Blockchains, Security and Privacy
Clemson University, Spring 2021

Cross Listed:
Math 9850, Math 4500
ECE 6930, ECE 4990

Online: 5:00pm--6:15pm TR
(Zoom Meeting ID: 951 9639 1608 Passcode: 058452**)**

Instructors: Dr. Richard Brooks (ECE), Email: rrb@clemson.edu
Dr. Shuhong Gao (Math), Email: sgao@clemson.edu

Office Hours: Online by appointment.

Textbook: **No textbook, Online Materials and Lecture Notes**

Objective: This course is an introduction to blockchain technology and its business applications. The course consists of three parts: the first part is a series of lectures covering the basic concepts and cryptographical tools used in blockchains and crypto-currencies, the second part is on programming experience on smart contracts (in Ethereum), and the third part is for teams to work on projects in various business applications. Ideally each team consists of students from Math, CS, ECE and others, a mixture of graduate and undergraduate students. Each team will be advised by one or both instructors, and the students have the option to continue working on the project in the summer or Fall in the goal of writing up a technology transition plan.

Grading:		
	Homework	50%
	Midterm Exam (take home)	20%
	Project and Presentation	30%

Project: The final project is a team based project (teams of 3 students each). The project will be design of a decentralized application, leveraged on a blockchain (e.g. Ethereum). Teams will have to show the design methodology, implementation details, viability of the application, and the potential disruption to existing business or industry.

Homework: Five homework will be assigned related to basic concepts and programs; see the course calendar for more details including the due dates.

The grading scale is as follows.

A: 100--90 B: 89--80 C: 79--70 D: 69--60 F: 59--0

Learning Objectives: Upon completion of this course, the students should have a comprehensive and clear understanding of blockchains and smart contracts programming, security and privacy attributes of the system, homomorphic encryption, zero knowledge proof, and the ability to implement appropriate systems.

Course Modality: Online Synchronous: The class will meet virtually (through Zoom) at the scheduled class time on TR. **All course materials and announcements will be posted on Canvas.**

Attendance Policy: All students are expected to be regular and punctual online at Zoom. Attendance will be taken in Zoom for the instructor's records. If the instructor does not show up on Zoom within 15 minutes after the scheduled start time, the class is dismissed for the day. If the instructor's connection is lost during a virtual class, students are expected to work together until the end of the class meeting time even if the instructor is not able to reconnect.

Academic Integrity: Students are expected to adhere to the following official Clemson academic integrity statement. "As members of the Clemson University community, we have inherited Thomas Green Clemson's vision of this institution as a high seminary of learning. Fundamental to this vision is a mutual commitment to truthfulness, honor, and responsibility, without which we cannot earn the trust and respect of others. Furthermore, we recognize that academic dishonesty detracts from the value of a Clemson degree. Therefore, we shall not tolerate lying, cheating, or stealing in any form."

Providing or using materials (like Chegg) to provide or obtain an academic advantage is in violation of the University's academic integrity policy. Giving someone else access to your Canvas and/or MyLab Math account violates the code of student conduct computer use policy and could be considered in violation of the academic integrity policy.

The penalties for academic integrity violations can be severe and any student found to be in violation will be subject to penalties as outlined in the Undergraduate Academic Integrity Policy. See the Undergraduate Academic Integrity Policy (http://catalog.clemson.edu/content.php?catoid=16&navoid=478#undergraduate-academic-integrity) for additional information.

Required Technology:

- Adobe Reader
- Computer with speakers or headphones. (This course includes audio components.)
- Web camera and microphone (integrated microphone with laptop is sufficient).
- Reliable internet connection (see https://ccit.clemson.edu/working-remotely/ if you need assistance with internet connectivity).
- Ability to scan and upload written work. Suggested scanning apps are CamScanner and AdobeScan. (If you have a tablet, submitting written work from the tablet is also acceptable.)
- Other apps/websites to be used include: Zoom and Gradescope.

Non-Discrimination: Clemson University is committed to a policy of equal opportunity for all persons and does not discriminate on the basis of race, color, religion, sex, sexual orientation, gender, pregnancy, national origin, age, disability, veteran's status, genetic information or protected activity in employment, educational programs and activities, admissions and financial aid. This includes a prohibition against sexual harassment and sexual violence as mandated by Title IX of the Education Amendments of 1972. This policy is located at http://www.clemson.edu/campus-life/campus-services/access/title-ix/.
Ms. Alesia Smith is the Clemson University Title IX Coordinator, and the Executive Director of Equity Compliance. Her office is located at 110 Holtzendor_ Hall, 864.656.3181 **(voice) or 864.656.0899 (TDD).**

Blockchains, Security and Privacy
Spring 2021 Tentative Schedule

	Date	Lecture topic	Teacher
Thursday	1/7/2021	Overview and syllabus	Both
Tuesday	1/12/2021	Blockchain overview	RRB
Thursday	1/14/2021	Bitcoin and Ethereum data structures	RRB
Tuesday	1/19/2021	Hash Functions and Digital Signatures	Shuhong
Thursday	1/21/2021	Finite Fields and Elliptic Curve Groups	Shuhong
	1/26/2021	Homework 1 due	
Tuesday	1/26/2021	Byzantine Generals and Consensus Algorithms	RRB
Thursday	1/28/2021	Byzantine Generals and Consensus Algorithms	RRB
Tuesday	2/2/2021	Zero Knowledge proofs	Shuhong
Thursday	2/4/2021	Zero Knowledge proofs	Shuhong
Tuesday	2/9/2021	Zero Knowledge proofs	Shuhong
	2/11/2021	Homework 2 due	
Thursday	2/11/2021	Trusted/trustless, and Mining	RRB
Tuesday	2/16/2021	Smart contracts	RRB
Thursday	2/18/2021	Smart contracts	RRB
	2/18/2021	Homework 3 (Blockchain Program) due	
Tuesday	2/23/2021	Midterm Exam (take home)	
Thursday	2/25/2021	Smart contracts	RRB
Tuesday	3/2/2021	Homomorphic Encryption	Shuhong
Thursday	3/4/2021	Homomorphic Encryption	Shuhong
	3/9/2021	Home 4 (Private Program) due	
Tuesday	3/9/2021	Project design	Both
Thursday	3/11/2021	Design evaluation	Both
Tuesday	3/16/2021	**Spring Break**	
Thursday	3/18/2021	**Spring Break**	
Tuesday	3/23/2021	Dark Coin/Dash	RRB
Thursday	3/25/2021	Monero and Ring Signatures	Shuhong
Tuesday	3/30/2021	Zcash, zk-Rollup, and Confidential Arithmetic	Shuhong
Thursday	4/1/2021	Integration of key trees and blockchain	Both
	4/6/2021	Home 5 (Private Smart Contract) due	
Tuesday	4/6/2021	Trusted Enclaves	Both
Thursday	4/8/2021	Integration of zero knowledge proofs and blockchain	Both
Tuesday	4/13/2021	Integration of Enclaves and blockchain	Both
Thursday	4/15/2021	Integration of homomorphic computing and smart contracts	Both
Tuesday	4/20/2021	Project Presentation	Both
Thursday	4/22/2021	Project Presentation	Both
Tuesday	4/27/2021		
Thursday	4/29/2021	Project Presentation (7:00 to 9:30 PM)	Both