CSE 5392-002: Fundamentals of Blockchain and Cryptocurrency Technologies - Summer 2020

Course Syllabus

Course Information

Instructor: Sajib Datta

Contact Information: sajib.datta@uta.edu

Office hours: TBA

Credit: 3 credit hours

Class time and location: TBA

Class Website: TBA

GTA: TBA

Course Overview

Decentralized cryptocurrencies, such as Bitcoin and Ethereum, have gained rapid popularity and the future potential of blockchains has captured the attention of academics, researchers, entrepreneurs, economists, and policy-makers. Blockchains and cryptocurrencies promise to create new disruptive markets, and revolutionize how we think of banking and finance, corporate governance, voting, law, and online gaming. This course will cover the technical concepts underlying these systems: decentralized ledgers (blockchains), decentralized consensus, smart contracts and zero-knowledge proof systems.

Objectives

The goal of this course is to introduce students to current state of the art in blockchains and cryptocurrencies. We'll cover the technical background of applied cryptography and incentive mechanisms. To really understand what is special about Blockchain and Cryptocurrency, we need to understand how it works at a technical level. We'll address the important questions about Bitcoin, such as: How does Bitcoin work? What makes Bitcoin different? How secure are your Bitcoins? How anonymous are Bitcoin users? What determines the price of Bitcoins? Can cryptocurrencies be regulated? What might the future hold? Projects will involve hands-on practice with cryptocurrency tools, such as sending and receiving cryptocurrency payments, and programming smart contracts. The course will also survey the wide variety of potential future applications.

Outcomes

Students will understand how cryptocurrencies work and the ideas, technologies, and organizations sprouting from it. Students will gain working familiarity with blockchain technology through practical projects. After this

course, students will know everything they need to be able to separate fact from fiction when reading claims about Bitcoin and other cryptocurrencies. Students will have the conceptual foundations they need to engineer secure software that interacts with the Bitcoin network and with the network of other cryptocurrencies. And students will be able to integrate ideas from Bitcoin in their own projects.

Textbook & Materials

Bitcoin and Cryptocurrency Technologies. Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller, Steven Goldfeder and Jeremy Clark. Available free online at https://d28rh4a8wq0iu5.cloudfront.net/bitcointech/readings/princeton_bitcoin_book.pdf

Bitcoin: A Peer-to-Peer Electronic Cash System. Satoshi Nakamoto. Available free online at https://bitcoin.org/bitcoin.pdf

How the Bitcoin protocol actually works. Michael Nielsen. Available free online at http://www.michaelnielsen.org/ddi/how-the-bitcoin-protocol-actually-works/

Grading Policy:

Quizzes 60% (8 quizzes – 4 announced and 4 unannounced)
Projects 40% (3 projects that will require both programming and problem solving)
- Project 1: Bitcoin transactions
- Project 2: Consensus from trust
- Project 3: Reading
- Project 4: Implementation of a blockchain node

Final grades are based on the standard ranges of A: 90–100, B: 80–89, C: 70–79, D: 60–69, F: 0–59.

Course Content (in chronological order)

Introduction to Crypto and Blockchain: Basics, History and Cryptography (Week 1)

Learn about cryptographic building blocks ("primitives") and reason about their security. Work through how these primitives can be used to construct simple cryptocurrencies.

1. Overview
2. What is Blockchain
3. Public Ledgers
4. Blockchain as public ledgers
5. Bitcoin
6. Blockchain 2.0
7. Smart Contracts
8. Block in a Blockchain
9. Transactions
10. Distributed Consensus
11. The Chain and the Longest Chain
12. Cryptocurrency to Blockchain 2.0
13. Permissioned Model of Blockchain

14. Cryptographic Hash Functions
15. Properties of a hash function
16. Hash Pointers and Data Structures
17. Digital Signatures
18. Public Keys as Identities
19. A Simple Cryptocurrency

A Cryptographic Description and Bitcoin Basics (Week 1)

Learn about cryptographic tools and digital currency protocols.

1. Public-Key Cryptographic Tools
2. A Simplified Electronic Cash Protocol
3. Untraceable Electronic Payments
4. A Basic Electronic Cash Protocol
5. Creation of coins
6. Payments and double spending
7. FORTH – the precursor for Bitcoin scripting
8. Bitcoin Scripts
9. Bitcoin P2P Network
10. Transaction in Bitcoin Network
11. Block Mining
12. Block propagation and block relay
13. Why Consensus
14. Distributed consensus in open environments
15. Consensus in a Bitcoin network

Security Issues (Week 1)

Learn about security issues in blockchain and cryptocurrency ecosystem.

1. Multiple Spending Prevention
2. Wallet Observers
3. Security Failures
4. Restoring Traceability

Distributed Consensus and Permissioned Blockchain (Week 2)

Learn about distributed consensus and permissioned blockchain.

1. Bitcoin Consensus
2. Introduction to Proof of Work (PoW)
3. Hashcash PoW
4. Bitcoin PoW
5. Attacks on PoW and the monopoly problem
6. Proof of Stake, Proof of Burn and Proof of Elapsed Time
7. The life of a Bitcoin Miner
8. Mining Difficulty
9. Mining Pool
10. Permissioned model and use cases
11. Design issues for Permissioned Blockchains
12. Execute contracts

13. State machine replication
14. Consensus models for permissioned Blockchain
15. Distributed consensus in closed environment
16. Paxos

How Bitcoin Achieves Decentralization (Week 2)

Learn Bitcoin's consensus mechanism and reason about its security. Appreciate how security comes from a combination of technical methods and clever incentive engineering.

1. Centralization vs. Decentralization
2. Distributed Consensus
3. Consensus without Identity: the Block Chain
4. Incentives and Proof of Work
5. Putting It All Together

Mechanics of Cryptocurrency (Week 2)

Learn how the individual components of the Bitcoin protocol make the whole system tick: transactions, script, blocks, and the peer-to-peer network.

1. Bitcoin Transactions
2. Bitcoin Scripts
3. Applications of Bitcoin Scripts
4. Bitcoin Blocks
5. The Bitcoin Network
6. Limitations & Improvements

How to Store and Use Cryptocurrencies (Week 3)

We'll explore how using Bitcoins works in practice: different ways of storing Bitcoin keys, security measures, and various types of services that allow you to trade and transact with bitcoins.

1. How to Store and Use Bitcoins
2. Hot and Cold Storage
3. Splitting and Sharing Keys
4. Online Wallets and Exchanges
5. Payment Services
6. Transaction Fees
7. Currency Exchange Markets

Cryptocurrency Mining (Week 3)

We already know that Bitcoin relies crucially on mining. But who are the miners? How did they get into this? How do they operate? What's the business model like for miners? What impact do they have on the environment?

1. The Task of Bitcoin Miners
2. Mining Hardware

3. Energy Consumption & Ecology
4. Mining Pools
5. Mining Incentives and Strategies

Bitcoin and Anonymity (Week 4)

Is Bitcoin anonymous? What does that statement even mean—can we define it rigorously? We'll learn about the various ways to improve Bitcoin's anonymity and privacy and learn about Bitcoin's role in Silk Road and other hidden marketplaces.

1. Anonymity Basics
2. How to de-anonymize Bitcoin
3. Mixing
4. Decentralized Mixing
5. Zerocoin and Zerocash
6. Tor and the Silk Road

Community, Politics, and Regulation (Week 4)

We'll look at all the ways that the world of Bitcoin and cryptocurrency technology touches the world of people. We'll discuss the community, politics within Bitcoin and the way that Bitcoin interacts with politics, and law enforcement and regulation issues.

1. Consensus in Bitcoin
2. Bitcoin Core Software
3. Stakeholders: Who's in Charge?
4. Roots of Bitcoin
5. Governments Notice Bitcoin
6. Anti Money-Laundering
7. Regulation
8. New York's BitLicense Proposal

Alternative Mining Puzzles (Week 4)

Not everyone is happy about how Bitcoin mining works: its energy consumption and the fact that it requires specialized hardware are major sticking points. Here we'll look at how mining can be re-designed in alternative cryptocurrencies.

1. Essential Puzzle Requirements
2. ASIC Resistant Puzzles
3. Proof-of-useful-work
4. Nonoutsourceable Puzzles
5. Proof-of-Stake "Virtual Mining"

Bitcoin as a Platform (Week 5)

One of the most exciting things about Bitcoin technology is its potential to support applications other than currency. We'll study several of these and study the properties of Bitcoin that makes this possible.

1. Bitcoin as an Append-Only Log
2. Bitcoin As Smart Property
3. Secure Multi-Party Lotteries in Bitcoin
4. Bitcoin As Randomness Source
5. Prediction Markets & Real-World Data Feeds

Altcoins and the Cryptocurrency Ecosystem (Week 5)

Hundreds of altcoins, or alternative cryptocurrencies, have been started, either to fix Bitcoin's perceived flaws or to pursue different goals and properties. We'll look at everything that goes into an altcoin and how they interact with Bitcoin.

1. Short History of Altcoins
2. Interaction Between Bitcoin and Altcoins
3. Lifecycle of an Altcoin
4. Bitcoin-Backed Altcoins, "Side Chains"

The Future of Blockchain and Cryptocurrency (Week 5)

The use of Bitcoin technology for decentralizing property, markets, and so on has been hailed as a recipe for economic and political disruption. We'll look at the technological underpinnings of these proposals and the potential impact on society.

1. The Block Chain as a Vehicle for Decentralization
2. Routes to Blockchain Integration
3. What Can We Decentralize?
4. When Is Decentralization a Good Idea?

Projects: Every project has a given due date. No late projects will be accepted without prior permission from the course instructor. (Five minutes late is still late.) Projects will be posted on the class website. Projects must be individual effort. The Statement of Ethics you will receive details the definitions of collusion, plagiarism, and academic dishonesty as related to lab assignments in CSE. Each project will be graded on a number of factors. Always make sure that a turned in project compiles without warnings or errors even if it is not complete. You will receive partial credit for a working stubbed (incomplete) program. Programs that do not compile successfully (with compiler warnings or errors) will receive no credit. In addition to compiling successfully, the program must run without errors. If the program is only partially complete, the parts that are complete must run without errors to receive credit for those parts. The program documentation should indicate which parts of the program are working. The TAs grading the projects will be running the programs to verify their performance.

Attendance: At The University of Texas at Arlington, taking attendance is not required. Rather, each faculty member is free to develop his or her own methods of evaluating students' academic performance, which includes establishing course-specific policies on attendance. As the instructor of this section, I have decided that attendance at class meetings is not required but strongly encouraged.

Exams: Material covered on the exams will be based on the class lectures and assigned chapters. All exams are mandatory. There are NO make-up exams after the scheduled times. All exams will be kept by the instructor.

Drop Policy: Students may drop or swap (adding and dropping a class concurrently) classes through self-service in MyMav from the beginning of the registration period through the late registration period. After the late registration period, students must see their academic advisor to drop a class or withdraw. Undeclared students must see an advisor in the University Advising Center. Drops can continue through a point two-thirds of the way through the term or session. It is the student's responsibility to officially withdraw if they do not plan to attend after registering. Students will not be automatically dropped for non-attendance.

American with Disabilities Act: The University of Texas at Arlington is on record as being committed to both the spirit and letter of all federal equal opportunity legislation, including the Americans with Disabilities Act (ADA). All instructors at UT Arlington are required by law to provide "reasonable accommodations" to students with disabilities, so as not to discriminate on the basis of that disability. Any student requiring an accommodation for this course must provide the instructor with official documentation in the form of a letter certified by the staff in the Office for Students with Disabilities, University Hall 102. Only those students who have officially documented a need for an accommodation will have their request honored. Information regarding diagnostic criteria and policies for obtaining disability-based academic accommodations can be found at www.uta.edu/disability or by calling the Office for Students with Disabilities at (817) 272-3364.

Title IX: The University of Texas at Arlington is committed to upholding U.S. Federal Law "Title IX" such that no member of the UT Arlington community shall, on the basis of sex, be excluded from participation in, be denied the benefits of, or be subjected to discrimination under any education program or activity. For more information, visit www.uta.edu/titleIX.

Academic Integrity: At UT Arlington, academic dishonesty is completely unacceptable and will not be tolerated in any form, including (but not limited to) cheating, plagiarism, collusion, the submission for credit of any work or materials that are attributable in whole or in part to another person, taking an examination for another person, any act designed to give unfair advantage to a student or the attempt to commit such acts (UT System Regents Rule 50101, 2.2). Suspected violations of academic integrity standards will be referred to the Office of Student Conduct. Violators will be disciplined in accordance with University policy, which may result in the students' suspension or expulsion from the University. Homework assignments are not group projects; each student is expected to write his or her own programs individually. Students should not be showing each other their code prior to the deadline for submission.

Student Support Services: UT Arlington provides a variety of resources and programs designed to help students develop academic skills, deal with personal situations, and better understand concepts and information related to their courses. Resources include tutoring, major-based learning centers, developmental education, advising and mentoring, personal counseling, and federally funded programs. For individualized referrals, students may contact the Maverick Resource Hotline by calling 817-272-6107, sending a message to resources@uta.edu, or visiting www.uta.edu/resources.

Electronic Communication Policy: UT Arlington has adopted MavMail as its official means to communicate with students about important deadlines and events, as well as to transact universityrelated business regarding financial aid, tuition, grades, graduation, etc. All students are assigned a MavMail account and are responsible for checking the inbox regularly.

Campus Carry: Effective August 1, 2016, the Campus Carry law (Senate Bill 11) allows those licensed individuals to carry a concealed handgun in buildings on public university campuses, except in locations the University establishes as prohibited. Under the new law, openly carrying handguns is not allowed on college campuses. For more information, visit http://www.uta.edu/news/info/campus-carry/

Student Feedback Survey: At the end of each term, students enrolled in classes categorized as lecture, seminar, or laboratory will be asked to complete an online Student Feedback Survey (SFS) about the course and how it was taught. Instructions on how to access the SFS system will be sent directly to students through MavMail approximately 10 days before the end of the term. UT Arlingtons effort to solicit, gather, tabulate, and publish student feedback data is required by state law; student participation in the SFS program is voluntary.

Final Review Week: A period of five class days prior to the first day of final examinations in the long sessions shall be designated as Final Review Week. The purpose of this week is to allow students sufficient time to prepare for final examinations. During this week, there shall be no scheduled activities such as required field trips or performances; and no instructor shall assign any themes, research problems or exercises of similar scope that have a completion date during or following this week unless specified in the class syllabus. During Final Review Week, an instructor shall not give any examinations constituting 10% or more of the final grade, except makeup tests and laboratory examinations. In addition, no instructor shall give any portion of the final examination during Final Review Week. During this week, classes are held as scheduled. In addition, instructors are not required to limit content to topics that have been previously covered; they may introduce new concepts as appropriate.