CIS700: Security Protocols with Application to Blockchains

Dr. Yuzhe Tang, Email: ytang100@syr.edu, Phone: 315.443.4350, Office: 4-193 CST

Learning Objectives

Students will be able to 1) Understand Ethereum internal mechanisms, 2) Analyze the security of Blockchain-based decentralized applications, 3) Design and develope Blockchain-based decentralized applications, 4) Understand and analyzing existing security protocols

Pre-requisite: 1) CIS600/FIN600, Blockchain and Cryptocurrency [ink] or 2) Completion of Blockchain labs [ink]

Big questions to answer in this seminar:

- "What's the future of Ethereum?"
- "What's the future of DApp and DAO?"

Schedule (Tentative)

- Topic 1: Blockchain learning
  - Read Ethereum source code
    - Reports & lectures
  - Read codebase change (EIP, BIP, ERC)
    - Reports & lectures
  - Read JS code in Contract-based DApps
    - Reports & lectures
    - Programming projects (Reinvent the wheel)
  - Read protocol papers: blockchain applications, altcoin blockchain design
    - Lectures
- Topic 2: Information-security protocols and security infrastructures
  - Theory: Textbook learning
    - Lectures
    - Research paper presentations
  - Practice: Measurement

Texts

- Mastering Ethereum: Smart contract and decentralized applications, Andreas M. Antonopoulos, Gavin Wood [online book]
- Mastering Bitcoin: Programming the Open Blockchain, Andreas Antonopoulos, [online book]
- Information Security, Mark Stamp

Grading

Programming projects/paper presentations (50%), reports & lectures (50%).

- Late submission policy: 10% off within one day, 40% off within two days, 50% off within three days, 70% off within one week.