoc
- *Bitcoin and Cryptocurrency Technologies*, by Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller, and Steven Goldfeder.
    - A pre-published pdf version can be found at: https://d28rh4a8wq0iu5.cloudfront.net/bitcointech/readings/princeton_bitcoin_book.pdf

Grading and Course Work

Homeworks	45%
Term Project	45%
In-class Discussion	10%

Homeworks will consist of a small number of problems. These may include questions to test understanding of the concepts covered by the course, some research-oriented questions to explore further concepts not covered in class, and some programming assignments to apply the tools we study, develop decentralized applications, and experiment with various technologies introduced in class. We will have 4 or 5 homeworks, depending on the class progress.

Submission and late policy.
You will have a free 3 days delay that you can use without any deductions if needed. After that, a late submission will receive a 10% deduction of its score per day. Any homework can have three days delay at maximum.

Collaboration. Homeworks are done and submitted individually. However, students are encouraged to discuss high level ideas with each other given that they write their solutions individually and list the names of the students with whom they discussed/collaborated in the submission. Copied solutions are considered cheating. You can collaborate with another two students at maximum (i.e., total is three students). I encourage you to solve the problems on your own first and then resort to group discussion for further understanding and brainstorming.

Term project has a considerable weight of the course grade since the course is a research-oriented one. It consists of: group formation and proposal, progress report, presentation, and final report submission. Each group (maximum 3 students) will submit one page proposing a project to work on by no later than 9/30/2022 (a list of suggested topics will be distributed later). I encourage you to start this process as early as possible.

Then, each group will submit a progress report (no later than 10/28/2022) to track the work status and get preliminary feedback from the instructor. Project presentations (a 15 - 20 min long presentation) will be during the last week of classes (the week of 12/5/2022, we may take another class from the previous week if the number of groups is larger than expected), and the final report submission will be due on the last day of class 12/9/2022. The project grade will be based on the progress report, presentation and the final report (5%, 15%, and 25%, respectively).

In-class discussion, students will lead discussions in class concentrated around any of the following:

- An article/paper about a related topic to cryptocurrency and blockchains (applications, attacks, new technologies, effect on society, etc.).
- A meetup/workshop/conference the student attended about a related topic as above.
- A personal experience in dealing with cryptocurrencies/blockchains.

Based on the number of enrolled students, we will have 1 student discussion per week (last 10 or 15 minutes of class). Later, a schedule will be distributed so each student can sign up for a date.

Course Content (Tentative, will be adjusted as needed)

This course will provide an extensive treatment of the blockchain technology covering the following topics:

- Semantics of blockchain-based systems.
- Essential cryptographic primitives used in cryptocurrency and blockchain-based systems.
- Bitcoin, the first successful cryptocurrency, including its consensus protocol, blockchain design, transactions, and its security.
- Ethereum, a more generalized cryptocurrency that provides a very rich feature set with a variant blockchain design and consensus protocol.
- Closer look into the types of consensus protocols, blockchains, and wallets including their basic operation, features, and security aspects.
- Blockchain-based decentralized services.
- Threat modeling for cryptocurrency-based systems.
- Decentralized micropayments.
- Privacy preserving cryptocurrencies.
- Applications of cryptocurrencies and blockchains.
- Social and financial aspects of blockchain and cryptocurrencies.

Course Schedule. (Tentative, will be adjusted as needed)

Week of	**Topic**
8/29/2022	Course overview, the history of blockchains and cryptocurrencies, and some useful resources. Semantics of blockchain-based systems and overview of basic cryptographic primitives.

9/5/2022	Bitcoin (work model, participants, transactions, blockchain, mining, consensus protocol).
9/12/2022	Bitcoin (scripting language, transaction processing, scalability, security issues)
9/19/2022	Ethereum (work model, blockchain, consensus protocol, smart contracts)
9/26/2022	Ethereum (more about smart contracts and tokens on top of Ethereum) Smart contracts security issues
10/3/2022	Types of mining and consensus protocols
10/10/2022	Types of blockchains Wallets
10/17/2022	Blockchain-based decentralized services
10/24/2022	Threat modeling for blockchain-based decentralized systems Decentralized micropayments
10/31/2022	Privacy preserving cryptocurrencies
11/7/2022	More applications of the blockchain model
11/14/2022	Environmental and/or social considerations of blockchain-based systems Decentralized Finance (DeFi)
11/21/2022	*Thanksgiving Recess, No classes!*
11/28/2022	Buffer (either for other classes and/or term project presentations)
12/5/2022	***Term project presentations***

Policies

Academic honesty. This course expects all students to act in accordance with the Guidelines for Academic Integrity at the University of Connecticut. Additionally, consult UConn's guidelines for academic integrity. The collaboration policy described above is designed to allow students the resources to succeed while ensuring they learn and master the material. If you are unsure if something is acceptable according to the collaboration policy, talk to me!

Violations of this policy will be considered violations of the academic integrity policy and will be reported to the Academic Integrity Hearing Board. Consequences may include (but are not limited to) failure of the class. Example violations include: not reporting collaborators, jointly writing solutions, copying or plagiarizing solutions and projects from other sources.

Student conduct code. Students are expected to conduct themselves in accordance with UConn's student conduct code (https://community.uconn.edu/the-student-code/).

Copyright. My lectures, notes, handouts, and displays are protected by state common law and federal copyright law. They are my own original expressions. Students may take notes. In addition, students will be consulted before using their solutions either with or without their name.

Students with Disabilities. The University of Connecticut is committed to protecting the rights of individuals with disabilities and assuring that the learning environment is accessible. If you are a student with approved academic accommodations through the Center for Students with Disabilities (CSD), please let me know immediately so we can discuss implementation. If you anticipate or experience any physical or academic barriers based on disability or pregnancy, you should contact the CSD to request accommodations at csd@uconn.edu or (860) 486-2020. Information about requesting accommodations is available on the CSD website at http://csd.uconn.edu/

Resources for Students Experiencing Distress. The University of Connecticut is committed to supporting students in their mental health, their psychological and social well-being, and their connection to their academic experience and overall wellness. The university believes that academic, personal, and professional development can flourish only when each member of our community is assured equitable access to mental health services. The university aims to make access to mental health attainable while fostering a community reflecting equity and diversity and understands that good mental health may lead to personal and professional growth, greater self-awareness, increased social engagement, enhanced academic success, and campus and community involvement.

Students who feel they may benefit from speaking with a mental health professional can find support and resources through the Student Health and Wellness-Mental Health (SHaW-MH) office. Through SHaW-MH, students can make an appointment with a mental health professional and engage in confidential conversations or seek recommendations or referrals for any mental health or psychological concern.

Mental health services are included as part of the university's student health insurance plan and also partially funded through university fees. If you do not have UConn's student health insurance plan, most major insurance plans are also accepted. Students can visit the Student Health and Wellness-Mental Health located in Storrs on the main campus in the Arjona Building, 4th Floor, or contact the office at (860) 486-4705, or https://studenthealth.uconn.edu/ for services or questions.

Accommodations for Illness or Extended Absences. Please stay home if you are feeling ill and please go home if you are in class and start to feel ill. If illness prevents you from attending class, it is your responsibility to notify your instructor as soon as possible. You do not need to disclose the nature of your illness, however, you will need to work with your instructor to determine how you will complete coursework during your absence.

If life circumstances are affecting your ability to focus on courses and your UConn experience, students can email the Dean of Students at dos@uconn.edu to request support. Regional campus students should email the Student Services staff at their home campus to request support and faculty notification.

COVID-19 Specific Information: People with COVID-19 have had a wide range of symptoms reported – ranging from mild symptoms to severe illness. These symptoms may appear 2-14 days after exposure to the virus and can include: Fever, Cough, Shortness of breath or difficulty breathing, Chills, Repeated shaking with chills, Muscle pain, Headache, Sore throat, New loss of taste or smell. Additional information including what to do if you test positive or you are informed through contract tracing that you were in contact with someone who tested positive, and answers to other important questions can be found here: https://studenthealth.uconn.edu/updates-events/coronavirus/