BLOCKCHAIN, CRYPTOCURRENCIES & FINTECH

Grado en Computación e Inteligencia Artificial / Bachelor in Computer Science and Artificial Intelligence BCSAI SEP-2025 BCF-CSAI.4.M.A

Area Computer Science

Number of sessions: 15

Academic year: 25-26

Degree course: FOURTH

Number of credits: 3.0

Semester: 2º

Category: COMPULSORY

Language: English

Professor: **MILAN GROSHEV**

E-mail: mgroshev@faculty.ie.edu

Dr. Milan Groshev is a robotics researcher who combines robotic systems with next-generation information and communication technologies. His work explores how concepts like virtualization, semantic orchestration, edge computing, sensing, and blockchain can help create collaborative and cost-effective robotic systems. Before joining IE University, Milan led the Innovation Hub at Laude Technology. There, he managed applied R&D projects alongside universities, research centers, and industry partners. His work focused on solving technological challenges in Open Radio Access Networks using artificial machine learning, and optimization algorithms. He was also involved in leading European and national research projects and securing funding for innovation initiatives. Milan completed his PhD in the NETCOM Research Group at Universidad Carlos III de Madrid (UC3M), where he later continued as a postdoctoral researcher. His work during this period focused on networked robotic systems and emerging communication protocols. In 2022, Milan received the Best Demo Award at ACM SIGCOMM for a forecast-based recovery mechanism for real-time remote control of robotic manipulators. His research has been published in journals and magazines such as IEEE Transactions on Network and Service Management, ACM Transactions on Networking, IEEE Communications Magazine, and IEEE Network. At IE, Milan leads the ROBOPRENEUR research line, where he studies new ways for robots to engage with humans not just as tools but as economic peers capable of acting independently in social and economic environments.

Office Hours

Office hours will be on request. Please contact at:

Office hours will be on request. Please contact at: mgroshev@faculty.ie.edu

SUBJECT DESCRIPTION

Bitcoin and other cryptographic currencies have gained attention over the years as the systems continue to evolve. This course looks at the design of the underlying mechanism behind Bitcoin and other cryptocurrencies: blockchain. In this course, we will focus on how blockchains function in practice, focusing on cryptography, programming, and network architecture. Future developments in smart contracts and privacy will be covered as well. Programming assignments in the course will give way to practical experiences interacting with these currencies.

LEARNING OBJECTIVES

By the end of this course, students should be able to:

- Understand the basic concepts behind a modern blockchain-based systems
- Program and simulate custom programs (i.e., smart contracts) for currency and consensus formalizationGet acquainted with the latest blockchain-based research and have the ability to analyze research papers in the crypto ecosystem

TEACHING METHODOLOGY

IE University teaching method is defined by its collaborative, active, and applied nature. Students actively participate in the whole process to build their knowledge and sharpen their skills. Professor's main role is to lead and guide students to achieve the learning objectives of the course. This is done by engaging in a diverse range of teaching techniques and different types of learning activities such as the following:

Learning Activity	Weighting	Estimated time a student should dedicate to prepare for and participate in
Lectures	20.0 %	15.0 hours
Discussions	13.3 %	10.0 hours
Exercises in class, Asynchronous sessions, Field Work	33.3 %	25.0 hours
Group work	13.3 %	10.0 hours
Individual studying	20.0 %	15.0 hours
TOTAL	100.0 %	75.0 hours

AI POLICY

Generative artificial intelligence (GenAI) tools may be used in this course for assignment and code writing with appropriate acknowledgement. GenAI may not be used for presentations, group submissions, and exams. If a student is found to have used AI-generated content inappropriately, it will be considered academic misconduct, and the student might fail the respective assignment or the course.

PROGRAM

SESSION 1 (LIVE IN-PERSON)

In this lecture we will provide a brief introduction to the concept of a cryptographic ledger (a.k.a. a blockchain); a tamperproof sequence of data that can be read and augmented by users. During the lecture, the instructor will introduce his background in the blockchain field and will present the latest research advances in the fields of blockchain and cryptocurrencies.

SESSION 2 (LIVE IN-PERSON)

Signatures, hashing and hash chains. Hashing and digital signatures are important terms that bring desired security level in blockchain to keep information private. During the lecture, students will get familiar with concepts such as: public key cryptography, elliptic curve digital signature algorithm, or different hashing algorithms. This lecture will be complemented by a programming exercise students will have to finalize before next session of the course.

SESSION 3 (LIVE IN-PERSON)

Proof of Work vs Proof of Stake. Proof of work (Bitcoin) is a consensus mechanism used by cryptocurrencies to verify the accuracy of new transactions that are added to a blockchain. Despite its security, this technique represents serious challenges to the scalability and performance of future blockchain-based systems such as Bitcoin. In contrast, Proof of Stake (Ethereum) is a consensus mechanism that is supposed to overcome the limitations of previous solutions. However, new security challenges open up while thi method becomes more popular. In this lecture, students will deep-dive into these blockchain consensus models and will spot their advantages and disadvantages. This lecture will be complemented by a programming exercise students will have to finalize before next session of the course.

SESSION 4 (LIVE IN-PERSON)

Bitcoin Introduction and Core Concepts. This session covers Bitcoin as the first decentralized digital currency and its core building blocks. It will include concepts such as transaction verification by network nodes through cryptography, and the public distributed ledger. In addition this session will cover, the UTXO model, synchronization, and pruning. This lecture will be complemented by a programming exercise for the students.

SESSION 5 (LIVE IN-PERSON)

Bitcoin Advanced Concepts and Programming Exercise. Students will learn about advanced Bitcoin concepts including SPV, wallet types, OP_RETURN, and Catena will be introduced during the lecture. The session concludes with a programming exercise that students must complete before the next class.

SESSION 6 (LIVE IN-PERSON)

Ethereum and Smart Contracts Fundamentals. Introduction to smart contracts as the foundational elements of Ethereum’s application layer, emphasizing the "if this then that" logic executed by blockchain technology. They are computer programs stored on the blockchain that follow "if this then that" logic, and are guaranteed to execute according to the rules defined by its code.

SESSION 7 (LIVE IN-PERSON)

Solidity and Programming Exercise. This session covers Ethereum's programming language Solidity. In this lecture, students will get acquiantied with all the crucial concepts behind Ethereum including its programming language Solidity. This set of lectures will be complemented by a programming exercise students will have to finalize before next lecture of the course.

SESSION 8 (LIVE IN-PERSON)

DAOs: Principles and Mechanisms. This session introduces Decentralized Autonomous Organizations (DAOs), exploring their governance through smart contracts and the interaction between algorithms and individuals without traditional corporate structures.

Dapps and DAOs. A Decentralized Autonomous Organization (DAO) is an organization that is run through rules encoded as smart contract. In DAOs, algorithms and people can cooperate without the need to be incorporated in traditional business entities. In this lecture, students will get acquiantaied with the necessary tools and mechanisms to build a DAO, deploy it a in public blockchain, and interface with it throught a Dapp (Decentralized Application).

SESSION 9 (LIVE IN-PERSON)

Deploying DAOs and Building Dapps. Students will learn how to deploy DAOs on public blockchains and interact with them via Decentralized Applications (Dapps). This session includes a practical programming exercise to be finalized before the next meeting.

SESSION 10 (LIVE IN-PERSON)

Zero Knowledge proofs. In cryptography, a zero-knowledge proof is a method by which one party (the prover) can prove to another party (the verifier) that a given statement is true, while avoiding conveying to the verifier any information beyond the mere fact of the statement's truth. In this lecture, students will get acquiantaied with the necessary tools and mechanisms to create and verify zero-knowledge proofs. This lecture will be complemented by a programming exercise students will have to finalize before next session of the course.

SESSION 11 (LIVE IN-PERSON)

New directions in Web3. Web 3.0 is an idea for a new iteration of the World Wide Web which incorporates concepts such as decentralization, blockchain technologies, and token-based economics. In this lecture, students will deep dive into the web3 ecosystem understanding what differentiaties this new paradigm from previous approaches. This lecture will be complemented by a programming exercise students will have to finalize before next session of the course.

SESSION 12 (LIVE IN-PERSON)

Fintech Guest Lecture I

SESSION 13 (LIVE IN-PERSON)

Fintech Guest Lecture II

SESSION 14 (LIVE IN-PERSON)

Fintech Guest Lecture III

SESSION 15 (LIVE IN-PERSON)

Final research paper presentations

EVALUATION CRITERIA

At the end of sessions 2 to 11, a programming exercise will be provided to the students (due date: beginning of the next session). The idea behind these exercies is to demonstrate the student's proficiency by using blockchain-based tools and programming frameworks. Complementarily, in session 15, a group (~5 students) presentation will be conducted. In this group presentation, students will pick a blockchain research paper (paper candidates will be provided throughout sessions 12 to 14) and conduct a deep scientific analysis. This analysis will include the strengths, weaknesses, opportunities, and threats of the chosen research paper.

criteria	percentage	Learning Objectives	Comments
Group Presentation	40 %		
Class Participation	10 %		
Intermediate exercises	50 %		

RE-SIT / RE-TAKE POLICY

Each student has four chances to pass any given course distributed over two consecutive academic years: ordinary call exams and extraordinary call exams (re-sits) in June/July.

Students who do not comply with the 80% attendance rule during the semester will fail both calls for this Academic Year (ordinary and extraordinary) and have to re-take the course (i.e., re-enroll) in the next Academic Year.

Evaluation criteria:

- Students failing the course in the ordinary call (during the semester) will have to re-sit the exam in June / July (except those not complying with the attendance rule, who will not have that opportunity and must directly re-enroll in the course on the next Academic Year).
- The extraordinary call exams in June / July (re-sits) require your physical presence at the campus you are enrolled in (Segovia or Madrid). There is no possibility to change the date, location or format of any exam, under any circumstances. Dates and location of the June / July re-sit exams will be posted in advance. Please take this into consideration when planning your summer.
- The June/July re-sit exam will consist of a comprehensive exam. Your final grade for the course will depend on the performance in this exam only; continuous evaluation over the semester will not be taken into consideration. Students will have to achieve the minimum passing grade of 5 and can obtain a maximum grade of 8.0 (out of 10.0) – i.e., “notable” in the in the re-sit exam.
- Retakers: Students who failed the subject on a previous Academic Year and are now reenrolled as re-takers in a course will be needed to check the syllabus of the assigned professor, as well as contact the professor individually, regarding the specific evaluation criteria for them as retakers in the course during that semester (ordinary call of that Academic Year). The maximum grade that may be obtained in the retake exam (3rd call) is 10.0.

After ordinary and extraordinary call exams are graded by the professor, you will have a possibility to attend a review session for that exam and course grade. Please be available to attend the session in order to clarify any concerns you might have regarding your exam. Your professor will inform you about the time and place of the review session. Any grade appeals require that the student attended the review session prior to appealing. Students failing more than 18 ECTS credits in the academic year after the June-July re-sits will be asked to leave the Program. Please, make sure to prepare yourself well for the exams in order to pass your failed subjects. In case you decide to skip the opportunity to re-sit for an exam during the June/July extraordinary call, you will need to enroll in that course again for the next Academic Year as a re-taker and pay the corresponding extra cost. As you know, students have a total of four allowed calls to pass a given subject or course, in order to remain in the program.

BIBLIOGRAPHY

Recommended

- Oded Goldreich. (2019). *Providing Sound Foundations for Cryptography: On the work of Shafi Goldwasser and Silvio Micali.* ISBN 9781450372671 (Digital)
- Andreas Antonopoulos, Gavin Wood. (2018). *Mastering Ethereum: Building Smart Contracts and Dapps.* O'Reilly Media. ISBN 978149197194 (Digital)
- Andreas M. Antonopoulos. (2017). *Mastering Bitcoin: Programming the Open Blockchain.* O'Reilly Media. ISBN 978149195438 (Digital)
- Vitalik Buterin, Nathan Schneider. (2022). *Proof of Stake: The Making of Ethereum and the Philosophy of Blockchains.* Seven Stories Press. ISBN 978164421248 (Digital)

BEHAVIOR RULES

Please, check the University's Code of Conduct here. The Program Director may provide further indications.

ATTENDANCE POLICY

Please, check the University's Attendance Policy here. The Program Director may provide further indications.

ETHICAL POLICY

Please, check the University's Ethics Code here. The Program Director may provide further indications.