ITP256 – Blockchain

Units: 4

Catalogue Description

Explore blockchain technology, a secure and immutable way to record transactions. Learn the workings of cryptocurrencies. Explore the impact on financial services, business and contracting.

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 US Dollar. 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, anonymity, security, immutability, history
- How is blockchain secured without any central controlling or trusted agency
- How is the blockchain incentivized
- How bitcoin cryptocurrency works
- What are the economics of bitcoin (limited supply cryptocurrency)
- Why people value a ‘digital’ currency, how it can be protected against scams, fraud, hacks and attacks
- Explore platforms such as Ethereum to build applications on blockchain
- Explore new ways of using blockchain for applications other than cryptocurrency

Prerequisites

None

Co-requisites

None

Concurrent Enrollment

None

Recommended Preparation

None

Lecture

Time: 2 x 110 minute lectures per week
Room: TBD

Instructor

Name: Nitin Kalé, Associate Professor of Engineering Practice, Viterbi School of Engineering
Office: Olin Hall of Engineering 412
Office Hours: TBD
Contact Info: kale@usc.edu | (213) 740-7083

Teaching Assistant(s)

Name: TBD
Office: TBD
Office Hours: 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 Notes

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.

Required Readings and Supplementary Materials

Textbook

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

Draft version of textbook can be downloaded here -

https://d28rh4a8wq0iu5.cloudfront.net/bitcointech/readings/princeton_bitcoin_book.pdf

Supplementary Materials

- Additional reading materials will be assigned and provided through Blackboard

Description and Assessment of 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: Two exams. They are written, in-class tests.

Final Project: Final project is a team based project (teams of 3 students each). The final project will entail the application of blockchain technology to non-currency use cases. Students will use the Ethereum platform to propose and design this application. Although no coding will be required, the algorithm for the application must be designed as part of the final project.

Grading of final project:	Design	40%
	Validation	30%
	Viability and incentivizing*	30%

* 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 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. The points for each category of assessment will be posted on Blackboard during the semester.

No extra credit assignments will be offered.

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

Grading Scale

Course final grades will be determined using the following scale

A	95-100
A-	90-94
B+	87-89
B	83-86
B-	80-82
C+	77-79
C	73-76
C-	70-72
D+	67-69
D	63-66
D-	60-62
F	59 and below

Assignment Submission Policy

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, family emergencies or religious observation) 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.

Grading Timeline

Every effort will be made to provide Grades and feedback within 7 business days of the assignment deadline.

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)."

Blockchain

ITP 256 (4 units)

Course Outline

Week	Lecture	Topic	Reading	Homework	Due Date
1	1	From Bullae to Bitcoin: Course introduction and motivation	https://sites.utexas.edu/dsb/	HW1: Questions on ledgers, accounting and origins of writing	End of Week 2
	2	History of money	Lecture notes		
2	3	Landmark technological advances	Lecture notes	HW2: Questions on forms of money in history	End of Week 3
	4	Introduction to peer-to-peer networks	Narayanan: Chapter 1 Read Nakamoto Paper		
3	5	The birth of Bitcoin	Narayanan: Chapter 1	HW3: Questions on earlier attempts at digital money.	End of Week 4
	6	Features of bitcoin	Narayanan: Chapter 2		
4	7	Hash cryptography	Narayanan: Chapter 1	HW4: Hands-on exercises with SHA256. Demonstrate properties of hash functions	End of Week 5
	8	Basics of peer-to-peer transactions	Narayanan: Chapter 3		
5	9	Digital signatures	Narayanan: Chapter 3	HW5: Create digital signatures using ECDSA and SHA256. Questions on digital signatures and the working of ECDSA.	End of Week 6
	10	ECDSA	Narayanan: Chapter 3		

6	11	Blocks	Narayanan: Chapter 2	HW6: Install/explore the bitcoin blockchain. Questions on blockchain.	End of Week 7
	12	Merkle trees	Narayanan: Chapter 2		
7	13	Blockchain	Narayanan: Chapter 2	HW7: Questions on merkle proofs	End of Week 8
	14	Blockchain contd.	Narayanan: Chapter 2		
8	15	Byzantine generals’ problem	Lecture notes	HW8: How does bitcoin solve BGP.	End of Week 9
	16	**Exam I**			
9	17	Mining and incentivizing blockchain	Narayanan: Chapter 5	HW9: Compute mining difficulty, bits and target for bitcoin blockchain	End of Week 10
	18	Mining difficulty	Narayanan: Chapter 5		
10	19	Mining details	Narayanan: Chapter 5	HW10: Cost of mining calculations	End of Week 11
	20	Consensus building	Narayanan: Chapter 5, 8		
11	21	Bitcoin supply	Narayanan: Chapter 3	HW11: Calculate the bitcoin supply curve, totals, inflation, value	End of Week 12
	22	Forks	Narayanan: Chapter 3		
12	23	How to acquire and store bitcoin	Narayanan: Chapter 4	HW12: Install bitcoin wallet. Create a transaction. Create multisig transaction.	End of Week 13
	24	Scalability of bitcoin	Narayanan: Chapter 3		
13	25	How to break bitcoin	Narayanan: Chapter 6	HW13: Questions on various ways to attack bitcoin	End of Week 14
	26	Ethereum	Lecture notes	Final Project	Week 16
14	27	Ethereum contd.	Lecture notes		
	28	Blockchain use cases	Narayanan: Chapter 9		
15	29	Blockchain use cases contd.	Lecture notes		
	30	**Exam II**			
16	Final Project Due				

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