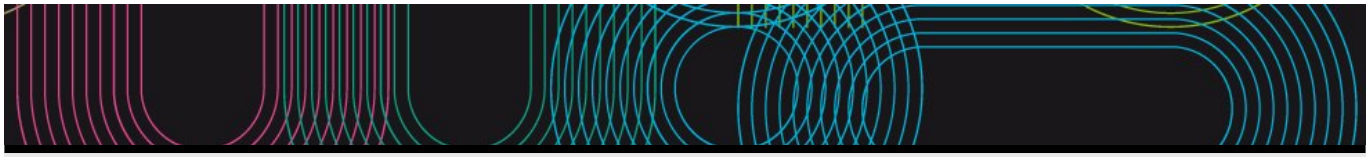

DATOS IDENTIFICATIVOS				
Smart Contracts e dApps				
Asignatura	Smart Contracts e dApps			
Código	V05M175V11219			
Titulacion	Máster Universitario en Ciberseguridad			
Descriptores	Creditos ECTS	Seleccione	Curso	Cuatrimestre
	3	OP	1	2c
Lengua Impartición	Castellano			
Departamento	Dpto. Externo Ingeniería telemática			
Coordinador/a	Fernández Iglesias, Manuel José			
Profesorado	Álvarez Sabucedo, Luis Modesto Fernández Caramés, Tiago Manuel Fernández Iglesias, Manuel José			
Correo-e	manolo@uvigo.es			
Web				
Descripción general	Esta asignatura ofrece una visión introductoria de los conceptos y prácticas relacionados con el desarrollo y despliegue de contratos inteligentes y aplicaciones descentralizadas seguras. Los y las estudiantes explorarán las especificidades de la programación de contratos inteligentes y examinarán diversas vulnerabilidades y amenazas de seguridad específicas de los contratos inteligentes y las aplicaciones descentralizadas. A través de ejercicios prácticos, ejemplos de casos reales y explicaciones en el aula, el alumnado aprenderá a emplear las mejores prácticas para mitigar los riesgos y protegerse contra los ataques en el ecosistema blockchain. Al final del curso, se dispondrá de conocimientos y habilidades para desarrollar contratos inteligentes seguros y diseñar aplicaciones descentralizadas robustas que puedan soportar los desafíos que presentan estas tecnologías.			

Resultados de Formación y Aprendizaje
Código

Resultados previstos en la materia	
Resultados previstos en la materia	Resultados de Formación y Aprendizaje

Contenidos	
Tema	
Conceptos básicos	Presentación de los conceptos básicos relacionados con el desarrollo de contratos inteligentes y aplicaciones descentralizadas.
Diseño y desarrollo de contratos inteligentes	Se abordar el desarrollo de contratos inteligentes, teniendo en cuenta los aspectos relacionados con la seguridad más relevantes en su desarrollo.
Sistemas de archivos peer-to-peer	Se presentan las características básicas de las redes peer-to-peer, para a continuación describir los elementos esenciales de los sistemas de archivos descentralizados y su relación con las tecnologías blockchain. Se presenta IPFS como caso de estudio.
Oráculos. Buenas prácticas	Se presentan los oráculos como servicios de terceros que proporcionan datos o eventos externos a un contrato inteligente en una blockchain. Se identifican buenas prácticas para su desarrollo y utilización.
Tokens no fungibles	Se presenta un caso de uso concreto muy popular en el mundo de los contratos inteligentes y las aplicaciones decentralizadas: los tokens no fungibles o NFT.

BaaS como modelo de externalización	Se presentan los elementos básicos de Blockchain como servicio (Blockchain as a Service, BaaS) para desarrollar, desplegar y gestionar aplicaciones blockchain sin necesidad de configurar y mantener infraestructura de cadena de bloques.
Aspectos relacionados con la ciberseguridad	Se realiza una recapitulación de los elementos clave para el diseño de contratos inteligentes, oráculos y aplicaciones descentralizadas seguras.

Planificación

	Horas en clase	Horas fuera de clase	Horas totales
Lección magistral	10.5	22.5	33
Prácticas con apoyo de las TIC	2.5	5.5	8
Prácticas con apoyo de las TIC	4	8.5	12.5
Prácticas con apoyo de las TIC	4	8.5	12.5
Examen de preguntas de desarrollo	1.5	3	4.5
Examen de preguntas de desarrollo	1.5	3	4.5

*Los datos que aparecen en la tabla de planificación son de carácter orientativo, considerando la heterogeneidad de alumnado

Metodologías

	Descripción
Lección magistral	Se expondrán en clase los conceptos teóricos y su aplicación práctica. Se intentará que el alumnado participe intercalando la resolución de supuestos prácticos (estudio de casos), de tal forma que en cada sesión de clase se combine la presentación del profesorado con la participación del alumnado.
Prácticas con apoyo de las TIC	Se plantearán pequeños proyectos o ejercicios de programación de contratos inteligentes o aplicaciones descentralizadas, a realizar en el laboratorio y/o mediante trabajo autónomo, bajo la supervisión del profesorado. Se utilizarán plataformas y lenguajes de referencia en el ámbito de las cadenas de bloques.
Prácticas con apoyo de las TIC	Se plantearán pequeños proyectos o ejercicios de programación de contratos inteligentes o aplicaciones descentralizadas, a realizar en el laboratorio y/o mediante trabajo autónomo, bajo la supervisión del profesorado. Se utilizarán plataformas y lenguajes de referencia en el ámbito de las cadenas de bloques.
Prácticas con apoyo de las TIC	Se plantearán pequeños proyectos o ejercicios de programación de contratos inteligentes o aplicaciones descentralizadas, a realizar en el laboratorio y/o mediante trabajo autónomo, bajo la supervisión del profesorado. Se utilizarán plataformas y lenguajes de referencia en el ámbito de las cadenas de bloques.

Atención personalizada

Metodologías	**Descripción**
Lección magistral	El alumnado tendrá ocasión de acudir a tutorías personalizadas de acuerdo con el procedimiento que se establecerá a tal efecto al principio del curso. Este procedimiento se publicará en la web de la asignatura.
Prácticas con apoyo de las TIC	El alumnado tendrá ocasión de acudir a tutorías personalizadas de acuerdo con el procedimiento que se establecerá a tal efecto al principio del curso. Este procedimiento se publicará en la web de la asignatura.

Evaluación

	Descripción	Calificación	Resultados de Formación y Aprendizaje
Prácticas con apoyo de las TIC	Se evaluará la solución ofrecida a la primera práctica de la materia, teniendo en cuenta la corrección de la solución propuesta, la calidad del código, la eficiencia del mismo, las habilidades de resolución de problemas y la documentación del código.	10	
Prácticas con apoyo de las TIC	Se evaluará la solución ofrecida a la segunda práctica de la materia, teniendo en cuenta la corrección de la solución propuesta, la calidad del código, la eficiencia del mismo, las habilidades de resolución de problemas y la documentación del código.	20	
Prácticas con apoyo de las TIC	Se evaluará la solución ofrecida a la tercera práctica de la materia, teniendo en cuenta la corrección de la solución propuesta, la calidad del código, la eficiencia del mismo, las habilidades de resolución de problemas y la documentación del código.	20	

Examen de preguntas de desarrollo	Cada estudiante realizará, individualmente y sin ningún tipo de material de apoyo, un examen de teoría a mitad del cuartrimestre (la fecha exacta se publicará a principio de curso en la web de la materia) sobre los contenidos que se hayan explicado hasta la semana anterior a la prueba.	20
Examen de preguntas de desarrollo	Cada estudiante realizará, individualmente y sin ningún tipo de material de apoyo, un examen de teoría a final del cuatrimestre (la fecha exacta se publicará a principio de curso en la web de la materia) sobre la totalidad de los contenidos de la materia.	30

Otros comentarios sobre la Evaluación

Existen dos mecanismos de evaluación, evaluación continua (EC) y evaluación global (EG), regidos por las siguientes condiciones:

- La modalidad de evaluación elegida (EC o EG) será única y, por tanto, aplicable tanto a la teoría como a las prácticas.
- La EC incluye las pruebas descritas en el apartado anterior: dos puntuables de teoría, y tres prácticas.
- El alumnado confirmará la modalidad de evaluación definitiva a través de la entrega de las prácticas, en función del plazo de entrega (de EC o EG) al que se acoja. Dicha modalidad de evaluación será la que se aplicará también en la parte de teoría, de ahí que en el caso de que un estudiante opte finalmente por EG, la nota del primer puntuable de teoría, de ser el caso, quedaría anulada.
- Con independencia de la modalidad elegida, las prácticas se realizarán siempre individualmente.
- Se establece una nota mínima de 2 puntos (sobre 5) tanto en teoría como en prácticas para poder aprobar la asignatura.
- Si la nota resultante de sumar las calificaciones de teoría y prácticas es igual o mayor que 5 puntos pero el/la estudiante no alcanza la nota mínima exigida en alguna de ellas, su calificación final será suspenso (4.5).
- Si el alumnado se presenta a alguna de las pruebas de evaluación de la asignatura no podrá figurar en el acta como "no presentado".
- Las pruebas de EC sólo se llevarán a cabo en las fechas estipuladas por el equipo docente, no pudiendo repetirse más tarde.
- En caso de plagio, se asignará la nota *suspenso (0)* y este hecho será notificado a la dirección del Centro a los efectos oportunos.

Procedimiento de evaluación en la oportunidad ordinaria para el alumnado que opte por EC:

- **Parte teórica (50%):** La nota de esta parte resulta de sumar las calificaciones de los dos puntuables de teoría descritos anteriormente (a mitad y a final de cuatrimestre), cuyas calificaciones máximas son 2 y 3 puntos, respectivamente.
- **Parte práctica (50%):** La nota de esta parte depende de las calificaciones obtenidas en las prácticas (hasta 1, 2 y 2 puntos respectivamente, hasta 5 puntos en total).

El estudiantado que no apruebe la asignatura en la oportunidad ordinaria, podrá conservar la calificación obtenida tanto en teoría como en prácticas para la oportunidad extraordinaria, siempre que haya alcanzado la nota mínima exigida en la parte que deseen guardar (2 puntos sobre 5, en ambos casos).

Procedimiento de evaluación en la oportunidad ordinaria para el alumnado que opte por EG:

- **Parte teórica (50%):** La nota de esta parte corresponde al examen final realizado en la fecha aprobada por la Junta de Escuela, sobre un máximo de 5 puntos.
- **Parte práctica (50%):** La nota de esta parte depende de las calificaciones obtenidas en las prácticas (hasta 1, 2 y 2 puntos respectivamente, hasta 5 puntos en total). Los entregables podrán ser idénticos a los exigidos en EC o incluir modificaciones en las funcionalidades a desarrollar. Se entregarán en formato digital y serán evaluados por el profesorado fuera de clase.

Procedimiento de evaluación en la oportunidad extraordinaria y la convocatoria fin de carrera:

- **Parte teórica (50%)**. La nota de esta parte corresponde al examen final realizado en la fecha aprobada por la Junta de Escuela, sobre un máximo de 5 puntos.
- **Practical part (50%)**. Se entregarán los correspondientes prácticas digitalmente. Las funcionalidades exigidas podrán ser las mismas que en la oportunidad ordinaria o incluir modificaciones que serán publicadas con la debida

antelación. Dado que no existe la modalidad de EC, las condiciones de evaluación son idénticas a las descritas en el apartado de EG de la oportunidad ordinaria.

Fuentes de información

Bibliografía Básica

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

Bibliografía Complementaria

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

Recomendaciones

Asignaturas que se recomienda haber cursado previamente

Tecnologías de resgistro distribuído y Blockchain/V05M175V11113