Pre-requisites: Students must have passed Introduction to Cryptography (IT325), or equivalent course
Instructor: Anish Mathuria
Lectures: online, via Google Meet, as per the timetable

Objectives: This course explores the fundamentals of blockchains and cryptocurrencies.

Course topics

Topics covered include basic cryptographic tools, early digital cash (Chaum et al), Bitcoin blockchain, Script language, Bitcoin wallets, applications of Bitcoin scripts, distributed consensus algorithms, proof of work, mining pools, mining attacks, altcoins, virtual mining, cross-chain transactions, Bitcoin exchanges, anonymity and privacy techniques, scaling blockchains, smart contracts, decentralized applications, and Ethereum blockchain.

References


The Princeton text covers some but not all of the lecture material. In addition to the text, we will use selected papers and references available on the web.

Evaluation

- Mid-semester exam: 16%
- End-semester exam: 32%
- Assignments: 32%
- Term paper: 20%

Term Paper

- Teams of 2 or 3 students will pick a topic for their term paper.
- A list of suggested domains and papers is available at the website [https://github.com/decrypto-org/blockchain-papers](https://github.com/decrypto-org/blockchain-papers). This is not an exhaustive list.
- At least 3 papers must be included in the study. A typical term paper would be 4-6 pages long.
- The evaluation for the term paper is split into 5% for the proposal and 15% for the paper itself.