



DATOS IDENTIFICATIVOS

Smart Contracts e dApps

Materia	Smart Contracts e dApps			
Código	V05M175V11219			
Titulación	Máster Universitario en Ciberseguridade			
Descritores	Creditos ECTS	Sinale	Curso	Cuadrimestre
	3	OP	1	2c
Lingua de impartición	Castelán			
Departamento	Enxeñaría telemática			
Coordinador/a	Fernández Iglesias, Manuel José			
Profesorado	Álvarez Sabucedo, Luis Modesto Fernández Iglesias, Manuel José			
Correo-e	manolo@uvigo.es			

Web

Descrición xeral	Esta materia ofrece unha visión introdutoria dos conceptos e prácticas relacionados co desenvolvemento e despregamento de contratos intelixentes e aplicacións descentralizadas seguras. Os e as estudantes explorarán as especificidades da programación de contratos intelixentes e examinarán diversas vulnerabilidades e ameazas de seguridade específicas dos contratos intelixentes e as aplicacións descentralizadas. A través de exercicios prácticos, exemplos de casos reais e explicacións na aula, o alumnado aprenderá a empregar as mellores prácticas para mitigar os riscos e protexerse contra os ataques no ecosistema blockchain. Ao final do curso, dispoñerá de coñecementos e habilidades para desenvolver contratos intelixentes seguros e deseñar aplicacións descentralizadas robustas que poidan soportar os desafíos que presentan estas tecnoloxías.			
------------------	--	--	--	--

Resultados de Formación e Aprendizaxe

Código	
--------	--

Resultados previstos na materia

Resultados previstos na materia	Resultados de Formación e Aprendizaxe
---------------------------------	---------------------------------------

Contidos

Tema	
Conceptos básicos	Presentación dos conceptos básicos relacionados co desenvolvemento de contratos intelixentes e aplicacións descentralizadas.
Deseño e desenvolvemento de contratos intelixentes	Abordarse o desenvolvemento de contratos intelixentes, tendo en conta os aspectos relacionados coa seguridade máis relevantes no seu desenvolvemento.
Sistemas de arquivos peer-to-peer	Preséntanse as características básicas das redes peer-to-peer, para a continuación describir os elementos esenciais dos sistemas de arquivos descentralizados e a súa relación coas tecnoloxías blockchain. Preséntase IPFS como caso de estudo.
Tokens non funxibles	Preséntase un caso de uso concreto moi popular no mundo dos contratos intelixentes e as aplicacións descentralizadas: os tokens non funxibles ou NFT.
Oráculos. Boas prácticas	Preséntanse os oráculos como servizos de terceiros que proporcionan datos ou eventos externos a un contrato intelixente nunha blockchain. Identifícanse boas prácticas para o seu desenvolvemento e utilización.
Aspectos relacionados coa ciberseguridade	Realízase unha recapitulación dos elementos cruce para o deseño de contratos intelixentes, oráculos e aplicacións descentralizadas seguras.

Planificación			
	Horas na aula	Horas fóra da aula	Horas totais
Lección maxistral	11.5	24.5	36
Prácticas con apoio das TIC	2.5	6	8.5
Prácticas con apoio das TIC	4	9	13
Prácticas con apoio das TIC	4	9	13
Exame de preguntas obxectivas	1.5	3	4.5

*Os datos que aparecen na táboa de planificación son de carácter orientador, considerando a heteroxeneidade do alumnado.

Metodoloxía docente	
	Descrición
Lección maxistral	Expoñeranse en clase os conceptos teóricos e a súa aplicación práctica. Tentarase que o alumnado participe intercalando a resolución de supostos prácticos (estudo de casos), de tal forma que en cada sesión de clase combíñase a presentación do profesorado coa participación do alumnado.
Prácticas con apoio das TIC	Exporanse pequenos proxectos ou exercicios de programación de contratos intelixentes ou aplicacións descentralizadas, a realizar no laboratorio e/ou mediante traballo autónomo, baixo a supervisión do profesorado. Utilizaranse plataformas e linguaxes de referencia no ámbito das cadeas de bloques.
Prácticas con apoio das TIC	Exporanse pequenos proxectos ou exercicios de programación de contratos intelixentes ou aplicacións descentralizadas, a realizar no laboratorio e/ou mediante traballo autónomo, baixo a supervisión do profesorado. Utilizaranse plataformas e linguaxes de referencia no ámbito das cadeas de bloques.
Prácticas con apoio das TIC	Exporanse pequenos proxectos ou exercicios de programación de contratos intelixentes ou aplicacións descentralizadas, a realizar no laboratorio e/ou mediante traballo autónomo, baixo a supervisión do profesorado. Utilizaranse plataformas e linguaxes de referencia no ámbito das cadeas de bloques.

Atención personalizada	
Metodoloxías	Descrición
Lección maxistral	O alumnado terá ocasión de acudir a titorías personalizadas de acordo co procedemento que se establecerá para ese efecto ao principio do curso. Dito procedemento publicárase na web da materia.
Prácticas con apoio das TIC	O alumnado terá ocasión de acudir a titorías personalizadas de acordo co procedemento que se establecerá para ese efecto ao principio do curso. Dito procedemento publicárase na web da materia.

Avaliación		
	Descrición	Cualificación Resultados de Formación e Aprendizaxe
Prácticas con apoio das TIC	Avaliarase a solución ofrecida á primeira práctica da materia, tendo en conta a corrección da solución proposta, a calidade do código, a eficiencia do mesmo, as habilidades de resolución de problemas e a documentación do código.	10
Prácticas con apoio das TIC	Avaliarase a solución ofrecida á segunda práctica da materia, tendo en conta a corrección da solución proposta, a calidade do código, a eficiencia do mesmo, as habilidades de resolución de problemas e a documentación do código.	25
Prácticas con apoio das TIC	Avaliarase a solución ofrecida á terceira práctica da materia, tendo en conta a corrección da solución proposta, a calidade do código, a eficiencia do mesmo, as habilidades de resolución de problemas e a documentación do código.	25
Exame de preguntas obxectivas	Cada estudante realizará, individualmente e sen ningún tipo de material de apoio, un exame de teoría a final do cuadrimestre (a data exacta publicárase a principio de curso na web da materia) sobre a totalidade dos contidos da materia.	40

Outros comentarios sobre a Avaliación

Existen dous mecanismos de avaliación, avaliación continua (AC) e avaliación global (AG), rexidos polas seguintes condicións:

- A modalidade de avaliación elixida (AC ou AG) será única e, por tanto, aplicable tanto á teoría como ás prácticas.
- A AC inclúe as probas descritas no apartado anterior: un puntuable de teoría, e tres prácticas.
- O alumnado confirmará a modalidade de avaliación definitiva a través da entrega das prácticas, en función do prazo

(de AC ou AG) ao que se acolla.

- Con independencia da modalidade elixida, as prácticas realizaranse sempre individualmente.
- Establécese unha nota mínima de 2 puntos tanto en teoría (dun total de 4 puntos) como en prácticas (dun total de 6 puntos) para poder aprobar a materia.
- Se a nota resultante de sumar as cualificacións de teoría e prácticas é igual ou maior que 5 puntos pero o/a estudante non alcanza a nota mínima esixida nalgunha delas, a súa cualificación final será suspenso (4.5).
- Se o alumnado se presenta a algunha das probas de avaliación da materia non poderá figurar na acta como "non presentado".
- As probas de AC só se levarán a cabo nas datas estipuladas polo equipo docente, non podendo repetirse máis tarde.
- En caso de plaxio, asignarase a nota suspenso (0) e este feito será notificado á dirección do Centro para os efectos oportunos.

Procedemento de avaliación na oportunidade ordinaria para o alumnado que opte por AC:

- **Parte teórica (40%):** A nota desta parte resulta da cualificación do exame de teoría final de cuadrimestre, cuxa cualificación máxima é de 4 puntos.
- **Parte práctica (60%):** A nota desta parte depende das cualificacións obtidas nas practicas (ata 1, 2,5 e 2,5 puntos respectivamente, ata 6 puntos en total).

O estudiantado que non aprobe a materia na oportunidade ordinaria, poderá conservar a cualificación obtida tanto en teoría como en prácticas para a oportunidade extraordinaria, sempre que alcanzase a nota mínima esixida na parte que desexen gardar (2 puntos en ambos os casos).

Procedemento de avaliación na oportunidade ordinaria para o alumnado que opte por AG:

- **Parte teórica (40%):** A nota desta parte corresponde ao exame final realizado na data aprobada pola Xunta de Escola, sobre un máximo de 4 puntos.
- **Parte práctica (60%):** A nota desta parte depende das cualificacións obtidas nas prácticas (ata 1, 2,5 e 2,5 puntos respectivamente, ata 6 puntos en total). Os entregables poderán ser idénticos aos esixidos en AC ou incluír modificacións nas funcionalidades para desenvolver. Entregaranse en formato electrónico e serán avaliados polo profesorado fóra de clase.

Procedemento de avaliación na oportunidade extraordinaria e na convocatoria fin de carreira:

- **Parte teórica (40%).** A nota desta parte corresponde ao exame final na data que aprobará a Xunta de Escola, sobre un máximo de 4 puntos.
- **Parte práctica (60%).** Entregaranse as 3 prácticas en formato dixital. As funcionalidades esixidas poderán ser as mesmas que na oportunidade ordinaria ou incluír modificacións que serán publicadas coa debida antelación. Dado que non existe a modalidade de AC, as condicións de avaliación son idénticas ás descritas no apartado de AG da oportunidade ordinaria.

Bibliografía. Fontes de información

Bibliografía Básica

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

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

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

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

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

Bibliografía Complementaria

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

Ethereum.org, **Ethereum Development Tutorials**, 2023

Bina Ramamurthy, **Blockchain Basics**, Coursera, 2023

Mark Parzygnat, **IBM Blockchain 101: Quick-start guide for developers**, IBM Developer, 2023

Recomendacións

Materias que se recomienda ter cursado previamente

Tecnoloxías de rexistro distribuído e Blockchain/V05M175V11113
