Blockchains & Distributed Ledgers

Lecture 00 - Course Administrativia

Aggelos Kiayias

Administrivia

- Course times: Weekly, Wednesday 11.10 - 13.00
  - 2.13 - Geography (Old Infirmary Building)
- Website:
  https://opencourse.inf.ed.ac.uk/bdl

  http://www.drps.ed.ac.uk/25-26/dpt/cxinfr11144.htm

- Assessment
  - Coursework requires smart contract programming (30%)
    - To be released October 8th, 2025. Due date: 23:59 Tuesday 11/11/2025.
  - Multiple choice test (70%)

Office hours

- We use Piazza as a forum for questions and answers
- https://piazza.com/ed.ac.uk/
- You **must** sign up to be able to ask questions and read the answers!
- Feel free to answer the questions by your fellow students if you know the answer

Contact

- Aggelos Kiayias
  - Instructor
  - Professor, Chair in Cyber Security and Privacy
  - E-mail: Aggelos.kiayias@ed.ac.uk
  - Office: IF 4.20
- Damiano Abram
  - Instructor
  - Lecturer in Cyber Security and Privacy
  - E-mail: damiano.abram@ed.ac.uk
  - Office: IF 5.25
- Christina Ovezik &
  - Teaching Assistants
  - PhD students, Informatics
  - E-mail: christina.ovezik@ed.ac.uk, Jingxin Qiao, j.qiao-3@sms.ed.ac.uk
    - Preferred contact via piazza.com

Tentative Schedule

Lecture 01 (17.09.2025) Introduction to blockchains and distributed ledgers, hashes, signatures
Lecture 02 (24.09.2025) The blockchain network and related data structures
Lecture 03 (01.10.2025) The blockchain as a platform.
Lecture 04 (08.10.2025) Pitfalls and security vulnerabilities in smart contracts. **Course Project**.
Lecture 05 (15.10.2025) The consensus problem.
Lecture 06 (22.10.2025) Byzantine fault tolerance. Permissionless vs. Permissioned Ledgers.
Lecture 07 (29.10.2025) Distributed ledger economics and incentives.
Lecture 08 (05.11.2025) Scalability. Anonymity and Privacy. Zero-Knowledge Proofs.
Lecture 09 (12.11.2025) DeFi. Secure Multiparty Computation.
Lecture 10 (19.11.2025) Post Quantum Security. Legal aspects. Applications.
Summary & Overview (26.11.2025) Summary and Overview. Student Questions.

Bibliography

- We will study from the class notes and slides. Also\ papers, such as
  - Bitcoin: A Peer-to-Peer Electronic Cash System, Satoshi Nakamoto
  - Ethereum Whitepaper, Vitalik Buterin
  - The Bitcoin Backbone Protocol: Analysis and Applications, Juan Garay, Aggelos Kiayias, Nikos Leonardos
  - The Advent of Resource Based Systems. Aggelos Kiayias.
  - More at: https://github.com/jianyu-niu/blockchain_conference_paper
- A relevant overview book (with freely available preprint, a bit dated) that you may find interesting (it is **not** necessary for the course)
  - "Bitcoin and Cryptocurrency Technologies", Princeton
    - Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller, Steven Goldfeder