Blockchain Fundamentals DeCal - Spring 2018

Blockchain at Berkeley DeCal

Course Name: Blockchain Fundamentals Decal
Course Numbers: CS 198-078 (#42563)
Units: 2

Website: blockchain.berkeley.edu/decal/sp18/fund
Piazza: piazza.com/berkeley/spring2018/compsci19878/home

Course Staff:
Nadir Akhtar (nadir@blockchain.berkeley.edu): Lecturer
Gillian Chu (gillichu@berkeley.edu): Lecturer
Brian Ho (brian.ho@berkeley.edu): Lecturer
Sara Reynolds (snreynolds@berkeley.edu): Course Administrator

Noah Alcus: Discussion Leader
Jason Bi: Discussion Leader
Derrick Li: Discussion Leader
Gloria Wang: Discussion Leader
Ashwinee Panda: Discussion Leader

Lectures: Saturday 2 - 4 PM (Hearst Mining 390)

Discussions:
A: Monday 10 - 11 AM: Ashwinee Panda
B: Tuesday 3 - 4 PM: Gloria Wang
C: Wednesday 3 - 4 PM: Derrick Li
D: Wednesday 1 - 2 PM: Jason Bi
E: Thursday 12 - 1 PM: Sara Reynolds
F: Friday 10 - 11 AM: Noah Alcus

Class Capacity: 160 (approx. 30 per discussion)

Course Information

Description: The Blockchain Fundamentals is a comprehensive survey of relevant topics in blockchain offered through the UC Berkeley Decal program. From a technological standpoint, we start with the basics of cryptography and economics, establish a solid fundamental understanding of Bitcoin by building it from the bottom up, and from there, explore the myriad of ideas and technologies relating to blockchain technology. On the non-technical side, we start with the history of digital currency, then look at the laws, organizations, trends, and communities behind it to build a complete picture of the ecosystem surrounding blockchain technology.

Goal: Premise. Many people find it difficult to understand blockchain because it requires the coordination of many components for it to function, and it's hard to see the full picture until all the individual components are fully understood. Furthermore, since the field is very technical and relatively new, blockchain-related discussion by nature is full of jargon. Therefore, it is easy to get lost trying to follow nearly any conversation on blockchain if you have not built up the right background.

Therefore, the goal of this course is to surmount the steep learning curve of blockchain. By the end of this course you will understand how blockchain works and the ideas, technologies, and organizations sprouting from it.

Class Format: 2.5 (non-consecutive) hours a week. The first 1.5 hours will consist of lecture. The other hour will consist of a discussion of topics taught in lecture. These discussions will go in depth on the material and will require participation from everyone. Each student may be required to formulate one question about the lecture material. Due to course size, discussions will be optional replacements for homework, but we will strongly encourage students to attend discussion regularly.

Prerequisites: This course have no formal prerequisites. However, blockchain is very technical in nature, so coming into this course with knowledge of computer science or cryptography will be extremely helpful, although not required. If you have any concerns about the nature of this course, do not hesitate to reach out to the facilitators.

Enrollment: By permission code. Students are required to (1) attend the first lecture and (2) fill out the discussion preference form to receive a discussion assignment. Students who attend their assigned discussion section in the first week of school are given a permission code and course number to enroll with.

Grading: P/NP. You must get at least a 70% to pass the class - to be clear, a lower score equates to a No Pass. Grading will be based on Homework and Quizzes (30%), Attendance (30%), a Final Paper (30%) and Participation (10%). There will be assigned readings each week, which you should complete in order to do well. If you have any questions regarding grades, email your discussion leader.

Homework and Quizzes (30%): There will be homeworks and quizzes dispersed throughout the course and will be weighted equally. Quizzes will be given during the first 5 minutes of class. Homework will be released after Saturday evening after lecture and will be due the following Friday at 11:59 pm.

Quizzes: Quizzes are intended to be a quick, easy screen designed for you to demonstrate that you completed your readings for the current week's topic. We will administer quizzes on random weeks. They will be in the form of 6 multiple choice questions and administered in the first 5 minutes of class. You only have to get 4 of the 6 questions right to get a full score.

Example quiz question:
The creator of Bitcoin is currently unknown. What online alias did they go by?
A) Craig Wright
B) Dorian S. Nakamoto
C) Satoshi Nakamoto
D) Gavin Andresen
E) Nick Szabo

Homework: Homeworks are intended to be interesting prompts. For example, in addition to the occasional write-up, we may have you write your name on the blockchain, or dig up a transaction originating from Silk Road, or comment on Piazza with a paragraph arguing for or against the scalability debate.

Attendance (30%): We will take attendance at the beginning of every class. Please go to only your **ASSIGNED discussion** section. No, you may not switch discussion sections, as we decide sections based on your availability in the beginning of the semester and have limited class sizes. If you are expecting an academic conflict such as a midterm, or have a medical/family emergency, please let your discussion leader know at least 24 hours in advance. We expect excused absences to be rare; we grant you **2 unexcused lecture absences and 2 unexcused discussion absences** without grade penalty.

Final Paper (30%): All students will be required to write a 3-4 page final paper on a topic of their choice relating to the cryptocurrency and blockchain fields. This could relate to a topic covered explicitly in class or something else related to cryptocurrencies. Submitting a final paper is required to pass the class.

Participation (10%): If you actively pay attention and ask questions/contribute in discussion, you can expect a full score. Don't stress out over this.

Textbooks: You are free to read from these books, which are both freely distributed and available online. Please do NOT go out and buy them. Some readings may be pulled from these books during the course.

- Bitcoin and Cryptocurrency Technologies (Princeton textbook) by Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller, and Steven Goldfeder: https://d28rh4a8wq0iu5.cloudfront.net/bitcointech/readings/princeton_bitcoin_book.pdf?a=1
- (Optional/Additional) Mastering Bitcoin by Andreas Antonopoulos: https://drive.google.com/file/d/0B8lgcDXI8hEfbXFYcTh6aXNqRkk/view?usp=sharing
  Source: https://github.com/bitcoinbook/bitcoinbook

Topics

Week of 1/27 — Bitcoin Protocol and Consensus: A High Level Overview

Week of 2/3 — Bitcoin and Blockchain History: From the Cypherpunk Movement to JPMorgan Chase

Week of 2/10 — Bitcoin Mechanics and Optimizations: A Technical Overview

Week of 2/17 — Bitcoin IRL: Wallets, Mining, and More

Week of 2/24 — Ethereum & Smart Contracts: Enabling a Decentralized Future

Week of 3/3 — Game Theory and Network Attacks: How to Destroy Bitcoin

Week of 3/10 — Cryptoeconomics and Proof-of-State

Week of 3/17 — Distributed Systems and Alternative Consensus

Week of 3/24 — Scaling Blockchain: Cryptocurrencies for the Masses

Week of 4/7 — Enterprise Blockchain: Real-World Applications

Week of 4/14 — Anonymity: Mixing and Altcoins

Week of 4/28 — Conclusion: Cool Ideas, Blockchain Hype, and the Future

Questions?

- If you have a content-related question: **Post in Piazza!**
- If you have an administrative question - enrollment, auditing, logistics: **Email Sara** (snreynolds@berkeley.edu).
- If you have a grade or attendance question - excused absence, grade clarification: **Email your discussion leader.**