RESOLUCIÓN 25/18/200-00
ACTA 1226/25/08/2025

"POR LA CUAL SE APRUEBA EL PROGRAMA DE ESTUDIO DE LA ASIGNATURA *TECNOLOGÍAS DE BLOCKCHAIN*, DE CARRERAS DE GRADO, SEDE SAN LORENZO, FILIAL VILLARRICA Y FILIAL CORONEL OVIEDO"

VISTO: El Memorando DA/1707/2025 del Director Académico de la FP-UNA, Prof. MSc. Felipe Santiago Uzabal Escurra, con el cual remite el Memorando CCPTCC/030/2025 de la Comisión Coordinadora del Proyecto de Transformación Curricular de Carreras de Grado de la FP-UNA, en el que presenta la propuesta de Programa de Estudio de Asignatura de las Carreras de Grado.

CONSIDERANDO: La Ley 4995/2013 de Educación Superior, el Estatuto de la Universidad Nacional de Asunción y las deliberaciones sobre el tema.

Que la Comisión Coordinadora del Proyecto de Transformación Curricular de Carreras de Grado, solicita la aprobación del Programa de Estudio de la asignatura **"Tecnologías de Blockchain",** la cual es común entre Carreras de Grado.

Que los programas fueron elaborados conforme a las disposiciones establecidas por el Consejo Nacional de Educación Superior (CONES) en materia de **créditos académicos**, según lo dispuesto en la Resolución CONES N.° 221/2024, que regula el *Sistema de Créditos Académicos – Paraguay* y los criterios para su publicación en las carreras de grado.

EL CONSEJO DIRECTIVO DE LA FACULTAD POLITÉCNICA
RESUELVE:

25/18/200-01 APROBAR el Programa de Estudio de la Asignatura **"Tecnologías de Blockchain",** de carreras de Grado, Sede San Lorenzo, Filial Villarrica y Filial Coronel Oviedo, detallado en el ANEXO 162 de la presente Acta.

25/18/200-02 COMUNICAR, copiar y archivar.

Prof. Abg. Joel Arsenio Benítez Santacruz
Secretario

Prof. Ing. Silvia Teresa Leiva León, MSc.
Presidenta

TEL/FAX: +595 21 5887000 – C.C. 1130 (Asunción) – 2111 (San Lorenzo)
www.pol.una.py

DEPARTAMENTO DE ENSEÑANZA DE INFORMÁTICA
PROGRAMA DE ESTUDIO

I. IDENTIFICACIÓN

Nivel	Grado				
Asignatura	Tecnologías de Blockchain				
Carrera	**Plan**	**Sede/Filial**	**Carácter**	**Semestre**	**Prerrequisitos**
Ingeniería en Informática	2026	Sede San Lorenzo	Electiva 2, 3 o 4	***	Ingeniería de Software 1, Bases de Datos 2, Programación de Aplicaciones 2, Seguridad Informática, Algoritmos Numéricos.
Licenciatura en Ciencias Informáticas	2026	Sede San Lorenzo/Filial Villarrica/Filial Coronel Oviedo	Electiva	***	Ingeniería de Software I, Base de Datos II, Seguridad Informática, Programación Frontend.

Semanal					**Periodo**				
HT	**HP**	**HTD**	**HTI**	**HS**	**PA**	**THTD**	**THTI**	**THA**	**CA-PY**
2	2	4	4	8	18	72	72	144	5

***HT: Horas Teóricas semanales.**
***HP: Horas Prácticas semanales.**
***HTD: Horas semanales de Trabajo académico con acompañamiento Docente.**
***HTI: Horas semanales de Trabajo académico Independiente del estudiante.**
***HS: Horas Semanales (HTD+HTI).**
***PA: Periodo Académico en semanas.**
*** THTD: Total de Horas de Trabajo académico con acompañamiento Docente (HTD*PA).**
*** THTI: Total de Horas de Trabajo académico Independiente del estudiante (HTI*PA).**
*** THA: Total de Horas de trabajo Académico (THTD+THTI).**
*** CA-PY: Créditos académicos de la asignatura.**

II. FUNDAMENTACIÓN

La tecnología blockchain, o cadena de bloques en español, es un registro compartido e inmutable que facilita el registro de transacciones en línea y el rastreo de activos. Blockchain surgió con la necesidad de realizar intercambios de dinero P2P de forma anónima y privada, sin embargo, en la actualidad está encontrando muchas aplicaciones en el intercambio de activos digitales, contratos inteligentes, videojuegos, finanzas distribuidas, por nombrar algunas. En la Web 3.0, blockchain resulta ser un componente principal permitiendo nuevas aplicaciones y servicios.

En esta asignatura se introduce al estudiante a todo el ecosistema de tecnologías que conciernen a blockchain, desde un punto de vista técnico. De esta forma, el estudiante podrá construir sus propias aplicaciones descentralizadas y estará preparado para adaptarse a los cambios que requiere esta tecnología.

La gran adopción que se está realizando de la tecnología blockchain a nivel mundial requiere de profesionales que sepan adaptarse a los vertiginosos cambios y que estén preparados para construir aplicaciones descentralizadas.

En relación a la naturaleza de la asignatura, se aborda de manera teórico-práctica, se combinarán conceptos teóricos con ejercicios prácticos. La organización de la asignatura se basa en los ejes temáticos, se incluyen conceptos fundamentales como: Fundamentos de blockchain. Criptografía en blockchain. Estructura de datos: bloques y cadenas. Protocolos de consenso. Redes públicas versus privadas. Contratos inteligentes. Plataformas blockchain. Desarrollo de aplicaciones descentralizadas. Interacción con APIs. Casos de uso y aplicaciones reales. Tendencias futuras y desafíos.

III. COMPETENCIAS DEL PERFIL DE EGRESO ASOCIADAS

1. Liderar y trabajar en equipo con eficacia y responsabilidad tomando decisiones basadas en evidencias.

2. Evaluar el comportamiento de diversos fenómenos disciplinares e interdisciplinares relacionados con la informática con una visión de sistema, mediante modelos teóricos validados y actualizados, capaces de abarcarlos integralmente en un contexto de incertidumbre.

3. Seleccionar, utilizar y construir instrumentos innovadores asociados al ejercicio de la informática.

4. Aplicar, producir y difundir conocimientos técnicos y científicos en el área de la informática.

5. Planificar, proyectar, diseñar y ejecutar proyectos sostenibles e integrales para la resolución de problemas, la mejora y la innovación en el ámbito de la informática.

6. Interpretar, modelar y comunicar información referida a la informática en forma gráfica.

IV. ORGANIZACIÓN DE LA ASIGNATURA

Unidades	Contenidos	Resultados de aprendizaje
1. Arquitectura Blockchain.	1.1. Arquitectura general. 1.2. Introducción a la criptografía computacional. 1.2.1. Seguridad semántica. 1.2.2. Funciones One-Way. 1.2.3. Hash criptográfico. 1.2.4. Árboles de Merkle. 1.2.5. Firma digital. 1.2.6. Commitments. 1.2.7. Proof-of-Work. 1.3. Protocolos de Consenso. 1.3.1. El problema del doble gasto. 1.3.2. Consenso 1.3.2.1. Modelos de red. 1.3.2.2. Tolerancia a corrupciones. 1.3.2.3. Acuerdo bizantino. 1.3.2.4. Protocolo Strong-Dolev. 1.3.2.5. Consenso blockchain.	1. Explica los fundamentos y la arquitectura general de los sistemas criptográficos y blockchain. 2. Analiza y aplica conceptos clave de criptografía computacional, incluyendo seguridad semántica, funciones one-way, y hash criptográfico. 3. Implementa y evalúa mecanismos de firma digital y árboles de Merkle. 4. Describe y compara diferentes protocolos de consenso utilizados en sistemas blockchain, incluyendo Proof-of-Work y Proof-of-Stake. 5. Analiza el problema del doble gasto y explica cómo lo resuelven los sistemas blockchain.

Unidades	Contenidos	Resultados de aprendizaje
	1.3.2.6. Consenso de Nakamoto. 1.3.2.7. Seguridad. 1.3.2.8. Ataques. 1.3.2.9. Incentivos. 1.3.2.10. Consenso en Ethereum. 1.3.2.11. Casper 1.3.2.12. Ghost 1.3.2.13. Proof-of-Stake 1.4. Redes de Capa 2. 1.4.1. Rollups. 1.4.2. Computación verificable.	6. Evalúa los modelos de red y la tolerancia a corrupciones en sistemas distribuidos. 7. Implementa y analiza el protocolo de acuerdo bizantino y el protocolo Strong-Dolev. 8. Compara y contrasta el consenso blockchain y el consenso de Nakamoto. 9. Identifica y evalúa las vulnerabilidades de seguridad y los posibles ataques en sistemas blockchain. 10. Analiza los mecanismos de incentivos en sistemas blockchain como Bitcoin y Ethereum. 11. Explica y evalúa las propuestas de consenso en Ethereum, incluyendo Casper y Ghost. 12. Describe y analiza las soluciones de escalabilidad en blockchain, incluyendo redes de capa 2 y rollups]. 13. Explica los principios de la computación verificable y su aplicación en sistemas blockchain. 14. Diseña e implementa sistemas criptográficos seguros utilizando técnicas y protocolos modernos. 15. Evalúa críticamente las implicaciones éticas y legales del uso de criptografía y tecnología blockchain.
2. Contratos inteligentes	2.1. Introducción a los contratos inteligentes 2.1.1. Remix IDE 2.2. Solidity 2.2.1. Tipos de datos. 2.2.2. Condicionales y bucles. 2.2.3. Modificadores de acceso. 2.2.4. Depósitos y retiros. 2.2.5. Metamask.	1. Comprende los conceptos básicos de los contratos inteligentes y su importancia en la tecnología blockchain. 2. Familiariza el entorno de desarrollo Remix IDE para la creación y prueba de contratos inteligentes. 3. Adquiere conocimientos fundamentales del lenguaje de programación Solidity, utilizado para desarrollar contratos inteligentes en Ethereum. 4. Identifica y utiliza correctamente los diferentes tipos de datos en Solidity, incluyendo enteros, booleanos, direcciones y estructuras. 5. Aplica estructuras de control como condicionales y bucles para crear lógica compleja en contratos inteligentes. 6. Comprende e implementa adecuadamente los modificadores

Unidades	Contenidos	Resultados de aprendizaje
		de acceso para controlar la visibilidad y accesibilidad de funciones y variables en los contratos. 7. Desarrolla funciones para manejar depósitos y retiros de forma segura en contratos inteligentes. 8. Integra y utiliza MetaMask para interactuar con contratos inteligentes y realizar transacciones en la red Ethereum. 9. Crea, compila y despliega contratos inteligentes básicos utilizando Remix IDE y Solidity. 10. Implementa buenas prácticas de seguridad en el desarrollo de contratos inteligentes para prevenir vulnerabilidades comunes. 11. Diseña y ejecuta pruebas para verificar el correcto funcionamiento de los contratos inteligentes desarrollados.
3. Aplicaciones descentralizadas.	3.1. Definición de DApp. 3.2. Tokens ERC20, ERC721. 3.3. Ethereum API. 3.4. Truffle, Hardhat, Forge. 3.5. DeFi. 3.6. DePIN. 3.7. IA Descentralizada.	1. Define y explica el concepto de aplicaciones descentralizadas (DApps) y su funcionamiento en una blockchain. 2. Compara y contrasta los tokens ERC20 y ERC721, incluyendo sus características, usos y diferencias clave. 3. Describe las principales bibliotecas y herramientas de API de Ethereum para desarrollar aplicaciones blockchain, como Web3.js y Ethers.js. 4. Identifica y explica el propósito de frameworks de desarrollo como Truffle, Hardhat y Forge en el ecosistema Ethereum. 5. Define las finanzas descentralizadas (DeFi) y explica sus principios fundamentales y aplicaciones. 6. Analiza el concepto de redes de infraestructura física descentralizada (DePIN) y su potencial impacto en diversos sectores. 7. Explora el concepto emergente de inteligencia artificial descentralizada y sus posibles aplicaciones en el contexto blockchain. 8. Comprende la importancia de los contratos inteligentes en el funcionamiento de DApps y

Unidades	Contenidos	Resultados de aprendizaje
		protocolos DeFi. 9. Identifica los principales desafíos y ventajas de los sistemas descentralizados en comparación con sus contrapartes centralizadas. 10. Evalúa el papel de los tokens criptográficos en la incentivación y gobernanza de ecosistemas descentralizados.

V. ESTRATEGIAS DIDÁCTICAS

En el desarrollo del programa se aplicarán estrategias didácticas conducentes a la apropiación teórica y la ejecución práctica de procesos y procedimientos, a saber:

- **Debate:** exposición por parte del docente de los conceptos básicos por unidad, con materiales de lectura y ejemplos orientados a la enseñanza de las competencias específicas de la asignatura. El docente asume el rol de expositor y buscará generar el debate a través de preguntas sobre lo expuesto y desde la participación de los estudiantes.

- **Solución de problemas:** se plantean problemas de benchmark y reales para la aplicación de técnicas aprendidas a la solución de estos, de manera a permitir realizar prácticas de aplicación a los estudiantes utilizando entornos y datos reales, y verificando el comportamiento de las técnicas estudiadas en diversos entornos y problemáticas.

- **Trabajos Colaborativos:** se realizarán trabajos prácticos por temáticas en equipos, se busca la cooperación y el trabajo grupal, incentivando la designación de roles y responsabilidades dentro de un equipo de trabajo, el compromiso grupal para el logro del objetivo del trabajo y la práctica de aplicación de la teoría a problemas reales para permitir validar la teoría con la práctica.

- **Estudios de casos:** se presentan varios estudios de casos de investigación que han aplicado diferentes técnicas estudiadas, permite identificar al estudiante un escenario real de aplicación de las técnicas aprendidas, comprender la manera de cómo encarar la resolución de un problema en un escenario real y aprender en base a la experiencia previa de trabajos de investigación publicados.

La elección particular de la estrategia didáctica aplicada será explícita en el Planeamiento de la Asignatura, de acuerdo con el perfil de los estudiantes, los recursos disponibles y el contexto educativo.

VI. ESTRATEGIAS EVALUATIVAS

Procesos de producción grupales e individuales, pruebas individuales orales y/o escritas durante el desarrollo de las unidades con diálogos e interpretaciones que los estudiantes realicen sobre los contenidos, debates, retroalimentación en casos necesarios y actividades que amplíen el conocimiento.

Con fines de calificación y promoción se aplicará el Reglamento Académico vigente en la institución que prevé valoraciones de proceso y final.

VII. MEDIOS AUXILIARES

Pizarras, marcadores, computadoras, proyector, parlantes para multimedia, plataforma virtual, sala de laboratorio equipada para prácticas con sistemas operativos Linux o Windows y acceso a Internet.

VIII. BIBLIOGRAFÍA

- Narayana, A.; Bonneau, J.; Felten, E.; Miller, A.; Goldfeder, S. (2016) Bitcoin and Cryptocurrency Technologies: A ComprehensiveIntroduction. Princeton UniversityPress.
- Shi, E. (2020) Foundations of DistributedConsensus and Blockchains. http://elaineshi.com/docs/blockchain-book.pdf
- BitcoinDeveloperGuide. https://developer.bitcoin.org/reference/
- Nakamoto, S. (2008) Bitcoin: A Peer-to-Peer Electronic Cash System.
- Chan, B. Y., &Shi, E. (2020, October). Streamlet: Textbookstreamlinedblockchains. In Proceedings of the 2nd ACM ConferenceonAdvances in Financial Technologies (pp. 1-11). https://eprint.iacr.org/2020/088
- Ren, L. (2019). Analysis of nakamotoconsensus. CryptologyePrint Archive. https://eprint.iacr.org/2019/943
- Dembo, A., Kannan, S., Tas, E. N., Tse, D., Viswanath, P., Wang, X., &Zeitouni, O. (2020, October). Everythingis a race and Nakamotoalwayswins. In Proceedings of the 2020 ACM SIGSAC ConferenceonComputer and Communications Security (pp. 859-878). https://arxiv.org/abs/2005.10484
- Sheng, P., Wang, G., Nayak, K., Kannan, S., &Viswanath, P. (2021, November). BFT protocolforensics. In Proceedings of the 2021 ACM SIGSAC conferenceoncomputer and communicationssecurity (pp. 1722-1743). https://arxiv.org/pdf/2010.06785.pdf
- Neu, J., Tas, E. N., &Tse, D. (2021, May). Ebb-and-flowprotocols: A resolution of theavailability-finalitydilemma. In 2021 IEEE Symposiumon Security and Privacy (SP) (pp. 446-465). IEEE. https://arxiv.org/abs/2009.04987
- Ethereum White Paper. https://github.com/ethereum/wiki/wiki/White-Paper
- Wood, G. (2014). Ethereum: A securedecentralisedgeneralisedtransactionledger. Ethereumprojectyellowpaper, 151(2014), 1-32. http://gavwood.com/paper.pdf
- Solidітydocumentation. https://docs.soliditylang.org/en/latest/
- Ito, K., Mita, M., Ohsawa, S., &Tanaka, H. (2020). Whatisstablecoin?: A surveyonitsmechanism and potential as decentralizedpaymentsystems. International Journal of Service and Knowledge Management, 4(2), 71-86. https://arxiv.org/pdf/1906.06037.pdf
- Kahya, A., Krishnamachari, B., &Yun, S. (2021). ReducingtheVolatility of Cryptocurrencies--A Survey of Stablecoins. arXivpreprint arXiv:2103.01340. https://arxiv.org/ftp/arxiv/papers/2103/2103.01340.pdf
- Uniswapwhitepaper. https://arxiv.org/ftp/arxiv/papers/2103/2103.01340.pdf
- Qin, K., Zhou, L., Livshits, B., &Gervais, A. (2021, March). Attackingthedefiecosystemwith flash loansforfun and profit. In International ConferenceonFinancialCryptography and Data Security (pp. 3-32). Springer, Berlin, Heidelberg. https://arxiv.org/abs/2003.03810
- Dunaif, G.; Boneh, D. How to Build a Private DAO onEthereum. https://hackmd.io/nCASdhqVQNWwMhpTmKpnKQ.