Course program and reading list

Semester 2 Year 2024

School: Efi Arazi School of Computer Science M.Sc.

Blockchains and Cryptocurrencies

Lecturer:

Prof. Tal Moran   talm@runi.ac.il

Teaching Assistant:

Mr. Ziv Huppert   Ziv.Huppert@post.runi.ac.il

Course No.:	Course Type :	Weekly Hours :	Credit:
3626	Elective	3	3

Course Requirements :	Group Code :	Language:
Final Paper	242362601	English

Prerequisites

Prerequisite:

52 - Calculus I
53 - Calculus II
54 - Linear Algebra I
55 - Linear Algebra II
56 - Discrete Mathematics
59 - Data Structures
69 - Logic And Set Theory
417 - Introduction To Computer Science

Course Description

Traditional currency systems rely on a state, bank or other institution to control and guarantee their value. Bitcoin is the first of a new form of digital currency: "crypto-currencies". Using the "magic" of cryptography, crypto-currencies can be entirely decentralized—they work even though no single entity controls them. The technology underlying crypto-currencies—the "blockchain" is rapidly developing area of research, both in theory and in practice.

The subject of this course will be the computer-science behind blockchains and crypto-currencies, with a focus on some of the cryptographic technologies they use.

We will not assume prior cryptographic knowledge (although it will help), but students should be familiar with the basics of probability and linear algebra, and comfortable programming in some high-level language (e.g., most of the programming exercises will be in Python).

📋 Course Goals

The course aims to give students a basic understanding of blockchain technology, the problems it aims to solve, and how it can be used in the context of crypto-currencies.

🅰️ Grading

The course will have both homework exercises and a final project. The homework exercises will consist of both theory and implementation (programming), while the final project (in small groups) will be mostly implementation.

The final grade will consist of the homework; (70%) and the final project (30%).

💬 Reading List

- Princeton Bitcoin book
- Foundations of Distributed Consensus and Blockchains (Elaine Shi)
- Papers that are published on the course website.