Developing Blockchain Use Cases

Michael McCarthy and Ariel Zetlin-Jones

Instructors

Michael McCarthy
e-mail: mm6@andrew.cmu.edu
Office: Hamburg 3015
Office Hours: TBD

Ariel Zetlin-Jones
e-mail: azj@cmu.edu
Office: Tepper 5141
Office Hours: W/1pm-3pm

Teaching Assistant:

Pshkar Saraf
e-mail: psaraf@andrew.cmu.edu

Course Listings:

- **15-621, 45-981, 70-258, 73-258, 95-788**

Class Time

- Time: Monday and Wednesday from 7:00PM to 8:20PM
- Location: Tepper 2611
- 13 meetings; first meeting **Wednesday, March 12**

Class Website: http://canvas.cmu.edu

Course Description

Blockchains, or distributed ledger and consensus technologies, hold tremendous promise for improving markets and organically handling private, secure data. What is blockhchain's "killer app" or whether such an application even exists remains an open question. This course is designed for students to evaluate blockchain use cases and highlight how blockchain-based applications offer different solutions to business-oriented challenges than traditional technologies provide.

The course begins with a brief introduction to blockchain using Bitcoin as an example of a blockchain protocol. We will examine the market failure Bitcoin was intended to resolve as well as the role of cryptography and distributed systems in enabling this new technology to create societal value. The course will go on to discuss the boundaries of the role of cryptography

in blockchain. Next, we will use these tools to evaluate existing, real-world blockchain use cases with an eye towards evaluating business applications that make use of these emerging technologies. Along the way, we will learn practical development skills in distributed ledger technologies to understand blockchain programming and application development. Finally, students will prepare a business plan and code demo for a specific application of their own choosing.

That not all of us knows the same thing is to be celebrated in this interdisciplinary setting. While the course will not be overly technical on any specific dimension, it will be hands-on, and you will need to be creative. There is no formal prerequisite. We expect folks to be coming at this from economics/business or computer science (perhaps both). If you are not, at the core, a "coder," the labs are designed to get you familiar enough with the setting to appreciate the possibilities and limitations. The labs are in steps and designed to walk you through things and not code-from-scratch. (Similar to how, say, as analogy, you might run an R-markdown file and then make changes).

Learning Objectives:

By the end of this course, students will be able to...

1. ...describe the intrinsic value of leading cryptocurrencies, Bitcoin and Ethereum;
2. ...explain the role cryptography plays in securing blockchain-based cryptocurrencies;
3. ...understand and program a smart contract on the Ethereum test network;
4. ...build a Decentralized Application running on a decentralized peer-to-peer network;
5. ...understand risks to the usefulness of different blockchains;
6. ...propose or evaluate use cases for a new blockchain and/or cryptocurrency.

Requirements and Grading:

The course deliverables will count toward the final grade according to the following distribution:

- Course Project: 30%
- Assignments: 30%
- Labs (1-3): 40%

Course assignments and labs will help us learn the details of the material. They will also prompt discussions and questions. (I.e., they are not the usual study-for-the-exam problems). Aim to hit the deadlines for due dates. If it looks like the deadline will cause some stress, let me know. Life is stressful all around and sometimes everyone needs a bit of flexibility. In general, less-than-perfect is much better than not submitting anything. But reach out to me if needed. I am here.

Students may submit their "assignments" in groups of 4 or less, just let us know who you worked with on your submission. In addition, students will *individually* complete "labs" designed to augment what we do in class and help you make progress toward your final project during the mini.

Course Project:

The course project consists of preparing a business plan and code demo for a proposed use case of blockchain technologies. All projects will require (i) a business plan and (ii) a code demo (i.e. code). You will choose which aspect of these requirements to emphasize including (but not limited to):

- A novel use-case and business strategy for blockchain;
- A case study of an existing use case, with a focus on how the blockchain solution differs from solutions using traditional technologies;
- Analysis of cryptography in a proposed use case;
- Analysis of the impact of regulation on an existing use case;
- A working code demo of a proposed application.

Regardless of the specific nature of your group project, each project should include original, creative thinking on the business or societal value of the use case and on the use of smart contracts and/or cryptography needed to achieve this business or societal value. Groups may choose to emphasize their proposal or their developed program/smart contract in the sense that we will accept "psuedo-code"—or a descriptive explanation of what a fully developed program does to implement students' or existing proposed applications—as long as students have a well developed market application. Alternatively, to the extent that students deliver a fully developed program, they may submit a shorter description of their proposed application and any associated risks. We will guide groups throughout the mini on our expectations for their project based on their proposed course of study. Groups will present their proposed application and code (or pseudo-code) to the class at the end of the Mini.

Diversity is Important

We must treat every individual with respect. We are diverse in many ways, and this diversity is fundamental to building and maintaining an equitable and inclusive campus community. Diversity can refer to multiple ways that we identify ourselves, including but not limited to race, color, national origin, language, sex, disability, age, sexual orientation, gender identity, religion, creed, ancestry, belief, veteran status, or genetic information. Each of these diverse identities, along with many others not mentioned here, shape the perspectives our students, faculty, and staff bring to our campus. At CMU, we all will work to promote diversity, equity and inclusion not only because diversity fuels excellence and innovation, but because we want to pursue justice. We acknowledge our imperfections while we also fully commit to the work, inside and outside of our classrooms, of building and sustaining a campus community that

increasingly embraces these core values.

I value diversity. I work for and hope for a world that is safer and more inclusive. I welcome your views and ideas for how we can make this goal a reality in our Blockchain community.

Center for Student Diversity and Inclusion: csdi@andrew.cmu.edu, (412) 268-2150.

Your Well-Being:

Take care of yourself: Do your best to maintain a healthy lifestyle this semester by eating well, exercising, avoiding drugs and alcohol, getting enough sleep and taking some time to relax. This will help you achieve your goals and cope with stress.

All of us benefit from support during times of struggle. You are not alone. There are many helpful resources available on campus and an important part of the college experience is learning how to ask for help. Asking for support sooner rather than later is often helpful.

If you or anyone you know experiences any academic stress, difficult life events, or feelings like anxiety or depression, we strongly encourage you to seek support. Counseling and Psychological Services (CaPS) is here to help: call 412-268-2922 and visit their website at

http://www.cmu.edu/counseling/

Consider reaching out to a friend, faculty or family member you trust for help getting connected to the support that can help.

TENTATIVE SCHEDULE

Week 1: Introduction to Blockchain.

- Distributed Ledger technologies. Blockchain. Cryptography. Consensus Mechanisms.

Week 2: Money as a Blockchain Use Case. Cryptography for Blockchains

- Cryptocurrencies. Bitcoin. Money.
- Public Key Encryption. Digital Signatures. Hash Functions.
- Assignment 1: Logic and Challenges of Smart Contracts.
- Lab 1: Installing Node.js and Hardhat and deploying your first smart contract.

Week 3: Applied Cryptography for Blockchains. Introduction to Smart Contracts

- Hash Functions, Merkle Trees, Merkle-Patricia Tries.
- Zero Knowledge Proofs (if time).
- Smart contract programming architecture. Programming, deployment and execution.
- Assignment 1 Due: Logic and Challenges of Smart Contracts.

Week 4: Ethereum Development Tools. Sample Use Case I.

- Ethereum Development Tools.
- Sample Business Plan 1: International Remittances and Ripple Case Study.
- Lab 2: Deploying and interacting with a token contract.
- Assignment 2 Due: Cryptographic Primitives for Blockchains. Brief pitch about proposed Case Study.

Week 5: Sample Use Case II. Tokens.

- Sample Business Plan 2: Financial Exchange on Blockchains
- Key elements in Ethereum. ERC-20 Token Code.
- Lab 3: Interacting with smart contracts via the web.

Week 6: dApps. Guest Lecture. Project Help.

- Decentralized applications running on peer-to-peer networks. The DeFi Stack.
- Lab 4: Open and defined by student groups.

Week 7: Presentations

- Student Presentations I & II