Bitcoin:
Programming the Future of Money

Topics in Computer Science - ITCS 4010/5010, Spring 2025

Dr. Christian Kümmerle

Lecture 1

Bitcoin: Programming the Future of Money

Questions relevant for this course:

- What is Bitcoin?
- What is money?
- What could the future of money look like?
- What role does programming play?
- What else do we need to learn to understand all this?

COURSE ORGANIZATION

Instructor:
Christian Kümmerle (kuemmerle@charlotte.edu)
Assistant Professor in Department of Computer Science since 2022

Background:
- Ph.D. in Mathematics (Technical University of Munich, Germany)
- Postdoc in Applied Mathematics at Johns Hopkins University

Research Interests:
- Resource & data efficiency in machine learning through parsimonious data models
- Optimization and scalable algorithms with provable guarantees
- Bitcoin-adjacent payment channel networks

Weekly Office Hours:
- Time: **Thursdays, 4:00–5:00 PM**
- Location: Woodward 410D (or Zoom of scheduled by email)
- **Please feel free to drop by!** No need to make appointments.

COURSE ORGANIZATION

Instructional Assistants:

Abheek Das (adas11@charlotte.edu)
Hariharan Vijay Iswaran (hvijayis@charlotte.edu)

Weekly Office Hours:

- Time: **Tuesdays, 1:00-2:00 PM & Fridays, 10:00–11:00 AM**
- Location: Burson Hall 239B or on Zoom
- Zoom Link: https://charlotte-edu.zoom.us/j/95526959172

COURSE ORGANIZATION

Course Lecture Location & Times:

- Tuesdays, **5:30-6:45 PM** in **Cameron Hall 101**
- Thursdays, **5:30-6:45 PM** in **Cameron Hall 101**

Purpose:

- Presentation of new concepts by instructor
- In-class discussion of review questions, prior readings
- Joint study of new concepts

Attendance is required.

WHAT YOU CAN EXPECT IN THIS COURSE

- 25% Economics/ Financial Education <- Indispensable for understanding why we need it
- 50% Computer Science <- Making the concepts work together in practice
- 25% Mathematics <- Indispensable for Cryptography behind Bitcoin

Requirements for this course:

- Curiosity for an interdisciplinary topic
- Knowledge of algorithms and data structures
- Ability to program in Python (object-oriented)

FOCUS OF COURSE

What this **not** the focus of this course:

- About “blockchain” in general (Why not?)
- A course on cryptography in general
- Trading crypto markets
- How to create your own cryptocurrency

COURSE STRUCTURE: DELIVERABLES FOR ASSESSMEN

- **Reading Quizzes** (due each week) & **Class Participation**: Based on concepts in class & required readings
- **Homework** (each 10-14 days, mostly due Tuesdays):
- One pen-and-paper **midterm exam: Tuesday, February 25**
- Pen-and-paper **final exam: Tuesday, May 6**

Breakdown of course grade:

- Homework: **30%**
- Reading Quizzes & Class Participation: **20%**
- Midterm: **20%**
- Final exam: **30%**

HOMEWORKS

- Announced on Canvas, submission in **Gradescope** (link on Canvas site)
- Due every 10-14 days
- Most homework questions: Programming based, or mathematical
- **Collaboration rule:** Discussing problems with colleagues is acceptable if discussion partners are indicated in list of collaborators. However, answers need to be written down individually.
- **Submission format:** Homework submission includes both a PDF and a Jupyter notebook .ipnyb file. Answers should be **written down individually**!
- Count 30% of total grade

READING QUIZZES

- Announced & submission on Canvas,
- Due every week (usually Fridays)
- More focused on the conceptual, philosophical and economics part of class

ACADEMIC INTEGRITY

You are expected to do your own work!

- You may talk to other students about your homework.
- If so: Add those students to a **list of collaborators** when on homework submission.
- You need to write your solution by yourself and **cannot** show it to other students.
- Indicate any online resource you use beyond course materials.

-> Cheating and Plagiarism is taking seriously.

Note: Code of Student Academic Integrity

Questionnaire

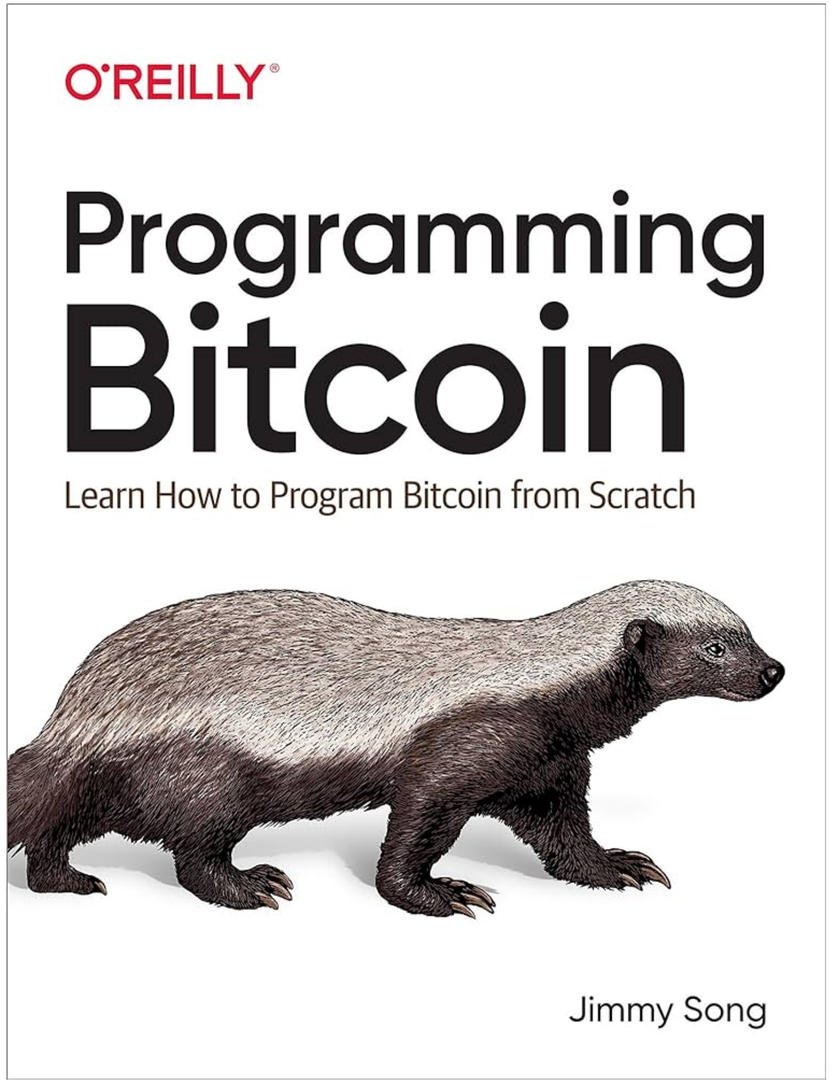
Learning Outcomes

EXPECTED LEARNING OUTCOMES OF THIS CLASS

- **Ability to create your own bitcoin library** from scratch in Python.
- **Analyze how bitcoin works** and **evaluate its strengths and limitations**. Connect to another node on the bitcoin network, calculate what you can spend, construct a transaction of your choice, and broadcast it over the bitcoin network.
- Solid understanding of the b**asics of public key cryptography** and **digital signatures**
- Familiarity with the **challenges and approaches for decentralized consensus mechanisms**
- Understanding of the **economic and philosophical foundations of bitcoin** and the economic problem that bitcoin attempts to solve, evaluate its impact on the global financial system
- Experience the a**bility to recreate and reimplement an end-to-end system** with real-life implications
- Gain literacy in digital assets, gain **insights into career paths in the digital assets / cryptocurrency industry**

Textbooks and other References

PRIMARY TEXTBOOK



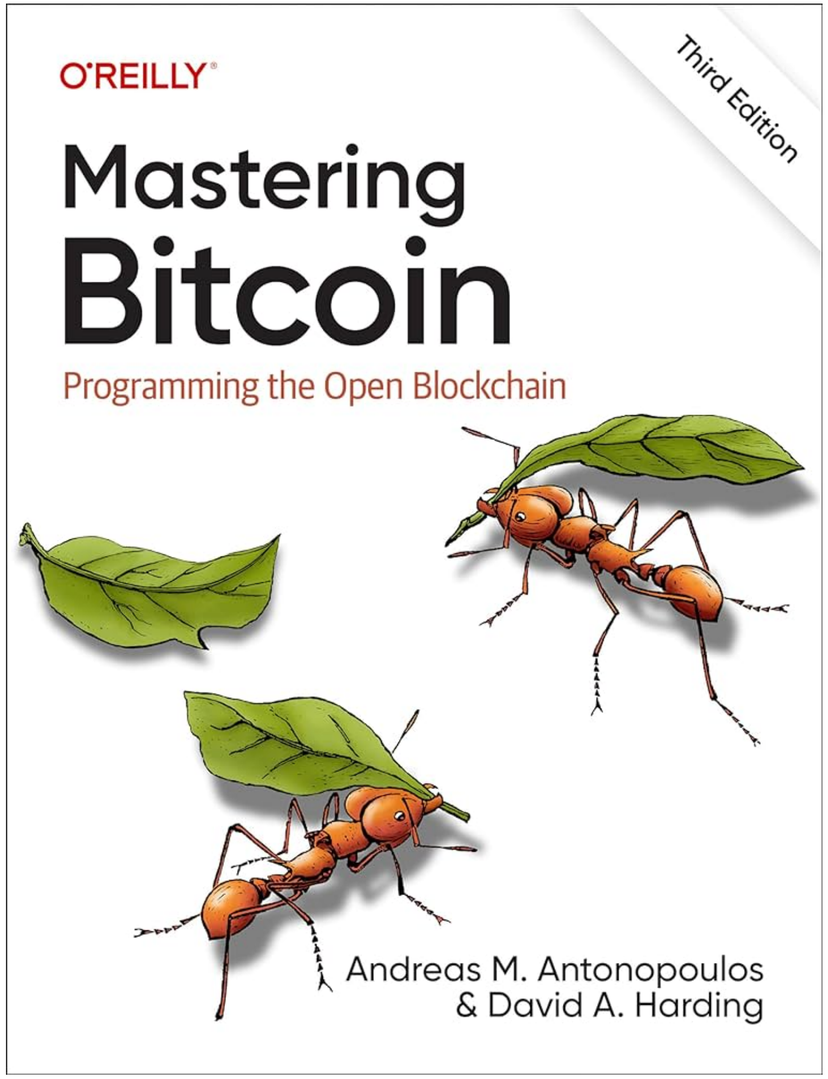
Jimmy Song. **Programming Bitcoin: Learn How to Program Bitcoin from Scratch**, 1st Edition, O'Reilly, 2019.

- Link to publisher
- All chapters are available in html on GitHub
- Recommendation: **Buy a copy of this book!**

Guide for technical part of learning
to understand bitcoin from the scratch.

Uses object-oriented Python for coding exercises!

SECONDARY TEXTBOOK

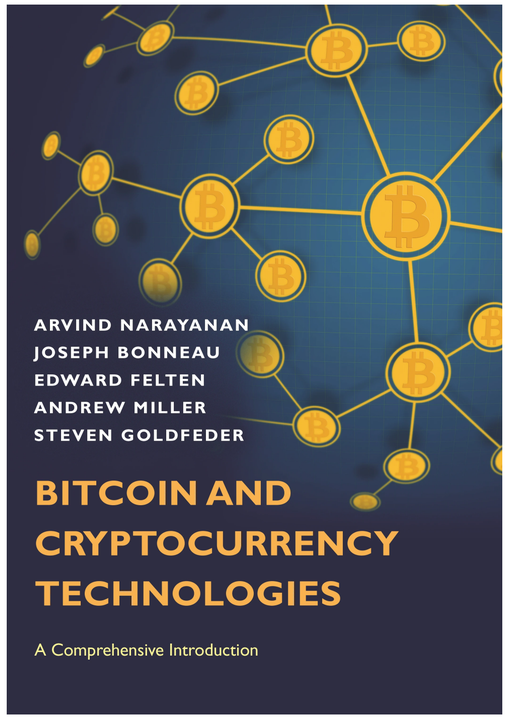


Andreas Antonopoulos, David Harding.
Mastering Bitcoin: Programming the Open Blockchain, 3rd Edition,
O'Reilly, 2023.

- Link to book page at publisher O'Reilly
- All chapters are available in html on GitHub

More conceptual than the book by Jimmy Song, but also great technical resource.

TERTIARY TEXTBOOK



Bitcoin and Cryptocurrency Technologies

Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller, Steven Goldfeder

with a preface by Jeremy Clark

Draft — Feb 9, 2016

Feedback welcome! Email bitcoinbook@lists.cs.princeton.edu

For the latest draft and supplementary materials including programming assignments, see our Coursera course.

The official version of this book will be published by Princeton University Press in 2016. If you'd like to be notified when it's available, please sign up here.

Narayanan, Bonneau, Felten, Miller, Goldfeder.
Bitcoin and Cryptocurrency Technologies,
Princeton University Press, 2016.

- Free PDF available

Focus slightly more on cryptocurrencies in general and their challenges, and connection to economical considerations

WHY SHOULD YOU TAKE THIS CLASS? - STUDENT OPINIONS FROM LAST SEMESTER

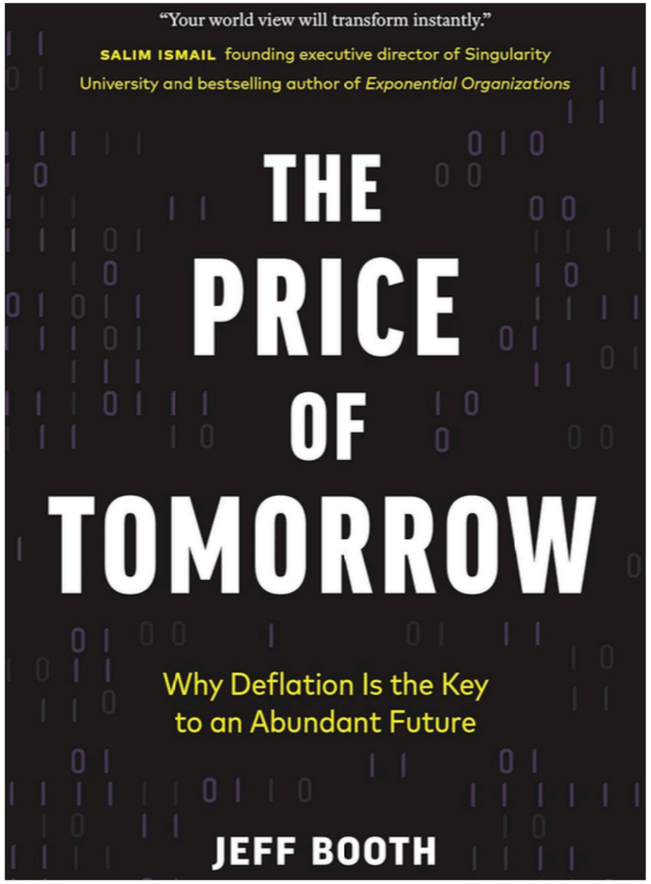
- “This class is great not just for because it's fun or interesting but it can definitely impact your career and financial choices.”

- “I would recommend this course to anyone interested in understanding the fundamentals of Bitcoin and cryptocurrency. It provides a solid foundation on blockchain technology, its real-world applications, and the potential impact on the financial system. However, be prepared to engage with technical concepts and financial theories—it’s a mix of hands-on and conceptual learning.”

- “If you are looking for a challenging programming class and you are interested in Bitcoin specifically then it might be a good choice.”

Why Bitcoin?

BITCOIN AS GLOBAL PERMISSIONLESS MONETARY NETWORK



IN THE SENATE OF THE UNITED STATES

Ms. LUMMIS introduced the following bill; which was read twice and referred to the Committee on _____

A BILL

To establish a Strategic Bitcoin Reserve and other programs to ensure the transparent management of Bitcoin holdings of the Federal Government, to offset costs utilizing certain resources of the Federal Reserve System, and for other purposes.

Be it enacted by the Senate and House of Representa-

(4) The acquisition and long-term storage of substantial quantities of Bitcoin by the United States can strengthen the financial condition of the United States, providing a hedge against economic

Motivation:

- AI & technology as deflationary force
- Weaponization of US-centered financial system
- Debt and Affordability Crisis, Short-Termism
- Lack of Access for Global South / ``Unbanked''

What is Bitcoin?

THE BITCOIN WHITEPAPER (OCTOBER 31, 2008)

[Link to the Bitcoin whitepaper]

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

1. Introduction

Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust based model. Completely non-reversible transactions are not really possible, since financial institutions cannot

THE BITCOIN NETWORK

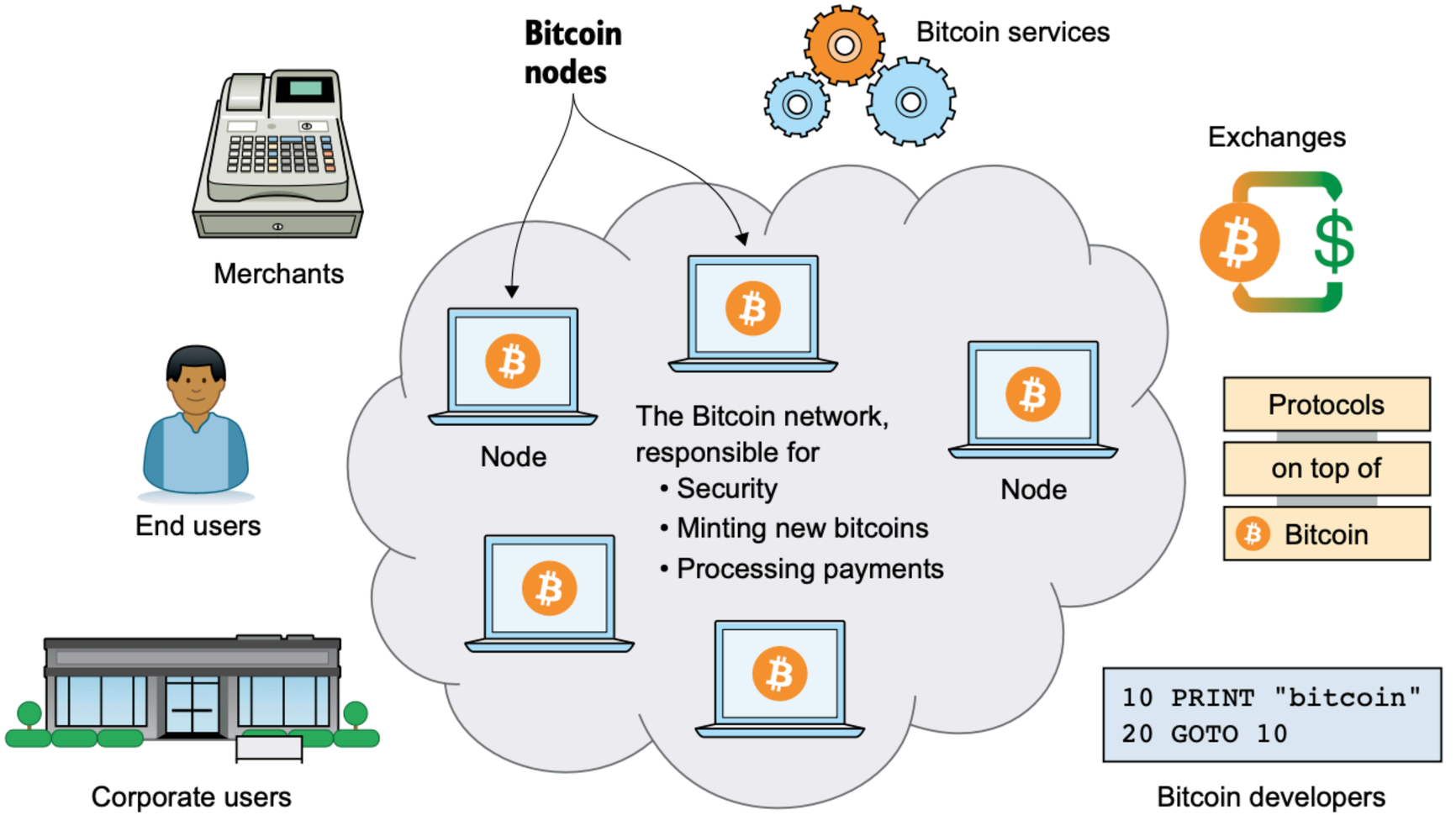


Figure 1.1 The Bitcoin network and its ecosystem