Blockchains: Aspectos teóricos y prácticos

Dr. Juan Garay (Profesor visitante, Texas A&M University, Estados Unidos) & Esteban Mocskos (Profesor, FCEyN, UBA)

Programa:

Las Blockchains han generado mucha atención, no solo por sus características innovadoras, sino porque han logrado dar sustento a instrumentos financieros que no requieren de terceras parte de confianza (*trusted intermediaries*) tales como Bitcoin y otras *ledgers* descentralizadas, así como otras aplicaciones, tales como *smart contracts*, sistemas de reputación, servicios de nombres, y *digital assets* (NFTs). También emergen como una alternativa para resolver problemas clásicos de cómputo distribuido tolerante a fallas, tal como llegar a un consenso distribuido en presencia de actores potencialmente maliciosos.

Sin embargo, la solidez y seguridad de estas aplicaciones dependen del entendimiento de propiedades fundamentales de la estructura de datos subyacente: la *blockchain*.

La blockchain es mantenida y extendida por actores que son elegidos por distintas estrategias de selección, tales como generar una prueba de trabajo por medio de resolver un problema computacionalmente intensivo (*proof of work*) o demostrando a otros su interés y compromiso con el sistema (*proof of stake*).

Este curso cubre tanto los aspectos fundamentales y prácticos de las *blockchains* junto con sus aplicaciones. Para cubrir el primer aspecto, se formularán las propiedades que debe cumplir una *blockchain* y qué características de las aplicaciones pueden cumplir en base a las hipótesis de funcionamiento y herramientas criptográficas que emplean. El segundo objetivo será cubierto por medio del uso de una red privada basada en Ethereum, que es un sistema cuyo objetivo es permitir realizar pruebas de concepto sin involucrar valor verdadero en sus transacciones. En este sistema se desarrollarán trabajos prácticos que irán desde simples transferencias entre cuentas hasta entender el diseño y desarrollo de *smart contracts* de complejidad creciente.

Al terminar este curso, se espera que los alumnos puedan:

- Entender las propiedades y técnicas usadas en los protocolos de las *blockchains*, incluyendo los diversos mecanismos de prueba de esfuerzo.
- Poder escribir *smart contracts* en Solidity (el lenguaje de programación usado en Ethereum).
- Poder entender y proponer aplicaciones y mejoras a protocolos de *blockchain*.
- Leer, analizar, resumir y presentar trabajos de investigación recientes relacionados a *blockchain*.

Temario:

- Introducción a *blockchains*, *ledgers* distribuidas, modelos de cómputo.
- Elementos matemáticos necesarios y repaso de criptografía.
- Proof of work (PoW): estructuras de datos relevantes.
- La blockchain como plataforma: transacciones en Bitcoin, *smart contracts*, replicación de máquinas de estado, transacciones en Ethereum.
- Vulnerabilidades en contratos: *Denial of Service*, *Overflow/Underflow*, *Reentrancy*, DAO.
- El problema del consenso: consenso estándar, consenso de Nakamoto.

- Practical Byzantine Fault Tolerance (PBFT): ledgers con y sin permisos, VRFs (*Verifiable Random Functions*), *proof of stake* (PoS), blockchain de Algorand.
- *Ledgers* distribuidas vis à vis replicación de máquinas de estado: consistencia, persistencia, *liveness*.
- Bloque génesis impredecible y *bootstrapping* de una *blockchain*: suposiciones iniciales y resultados acerca de su factibilidad, criptografía restringida por los recursos.
- Anonimato y privacidad en protocolos de blockchain: anonimato y pseudo-anonimato, privacidad en Bitcoin, seguridad de la red, billeteras.
- Cómputo seguro multi-agente: compartir de manera segura, *threshold signatures*.
- Aplicaciones de las *ledgers* distribuidas. Economía digital (en blockchain) – distintos ejemplos y finanzas descentralizadas.

Bibliografía

- J. Garay, A. Kiayias and N. Leonardos, "The Bitcoin Backbone Protocol: Analysis and Applications." Proc. Eurocrypt 2015. Available from the Cryptology ePrint Archive, https://eprint.iacr.org/2014/765.
- J. Garay and A. Kiayias, "SoK: A Consensus Taxonomy in the Blockchain Era." Proc. CT-RSA 2020. Full version available from the Cryptology ePrint Archive, https://eprint.iacr.org/2018/754.
- J. Chen and S. Micali, "Algorand: A secure and efficient distributed ledger." Theor. Comput. Sci. 777: 155-183 (2019).
- "Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction" (Princeton University Press), by A. Narayanan, J. Bonneau, E. Felten, A. Miller and S. Goldfeder. Preliminary version available as "SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies," J. Bonneau, A. Miller A, J. Clark, A. Narayanan, J. Kroll and E. Felten, and as a freely available preprint here.
- "Principles of Blockchain Systems," A. Fernández Anta, C. Georgiu, M. Herlihy and M. Potop-Butucaru (Eds.), Synthesis Lectures on Computer Science, Morgan and Claypool Publishers, 2021.
- C. Badertscher, J. Garay, U. Maurer, D. Tschudi and V. Zikas, "But Why Does It Work? A Rational Protocol Design Treatment of Bitcon." Proc. Eurocrypt 2018. Available from the Cryptology ePrint Archive, https://eprint.iacr.org/2018/138.
- "Introduction to Modern Cryptography, Second Edition" (Chapman & Hall/CRC Cryptography and Network Security Series), by J. Katz and Y. Lindell.
- J. Garay, A. Kiayias, N. Leonardos and G. Panagiotakos, "Bootstrapping the Blockchain, with Applications to Consensus and Fast PKI Setup." Proc. PKC 2018. Available from the Cryptology ePrint Archive, https://eprint.iacr.org/2016/991.