



Course guide

200251 - DEB - Data Engineering and Blockchain

Last modified: 21/06/2023

Unit in charge: School of Mathematics and Statistics
Teaching unit: 744 - ENTEL - Department of Network Engineering.
Degree: BACHELOR'S DEGREE IN MATHEMATICS (Syllabus 2009). (Optional subject).
Academic year: 2023 **ECTS Credits:** 3.0 **Languages:** English

LECTURER

Coordinating lecturer: JOSE LUIS MUÑOZ TAPIA
Others: Primer quadrimestre:
JOSE LUIS MUÑOZ TAPIA - M-A

PRIOR SKILLS

Basic programming skills.

REQUIREMENTS

There are no pre-requisites.

DEGREE COMPETENCES TO WHICH THE SUBJECT CONTRIBUTES

Specific:

GM-CE1. CE-1. Propose, analyze, validate and interpret simple models of real situations, using the mathematical tools most appropriate to the goals to be achieved.

Generical:

GM-CB4. CB-4. Have the ability to communicate their conclusions, and the knowledge and rationale underpinning these to specialist and non-specialist audiences clearly and unambiguously.

Transversal:

06 URI. EFFECTIVE USE OF INFORMATION RESOURCES. Managing the acquisition, structure, analysis and display of information from the own field of specialization. Taking a critical stance with regard to the results obtained.

TEACHING METHODOLOGY

Master classes mixed with practices.

LEARNING OBJECTIVES OF THE SUBJECT



STUDY LOAD

Type	Hours	Percentage
Hours small group	15,0	20.00
Hours large group	15,0	20.00
Self study	45,0	60.00

Total learning time: 75 h

CONTENTS

Introduction to cryptography

Description:

Introduction to basic cryptography

Specific objectives:

Introduction to cryptographic algorithms
Symmetric cryptography
Asymmetric cryptography
Hash functions

Full-or-part-time: 5h

Theory classes: 1h
Practical classes: 1h
Self study : 3h

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: 5h

Theory classes: 1h
Practical classes: 1h
Self study : 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: 12h 30m

Theory classes: 2h 30m
Practical classes: 2h 30m
Self study : 7h 30m

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: 12h 30m

Theory classes: 2h 30m
Practical classes: 2h 30m
Self study : 7h 30m

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: 12h 30m

Theory classes: 2h 30m
Practical classes: 2h 30m
Self study : 7h 30m



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: 12h 30m

Theory classes: 2h 30m
Practical classes: 2h 30m
Self study : 7h 30m

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: 15h

Theory classes: 3h
Practical classes: 3h
Self study : 9h

GRADING SYSTEM

35% partial test and questions.

35% Laboratory.

30% Final work (this is a work that will be delivered as a small research paper and that will be presented by students in the class).

BIBLIOGRAPHY

Basic:

- Antonopoulos, Andreas M. Mastering Bitcoin : programming the open blockchain [on line]. 2nd edition. Beijing: O'Reilly Media, 2017 [Consultation : 27/06/2023]. Available on : <https://ebookcentral-proquest-com.recursos.biblioteca.upc.edu/lib/upcatalunya-ebooks/detail.action?pq-origsite=primo&docID=4875878>. ISBN 9781491954362.
- Rosenbaum, Kalle. Grokking bitcoin [on line]. Manning, 2019 [Consultation: 27/06/2023]. Available on: <https://ebookcentral-proquest-com.recursos.biblioteca.upc.edu/lib/upcatalunya-ebooks/detail.action?pq-origsite=primo&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]. O'Reilly Media, 2020 [Consultation: 27/06/2023]. Available on: <https://ebookcentral-proquest-com.recursos.biblioteca.upc.edu/lib/upcatalunya-ebooks/detail.action?pq-origsite=primo&docID=5984595>. ISBN 9781492045236.
- Narayanan, Arvind; Bonneau, Joseph; Felten, Edward. Bitcoin and cryptocurrency technologies : a comprehensive introduction. Princeton: Princeton University Press, 2016. ISBN 9780691171692.