

CRIPTOMONEDAS: ¿EL DINERO DEL FUTURO?

Por Ana Gabriela Martínez A.

La irrupción de criptomonedas como Bitcoin y Ethereum está revolucionando la forma de realizar transacciones en Internet, abriendo interrogantes en torno a sus ventajas y a la masividad con que se podrían utilizar.

ACTUALIDAD

Un sistema de comercio electrónico que funciona a nivel mundial de manera independiente y descentralizada. Esa es la gran promesa de las criptomonedas, divisa digital cuya popularidad va en ascenso siendo hoy Bitcoin y Ethereum las más utilizadas entre las más de mil criptomonedas existentes.

Previo a su aparición, los sistemas de dinero electrónico se caracterizaban en su mayoría por depender de una entidad centralizada (similar a un banco) y por presentar problemas como la posibilidad del doble gasto. Durante años se plantearon soluciones para corregir esto, pero ninguna tuvo éxito. Recién en 2008, Satoshi Nakamoto –cuya identidad es aún un misterio– propuso una idea radical que dio vida a Bitcoin, criptomoneda cuyo valor hoy supera los siete mil dólares.

Satoshi creó una moneda que no depende de un gobierno u organización, cuya mayor innovación es la Blockchain, columna vertebral del sistema. En términos simples, es un libro contable distribuido donde se especifica el dinero que cada usuario tiene y las transacciones realizadas. Estas transacciones se agrupan en bloques que se van enlazando con los bloques

anteriores a través de un proceso que se conoce como ‘minar’ y en el que los ‘mineros’ deben resolver un puzle matemático: el primero que lo logra no sólo agrega un nuevo bloque a la cadena, sino también gana dinero. El académico del Departamento de Ciencias de la Computación, Alejandro Hevia, afirma que “ésta es la primera vez en Internet que tenemos un sistema de comercio electrónico global y casi sin costo, lo cual revoluciona las finanzas a nivel mundial”.

Sin embargo, sus potenciales beneficios también pueden ser potenciales problemas: “Por ejemplo no está claro cómo aplican regulaciones relativas al lavado de dinero u otras que buscan evitar el financiamiento de actividades ilegales”, dice. De hecho, si bien Bitcoin se puede utilizar para comprar productos y servicios, también se ha usado para solicitar pagos en casos de *ransomware*, tal como sucedió en mayo de 2017 tras el ciberataque Wannacry. ¿Se debe entonces regular su uso? A juicio del Profesor Hevia, esto podría provocar la pérdida de interés de parte de algunos usuarios que eventualmente podrían dejar el sistema o crear una red paralela, una nueva moneda. “Esto no es necesariamente bueno ni malo.

Sin embargo, pone en evidencia la filosofía tras las criptomonedas: frecuentemente se dice que el ‘código es la ley’ porque las reglas que parecen importar no son las del país de uso, sino aquellas que están programadas en el sistema y que fueron fijadas por los desarrolladores de la moneda”, señala el académico.

El revuelo causado por las criptomonedas también ha generado gran interés de investigación, particularmente en torno a la Blockchain, ya que según el Profesor Hevia puede convertirse en una base de datos mundial para múltiples nuevas aplicaciones, por ejemplo para guardar registros públicos, transformándose así en una especie de sitio web global. “Y ese es también uno de los principales problemas hoy –afirma– porque las instituciones financieras quieren usarla pero al estar más reguladas tienen que cumplir primero ciertos requisitos de privacidad. Además, las criptomonedas posibilitan ‘contratos inteligentes’, programas computacionales interactivos ejecutados en forma distribuida por la red de mineros, y que en teoría permiten crear empresas o servicios virtuales distribuidos, sin tener que confiar en nadie en particular”.



En este contexto, hoy el Profesor Alejandro Hevia trabaja con el alumno de Magíster, Francisco Montoto, en el desarrollo de un sistema que permita realizar apuestas sobre eventos externos a Bitcoin. “En las apuestas existen los oráculos, que son participantes de la Blockchain y ellos son los que deciden quién gana, son una especie de jueces que además obtienen dinero por ejercer esta función. Los oráculos son escogidos al azar dentro de los participantes. Cualquier miembro de Bitcoin puede ganar dinero como oráculo. Parte de nuestra investigación tiene que ver con cómo utilizar técnicas de criptografía para darle a la Blockchain esta nueva funcionalidad de arbitraje distribuido. Esto es nuevo, no existe al menos en Bitcoin y permitirá también resolver disputas, por ejemplo, contratos civiles” explicó el académico.

El futuro de las criptomonedas

Si bien las criptomonedas presentan un enorme potencial y la tecnología que la sustenta es sólida, el Profesor Hevia explica que aún no hay una comprensión cabal de “los factores que las hacen funcionar como aquello que las podría destruir. Es frecuente ver algo que es un riesgo y piensas que pueden colapsar, pero esto no ocurre. Y te das cuenta que los mismos participantes, ‘los mineros’, se autorregulan y hacen que no pase. Ese tipo de comportamiento no es fácil de modelar”.

Lo que sí está claro, es que hoy las criptomonedas están impactando el mundo financiero y muchas instituciones ya toman conciencia que es una tecnología que deberán incorporar. El problema

es cómo y bajo qué reglas: “¿están dispuestas las entidades financieras a ceder el control? –pregunta el Profesor Hevia-. Esto les significaría operar bajo las reglas de cada moneda. Más aún, un gran problema que tienen muchos países es que no hay clasificación clara respecto a qué es Bitcoin desde el punto de vista legal o de impuestos”. Sin embargo, hoy ya hay países como Japón que están avanzando y ofreciendo incentivos para incorporarlas. 

Contacto:
ahevia@dcc.uchile.cl