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.

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 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 (20%)
2. A 5-minute presentation on any blockchain-related topic (10%)
3. Programming projects (70%). Late submissions: Total 3 days late across all homeworks. Then, 30% off the homework 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

Intro to Cryptography
Intro to Cryptocurrency
Transactions, Blocks and Scripts
Decentralization and Distributed Consensus
Incentives and Proof of Work
Peer-to-Peer Networks
Blockchain Applications
Cryptocurrency Ecosystem
Research Perspectives and Challenges
Intro to Ethereum Smart Contracts
Ethereum Contract Security