Viaje al centro de las criptomonedas

Francisco Rodríguez-Henríquez
Departamento de Computación
CINVESTAV-IPN

Resumen En esta charla se presenta un recuento de la procelosa historia de las criptomonedas, desde sus inicios en los años ochenta del siglo pasado con el trabajo pionero de David Chaum en dinero digital centralizado, hasta el triunfo del dinero digital distribuido propuesto por Satoshi Nakamoto en octubre de 2008. Se explica la maquinaria criptográfica que permite el correcto funcionamiento de las criptomonedas evitando el problema del doble gasto mediante el uso de sus cadenas de blo- ques Blockchain y protocolos de consenso. En la segunda parte de esta presentación se describen nuevas primitivas criptográficas tales como las funciones de retraso verificable (VDF por sus siglas en inglés), las cuales se espera que permitan substituir la onerosa prueba de trabajo de Nakamoto por las computacionalmente más baratas y ecológicas pruebas de tiempo y espacio.

Francisco Rodríguez-Henríquez

Francisco Rodríguez-Henríquez obtuvo el grado de doctor en junio del 2000 en el departamento de ingeniería eléctrica y computación de la Universidad Oregon State en Estados Unidos.

De julio de 2000 a mayo de 2002 el doctor Rodríguez-Henríquez trabajó en compañías de seguridad informáticas de Estados Unidos y Alemania. A partir de mayo del 2002, el Dr. Rodríguez-Henríquez colabora con el Departamento de Computación del CINVESTAV-IPN en la ciudad de México, donde actualmente es profesor titular 3-D. Es co-autor de más de 80 artículos técnicos y capítulos de libro. Asimismo, él es el primer autor del libro: *"Cryptographic Algorithms on Reconfigurable Hardware"*, publicado por Springer en noviembre del 2006.

Sus principales áreas de investigación son criptografía, aritmética computacional y seguridad informática. En su grupo de investigación, junto a sus tesistas de posgrado y colaboradores internacionales, el doctor Rodríguez-Henríquez ha obtenido varios récords de velocidad en implementaciones de algoritmos criptográficos basados en curvas elípticas, así como el récord mundial del quebramiento del logaritmo discreto para campos finitos de característica tres, el cual fue calculado utilizando la súper computadora Abacus del Cinvestav en julio del 2016. El Dr. Rodríguez-Henríquez es cofundador de la conferencia internacional en criptología y seguridad de la información (Latincrypt) y de la Escuela Avanzada de Criptología (ASCrypto), cuyas primeras ediciones fueron celebradas en Puebla en 2010 y en Sao Paulo en 2011, respectivamente.