

Blockchains & Distributed Ledgers

Lecture 00 - Course Administrativia

Aggelos Kiayias

Administrivia

- Course times: Weekly, Wednesday 11.10 - 13.00
 - Lecture Theatre C - 40 George Square Lecture Theatres

- Website:

<https://opencourse.inf.ed.ac.uk/bdl>

<http://www.drps.ed.ac.uk/24-25/dpt/cxinfr11144.htm>

- Assessment
 - Coursework requires smart contract programming (30%)
 - 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: akiayias@inf.ed.ac.uk
 - Office: IF 5.16
- Christina Ovezik & Yu Shen
 - Teaching Assistants
 - PhD students, Informatics
 - E-mail: christina.ovezik@ed.ac.uk, yu.shen@ed.ac.uk
 - Preferred contact via piazza.com

Tentative Schedule

- Lecture 01 (18.09.2024) Introduction to blockchains and distributed ledgers
- Lecture 02 (25.09.2024) The blockchain network and related data structures.
- Lecture 03 (02.10.2024) The blockchain as a platform.
- Lecture 04 (09.10.2024) Pitfalls and security vulnerabilities in smart contracts. **Course Project.**
- Lecture 05 (16.10.2024) The consensus problem.
- Lecture 06 (23.10.2024) Byzantine fault tolerance. Permissionless vs. Permissioned Ledgers.
- Lecture 07 (30.10.2024) Distributed ledger economics and incentives.
- Lecture 08 (06.11.2024) Networking. Anonymity and Privacy in blockchain protocols.
- Lecture 09 (13.11.2024) DeFi. Secure Multiparty Computation.
- Lecture 10 (20.11.2024) Post Quantum Security. Legal aspects. Applications.
- Summary & Overview (27.11.2024) 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
 - [SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies](#)
 - Bonneau J, Miller A, Clark J, Narayanan A, Kroll JA, Felten EW
 - 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