

Introduction to Blockchain and Cryptocurrencies Spring 2023 Syllabus

INSTRUCTORS

Professor Gur Huberman

E-mail: gh16@columbia.edu

Professor Omid Malekan

E-mail: om44@columbia.edu

[Office Hours: By Appointment](#)

Course Description

This course will introduce the fundamental building blocks of blockchain technology as well as its application in cryptocurrencies, stablecoins, decentralized finance and non-fungible tokens (NFTs). It will begin by covering the fundamentals of money, banking, and payment systems, as well as relevant areas of computer science such as cryptography and distributed systems. Special attention will be paid to the different building blocks of the Bitcoin network and how they work together, and the unique attributes of the Ethereum platform.

The course will then shift towards specific applications beyond cryptocurrency, including stablecoins, central bank digital currencies, decentralized finance, non-fungible tokens, gaming, DAOs and Layer 2 solutions. It will touch on alternative consensus mechanisms such as proof of stake and wrap up with a focus on the legal and regulatory implications.

Given the evolving nature of the topic, the content will be modified on the fly to address real world developments. While not an investment class, it will touch on important market developments as a lens through which we can revisit first principles. Every class will begin with a quick analysis of recent headlines. There will be speaker presentations throughout the course as well as live demos.

Course Co-Requisites

Capital Markets and Investments (B8306/B7306)

Grading

There will be reading and homework assignments throughout the course, some of which will be completed in groups. The midterm will be a take-home closed book individual exam on fundamental concepts. For the final, each group will pick either an existing platform or application to conduct a critical review of or submit a proposal for something new. They will give a brief presentation in class and submit a five-page paper. The final project grade will be based on overall comprehension, analysis of the economics of the solution, governance, and the go-to-market strategy.

Course grades will be determined as follows: 30% final project, 30% assignments, 20% midterm and 20% participation.

TENTATIVE OUTLINE:**Class 1 – Money, banking & payment systems**

This session will provide theories on the origins of money and its history. It will cover the generally accepted functions of money as well as its characteristics. It will discuss the basics of banking and the design of payment systems.

Class 2 – Consensus, hash functions & asymmetric cryptography

The primary focus of this class will be the computer science foundations of blockchain & cryptocurrencies. We will cover distributed systems and the challenges of reaching consensus. We will also review hash functions and public-key cryptography.

Class 3 – Blockchain, Immutability and Nakamoto Consensus

We will begin by learning about the invention of blockchain and how it predated Bitcoin. We'll then shift gears to Bitcoin, with a focus on Nakamoto Consensus, its use of economic incentives, mining & transaction fees, cryptographic identity and algorithmic inflation.

Class 4 – Bitcoin, Mining, and the Longest Chain

This class will focus on how all the topics covered so far come together to form a living ecosystem that continuously pulls order out of chaos. It will cover probabilistic finality, transaction fees and the mining tournament. It will end with a live demo of a Bitcoin transaction.

Class 5 – Ethereum, Smart contracts and Tokens

This session will cover conditional transactions as enabled by the second most prominent blockchain platform, tokens, and the notion of trustless computing. It will provide a history of the Ethereum ecosystem, discuss its challenges, and review several prominent applications built on top of it.

Class 6 – Midterm review, Attacks, Forks and The DAO.

This session will review all of the concepts covered so far and discuss how a miner with sufficient hash power can successfully execute a double spend attack. It will then cover different types of forks as resulting from latency or a change in the rules of the protocol. It will culminate with a review of a famous attack on a decentralized application on Ethereum and the resulting controversy.

Class 7– Stablecoins central bank digital currencies (CBDCs)

This class will begin by discussing the nature of banking and cover the celebrated Diamond-Dybvig model of bank runs. It will then review the existing payment industry, before shifting to fiat-backed stablecoins, their history, unique properties, and challenges. It will end with the possibility of governments using blockchain tech to issue central bank digital currencies (CBDCs).

Class 8 – Decentralized Finance

This session will cover decentralized applications for trading, credit creation, money markets and synthetic assets, with a deep dive into several prominent projects and a live demo of using one. It will cover the emergence of new financial primitives, yield farming and the power of composability.

Class 9: Proof of stake, Alternative L1s, Lightning and L2s

This class will review proof of stake consensus, the coming change in Ethereum's consensus mechanism and competing proof-of-stake Layer-1 blockchains (L1s). It will then shift to the Lightning Network, the most prominent Layer-2 solution for Bitcoin, and end with a review of various L2s on Ethereum.

Class 10 – Web3, Non-Fungible tokens and DAOs

This session will focus on the emergence of NFTs and the implications for content creation, digital art, collectibles and gaming. It will review the proposed benefits and limitations of decentralized versions of existing online platforms (known collectively as Web3) and touch on DAOs and blockchain gaming.

Class 11 – Web3 continued, Regulatory & legal issues; The world to come

This session will continue to expound on the broader applications of blockchain tech and cryptocurrencies to domains beyond money and banking. It will then cover the regulatory and legal challenges of this domain, including securities laws and anti-money laundering.

Class 12 – Student presentations of their final projects