Facultad de Informática | UNIVERSIDAD NACIONAL DE LA PLATA

INTRODUCCIÓN A Blockchain, Criptomonedas y Smart Contracts	**Carrera/ Plan:** *(Dejar lo que corresponda)* *Licenciatura en Informática* Plan 2015/Plan 2012/ *Licenciatura en Sistemas* Plan 2015/Plan 2012/ *Analista Programador Universitario* Plan 2015/Plan 2007 *Analista en TIC* Plan 2017
Año 2023	**Año:** 4º o 5º año **Régimen de Cursada:** Semestral (1er Semestre) **Carácter:** Optativa **Correlativas:** Orientación a Objetos 2, Introducción a Sistemas operativos, y Algoritmos y estructura de datos. **Profesor:** Matías Urbieta **Hs semanales teoría:** 2 hs **Hs semanales práctica:** 2 hs **Inicio - Fin:** 15/3 - 15/7

FUNDAMENTACIÓN

El advenimiento de la tecnología blockchain y la descentralización de aplicaciones (DApp) han permitido repensar muchas soluciones tradicionales utilizando un enfoque descentralizado tal como es el caso de las criptomonedas (por ejemplo Bitcoin o Ethereum).

Las soluciones basadas en blockchain involucran la definición de esquemas de cifrado para resguardar la información y proteger la propiedad, mecanismos de consenso para establecer la validez de la información, y el uso de registros descentralizados para su almacenamiento como es el caso de las mayormente adoptadas Distributed Ledger Technologies (DLT).

Por otro lado, los contratos inteligentes se benefician de las DLT para implementar algoritmos que representan acuerdos registrados entre partes asegurando cumplimiento.

OBJETIVOS GENERALES

- Introducir conceptos básicos de criptografía, y aplicaciones descentralizadas.
- Analizar y comprender metodológicamente soluciones basadas en blockchain
- Abordar la problemática de la construcción de una solución blockchain
- Analizar casos de uso mas conocidos tal como criptomonedas y contratos inteligentes

CONTENIDOS MÍNIMOS (de acuerdo al Plan de Estudios)

1. Introducción al blockchain. Conceptos básicos, y breve introducción a la criptografía.
2. Conceptos de aplicaciones distribuidas, centralizadas y descentralizadas. Principales implementaciones. Distributed Ledger Technologies (DLT).
3. Algoritmos de consenso.
4. Introducción a Criptomonedas. Modelo UTXO,Transacciones, Merkle root. Esquema de billeteras/wallets Custodian vs non-custodian. Generación de llaves. Minado
5. Criptomonedas. Revisión de las criptomonedas más importantes Bitcoin, Bitcoin forks, Etherium, Altcoins (Dogecoin), Privacy-Focused Cryptocurrencies (Zcash)
6. NFT: qué son y cómo funcionan.
7. Smart contracts. Introducción a Solidity. Ejemplos.
8. Seguridad. Ataques, estafas, scams (Ponzi schemes, Dutch tulip frenzy, speculative bubbles)

COMPETENCIAS

- LI-CE4- Comprender el funcionamiento de las soluciones Descentralizadas y blockchain, diagnosticar la correcta aplicación de este tipo de soluciones en el contexto del sistema, y diseñar soluciones basadas en blockchain. Analizar el principal uso de blockchain, las criptomonedas, y sus principales variantes.

- LS-CE1- Comprender el funcionamiento de las soluciones blockchain, diagnosticar la correcta aplicación de este tipo de soluciones en el contexto del sistema, y diseñar soluciones basadas en blockchain. Analizar el principal uso de blockchain, las criptomonedas, y sus principales variantes.

RESULTADOS DE APRENDIZAJE

- Aplicar conceptos de criptografia para construir una blockchain ad-hoc
- Registrar transaciones en blockchain publicos. Por ejemplo, criptomonedas.
- Diseñar e instanciar un smartcontract

BIBLIOGRAFÏA

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

Andreas M. Antonopoulos. 2014. Mastering Bitcoin: Unlocking Digital Crypto-Currencies (1st. ed.). O'Reilly Media, Inc.

Tomas Sander and Amnon Ta-Shma. Auditable, anonymous electronic cash. In Michael Wiener, editor, Advances in Cryptology — CRYPTO' 99, pages 555–572, Berlin, Heidelberg, 1999. Springer Berlin Heidelberg.

Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system," http://bitcoin.org/bitcoin.pdf.

Ian Miers, Christina Garman, Matthew Green, and Aviel D. Rubin. Zerocoin: Anonymous distributed e-cash from bitcoin. In Proceedings of the 2013 IEEE Symposium on Security and Privacy, SP '13, page 397–411, USA, 2013. IEEE Computer Society.

Eli Ben Sasson, Alessandro Chiesa, Christina Garman, Matthew Green, Ian Miers, Eran Tromer, and Madars Virza. Zerocash: Decentralized anonymous payments rom bitcoin. In Proceedings of the 2014 IEEE Symposium on Security and Pri-vacy, SP '14, page 459–474, USA, 2014. IEEE Computer Society.

Gavin Wood. Ethereum: A secure decentralised generalised transaction ledger. Ethereum project yellow paper, 151:1–32, 2014.

Corbet, Shaen. Understanding cryptocurrency fraud: The challenges and headwinds to regulate digital currencies, Berlin, Boston: De Gruyter, 2021. https://doi.org/10.1515/9783110718485

METODOLOGÍA DE ENSEÑANZA

Las clases comprenden instancias teórico-práctico. Los conceptos teóricos son presentados y desarrollados en las clases teóricas.

En las clases prácticas se profundizan y resuelven casos a partir de trabajos prácticos, que parten de lo trabajado en los teóricos. Adicionalmente existe un soporte virtual utilizando listas de correo o grupos para asistir a los alumnos de forma remota.

Se enfatiza la realización de actividades de laboratorio (construcción de prototipos, desarrollo de aplicaciones) con mucha interacción con la asignatura. Estas actividades se llevan a cabo en las salas de PC de la facultad.

EVALUACIÓN

La aprobación de la cursada se obtiene mediante la aprobación de distintas instancias de evaluación. En primer lugar se requiere la aprobación de los trabajos prácticos propuestos durante el curso y en segundo lugar se requiere la exposición de un tópico definido por la cátedra.

La evaluación final consiste en un examen escrito o la presentación de un trabajo final integrador para promocionar la materia.

CRONOGRAMA DE CLASES Y EVALUACIONES

Clase	Contenidos/Actividades
Semana 1	Introducción al blockchain. Contexto histórico, motivación, actualidad.
Semana 2	Breve introducción a la criptografía. Generación de claves públicas y privadas
Semana 3	Conceptos de aplicaciones distribuidas, centralizadas y descentralizadas. Principales implementaciones. Distributed Ledger Technologies (DLT).
Semana 4	Algoritmos de consenso, armado del blockchain y validación.
Semana 5	Introducción a Criptomonedas. Modelo UTXO,Transacciones, Merkle root. Generación de llaves. Minado.
Semana 6	Revisión de las criptomonedas más importantes Bitcoin, Bitcoin forks, Etherium, Altcoins (Dogecoin), Privacy-Focused Cryptocurrencies (Zcash)
Semana 7	Esquema de billeteras/wallets custodian vs non-custodian.
Semana 8	Introducción a smart contracts. Ejemplos.
Semana 9	Implementación de smart-contract en Solidity
Semana 10	NFT: Qué son y cómo funcionan.
Semana 11	Seguridad. Ataques, estafas, scams (Ponzi schemes, Dutch tulip frenzy, speculative bubbles)
Semana 12	Futuro y perspectives: temas de investigación en blockchain, crypomodedas y smart-contracts
Semana 13	Propuesta y selección de tópicos para la exposición final. ¿Cómo preparar y ofrecer una exposición oral?
Semana 14	Consulta y guía para la preparación de la exposición oral
Semana 15	Exposición oral del tema seleccionado
Semana 16	Exposición oral del tema seleccionado

Contacto de la cátedra (mail, sitio WEB, plataforma virtual de gestión de cursos):

matias.urbieta@lifia.info.unlp.edu.ar

Firma del/los profesor/es