CS438/SEC532 – Blockchain: Security and Applications
Spring 2023-2024

Description and objectives

- This course aims to provide a survey on blockchain and the topics around such as history of blockchain, cryptography it uses, Bitcoin and other currencies, consensus algorithms, smart contracts, scalability etc.
- The main motivation is making the students understand the components of blockchain, the terms, jargon people use, the things one need to consider while designing and implementing one, integrating a blockchain to a real-life application. In addition, after the lecture, the students can implement objects on a blockchain such as a smart contract on Ethereum.

Topics to be covered

- Introduction to Blockchain: its history and current state
- Practical applications of public and private blockchains
- Bitcoin internals
- Ethereum and smart contracts
- Proof of Stake, BFT and other consensus algorithms
- Blockchain scalability and interoperability
- Decentralized Finance
- Conclusions and recap

Instructor

- Dr. Kamer Kaya, FENS G012, ext. 9566.
- Office Hour: by appointment – you can also send e-mails.

Textbook(s)

There are no formal books but you are free to read the following. They are free. You do not need to buy them.

- *Mastering Bitcoin by Andreas Antonopoulos*:
  https://drive.google.com/file/d/0B8lgcDXI8hEfbXFYcTh6aXNqRkk/view?usp=sharing
  Source: https://github.com/bitcoinbook/bitcoinbook
- *Mastering Ethereum, by Andreas M. Antonopoulos, Gavin Wood:*
  https://github.com/ethereumbook/ethereumbook
- *Bitcoin and Cryptocurrency Technologies (Princeton textbook)* by Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller, and Steven Goldfeder:
  https://d28rh4a8wq0iu5.cloudfront.net/bitcointech/readings/princeton_bitcoin_book.pdf

Schedule

- Monday 13:40-14:30, FASS G022
- Tuesday 13:40-15:30, FASS G022

Grading:

- Midterm (20%): During the lecture (21/05/2024, Tuesday)
- Group project (40%)
  - Proposal: 29/03/2024, Friday
  - Final presentations: After the lectures, during the final exam period.
  - Final code submission with corrections: TBA
- Homework assignments (30% - 40%): There will be 4-5 (technical and non-technical) HWs.
- Paper presentation (%10) – only for SEC 532 students.