

CS 5594: BLOCKCHAIN TECHNOLOGIES

Spring 2021

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 (Dec 2020 – current)
 - Applied Crypto Lab: We are recruiting Ph.D. and M.S. students!
 - Research Topics: Privacy-Enhancing Technologies, Applied Cryptography, Network Security
 - 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, but...
- **Homework (30%)**: Tentative 3-4 HW problem sets with programming involved (Python or Java)
 - Ask to explore deeper in topics covered throughout the class
- **Presentation (20%)**: Present paper(s) from top-tier security/blockchain conferences
 - Important chance to practice for future career!
- **Survey Paper (a team of two) (45%)**: Extra-credit for research-oriented papers
 - Select a topic and write a detailed survey paper (6 pages IEEE double column style)
 - Develop a knowledge based on an important topic -> Practice executive reports
- **Participation (5%)**: Constructive feedback for student presentations will be collected plus in-class engagement
- **Grading Scale**: A (90+); B(81-89); C(71-80); D(61-70); E (51-60); F(50-)

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 (PoW, PoS, PoA)
 - Private blockchain

Course Topics (Tentative)

- **Week 5-8: Blockchain Technologies (cont.)**
 - Building decentralized/distributed applications with blockchain
 - Smart contracts
 - Ethereum, solidity
- **Week 9-12: 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**

Student Presentation

- Finalize your presentation schedule soon
 - Volunteering preferred, or other policies will be implemented
- **No re-scheduling:** Only possible with a doctor note
- Select papers from top-tier cyber-security or blockchain conferences
 - 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
 - Published between 2015 – 2020
 - Blockchain-related

Final Project

- Select some papers in the previous list, but publication date can be older
- Potential topic list (but not limited to)
 - Security & privacy of blockchain technology,
 - Blockchain platforms
 - Blockchain in specific domain (e.g., IoT, cryptocurrency, cloud computing, social networking, machine learning, etc)
 - Smart contracts
- Form a group of two, and inform the instructor your topic ASAP
 - Single-person project possible
 - Email your group info including students' name and ID, and your selected topic to thanghoang@vt.edu
 - Deadline: **Jan 29, 2021 (Fri) 11:59 PM EST**

Final Project

- **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 topic OK, but must be blockchain-related and allowed from 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 in trouble for all of us!
- **There will be interim report at the middle of semester, and you will be given one-to-one feedback on your report**
 - Will be 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/Spring21/CS5594/>
- Teaching Team
 - Instructor: Thang Hoang, Ph.D.
 - Office: Suite 2202, VT Knowledge Works II Building
 - Email: thanghoang@vt.edu
 - Webpage: <https://thanghoang.github.io>
 - TA: Waad Aldndni
 - Email: waada@vt.edu
- Announcement & communication: via Canvas

Logistics and Notes

- Lecturer (Thang Hoang)
 - Office hours: **Friday @ 2 PM – 4 PM**
 - Zoom link:
<https://virginiatech.zoom.us/j/84859897740?pwd=Nk53bCtEWnArTGtZdUQva1l5Q0oxQT09>

- TA (Waad Aldndni)
 - Office hours: **Monday @ 3 PM – 5 PM**
 - Zoom link: <https://virginiatech.zoom.us/j/6641881060>

Logistics and Notes

- **Check course webpage and Canvas regularly**
 - Slides, research papers, assignment will be put at course webpage and announced on Canvas
- Register for Canvas Announcement
- Free online blockchain resources:
 - Crypto books
 - Introduction to Modern Cryptography, by Jonathan Katz and Yehuda Lindell
 - Blockchain books:
 - “Bitcoin and Cryptocurrency Technologies”, by Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller, Steven Goldfeder
 - “Mastering Bitcoin”, by Andreas M. Antonopoulos
 - Google, IACR, arxiv, etc
- Read syllabus!

Question?

- Question?