Universitat Autònoma de Barcelona

2023/2024

Tecnología Blockchain y Criptomonedas

Código: 105072
Créditos ECTS: 6

Titulación	Tipo	Curso	Semestre
2502441 Ingeniería Informática	OT	4	1

Contacto

Nombre: Jordi Herrera Joancomarti

Correo electrónico: jordi.herrera@uab.cat

Idiomas de los grupos

Puede consutarlo a través de este enlace. Para consultar el idioma necesitará introducir el CÓDIGO de la asignatura. Tenga en cuenta que la información es provisional hasta el 30 de noviembre del 2023.

Equipo docente

Cristina Perez Sola

Prerrequisitos

Para cursar esta asignatura es necesario haber superado las asignaturas de Información y Seguridad (IS) y la de Fundamentos de Tecnología de la Información (FTI), que introduce distintos conceptos importantes a tener consolidados para cursar la asignatura de TBC. En concreto:

- FTI consolida los conocimientos de criptografía que los estudiantes han obtenido en la asignatura de IS.
- El algoritmo de firma del ElGamal, que se estudia en FTI, es la base del algoritmo ECDSA que se utiliza en la mayoría de criptomonedas y que se trata en la asignatura de TBC.
- En FTI se explican algunos ataques de mala implementación de algoritmos de firma digital que pueden dar lugar a robos de criptomonedas, temas que se tratan en la asignatura de TBC.
- En FTI se explican en detalle el funcionamiento y las propiedades de las funciones hash, que son cruciales en la implementación y seguridad de la tecnología blockchain.
- El último tema de FTI es una introducción a la tecnología blockchain ya las criptomonedas. Una introducción que sirve para dar una base inicial con la que después se trabajará en la asignatura TBC.

Objetivos y contextualización

Los objetivos de esta asignatura son:

- Entender los conceptos teóricos de la tecnología blockchain
- Comprender el funcionamiento de las criptomonedas
- Entender cómo funcionan los Bitcoin, desde un punto de vista técnico

- Entender el concepto de smart contract.
- Entender la diferencia entre una blockchain basada en UTXO y una basada en cuentas.
- Conocer algunos de los mecanismos de escalabilidad de la tecnología blockchain

Competencias

- Adquirir hábitos de pensamiento.
- Adquirir hábitos de trabajo personal.
- Capacidad para concebir, redactar, organizar, planificar, desarrollar y firmar proyectos en el ámbito de la ingeniería en informática que tengan por objeto la concepción, el desarrollo o la explotación de sistemas, servicios y aplicaciones informáticas.
- Capacidad para diseñar, desarrollar, evaluar y asegurar la accesibilidad, ergonomía, usabilidad y seguridad de los sistemas, servicios y aplicaciones informáticas, así como de la información que gestionan.
- Capacidad para diseñar, desarrollar, seleccionar y evaluar aplicaciones y sistemas informáticos, asegurando su fiabilidad, seguridad y calidad, conforme a principios éticos y a la legislación y normativa vigente.
- Capacidad para seleccionar, desplegar, integrar y gestionar sistemas de información que satisfagan las necesidades de la organización, con los criterios de coste y calidad identificados.

Resultados de aprendizaje

1. Desarrollar la capacidad de análisis, síntesis y prospectiva.
2. Diseñar las soluciones informáticas que permitan integrar en un sistema distribuido las necesidades de accesibilidad y seguridad.
3. Diseñar, desarrollar, seleccionar y evaluar aplicaciones asegurando su fiabilidad y seguridad.
4. Identificar los principales ataques que puede recibir un sistema informático, así como los posibles métodos de protección, detección y aplicación de políticas de seguridad que permitan evitar el daño al sistema o minimizar su repercusión.
5. Incorporar sistemas distribuidos de tratamiento de la información en una organización para incrementar la capacidad operativa.
6. Trabajar de forma autónoma.

Contenido

Los contenidos de esta asignatura son los siguientes:

1. Conceptos básicos de tecnología blockchain
2. Criptografía para tecnología blockchain
3. Bitcoin
4. Protocolos de segunda capa: Lightning Network
5. Ethereum
6. Otras blockchains

Metodología

La asignatura se estructura en sesiones de dos horas con una formulación muy dinámica donde se pedirá a los estudiantes que intervengan activamente. La tipología de sesiones incluirá de contenido más teórico y otros más práctico.

Las sesiones de contenido más teórico se basarán en material que el profesor previamente hará llegar a los estudiantes a través del campus virtual. En base a este material, se estructurarán dos tipologías diferentes de sesiones. Por un lado, sesiones de preguntas y respuestas donde los estudiantes formularán las dudas que les hayan surgido del trabajo previo sobre el material proporcionado. En estas sesiones, el profesor también interpelará a los estudiantes para hacer aflorar los aspectos más relevantes del material que se está trabajando. Por otra parte, habrá sesiones donde los estudiantes, en grupos de dos, presentarán algún estudio más detallado de alguno de los temas tratados en la asignatura.

Las sesiones de contenido más práctico incluirán tanto la resolución de cuestiones a modo de ejercicios como la realización de tareas más técnicas donde se combinará el uso de herramientas específicas de la asignatura (wallets, exploradores de blockchain, compiladores de smart contracts , etc.) con el desarrollo de funciones específicas utilizando el lenguaje de programación Python.

Competencias transversales. En esta asignatura se trabajarán y evaluarán las siguientes competencias transversales del Grado de Ingeniería Informática:

- T01.02 - Desarrollar la capacidad de análisis, síntesis y prospectiva:esta competencia se trabajará de forma más intensa en las sesiones más teóricas donde los estudiantes deberán demostrar la comprensión de los contenidos propuestos a través de las preguntas que el profesor les propondrá durante las sesiones de teoría. También se trabajará esta competencia en los diferentes trabajos que los estudiantes presentarán a lo largo del curso.
- T02.01 Trabajar de forma autónoma: ésta se focaliza en aquellas actividades individuales, como la realización de los trabajos prácticos que los estudiantes harán a lo largo del curso.

Nota: se reservarán 15 minutos de una clase dentro del calendario establecido por el centro o por la titulación para que el alumnado rellene las encuestas de evaluación de la actuación del profesorado y de evaluación de la asignatura o módulo.

Actividades

Título	Horas	ECTS	Resultados de aprendizaje
Tipo: Dirigidas			
Clases prácticas	25	1	2, 3, 5, 6
Clases teóricas	25	1	1, 4, 5
Tipo: Supervisadas			
Tutorías y consultas	10	0,4	1, 2, 3, 4, 5
Tipo: Autónomas			
Preparación de las clases prácticas	25	1	1, 2, 3, 6
Preparación de las clases teóricas	37,5	1,5	1, 4, 5, 6

Evaluación

El modelo de evaluación de esta asignatura será íntegramente de evaluación continua. Dado el dinamismo de la misma y la implicación que se pide a los estudiantes en todas las sesiones de clase (tanto las de tipo más teórico como las más prácticas) el profesor tendrá múltiples elementos para poder evaluar a los alumnos. La participación activa en las clases preguntando dudas al profesor y respondiendo dudas de los otros estudiantes o de las cuestiones del profesor supondrá un 20% de la nota de la asignatura. Es por este motivo

que la asistencia a clase de esta asignatura es obligatoria.

Más allá de la evaluación en base a las aportaciones en las clases, los estudiantes también deberán entregar diferentes trabajos más prácticos que se irán proponiendo a lo largo del curso en el campus virtual de la UAB, entregas que complementarán las evidencias de evaluación del estudiante. Estas actividades más prácticas supondrán un 50% de la nota de la asignatura.

Por otra parte, la presentación del tema que los estudiantes realizarán en las sesiones teóricas de la asignatura también formará parte de las evidencias de evaluación y supondrá un 30% de la nota de la asignatura.

Para superar la asignatura será necesario haber superado cada una de las actividades evaluables entendiendo que las actividades evaluables son: participación en clase, trabajos prácticos y presentación. Cada uno de los trabajos prácticos se deberán superar por separado.

En caso de no superar alguno de los trabajos prácticos se podrán recuperar volviendo a presentar, si bien en este caso la nota máxima del trabajo recuperado que se obtendrá será un 5.

En caso de no superar el trabajo de presentación, habrá recuperarlo presentando una versión extendida del mismo trabajo que será presentado oralmente al profesor de la asignatura.

En caso de no superar la evaluación de la participación en clase, esta no se podrá recuperar.

No se contempla ningún tipo de convalidación de ninguna de las actividades evaluables para los estudiantes repetidores.

Sin perjuicio de otras medidas disciplinarias que se estimen oportunas, y de acuerdo con la normativa académica vigente, las irregularidades cometidas por un estudiante que puedan conducir a una variación de la calificación se calificarán con un cero (0). Las actividades de evaluación calificadas de esta forma y por este procedimiento no serán recuperables. Si es necesario superar cualquiera de estas actividades de evaluación para aprobar la asignatura, esta asignatura quedará suspendida directamente, sin oportunidad de recuperarla en el mismo curso. Estas irregularidades incluyen, entre otros:

- la copia total o parcial de una práctica, informe, o cualquier otra actividad de evaluación;
- dejar copiar;
- presentar un trabajo de grupo no hecho íntegramente por los miembros del grupo;
- presentar como propios materiales elaborados por un tercero, aunque sean traducciones o adaptaciones, y en general trabajos con elementos no originales y exclusivos del estudiante;

En resumen: copiar, dejar copiar o plagiar (o el intento de) en cualquiera de las actividades de evaluación equivale a un SUSPENSO, no compensable y sin convalidaciones de partes de la asignatura en cursos posteriores.

Los alumnos que alcancen el número mínimo de puntos para aprobar la asignatura, pero no hayan alcanzado la nota mínima en alguna de las actividades de evaluación, serán evaluados con una nota final de 4.5. En caso de que no se haya aprobado la asignatura para la calificación de un cero de una actividad por motivo de copia, la nota final de la asignatura será un 3, lo que no permitirá compensar esta asignatura.

Finalmente, obtendrán la calificación de "No Evaluable" aquellos estudiantes que no entreguen ninguna de las actividades prácticas que se propongan. La participación en alguna de estas actividades de evaluación supondrá recibir una calificación diferente de "No Evaluable".

No se hará ninguna actividad de evaluación a ningún alumno en un horario distinto al establecido a menos que existe una causa justificada, se ha avisado con anterioridad a la actividad y el profesor ha dado su consentimiento. En otro caso, si un alumno no ha asistido a una actividad, ésta no se puede recuperar.

En cuanto a las matrículas de honor, estas se podrán conceder a aquellos estudiantes que hayan superado la

asignatura con una nota final igual o superior a 9. Dado que el número de matriculas de honor no puede superar el 5% de los estudiantes matriculados, se concederán a los estudiantes con las notas más altas. En caso de empate, se podrá requerir a los estudiantes que realicen una prueba oral para desempatar.

Actividades de evaluación continuada

Título	Peso	Horas	ECTS	Resultados de aprendizaje
Actividades pràcticas	50	12,5	0,5	1, 2, 3, 4, 5, 6
Participación en clase	20	14	0,56	4
Presentación oral de un tema	30	1	0,04	1, 2, 3, 4, 5, 6

Bibliografía

- Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller, Steven Goldfeder. Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction. Princeton University Press (2016). ISBN: 978-0691171692
- Andreas M. Antonopoulos, Mastering Bitcoin: Programming the Open Blockchain. O'Reilly Media; 2nd Edition. (2017) ISBN: 978-1491954386
- Andreas M. Antonopoulos y Gavin Wood, Mastering Ethereum: Building Smart Contracts and DApps. O'Reilly Media. (2018) ISBN: 978-1491971949
- C. Pérez Solà i J. Herrera Joancomartí, La criptografia que et cal saber. (2023) Disponible on-line: https://criptografia.cat/
- Kalle Rosenbaum, Grokking Bitcoin. Manning Publications (2019) ISBN 9781617294648
- Roger Wattenhofer. Blockchain Science: Distributed Ledger Technology. Inverted Forest Publishing; 3rd Edition (2019) ISBN: 978-1793471734
- Andreas Antonopoulos, Olaoluwa Osuntokun, René Pickhardt. Mastering the Lightning Network: A Second Layer Blockchain Protocol for Instant Bitcoin Payments. O'Reilly Media; 1st edition (January 4, 2022) ISBN: 978-1492054863

Software

Las sesiones de contenido más práctico incluirán tanto la resolución de cuestiones a modo de ejercicios como la realización de tareas más técnicas donde se combinará el uso de herramientas específicas de la asignatura (wallets, exploradores de blockchain, compiladores de smart contracts , etc.) con el desarrollo de funciones específicas utilizando el lenguaje de programación Python.