

Nos complace reiniciar la popular serie de F&D "Vuelta a lo esencial", interrumpida a finales de 2015. En esta serie explicamos los términos económicos con que se cruzan a diario nuestros lectores. Vea también los vídeos de "Vuelta a lo esencial" en www.fandd.org.

¿Qué son las criptomonedas?

La posibilidad de un nuevo tipo de dinero ofrece beneficios y comporta riesgos

Antoine Bouveret y Vikram Haksar

SURGIERON CIENTOS, con nombres imaginativos como Primecoin, Dash y Verge. Captaron seguidores fervientes entre los conocedores de la tecnología. Sus valores fluctúan sin control. Hay quienes dicen que algún día estos misteriosos bits de código informático reemplazarán al dinero tal como lo conocemos. ¿Qué son exactamente las criptomonedas, y por qué la gente piensa que tienen valor alguno? Para responder a estos interrogantes, consideremos primero la evolución del dinero.

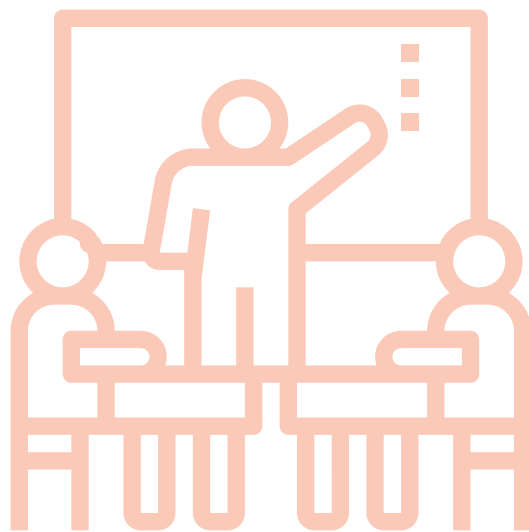
Usos del dinero

El dinero funciona como reserva de valor, medio de intercambio de bienes y servicios, y unidad de cuenta de medición de valor. Antes del dinero, las sociedades intercambiaban bienes y servicios de forma directa (por ejemplo, una fanega de granos por un cerdo), lo que no era muy eficiente. A medida que aumentó la complejidad de las sociedades se desarrolló el dinero mercancía, que empleaba desde caracolas hasta cobre, plata y oro. Ciertos Estados introdujeron el dinero fiduciario, que no tiene un valor intrínseco más allá de la promesa de pago, como el papel moneda en China en el siglo VIII bajo la dinastía Tang.

Las primeras versiones del dinero fiduciario no eran muy estables ni de amplia aceptación, dado que no se creía que el emisor honraría su compromiso de canjear el dinero. Los gobiernos caían en la tentación de imprimir más dinero para comprar bienes o aumentar sueldos, estimulando la inflación (recordemos a las personas con dinero en carretillas en Alemania tras la Primera Guerra Mundial). Los bancos centrales modernos procuran mantener la estabilidad de precios regulando la oferta monetaria en nombre de los gobiernos.

Contabilidad y registros

Un sistema financiero cada vez más amplio y complejo generó la necesidad de intermediarios y



sistemas contables confiables. El desarrollo de la contabilidad por partida doble en la Italia renacentista fue una importante innovación que fortaleció el papel de los grandes bancos privados. En los tiempos modernos, los bancos centrales se ubicaron en la cima de los sistemas de pagos. Con los registros bancarios informáticos aumentó el papel coordinador de los bancos centrales.

¿Cómo funcionan estos registros? Las instituciones financieras ajustan en sus registros internos las posiciones de los titulares de sus cuentas, mientras que el banco central valida las transacciones entre instituciones financieras en un registro central. Por ejemplo, Mehrnaz usa dinero de su cuenta en el banco A para comprar bienes de Mary, que tiene una cuenta en el banco B. El banco A debita el dinero de la cuenta de Mehrnaz. El banco central transfiere el dinero del banco A al banco B e incorpora la transacción en su registro central. Luego el banco B acredita el dinero en la cuenta de Mary. Como pueden ver, el sistema se basa en la confianza en el banco central y en su

capacidad de proteger la integridad del registro central y garantizar que no se gaste dos veces el mismo dinero.

Por el contrario, con las criptomonedas no hay necesidad de un agente central confiable. En su lugar, se basan en la tecnología de registros distribuidos, como las cadenas de bloques, para crear una base de datos que se mantiene a través de una red. Para asegurar que no se gaste dos veces la misma criptomoneda, cada miembro de la red verifica y valida las transacciones empleando tecnologías derivadas de la informática y la criptografía. Una vez logrado el consenso entre los miembros de la red, la transacción se añade al registro, que es validado. El registro alberga la historia completa de las transacciones asociadas con una criptomoneda en particular, de forma permanente y sin admitir que una entidad pueda manipularla por sí sola. Esta capacidad de forjar consensos sobre la validez de las cuentas en una red distribuida es un cambio tecnológico fundamental.

Usualmente se recompensa con criptomonedas de nueva generación a los miembros de la red que verifican y validan transacciones. Muchas criptomonedas también son pseudoanónimas. Los tenedores del activo tienen dos claves: una clave pública, como su número de cuenta; y una clave privada, necesaria para efectuar una transacción. Retomemos el ejemplo anterior: Mehrnaz desea usar criptomonedas para comprar bienes de Mary. Para hacerlo, da inicio a una transacción con su clave privada. Mehrnaz se identifica en la red con su clave pública, ABC; y Mary, con la suya, XYZ. Mediante la solución a un acertijo criptográfico los miembros de la red verifican que ABC cuente con el dinero que desea transferir a XYZ. Una vez resuelto el acertijo se valida la transacción, se añade a la cadena de bloques un nuevo bloque que representa la transacción y el dinero se transfiere de la billetera de ABC a la de XYZ.

Beneficios y riesgos

Ahora que entendemos la tecnología, volvamos al origen de las criptomonedas. La primera, el bitcoin, fue creada en 2009 por un programador (o grupo de programadores) con el pseudónimo Satoshi Nakamoto. Para abril de 2018 había más de 1.500 criptomonedas, según coinmarketcap.com; además del bitcoin, las más usadas son Ether y Ripple.

Pese al furor, las criptomonedas aún no cumplen las funciones básicas del dinero como reserva de valor, medio de intercambio y unidad de cuenta.

Dado que su valor es tan volátil tienen poca utilidad como unidad de cuenta o reserva de valor. Su limitada aceptación para efectuar pagos restringe su uso como medio de intercambio. A diferencia de la moneda fiduciaria, el costo de producir muchas criptomonedas es elevado dada la enorme cantidad de energía necesaria para alimentar las computadoras que resuelven los acertijos criptográficos. Por último, la emisión descentralizada implica que no hay una entidad que respalde el activo, de modo que la aceptación se basa completamente en la confianza de los usuarios.

Las criptomonedas y las tecnologías en que se basan ofrecen beneficios, pero también comportan riesgos. La tecnología de registros distribuidos podría reducir el costo de las transferencias internacionales, incluidas las remesas, así como propiciar la inclusión financiera. Hoy ciertos servicios de pagos realizan transferencias al extranjero en cuestión de horas, no días. La tecnología puede

La tecnología de registros distribuidos podría reducir el costo de las transferencias internacionales, incluidas las remesas, así como propiciar la inclusión financiera.

ofrecer beneficios más allá del sistema financiero. Por ejemplo, puede emplearse para archivar de manera segura registros importantes, como historias clínicas y títulos inmobiliarios. Por otro lado, debido al carácter pseudoanónimo de la mayoría de las criptomonedas, son vulnerables a que se las emplee con fines de lavado de dinero y financiamiento del terrorismo, dado que ningún intermediario verifica la integridad de las transacciones o la identidad de quienes las efectúan. Las criptomonedas también podrían plantear retos a los bancos centrales si llegaran a afectar el control de la oferta de dinero, y por lo tanto la conducción de la política monetaria. **FD**

ANTOINE BOUVERET es Economista y **VIKRAM HAKSAR** es Director Adjunto en el Departamento de Estrategia, Políticas y Evaluación del FMI.