FACULTAD DE CIENCIAS FÍSICAS Y MATEMÁTICAS UNIVERSIDAD DE CHILE

PROGRAMA DE CURSO

Código	**Nombre**			
CC5324	Bitcoin y Criptomonedas			
Nombre en Inglés				
Bitcoin and Cryptocurrencies				
SCT	**Unidades Docentes**	**Horas de Cátedra**	**Horas Docencia Auxiliar**	**Horas de Trabajo Personal**
6	10	3	0	7
Requisitos			Carácter del Curso	
CC3001 Algoritmos y Estructuras de Datos ó FI2002 Electromagnetismo			Electivo para ICC	

Resultados de Aprendizaje

Este curso entrega los fundamentos necesarios para entender, desarrollar y aplicar técnicas de criptomonedas en diversos ámbitos de la ciencia de la computación y explorar su impacto en nuevas tecnologías y la sociedad.

Este curso busca cubrir los aspectos técnicos detrás de las criptomonedas, de las tecnologías de blockchain y de consenso distribuido. Los estudiantes aprenderán cómo dichos sistemas funcionan y cómo desarrollar sistemas seguros que puedan interactuar con la red Bitcoin y otras criptomonedas.

Al final de este curso el alumno será capaz de:

- Identificar el rol de las tecnologías de blockchain y de consenso distribuido en el campo del desarrollo de sistemas resilientes distribuidos.
- Aplicar los conceptos relacionados con criptomonedas (blockchain, consenso, incentivos) en aplicaciones distribuidas concretas.
- Implementar transacciones en una criptomoneda, explorar estrategias de minado, y desarrollar un contrato inteligente
- Aplicar el concepto de contrato inteligente a aplicaciones prácticas

Metodología Docente	Evaluación General
Clases de cátedra, discusión de casos en clases, y trabajo individual vía tareas y proyecto.	Cada alumno será evaluado vía un proyecto, ejercicios escritos y tareas de implementación. • 1 proyecto del curso con dos entregas parciales (evaluadas por sus pares) y una entrega final. • 2 o 3 ejercicios escritos cortos teóricos o de concepto, y • 3 o 4 tareas cortas de implementación. La nota final (NF) del curso se calculará como NF=0.5*NP +30*NTI+0.2*NTT donde NP es la nota del proyecto (calculada como se indica) y NTI es el promedio de las tareas de implementación, y NTT es el promedio de las tareas escritas.

Unidades Temáticas

Número	Nombre de la Unidad	Duración en Semanas
1	Introducción	1

Contenidos	Resultados de Aprendizajes de la Unidad	Referencias a la Bibliografía
1. Introducción a Bitcoin y las criptomonedas: historia, impacto, terminología, proble-mas.	El estudiante: - Define los conceptos básicos detrás de las criptomonedas, - Identifica las componentes de la tecnología de una criptomoneda. - Identifica las peculiaridades y decisiones de diseño hechas en un caso especial, Bitcoin.	[1]

Número	Nombre de la Unidad	Duración en Semanas
2	Bitcoin	4

Contenidos	Resultados de Aprendizajes de la Unidad	Referencias a la Bibliografía
1. Consenso distribuido de Nakamoto Los protocolos de Bitcoin Proof of Work. 2. Aplicaciones de bitcoin y su seguridad. 3. Mecánica de minado 4. Estrategias de minado y ataques posibles. 5. Aspectos sociales: comunidad, economía y política.	El estudiante: - Define qué es el consenso distribuído de Nakamoto. - Identifica los protocolos de Bitcoin, en particular los protocolos de proof of work . - Identifica los desafíos de seguridad de distintas aplicaciones de bitcoin. - Conoce las distintas estrategias de minado. - Interpreta la influencia de los aspectos sociales en Bitcoin.	[1], [2]

Número	Nombre de la Unidad	Duración en Semanas
3	Extensiones y Monedas Alternativas	6

Contenidos	Resultados de Aprendizajes de la Unidad	Referencias a la Bibliografía
1. Mecanismos y enfoques alternativos para minado y consenso. 2. Anonimato trazabilidad y mezclado. 3. Criptomonedas orientadas a la privacidad. 4. Introducción a las altcoins 5. Introducción a Ethereum 6. Contratos en Ethereum 7. Sidechains 8. Off chain channels.	El estudiante: - Identifica enfoques alternativos para minado y consenso. - Aplica los protocolos propuestos para obtener anonimato. - Identifica los nuevas monedas orientadas a la privacidad y los algoritmos propuestos. - Conoce y aplica las técnicas de desarrollo y uso de contratos inteligentes. - Identifica estrategias para mejorar la eficiencia de blockchain.	[1], [3]

FACULTAD DE CIENCIAS FÍSICAS Y MATEMÁTICAS UNIVERSIDAD DE CHILE

Número	Nombre de la Unidad	Duración en Semanas
4	Criptomonedas y el mundo real	4

Contenidos	Resultados de Aprendizajes de la Unidad	Referencias a la Bibliografía
1. Aspectos legales de las monedas virtuales. 2. Temas avanzados I: Criptografía Post-cuántica, seg wit y firmas agregadas. 3. Temas avanzados II: Propiedades inteligentes, data feeds, y aleatoriedad pública.	El estudiante: - Identifica la problemática y desafíos legales detrás de las monedas virtuales. - Identifica aspectos de mejoras e investigación en criptomonedas, como nuevas tipos de firmas, propiedades inteligentes y aleatoriedad pública.	[1]

Bibliografía

[1] "**Bitcoin and Cryptocurrency Technologies**", Narayanan, Bonneau, Felten, Miller and Goldfeder, Princeton University Press (July 19, 2016)
[2] "Bitcoin Developer Reference", https://bitcoin.org/en/developer-reference
[3] "Ethereum Wiki", https://github.com/ethereum/wiki/wiki

Vigencia desde:	Otoño 2018
Elaborado por:	Alejandro Hevia