ITP499 – Blockchain

Units: 3

Spring 2018

USC Viterbi School of Engineering

Course Description

Bitcoin! The cryptocurrency that has been applauded, ridiculed, hacked (well, not directly), and dismissed. Yet it is trading at a high exchange rate against the USD. Whatever the fate of bitcoin, the technological breakthrough is worth studying. Blockchain is the distributed and decentralized database technology behind this cryptocurrency. This course explores the fundamentals of the public, transparent, secure, immutable and distributed database called blockchain. Blockchains can be used to record and transfer any digital asset not just currency. This course will introduce students to the workings and applications of this potentially disruptive technology. Its potential impact on financial services, government, banking, contracting and identity management will be discussed.

Learning Objectives

Students will be able to achieve the following learning objectives at the completion of the course.

- Be able to explain what is blockchain
- Be able to explain why we need blockchain. What is the real world problem(s) that blockchain is trying to solve
- Understand and describe how blockchain works
- Explain the underlying technology of transactions, blocks, proof-of-work, and consensus building
- How does blockchain exist in the public domain (decentralized, distributed) yet maintain transparency, privacy, anonymity, security, immutability, history
- How is blockchain incentivized without any central controlling or trusted agency
- How bitcoin cryptocurrency works
- Why people value a 'digital' currency, how it can be protected against scam, fraud, hacking attacks, and forks
- Design and implement new ways of using blockchain for applications other than cryptocurrency
- Explore platforms such as Ethereum to build applications on blockchain

Prerequisites

None

Course Format/Location

Lecture: 2-3:20 TTh
Room: ZHS163

Instructor

Name: Nitin Kalé, Associate Professor of Engineering Practice, Viterbi School of Engineering
Office: Olin Hall of Engineering 412
Office Hours: 4 hours per week. Schedule varies by semester
Contact Info: kale@usc.edu | (213) 740-7083

Teaching Assistant

Name: TBD
Contact Info: TBD

IT Help

IT Support: Provided by Viterbi IT
Hours of Service: 8am – 5pm M-F
Walk-in: DRB 205
Phone: (213) 740-0517
Email: engrhelp@usc.edu

Course Materials

Lectures are delivered face to face in classroom. Lectures are not recorded so attendance is strongly recommended. All course materials will be made available through Blackboard. These include –

- Lecture slides
- Homework Assignments
- Readings
- Software details and instructions for accessing Viterbi Virtual Lab
- Grades and feedback
- In-office and online office hours
- Online discussion forums will be used for out-of-class discussions

Technology Proficiency and Hardware/Software Required

The assignments for this class will include both reading assignments as well as hands-on computer assignments. Tools for doing the computer based assignments will be provisioned through a **virtual lab** from Viterbi Information Technology (VIT). Students will be able to use their personal computer to access the virtual lab at any time during the semester. Students ***must*** bring their laptop computers to lecture sessions to participate in hands-on activities. Students will be given tutorials to gain familiarity with software tools.

Textbook

Title: Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction,
Author: Arvind Narayanan
Publisher: Princeton University Press (July 19, 2016)
ISBN-10: 0691171696
ISBN-13: 978-0691171692

Assignments

Homework: Most homework is computer based. Homework should be turned in to Blackboard on time. Grading will be based on completeness, accuracy, and timeliness. Feedback will be provided through Blackboard. These are individual effort assignments.
Exams and Quizzes: are written, in-class tests (either on paper or online).

Final Project: Final project is a team based project (teams of 3 students each). The project will be design a blockchain database to be used in an application of the team's choice. The blockchain can be designed on a platform such as Ethereum. Teams will have to show the design methodology, implementation details, viability of the application, and incentive for miners to join the blockchain and the potential disruption to existing business or industry.

Grading of final project:		
	Design	40%
	Implementation	20%
	Testing and deployment	20%
	Viability and incentivizing*	20%

* Viability, in this project, means if the blockchain application has potential for success in terms of adoption, resistance to hacking, sustainable population interest, and sufficient business investment.
Incentivizing, in this project, means if the blockchain application has the potential to attract independent 'miners' without whom the blockchain does not progress. Miners are computers that expend computational power to mine for rewards and get to update the blockchain as a database of permanent record.

Grading Breakdown

The weight of graded material during the semester is listed below.
No extra credit assignments will be offered.

Homework	35%
Final Project	15%
Exam I	25%
Exam II	25%
Total	100%

Assignment Submission Policies

It is the responsibility of the student to make sure problem solution and assignment are turned in on time. Make sure you follow the procedures outlined in each assignment (Blackboard submissions).

Late assignment submissions will be subject to a late penalty of 25% per day. No assignments will be accepted later than four days from the due date.

Additional Policies

No make-up exams (except for documented medical or family emergencies) will be offered nor will there be any changes made to the Final Exam schedule, except as permitted by university rules. Lecture attendance is not mandatory however it is recommended that students not miss any lecture.

Incomplete and Missing Grades

Excerpts for this section have been taken from the University Grading Handbook, located at http://www.usc.edu/dept/ARR/grades/gradinghandbook/index.html. Please see the link for more details on this and any other grading concerns.
A grade of Missing Grade (MG) "should only be assigned in unique or unusual situations… for those cases in which a student does not complete work for the course before the semester ends. All missing grades must be

resolved by the instructor through the Correction of Grade Process. One calendar year is allowed to resolve a MG. If an MG is not resolved [within] one year the grade is changed to [Unofficial Withdrawal] UW and will be calculated into the grade point average a zero grade points.

A grade of Incomplete (IN) "is assigned when work is no completed because of documented illness or other 'emergency' occurring after the twelfth week of the semester (or 12th week equivalency for any course scheduled for less than 15 weeks)."

Statement on Academic Conduct and Support Systems

Academic Conduct:
Plagiarism – presenting someone else's ideas as your own, either verbatim or recast in your own words – is a serious academic offense with serious consequences. Please familiarize yourself with the discussion of plagiarism in *SCampus* in Part B, Section 11, "Behavior Violating University Standards" https://policy.usc.edu/scampus-part-b/. Other forms of academic dishonesty are equally unacceptable. See additional information in *SCampus* and university policies on scientific misconduct, http://policy.usc.edu/scientific-misconduct.

Support Systems:
Student Counseling Services (SCS) - (213) 740-7711 – 24/7 on call
Free and confidential mental health treatment for students, including short-term psychotherapy, group counseling, stress fitness workshops, and crisis intervention. https://engemannshc.usc.edu/counseling/

National Suicide Prevention Lifeline - 1-800-273-8255
Provides free and confidential emotional support to people in suicidal crisis or emotional distress 24 hours a day, 7 days a week. http://www.suicidepreventionlifeline.org

Relationship and Sexual Violence Prevention Services (RSVP) - (213) 740-4900 - 24/7 on call
Free and confidential therapy services, workshops, and training for situations related to gender-based harm.
https://engemannshc.usc.edu/rsvp/

Sexual Assault Resource Center
For more information about how to get help or help a survivor, rights, reporting options, and additional resources, visit the website: http://sarc.usc.edu/

Office of Equity and Diversity (OED)/Title IX Compliance – (213) 740-5086
Works with faculty, staff, visitors, applicants, and students around issues of protected class. https://equity.usc.edu/

Bias Assessment Response and Support
Incidents of bias, hate crimes and microaggressions need to be reported allowing for appropriate investigation and response. https://studentaffairs.usc.edu/bias-assessment-response-support/

The Office of Disability Services and Programs
Provides certification for students with disabilities and helps arrange relevant accommodations. http://dsp.usc.edu

Student Support and Advocacy – (213) 821-4710
Assists students and families in resolving complex issues adversely affecting their success as a student EX: personal, financial, and academic. https://studentaffairs.usc.edu/ssa/

Diversity at USC

Information on events, programs and training, the Diversity Task Force (including representatives for each school), chronology, participation, and various resources for students. https://diversity.usc.edu/

USC Emergency Information
Provides safety and other updates, including ways in which instruction will be continued if an officially declared emergency makes travel to campus infeasible, http://emergency.usc.edu

USC Department of Public Safety – 213-740-4321 (UPC) and 323-442-1000 (HSC) for 24-hour emergency assistance or to report a crime.
Provides overall safety to USC community. http://dps.usc.edu

Blockchain
ITP 499 (3 units)

Course Outline

Week 1– Course Introduction

- Course objectives and outcomes
- History of centralized services, trusted third party for transactions
- Making a case for a trustless system
- Why blockchain
- You are your own bank?
- Decentralized transactions
- No permission for transactions needed

Reading: *None*
Assignment: None

Week 2 – History

- How and when blockchain/bitcoin started
- Milestones on the development of bitcoin
- Criticism, ridicule and promise of bitcoin
- Sharing economy
- Internet of Value

Reading: *https://bitcoin.org/bitcoin.pdf*
Assignment: Explore various popular blockchain applications. Create a list of those applications and the industries/businesses they are impacting
Due Date: Week 3

Week 3 – Overview of blockchain technology

- What is blockchain
- Transactions
- Blocks
- Hashes
- Consensus
- Verify and confirm blocks

Reading: *http://scet.berkeley.edu/wp-content/uploads/BlockchainPaper.pdf*
Assignment: Explore the bitcoin blockchain on blockchain.info
Due Date: Week 4

Week 4 – Hashes

- Hash cryptography
- Encryption vs hashing

Reading: *http://scet.berkeley.edu/wp-content/uploads/BlockchainPaper.pdf*

Assignment: Use an online service to generate hashes for content
Due Date: Week 5

Week 5 – Transactions

- Recording transactions
- Digital signature
- Verifying and confirming transactions

Reading: *http://chimera.labs.oreilly.com/books/1234000001802/ch02.html*
Assignment: Build a transaction and then hash it. Generate public and private keys. Digitally sign a transaction
Due Date: Week 6

Week 6 – Blocks and blockchain

- Hash pointers
- Blocks

Reading: *http://chimera.labs.oreilly.com/books/1234000001802/ch07.html#_introduction_2*
Assignment: Explore the bitcoin blockchain on blockchain.info for block generation. Explore how long it takes a block to be confirmed.
Due Date: Week 7

Week 7 – Consensus building

- Distributed consensus
- Byzantine generals problem
- Proof of work, Proof of Stake, Proof of Space etc.
- Writing to the blockchain

Reading: *http://chimera.labs.oreilly.com/books/1234000001802/ch08.html*
Assignment: Use an online service to illustrate how consensus is built in a distributed system with no central authority.
Due Date: Week 8

Week 8 – Exam I

Week 9 – Mining and incentivizing blockchain

- Game theory behind competitive mining
- Race to beat the others (including hackers)
- Proof of work
- Incentives – mining and transaction fees
- CPU considerations
- Energy expended in mining
- Profitability
- Mining pools

Reading: *http://chimera.labs.oreilly.com/books/1234000001802/ch08.html*
Assignment: What is the computing power needed to mine and generate bitcoin? Explore if miner pools are dominating bitcoin mining. Compare incentives from mining activity vs transaction fees.

Due Date: Week 11

Week 10 – Security and safeguards

- Protecting blockchain from attackers
- Forks – soft and hard

Reading: *https://www.bbvaopenmind.com/en/a-secure-model-of-iot-with-blockchain/?utm_source=views&utm_medium=article06&utm_campaign=MITcompany&utm_content=banafa-jan07*

Week 11 – Bitcoin

- Bitcoin creation and economy
- Bitcoin exchanges
- Bitcoin limited supply and deflation?
- Famous hacks
- Scalability (1MB problem)
- Wallets

Reading (second time): *https://bitcoin.org/bitcoin.pdf*
Assignment: Install a bitcoin wallet. Generate and secure your private key. Send a small transaction amount (to be monetized by instructor) to another user. Track the transaction through blockchain. Verify the confirmation and commitment of the transaction to the bitcoin blockchain.
Due Date: Week 13

Week 12 – Blockchain applications

- Government
- Identity management
- Auto executing contracts
- Three signature escrow
- Triple entry accounting
- Elections and voting?

Reading: *https://www.evry.com/globalassets/insight/bank2020/bank-2020---blockchain-powering-the-internet-of-value---whitepaper.pdf*
Assignment: Pick three industries. Research the application of blockchain in those industries. Describe how blockchain could be successful in those industries.
Due Date: Week 14

Week 13 – Blockchain applications (cont.)

- Identity management
- Property records, titles
- Micropayments
- Notary
- Sidechains

Reading: *https://www.evry.com/globalassets/insight/bank2020/bank-2020---blockchain-powering-the-internet-of-value---whitepaper.pdf*

Week 14 – Final Project

- Introduction to Ethereum platform
- Design a new blockchain
- Potential for disruption
- How to incentivize blockchain
- Design a *Distributed Application* (DAPP)

Reading: *https://media.consensys.net/programmable-blockchains-in-context-ethereum-s-future-cd8451eb421e#.z4788f3kx*
Assignment: Work on final project
Due Date: Week 16

Week 15 – Exam II

Week 16 – Final Project **Due**