Carnegie Mellon University

95-810 Blockchain Fundamentals

Meeting Days, Times, Location: MW 4:30–5:50 PM

Semester: Fall, Mini 2**, Year:** 2018

Units: 6**, Section:** A2

Instructor information

Name	Dr. Eliezer Kanal
Contact Info	ekanal@cmu.edu
Office location	CIC 3246 (appointment required)
Office hours	Tue 1-2 PM

TA Information [If applicable]

TA name	Harsh Johari
TA Contact Info	hjohari@andrew.cmu.edu

Course Description

This class will be a deep-dive into blockchain technology. We will discuss the fundamental cryptographic underpinnings of the technology as well as different consensus mechanisms currently available. We'll discuss both single-purpose blockchains such as Bitcoin as well as general-purpose implementations. We'll discuss governance of blockchain technology and related challenges, as well as legal challenges and concerns. This course will also provide an overview of blockchain programming, highlighting both existing challenges and specific nuances in blockchain programming. Students should leave the class with a better understanding of what blockchain technology is, what types of problems are best suited for blockchain-based solutions, as well as a more thorough understanding of the impact that blockchain technology is having across the board.

Learning Objectives

After completing this course, students should be able to…

- Be able to explain cryptographic concepts underlying blockchain technology in layman terminology
- Describe how cryptography applies to blockchain and impacts implementation-related decisions
- Describe blockchain technology, how it relates to the myriad of associated technologies and concepts (communication, consensus, architecture, identity, among others)
- Assess the relevance of blockchain technology to arbitrary use cases
- Evaluate the risks of using blockchain technology
- Describe current attacks on blockchain technology, as well as possible attack surfaces to be aware of in the future
- Discuss how blockchain fits in existing legal, political, and societal frameworks
- Create a minimalist blockchain application

Learning Resources

- No book required; readings will be assigned throughout the course

Assessments

The final course grade will be calculated using the following categories:

Assessment	Percentage of Final Grade
Written assignments	50%
Final project & presentation	30%
Attendance	10%
Participation	10%

- There will be multiple written assignments throughout the semester related to the topics being discussed.
- There will be a final group project starting midway through the semester related to developing blockchain use cases, culminating in a presentation to the class during finals week
- There may be unannounced in-class exercises, which will be included in the "Participation" section

Students will be assigned the following final letter grades, based on calculations coming from the course assessment section.

Grade	Percentage Interval
A	≥90%
B	<90%, ≥80%
C	<80%, ≥70%
D	<70%, ≥60%
R (F)	<60%

Grading Policies

- **Late-work policy**: Late work will not be accepted. If you believe there are mitigating circumstances please let me know, and be prepared to provide documentation.
- **Attendance and/or participation policy**: Attendance will be measured through a sign-in sheet to be signed as students enter class each day. Participation is expected from all students in the form of class discussion, in-class exercises, and group work.

Course Policies

- **Academic Integrity & Collaboration**: Individual assignments are expected to be completed by the individual; no collaboration allowed. Group assignments will be assigned occasionally and it is expected that all

group members participate approximately equally.

- **Accommodations for students with disabilities**: If you have a disability and require accommodations, please contact Catherine Getchell, Director of Disability Resources, 412-268-6121, getchell@cmu.edu. If you have an accommodations letter from the Disability Resources office, I encourage you to discuss your accommodations and needs with me as early in the semester as possible. I will work with you to ensure that accommodations are provided as appropriate.
- **Statement on student wellness**: As a student, you may experience a range of challenges that can interfere with learning, such as strained relationships, increased anxiety, substance use, feeling down, difficulty concentrating and/or lack of motivation. These mental health concerns or stressful events may diminish your academic performance and/or reduce your ability to participate in daily activities. CMU services are available, and treatment does work. You can learn more about confidential mental health services available on campus at: http://www.cmu.edu/counseling/. Support is always available (24/7) from Counseling and Psychological Services: 412-268-2922.
- **Mobile Devices**: Mobile device usage in class is discouraged. Students disrupting the class with their devices may be asked to leave the class.

Fall 2018 Course Schedule

2019 students – note that this will be updated and slightly modified before the Fall 2019 course starts

Date	Theme/Topic
10/22	Hash functions, proof-of-work systems
10/24	Encryption, Diffie-Hellman, RSA, PKI
10/29	Bitcoin, Gossip protocol, Consensus mechanism part , Ethereum
10/31	*Guest lecture, Eugene Leventhal* – Consensus mechanism part 2
11/5	Privacy in Bitcoin, Monero, attacks on Monero, ZCash, other blockchains
11/7	GPB architecture - auth, channels, private/public, roles, etc
11/12	Governance & policy
11/14	*Guest lecture, Eugene Leventhal* – Exchanges, ICOs, risks
11/19	Legal
11/21	Attacks on Blockchain
11/26	Solidity, Go for fabric
11/28	*Guest lecture, Mike Annichiarico* – Ethereum security potpourri
12/3	*Guest lecture, Dr. Scott Ruoti* – Blockchain use cases
12/5	TBD