Course guide
230991 - BKCHAIN - Blockchain

Last modified: 26/05/2023

Unit in charge: Barcelona School of Telecommunications Engineering
Teaching unit: 744 - ENTEL - Department of Network Engineering.

Degree: MASTER'S DEGREE IN TELECOMMUNICATIONS ENGINEERING (Syllabus 2013). (Optional subject).
MASTER'S DEGREE IN ADVANCED TELECOMMUNICATION TECHNOLOGIES (Syllabus 2019). (Optional subject).
MASTER'S DEGREE IN CYBERSECURITY (Syllabus 2020). (Optional subject).

Academic year: 2023 **ECTS Credits:** 5.0 **Languages:** English

LECTURER

Coordinating lecturer: Consultar aquí / See here: https://telecos.upc.edu/ca/estudis/curs-actual/professorat-responsables-coordinadors/responsables-assignatura

Others: Consultar aquí / See here: https://telecos.upc.edu/ca/estudis/curs-actual/professorat-responsables-coordinadors/professorat-assignat-idioma

DEGREE COMPETENCES TO WHICH THE SUBJECT CONTRIBUTES

Specific:
CE15. Ability to integrate Telecommunication Engineering technologies and systems, as a generalist, and in broader and multidisciplinary contexts, such as bioengineering, photovoltaic conversion, nanotechnology and telemedicine.

Transversal:
CT4. EFFECTIVE USE OF INFORMATION RESOURCES: Managing the acquisition, structuring, analysis and display of data and information in the chosen area of specialisation and critically assessing the results obtained.

CT5. FOREIGN LANGUAGE: Achieving a level of spoken and written proficiency in a foreign language, preferably English, that meets the needs of the profession and the labour market.

TEACHING METHODOLOGY

Master classes mixed with practices.

LEARNING OBJECTIVES OF THE SUBJECT

Understand the concepts and design goals of digital cyrptocurrencies.
Understand the different types and implementations of consensus algorithms.
Understand the operation of blockchain systems in their main variants.
Understand smart contracts.

STUDY LOAD

Type	Hours	Percentage
Hours large group	26,0	20.80
Hours small group	13,0	10.40
Self study	86,0	68.80

Total learning time: 125 h

CONTENTS

Centralized digital currencies

Description:
Centralized digital currencies

Specific objectives:
The problem of double spending.
Blind signatures.
Anonymous payment systems with centralized ledger.

Full-or-part-time: 3h
Theory classes: 3h

Decentralization

Description:
Decentralization

Specific objectives:
Introduction and decentralization motivation.
State replication versus state machine replication.
Consensus protocols.
Fail-stop and Byzantine systems.
Synchronous and asynchronous networks.
The Reliable, Replicated, Redundant, And Fault-Tolerant (RAFT) algorithm.
The Practical Byzantine Fault Tolerant (PBFT) algorithm.

Full-or-part-time: 5h
Theory classes: 5h

Blockchain and Proof of Work (PoW)

Description:
Blockchain and Proof of Work (PoW)

Specific objectives:
Sybil attacks and consensus with Proof of Work (PoW).
The blockchain.
Verifying transactions.
Attacks to PoW.
Mining pools.
Mining with Application-Specific Integrated Circuits (ASICs).
Governance and forks.

Full-or-part-time: 6h
Theory classes: 6h

Proof of Stake (PoS)

Description:
Proof of Stake (PoS)

Specific objectives:
Staking principles.
Types of PoS networks.
Stake distribution.
Chain-based PoS and Byzantine-based PoS.
Block timing.

Full-or-part-time: 3h
Theory classes: 3h

Coin-based Ledgers

Description:
Coin-based Ledgers

Specific objectives:
Unspent Transaction Outputs (UTXOs).
Introduction to Bitcoin.
Bitcoin’s script.
Wallets and Hierarchical Deterministic (HD) wallets.

Full-or-part-time: 6h
Theory classes: 6h

Balance-based ledgers

Description:
Balance-based ledgers

Specific objectives:
Basic principles of balance-based ledgers.
Attacks and countermeasures to balance-based ledgers.
Introduction to Ethereum.
Simulation of an Ethereum blockchain.

Full-or-part-time: 6h
Theory classes: 6h

Smart contracts

Description:
Smart contracts

Specific objectives:
Introduction to programming smart contracts.
Basic game theory applied to smart contracts.
Study of use cases: remote purchase, tokenization, Initial Coin Offerings (ICOs).

Full-or-part-time: 6h
Theory classes: 6h

GRADING SYSTEM

35% partial test and questions.
25% Laboratory
40% Final work

BIBLIOGRAPHY

Basic:
- Narayanan, A.; Bonneau, J.; Felten, E.; Miller, A.; Goldfeder, S. Bitcoin and cryptocurrency technologies: a comprehensive introduction. Princeton: Princeton University Press, 2016. ISBN 9780691171692.
- Antonopoulos, Andreas M. Mastering bitcoin [on line]. 2nd. ed. Beijing: O'reilly Media, 2017 [Consultation: 02/06/2022]. Available on: https://ebookcentral.proquest.com/lib/upcatalunya-ebooks/detail.action?docID=4875878. ISBN 9781491954362.
- Rosenbaum, Kalle. Grokking bitcoin [on line]. Shelter Island, New York: Manning Publications, 2019 [Consultation: 02/06/2022]. Available on: https://ebookcentral.proquest.com/lib/upcatalunya-ebooks/detail.action?docID=6642506. ISBN 9781638355977.
- Solorio, Kevin; Kanna, Randall; Hoover, David H. Hands-on smart contract development with solidity and ethereum: from fundamentals to deployment [on line]. Sebastopol, CA: O'Reilly Media, 2020 [Consultation: 02/06/2022]. Available on: https://ebookcentral.proquest.com/lib/upcatalunya-ebooks/detail.action?docID=5984595. ISBN 9781492045236.