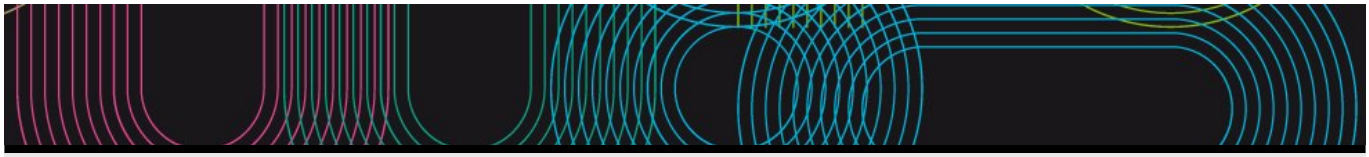

IDENTIFYING DATA				
Smart Contracts and dApps				
Subject	Smart Contracts and dApps			
Code	V05M175V11219			
Study programme	Máster Universitario en Ciberseguridad			
Descriptors	ECTS Credits	Choose	Year	Quadmester
	3	Optional	1st	2nd
Teaching language	Spanish			
Department				
Coordinator	Fernández Iglesias, Manuel José			
Lecturers	Álvarez Sabucedo, Luis Modesto Fernández Caramés, Tiago Manuel Fernández Iglesias, Manuel José			
E-mail	manolo@uvigo.es			
Web				
General description	This course offers students an introductory understanding of the concepts and practices related to the development and deployment of secure smart contracts and decentralized applications. Students will explore the specificities of smart contract programming, and examine various security vulnerabilities and threats specific to smart contracts and decentralized applications. Through hands-on exercises, real-world case examples and classroom discussions, students will learn how to employ best practices to mitigate risks and protect against attacks in the blockchain ecosystem. By the end of the course, students will be equipped with the knowledge and skills to develop secure smart contracts and design resilient decentralized applications that can withstand the challenges of these technologies.			

Training and Learning Results
Code

Expected results from this subject	
Expected results from this subject	Training and Learning Results

Contents	
Topic	
Basic concepts	Discussion of the basic concepts related to the development of smart contracts and decentralized applications.
Design and development of smart contracts	The development of smart contracts is addressed, taking into account the most relevant security aspects.
Peer-to-peer file systems	The basic characteristics of peer-to-peer networks are presented, followed by a description of the essential elements of decentralized file systems and their relationship with blockchain technologies. IPFS is presented as a case study.
Oracles. Good practices	Oracles are presented as third-party services that provide external data or events to a smart contract in a blockchain. Best practices for their development and use are identified.
Non-fungible tokens	A specific use case very popular in the world of smart contracts and decentralized applications is discussed: non-fungible tokens or NFTs.
BaaS as an outsourcing model	The basic elements of Blockchain as a Service (BaaS) to develop, deploy and manage blockchain applications without the need to set up and maintain blockchain infrastructure are discussed.
Cybersecurity aspects	A recap of the key elements for designing secure smart contracts, oracles and decentralized applications is offered.

Planning

	Class hours	Hours outside the classroom	Total hours
Lecturing	10.5	22.5	33
Practices through ICT	2.5	5.5	8
Practices through ICT	4	8.5	12.5
Practices through ICT	4	8.5	12.5
Essay questions exam	1.5	3	4.5
Essay questions exam	1.5	3	4.5

*The information in the planning table is for guidance only and does not take into account the heterogeneity of the students.

Methodologies

	Description
Lecturing	Theoretical concepts and their practical application will be presented in class. Students will be encouraged to participate in the resolution of practical cases (case studies), in such a way that in each class session the teacher's presentation will be combined with the students' participation.
Practices through ICT	Small projects or programming exercises of smart contracts or decentralized applications will be proposed, to be carried out in the laboratory and/or through autonomous work, under the supervision of the teacher. Reference platforms and languages in the field of blockchain will be utilized.
Practices through ICT	Small projects or programming exercises of smart contracts or decentralized applications will be proposed, to be carried out in the laboratory and/or through autonomous work, under the supervision of the teacher. Reference platforms and languages in the field of blockchain will be utilized.
Practices through ICT	Small projects or programming exercises of smart contracts or decentralized applications will be proposed, to be carried out in the laboratory and/or through autonomous work, under the supervision of the teacher. Reference platforms and languages in the field of blockchain will be utilized.

Personalized assistance

Methodologies	Description
Lecturing	Students will have the opportunity to attend personalized tutorial sessions in accordance with the procedure that will be established for this purpose at the beginning of the semester. This procedure will be published on the course website.
Practices through ICT	Students will have the opportunity to attend personalized tutorial sessions in accordance with the procedure that will be established for this purpose at the beginning of the semester. This procedure will be published on the course website.

Assessment

	Description	Qualification	Training and Learning Results
Practices through ICT	The solution offered to the first course assignment will be evaluated, taking into account the correctness of the proposed solution, the quality of the code, the efficiency of the code, the problem-solving skills and the documentation of the code.	10	
Practices through ICT	The solution offered to the second course assignment will be evaluated, taking into account the correctness of the proposed solution, the quality of the code, the efficiency of the code, the problem-solving skills and the documentation of the code.	20	
Practices through ICT	The solution offered to the third course assignment will be evaluated, taking into account the correctness of the proposed solution, the quality of the code, the efficiency of the code, the problem-solving skills and the documentation of the code.	20	
Essay questions exam	Each student will sit, individually and without any supporting material, a classroom exam in the middle of the semester (the exact date will be published at the beginning of the semester at the course web) about the contents explained up to the week before the exam.	20	
Essay questions exam	Each student will sit, individually and without any supporting material, a classroom exam at the end of the semester (the exact date will be published at the beginning of the semester at the course web) on the totality of the course syllabus.	30	

Other comments on the Evaluation

There are two assessment modalities, continuous assessment (CA) and global assessment (GA), which must be chosen by the students considering the following conditions:

- Both the classroom and lab parts will be evaluated according to the same mechanism, CA or GA, as selected by the student.
- CA includes the exams described in the previous section: two theory exams, design and development of three programming assignments.
- Students will confirm the final evaluation modality (CA or GA) when submitting lab deliverables, depending on the submission date. The chosen evaluation modality will also be applied to the theory/classroom part. Therefore, in the case that a student finally chooses GA, the grade of the first classroom exam, if any, would be discarded.
- Regardless of the chosen evaluation modality, lab assignments will always be carried out individually.
- A minimum grade of 2 points (out of 5) in both theory/classroom and lab parts is required to pass the course.
- If the grade resulting from adding the classroom and lab grades is equal or higher than 5 points, but the student does not reach the minimum grade required in any of them, his/her final grade will be Fail (4.5).
- If a student attends any of the evaluation tests of the course, he/she will not be able to appear in transcripts as "no-show".
- The CA tests will only take place on the dates established by the lecturers, and cannot be resit or delayed.
- Plagiarism is regarded as serious dishonest behavior. If any form of plagiarism is detected in any of the tests or exams, the final grade will be *Fail(0)*, and the incident will be reported to the corresponding academic authorities for prosecution.

Assessment procedure for the ordinary call for students who opt for Continuous Assessment (CA)

- **Theory/classroom part (50%)**: The grade of this part (5 points) is obtained by adding the corresponding grades of the two classroom exams (midterm and end-of-semester), with maximum grades of 2 and 3 points, respectively.
- **Lab part (50%)**: The grade for this part depends on the grades obtained in each lab assignment (up to 1, 2 and 2 points respectively, up to 5 points in total).

Students who do not pass the course in the ordinary opportunity, may redeem the grade obtained in both theory and lab for the extraordinary opportunity, as long as they have achieved the minimum grade required in the part they wish to keep (2 points out of 5, in both cases).

Assessment procedure for the ordinary call for students who opt for Global Assessment (GA):

- **Classroom part (50%)**: The grade of this part (5 points) corresponds to an individual exam without any type of supporting material at the end of the academic semester (on the date approved by the school).
- **Lab part (50%)**: The grade for this part depends on the grades obtained in the three assignments (up to 1, 2 and 2 points respectively, up to 5 points in total). The deliverables may be identical to those required in CA or include modifications in the functionalities to be developed. They will be delivered in digital format and will be evaluated by lecturers outside lab sessions.

Assessment procedure for the extraordinary call and end-of-program call:

- **Classroom part (50%)**. Individual exam on the date to be approved by the school, requiring a minimum grade of 2 points (out of 5).
- **Lab part (50%)**. The corresponding assignments must be submitted in digital. Assignments may be the same CA/GA assignments or may include modifications in functionality and/or scoring. As there is no CA, assessment procedures are the same as as ordinary call's GA.

Sources of information

Basic Bibliography

Lorne Lantz e Daniel Cawrey, **Mastering Blockchain: Unlocking the Power of Cryptocurrencies, Smart Contracts, and Decentralized Applications**, 978-1492054702, O□Reilly Media., 2020

Daniel Drescher, **Blockchain Basics:A Non-Technical Introduction in 25 Steps**, 978-1484226032, Apress, 2017

Don Tapscott e Alex Tapscott, **Blockchain Revolution: How the Technology Behind Bitcoin is Changing Money, Business, and the World**, 978-1101980149, New enlarged edition, Penguin Publishing Group, 2018

Paul Vigna e Michae lJ. Case, **The Truth Machine: The Blockchain and the Future of Everything**, 978-0008301774, Harper Collins, 2019

Manuel J. Fernández Iglesias, **Introduction to Blockchain, Smart Contracts and Decentralized Applications**, bit.ly/intro_ciad, 2023

Complementary Bibliography

Andreas M. Antonopoulos, **The Internet of Money**, 978-1537000459, CreateSpace Independent Publishing Platform, 2016

Ethereum.org, **Ethereum Development Tutorials**, https://ethereum.org/en/developers/tutorials/, 2023
Bina Ramamurthy, **Blockchain Basics**, https://www.coursera.org/learn/blockchain-basics, Coursera, 2023
Mark Parzygnat, **IBM Blockchain 101: Quick-start guide for developers**, https://bit.ly/ibm_bc_basics, IBM Developer, 2023

Recommendations

Subjects that it is recommended to have taken before

Distributed ledger and Blockchain technologies/V05M175V11113