# Criptomonedas

Por Adair Chavez

Imaginemos que queremos hacer una moneda alternativa para nuestra nueva ecoaldea. La idea es darle a cada miembro una cantidad igual para empezar e intercambiarlo entre nosotros por bienes. El valor de ésta moneda depende totalmente de la comunidad que la usa.

Logísticamente lo más obvio/fácil sería crear un sistema de auditoría centralizado: un cuaderno. En éste cuaderno podemos anotar cada transacción para llevar un registro: Juan le da a Pedro 3 monedas. En cada renglón podemos escribir otra transacción. Todo funciona bien excepto por los problemas inherentes que vienen de un auditor central. Puede ser corrupto y anotar cosas que no son. Puede perder el control del cuaderno. Puede querer cobrar por auditar, etc.

Las criptomonedas resuelven el conflicto del auditor central haciendo a cada usuario un nodo de una red auditora. La idea fue propuesta por Satoshi Nakamoto en su artículo: "Bitcoin: A Peer-to-Peer Electronic Cash System".

Para explicar como funciona esto regresaremos a la analogía del cuaderno. En una red de auditores, todos tienen un cuaderno completo con todas las transacciones que han existido. Ésto es la famosa blockchain.

¿Pero cómo se ponen de acuerdo para ir agregando las transacciones a los cuadernos de todos?

Cuando hay una nueva transacción que necesita ser validada en el sistema de auditoría, se distribuye por la red y cada nodo intenta agregarlo a su cuaderno.

La idea detrás de bitcoin y otras criptomonedas basadas en blockchain es que el validar transacciones sea matemáticamente difícil de hacer pero fácil de verificar. Esto permite que los nodos compiten para ver quién encuentra la solución a como validar la transacción, pero cuando uno lo logra, éste lo publica en la red y ésta lo puede verificar rápidamente volviéndose consenso y todos los nodo intentarán validar las transacciones siguientes. Finalmente como incentivo para hacer el trabajo de validador y para generar nuevas monedas, el nodo que cierra el bloque recibe monedas a cambio. Esta recompensa baja con el tiempo para no devaluar la moneda. Esto es minar criptomonedas: participar en una red de auditoria de transacciones a cambio de unas monedas en el mismo sistema.

Como solamente el nodo que cierra el bloque recibe la recompensa, existen “pools” de minado en donde muchas computadoras participan juntas en búsqueda del bloque y cuando se encuentra se reparten las ganancias en proporción al trabajo otorgado.

Las criptomonedas se venden y compran todos los días en mercados especializados como los de las divisas. En bitcoin se compra-venden alrededor de $1,500,000,000 USD diarios y tiene un circulante de $73,709,026,706 USD [referencia]. Las personas dueñas de todas estas monedas son las que respaldan a red misma.

Al cambiar un detalle en cómo se busca el sello del bloque o simplemente otra blockchain se puede hacer otra criptomoneda, hoy en dia es muy fácil hacer una criptomoneda y hay miles de ellas y 60 de ellas tienen más de $100,000,000 USD circulante. A pesar de que es fácil crear una criptomoneda no es nada fácil crear una idea novedosa que genere comunidad.