SJSU SAN JOSÉ STATE UNIVERSITY

College of Science · Computer Science

Blockchain and Cryptocurrencies

CS 168

Spring 2026 Section 01 In Person 3 Unit(s) 01/22/2026 to 05/11/2026 Modified 01/22/2026

Contact Information

Professor: Thomas H. Austin

Email: thomas.austin@sjsu.edu
Office: MacQuarrie Hall 216

Office Hours

Mondays 3-4pm, Thursdays 11am-noon
MacQuarrie Hall 216

Check https://www.cs.sjsu.edu/~austin/office-hours-updates.txt for updates.

Zoom appointments only available with advance notice.

Course Information

Monday, Wednesday, 1:30 PM to 2:45 PM, Duncan Hall 415

Course Description and Requisites

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.

Prerequisite(s): CS 166 (with a grade of "C-" or better). Computer Science or Software Engineering majors only, or instructor consent.

Letter Graded

Classroom Protocols

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-spring25 (http://www.cs.sjsu.edu/~austin/cs168-spring25) and Canvas. You are responsible for regularly checking with the messaging system through Canvas to learn of any updates.
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.

Program Information

Diversity Statement - At SJSU, it is important to create a safe learning environment where we can explore, learn, and grow together. We strive to build a diverse, equitable, inclusive culture that values, encourages, and supports students from all backgrounds and experiences.

Course Learning Outcomes (CLOs)

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

Course Materials

Mastering Bitcoin: Unlocking Digital Cryptocurrencies

Author: Andreas M. Antonopoulos
Publisher: O'Reilly

Bitcoin: A Peer-to-Peer Electronic Cash System, Satoshi Nakomoto.

Availability: Online

SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies, Bonneau et al., IEEE 2015.

Availability: Online

Other readings TBD

Course Requirements and Assignments

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/ (%20http%3A/sjsu.instructure.com/) for more details.

Grading Information

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.
Determination of Grades
30% -- Homework assignments (individual)
20% -- Class project (team)
20% -- Midterm
20% -- Final
10% -- Participation (labs)

Assignments are due by 11:59 PM Pacific Time on the specified day.
Late homework assignments will not be accepted.

Breakdown
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

University Policies

Per University Policy S16-9 (PDF) (http://www.sjsu.edu/senate/docs/S16-9.pdf), relevant university policy concerning all courses, such as student responsibilities, academic integrity, accommodations, dropping and adding, consent for recording of class, etc. and available student services (e.g. learning assistance, counseling, and other resources) are listed on the Syllabus Information (https://www.sjsu.edu/curriculum/courses/syllabus-info.php) web page. Make sure to visit this page to review and be aware of these university policies and resources.

Course Schedule

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 by week (TENTATIVE)

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

Introduction to Ethereum

12. Ethereum smart contracts
    Ethereum virtual machine (EVM)
13. Oracles and tokens
    Decentralized applications (DApps)
14. Cross-chain protocols
    Non-outsourceable puzzles
15. Selfish mining attack
    Other topics TBD
16. Project presentations
17. Review for final

FINAL: May 15th, 1-3pm