San José State University
College of Science/Department of Computer Science
CS 168, Blockchain and Cryptocurrencies, Spring 2023

Course and Contact Information

Instructor:	Thomas Austin
Office Location:	MacQuarrie Hall 216 Zoom: https://sjsu.zoom.us/j/3796767168?pwd=SzNVOE4zSTNyNHNqR1RhNlJ6cDAwUT09
Telephone:	408-924-7227
Email:	thomas.austin@sjsu.edu
Office Hours:	Mondays, 3-4pm (Zoom and in-person) Thursdays, 10-11am (Zoom only) Other times by appointment SEE http://www.cs.sjsu.edu/~austin/office-hours-updates.txt FOR LAST MINUTE CHANGES
Class Days/Time:	Monday/Wednesday, 1:30-2:45
Classroom:	Duncan Hall 450
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/cs168-spring23 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, Andreas M. Antonopoulos,
(O'Reilly, December 2014, ISBN-13: 978-1449374044, ISBN-10: 1449374042)

Other Readings

- Bitcoin: A Peer-to-Peer Electronic Cash System, Satoshi Nakomoto.
- Bitcoin and Cryptocurrency Technologies (PRE-PUBLICATION VERSION), Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller, Steven Goldfeder, 19-Feb-2016.
- 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. There will also be a group project involving teams of 1-2 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.

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 168 / Blockchain and Cryptocurrencies, Spring 2022

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	1/25	Introduction
2	1/30	Crash course on JavaScript and Node.js
2	2/1	Review of cryptography
3	2/6	A first cryptocurrency and the double-spending problem
3	2/8	DigiCash and blinded signatures
4	2/13	DigiCash and blinded signatures, continued
4	2/15	Introduction to Bitcoin. Byzantine fault tolerance. **Reading:** • Mastering Bitcoin – Chapter 1. • Bitcoin: A Peer-to-Peer Electronic Cash System.
5	2/20	Bitcoin transactions **Reading:** • Mastering Bitcoin – Chapter 2. • Mastering Bitcoin – Chapter 5.
5	2/22	Introduction to SpartanGold
6	2/27	Bitcoin – mining and UTXOs **Reading:** Mastering Bitcoin – Chapter 7.
6	3/1	Bitcoin – the blockchain **Reading:** Mastering Bitcoin – Chapter 8.
7	3/6	Beyond Bitcoin – challenges to be addressed. **Reading:** Bonneau et al., IEEE 2015
7	3/8	Bitcoin – wallets and mnemonics **Reading:** Mastering Bitcoin – Chapter 4.
8	3/13	Review for midterm
8	3/15	****MIDTERM EXAM****
9	3/20	Alternate proof schemes
9	3/22	Pure proof-of-stake protocols
10	3/27	****SPRING BREAK****

Week	Date	Topics, Readings, Assignments, Deadlines
10	3/29	****SPRING BREAK****
11	4/3	Mining pools **Reading:** Meni Rosenfeld, “Analysis of Bitcoin Pooled Mining Reward Systems”
11	4/5	Introduction to Ethereum
12	4/10	Ethereum smart contracts
12	4/12	Ethereum virtual machine (EVM)
13	4/17	Oracles and tokens
13	4/19	Decentralized applications (DApps)
14	4/24	Cross-chain protocols
14	4/26	Non-outsourceable puzzles
15	5/1	Selfish mining attack
15	5/3	TBD
16	5/8	Project presentations
16	5/10	Project presentations
17	5/15	Review for final
Final Exam	5/23	FINAL EXAM: 12:15-2:15