CS414/614 Blockchain Technology – Spring 2022 Syllabus

Instructor Information

Prof. Duc A. Tran, PhD
duc.tran@umb.edu (preferred way of contact for quick response)
Phone (W): *617-287-6452*
Office Location: *M3-0201-18*
Office Hours: *Tue & Thu 1PM-2:30PM*

Note: The following link will assist you in forwarding your UMB email account to your personal account: Use this link. Throughout the semester, I will communicate with you via your UMB *e*-mail account. You may have e-mail redirected from your official UMass Boston address to another *e*-mail address at your own risk. The University will not be responsible for the handling of *e*-mail by outside vendors or by departmental servers.

Course Information

Course Title: Blockchain Technology

Credits: 3

Online Course?: No

Description: Blockchain enables a digital society where people can contribute, collaborate, and transact without having to second-guess trust and transparency. It is the technology behind the success of Bitcoin, Ethereum, and many disruptive applications and platforms that have positive impact in numerous sectors, including finance, education, health care, environment, transportation, and philanthropy, to name a few. This course covers a basic set of essential concepts, mathematics, and algorithms suitable for aspiring students who want to be technologically ready for a blockchain venture. Topics touch various issues in mathematical cryptography and decentralized computing. Students will learn programming tools sufficiently to develop a blockchain project from scratch.

Context: This course is an elective. It complements the existing database, networking, and cryptography courses with knowledge needed to build decentralized computing systems.

Prerequisites: CS310 Advanced Data Structures and Algorithms OR permission of the instructor.

Prerequisite Skills: Proficiency in one programming language.

Course Objectives: By fully participating in this course, you should be able to:

1. Understand blockchain technology's history, transformative value and real-world applications
2. Understand the mathematical and algorithmic aspects of a blockchain network, its architectures, and constituent components
3. Understand how blockchain is implemented in state-of-the-art blockchain networks

4. Determine the applicability of blockchain given its capabilities and limitations
5. Develop a small blockchain application from scratch and be technologically ready for larger blockchain projects

Core Competencies:

The objectives for this course focus on the following core competencies: analytical skills, problem-solving skills, creativity, critical-thinking skills, and resilience.

Required Assignments: There are four types of assignments: Homework, Exams, and Term Project.

Homework: Students are each assigned to read a technical paper and explain it in a 20-minute slide presentation in the class. This will be evaluated by the instructor (50%) and the class audience (50%)

Exams: There is a midterm exam and a final exam. Both are in the form of multi-choice questions. The final exam is accumulative, covering all the topics discussed in the class from the beginning to the end of the course.

Term Project: This is a group project to develop a blockchain application, requiring coding, presentation, and a written summary of the work as the deliverables. The term project will start immediately after the midterm exam.

Course Rubric:

Tests/Assignments/Deliverables	Number	Grade %
1. Homework	**1**	**15%**
2. Midterm	**1**	**20%**
3. Final	**1**	**25%**
4. Group Project *(Coding/Presentation/Paper)*	**1**	**30%**
5. Participation + Attendance		**10%**

Course Policies:

Participation – Complete all required assignments prior to class, thoughtfully participating in discussions, and taking responsibility for helping create a positive learning environment by arriving promptly, listening respectfully, and participating constructively. Participation also include your efforts in group work which is required by the group project.

Attendance – Must attend every class session, except absences justifiable with supporting documents and approval by instructor

Late Work – Subject to 10% deduction from the original grade of the submitted work.

Grading

Grading: Grade type for the course is a whole or partial letter grade. (Please see table below)

	Letter Grade	Percentage
	A	93-100%
	A-	90-92%
	B+	87-89%
	B	83-86%
	B-	80-82%
	C+	77-79%
	C	73-76%
	C-	70-72% (F for graduate students)
	D+	67-69% (F for graduate students)
	D	63-66% (F for graduate students)
	D-	60-62% (F for graduate students)
	F	0-59% (F for graduate students)

Required Text(s):

Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction. Narayanan et al. Princeton University Press. ISBN-10 0691171696.

Technical Requirements:

Basic understanding of discrete math, data structures and algorithms and proficiency in at least one programming language

Recommended Texts:

Foundations of Distributed Consensus and Blockchains.
http://elaineshi.com/docs/blockchain-book.pdf

Other Reading: Instructor may post readings/notes as and when required on course website.

Course Schedule

- Week 1:
  - Intro to Blockchain: history, data structure, cryptography, network architecture, consensus, taxonomy
- Week 2:
  - Cryptocurrency blockchain (Bitcoin): UTXO transaction model, merkle tree, validation, proof-of-work consensus, mining model, security
- Week 3:

  - Smart contract blockchain (Ethereum): account-based transaction model, validation, smart contracts, proof-of-stake consensus, token creation (fungible and NFT), smart contract interaction
- Week 4:
  - Blockchain Applications: Use Cases
  - Group assignments for project, idea brainstorming for project
- Week 5, 6
  - Hands-on programming with Ethereum (Solidity, Javascript, Web3)
- Week 7
  - Decentralized Finance, Algorithmic Stablecoin, Automated Market Making
- Week 8, 9:
  - P2P networking: Gossip broadcast, Distributed Hash Tables, Kademlia protocol
  - Internet Planetary File System (IPFS): P2P storage network
- Week 10
  - Consensus problem: classic mechanisms (Byzantine Broadcast, deterministic/randomized, Dolev-Strong, PBFT, GHOST), modern mechanisms (Proof of Work, Proof of Stake, and other Proof-of-X approaches)
- Week 11:
  - Cryptography primitives: public key cryptography, elliptic curve cryptography, cryptographic hash functions, digital signatures, commitment scheme
- Week 12
  - Challenges, recent advances, and future directions in blockchain development
- Week 13, 14
  - Project presentations
- Week 15
  - Class review for final exam
  - Brainstorming on continuation of projects and future ventures

---

Methods of Instruction

Methods:

The class-time will be spent on three distinct type of activities: i) lecture (theory and code demonstration) by the Instructor, ii) interactive discussions involving the entire class, and iii) presentations by the students, of assigned work and any findings useful they want to share with the whole class.

Accommodations

The University of Massachusetts Boston is committed to providing reasonable academic accommodations for all students with disabilities. This syllabus is available in alternate format upon request. Students with disabilities who need accommodations in this course must contact the instructor to discuss needed accommodations. Accommodations will be provided after the student has met with the instructor to request accommodations. Students must be registered with the Ross Center for Disability Services, CC UL 211 (617.287.7430) before requesting accommodations from the instructor. http://www.umb.edu/academics/vpass/disability/. After registration with the Ross Center, a student

should present and discuss the accommodations with the professor. Although a student can request accommodations at any time, we recommend that students inform the professor of the need for accommodations by the end of the Drop/Add period to ensure that accommodations are available for the entirety of the course.

Academic Integrity and The Code of Student Conduct

It is the expressed policy of the University that every aspect of academic life not only formal coursework situations, but all relationships and interactions connected to the educational process shall be conducted in an absolutely and uncompromisingly honest manner. The University presupposes that any submission of work for academic credit indicates that the work is the student's own and is in compliance with University policies. In cases where academic dishonesty is discovered after completion of a course or degree program, sanctions may be imposed retroactively, up to and including revocation of the degree. Any student who reasonably believes another student has committed an act of academic dishonesty should inform the course instructor of the alleged violation. These policies are spelled out in the Code of Student Conduct. Students are required to adhere to the Code of Student Conduct, including requirements for academic honesty

UMB Code of Student Conduct

You are encouraged to visit and review the UMass website on Plagiarism*:* Plagiarism Prevention & Awareness: Home

Other Pertinent and Important Information

You are advised to retain a copy of this syllabus in your personal files for use when applying for future degrees, certification, licensure, or transfer of credit.