Columbia Business School

Introduction to Blockchain and Cryptocurrencies
Fall 2023

INSTRUCTOR
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 present each in the context of how the world works today and how it might be re-architected due to new methods of building trust in a digital setting.

It will begin by covering the fundamentals of money, then cover computer science topics such as cryptography and distributed systems. These building blocks will be combined to explain Bitcoin and its innovative use of Proof of Work, along with the unique attributes of Ethereum and Proof of Stake.

The course will then shift to specific applications like stablecoins, central bank digital currencies (CBDCs), decentralized finance (DeFi), non-fungible tokens (NFTs), Layer 2 solutions, and Web3. It will touch on alternative protocols. It will also cover the legal, regulatory, and geopolitical implications of a new financial order.

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. Every class will begin with a discussion of recent headlines. There will be speaker presentations and live demos throughout the course.

Every student will be given a small amount of cryptocurrency at the start of the semester. There will be weekly assignments and tutorials using actual crypto projects. All students will earn a commemorative NFT upon completion of the course.

Course Co-Requisites

Capital Markets and Investments (B8306/B7306)

Grading

There will be reading and homework assignments throughout the course, some to be completed in groups. Some assignments will involve on-chain tasks. The midterm will be a take-home closed-book individual exam on fundamental concepts.

For the final, each group will either review an existing crypto project or propose their own. They will give a short presentation in class then submit a five-page paper. Grades 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 – Why we are here, Money & Consensus

This session will begin with a demonstration of the disruptive power of crypto. It will move on to the origin and properties of money, covering its generally accepted functions and characteristics. It will introduce the topic of distributed consensus.

Class 2 – Consensus, Hash functions & Asymmetric cryptography

The primary focus of this class will be the computer science foundations of blockchain & cryptocurrencies. We will complete consensus and the challenges of reaching it in any decentralized setting. We will then cover hash functions and public-key cryptography.

Class 3 – Blockchain, Immutability & 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, the mining tournament, the longest chain rule, fees, and inflation.

Class 4 – Bitcoin & Ethereum

This class will review the mechanics of proof of work (PoW) and the process of continuously pulling order out of chaos. It will touch on the environmental question. It will then shift to Ethereum and introduce the novel features of tokens and smart contracts, gas fees, and the appeal of decentralized applications.

Class 5 – Ethereum & Proof of Stake

This session will cover proof of stake (PoS) and the use of pure financial incentives to secure a decentralized network. It will cover the mechanics of staking as compared to mining and the pros and cons of each. It will then introduce the notion of trustless computing and review popular applications on Ethereum.

Class 6 – Midterm review. Sybil Resistance, Attacks & Forks

This session will review all the concepts covered so far. To reemphasize important first principles, it will introduce the notion of a Sybil Attack and explain how PoW & PoS are

designed to deter one. It will introduce different types of forks resulting from latency or a change in the rules of a protocol.

Class 7– Stablecoins & Central bank digital currencies (CBDCs)

This class will begin by discussing the nature of banking and payment systems as understood in the worlds of finance and FinTech, their benefits and drawbacks. It will then shift to fiat-backed stablecoins, their history, current state, and overall appeal. It will end with the possibility of governments using blockchain tech to issue central bank digital currencies (CBDCs). Attention will be paid to the disruptive potential of both in banking and beyond.

Class 8 – Decentralized Finance (DeFi)

This session will cover decentralized applications for trading, credit creation, money markets and synthetic assets, with a deep dive into several prominent projects and the transformative power of automated market makers.

Class 9: DeFI continued. Alternative L1s, Scaling & Layer-2 solutions

This class will continue the DeFi lecture by introducing yield farming and the power of composability. It will then shift to a survey of the leading alternative layer-1 platforms. It will then shift to scaling solutions such as the Lightening Network for Bitcoin and rollups on Ethereum.

Class 10 – Digital Scarcity, Non-fungible tokens (NFTs) & DAOs

This session will kick off with a discussion of digital scarcity and its social and financial implications. It will review the emergence of NFTs and the potential impact on content creation, art, rewards, 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, anti-money laundering and macroprudential risk. It will wrap up with a discussion of what the future may hold.

Class 12 – Student presentations of their final projects