Course Syllabus

CS 5594: Blockchain Technologies

Spring 2023

1 General Course Information

CRN	13552 / 13554
Meeting Time	Tuesdays and Thursdays @ 11:00 AM - 12:15 PM
Classroom	TORG 1030 (Blacksburg) & Room 113 (NVC Campus)
Group Presentation	(Tentative) from April 02, 2024 (Tue) to May 02, 2024 (Thu)
Final Project	Due **11:59 PM @ May 05, 2024** (Sun)

Instructor: Thang Hoang

- Office Hours: Tuesdays @ 1:00 PM – 3:00 PM
- Modality: Zoom (link will be posted on Canvas)
- Email: thanghoang@vt.edu

Teaching Assistants:

	Tung Le	**Alex Tsai**
Email	tungle@vt.edu	alextsai1618@vt.edu
Office Hours	Fridays @ 10:00 AM – 12: 00 PM	Wednesdays & Fridays @ 1:00 PM – 3:00 PM
Modality	Hybrid	Hybrid
Phys. Location	MCB 122 (Blacksburg)	Room 314 (NVC Campus)
Zoom link	(posted on Canvas)	

Course website: http://thanghoang.github.io/teaching/sp24/cs5594/

Canvas: https://canvas.vt.edu

Textbook (Preferred):

- *Bitcoin and Cryptocurrency Technologies.* Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller, and Steven Goldfeder. Princeton University Press, 2016. ISBN: 978-0691171692.
- *Foundations of Distributed Consensus and Blockchain.* Elaine Shi. Book manuscript, 2020.
- *Introduction to Modern Cryptography (3rd edition).* Jonathan Katz and Yehuda Lindell. Chapman and Hall/CRC, 2020. ISBN: 978-0815354369.
- *A Graduate Course in Applied Cryptography.* Dan Boneh and Victor Shoup. Book manuscript, 2020.

2 Prerequisites

- N/A

3 Course Objectives

Principles of emerging blockchain technologies. Fundamental data structures and cryptographic building blocks in blockchain such as distributed systems, cryptographic primitives including cryptographic hash functions, asymmetric cryptography, and digital signatures. Critical blockchain components and infrastructures such as distributed ledger, consensus protocols, cryptocurrencies, and smart contracts. Security and privacy aspects in decentralized applications.

4 Grading

Grading for this course will be on a 100-point scale with the following distribution:

- Homework Assignments: 50%
- Group Presentation: 20%
- Final Project: 30%

Homework. There will be tentatively **four** assignments. The homework assignment will be posted on the course website approximately two weeks before the due date.

All homework must be typeset with LaTeX and submitted as a single PDF to Canvas by **11:59 PM** on the due date. Any required drawings must be drawn by a digital drawing program. *Handwritten submissions will not be accepted!*

Late Submission Policy: Late submission can only be accepted if the student can present a police report or a doctor's note indicating an emergency.

Group Presentation and Final Project: The students will form a group with 3-4 students per group to conduct research on selected topics related to blockchain technologies throughout the course. The potential topic list includes, but is not limited to:

- Security and privacy in blockchain and decentralized applications.
- Blockchain in specific domains (e.g., IoT, cloud computing, social networking, machine learning, finance, healthcare)
- Cryptocurrencies
- Smart contracts

The students can choose one of the following approaches for their group research:

- Theoretical analysis and comparison of existing works.
- Implementation and experimental comparison of existing methods.
- New blockchain algorithms and system designs.

Details about these approaches will be given in the first class. Reference materials are research articles published in top-tier cybersecurity, system and blockchain venues such as

- Conferences: IEEE S&P, ACM CCS, USENIX Security, ISOC NDSS, PETS, CRYPTO, EUROCRYPT, ASIACRYPT, TCC, IEEE ICBC, IEEE ICB, NSDI, OSDI
- Journals: ACM/IEEE Transactions.
- **Group Presentation**: Each group will present their research findings towards the end of the semester (tentatively starting from Week 13–16). There will be 25 minutes for each group presentation with 5 minutes for Q&A. **All the students in the group must present** to get credits.
- **Final Project:** Each group will submit a final report and source code (if required) as their final course project. The report must be typeset with LaTeX and submitted as a single PDF. Guidelines regarding the structure of the final report will be provided in class. The students will be graded individually; therefore, a statement of contribution will be mandatory to determine the contribution of each student in the group.

Grading Scale: A (93+) A- (90-92) 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-)

Grading will not be curved.

Grade Dissemination: Individually through Canvas.

5 Attendance

This class will be organized as hybrid synchronous, where the face-to-face meeting is in TORG 1030 along with a concurrent online session on Zoom. While there are PDF lecture notes available on the course website, some content will be delivered on the virtual whiteboard.

6 Readings

There will be reading assignment (will be posted on the course website) to be completed by class time. The reading assignment generally contains some research articles, few sections or chapters in the textbook.

7 Course Topics

Below is the list of tentative topics (subject to change) to be covered in this class.

Week 1: Introduction to Blockchain

- Course overview and logistics
- What is blockchain?
  - Centralized vs. decentralized systems
  - Blockchain = distributed system + cryptography + game theory
- Why blockchain?

Week 2-4: Fundamental Data Structures and Cryptographic Primitives

- Distributed systems, distributed consensus mechanisms
- Cryptographic hash functions and hash-based primitives
- Public-key cryptography
- Digital signatures
- Elliptic Curve Cryptography

Week 5-8: Blockchain Technologies

- Bitcoin as blockchain basics
  - Bitcoin network
  - Bitcoin address
  - Bitcoin transactions
  - Bitcoin blocks and chain of blocks
  - Bitcoin consensus protocols: byzantine fault tolerance, proof-of work
  - Mining and incentivizing model in bitcoin
  - Bitcoin limitations and challenges
- Other useful consensus protocols
  - Proof of useful work, proof of stake, proof of burn, proof of elapsed time, etc.
- Permissioned blockchain
  - Raft, Paxos, Streamlet
- Building decentralized/distributed applications with blockchain
  - Smart contracts
  - Ethereum, solidity

Week 9-13: Advanced Topics in Blockchain

- Confidential transactions
  - Anonymity and deanonymization
  - Tor, Silkroad
  - Privacy-preserving computation
  - Zero-knowledge proofs
- Privacy-preserving blockchain platforms
- Decentralized storage and applications

Week 14-16: Group Presentations

8 Academic Accommodations

If the student anticipates or experiences academic barriers that may be due to disability, including but not limited to ADHD, chronic or temporary medical conditions, deaf or hard of hearing, learning disability, mental health, or vision impairment, please contact the Services for Students with Disabilities (SSD) office (540-231-3788, ssd@vt.edu, or visit https://ssd.vt.edu).

If the student has an SSD accommodation letter, please meet with the instructor privately during office hours as early in the semester as possible to deliver the letter and discuss accommodations. The student

must give the instructor reasonable notice to implement the accommodations, which is generally 5 business days and 10 business days for final exams.

9 Academic Integrity

The Honor Code applies. All work submitted must be the student's own work. Students may solicit help *only* from the instructor or the teaching assistant. The Undergraduate Honor Code pledge that each member of the university community agrees to abide by the states:

"As a Hokie, I will conduct myself with honor and integrity at all times. I will not lie, cheat, or steal, nor will I accept the actions of those who do."

Students enrolled in this course are responsible for abiding by the Honor Code. A student who has doubts about how the Honor Code applies to any assignment is responsible for obtaining specific guidance from the course instructor before submitting the assignment for evaluation. Ignorance of the rules does not exclude any member of the University community from the requirements and expectations of the Honor Code. See additional information about the Honor Code here.

All the lecture notes, assignments, quizzes, tests, exams, solutions, and other materials distributed to or generated in this class are intended for use only by students enrolled in this CRN (section) this semester. Without the instructor's written permission, no one may show, give, or otherwise make such class materials available to anyone not enrolled in this CRN this semester. Prohibited activities include, but are not limited to, uploading a test, uploading solutions to problems, and submitting such class materials for online posting. The prohibition on sharing solutions applies to all solutions, regardless of who wrote the solutions.