BLOCKCHAIN, CRYPTOCURRENCIES & FINTECH

Bachelor in Computer Science and Artificial Intelligence
BCSAI SEP-2024 BCF-CSAI.4.M.A

Area Data Science
Number of sessions: 15
Academic year: 24-25
Degree course: FOURTH
Number of credits: 3.0
Semester: 2º
Category: COMPULSORY
Language: English

Professor: **EDUARDO CASTELLÓ FERRER**

E-mail: ecastello@faculty.ie.edu

Prof. Eduardo Castelló Ferrer received the B.Sc. (Hons.) degree in intelligent systems from the University of Portsmouth (U.K.) in 2007, and the M.Eng. and Ph.D. degrees in robotics engineering from Osaka University (Japan) in 2011 and 2016, respectively. Dr. Castelló's experience and interests comprise robotics, cryptography, and complex systems. He was a Marie Curie Fellow at the MIT Media Lab, where he innovated the combination of distributed robotic systems and blockchain technology. In addition to his position as an assistant professor at IE, Dr. Castelló is a research fellow at the MIT Connection Science group where he focuses on implementing new security, behavior, and business models for robotics using novel cryptographic methods.

Office Hours

Office hours will be on request. Please contact at:

ecastello@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 formalization
- Get 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
Individual studying	33.3 %	25.0 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)

Introduction. 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, cryptocurrencies, and fintech. Finally, the course schedule as well as other admin procedures will finalize the lecture.

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.

SESSIONS 4 - 5 (LIVE IN-PERSON)

Bitcoin. Bitcoin was the first decentralized digital currency. Bitcoin transactions are verified by network nodes through cryptography and recorded in a public distributed ledger. In this lecture (2 sessions long), students will get acquiantied with all the crucial concepts behind Bitcoin. Concepts like transactions, UTXO model, synchronization process, pruning, SPV and wallet types, OP_RETURN, Catena will be introduced during the lecture. This set of lectures will be complemented by a programming exercise students will have to finalize before the next lecture of the course.

SESSIONS 6 - 7 (LIVE IN-PERSON)

Ethereum and smart contracts. Smart contracts are the fundamental building blocks of Ethereum's application layer. 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. In this lecture (2 sessions long), 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.

SESSIONS 8 - 9 (LIVE IN-PERSON)

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 (2 sessions long), 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). This set of lectures will be complemented by a programming exercise students will have to finalize before next session of the course.

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 exervises 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
Intermediate exercises	50 %		
Group Presentation	40 %		
Class Participation	10 %		

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 re-enrolled 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.

CLASS PARTICIPATION

The rating of the class participation is based on two aspects, the presence and contributions to class discussions. Contributions on class discussions will focus on quality, not quantity of the contribution, so that students who participate often do not necessarily receive a better rating than those who participate less frequently. Therefore, students are encouraged to start contributing to the discussions since the beginning of the course.

INDIVIDUAL AND WORKGROUP ASSIGNMENTS

You are expected to complete several labs exercises individually and submit them to the instructor before the next lecture. In addition, you will be evaluated based on your contribution to the final group presentation that will take place at the end of course. These practices will give you the opportunity to reflect on what you have learnt in class and apply it to some practical problems. More details of the labs will be provided by the start of the course.

BIBLIOGRAPHY

Recommended

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