UNIVERSITY OF NORTH CAROLINA CHARLOTTE

Topics in Computer Science
Bitcoin: Programming the Future of Money
ITCS 4010 & 5010 - Fall 2024

Draft of Course Syllabus

Instructor: Dr. Christian Kümmerle	**Course Number:** ITCS 6156 and ITCS 8156
Email: kuemmerle@charlotte.edu	
Course Lecture:	**Instructor's Office Hours:**
Tuesdays, 5:30-6:45 PM	Tuesdays, 3:00-4:00 PM
Thursdays, 5:30-6:45 PM	Thursdays, 3:00-4:00 PM
Location: Woodward 130	in Woodward 410D & via Zoom
Teaching Assistant: To be determined	

Summary: 15 years after its inception, the bitcoin cryptocurrency and its protocol has not only achieved a significance presence in national and global financial markets, but also has established itself as a tool for freedom from authoritarianism, political strife and inflation. While the context and implications of decentralized, sound money are economic, its implementation and technical foundations combine a variety of ideas in computing.

In this class, we examine the technical and economic foundations of bitcoin. In particular, we study public key cryptography, digital signatures, the blockchain, consensus via proof-of-work, hash functions, networking, as well as monetary theory, game theory and central and commercial banking. We also study alternative cryptocurrency designs and consensus mechanisms such as proof-of-stake, as well as attacks and challenges and possible approaches for their mitigation.

Learning Objectives:

- 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 basics 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 ability 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

Expected Background: Students are expected to be comfortable with Python programming in Python (at least, you should be willing to learn it while taking the class). Data Structures and Algorithms (ITSC 2214) is also expected to be known.

More generally, interest in interdisciplinary ideas is important in this class as we will cover across mathematics, computer science and economics.

Course Topics (Tentative List):

- Properties of money
- Fundamentals of banking
- The role of central banks / the Federal Reserve
- The problem of electronic cash
- Hash functions
- Basics of cryptography
- Finite fields and elliptic curve cryptography
- Nakamoto consensus
- Bitcoin transactions
- Bitcoin script
- Multisignature
- Basics of networking
- Game theory of Bitcoin
- Bitcoin & Energy markets
- Ethical aspects of Bitcoin vs. fiat money
- Scaling approaches for Bitcoin
- Lightning Network
- Proof-of-stake consensus

Grading: Your final grade for the class will be given as a weighted average with the weights given as follows:

- Homeworks: 30%
- Class participation: 10%
- Midterm exam: 25%
- Final exam: 35%

Academic Integrity: You are expected to work independently on your homework and quiz submissions. Any violation of the Code of Student Academic Integrity will be taken very seriously.
Discussion of homework questions on a high level with another student(s) is allowed **if this is indicated** in the list of collaborators when submitting a homework, **and only in this case.** Even in this case, the solutions need to be written up individually.

Textbooks & Relevant Literature:

- Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, USENET Cryptography Mailing List, Nov 2008.
- Andreas Antonopoulos, David Harding, *Mastering Bitcoin: Programming the Open Blockchain* 3rd Edition, OReilly, 2023.

- Jimmy Song, *Programming Bitcoin: Learn How to Program Bitcoin from Scratch*, 1st Edition, O'Reilly, 2019.
- Micah Warren, *Bitcoin: A Game-Theoretic Analysis,* De Gruyter, 2023.
- Saifedean Ammous, *The Bitcoin Standard: The Decentralized Alternative to Central Banking*, Wiley, 2018.
- Lyn Alden, *Broken Money: Why Our Financial System Is Failing Us and How We Can Make It Better,* Timestamp Press, 2023.
- Alex Gladstein, *Check Your Financial Privilege*, BTC Media, 2022.