IT486: Blockchains and Cryptocurrencies (3-0-0-3)  
Autumn 2022-23

Course Placement
This course is open to the students in the final year of B.Tech (ICT) and M.Tech (ICT) programs.

Pre-requisites: Students must have passed Introduction to Cryptography (IT325), or equivalent course
Instructor: Anish Mathuria
Lectures: see 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: 20%
- End-semester exam: 40%
- Homeworks + pop-quizzes: 25%
- Research paper presentation: 15%

Course Outcomes
Upon completion of the course:
- Students should be able to understand properties of blockchains and their applications
- Students should be able to understand the fundamental principles and algorithms underlying bitcoin
- Students should be able to understand the limitations of cryptocurrencies such as bitcoin

<table>
<thead>
<tr>
<th>P1</th>
<th>P2</th>
<th>P3</th>
<th>P4</th>
<th>P5</th>
<th>P6</th>
<th>P7</th>
<th>P8</th>
<th>P9</th>
<th>P10</th>
<th>P11</th>
<th>P12</th>
</tr>
</thead>
<tbody>
<tr>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>