

Carrera/ Plan:

***INTRODUCCIÓN A Blockchain,
Criptomonedas y Smart Contracts***

Licenciatura en Informática Plan 2015/Plan 2021
Licenciatura en Sistemas Plan 2015/Plan 2021

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 Urbietta

Hs semanales teoría: 3 hs

Hs semanales práctica: 3 hs

Año 2026

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, Ethereum, 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 criptografía para construir una blockchain ad-hoc
- Registrar transacciones en blockchain públicos. Por ejemplo, criptomonedas.
- Diseñar e instanciar un smartcontract

BIBLIOGRAFÍA

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 from bitcoin. In Proceedings of the 2014 IEEE Symposium on Security and Privacy, 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>

Babbush, Ryan & Zalcman, Adam & Gidney, Craig & Broughton, Michael & Khattar, Tanuj & Neven, Hartmut & Bergamaschi, Thiago & Drake, Justin & Boneh, Dan. (2026). Securing Elliptic Curve Cryptocurrencies against Quantum Vulnerabilities: Resource Estimates and Mitigations. 10.48550/arXiv.2603.28846.

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 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. Introducción a Criptomonedas. Modelo UTXO, Transacciones, Merkle root. Generación de llaves. Minado. Esquema de billeteras/wallets custodian vs non-custodian.
Semana 2	Laboratorio de Bitcoin - gestión de wallets y transferencias.
Semana 3	Algoritmos de consenso, armado del blockchain y validación. Criptografía y ataques a blockchains. Seguridad. Ataques, estafas, scams (Ponzi schemes, Dutch tulip frenzy, speculative bubbles)
Semana 4	Laboratorio Gestión del “vuelto” en transacciones y ataque de double spend
Semana 5	Introducción a Ethereum - Capas de consenso y ejecución. Introducción a smart contracts. Implementación de smart-contract en Solidity. Ejemplos.
Semana 6	Laboratorio de gestión de wallets Ethereum y despliegues de smart-contracts en la red testnet Sepolia.
Semana 7	Vulnerabilidades en smart-contracts y consumo de GAS.
Semana 8	Laboratorio: Exploits en smart-contracts.
Semana 9	Privacidad en blockchains. Introducción a Zcash y Monero. Transacciones transparentes y blindadas. Introducción a red TOR
Semana 10	Laboratorio de TOR y ZCash
Semana 11	Requerimientos de software en wallets custodian y patrones de usabilidad. Revisión de principales casos de uso.
Semana 13	Post-quantum blockchain, quantum-resistant algorithms (PQC) y ataques quantum a blockchains Pre-quantum.
Semana 14	Futuro y perspectivas: temas de investigación en blockchain, cryptomonedas y smart-contracts Propuesta y selección de tópicos para la exposición final. ¿Cómo preparar y ofrecer una 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@lifa.info.unlp.edu.ar

Firma del/los profesor/es

Prof. Matías Urbietta