INFO7500 - Cryptocurrency and Smart Contracts

Instructor

Dr. Suhabe Bugrara received a Ph.D. in computer science from Stanford University and B.Sc. from MIT. He has published in top academic conferences in operating systems, computer security, and software engineering. He wrote his Ph.D. dissertation on state space reduction techniques for program analysis and verification. His is currently a security researcher at ConsenSys focusing on smart contract security. Previously, he was founder of *Wise OR*, a software startup in Silicon Valley focusing on optimizing the profitability of surgical cases at world-class hospitals. Contact: sbugrara@northeastern.edu.

Course description

Understand how cryptocurrencies and blockchain protocols work in practice by examining the underlying technical mechanisms such as cryptography, peer-to-peer networks, decentralized ledgers, distributed consensus, mining, and incentive engineering. Explore the novel decentralized applications enabled by cryptocurrency such as smart contracts and decentralized autonomous organizations. Learn about surrounding issues such as privacy, anonymity, security, legislation, and market. Gain practical expertise through challenging programming projects on cryptography, blockchains, distributed consensus, Bitcoin and Ethereum.

Textbook

Required: *Bitcoin and Cryptocurrency Technologies* by Narayanan, Bonneau, Felten, Miller, Goldfeder.
An earlier draft of the textbook can be found online: http://bit.ly/1Qr0PZI. This earlier draft should be close to the published textbook. However, officially, you are responsible for the content in the most recently published textbook.

Grading Policy

Final grades will depend on:
1. Weekly in-class quizzes (30%). Lowest quiz grade will be dropped.
2. Programming projects (70%). Late submissions: Total 7 days late across all projects. Then, 30% off the project grade for each additional late day.

Academic Integrity Policy

1. Absolutely no collaboration on homework projects is allowed unless specifically indicated. Approved group projects will be possible later in the course.
2. Please read carefully the University's policy on academic integrity, which is taken very seriously in this course. Dishonesty will result in an automatic failure of the course and reported to the Program Director and the Office of Student Conduct.

Prerequisites: Strong programming skills in Java.

Syllabus

Applied Cryptography – Hashing, Signatures, Commitments, Asymmetric Encryption
Intro to Cryptocurrency – Transactions, Blocks, Authenticated Data Structures, Scripting
Distributed Consensus – Byzantine Fault Tolerance, Proof of Work, Incentives, GHOST Protocol
Distributed Systems – Bitcoin, Ethereum
Mining – Selfish-Mining Attacks, Mining Pool Centralization
Peer-to-Peer Networks – Transaction Propagation, Network Latency, Connectivity
Smart Contracts – Solidity, Web3, Solidity, Decentralized Applications
Security Vulnerabilities – Smart Contract Auditing
Research Perspectives and Challenges