UAB
Universitat Autònoma de Barcelona

Blockchain Technology and Cryptocurrency

Code: 105072
ECTS Credits: 6

2024/2025

Degree	Type	Year
2502441 Computer Engineering	OT	4

Contact

Name: Jordi Herrera Joancomarti

Email: jordi.herrera@uab.cat

Teachers

Cristina Perez Sola

Teaching groups languages

You can view this information at the end of this document.

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

Activities and Methodology

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

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.

Assessment

Continous 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

The evaluation model for this subject will be entirely based on continuous assessment. Given its dynamic nature and the involvement required from students in all class sessions (both theoretical and practical), the professor will have multiple elements to evaluate the students. Active participation in class, by asking questions and responding to questions from other students or the professor, will constitute 20% of the course grade. Therefore, attendance in this subject's classes is mandatory.

Beyond assessment based on class contributions, students will also have to submit various practical assignments that will be proposed throughout the course on the UAB virtual campus. These assignments will complement the evaluation evidence of the student and will account for 50% of the course grade.

Additionally, the presentation of a topic that students will make in the theoretical sessions of the course will also form part of the evaluation evidence and will constitute 30% of the course grade.

To pass the course, each evaluable activity must be passed, meaning that the evaluable activities are: class participation, practical assignments, and the presentation of work.

Each practical assignment must be passed separately. If a practical assignment is not passed, it can only be retaken if the obtained grade was higher than 3.5, and it must be resubmitted. In the case of resubmission, the maximum grade for the retaken assignment will be a 5. If a practical assignment has a grade lower than 3.5, it cannot be retaken.

If the presentation work is not passed, it cannot be retaken.

If the class participation evaluation is not passed, it cannot be retaken.

If, at the end of the course, any of the evaluable activities (class participation, practical assignments, or presentation work) are not passed, there will still be the possibility to pass the course through a final oral exam. This final exam will account for 80% of the grade. The 20% participation grade will remain as obtained during the course.

No form of validation of any evaluable activities is considered for repeating students.

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

- Total or partial copying of a practical assignment, report, or any other evaluation activity;
- Allowing copying;
- Submitting a group work not entirely done by the group members (applied to all members, not just those who didn't work);
- Unauthorized use of AI (e.g., Copilot, ChatGPT, or equivalents) to solve exercises, practical assignments, and/or any other evaluable activity;
- Submitting as one's own materials created by a third party, even if they are translations or adaptations, and in general, works with non-original elements exclusive to the student;

In summary: copying, allowing copying, or plagiarizing (or attempting to) in any evaluable activity results in a FAIL, non-compensable, and without validation of parts of the course in future terms.

Students who achieve the minimum number of points to pass the course but have not reached the minimum grade in any of the evaluable activities will be graded with a final mark of 4.5. If the course is not passed due to a grade of zero in an activity due to copying, the final grade for the course will be a 3, which does not allow compensation for this course.

Finally, students who do not submit any of the practical assignments proposed will receive a grade of "Not Evaluated." Participation in any of these evaluation activities will result in a grade different from "Not Evaluated."

No evaluation activity will be conducted for any student at a time different from the established schedule unless there is a justified reason, it has been notified prior to the activity, and the professor has given consent. In any other case, if a student does not attend an activity, it cannot be retaken.

Regarding honors distinctions, these may be granted to students who have passed the course with a final grade equal to or higher than 9. Since the number of honors distinctions cannot exceed 5% of the enrolled students, they will be awarded to the students with the highest grades. In case of a tie, students may be required to take an oral exam to break the tie.

This course does not provide for a single assessment system.

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; 3d Edition. (2023) ISBN: 978-1098150099
- Andreas M. Antonopoulos y Gavin Wood, Mastering Ethereum: Building Smart Contracts and DApps. O'Reilly Media. (2018) ISBN: 978-1491971949
- C. Pérez Solà i J. Herrera Joancomartí, La criptografia que et cal saber. (2023) Disponible on-line: https://criptografia.cat/
- 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.

Language list

Name	Group	Language	Semester	Turn
(PAUL) Classroom practices	450	Catalan	first semester	morning-mixed