# Developing Blockchain Use Cases


## Vipul Goyal, Michael McCarthy, Ariel Zetlin-Jones

**Instructors**

Vipul Goyal
**e-mail**: vipul@cmu.edu
**Office**: Gates 7009
**Office Hours**: TBD

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**: TBD


**Course Listings:**

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

**Class Time**

- Monday and Wednesday from 6:30PM to 8:15PM
- 13 meetings; first meeting **Monday, March 16**

**Class Website**: https://www.andrew.cmu.edu/user/azj/cmucoin/

---

**Course Description**

Blockchains, or distributed ledger and consensus technologies, hold tremendous promise for improving markets and organically handling private, secure data. As CMU develops its own blockchain and token—CMU Coin—a central concern is to determine the set of applications that such technology would be most useful for. This course is designed for students to propose and, potentially, develop applications or use cases for a campus blockchain.

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 developing our own applications 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 propose their own blockchain use cases for CMU's own proprietary blockchain.

**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 and evaluate use cases for a new blockchain and/or cryptocurrency.

**Prerequisites:**

While the course will not be overly technical on any specific dimension, it will be hands on and you will need to be creative. Therefore, **while there are no formal prerequisites, we expect students to have a background in economics, cryptography, or computer science and all students should have some basic comfortability with programming.** The overall goal is to deliver enough knowledge about the potential and capabilities of blockchain technologies to enable students interested in this space to develop their own uses cases or applications.

**Requirements and Grading:**

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

- Course Project: 30%
- Assignments: 20%
- Labs (1-3): 40%
- Class participation: 10%

Students will submit their assignments and course project in groups of 4 or less for the duration of the mini. 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.

The course project consists of a proposed use case for CMU Coin. All projects will require (i) a proposed application and (ii) a program. Groups may choose to emphasize their proposal or their developed program in the sense that we will accept "psuedo-code"—or a descriptive explanation of what a fully developed program should do to implement students' proposed application—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. Groups will present their proposed application and code in class at the end of the Mini.

Participation based (objectively) on class attendance and (subjectively) on in class engagement.

## TENTATIVE SCHEDULE

**Week 1: Introduction to Blockchain.**

- Case Study: Bitcoin.
- Distributed Ledger technologies. Blockchain. Cryptography. Consensus Mechanisms. Public vs Permissioned blockchains.
- Lab 1: Installing Truffle and Ganache and deploying your first smart contract.

**Week 2: Ethereum and Cryptography**

- Ethereum vs. Bitcoin. Smart Contracts.
- Public Key Encryption. Digital Signatures. Hash Functions.
- Assignment 1: Logic and Challenges of Smart Contracts.

**Week 3: Cryptography and Sample Proposals**

- Zero-Knowledge Proofs. Secure Multi-Party computation.
- Sample Proposals: Guaranteed backing through Point-of-Sale. Course Enrollment Credits. Creating a market for the Campus Parking Waitlist.
- Lab 2: Deploying and interacting with a token contract.
- Assignment 2: Brief pitch about potential CMU Coin Use Case.

**Week 4: Introduction to Solidity and Smart Contracts**

- Smart contract programming architecture. Programming, deployment and execution. Solidity and Remix.

**Week 5: DApps**

- Decentralized Applications running on peer-to-peer networks. Dapp User interfaces.
- Lab 3: Interacting with smart contracts via the web.

**Week 6: Case Study and Lab 4**

- Case Study: Ripple. Global payments networks. Ripple Protocol Consensus Mechanism. XRP. Competitive Risk landscape. Regulatory risk landscape.
- Lab 4: Open and defined by student groups.

**Week 7: Presentations**

- Student Presentations I & II

**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.