UNIVERSIDAD NACIONAL DE ASUNCIÓN
FACULTAD POLITÉCNICA
INGENIERÍA EN INFORMÁTICA
PLAN 2008
PROGRAMA DE ESTUDIOS

Resolución 24/02/83-00 Acta 1184/31/01/2024 - ANEXO 05

I. - IDENTIFICACIÓN

1.	Asignatura	: Electiva 4 o 5 – Blockchain.
2.	Semestre	: Noveno.
3.	Horas semanales	: 7 horas.
	3.1. Clases teóricas	: 3 horas.
	3.2. Clases prácticas	: 4 horas.
4.	Total real de horas disponibles	: 112 horas.
	4.1. Clases teóricas	: 48 horas.
	4.2. Clases prácticas	: 64 horas.

II. - JUSTIFICACIÓN

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.

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, esto incluye al futuro ingeniero en informática, por lo que con el desarrollo de esta asignatura se pretende introducir al estudiante a todo el ecosistema de tecnologías que conciernen a blockchain, desde un punto de vista técnico, para de esta forma pueda estar preparado para adaptarse a los cambios que requiere esta tecnología.

III. - OBJETIVOS

1. Relacionar conceptos de criptografía computacional necesarios para un entendimiento de las tecnologías blockchain.
2. Discernir conceptos de consenso distribuido necesarios para un entendimiento de las tecnologías blockchain.
3. Abstraer los detalles técnicos de las diferentes capas de una computadora blockchain.
4. Determinar los diferentes algoritmos que hacen funcionar a una computadora blockchain.
5. Comprender el rol de la criptografía, la economía y los sistemas distribuidos en una arquitectura de blockchain.
6. Distinguir las diferentes aplicaciones que surgen de blockchain: DeFi, NFTs, criptomonedas, DAOs.
7. Construir aplicaciones descentralizadas.

IV. - PRE – REQUISITO

1. 70% de créditos aprobados y haber realizado 300 horas de pasantía.

V. - CONTENIDO

5.1. Unidades programáticas

1. Arquitectura Blockchain.
2. Contratos Inteligentes.
3. Aplicaciones descentralizadas.

UNIVERSIDAD NACIONAL DE ASUNCION FACULTAD POLITECNICA 1979 CONSTRUYENDO EL FUTURO

5.2. Desarrollo de las unidades programáticas

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.
        1.3.3. Consenso de Nakamoto.
            1.3.3.1. Seguridad.
            1.3.3.2. Ataques.
            1.3.3.3. Incentivos.
        1.3.4. Proof-of-Stake
    1.4. Redes de Capa 2.
        1.4.1. Rollups.
        1.4.2. Computación verificable.
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.
3. Aplicaciones descentralizadas.
    3.1. Definición de DApp.
    3.2. Tokens ERC20, ERC721.
    3.3. Ethereum API.
    3.4. Truffle.

VI. - ESTRATEGIAS METODOLÓGICAS

1. Clases expositivas participativas.
2. Técnicas individuales y grupales para la resolución de ejercicios.
3. Trabajos prácticos de programación.
4. Realización y presentación de proyecto final.

VII. - MEDIOS AUXILIARES

1. Pizarra.
2. Marcadores y borrador de pizarra.
3. Equipo multimedia.

4. Bibliografía de apoyo.
5. Aula virtual.

VIII. - EVALUACIÓN

- Acorde a las reglamentaciones y normativas vigentes en la Facultad Politécnica-UNA.

IX. - BIBLIOGRAFÍA

1. Básica

- Narayana, A.; Bonneau, J.; Felten, E.; Miller, A.; Goldfeder, S. (2016) Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction. Princeton University Press.
- Shi, E. (2020) Foundations of Distributed Consensus and Blockchains. Disponible en: http://elaineshi.com/docs/blockchain-book.pdf
- Bitcoin Developer Guide. Disponible en: https://developer.bitcoin.org/reference/
- Chan, B. Y., & Shi, E. (2020, October). Streamlet: Textbook streamlined blockchains. In *Proceedings of the 2nd ACM Conference on Advances in Financial Technologies* (pp. 1-11). Disponible en: https://eprint.iacr.org/2020/088
- Ren, L. (2019). Analysis of nakamoto consensus. *Cryptology ePrint Archive*. Disponible en: https://eprint.iacr.org/2019/943
- Dembo, A., Kannan, S., Tas, E. N., Tse, D., Viswanath, P., Wang, X., & Zeitouni, O. (2020, October). Everything is a race and Nakamoto always wins. In *Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security* (pp. 859-878). Disponible en: https://arxiv.org/abs/2005.10484
- Sheng, P., Wang, G., Nayak, K., Kannan, S., & Viswanath, P. (2021, November). BFT protocol forensics. In *Proceedings of the 2021 ACM SIGSAC conference on computer and communications security* (pp. 1722-1743). Disponible en: https://arxiv.org/pdf/2010.06785.pdf
- Ito, K., Mita, M., Ohsawa, S., & Tanaka, H. (2020). What is stablecoin?: A survey on its mechanism and potential as decentralized payment systems. *International Journal of Service and Knowledge Management*, *4*(2), 71-86. Disponible en: https://arxiv.org/pdf/1906.06037.pdf
- Kahya, A., Krishnamachari, B., & Yun, S. (2021). Reducing the Volatility of Cryptocurrencies--A Survey of Stablecoins. *arXiv preprint arXiv:2103.01340*. Disponible en: https://arxiv.org/ftp/arxiv/papers/2103/2103.01340.pdf
- Uniswap whitepaper. Disponible en: https://arxiv.org/ftp/arxiv/papers/2103/2103.01340.pdf
- Qin, K., Zhou, L., Livshits, B., & Gervais, A. (2021, March). Attacking the defi ecosystem with flash loans for fun and profit. In *International Conference on Financial Cryptography and Data Security* (pp. 3-32). Springer, Berlin, Heidelberg. Disponible en: https://arxiv.org/abs/2003.03810

2. Complementaria

- Nakamoto, S. (2008) Bitcoin: A Peer-to-Peer Electronic Cash System.
- Tanenbaum, A. S., & Wetherall, D. J. (2012). *Redes de computadora* (Quinta ed.). México: Pearson Educación.
- Ethereum White Paper. Disponible en: https://github.com/ethereum/wiki/wiki/White-Paper
- Neu, J., Tas, E. N., & Tse, D. (2021, May). Ebb-and-flow protocols: A resolution of the availability-finality dilemma. In *2021 IEEE Symposium on Security and Privacy (SP)* (pp. 446-465). IEEE. Disponible en: https://arxiv.org/abs/2009.04987
- Dunaif, G.; Boneh, D. How to Build a Private DAO on Ethereum. Disponible en: https://hackmd.io/nCASdhqVQNWwMhpTmKpnKQ
- Wood, G. (2014). Ethereum: A secure decentralised generalised transaction ledger. *Ethereum project yellow paper*, *151*(2014), 1-32. Disponible en: http://gavwood.com/paper.pdf
- Solidity documentation. Disponible en: https://docs.soliditylang.org/en/latest/