Universitat Autònoma de Barcelona

2022/2023

Blockchain Technology and Cryptocurrency

Code: 105072
ECTS Credits: 6

Degree	Type	Year	Semester
2502441 Computer Engineering	OT	4	1

Contact

Name: Jordi Herrera Joancomarti
Email: jordi.herrera@uab.cat

Use of Languages

Principal working language: catalan (cat)
Some groups entirely in English: No
Some groups entirely in Catalan: Yes
Some groups entirely in Spanish: No

Teachers

Cristina Perez Sola

Prerequisites

To take this subject it is necessary to have passed the subjects of Information and Security (IS) and Fundamentals of Information Technology (FTI), which introduces different important concepts to be consolidated to take the subject of TB. Specifically:

- FTI consolidates the knowledge of cryptography that students have acquired in the subject of IS.
- ElGamal's signature algorithm, which is studied at FTI, is the basis of the ECDSA algorithm used in most cryptocurrencies and which is covered in the TBC subject.
- The FTI explains some of the attacks on the poor implementation of digital signature algorithms that can lead to cryptocurrency theft, topics that are covered in the TBC subject.
- FTI explains in detail the operation and properties of hash functions, which are crucial in the implementation and security of blockchain technology.
- The latest topic of FTI is an introduction to blockchain technology and cryptocurrencies. A tasting that serves to give an initial basis with which to work later in the subject TBC.

Objectives and Contextualisation

The objectives of this subject are:

- Understand the theoretical concepts of blockchain technology
- Understand how cryptocurrencies work.
- Understand how Bitcoin works, from a technical point of view.
- Understand the concept of smart contract.
- Understand the diference between an UTXO-based blockchain and an account-based blockchain
- Know some of the scalability mechanisms of blockchain technology.

Competences

- Acquire personal work habits.
- Acquire thinking habits.
- Capacity to design, develop, evaluate and ensure the accessibility, ergonomics, usability and security of computer systems, services and applications, as well as of the information that they manage.
- Capacity to design, develop, select and evaluate computer applications and systems, ensuring reliability, security and quality, in accordance with ethical principles, and applicable standards and legislation.
- Have the capacity to conceive, draft, organise, plan, develop and sign projects in the field of computer engineering for the conception, development and exploitation of computer systems, services and applications.
- Have the capacity to select, deploy, integrate and manage information systems that satisfy the needs of an organisation, identifying the cost and quality criteria.

Learning Outcomes

1. Design computer solutions that integrate accessibility and security needs in a distributed system.
2. Design, develop, select and evaluate applications, ensuring their reliability and security.
3. Develop a capacity for analysis, synthesis and prospection.
4. Identify the main attacks that a computer system can receive, as well as the possible protection and detection methods and the application of security policies to avoid damage to the system or minimise the repercussions.
5. Incorporate distributed information treatment systems in an organisation in order to increase operative capacity.
6. Work independently.

Content

Subject contents:

1. Basic concepts of blockchain technology
2. Cryptography basic for blockchain technology
3. Bitcoin
4. Second layer protocols: Lightning Network
5. Ethereum
6. Other blockchains

Methodology

The subject is structured in two-hour sessions with a very dynamic approach where students will be asked to actively participate. The typology of sessions will include more theoretical content and more practical content.

The sessions of more theoretical content will be based on material that the teacher will previously make available to students through the virtual campus. Based on this material, two different types of sessions will be structured. On the one hand, question and answer sessions where students will formulate the doubts that have arisen from the previous work on the material provided. In these sessions, the teacher will also challenge the students to highlight the most relevant aspects of the material being worked on. On the other hand, there will be sessions where students, in groups of two, will present a more detailed study of some of the topics covered in the course.

The most practical content sessions will include both solving questions as exercises and performing more technical tasks where the use of specific tools of the subject will be combined (wallets, blockchain browsers, smart contract compilers , etc.) with the development of specific functions using the Python programming language.

Transversal competences. In this subject the following transversal competences of the Degree in Computer Engineering will be worked and evaluated:

- T01.02 - Develop the capacity of analysis, synthesis and prospective: this competence will work of more intense form in the most theoretical sessions where the students will have to show the comprehension of the contents proposed through the questions that the professor will propose them during the theory sessions. This competence will also be worked on in the different works that the students will present throughout the course.
- T02.01 Work autonomously: this focuses on those individual activities, such as carrying out the practical work that students will do throughout the course.

Annotation: Within the schedule set by the centre or degree programme, 15 minutes of one class will be reserved for students to evaluate their lecturers and their courses or modules through questionnaires.

Activities

Title	Hours	ECTS	Learning Outcomes
Type: Directed			
Practical Lab	25	1	1, 2, 5, 6
Teorethical Lecture	25	1	3, 4, 5
Type: Supervised			
Help desk	10	0.4	3, 1, 2, 4, 5
Type: Autonomous			
Practical lab workhome	25	1	3, 1, 2, 6
Theoretical lecture study	37.5	1.5	3, 4, 5, 6

Assessment

The evaluation model of this subject will be entirely of continuous evaluation. Given the dynamism of the same and the involvement that is required of students in all class sessions (both more theoretical and more practical) the teacher will have multiple elements to assess students. Active participation in the lectures, asking questions to the teacher and answering questions from other students or the teacher's questions, will account for 20% of the grade of the subject. It is for this reason that class attendance in this subject is mandatory.

Beyond the evaluation based on the contributions in the classes, the students will also have to deliver different more practical works that will be proposed throughout the course in the virtual campus of the UAB, deliveries that will complement the evidences of evaluation of the student. These more practical activities will account for 50% of the grade for the subject.

On the other hand, the presentation of the subject that the students will do in the theoretical sessions of the subject will also form part of the evidences of evaluation and will suppose 30% of the grade of the subject.

To pass the subject it will be necessary to have passed each one of the evaluable activities understanding that the evaluable activities are: participation in class, practical works and presentation. Each of the practical works must be passed separately.

In case of not passing any of the practical works they will be able to recover returning them to present,

although in this case the maximum note of the recovered work that will obtain will be a 5.

In case of not passing the presentation work, it will be necessary to recover it presenting an extended version of the same work that will be presented orally to the professor of the subject.

In case of not passing the evaluation of the participation in class,this will not beable to recover.

No validation of any of the assessable activities for repeat students is contemplated.

Without prejudice to other disciplinary measures deemed appropriate, and in accordance with current academic regulations, irregularities committed by a student that may lead to a variation in the grade will be graded with a zero (0). Assessment activities qualified in this way and by this procedure will not be recoverable. If it is necessary to pass any of these assessment activities to pass the course, this course will be suspended directly, without the opportunity to retake it in the same course. These irregularities include, but are not limited to:

- the total or partial copy of a practice, report, or any other assessment activity;
- let copy;
- present group work not done entirely by group members;
- present as own materials prepared by a third party, even if they are translations or adaptations, and in general works with non-original and exclusive elements of the student;

In short: copying, copying or plagiarizing (or attempting to) in any of the assessment activities is equivalent to a SUSPENSION, not compensable and without validations of parts of the subject in later courses.

Students who achieve the minimum number of points to pass the course but have not reached the minimum grade in any of the assessment activities, will be assessed with a final grade of 4.5. In the event that the subject has not been passed due to the grade of zero of an activity due to copying, the final grade of the subject will be a 3, which will not compensate for this subject.

Finally, those students who do not submit any ofthe proposed practical activities will obtain the qualification of "Non-Evaluable". Participation in any of these evaluation activities will mean receivinga different rating of "Not Evaluable".

No assessment activity will be carried out on any student at a different time than the established one unless there is a justified cause, the activity has been notified in advance and the teacher has given his / her consent. In any other case, if a student has not attended an activity, it cannot be recovered.

With regard to honors enrollments, these may be awarded to those students who have passed the subject with a final grade equal to or greater than 9. Given that the number of honors enrollments may not exceed 5% of students enrolled, will be awarded to students with the highest grades. In the event of a tie, students may be required to take an oral test to break the tie.

Assessment Activities

Title	Weighting	Hours	ECTS	Learning Outcomes
Oral presentation	30	1	0.04	3, 1, 2, 4, 5, 6
Participación en clase	20	14	0.56	4
Practical activities	50	12.5	0.5	3, 1, 2, 4, 5, 6

Bibliography

- Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller, Steven Goldfeder. Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction. Princeton University Press (2016). ISBN: 978-0691171692
- Andreas M. Antonopoulos, Mastering Bitcoin: Programming the Open Blockchain. O'Reilly Media; 2nd Edition. (2017) ISBN: 978-1491954386
- Andreas M. Antonopoulos y Gavin Wood, Mastering Ethereum: Building Smart Contracts and DApps. O'Reilly Media. (2018) ISBN: 978-1491971949
- Kalle Rosenbaum, Grokking Bitcoin. Manning Publications (2019) ISBN 9781617294648
- Roger Wattenhofer. Blockchain Science: Distributed Ledger Technology.Inverted Forest Publishing; 3rd Edition (2019) ISBN: 978-1793471734
- Andreas Antonopoulos, Olaoluwa Osuntokun, René Pickhardt. Mastering the Lightning Network: A Second Layer Blockchain Protocol for Instant Bitcoin Payments. O'Reilly Media; 1st edition (January 4, 2022) ISBN: 978-1492054863

Software

The most practical content sessions will include both solving questions as exercises and performing more technical tasks where the use of specific tools of the subject will be combined (wallets, blockchain browsers, smart contract compilers , etc.) with the development of specific functions using the Python programming language.