San José State University
Computer Science Department
CS266: Topics in Information Security - Autumn 2019

Blockchain Technologies

Course and Contact Information

Instructor:	Guha Jayachandran
Email:	guha.jayachandran@sjsu.edu (note this address is not yet activated)
Class Days/Time:	M/W 7:30-8:45AM
Classroom:	MH422
Office Hours:	M/W 7:15-7:30AM in MH422 and from 8:45AM MH422→TBA
Prerequisites:	CS166 or instructor consent

Web Page

Course materials will be made available online at http://blockchaincourse.onai.com/.

Course Description

"Advanced topics in the area of information security. Content differs with each offering. Possible topics include, but are not restricted to: Network Security, Software Reverse Engineering and Cryptanalysis. Prerequisite: CS 166 or instructor consent."

Specific Description

Blockchains have emerged as exciting means of achieving decentralized consensus, notably in the realm of cryptocurrencies and electronic payments. The space has seen rapid methodological advances and melds cryptography, algorithms, distributed systems, game theory, and more. In this course, we will start with a review of sufficient cryptography to understand the workings of Bitcoin, including Proof of Work. We will then cover Byzantine fault-tolerant consensus protocols, various algorithms to prevent Sybil attacks, Merkle trees and other primitives, "smart contracts," privacy-preserving techniques, homomorphic encryption, network layer technologies, Lightning transfers and related methods, zero-knowledge proofs, and application case studies. We will also cover reasons for global and industrial enthusiasm about the technology, potential for misuse, examples of vulnerabilities, and governance. Lectures will be supplemented with primary sources and student presentations.

Course Learning Outcomes

Upon successful completion of this course, students will be able to:

1. Explain the technical workings of blockchain protocols.
2. Design blockchain protocols, smart contracts, and applications.
3. Evaluate new published work.

Required Texts/Readings

Textbook

There is no required textbook. Notes and papers will be assigned as reading.
Those who desire an introductory supplement can use *Bitcoin and Cryptocurrency Technologies*. You can download a prepublication version for free from https://bitcoinbook.cs.princeton.edu or buy a print copy.

Other Readings

Links to online papers will be provided or copies will be provided.

Other technology requirements / equipment / material

Students will need a computer, or access to a computer, on which you can install open source blockchain applications and perform programming assignments.

Course Requirements and Assignments

Course requirements and assignments all directly contribute to the course learning outcomes listed above.

- At the end of each lecture, each student should submit a piece of paper (with your name) with at least one key fact covered that day. Before each lecture, each student should submit one question about the material covered to date.
- Most classes, there will be time set aside for questions and you're encouraged to take advantage of it to resolve any doubts.
- Readings will be assigned. Each student will orally present a couple papers to the class over the course of the semester. Come show your presentation in office hours before the day you are scheduled to present, and email your presentation as a pdf one week before the class you are scheduled to present.
- There will be two other homework assignments.
- Each student will contribute to a final project, presenting it as a poster and including a brief report.
- There will be one examination (final exam).
- Each homework assignment, and the final project instructions, will include guidelines on working as a group.

Final Examination or Evaluation

There will be a final examination at the scheduled time of 7:15-9:30AM on December 11, 2019.

Grading Information

Weightings and Letter Grades

Grades will be determined according to the following weights:

- Participation (learnings and questions submitted each lecture): 10%
- Homework assignments: 20% (each equally weighted)
- Paper presentations: 30% (each equally weighted)
- Final project poster/report: 25%
- Final exam: 15%

Based on the weightings above, the following conversion scale will be used to assign letter grades:

[97, 100]	A+
[93, 97)	A
[90, 93)	A-
[87, 90)	B+
[82, 87)	B
[80, 82)	B-
[77, 80)	C+
[72, 77)	C
[70, 72)	C-
[67, 70)	D+
[62, 67)	D
[60, 62)	D-
[0, 60)	F

Late Work or Rescheduling

Absent a valid excuse, a late homework assignment will be penalized 10% per class that it is late. Paper presentations, the final project, and the final exam will receive a zero if not performed on time. If you will be unable to make your scheduled paper presentation, let the instructors know at least 3 weeks in advance.

Classroom Protocol

Arrive before 7:30AM and submit a slip of paper (with your name) with any question about the material to date, so that it can be answered for the benefit of all. Be ready for class to start at 7:30. Submit at the end of the lecture a slip of paper with at least one key fact from that day's lecture. Feel free to ask questions. Lectures will be video recorded and likely will be posted publicly online at some point, but not immediately; do not expect to be able to miss attendance simply because the lecture may be posted online at a later date.

University Policies

Per University Policy S16-9, university-wide policy information relevant to all courses, such as academic integrity, accommodations, etc. will be available on Office of Graduate and Undergraduate Programs' Syllabus Information web page at http://www.sjsu.edu/gup/syllabusinfo/.

CS266 Schedule - Autumn 2019

This schedule is subject to change. Fair notice will be provided: Updates will be given in class and the schedule available on the course website will be updated.

Week	Date	Topic
1	8-21	Introduction
2	8-26	Byzantine Generals I
2	8-28	Byzantine Generals II
3	9-2	*Labor Day*
3	9-4	Cryptography Essentials and Data Structures
4	9-9	Proof of Work
4	9-11	Proof of Stake
5	9-16	Proof of Space
5	9-18	Network Layer I
6	9-23	Smart Contracts: Basics, Failures, and Auditing
6	9-25	Protocol Validation
7	9-30	Homomorphic Encryption I
7	10-2	Homomorphic Encryption II
8	10-7	Permissioned Blockchains vs. Databases
8	10-9	Network Layer II
9	10-14	Lightning Network and Side Chains
9	10-16	Mixing and Tumbling
10	10-21	Anonymization and Ring Signatures
10	10-23	Accumulators
11	10-28	VDFs, VRFs, and Random Beacons
11	10-30	Zero Knowledge Proofs I
12	11-4	Zero Knowledge Proofs II
12	11-6	Wallet Security
13	11-11	Genesis, Forks, and Disruptions
13	11-13	Analysis and Visualization
14	11-18	Investigations
14	11-20	Decentralized Exchange
15	11-25	Oracles and Off-chain Linkages
15	11-27	Governance
16	12-2	Cryptoeconomics
16	12-4	Final Projects
17	12-9	Review
Final Exam	12-11	7:15 - 9:30AM