Matemáticas en La Corrala (3ed)

Es para todos los públicos: sólo hace falta un poco de curiosidad

Matemáticas del anonimato y el consenso: Bitcoin y Blockchain

Anna Rio Doval

Universitat Politècnica de Catalunya

Jueves 4 de abril, 19:30

Colegio Mayor Juan Luis Vives (UAM)

Calle Francisco Suárez 7, Madrid

Resumen. Internet es hoy una red digital interconectada de intercambio de información convertida en herramienta imprescindible para el funcionamiento de la sociedad, desde múltiples aspectos de la vida cotidiana hasta el mundo de los negocios, pasando por los servicios públicos. La aparición de la tecnología Blockchain supone un paso en la evolución de la red: de la internet de la información a la internet del valor. Este nuevo concepto debe permitir compartir valor a través de la red, entendiendo por valor cualquier cosa (en formato digital) que tenga valor para alguien, ya sean archivos, certificaciones, transacciones, pólizas, votos, música, etc. El valor ha de poder intercambiarse con la misma libertad, inmediatez y facilidad que la información.

La internet del valor debe ser abierta y accesible, construida en base a la confianza y la seguridad. Debe ofrecer simultáneamente privacidad y transparencia. Debe ser una herramienta simple y con capacidad de adaptación, de estándares abiertos y no controlada por ninguna entidad centralizada. Por todo ello la tecnología Blockchain ha ido adquiriendo cada vez más popularidad.

Blockchain puede pensarse como un libro de registros que utiliza la criptografía para hacer que cada participante de la red pueda leer y escribir en él de forma segura, sin autoridad central que dé garantías. Puede considerarse como un medio para certificar y validar cualquier tipo de información. La validez de los datos registrados se certifica mediante el consenso descentralizado: para que la información se considere verificada debe obtener previamente el consenso del resto de usuarios de la red.

La criptomoneda Bitcoin, pionera en el uso de esta tecnología, une a este concepto de descentralización otra característica de gran impacto: el anonimato de las transacciones. No hay ninguna identificación "real" de los usuarios físicos, que pueden tener tantas direcciones (identidades) Bitcoin como deseen y darles la duración que estimen oportuna.

De entre la multitud de aplicaciones que pueden imaginarse (o que ya se empiezan a hacer realidad) una donde confluyen con fuerza los requerimientos de anonimato y descentralización es la votación electrónica.

En esta charla trataremos de ver cómo las matemáticas contribuyen a dar respuesta a todos estos requerimientos de anonimato, consenso descentralizado y transparencia que caracterizan la tecnología Blockchain.

La conferenciante. Anna Rio Doval es doctora en Matemáticas y profesora del Departamento de Matemáticas de la Universidad Politécnica de Cataluña. Sus líneas de investigación se desarrollan en el ámbito del Seminario de Teoría de Números de Barcelona, con diversos trabajos publicados sobre aspectos teóricos y computacionales de la teoría de curvas elípticas. Paralelamente ha impartido la asignatura de Criptografía en la Facultad de Informática desde el curso 97-98 y ha participado tanto en redes temáticas como en congresos de este ámbito.

Universidad Autónoma de Madrid