Course Information

Course Code	9700738
Course Section	1
Course Title	SPECIAL TOPICS: BLOCKCHAIN AND CRYPTOCURRENCIES: SECURITY & PRIVACY
Course Credit	3
Course ECTS	8.0
Course Catalog Description	The aim of this course is to present cryptocurrencies and blockchain technologies along with the underlying cryptographic primitives. Starting with Bircoin, this course will cover fundamental concepts, types of proof of works, consensus mechanisms, how cryptographic primitives are used for integrity, authentication and preserving of privacy.
Prerequisites	No prerequisites
Schedule	Monday , 09:40 - 12:30, S-208

Instructor Information

Name/Title	Assoc.Prof.Dr. OĞUZ YAYLA
Office Address	S220
Email	oguz@metu.edu.tr
Office Phone	
Office Hours	Monday 12:30-13:30

Course Objectives

The objective of this course is to study the mechanics of blockchain technologies along with the underlying cryptographic primitives, and to give a security and privacy point of view.

Course Learning Outcomes

The students will learn:

- the tools used in construction a cryptocurrency its underlying technology blockchain,
- Smart contracts and their implemention,
- Security measures and privacy solutions for blockchains
- Scalability issue of blockhain and its solutions
- Interoperability of blockchain in other areas

Instructional Methods

Lecture, assignments, discussion, group work, project work, peer assesment.

Tentative Weekly Outline

Week	Topic	Relevant Reading	Assignments
1	History, Fiat Currencies, Hash functions, Digital Signatures		
2	Bitcoin mechanics		
3	Bitcoin Wallet, Security, Privacy, Trust, Failures and Attacks		

Week	Topic	Relevant Reading	Assignments
4	Consensus Algorithms, Byzantine Agreement		
5	Etherium and Smart Contracts		
6	Programming in solidity		
7	Blockchain, Distributed Ledger Technologies, Hyperledger, Quorum		
8	Pairing-based Cryptography, zero knowledge proofs, range proofs,		
9	zk-STARK, zk-SNARKs, bulletproof,		
10	Privacy preserving coins, Stablecoins,		
11	Decentralized exchanges and Lending systems		
12	Decentralized exchanges and Lending systems		
13	Scaling the blockchain		
14	Blockchain interoperability, NFTs and governance		
15	The future of blockchains		

Course Textbook(s)

Narayanan, Arvind, Joseph Bonneau, Edward Felten, Andrew Miller, and Steven Goldfeder. *Bitcoin and cryptocurrency technologies: a comprehensive introduction*. Princeton University Press, 2016.

Bashir, Imran. *Mastering Blockchain: A deep dive into distributed ledgers, consensus protocols, smart contracts, DApps, cryptocurrencies, Ethereum, and more*. Packt Publishing Ltd, 2020.

Course Material(s) and Reading(s)

Material(s)

No meterail is needed.

Reading(s)

https://github.com/bitcoinbook/bitcoinbook

https://bitcoin.org/en/developer-reference

https://ethereum.org/en/whitepaper/

http://gavwood.com/paper.pdf

Supplementary Readings / Resources / E-Resources

Readings

https://bitcoin.org/bitcoin.pdf

http://elaineshi.com/docs/blockchain-book.pdf

Assessment of Student Learning

Assessment	Dates or deadlines
Assignments: The homework assignments will be designed to help you learn specific skills covered in class. They will be handed out at the end of each class (bi)weekly, and is due at the beginning of the next class.	*See Weekly Outline*
Research Project: You are expected to study/implement and present a research paper drawn from the recent literatur. Students are to write a report summarizing and criticizing their learining ouputs from the paper. It should be around 8-10 pages. A gorup work is wellcome.	End of the semester

Course Grading

Deliverable	Grade Points
Assignements	60
Final Project	40
Total	100

Course Policies

Class Attendance

Regular class attendance is important to benefit from the course at maximum level.

Class Participation

Active participation in class is strongly encouraged to have an interactive learning during the semester.

Information for Students with Disabilities

Students who experience difficulties due to their disabilities and wish to obtain academic adjustments and/or auxiliary aids must contact ODTU Disability Support Office and/or course instructor and the advisor of students with disabilities at academic departments (for the list: http://engelsiz.metu.edu.tr/en/advisor-students-disabilities) as soon as possible. For detailed information, please visit the website of Disability Support Office: https://engelsiz.metu.edu.tr/en/

Academic Honesty

The METU Honour Code is as follows: *"Every member of METU community adopts the following honour code as one of the core principles of academic life and strives to develop an academic environment where continuous adherence to this code is promoted. The members of the METU community are reliable, responsible and honourable people who embrace only the success and recognition they deserve, and act with integrity in their use, evaluation and presentation of facts, data and documents."*