

# 95-410/95810-Z2 Blockchain Fundamentals 2020

Instructor: Samuel Perl,  
Email [sperl@andrew.cmu.edu](mailto:sperl@andrew.cmu.edu)  
Phone: 412-268-4112

October 26, 2020 through December 11, 2020  
Monday and Wednesday 5:10pm - 6:30pm Eastern Standard Time

This will be a Remote Lecture (synchronous) via Zoom.  
The course Meeting Link will be posted to Canvas.

## Course Description

This course will be on the fundamentals of Blockchain and Blockchain Technology. The most well-known example of Blockchain Technology in wide use today is as the storage and transaction mechanism for the cryptocurrency Bitcoin. We will use historical examples, key concepts, key challenges, and their proposed (and implemented) solutions to help explain Blockchain Fundamentals. A key focus for the class will be on the decisions between challenge and implementation. This 'design' process can take a very long time, and the design and research process that ultimately led to a 'successful' implementation for a cryptocurrency took decades. Bitcoin represents an elegant technical solution to a series of long posed problems and partial solutions.

Whether these or similar technical solutions can be applied to other industry problems beyond cryptocurrency remains an interesting and ongoing research and implementation problem. After covering Blockchain technology, we will explore current and potential future applications of Blockchain Technology. Although we will use bitcoin to explain the blockchain technology, we will be focusing on potential uses of blockchains beyond cryptocurrency only.

Due to the ongoing COVID19 pandemic, this course will be offered entirely remotely. We will still be meeting interactively together via Zoom on Canvas. Remote instruction can be challenging for all of us. I understand the challenges of sitting in long remote meetings and attempting to focus on a single speaker and subject. I will do my best to keep the course engaging by supplementing lectures with online resources, videos, and demonstrations.

Planning around COVID19 has also provided us with engaging remote instruction opportunities to hear from experts on Blockchain, and on problems in Industry. Under normal circumstances, travel costs and schedule restrictions would limit our ability to have in person conversations with other experts, but due to our remote schedule this class will include presentations, question & answer sessions, and interactive conversations with researchers and/or practitioners from different fields. We will explore together how a system built using Blockchain may or may not meet the dynamic needs of these industries.

These professionals are very generously donating their time to us, so we will take care to be prepared for their lectures. The format for these sessions will generally be as follows:

- There will be a pre-lecture reading assignment.
- The invited guest will provide a lecture expecting that the audience is mostly familiar with Blockchain Fundamentals and has read the pre-read.
- The assignments for the lecture will be to read the pre-assigned material, create at least 3 questions related to the problem, challenge, solution, or Blockchain.
- Submit your questions prior to the lecture on a discussion board and we will use these to create a non-duplicate list of class interests for the speaker.
- After the lecture is over there may be time to ask one or more of your questions if they have not been answered.
- We will try to include time for you to have an interactive discussion with our speakers as well.

Please be sure to give our guest speakers your full attention. All are practicing researchers on the cutting edge of their Industry, Challenge Problem, and/or are using Blockchain or researching Blockchain uses in new and innovative ways. Guest speakers are our unique opportunity to learn about how Blockchain is used and being applied in the real world outside of cryptocurrencies.

## Textbooks

We will use a variety of books, articles, journal papers, sources, videos, demos, and interactive materials in the course. You are not required to purchase any text to have access to all of the course reading assignments or optional materials.

There is a textbook on cryptocurrency which we will read from titled *Bitcoin and Cryptocurrency Technologies*. You can download a free pre-publication version of the book at <http://bitcoinbook.cs.princeton.edu/>. You are not required to own a hard copy. The book website also contains a large number of interesting Blockchain related links which you are encouraged to explore.

We will also be using certain chapters from Ross Anderson's book: *Security engineering - a guide to building dependable distributed systems*. I will provide copies of the assigned chapters on Canvas which will be pre-print from the book's third edition (scheduled release November 2020). The author made the chapters available in digital form until the end of September. The book website is at <https://www.cl.cam.ac.uk/~rja14/book.html>

Other reading materials will come from Journals, Magazines, or Newspaper articles that CMU has online access to. We may use chapter excerpts from other books that will be made available to you on Canvas. All materials made available are only for use in this class.

# Learning Objectives

Upon successful completion of the course, each student will show tangible evidence of growth and maturity in the following areas:

1. Be able to state core Blockchain concepts, the benefits, and the limitations of blockchain technologies.
2. Be able to state the key differentiators for blockchain from other technology systems.
3. Understand the technical underpinnings of blockchain technology at sufficient depth to perform analysis.
4. Perform analysis of the implications of certain decisions upon blockchain proposals.
5. Understand relevant legal, ethical, and privacy issues and how they might impact policy and actions of organizations or individuals.
6. Apply various blockchain concepts to analyze examples, proposals, case studies, and preliminary blockchain system design discussions.
7. Make decisions about the use (or not) of blockchain technology in systems, and support decisions with relevant arguments.
8. Defend your blockchain analysis of real world systems and present relevant findings and arguments in a structured logical and compelling manner.
9. Determine real world challenges that blockchain technologies may assist (or explain why not) in solving.

## Schedule

Note: The schedule is subject to change during the semester. Please check Canvas for the latest updates including potential changes to the assigned weekly readings.

#	Date	Topics	Reading/Videos
1	10-26	Course Introduction and Learning Objectives  Blockchain Overview and Introduction  History and Origin of Blockchain (and Cryptocurrency)  Technical Concepts of Blockchain Systems	<i>Narayanan, et al. Preface</i>  <a href="#">The great chain of being sure about things</a> (Article, Economist) <i><a href="https://www.economist.com/briefing/2015/10/31/the-great-chain-of-being-sure-about-things">https://www.economist.com/briefing/2015/10/31/the-great-chain-of-being-sure-about-things</a></i>  <a href="#">Why I Wrote PGP by Phil Zimmerman</a> (Article) <i><a href="https://www.philzimmermann.com/EN/essays/WhyIWrotePGP.html">https://www.philzimmermann.com/EN/essays/WhyIWrotePGP.html</a></i>  <a href="#">(Article) The Money Myth by James Bridle (as a PDF)</a>

			<p><a href="#">Blockchain Expert explains one concept in 5 different levels (beginner to expert)</a> (Video, YouTube, 17 Min)  <a href="https://www.youtube.com/watch?v=hYip_Vuv8J0">https://www.youtube.com/watch?v=hYip_Vuv8J0</a></p> <p><a href="#">How Bitcoin Works in 5 Minutes</a> (Video, Youtube, 5 minutes)  <a href="https://www.youtube.com/watch?v=I9jOJk30eQs">https://www.youtube.com/watch?v=I9jOJk30eQs</a></p>
2	10-28	<p>Key Problem Challenges and Solutions</p> <p>Ownership</p> <p>Transaction Records (Ledger)</p> <p>Incentives</p> <p>Attacks</p> <p>(Distributed) Consensus</p>	<p>Narayanan, et al. Chapter 1.</p> <p><i>The Eureka Moment that made bitcoin possible</i> - Amy Whitaker (PDF)</p> <p><i>How to Time Stamp a Digital Document</i> - Haber and Stornetta (PDF)</p>
3	11-2	<p>Cryptographic Hash Functions</p> <p>Digital Signatures</p> <p>Distributed systems, Decentralized networks</p> <p>Proof of Work</p>	<p><i>Can you Crack the Code? A fascinating history of ciphers and cryptography</i> - Chapter 9 "Prime Time". by Ella Schwartz illustrated by Lily Williams.</p> <p><i>Security engineering</i> - Chapter 5 Cryptography by Ross Anderson (PDF)</p> <ul style="list-style-type: none"> <li>• 5.2 Historical Background</li> <li>• 5.3 Security Models</li> <li>• 5.4 Symmetric crypto algorithms</li> <li>• 5.6 Hash Functions</li> </ul> <p>How secure is 256 bit security?  <a href="https://youtu.be/S9JGmA5_unY">https://youtu.be/S9JGmA5_unY</a> (Video 5 minutes)</p> <p>Playing with <a href="#">Hash Collision Demonstrations</a>  <a href="https://natmchugh.blogspot.com/2015/02/create-your-own-md5-collisions.htm">https://natmchugh.blogspot.com/2015/02/create-your-own-md5-collisions.htm</a></p> <p>But how does bitcoin actually work? <a href="https://youtu.be/bBC-nXj3Ng4">https://youtu.be/bBC-nXj3Ng4</a> (video 26 min)</p> <p><a href="#">How Does Bitcoin Work?!</a>  <a href="https://learnmeabitcoin.com/">https://learnmeabitcoin.com/</a> (free to explore on your own)</p>

4	11-4	<p>Cryptosystems in practice.</p> <p>Bitcoin demonstration and examples</p> <p>Smart Contracts and Solidity</p> <ul style="list-style-type: none"> <li>- Smart contracts are “pieces of code that codify business logic. Store Rules, Verify Rules, Self Execute.” Olga Mack</li> </ul> <p>Altcoins (Extensions, ‘Remixes’)</p> <p>Theory vs. Practice - who is actually mining?</p>	<p><i>Narayanan, et al. in Chapter 2 (pages 51 - 74)</i></p> <p>Hashcash - A Denial of Service Counter-Measure (pdf)</p> <p>Nakamoto White Paper</p> <p><i>Blockchain and the Law - The Rule of Code - Chapter 4 “Smart Contracts as Legal Contracts” (pdf) (17 Pages)</i></p> <p>(Article) <a href="#">Introduction to Smart Contracts — Solidity 0.7.0 documentation</a></p> <p><a href="https://solidity.readthedocs.io/en/v0.7.0/introduction-to-smart-contracts.html">https://solidity.readthedocs.io/en/v0.7.0/introduction-to-smart-contracts.html</a></p> <p>(Video) <a href="#">How Smart Contracts Will Change the World   Olga Mack   TEDxSanFrancisco</a></p> <p>(17 minutes. Smart Contracts starts at about 6 minute mark)</p> <p><a href="https://www.youtube.com/watch?v=pA6CGuXEKtQ">https://www.youtube.com/watch?v=pA6CGuXEKtQ</a></p> <p>(Article) <a href="#">Inside the Icelandic Facility Where Bitcoin Is Mined</a></p> <p><a href="https://www.wired.com/story/iceland-bitcoin-mining-gallery/">https://www.wired.com/story/iceland-bitcoin-mining-gallery/</a></p> <p>(Video) <a href="#">Inside a Secret Chinese Bitcoin Mine</a> (10 minutes)</p> <p><a href="https://www.youtube.com/watch?v=K8kua5B5K3I">https://www.youtube.com/watch?v=K8kua5B5K3I</a></p>
5	11-9	<p>Key Considerations and Discussion</p> <p>Energy Usage</p> <p>Illicit Content</p> <p>Scammers</p> <p>Money laundering</p> <p>Exchange Frailty</p>	<p><i>Narayanan - ch.6 Bitcoin and Anonymity, (pgs. 165 – 169)</i></p> <ul style="list-style-type: none"> <li>- 6.1 anonymity basics</li> </ul> <p><i>Narayanan - ch.9 Bitcoin as a Platform, (pgs 237 – 247)</i></p> <ul style="list-style-type: none"> <li>- 9.1 Bitcoin as an append-only log</li> <li>- 9.2 Bitcoins as “smart property”</li> </ul> <p>(Article) <a href="#">Ethereum's smart contracts are full of holes</a> (MIT Technology Review)</p> <p><a href="https://www.technologyreview.com/2018/03/01/144962/ethereums-smart-contracts-are-full-of-holes/">https://www.technologyreview.com/2018/03/01/144962/ethereums-smart-contracts-are-full-of-holes/</a></p> <p><a href="#">Known Attacks - Ethereum Smart Contract Best Practices</a></p> <p><a href="https://consensys.github.io/smart-contract-best-practices/known_attacks/">https://consensys.github.io/smart-contract-best-practices/known_attacks/</a></p> <p><a href="#">Does regulation of illegal content need reconsideration in light of blockchains?</a></p>

			<p>Maurice Schellekens, <i>International Journal of Law and Information Technology</i>, Volume 27, Issue 3, Autumn 2019, Pages 292–305, <a href="https://doi.org/10.1093/ijlit/eaz009">https://doi.org/10.1093/ijlit/eaz009</a>  <a href="https://academic.oup.com/ijlit/article/27/3/292/5601120">https://academic.oup.com/ijlit/article/27/3/292/5601120</a></p> <p><a href="https://www.koomey.com/post/179556571967">Talking Sense About Bitcoin Electricity Use</a> (koomey)  <a href="https://www.koomey.com/post/179556571967">https://www.koomey.com/post/179556571967</a></p> <p><a href="https://www.nytimes.com/2013/05/29/nyregion/liberty-reserve-operators-accused-of-money-laundering.html">Liberty Reserve Operators Accused of Money Laundering</a> (\$6 Billion)  <a href="https://www.nytimes.com/2013/05/29/nyregion/liberty-reserve-operators-accused-of-money-laundering.html">https://www.nytimes.com/2013/05/29/nyregion/liberty-reserve-operators-accused-of-money-laundering.html</a></p> <p><a href="https://www.forbes.com/sites/billybambrough/2020/05/28/new-york-hacker-charged-in-100-million-dollar-bitcoin-case/#1f3d050ac90e">New York Man Charged In \$100 Million Bitcoin Case</a> (Forbes) <i>money laundering with bitcoin</i>  <a href="https://www.forbes.com/sites/billybambrough/2020/05/28/new-york-hacker-charged-in-100-million-dollar-bitcoin-case/#1f3d050ac90e">https://www.forbes.com/sites/billybambrough/2020/05/28/new-york-hacker-charged-in-100-million-dollar-bitcoin-case/#1f3d050ac90e</a></p>
6	11-11	<p>Discussion on Practical Pros &amp; Cons</p> <p>Societal Implications?</p> <p>Alternate views</p> <p>Disinformation</p> <p><b>Homework 1 is due</b></p>	<p><a href="https://www.coindesk.com/crypto-is-down-so-why-am-i-smiling">Crypto Is Down, So Why Am I Smiling?</a> By Dr. Stornetta  <a href="https://www.coindesk.com/crypto-is-down-so-why-am-i-smiling">https://www.coindesk.com/crypto-is-down-so-why-am-i-smiling</a></p> <p><a href="https://www.theverge.com/2018/3/7/17091766/blockchain-bitcoin-ethereum-cryptocurrency-meaning">'Blockchain' is meaningless</a> (TheVerge)  <a href="https://www.theverge.com/2018/3/7/17091766/blockchain-bitcoin-ethereum-cryptocurrency-meaning">https://www.theverge.com/2018/3/7/17091766/blockchain-bitcoin-ethereum-cryptocurrency-meaning</a></p> <p><a href="https://www.wired.com/story/whats-blockchain-good-for-not-much/">What's Blockchain Actually Good for, Anyway? For Now, Not Much</a>  <a href="https://www.wired.com/story/whats-blockchain-good-for-not-much/">https://www.wired.com/story/whats-blockchain-good-for-not-much/</a></p> <p>Podcast <a href="https://freakonomics.com/podcast/why-everybody-who-doesnt-hate-bitcoin-loves-it-a-new-freakonomics-radio-podcast/">Why Everybody Who Doesn't Hate Bitcoin Loves It (Ep. 160)</a> (freakonomics radio)  <a href="https://freakonomics.com/podcast/why-everybody-who-doesnt-hate-bitcoin-loves-it-a-new-freakonomics-radio-podcast/">https://freakonomics.com/podcast/why-everybody-who-doesnt-hate-bitcoin-loves-it-a-new-freakonomics-radio-podcast/</a></p>
7	11-16	<p>Nuances of Trust</p> <p>Blockchain use Beyond Currency</p> <p>Other 'types' of Blockchains</p> <p>Public vs. Private</p>	<p><a href="https://hbr.org/2017/04/who-controls-the-blockchain">Who Controls the Blockchain?</a>  <a href="https://hbr.org/2017/04/who-controls-the-blockchain">https://hbr.org/2017/04/who-controls-the-blockchain</a></p> <p><a href="https://www.schneier.com/blog/archives/2019/02/blockchain_and_.html">Blockchain and Trust</a> by Bruce Schneier  <a href="https://www.schneier.com/blog/archives/2019/02/blockchain_and_.html">https://www.schneier.com/blog/archives/2019/02/blockchain_and_.html</a></p>

		<p>Tokens</p> <p>Usability?</p>	<p><a href="https://blog.cloudflare.com/how-the-nsa-may-have-put-a-backdoor-in-rsas-cryptography-a-technical-primer/">How the NSA (may have) put a backdoor in RSA's cryptography: A technical primer</a> https://blog.cloudflare.com/how-the-nsa-may-have-put-a-backdoor-in-rsas-cryptography-a-technical-primer/</p> <p><a href="https://blockchainhub.net/blockchains-and-distributed-ledger-technologies-in-general/">Types of Blockchains &amp; DLTs (Distributed Ledger Technologies)</a> https://blockchainhub.net/blockchains-and-distributed-ledger-technologies-in-general/</p> <p><a href="https://www.cnn.com/travel/article/akon-city-senegal-wakanda-intl/index.html">R&amp;B singer Akon is building a 'real-life Wakanda' worth \$6 billion in Senegal</a> https://www.cnn.com/travel/article/akon-city-senegal-wakanda-intl/index.html</p> <p><a href="https://fortune.com/2018/02/25/cryptocurrency-ico-collapse/">Nearly Half of 2017's Bitcoin-Backed 'ICO' Projects Have Collapsed - \$233 million in funding raised through ICOs has vanished.</a> https://fortune.com/2018/02/25/cryptocurrency-ico-collapse/amp/</p> <p><a href="https://people.eecs.berkeley.edu/~tygar/papers/Why_Johnny_Cant_Encrypt/OReilly.pdf">Why Johnny Can't Encrypt</a> This paper was originally published in the Proceedings of the 8th USENIX Security Symposium (Washington, D.C., Aug. 23–36, 1999), 169–184 https://people.eecs.berkeley.edu/~tygar/papers/Why_Johnny_Cant_Encrypt/OReilly.pdf</p>
8	11-18	<p>Art and Blockchain</p> <p><b>Guest Speaker: Amy Whitaker,</b> <i>New York University, Assistant Professor of Visual Arts Administration</i></p>	<p>Whitaker, Amy, and Roman Kräussl. <a href="https://www.econstor.eu/bitstream/10419/182451/1/1031263918.pdf">Blockchain, Fractional Ownership, and the Future of Creative Work</a> <i>Available at SSRN 3100389</i> (2019). https://www.econstor.eu/bitstream/10419/182451/1/1031263918.pdf</p> <p><a href="https://artivate.org/artivate/article/view/94">Art and Blockchain</a> (Article, Artivate.org) A Primer, History, and Taxonomy of Blockchain Use Cases in the Arts https://artivate.org/artivate/article/view/94</p>
9	11-23	<p>Legal Discussions</p> <p>Property Law</p> <p>Digital Ownership</p>	<p><a href="https://theconversation.com/can-blockchain-a-swiftly-evolving-technology-be-controlled-73471">Can blockchain, a swiftly evolving technology, be controlled?</a> (Article) https://theconversation.com/can-blockchain-a-swiftly-evolving-technology-be-controlled-73471</p> <p><a href="#">View of Blockchain technology as a regulatory technology:</a></p>

		<p>Regulations</p> <p>Code is Law</p> <p><b>Homework 2 is due</b></p>	<p><a href="https://firstmonday.org/ojs/index.php/fm/article/view/7113/5657">From code is law to law is code</a>  <a href="https://firstmonday.org/ojs/index.php/fm/article/view/7113/5657">https://firstmonday.org/ojs/index.php/fm/article/view/7113/5657</a></p>
10	11-25	<p>Emerging Applications of Blockchain in the Agriculture industry (such as Food traceability). And thoughts on the future.</p> <p><b>Guest Speaker: Sven Verlinden</b>  <i>West Virginia University, Director of Plant and Soil Sciences</i></p>	<p><a href="https://www.pma.com/content/articles/blockchain">Blockchain: What It Is, What It Isn't, and What It Means for The Produce Industry</a>  <a href="https://www.pma.com/content/articles/blockchain">https://www.pma.com/content/articles/blockchain</a></p> <p>Explore IBM  <a href="https://www.ibm.com/blockchain/solutions/food-trust">IBM Food Trust - Blockchain for the world's food supply</a>  <a href="https://www.ibm.com/blockchain/solutions/food-trust">https://www.ibm.com/blockchain/solutions/food-trust</a>  and  <a href="https://www.thepacker.com/article/brightfarms-adds-blockchain-tech-through-ibm-food-trust-network">BrightFarms adds blockchain tech through IBM Food Trust Network</a>  <a href="https://www.thepacker.com/article/brightfarms-adds-blockchain-tech-through-ibm-food-trust-network">https://www.thepacker.com/article/brightfarms-adds-blockchain-tech-through-ibm-food-trust-network</a></p> <p>(BrightFarms is now in 2000 stores)</p> <p><a href="https://www.thepacker.com/article/produce-industry-keeping-tabs-blockchain">Produce industry keeping tabs on blockchain   Packer</a>  <a href="https://www.thepacker.com/article/produce-industry-keeping-tabs-blockchain">https://www.thepacker.com/article/produce-industry-keeping-tabs-blockchain</a></p> <p><a href="https://www.thepacker.com/article/california-giant-blockchain-use-boosts-freshness-food-safety">California Giant blockchain use boosts freshness, food safety</a>  <a href="https://www.thepacker.com/article/california-giant-blockchain-use-boosts-freshness-food-safety">https://www.thepacker.com/article/california-giant-blockchain-use-boosts-freshness-food-safety</a></p>
11	11-30	<p>Implementing Digital Rights for a variety of use cases on a blockchain</p> <p><b>Guest Speaker: Michael Nguyen</b>  <i>Bitmark</i></p>	<p><i>Defining Property in the Digital Environment, Bitmark Inc.</i>  By Casey Alt, Sean Moss-Pultz, Amy Whitaker, &amp; Timothy Chen (26 min read)(PDF on Canvas)</p> <p>Read about some of the projects here  <a href="https://bitmark.com/projects/">https://bitmark.com/projects/</a></p>
12	12-2	<p>Air Force Acquisition and Blockchain</p> <p>Misinformation and Blockchains</p> <p><b>Guest Interview: Geoff Dobson,</b>  <i>Major, Research Scientist, 711th Human Performance Wing, Air Force Research Lab. Carnegie</i></p>	<p><a href="https://calhoun.nps.edu/handle/10945/61355">BLOCKCHAIN TECHNOLOGY IN THE DEPARTMENT OF DEFENSE</a>  <a href="https://calhoun.nps.edu/handle/10945/61355">https://calhoun.nps.edu/handle/10945/61355</a></p> <p><a href="https://www.nytimes.com/2020/07/06/insider/could-we-fight-misinformation-with-blockchain-technology.html">Could We Fight Misinformation With Blockchain Technology?</a> (Article, NYT)  <a href="https://www.nytimes.com/2020/07/06/insider/could-we-fight-misinformation-with-blockchain-technology.html">https://www.nytimes.com/2020/07/06/insider/could-we-fight-misinformation-with-blockchain-technology.html</a></p>



		<p><i>Mellon University Ph.D. Candidate, SCS. CERT Member of the Technical Staff and Team Lead.</i></p>	<p><a href="https://www.computerworld.com/article/3481633/how-blockchain-will-kill-fake-news-and-four-other-predictions-for-2020.html">How blockchain will kill fake news (and four other predictions for 2020)</a> https://www.computerworld.com/article/3481633/how-blockchain-will-kill-fake-news-and-four-other-predictions-for-2020.html</p> <p><a href="https://open.nytimes.com/introducing-the-news-provenance-project-723dbaf07c44">Introducing the News Provenance Project   by Sasha Koren   NYT Open</a> https://open.nytimes.com/introducing-the-news-provenance-project-723dbaf07c44</p>
13	12-7	<p>Open Discussion and Formulating Research Questions</p> <p>Can Blockchain provide solutions to COVID related challenges?</p> <p>COVID has had a transformative effect on many workplaces, markets, and businesses today. Can blockchain models be used to solve new problems encountered by global disruptions to traditional supply chains?</p> <p>What about traditional modes of human interaction or traditional business models involving physical touch?</p>	<p><a href="https://www.wsj.com/articles/a-cryptocurrency-technology-finds-new-use-tackling-coronavirus-11587675966">A Cryptocurrency Technology Finds New Use Tackling Coronavirus</a> https://www.wsj.com/articles/a-cryptocurrency-technology-finds-new-use-tackling-coronavirus-11587675966</p> <p><a href="https://www.forbes.com/sites/nishandegnarain/2020/03/22/5-ways-blockchain-can-unblock-the-coronavirus-medical-supply-chain/">Five Ways Blockchain Can Unblock The Coronavirus Medical Supply Chain</a> https://www.forbes.com/sites/nishandegnarain/2020/03/22/5-ways-blockchain-can-unblock-the-coronavirus-medical-supply-chain/</p> <p><a href="https://www.coindesk.com/how-blockchain-tech-can-make-coronavirus-relief-more-effective">Blockchain Can Bring Transparency To Coronavirus Response</a> https://www.coindesk.com/how-blockchain-tech-can-make-coronavirus-relief-more-effective</p> <p><a href="https://fortune.com/2020/07/07/blockchain-technology-regulation-coronavirus-economy/">Overstock CEO: How blockchain can help pull us out of the coronavirus recession</a> Article in Fortune Magazine https://fortune.com/2020/07/07/blockchain-technology-regulation-coronavirus-economy/</p>
14	12-9	<p>Wrap up</p> <p><i>Final Project is due</i></p>	<p><a href="https://www.youtube.com/watch?v=Ygq9ci0GFhA">Crypto for the People, Invited talk at Crypto 2020 by Seny Kamara</a> https://www.youtube.com/watch?v=Ygq9ci0GFhA</p>

## Assessments and Final Project

This course with consist of the following major assessments:

### Homework Assignment 1 - Explanation of key concepts in your own words

You will be asked to write a short essay to explain the major concepts of blockchains. You may supplement your writing with drawings or pictures and contrast blockchains with other kinds of technology. You will also be asked to think of your own anecdotes to help explain blockchain

concepts, key challenges, and solutions to someone who is unfamiliar with the underlying technical elements. Assignment details will be posted on canvas.

### **Homework Assignment 2 - Challenge Problem Sources, Outline**

In your final project, you will be asked to choose a challenge problem and analyze how a blockchain might be used to solve it. Your assignment in homework 2 will be to choose a challenge problem and clearly articulate why it is a challenge, explain the particulars of the problem, attempt to explain the current state solutions and why they may or may not be an improvement over a blockchain. You will also identify a minimum of 4 sources that you will use in your final project. You will write an outline for each of the sections in your final project.

### **Final Project**

After you have chosen your challenge problem, you should articulate the details of that challenge further, and explain the challenge that you think a blockchain system might help to solve. In short, you will explore the challenge and articulate the parts of the challenge that make it hard.

Explain why a blockchain might be a possible solution for this problem - and what benefits are derived in the case that blockchain technology would be used over other alternatives (to include a private database, or an intermediary company that stores data and helps perform 'transactions' for others). You should pose a list of questions to yourself on why blockchain might be a good fit for the problem you have chosen. You should also explain what changes, design decisions, or tweaks you would need to make to your proposed blockchain solution so that it would appropriately fit your problem.

Each major assessment and its due date will be posted in more detail to Canvas.

In addition to these assessments, you will be asked to answer questions on the reading and lectures throughout the course. These short assignment questions will also be posted to canvas. These minor assignments will typically ask for a written paragraph or two, or will ask a series of questions each of which will ask for short answers (eg. 1-2 sentences).

All assessments will be conducted through Canvas. Class discussion will be via Zoom or the class Discussion board which is hosted on Canvas

## Academic Integrity

Academic integrity is about enhancing your education and being a trusted member of the CMU community. This course is intended to grow your knowledge of blockchain technologies, research techniques, argument construction, and written reports/essays. These are all skills that you will be asked to have when working in real world situations, and the course attempts to provide an accepting and encouraging professional setting for you to practice and learn.

You are asked to complete all assessments without collaboration or outside assistance. You are expected to use outside sources to discuss and learn the material. All outside materials should be cited when they are used on any assessment. These principles are directly taken from the Carnegie Mellon University Academic Integrity policy located at <https://www.cmu.edu/policies/student-and-student-life/academic-integrity.html>

## Evaluation Method

15% Course Reading, Comprehension, Assignment Question & Answer  
15% - Homework Assignment 1  
15% - Homework Assignment 2  
40% - Final Project  
10% - Class Discussion & Participation  
05% - Professionalism

## Grading Scale

100 - 98 A+  
97-92 A  
91-90 A-  
89-88 B+  
87-82 B  
81-80 B-  
79-78 C+  
77-72 C  
71-70 C-

## Grade Distribution

I plan on using the Heinz School guidelines in deciding on the overall grade distribution. Accordingly, the average grade will be around A-. However, I grade on an absolute scale. If every student does well in the class, each will get an A+ regardless of the recommended grading scale. The same holds true on the other end of the scale.

## Late/Make Up Work

Normally, I do not accept late work. However, Due dates for every assignment are provided on the course syllabus and course schedule (and posted in Canvas). Unless otherwise stated, assignments are due on those days. However, I recognize that sometimes “life happens.” COVID has caused major disruptions to many institutions, countries, and our society. If you need more time for an assignment please email me at [sperl@andrew.cmu.edu](mailto:sperl@andrew.cmu.edu) as soon as possible. I will do my best to work with you to find a fair way to evaluate any late work. Remember that many other students will have submitted the work on time, and I will try to work with you based upon your circumstances and the assessment.

## Accommodations

If you have a disability and require accommodations, please contact Catherine Getchell, Director of Disability Resources, 412-268-6121, [getchell@cmu.edu](mailto:getchell@cmu.edu). If you have an accommodation letter from the Disability Resources office, I encourage you to discuss your accommodations and needs with me as early in the semester as possible. I will work with you to ensure that accommodations are provided as appropriate.

## Student Wellness - Take Care of Yourself

We want you to succeed in this class. If you are finding that this is a struggle, know that you are not alone. If you are having issues, please ask for help. All of us benefit from support during times of struggle. You are not alone. There are many resources available to help you in the Heinz College, on the CMU campus, and among your instructors.

If you or anyone you know is experiencing academic stress, difficult life events, or feel anxiety or depression, we strongly encourage you to seek support. Counseling and Psychological Services (CaPS) is available to help. Call 412.268.2922 and visit the website <https://www.cmu.edu/counseling/> Consider reaching out to a friend, faculty or family member you trust for help getting connected to support that can help.

## Use of Zoom in the Class

In our class, we will be using Zoom for synchronous (same time) sessions. The link to the course Zoom will be available on Canvas.

Please make sure that your Internet connection and equipment are set up to use Zoom and able to share audio and video during class meetings. (See [this page](#) from Computing Resources for information on the technology you are likely to need.) Let me know if there is a gap in your technology set-up please email [sperl@andrew.cmu.edu](mailto:sperl@andrew.cmu.edu) as soon as possible, and we can see about finding solutions.

Sharing video: In this course, being able to see one another helps to facilitate a better learning environment and promote more engaging discussions. Therefore, I will encourage students to have their cameras on during lectures and discussions. However, I also completely understand there may be reasons students would not want to have their cameras on. If you have any concerns about using your camera, please email me as soon as possible [sperl@andrew.cmu.edu](mailto:sperl@andrew.cmu.edu) and we can discuss adjustments. Note: You may use a background image in your video if you wish; just check in advance that this works with your device(s) and internet bandwidth.

During our class meetings, please keep your mic muted unless you are sharing with the class or your breakout group.

If you have a question or want to answer a question, please use the chat or the “raise hand” feature (available when the participant list is pulled up). I (or a helper) will be monitoring these channels in order to call on students to contribute.

## Policy on cheating and plagiarism

This course follows Heinz School and Carnegie Mellon policies for student conduct, including policies that address inappropriate student collaboration and plagiarism. Each student is responsible for handing in their own work. For any assignment found to be the partial or complete result of cheating or plagiarism, your grade for that assignment will be zero. Cheating is defined as inappropriate collaboration among students on an assignment. This can include copying someone else’s work with or without alteration. When students are found to be collaborating in this way, BOTH will pay the penalty regardless of who originated the work. You must also properly cite sources of ideas, articles, and place any unaltered comments in quotes that you use in your work.

## Class Participation

Partly because we will be conducting class remotely via Zoom, we will also leverage the discussion board to show class participation in addition to remote sessions.

Discussion board - Based upon the readings each week you will be asked to respond to an instructor-posed question or asked to post a question/comment of your own on a weekly basis. The discussion board will serve as both a mechanism for prep work for class (e.g., you may be asked to post questions that you have about the assigned reading or for an upcoming guest speaker) or as post-class work (e.g., you may be asked to post a list of takeaways from today’s class session).

You will also be asked to answer questions about the readings in class, but since we have limited in-person time together, the discussion board may be a better way to record your participation.

Here are other ways you can show class participation and reading comprehension:

1. Completing any pre-class reading. Any required reading assignments for a class will be posted on Canvas at least 1 week prior to the start of the next class. Reading assignments will usually be reflective of basic and advanced topics, relevant research, current events, or new results on blockchain concepts that are directly related to the material being covered in class.
2. Complete any assigned pre-work. An example of class pre-work may include reading an assigned article and coming prepared with a list of questions about information security topics raised by the article. Other pre-work includes making postings on the discussion board about information security related topics. We will frequently be having guest speakers working on blockchain systems, industry problems, or researching future blockchains improvements/solutions. Come prepared to these sessions by reading all pre-work and bringing a list of questions to pose to the speaker about their work. You should also post your questions prior to or shortly after the lesson on the discussion board. All of our speakers have agreed to allow students to ask them questions about their work (time permitting). They want to share with you, so be sure to be engaged and show them courtesy for donating their time to discussing blockchain with us.
3. Participate in any group activities assigned in class
4. Participate in class discussions including attempting to answer questions from the instructor and from other students, performing active listening, and asking pertinent questions of your own. Active listening for purposes of this class means paying attention, reflecting, attempting to clarify information that you do not understand, and being able to summarize the information you have heard or read about.
5. Try to relate the concepts you are learning about in class to specific examples in your own life and sharing your own thoughts and experiences on these with the class.

## Professionalism

All students (and especially graduate students) are expected to conduct themselves with respect toward each other. Discourse on any topic can sometimes become heated. Students will be expected to act and behave as if they are in a professional setting.

Class participation is to encourage your active participation in discussions. If you are not answering a question, or asking a question, please try to focus your attention on the person that is speaking. I also understand that sometimes circumstances at home might make this difficult, so please let me know about your situation. Many of us are working from home, and that will present many new situations that you will not find in a

professional setting. For example, I have 3 small children who may take it upon themselves to make an unannounced appearance. I will understand. Please try your best to help each other during these times.

If you are ill or feeling overly tired, please contact the instructor prior to the beginning of class and we will make arrangements for you to make up the material that we covered in class.

If you are confused, your confusion may also be shared by other students so please ask the instructor a question. Many of the topics we are covering in class can have multiple viewpoints. This can cause confusion even among professionals in the field. Many professionals can have a difference of opinion on a given issue. This class is an attempt to help you participate in such conversations using the framework, language, and skills of practicing analysis of blockchain technologies. Asking questions and attempting to answer the questions of others is an important learning step and counts toward class participation.

## Class Recordings

All classes will be recorded via Zoom so that students in this course (and only students in this course) can watch or re-watch past class sessions. Please note that breakout rooms will not be recorded. CMU is encouraging all Instructors to provide asynchronous access to comprehensive course materials used during synchronous class sessions for all students to refer to as a resource remotely. I also want to ensure that students have access to the class. We are all dealing with different remote situations and possibly different time zones. Please do your best to attend as the course is intended to be interactive. If you know that you cannot attend class at the listed time, please contact me at [sperl@andrew.cmu.edu](mailto:sperl@andrew.cmu.edu) and we can discuss your situation.

I will make the recordings available on Canvas as soon as possible after each class session. Please note that you are not allowed to share these recordings. This is to protect your FERPA rights and those of your fellow students.

## Absences

We are all doing our best during this very trying time. I understand that things come up, many of which may be unplanned. Please do your best to attend, and I will also to my best to provide opportunities for asynchronous work. This will generally include reading the class reading materials, watching the class lecture (all classes will be recorded and posted on Canvas), and performing any make up work such as posting to the discussion board. If you become ill for a few days or encounter an emergency situation, contact me and we will make arrangements for you to make up the material that we covered in class.

# Diversity

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. We, at CMU, 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.

Each of us is responsible for creating a safer, more inclusive environment.

Unfortunately, incidents of bias or discrimination do occur, whether intentional or unintentional. They contribute to creating an unwelcoming environment for individuals and groups at the university. Therefore, the university encourages anyone who experiences or observes unfair or hostile treatment on the basis of identity to speak out for justice and support, within the moment of the incident or after the incident has passed. Anyone can share these experiences using the following resources:

- **Center for Student Diversity and Inclusion:** [csdi@andrew.cmu.edu](mailto:csdi@andrew.cmu.edu), (412) 268-2150
- **Report-It online anonymous reporting platform:** [reportit.net](https://reportit.net) username: *tartans* password: *plaid*

All reports will be documented and deliberated to determine if there should be any following actions. Regardless of incident type, the university will use all shared experiences to transform our campus climate to be more equitable and just.

## How to Succeed in This Class

1. Get started on the research project as soon as possible. Even just spending some time in week 1 thinking about topics you may be interested in learning more about can make a significant difference.
2. Complete the assigned readings for each week, if not before the class for which they are assigned, then after that class and before the next.
3. Participate in class - see section on Class Participation for more specific tips.
4. Use office hours productively. Get feedback on outlines of your research reports, suggestions for references, tips on homework or lab questions, and clarifications of lecture materials. Make sure you are comfortable applying the concepts and lessons



learned from course case studies to new requirements or use cases.

5. Complete as much of the research project for the first draft as is possible. You can provide as much of a draft as you like in HW2 and receive feedback in advance of your final draft.
6. Proof read your work before submitting it. Read each sentence out loud to yourself (or a patient family member) to ensure that it contains a complete thought.