Course guides
230991 - BKCHAIN - Blockchain

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: 2021  ECTS Credits: 5.0  Languages: English

LECTURER

Coordinating lecturer: Muñoz Tapia, Jose Luis
Others: Muñoz Tapia, Jose Luis

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 cryptocurrencies.
Understand the different types and implementations of consensus algorithms.
Understand the operation of blockchain systems in their main variants.
Understand smart contracts.

STUDY LOAD

<table>
<thead>
<tr>
<th>Type</th>
<th>Hours</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hours small group</td>
<td>13,0</td>
<td>10.40</td>
</tr>
<tr>
<td>Self study</td>
<td>86,0</td>
<td>68.80</td>
</tr>
<tr>
<td>Hours large group</td>
<td>26,0</td>
<td>20.80</td>
</tr>
</tbody>
</table>

Total learning time: 125 h
## CONTENTS

<table>
<thead>
<tr>
<th>Topic</th>
<th>Description</th>
<th>Specific objectives</th>
<th>Full-or-part-time:</th>
<th>Theory classes:</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Centralized digital currencies</strong></td>
<td>Centralized digital currencies</td>
<td>The problem of double spending.</td>
<td>3h</td>
<td>3h</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Blind signatures.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Anonymous payment systems with centralized ledger.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Decentralization</strong></td>
<td>Decentralization</td>
<td>Introduction and decentralization motivation.</td>
<td>5h</td>
<td>5h</td>
</tr>
<tr>
<td></td>
<td></td>
<td>State replication versus state machine replication.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Consensus protocols.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Fail-stop and Byzantine systems.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Synchronous and asynchronous networks.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>The Reliable, Replicated, Redundant, And Fault-Tolerant (RAFT) algorithm.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>The Practical Byzantine Fault Tolerant (PBFT) algorithm.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Blockchain and Proof of Work (PoW)</strong></td>
<td>Blockchain and Proof of Work (PoW)</td>
<td>Sybil attacks and consensus with Proof of Work (PoW).</td>
<td>6h</td>
<td>6h</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The blockchain.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Verifying transactions.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Attacks to PoW.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Mining pools.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Mining with Application-Specific Integrated Circuits (ASICs).</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Governance and forks.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
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: