CS5594: Blockchain Technologies
(Spring 2021)

Catalog Description: The course will explore the principles of emerging blockchain technologies. The course will first cover basic data structures and cryptographic building blocks in blockchain such as distributed systems, cryptographic primitives including cryptographic hash functions, asymmetric cryptography, digital signatures. The course will then focus on critical blockchain components and infrastructures such as distributed ledger, consensus protocols, cryptocurrencies and smart contracts. The course will also cover several recent advancements in blockchains such as privacy-preserving blockchain, decentralized applications. The successful students are expected to obtain a good understanding of cryptographic primitives and blockchain essentials, which will be a unique skill for competitive R&D positions in industry.

Pre-requisites:

- N/A

Learning Outcome: Having successfully completed this course, the students will be able to

- Harness blockchain technologies on various applications domains ranging from economics to healthcare.
- Propose a new blockchain design for specific application requirements by exploiting new data structures and algorithms
- Analyze the performance of existing blockchain technologies on the market
- Assess the pros and cons of blockchain applications including cryptocurrency, smart contracts.

Recommended Textbook

- "Bitcoin and Cryptocurrency Technologies, A Comprehensive Introduction".
  Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller, And Steven Goldfeder.
  Princeton University Press.

List of (Tentative) Topics

The list of topics may be subject to change as the course proceeds.

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: Basic 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 elapsed time, etc
- Permissioned blockchain
    - Raft, Paxos, Streamlet
- Building decentralized/distributed applications with blockchain
  - Smart contracts
  - Ethereum, solidity, etc

Week 9-12: Advanced Topics in Blockchain

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

Week 13-16: Student Presentation

Grading Policy:
Homework: 30%
In-class paper presentation: 25%
Research project: 40%
In-class participation and (potential) quizzes: 5%
No mid-term/final

Late Submission Policy: Late homework submission will be accepted until either (*i*) the solution is posted or (*ii*) the problem is discussed in class, but the penalty will be applied (15% reduction in grade for each late day submission). There will be no makeup for project reports and in-class presentations. Exception will be made if the student can present a police report or a doctor's note indicating emergency situation.

Grading Scale: A (90+); B(81-89); C(71-80); D(61-70); E (51-60); F(50-)

Grade Dissemination: Individually through online teaching platform (e.g., Canvas)

Academic Integrity: Commission of any of the acts, including *Cheating*, *Plagiarism*, *Falsification*, *Fabrication*, *Multiple Submission*, *Complicity*, *Violation of University, College, Departmental, Program, Course or Faculty Rules*, shall constitute academic misconduct. This listing is not, however, exclusive of other acts that may reasonably be said to constitute academic misconduct. Clarification is provided for each definition with some examples of prohibited behaviors in the Undergraduate Honor Code Manual located at https://www.honorsystem.vt.edu/

Student with Disabilities: If the student needs adaptation or accommodation because of a disability (learning disability, attention deficit disorder, psychological, physical, etc.), if the student has emergency medical information to share with the lecturer, or if the student needs special arrangements, please make contact the lecturer as soon as possible.

Covid-19 Statement: Virginia Tech is committed to protecting the health and safety of all members of its community. By participating in this class, all students agree to abide by the Virginia Tech Wellness principles. To uphold these principles, in this class the student must do the following when attending in-person meetings:

- Wear a face covering during class, including as you enter and exit the classroom.
- Maintain the designated distancing guidelines of the classroom.
- Enter and exit the classroom according to posted signage.

If the student is exhibiting even the slightest sign of illness, they must not attend an in-person class. Notify the lecture by email and follow the instructions posted at https://vt.edu/ready/health.html#tips.

Important Note: This class (Spring 2021) does not require in-person meetings and, therefore, will be held virtually. All the teaching materials (slides, lectures, group meetings, presentations) will be delivered via online teaching platforms.

Early Notification Requirement for Observed Religious Day: Consistent with the university's tradition of religious tolerance, faculty and staff are encouraged to be sensitive to students who wish to observe religious and ethnic holidays. The student should request and provide justification for a religious accommodation to the lecturer, preferably during the first two weeks of classes or as soon as the student becomes aware of the need for an accommodation.