BlockChain and Security Technologies

Academic Year: (2020 / 2021) **Review date: 10-07-2020**

Department assigned to the subject: Computer Science and Engineering Department

Coordinating teacher: FUENTES GARCIA ROMERO DE TEJADA, JOSE MARIA

Type: Electives ECTS Credits : 3.0

Year : 1 Semester : 2

REQUIREMENTS (SUBJECTS THAT ARE ASSUMED TO BE KNOWN)

None

OBJECTIVES

Learning outcomes
- Understand the use of IT system in financial markets
- Understand the main technologies in finances
- Analyse IT infrastructures in financial markets
- Understand the main use cases
- Understand the infrastructure requirements to develop IT systems for finance management

DESCRIPTION OF CONTENTS: PROGRAMME

1.- IT Security introduction
- 1.1. Definitions
- 1.2. Security services
- 1.3. Security mechanisms
- 1.4. Vulnerabilities and threats. Current situation

2.- Cryptography notions
- 2.1. Entropy and randomness
- 2.2. Attacks. Complexity

3.- Security mechanisms for financial data
- 3.1. Data encryption
- 3.2. Authentication
- 3.3. Hash functions
- 3.4. Digital signatures

4.- Blockchain fundamentals and its applications
- 4.1. Blockchain. Basic concepts
- 4.2. Consensus strategies
- 4.3. Smart contracts
- 4.4. Blockchain applications

5.- Cryptocurrencies
- 5.1. Bitcoin
- 5.2. Ethereum
- 5.3. Monero
- 5.4. Other altcoins

6.- Legal framework
- 6.1. GDPR
- 6.2. eIDAS
- 6.3. NIS Directive
- 6.4. Spanish National Security Scheme

LEARNING ACTIVITIES AND METHODOLOGY

Learning activities

AF1 Theoretical sessions
AF2 e-learning activities
AF3 Theoretical and practical assignments
AF4 Lab assignments
AF5 Tutorials
AF6 Work in groups
AF7 Individual work by the student

Methodology

MD1 Lectures in which the main concepts are developed and the bibliography is pointed out.
MD2 Reading of materials provided by the lecturer to support the notions addressed in the subject
MD3 Practical case resolution, either individually or in groups
MD5 Development of assignments and reports either individually or in groups
MD6 e-learning-related activities

Tutorials will be scheduled in two time frames per week. Their schedule will be published through Aula Global. Tutorials will be either physical or through online means. They will have to be requested sufficiently in advance by e-mail. Students may also request other schedules, upon availability of the lecturer.

ASSESSMENT SYSTEM

SE1 Active participation in sessions (10%)
SE2 Assignment(s) performed individually or in groups, either physically or online (60%)
SE3 Final exam (30%)

1. Ordinary sitting
Final exam
- It represents 30% of the final mark
- Theoretical / Practical
- Compulsory and individual

Theoretical and Practical assignments.
- It represents 60% of the final mark
- Compulsory
- Individual or in groups, it will be announced at the beginning of the subject

In order to pass the subject, the following two conditions apply:
- Minimum grade constraint in the exam of 4.0 marks
- All assignments must be handed in. Otherwise, non-continuous assessment applies.

2. Extraordinary sitting
In the extraordinary sitting, the following rules apply:

a. If the student followed the continuous assessment method, the exam will have the same relative weight as in the ordinary sitting. The mark of the continuous evaluation is kept.
b. Otherwise, students will have an exam counting for 100% of the final mark. This exam will contain additional questions related to the assignments. Assignments cannot be delivered in this sitting, unless explicitly stated at the beginning of the subject.

% end-of-term-examination:	30
% of continuous assessment (assigments, laboratory, practicals…):	70

BASIC BIBLIOGRAPHY

- Anderson, Ross Security Engineering: A guide to Building Dependable Distributed Sistems (2nd edition), Wiley, 2008
- Antonopoulos, Andreas Mastering Bitcoin, O'Reilly, 2015
- Antonopoulos, Andreas; Wood, Gavin Mastering Ethereum, O'Reilly, 2018
- Pfleeger, Charles et al Security in Computing (4th edition), Prentice Hall, 2007
- Stallings, William Cryptography and Network Security: Principles and Practice, Prentice Hall, 2013

ADDITIONAL BIBLIOGRAPHY

- Antonopoulos, Andreas Mastering Bitcoin, O' Reilly, 2015

- Antonopoulos, Andreas Mastering Ethereum: Building Smart Contracts and Dapps, O' Reilly, 2018

- Bishop, Matt Computer Security: Art & Science., Addison-Wesley, 2015

BASIC ELECTRONIC RESOURCES

- McGubbin, Gregory . Solidity for Beginners. Smart contract development crash course: https://www.dappuniversity.com/articles/solidity-tutorial