UNIVERSITY OF NORTH CAROLINA CHARLOTTE

Topics in Computer Science

Bitcoin: Programming the Future of Money

ITCS 4010 & 5010 - Fall 2024

Course Syllabus (Version of September 2, 2024)

Instructor: Dr. Christian Kümmerle	**Course Number:** ITCS 4010 and ITCS 5010
Email: kuemmerle@charlotte.edu	
Course Lecture:	**Instructor's Office Hours:**
Tuesdays, 5:30–6:45 PM	Wednesdays, 3:00–4:00 PM
Thursdays, 5:30–6:45 PM	Thursdays, 4:00–5:00 PM
Location: Woodward 130	Location: Woodward 410D
	(or on Zoom if scheduled by email)
Teaching Assistant: Sindura Saraswathi	**TA's Office Hours:**
Email: ssarasw2@charlotte.edu	Mondays, 10:00–11:00 AM
	Tuesdays, 3:00-4:00 PM
	Location: Woodward 412 and on Zoom
Zoom Link:	https://charlotte-edu.zoom.us/j/95526959172

This syllabus contains the policies and expectations I have established for this course. Please read the entire syllabus carefully before continuing in this course. These policies and expectations are intended to create a productive learning atmosphere for all students. Unless you are prepared to abide by these policies and expectations, you risk losing the opportunity to participate further in the course. The standards and requirements set forth in this syllabus may be modified at any time by the course instructor. Notice of such changes will be by announcement in class or by email.

Course 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

Homeworks: Every 10-14 days, a homework assignment will be due for submission. Each homework will be published on Canvas. The homework typically consists of Python coding exercises or are of mathematical nature. Less common are more economic questions.
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 (created from a Jupyter notebook .ipynb

file) and the .ipynb file itself, unless indicated otherwise. Please upload your homework submission to the respective Gradescope assignment. Depending on the grading load, we might take the freedom of grading only a subset of submitted answers. The due date of homework varies, but is either **Tuesday at midnight (11:59 pm)** or **Friday at midnight (11:59 pm)**. If you get stuck with a problem or have questions, please ask the instructor or the teaching assistant for help.
Late Submission Policy for Homeworks: Each student has can use two days for late homework submission to be used within the semester without penalty. Further late submission will be penalized as follows:

- Less than 24h late: Score is 75% of graded score.
- Between 24-48h late: Score is 50% of graded score.
- Between 48-72h late: Score is 25% of graded score.

Class Attendance and Participation: Due to its interdisciplinary nature, a crucial part of this course is in-class participation and discussion. For this reason, **class attendance is required**. Up to two unexcused absences during the semester do not affect negatively your attendance credit. We refer also to the UNC Charlotte Academic Policy: Course Attendance and Participation.

Reading Quizzes: You are expected to read assigned articles or chapters for each module. Each week, comprehension and discussion questions und quizzes need to be answered, some of which may be open-ended. The submission of your answers is typically due on **Friday at midnight (11:59 pm)**. Class participation and the reading quiz answers make up jointly for the "Reading Quizzes & Class Participation" grade.

Midterm Exam: A written, pen-and-paper midterm exam of 75 minutes duration will take place on **Tuesday, October 8**.

Final Exam: The final exam is a comprehensive, written, pen-and-paper course exam. It will take place on **Tuesday, December 10**, from 5:00PM to 7:30PM. **Grading:** Your final grade for the class will be given as a weighted average with the weights given as follows:

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

Academic Integrity: You are expected to work independently on your homework and quiz submissions. For homeworks, it is allowed to discuss problems with other students; if you do that, the discussion partner(s) have to be indicated on the submitted homework documents (see collaboration rule above). However, answers need to be written down individually. Any violation of the Code of Student Academic Integrity will be taken very seriously.
In this course, you are **not** permitted to use generative AI tools such as ChatGPT to obtain answers for quizzes or homework assignments. An exception to this policy only applied if explicitly mentioned by the instructor. Any unauthorized use of a generative AI tools may constitute a violation of the Code of Student Academic Integrity and can be sanctioned accordingly.

Course Textbooks (mandatory):

- Jimmy Song, *Programming Bitcoin: Learn How to Program Bitcoin from Scratch*, 1st Edition, O'Reilly, 2019. Chapters available on **[GitHub]**.
  This is the main technical textbook we follow in class. While the chapters are in a non-PDF format available on Github (and can be compiled into PDF locally), we recommend buying this book.

- Andreas Antonopoulos, David Harding, *Mastering Bitcoin: Programming the Open Blockchain* 3rd Edition, O'Reilly, 2023.
  This is the secondary technical textbook we follow in class. Chapters are also freely available on **[GitHub]**.

- Narayanan, Bonneau, Felten, Miller, Goldfeder, *Bitcoin and Cryptocurrency Technologies*, Princeton University Press, 2016.
  A free pre-publication version is ***available here***.

Additional Key Literature:

- Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, USENET Cryptography Mailing List, Nov 2008.

- Kalle Rosenbaum, *Grokking Bitcoin*, Manning, 2019. Full book available here.

- Micah Warren, *Bitcoin: A Game-Theoretic Analysis,* De Gruyter, 2023.

Relevant Literature on Philosophical, Political and Economic Foundations of Bitcoin:

- Saifedean Ammous, *The Bitcoin Standard: The Decentralized Alternative to Central Banking*, Wiley, 2018.

- Website of the *Satoshi Nakamoto Institute*.
  Website with full correspondence of S. Nakamoto and with links to key essays and papers on the foundations of digital money, economic, etc.

- 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.

Course Materials and Copyright: These lectures and course materials, including presentations, tests, exams, outlines, and similar materials, are protected by copyright. Myself, or the indicated authors of adapted materials are the exclusive owner of copyright in those materials. I encourage you to take notes and make copies of course materials for your own educational use. However, you may not, nor may you knowingly allow others to reproduce or distribute lecture notes and course materials publicly without my express written consent. This includes providing materials to commercial course material suppliers such as CourseHero, Chegg, and other similar services. Students who publicly distribute or display or help others publicly distribute or display copies or modified copies of an instructor's course materials may be in violation of University Policy 406, The Code of Student Responsibility, or University Policy 407, Code of Student Academic Integrity. This course has been partially inspired from the following courses:

- Korok Ray, *The Bitcoin Protocol*, Texas A&M University, ACCT/CSCE 489, Spring 2023.

- Gary Gensler, *Blockchain And Money*, MIT, 15.S12, Fall 2018, available at MIT OpenCourseWare.

- Arvind Narayanan, *Bitcoin and Cryptocurrency Technologies*, taught on Coursera, originally at Princeton University, more information available here.

Disability Services: Many students have visible or invisible disabilities. UNC Charlotte is committed to access to education and offers accommodations that allow all students to achieve their full potential. If you have a disability and need academic accommodations, please send me your accommodation letter as early as possible. You are encouraged to meet with me to discuss the accommodations outlined in your

letter. For more information on accommodations, contact the Office of Disability Services at 704-687-0040 or disability@uncc.edu.

Non-Discrimination: No student will be discriminated against in this class based on age, race, nationality, religion, sexual orientation, gender identity/expression, veterans status, country of origin, or group affiliation. You are expected to behave in a respectful manner towards others in the class, both in virtual and face-to-face settings. Continuous or repeated disrespectful behavior will be considered to be creating a hostile environment, which constitutes a violation to the University Policy 406, Code of Student Responsibility. In such a case, you will be referred to the Office of Student Conduct or the Office of Civil Rights and Title IX. Based on such referral, the Director or designee will determine whether a Formal Charge(s) shall be pursued and whether the Formal Charge(s) constitutes a Minor Violation or a Serious Violation, based on your prior record or facts and circumstances related to the case.