CS 5594: BLOCKCHAIN TECHNOLOGIES

Spring 2024

THANG HOANG, PhD

COURSE OVERVIEW AND ORGANIZATION

Outline

- About Instructor
- High-level Objectives
- Grading
- (Tentative) Schedule
- Course Details
- Q&A

About Instructor

- **Assistant Professor**, CS Dept, Virginia Tech (Jan 2021 – current)
  - Applied Security and Privacy Lab
  - Research Topics: Applied Cryptography, Privacy, Secure and Trustworthy Computation, Fuzzy Crypto, Privacy-Preserving Machine Learning
  - Publications, patents, open-source frameworks
- **Ph.D. (2020)**
  - University of South Florida (2019-2020)
  - Oregon State University (2015-2018)
  - Privacy-Preserving Functional Information Systems
- **M.S. (2014)**
  - Chonnam National University (S. Korea) (2012-2014)
  - Mobile Authentication with Machine Learning and Biometric Cryptosystem

Learning Objectives

- Understand principles of emerging blockchain technologies
- Harness blockchain on various applications domains (economics, healthcare)
- Design your own blockchains for specific application requirements

FOUNDATIONAL PRIMITIVES

- Distributed Systems
  - Peer-to-peer networks
  - Consensus
  - Security & Threat
- Cryptography
  - Hash function
  - Signatures

CORE TECHNIQUES

- Public blockchains
  - Architecture
  - How it works
- Private blockchains
  - Access control, consensus
- Smart contracts
  - Blockchain applications

ADVANCED TOPICS

- Confidential transactions
- Decentralized storage

Grading

- **NO** midterm and final
- **Homework (50%):** Tentative 4-5 HW problem sets with programming involved (Python, Java, Solidity)
  - Ask to explore deeper topics covered throughout the class
- **Presentation (20%):** Present paper(s) from top security/blockchain/system venues
  - Important chance to practice for a future career
- **Final Project (30%):** Extra credit for research-oriented papers
  - Select a topic and write a comprehensive research article (10-page IEEE double-column style)
  - Develop knowledge based on an important topic -> Practice executive reports

- **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-)
  - No curve, no late tolerance

Course Topics (Tentative)

- **Week 1: Introduction**
  - History of Blockchain. What is Blockchain?
  - Why Blockchain?
- **Week 2-4: Fundamental Data Structures and Cryptographic Primitives**
  - Distributed systems, distributed consensus
  - Cryptographic hash, hash-based primitives
  - Public key cryptography, digital signatures
  - Elliptic Curve cryptography
- **Week 5-8: Blockchain Technologies**
  - Bitcoin as public blockchain basics
    - Network, address, transactions, blocks, consensus, mining, challenges
  - Other consensus protocols (PoUW, PoS, PoA)
  - Private blockchain

Course Topics (Tentative)

- **Week 5-8: Blockchain Technologies (cont.)**
  - 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 (Zcash, Monero, Hawk)
  - Decentralized storage and applications
- **Week 14-16: Group Presentation**

Final Project

- Select papers from a topic of interest and conduct a comprehensive research
  - Recommended List: ACM CCS, IEEE S&P, NDSS, USENIX Security, IEEE ICBC, IEEE BLOCKCHAIN, EuroS&P, Crypto, Eurocrypt, IEEE INFOCOM, ACSAC, IEEE ICDSC, PoPETs, Asiacrypt, NSDI, OSDI
  - Published between 2020 – 2024
  - Blockchain-related
- **Potential topic list (but not limited to)**
  - Security & privacy of blockchain technology
  - Distributed ledgers
  - Distributed consensus
  - Blockchain in specific domains (e.g., IoT, cryptocurrency, cloud computing, social networking, machine learning, finance, healthcare, information forensics)
  - Smart contracts

Final Project

- Form a group of three/four, and inform your topic to the instructor ASAP
  - Email your group info including **group name**, **students' name and PID**, and your **selected topic** to thanghoang@vt.edu
  - Deadline: **Feb 01, 2023 (Thu) 11:59 PM EST**

- Link to keep track of your registration https://docs.google.com/spreadsheets/d/1g5j0aX5d0-0TxOc4gqqbAL2GHS1pMRNIye2U99VGCMU/edit?usp=sharing

Group Presentation

- Deliver research findings in your final project via a presentation
- Finalize your presentation schedule soon
  - Volunteering preferred, or randomization will be enforced
- **No re-scheduling:** Only possible with a doctor's note

Final Project Approaches

- **Theoretical analysis and comparison of existing results** ✓
- **Implementation and comparison of existing methods** ✓✓
  - Survey paper publications at the end of the course
- **New algorithm design, new system design** ✓✓✓
  - Publications at top-tier security or blockchain venues
- Different topics OK, but must be blockchain-related and allowed by your advisor
  - Your advisor may want to keep it secret (confidentiality requirement of your funding)
  - Do NOT bring it up unless you are permitted, or there will be trouble for all of us!
- There will be an interim report in the middle of the semester, and you will be given one-to-one feedback on your report
  - Will be partially graded, so do NOT put off your writing

Final Project

- A good opportunity to master your research and writing skills (very important)
- A good guideline to research writing
  - https://www.darpa.mil/work-with-us/heilmeier-catechism

- **The Heilmeier Catechism**
  - What are you trying to do? Articulate your objectives using absolutely no jargon.
  - How is it done today, and what are the limits of current practice?
  - What's new in your approach and why do you think it will be successful?
  - Who cares? If you're successful, what difference will it make?
  - What are the risks and the payoffs?
  - How much will it cost? How long will it take?
  - What are the midterm and final "exams" to check for success?

Logistics and Notes

- Teaching Tools and Resources
  - Canvas
  - Course webpage: https://thanghoang.github.io/teaching/sp24/cs5594/
- Teaching Team
  - **Instructor: Dr. Thang Hoang**
    - Office: Suite 4304, Gilbert Place Building
    - Email: thanghoang@vt.edu
    - Webpage: https://thanghoang.github.io
  - **TA 1: Tung Le**
    - Email: tungle@vt.edu
  - **TA 2: Alex Tsai**
    - Email: alextsai1618@vt.edu
- Announcement & communication: via Canvas (please turn on notification!)

Logistics and Notes

- Lecturer: Dr. Thang Hoang (@thanghoang)
  - Office hours: **Tuesdays @ 12:30 PM – 2:00 PM**
  - Zoom link: Announced on Canvas
- TA 1: Tung Le
  - Office hours:
    - **Fridays @ 10:00 AM – 12:00 PM (In-person & Zoom)**
  - In-person location: TBD
  - Zoom link: Announced on Canvas
- TA 2: Alex Tsai
  - Office hours:
    - **Wednesdays and Fridays @ 1:00 PM – 3:00 PM (In-person & Zoom)**
  - In-person location: TBD
  - Zoom link: Announced on Canvas

Logistics and Notes

- **Check the course webpage and Canvas regularly**
  - Slides, research papers, and assignments will be put on the course webpage
- Register for the Canvas announcement and read the syllabus!
- Free online resources:
  - Crypto books
    - Introduction to Modern Cryptography (3rd Edition). Jonathan Katz and Yehuda Lindell. Chapman and Hall/CRC. 2020.
    - A Graduate Course in Applied Cryptography (free). Dan Boneh and Victor Shoup, 2020
  - Blockchain books:
    - Bitcoin and Cryptocurrency Technologies. Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller, Steven Goldfeder. Princeton University Press, 2016. (draft)
    - Foundations of Distributed Consensus and Blockchain (free). Elaine Shi. 2020
  - Google, iacr, arxiv

Q&A

- Question?