San José State University
College of Science/Department of Computer Science
CS 185c, Cryptocurrencies and Security on the Blockchain

Section2, Spring 2019

Course and Contact Information

Instructor:	Thomas Austin
Office Location:	MacQuarrie Hall 216
Telephone:	408-924-7227
Email:	thomas.austin@sjsu.edu
Office Hours:	Mondays, noon-1pm Thursdays, 10-11am Other times by appointment
Class Days/Time:	Monday, Wednesday 10:30-11:45
Classroom:	MacQuarrie Hall 422
Prerequisites:	CS 166 or equivalent.

Course Format

Faculty Web Page and MYSJSU Messaging

Course materials such as syllabus, handouts, notes, assignment instructions, etc. can be found on my faculty web page at http://www.cs.sjsu.edu/~austin/cs185c-spring19 and Canvas (http://sjsu.instructure.com/). You are responsible for regularly checking with the messaging system through Canvas to learn of any updates.

Course Description

Cryptocurrencies and the blockchain. Centralized clearinghouse solutions vs. distributed consensus solutions. The blockchain and its validation approaches: proof-of-work, proof-of-stake, proof-of-storage, etc. Cryptocurrency wallets. Smart contracts.

Course Learning Outcomes (CLO)

The goal of this course is to equip students to be blockchain engineers. After completion of this course, the student is expected to be versed in the various subjects of interest in cryptocurrencies and comfortable with the technologies needed.

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

1. Build a cryptocurrency with a central clearinghouse.
2. Build a cryptocurrency with distributed consensus.
3. Design and implement a proof-of-work blockchain.
4. Design and implement a proof-of-stake blockchain.
5. Use mnemonics to save and reconstruct a cryptocurrency wallet.

6. Apply the blockchain outside of a cryptocurrency setting.

Required Texts/Readings

Textbook

Mastering Bitcoin: Unlocking Digital Cryptocurrencies, 2nd edition, Andreas M. Antonopoulos, (O'Reilly, June 2017, ISBN: 9781491954379)

Other Readings

- Bitcoin: A Peer-to-Peer Electronic Cash System, Satoshi Nakomoto.
- SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies, Bonneau et al., IEEE 2015.
- Other readings TBD.

Course Requirements and Assignments

SJSU classes are designed such that in order to be successful, it is expected that students will spend a minimum of forty-five hours for each unit of credit (normally three hours per unit per week), including preparing for class, participating in course activities, completing assignments, and so on. More details about student workload can be found in University Policy S12-3 at http://www.sjsu.edu/senate/docs/S12-3.pdf.

Homework assignments are in JavaScript using Node.js. Many of these homework assignments build on previous assignments. If you do poorly on one assignment, you may resubmit it and take a '0' on the next assignment.

There will also be a group project involving teams of 1-4 students. In this project, students will design their own blockchain-based cryptocurrency borrowing concepts from other cryptocurrencies.

There is a final and a midterm.

In-class labs are used as the basis for your participation grade. Any question in the lab is fair game for the exams.

See Canvas at http://sjsu.instructure.com/ for more details.

Final Examination or Evaluation

The final exam is worth 20% of the total grade for the class. It is a written exam. Paper will be provided. Bring something to write with.

Grading Information

Determination of Grades

1. 30% -- Homework assignments (individual)
2. 20% -- Class project (team)
3. 20% -- Midterm
4. 20% -- Final
5. 10% -- Participation (labs)

Assignments are due by 11:59 PM Pacific Time on the specified day.

Late homework assignments will not be accepted. However, you may elect to take a '0' on any assignment and resubmit a previous assignment instead.

Nominal grading scale:

Percentage	**Grade**
92 and above	A
90 - 91	A-
88 - 89	B+
82 - 87	B
80 - 81	B-
78 - 79	C+
72 - 77	C
70 - 71	C-
68 - 69	D+
62 - 67	D
60 - 61	D-
59 and below	F

Classroom Protocol

Attendance is recommended, but it is not mandatory, except for exam dates. Cell phone use is prohibited. Punctuality is appreciated.

Bring your laptop to class.

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/"

CS 185C / Advanced Topics in Information Security, Spring 2019

Please note that the schedule is subject to change with fair notice, which will be posted through Canvas at https://sjsu.instructure.com.

Course Schedule ***(TENTATIVE)***

Week	Date	Topics, Readings, Assignments, Deadlines
1	1/28	Introduction
1	1/30	Crash course on JavaScript and Node.js
2	2/4	Review of cryptography
2	2/6	A first cryptocurrency and the double-spending problem
3	2/11	DigiCash and blinded signatures
3	2/13	Introduction to Bitcoin. Byzantine fault tolerance. **Reading:** • Mastering Bitcoin – Chapter 1. • Bitcoin: A Peer-to-Peer Electronic Cash System
4	2/18	Bitcoin transactions **Reading:** Mastering Bitcoin – Chapter 2.
4	2/20	Bitcoin transactions, continued **Reading:** Mastering Bitcoin – Chapter 6.
5	2/25	Bitcoin – wallets and mnemonics **Reading:** Mastering Bitcoin – Chapter 5.
5	2/27	Bitcoin – mining and the blockchain **Reading:** Mastering Bitcoin – Chapter 9.
6	3/4	Bitcoin – mining and the blockchain **Reading:** Mastering Bitcoin – Chapter 10.
6	3/6	Beyond Bitcoin – challenges to be addressed. **Reading:** Bonneau et al., IEEE 2015
7	3/11	Mining pools
7	3/13	Midterm review
8	3/18	MIDTERM
8	3/20	Selfish mining attack
9	3/25	“Useful” proof-of-work.
9	3/27	Proof-of-stake protocols. Peercoin.
10	4/1	****SPRING BREAK****
10	4/3	****SPRING BREAK****
11	4/8	Proof-of-storage protocols. Permacoin.

Week	**Date**	**Topics, Readings, Assignments, Deadlines**
11	4/10	Filecoin, proof-of-replication, proof-of-spacetime.
12	4/15	High performance blockchains. Dfinity, Algorand, Thunderella.
12	4/17	High performance blockchains, continued.
13	4/22	Bitcoin – Bitscript
13	4/24	Ethereum – smart contracts
14	4/29	TBD
14	5/1	TBD
15	5/6	Project presentations
15	5/8	Project presentations
16	5/13	Final exam review
Final Exam		May 15th, 9:45-11:45