Blockchain, Cryptocurrencies and Digital Tokens Demystified

B8776-001 – Summer 2021
Blockweek Course, 3.0 Credits (live online)
Monday, May 3 to Friday, May 7 (all inclusive), 10:00 to 18:00 EST

Faculty
R.A. Farrokhnia

Office Hours (May 3-7)
After class, 18:00-19:00 EST

Email
farrokhnia@gsb.columbia.edu

IMPORTANT: The class curriculum is comprised of six modules, to be offered as an online/remote course. No prior technical or advanced math background is required. Nonetheless, given the accretive and sequential nature of the course lectures, it is imperative to attend all sessions and actively participate in class discussions. This course will cover introductory to intermediate-level topics in regard to the underlying technologies. Absence from the first day will result in automatic forfeiture of your registration. Auditing is not permitted (no exceptions)!

COURSE SUMMARY

The publication of the pioneering whitepaper by Satoshi Nakamoto on Bitcoin in October 2008 and the creation of its reference implementation heralded a new era in digital currencies and distributed systems, with many other innovations having followed since in a variety of disciplines. By solving a myriad of technical and financial challenges that had impeded the actualization of digital currencies, blockchain and Bitcoin protocols have also enabled the emergence of other imaginative and disruptive ideas for use in and beyond financial services. Given that nascent aspect of these concepts and the startups they have spawned, it may be too early to judge the success, or the lack thereof, of many of them. Nonetheless, there is little doubt about the profound potential effect and future impact of blockchain, cryptocurrencies, and distributed protocols (including consensus) on financial services, technology, economics, trade, healthcare, government, and other relevant realms.

Indeed, it is easy to recognize that we are still in the very early phases of development in this field, and many important questions in regard to implications in classical economics theories, monetary policies, role of central banks, economic growth, fiscal
policies and tax collection, access to financial products, national sovereignty, cybersecurity, and others are yet to be definitively addressed. As such, gaining a solid understanding of the innerworkings and underlying technologies, protocols, and ecosystems is critical in order to see through the hype and discern the real potential.

This class offers a comprehensive and interdisciplinary primer on the aforementioned subject matters, with a format particularly suitable and accessible for those who have little or no technical background. We will start by covering the basics and fundamental building blocks of the technological developments and innovations that made distributed systems and digital currencies such as blockchain and Bitcoin, respectively, possible. We will ultimately end the course on more complex topics and the latest research in the field, including the fundamental challenges to our existing economics and financial frameworks and the incumbent firms as well as potential solutions to such matters.

By the course’s conclusion, students will have a firm overview and thorough knowledge of blockchain, cryptocurrencies, and digital tokens ecosystems, real-world applications, and impending questions that are yet to be answered. Participants will also be able to follow literature and technical news with ease, interact with industry participants, formulate ideas and corporate strategy initiatives, and continue learning more advanced topics at their own pace after the completion of the course.

As for the intended audience, MBAs or students from engineering, law, medical, or other graduate schools with an interest in the curriculum who intend to pursue careers in finance, technology, or startups will find the course particularly beneficial, including those with roles as future managers, business development and operations, consultants, strategists, and entrepreneurs. As mentioned, no prior programming, technical, or advanced mathematical skills are required (see prerequisites).

**CURRICULUM FORMAT**

In summary, the course curriculum is divided into six modules, covering each of the following topics in sequence:

1. Fundamentals of communication networks and web protocols
2. Cryptography and encryption, with a special focus on construct and applications in Blockchain
3. The theory and practice of Blockchain and distributed systems as well as their implementations
4. Bitcoin, the most widely used (thus far!) use case of Blockchain
5. Cryptocurrencies and Digital Tokens
6. More complex topics + latest research and industry developments
In each module, we will cover the background, foundational elements, and technologies underlying the topics at hand, discuss and understand how all the elements, first individually and then as a group, fit together in the overall ecosystem. More details on each module will be shared during the first class session.

**COURSE PREREQUISITES**

There are no required prerequisites. Recommended, but not required, courses are: 1) "Capital Markets and Investments" (B8306), and 2) general familiarity with tech/programming through either a class such as “Web App Programming in Python” (B8126) or “Introduction to Programming Using Python” (B8136) – having taken these classes would be helpful, but again, it is not a requirement.

**GRADING**

This course has a demanding curriculum and requires active participation, diligence, and on-time completion of readings and assignments prior to each session. Relevant materials (articles, cases, notes, white- and research papers, news articles, videos, etc.) will be posted in Canvas and/or handed out in before each session.

The final course grades will be calculated using the following criteria:

a) Final Project and Presentation (50%)
b) Class Participation (40%)
c) In-class exercises and activities (10%)

Details of the grading components mentioned above are:

a) **Final Project** (with presentations): during the last day of class, students working in groups of up to 5 per team, will present a novel use of blockchain, application specific tokens, distributed consensus systems, or an innovative use-case of the technologies and protocols learned in class. These could be an existing startup or an idea put forth by the student groups themselves.

Each team will present for 5 minutes, followed by up to 5 minutes of Q&A. Electronic copies of the presentation should be delivered ahead of time. Additional instructions will be provided in class during our first session, including the idea generation and validation process (to be completed no later than the third session).

In addition to the final presentations, student groups are required to submit a “feasibility study” white paper (maximum of 15 pages, single-spaced) with a
comprehensive analysis detailing the idea’s origin, its business proposition, merit, market report, underlying technical implementation, competition, and other applicable evaluative analyses. The deadline to submit this written assignment is **Thursday May 20th, 2021 at 12:00 noon EST.** Please email your final paper to the course TAs before the deadline.

b) **Class Participation:** fairly self-explanatory! We will cover the details during our first class. Note that attendance is part of this, and be sure to have your camera on as it'll be part of your participation grade.

**Note on Class Attendance:** for Summer 2021 and in light of COVID-19 circumstances, for students who may be in different time zones than New York (EST), we will follow the CBS policy stating that "students located in a time zone where class falls outside the window from 6:00 to 22:30 (i.e. 6 am to 10:30 pm) local time will be permitted to attend class asynchronously via video recordings. Students who do not view the class live must watch the recording within 24 hours of posting in order to be considered as having attended."

c) **In-class exercises and activities:** throughout class, we will engage in a number of interactive exercises, polls, debates, discussions, quizzes, or similar activities, including with a handful of our guest presenters. Your active and constructive participation in these exercises is an important part of the learning process, and will contribute to your final grade.

**Note:** Students who cannot participate in class live due to time zone difference shall submit Company Debriefs in lieu of in-class exercises and activities for course grading. Each such student will choose a blockchain-based or a digital token venture to conduct research on and submit a two- to three-page executive summary report on its core product/service, funding, team, market, and competition. These reports will be due no later than Friday, May 10th, 2021 at 12 noon EST. Please email your reports to the course TAs before the deadline.

**EXPECTATIONS AND CONDUCT**

Given the complexity of the technical topics covered, students are expected to devote significant time to this class. In order to have meaningful discussions, it is imperative that you come prepared ahead of each session. Class attendance and participation is an integral part of this course learning process, and as such, unexcused absences and disruptive behavior will not only have a detrimental effect on your final grade, but also will be considered disrespectful to your classmates. PLEASE minimize disruptions and
distractions at your place of residence to maximize your learning and respect for your peers.

During the last two modules, we will interact via video conference calls with a few entrepreneurs, practitioners, and legal experts. In order to show the due respect and proper appreciation for the time and effort undertaken by such individuals to participate in and contribute to the course, it is imperative that all students be in full compliance with Columbia’s honor code of professional conduct.

OFFICE HOURS

Students are encouraged to take advantage of course faculty’s office hours. Given the scheduling format of block week classes, office hours will be offered after the end of each day’s session. If you need to schedule an individual time with the course faculty, please email the course TA and you’ll be given details for a one-on-one Zoom call.

Thank you for your interest in this course, and I look forward to having a fun, educational, and productive class with you all.
Curriculum

The course topics and content roadmap over its six modules are as follows:

Module 1: Communication Networks

In this module, we will introduce the fundamentals of how the internet and communication networks operate in general. We will cover some of the most relevant protocols and technologies (hardware and software) inherent and necessary to a functioning network – these include HTTP, TCP/IP, FTP, LAN, WLAN, 802.11, SMTP, POP/IMAP, DNS, SSH, TLS, and general routing and switching protocols. We will also introduce concepts on P2P, network security, points of failure, malware, countermeasures, and attack protection.

Module 2: Cryptography and Encryption

Building on previous week’s content, the second module will be a deep dive into the history of cryptography and cryptographic primitives, covering methods such as cipher shift, Vigenère cipher, one-time pad cipher, Enigma, Lucifer, key distribution problem, integer factoring, one-way functions, modular arithmetic, RSA, public/private key exchange and cryptography, digital signatures, PGP, elliptic curves, ECDSA, zero-knowledge proof, quantum computing and cryptography, Shor’s algorithm, and what the future may hold for cryptography. We will use a series of real-life case studies and exercises to understand the application and implications of a number of important tools discussed throughout this module.

Module 3: Blockchain and Distributed Systems

With the necessary knowledge and tools at hand, in this third module we will now begin studying decentralized systems and how all the prior topics come together to enable blockchain, which by itself was a notable and innovative development building upon years of progress in computer science, mathematics, and cryptography. We will study centralized and decentralized ledgers, cryptographically-verifiable transaction blocks, secure hash algorithms (MD-4 and 5 + SHA-0 to -3, with a special focus on SHA-256), applied one-way functions and modular arithmetic in blockchain, anonymity, pseudonymity, unlinkability, Byzantine agreement and fault tolerance, password salting and peppering, and how cryptographically-verifiable transaction blocks link together to form a chain while preventing rewrite, edits, and fraudulent transaction-insertion into the chain (“append-only” ledgers). Mining will also be introduced as a concept, and the details covered at length in module 4. We will also begin looking at the application of
blockchain (public and private) in various realms (e.g. finance, accounting, trade, government, social impact, NGOs, and creative enterprises).

Module 4: **Bitcoin**

Our coverage of the most well-known and successful (thus far!) digital currency begins in this fourth module, in which Bitcoin and all its moving parts as a cryptocurrency are discussed in detail. Topics include leveraging blockchain to create a decentralized cryptocurrency (including the original Bitcoin whitepaper), Bitcoin wallets, individual transactions and transaction blocks, block size, computational cryptographic “puzzles”, hash pointers, Merkle trees, nonce, nonce solver (block-specific), mining (including virtual mining), proof of work, proof of stake, (reward) tokens, difficulty levels and system adjustments, computing power and electricity usage, CPUs, GPUs, (ASSPs), FPGAs, ASICs, ASIC-resistant mining, transaction input and output, transaction fees, wallet types (web, paper, colored, multisig, hardware-based), mining pools, attacks (statistical, 51%), SPV and full nodes, thin client, forks (hard and soft), and the role and future of exchanges and investment funds, including at protocol level. We will also examine live blocks, some notable transactions, online resources related to Bitcoin, the dichotomy of centralized and decentralized models, and the inherent dynamics that might be pushing Bitcoin away from a completely decentralized system.

Module 5: **Cryptocurrencies and Digital Tokens**

Having a solid understanding of Bitcoin itself, it is time to cover other cryptocurrencies and digital tokens, their underlying fundamentals, consensus mechanisms, programmability, blockchains (including sidechains and RootStock), data layers, scalability, and economic models (including Initial Coin Offerings). In this module, we will specifically study Ethereum in depth (including its white- and yellowpaper), smart- and algorithmic-driven contracts, the history of DAO, and the Ethereum hard fork. We will also discuss others such as Golem, Ripple, Stellar, Zcash, and Litecoin, to name a few.

Module 6: **Advanced Topics and Latest Developments**

The last course module will afford an opportunity to deliberate on some of the advanced technical topics, in particular those related to the latest news and development in the fiat currency research, regulation, privacy, identity, key sharing and splitting, mass adoption, tradeoffs, environmental impact of mining (in particular, Bitcoin), data compression + storage (hot and cold) + retrieval, protocol-layer investing, general payments and micro-payments,
escrow, remittance, underbanked/unbanked/banked, anti-money laundering, prediction and auction markets, blockchain partnerships and consortia, Hyperledger, alternative consensus mechanisms, government transparency, and cash-less economies. We will conclude the course with student final presentations that shall showcase novel ideas and creative uses of the technologies and protocols covered in class to address identified and validated needs.