95-410/810 Blockchain Fundamentals

Heinz College, Carnegie Mellon University

Instructor:	Samuel Perl (sperl@andrew.cmu.edu)
TA:	TBD
Term:	Summer 2022, Mini 5

This class meets **REMOTELY** - Mondays 6:00pm - 8:50pm

Zoom link will be posted on Canvas

May 16, 2022 through June 20, 2022

Course Description

This course will be on the fundamentals of Blockchain Technology and its growing impact on society. After technical fundamentals we will cover applied uses and criticisms. The best 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 impacts. A second focus for the class will be on making decisions between the challenges of a given problem area and an implementation. This 'design' process can take a very long time. The history of the design and research process that ultimately led to a 'successful' implementation for a cryptocurrency is decades long. Bitcoin represents an elegant technical solution to a series of long posed problems which we can use to learn from.

Whether these technical solutions (or similar ones) can be applied to other industry problems beyond cryptocurrency remains an interesting and ongoing research and implementation problem. After covering Blockchain technology fundamentals, we will explore applications of Blockchain Technology and focusing on current and potential uses beyond that cryptocurrency.

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.

Other reading materials will come from Journals, Magazines, or Newspaper articles that CMU has online access to. We may occasionally 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 of the impacts of certain implementation decisions in proposals.
4. Understand relevant legal, ethical, and privacy issues around blockchains and how they might impact policy and actions of organizations or individuals.
5. Apply various blockchain concepts to analyze examples, proposals, case studies, and preliminary blockchain system design discussions.
6. Make decisions about the use (or not) of blockchain technology in systems, and support decisions with relevant arguments.
7. Perform and defend blockchain analysis of real world systems and present relevant findings and arguments in a structured, logical and compelling manner.
8. Determine real world challenges that blockchain technologies may assist in solving; or explain why they do not.

Schedule

Note: The topics and list of reading and videos is subject to change. ALWAYS Check Canvas for the latest updates including changes to the assigned weekly readings.

#	Date	Topics	Reading/Videos
1	05-16	Introduction and Learning Objectives Blockchain Overview History and Origin of Blockchain (and Cryptocurrency)	Narayanan, et al. Chapter 1 PKI & Digital Signature: Can you Crack the Code? A fascinating history of ciphers and cryptography by Ella Schwartz illustrated by Lily Williams. Chapter 9 “Prime Time”. (PDF on Canvas)

		Start of Technical Concepts of Blockchain Systems - Cryptographic Hash Functions - Digital Signatures - Decentralized networks - Distributed systems,	But how does bitcoin actually work https://www.youtube.com/watch?v=bBC-nXj3Ng4 (27 minutes) How secure is 256 bit security? https://youtu.be/S9JGmA5_unY (*Video, YouTube 5 minutes*)
			(Optional) Supplemental Material *How Bitcoin Works in 5 Minutes (Video, YouTube, 5 minutes)* *https://www.youtube.com/watch?v=l9jOJk30eQs* The Eureka Moment that made bitcoin possible - Amy Whitaker for WSJ (PDF) *Security engineering* by Ross Anderson - Chapter 6 Cryptography SEv3-ch5-7sep Security Engineering Cryptography.pdf ● 5.2 Historical Background ● 5.3 Security Models ● 5.4 Symmetric crypto algorithms 5.6 Hash Functions Create your own MD5 Hash Collisions https://natmchugh.blogspot.com/2015/02/create-your-own-md5-collisions.htm The great chain of being sure about things *(Article, Economist)* *https://www.economist.com/briefing/2015/10/31/the-great-chain-of-being-sure-about-things* The Money Myth by James Bridle (Article) *https://www.newstatesman.com/politics/2019/07/bitcoin-and-the-money-myth*
2	05-23	How traditional Electronic Payment Systems work Technical Concepts Continued - Mining - Distributed Consensus - Incentives	Narayanan et al. Chapter 2: How Bitcoin Achieves Decentralization Pages 51 – 72 Haber and Stornetta - How to Time Stamp a Digital Document (PDF)

		- Proof of Work - Cryptosystems in practice - Distributed Networks - Attacks - Introduction to Smart Contracts - Altcoins Electricity Use	Review a few pages of your choice from this website: How Does Bitcoin Work?l https://learnmeabitcoin.com/ Mining (Video) Inside a Secret Chinese Bitcoin Mine (10 minutes) https://www.youtube.com/watch?v=K8kua5B5K3I Estimating Bitcoin Electricity Use: A Beginner's Guide (By Jonathan Koomey) https://www.coincenter.org/estimating-bitcoin-electricity-use-a-beginners-guide/
			(Optional) Supplemental Material Narayanan et al. Chapter 3: Mechanics of Bitcoin (Page 75 - 98) But how does bitcoin actually work? https://youtu.be/bBC-nXj3Ng4 (video 26 min) Back, Adam. "Hashcash-a denial of service counter-measure." (2002). http://www.hashcash.org/hashcash.pdf Why I Wrote PGP by Phil Zimmerman *(Article)* *https://www.philzimmermann.com/EN/essays/WhyIWrotePGP.html* Nakamoto "The White Paper" (Article) Inside the Icelandic Facility Where Bitcoin Is Mined https://www.wired.com/story/iceland-bitcoin-mining-gallery/ "Pieces of code that codify business logic. Store Rules, Verify Rules, Self-Execute." Olga Mack
3	05-30	The Ethereum 'Ecosystem' - Smart Contracts Continued - Smart Contract Languages (Solidity & Others) - Layer 2 and Payment Channel Networks (Lightning)	*Narayanan et al.* Chapter 9: Bitcoin as a Platform pages 237 - 247 Narayanan et al. Chapter 10 (Altcoins): Ethereum and Smart Contracts 263 – 271 (Book Chapter) Blockchain and the Law - The Rule of Code - Chapter 4 Smart Contracts as Legal Contracts (pdf) (17 Pages)

			(Video) How Smart Contracts Will Change the World | Olga Mack | TEDxSanFrancisco (17 minutes. Smart Contracts starts at about 6 minute mark) https://www.youtube.com/watch?v=pA6CGuXEKtQ Layer 2, and the Lightning Network https://dci.mit.edu/lightning-network
			Optional Illustrated guide to Ethereum https://www.abra.com/resources/worlds-computer/ Introduction to Solidity, the language of smart contracts on Ethereum https://www.geeksforgeeks.org/introduction-to-solidity/ Solidity by example (voting) https://docs.soliditylang.org/en/v0.8.9/solidity-by-example.html (Article) Introduction to Smart Contracts (Solidity. For Developers) https://docs.soliditylang.org/en/v0.8.9/introduction-to-smart-contracts.html Some blockchain projects improve certain properties over the bitcoin original design. One such type is a Payment Channel Network and one example of such is the Bitcoin Lightning Network. These networks may be susceptible to new attack types as well. [2007.09047] Exploiting Centrality: Attacks in Payment Channel Networks with Local Routing https://arxiv.org/abs/2007.09047 *Decentralized Finance* Crypto Banking and Decentralized Finance, Explained https://www.nytimes.com/2021/09/05/us/politics/cryptocurrency-explainer.html And https://ethereum.org/en/defi/
4	06-06	NFTs and ERC-721 Tokens	*NFTs*

		Stablecoins and other ERC-20 Tokens Decentralized Finance (DeFi) *Begin discussion of Societal Impacts.* - The promise vs. the practice - Energy Usage - Crypto Exchanges - Cybersecurity Considerations - Illicit Content - Money laundering	• NFTs, explained | MIT CSAIL https://www.csail.mit.edu/news/nfts-explained Or What are NFTs https://www.nytimes.com/interactive/2022/03/18/technology/nft-guide.html • The untold story of the NFT boom https://www.nytimes.com/2021/05/12/magazine/nft-art-crypto.html *Stablecoins* • Stablecoins and the Future of Money https://hbr.org/2021/08/stablecoins-and-the-future-of-money • The Technology Underlying Stablecoins https://nehanarula.org/2021/09/23/stablecoins.html *DeFi* Crypto Banking and Decentralized Finance, Explained https://www.nytimes.com/2021/09/05/us/politics/cryptocurrency-explainer.html
			Optional Narayanan - ch. 6 Bitcoin and Anonymity, page 165 - 169 6.1 anonymity basics *Mining (Theory vs Practice)* The Evolution of Bitcoin Hardware https://michaeltaylor.org/papers/Taylor_Bitcoin_IEEE_Computer_2017.pdf *Illicit Content* Does regulation of illegal content need reconsideration in light of blockchains? By Maurice Schellekens, *International Journal of Law and Information Technology*, Volume 27, Issue 3, Autumn 2019, Pages 292–305, https://academic.oup.com/ijlit/article/27/3/292/5601120 *Energy Usage* • Cambridge Bitcoin Electricity Consumption Index (CBECI) https://cbeci.org/

			• Proof of Stake (PoS) Energy consumption of the leading PoS DLTs? http://blockchain.cs.ucl.ac.uk/blockchain-energy-consumption/ • And https://spectrum.ieee.org/ethereum-plans-to-cut-its-absurd-energy-consumption-by-99-percent *Cybersecurity* (Article) Ethereum's smart contracts are full of holes (MIT Technology Review) https://www.technologyreview.com/2018/03/01/144962/ethereums-smart-contracts-are-full-of-holes/ Known Attacks - Ethereum Smart Contract Best Practices https://ethereum-contract-security-techniques-and-tips.readthedocs.io/en/latest/known_attacks/ *Money Laundering* New York Man Charged In $100 Million Bitcoin Case (Forbes) money laundering with bitcoin https://www.forbes.com/sites/billybambrough/2020/05/28/new-york-hacker-charged-in-100-million-dollar-bitcoin-case/#1f3d050ac90e OFAC, the DPRK and the Tornado of Cash by Nicholas Weaver https://www.lawfareblog.com/ofac-dprk-and-tornado-cash *Exchanges* Ponzi Schemes, Private Yachts, and a Missing $250 Million in Crypto: The Strange Tale of Quadriga https://www.vanityfair.com/news/2019/11/the-strange-tale-of-quadriga-gerald-cotten Binance Exchange Outages https://www.cnbc.com/2021/08/19/cryptocurrency-traders-seek-damages-from-binance-after-major-outage.html Crypto Exchanges https://www.nbcnews.com/tech/security/bitcoin-crypto-exchange-hacks-little-anyone-can-do-rcna7870 Why Bitcoin is bullshit, explained by an expert

			https://www.vox.com/conversations/2018/4/11/17206018/bitcoin-blockchain-cryptocurrency-weaver
5	06-13	Governance DAO NFT Continued (as needed) Digital & Fractional Ownership Voting Impacts & Criticisms	**Possible Guest Lecture on Governance, Stay Tuned** ***check Canvas for Final Assigned Readings*** The complexity and arbitrariness of non-fungible tokens (NFTs) are a big part of their appeal. NFTs Show the Value of Owning the Unownable - The Atlantic.pdf Crypto Banking and Decentralized Finance, Explained - https://www.nytimes.com/2021/09/05/us/politics/cryptocurrency-explainer.html DeFi explained by SEC https://www.sec.gov/news/statement/crenshaw-defi-20211109 *Impacts & Criticisms* (Video)(30 min) “Burn it with Fire” by Nicholas Weaver, International Computer Science Institute (ICSI) and University of California, Berkeley at USENIX https://www.youtube.com/watch?v=MQDKMe6MDXQ The complete argument against Crypto by Software Engineer Stephen Diehl https://www.stephendiehl.com/blog/complete.html
			Optional Introduction: What is Web3? https://www.nytimes.com/interactive/2022/03/18/technology/web3-definition-internet.html Review a few abstracts from “Web3 is doing great” https://web3isgoinggreat.com/ Attacking the DeFi Ecosystem with Flash Loans for Fun and Profit - https://hackingdistributed.com/2020/03/11/flash-loans/

6	06-20	Emerging Applications of Blockchain in industry Central Bank Digital Currency (CBDC) Regulatory Discussions Emerging Risks Metaverse	Systemic Risk https://www.reuters.com/breakingviews/crypto-poses-systemic-risks-that-need-swift-remedy-2021-09-07/ *Central Bank Digital Currency (CBDC)* The federal reserve is considering a CBDC https://time.com/nextadvisor/investing/cryptocurrency/expert-reaction-to-fed-digital-currency-report/ *ICO Failures* Nearly Half of 2017's Bitcoin-Backed 'ICO' Projects Have Collapsed - $233 million in funding raised through ICOs has vanished. https://fortune.com/2018/02/25/cryptocurrency-ico-collapse/amp/ Crypto Is Down, So Why Am I Smiling? By Dr. Stornetta https://www.coindesk.com/crypto-is-down-so-why-am-i-smiling What Is the Metaverse, Exactly? https://www.wired.com/story/what-is-the-metaverse/
BELOW ARE ALL OPTIONAL READINGS. These may be helpful for final project sources as well			
		Philosophy and Nuances of Trust Other ‘types’ of Blockchains Public vs. Private	Blockchain and Trust by Bruce Schneier https://www.schneier.com/blog/archives/2019/02/blockchain_and_.html How the NSA (may have) put a backdoor in RSA's cryptography: A technical primer https://blog.cloudflare.com/how-the-nsa-may-have-put-a-backdoor-in-rsas-cryptography-a-technical-primer/ Types of Blockchains & DLTs (Distributed Ledger Technologies) https://blockchainhub.net/blockchains-and-distributed-ledger-technologies-in-general/
		Property Discussions Code is Law ideas ERC-721, NFTs	Art Market and NFTs https://www.nytimes.com/2022/04/14/arts/design/nft-art-market-sothebys.html

			Whitaker, Amy, and Roman Kräussl. Blockchain, Fractional Ownership, and the Future of Creative Work *Available at SSRN 3100389* (2019). https://www.econstor.eu/bitstream/10419/182451/1/1031263918.pdf Art and Blockchain (Article, Artivate.org) A Primer, History, and Taxonomy of Blockchain Use Cases in the Arts https://artivate.org/artivate/article/view/94 *Defining Property in the Digital Environment, Bitmark Inc.* By Casey Alt, Sean Moss-Pultz, Amy Whitaker, & Timothy Chen (26 min read)(PDF on Canvas) A Mid-Year Review of the art market 2021 (Basel) https://d2u3kfwd92fzu7.cloudfront.net/The_Art_Market_Mid_Year_Review_2021.pdf Boom or bubble: how sustainable is the recent success of the online art trade? (Part 3) https://www.hiscox.co.uk/sites/default/files/documents/2021-04/hoatr_report_2020_part3.pdf
		Industry Applications Regulations Alternate views	Who Controls the Blockchain? https://hbr.org/2017/04/who-controls-the-blockchain Can blockchain, a swiftly evolving technology, be controlled? (Article) https://theconversation.com/can-blockchain-a-swiftly-evolving-technology-be-controlled-73471 View of Blockchain technology as a regulatory technology: From code is law to law is code https://firstmonday.org/ojs/index.php/fm/article/view/7113/5657 Crypto Is Down, So Why Am I Smiling? By Dr. Stornetta https://www.coindesk.com/crypto-is-down-so-why-am-i-smiling 'Blockchain' is meaningless (TheVerge) https://www.theverge.com/2018/3/7/17091766/blockchain-bitcoin-ethereum-cryptocurrency-meaning What's Blockchain Actually Good for, Anyway? For Now, Not Much

			https://www.wired.com/story/whats-blockchain-good-for-not-much/ Podcast Why Everybody Who Doesn't Hate Bitcoin Loves It (Ep. 160) (freakonomics radio) https://freakonomics.com/podcast/why-everybody-who-doesnt-hate-bitcoin-loves-it-a-new-freakonomics-radio-podcast/
		Emerging Applications of Blockchain in industry Formulating Research Questions Agriculture (Food traceability). Blockchain for COVID - COVID-19 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? - Can Blockchain provide solutions to emerging COVID-19 related challenges? - What traditional modes of societal interaction or traditional business models have been less resilient than we hoped? Thoughts on the future.	A Cryptocurrency Technology Finds New Use Tackling Coronavirus https://www.wsj.com/articles/a-cryptocurrency-technology-finds-new-use-tackling-coronavirus-11587675966 Five Ways Blockchain Can Unblock The Coronavirus Medical Supply Chain https://www.forbes.com/sites/nishandegnarain/2020/03/22/5-ways-blockchain-can-unblock-the-coronavirus-medical-supply-chain/ Blockchain Can Bring Transparency To Coronavirus Response https://www.coindesk.com/how-blockchain-tech-can-make-coronavirus-relief-more-effective Overstock CEO: How blockchain can help pull us out of the coronavirus recession Article in Fortune Magazine https://fortune.com/2020/07/07/blockchain-technology-regulation-coronavirus-economy/ Blockchain: What It Is, What It Isn't, and What It Means for The Produce Industry https://www.pma.com/content/articles/blockchain IBM Food Trust - Blockchain for the world's food supply https://www.ibm.com/blockchain/solutions/food-trust and BrightFarms adds blockchain tech through IBM Food Trust Network (BrightFarms is now in 2000 stores) https://www.thepacker.com/article/brightfarms-adds-blockchain-tech-through-ibm-food-trust-network

			Produce industry keeping tabs on blockchain | Packer https://www.thepacker.com/article/produce-industry-keeping-tabs-blockchain California Giant blockchain use boosts freshness, food safety https://www.thepacker.com/article/california-giant-blockchain-use-boosts-freshness-food-safety
			More on Stablecoins (Optional) What are stablecoins? A blockchain expert explains https://theconversation.com/what-are-stablecoins-a-blockchain-expert-explains-164812 And Why Washington Worries About Stablecoins https://www.nytimes.com/2021/09/17/business/economy/federal-reserve-virtual-currency-stablecoin.html UnTethered https://slate.com/technology/2021/10/tether-crypto-danger-ben-mckenzie.html PWGR on Stablecoins https://www.sec.gov/news/statement/gensler-statement-presidents-working-group-report-stablecoins-110121 Liberty Reserve Operators Accused of Money Laundering ($6 Billion) https://www.nytimes.com/2013/05/29/nyregion/liberty-reserve-operators-accused-of-money-laundering.html How a $300K Bored Ape Yacht Club NFT accidentally sold for $3K https://www.cnet.com/news/how-a-300k-bored-ape-yacht-club-nft-was-accidentally-sold-for-3k/ Why Johnny Can't Encrypt 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

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 in person and via or the class Discussion board which is hosted on Canvas.

Academic Integrity

https://www.cmu.edu/student-affairs/theword/academic/statement-on-academic-integrity.html#statement
Carnegie Mellon is a self-governing institution that requires ethical behavior of its administration, faculty, staff and students that goes beyond simple compliance with the law. Respect for these requirements creates a moral authority for the university to insist upon appropriate behavior. This authority is essential to the accomplishment of the university's mission. Integrity as described in this statement is a defining feature of the university community's high expectations for the conduct of its members.

Further

Academic Integrity is a core CMU value, and as a member of the CMU community, it is important that the work you turn in for this class is wholly your own. As your instructor, I will strive to ensure that you develop the necessary knowledge and skills to meet the learning objectives for this class, just as it is your task to put in the effort to complete the work and ask for help if you need it. In this hybrid/remote environment, you might have questions about what is and is not acceptable. I will attempt to provide resources clarifying what cheating, plagiarism, and unauthorized assistance look like and how to avoid them. You should always refer to the CMU resources on academic integrity if you have any questions or concerns - https://www.cmu.edu/student-affairs/theword/academic/statement-on-academic-integrity.html#statement

In particular, for this class, if you use language in written submitted work you MUST encapsulate it in quotes AND cite the source of the work. These are not your words and you must cite all references. We will be using software in the class to identify sequences of words and statements that have been submitted elsewhere. You will need to ensure that you follow correct CITATION guidance which will be provided on the first day of this course. This applies to all assignments, all projects, and all submitted graded work.

This class is intended to make you think and to write down your thoughts. Your work will often rely upon the thoughts and words of others. You should cite and acknowledge these works but you should not be heavily quoting from material for the bulk of your written assignments. We are looking for your own work, not a rehash of the work done by others. If you intend to build or apply a point made by another author, and you state their point you MUST QUOTE THEM AND CITE THEM. If you do not, your submission can be considered plagiarism as you are indicating by not citing them that the words and the sequence they are put in are your own.

The consequences of plagiarism can be an academic referral. Please avoid plagiarism or any type of cheating in this class. You may of course ask questions and ask for help from the instructor if this is unclear.

Evaluation Method

15% - Course Reading & Comprehension 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

Heinz School guidelines will be used in deciding on the overall grade distribution. However, I grade individual assignments 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-19 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 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.

Late Final Projects

Late Final Projects submitted up to 24 hours after the due date and time will only be eligible for 80% of the maximum number of points allotted. Since Final Projects are the largest portion of your final grade, submitting them even a few hours late can drop your final score by nearly a full letter grade. I highly encourage you to submit Final Projects before the final due date. Assignments submitted more than 24 hours after the due date will not be accepted.

Accommodations for Students with Disabilities

If you have a disability and have an accommodations 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. If you suspect that you may have a disability and would benefit from accommodations but are not yet registered with the Office of Disability Resources, I encourage you to contact them at access@andrew.cmu.edu.

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 Technology in the Classroom

Research has shown that divided attention is detrimental to learning, so I encourage you to close any windows not directly related to what we are doing while you are in class. Please turn off your phone notifications and limit other likely sources of technology disruption, so you can fully engage with the material, each other, and me. This will create a better learning environment for everyone.

For in person class you will not need to bring your laptop.

See the professionalism section below for guidance on the use of devices in class. You will be expected to act and behave as in a professional setting. You may use a laptop to take notes during class if that is your preference.

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

We will be having discussion in person and 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 includes 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 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. I also want to ensure that students have access to the class. I will make the recordings available on Canvas 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 do my best to provide opportunities for reasonable asynchronous work. This will generally include reading the class reading materials, watching the class lecture, reviewing any handouts and slides, 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 using a short assignment.

DO NOT COME TO CLASS WITH SYMPTOMS OR IF YOU ARE AWAITING TEST RESULTS. PLEASE BE SAFE.

Lectures will be recorded. Contact me if you have questions.

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, (412) 268-2150
- **Report-It online anonymous reporting platform:** 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.