

# Las criptomonedas y la cadena de bloques

JOSÉ ANTONIO MENDOZA GARCÍA \*

LAS CRIPTOMONEDAS Y BITCOIN, A PESAR DE SER ASOCIADAS A MERCADOS ILEGALES, SE HAN INSTAURADO COMO MONEDA DE CAMBIO EN ALGUNOS PAÍSES, POR LO QUE ESTO COMIENZA A SER UNA FORMA DE PAGO CADA VEZ MÁS USUAL.

**H**oy en día se habla cada vez más de las criptomonedas como medio de pago en las transacciones comerciales. Sin embargo, aún hay resistencia por parte de los mercados financieros y de los gobiernos para aceptar esta nueva forma de pago. Sobre todo, porque a las criptomonedas, y en particular al bitcoin, se les sigue asociando con temas ilegales, como la compra de drogas, lavado de dinero y demás.

*Las criptomonedas y la tecnología de bloques surgieron como una propuesta de solución a la seguridad de los documentos digitales*

## **El origen de las criptomonedas**

Comencemos por mencionar que las criptomonedas y la tecnología de cadena de bloques no surgieron de la nada, ya que fue en 1991 que los programadores Stuart Haber y Scott Stornetta propusieron

---

\*Escuela de Relaciones Comerciales Internacionales, Universidad Intercontinental, México. Contacto: jose.mendoza@universidad-uic.edu.mx.

una solución práctica para firmar documentos de forma digital de manera que no pudieran ser alterados. Para 1992, surgió el concepto *Merkle Tree*, desarrollado por Ralph Merkle, científico estadounidense especializado en computación, quien creó el diseño de *Blockchain* o cadena de bloques para hacer más eficiente el copiado y almacenamiento de varios documentos en un mismo bloque.

No fue sino hasta 2008 que Satoshi Nakamoto —seudónimo de un hombre, mujer o grupo de personas— publicó un escrito llamado *Bitcoin: A peer to peer Electronic Cash System* (Nakamoto, 2008), en el que describía cómo funcionaba el bitcoin, primera criptomoneda creada, famosa a nivel mundial, de mayor valor, la más usada y la que dio origen a una revolución tecnológica que ha derivado en la creación de más de 8 mil criptomonedas.

A pesar de que se puede acreditar a Nakamoto el invento de estas monedas digitales, éstas no se crearon de la nada, pues se basan en investigaciones previas sobre monedas virtuales.

La primera transacción con Bitcoin fue realizada entre Nakamoto y Hal Finney, un desarrollador de programas estadounidense con renombre en el mundo de la criptografía. Esta transacción se realizó en junio de 2009, a una tasa de 1BTC (un bitcoin) = 0.0001 dólares, la cual fue considerada como una innovación sin precedentes en el mundo de la criptografía.

Para 2010, el sistema usado para la creación de bitcoins fue utilizado principalmente para el almacenamiento de transacciones, lo que posteriormente se conoció como tecnología de cadena de bloques o *Blockchain*.

---

*Los Bitcoin se convirtieron en un medio de pago virtual y a pesar de su controversia, algunos países instauraron esta moneda de cambio abiertamente*

---

En 2011, dicha moneda se convirtió en un medio de pago virtual; sin embargo, el anonimato de poder realizar transacciones con esta moneda la convirtió en el canal perfecto para ser usada en los mercados negros. Esto generó que surgieran sitios como Silk

Road, un sitio en línea dedicado a la venta de artículos ilegales como drogas, explosivos, armas, y demás, que al usar el bitcoin como medio de pago, detonó que fuera investigado por el gobierno de Estados Unidos de América. En 2013, Silk Road fue cerrado por dicho gobierno, lo que derivó en una caída estrepitosa en el valor del bitcoin, sumado a las diversas regulaciones relacionadas con el uso de la moneda.

### **El bitcoin se instaura como moneda de cambio**

A nivel mundial, el gobierno japonés reconoció el bitcoin y otras criptomonedas con el propósito de usarlas como moneda actual. Por otro lado, el mayor sitio de comercio en línea en Sudáfrica, *Bidorbuy*, comenzó a aceptar pagos con bitcoins. En Argentina, *Uber* aceptó como medio de pago esta moneda debido a que el gobierno de ese país prohibió a las compañías de tarjetas de crédito llevar a cabo relaciones comerciales con Uber.

Para 2017, el gobierno de Japón aprobó una ley que permitía el uso del bitcoin como medio de pago. A la par, Rusia declaró su interés por legalizar el uso de las criptomonedas y el banco en línea noruego, *Skandiabanken*, iniciaba operaciones con bitcoins.

Entre 2017 y hasta inicios de 2020, el valor del bitcoin tuvo varios incrementos y disminuciones ocasionadas por diversos factores. Para estabilizarse en los 5 mil dólares debido al efecto COVID-19, a finales de julio de 2020, alcanzó los 10 mil dólares. Tuvo



un incremento sostenido el resto de ese año y, hasta el 8 de enero de 2021, llegó a un valor récord de 42 mil dólares. Posteriormente, disminuyó a los 33 mil dólares, pero con un ligero incremento gracias a un *tweet* de Elon Musk. Ahí hace referencia al bitcoin, anunciando que haría una inversión millonaria con esa moneda y que su compañía, *Tesla*, productora de autos eléctricos, empezaría a aceptar dicho activo digital. Esto generó que la moneda llegara a un valor de 40 mil dólares. Finalmente, y a la fecha de elaboración de este trabajo, el valor del bitcoin rebasa los 55 mil dólares.

---

*Las criptomonedas existen de forma digital o virtual y usan tecnología de encriptación, que a diferencia de las monedas tradicionales, cuentan con una mayor seguridad*

---

### **Diferencias del bitcoin y las monedas tradicionales**

Son varios los factores que hacen diferente al bitcoin de las monedas tradicionales. Aquí mencionaremos algunas:

- a) Descentralizada. Las monedas tipo *fiat* como el dólar, euro, peso y otras están bajo las regulaciones de un gobierno, usualmente a través de un banco central. Por lo tanto, la producción de estas monedas está controlada. La creación y transacción que involucra al bitcoin está regulado por un código abierto y que depende de las conexiones P2P (*Peer to Peer* o persona a persona), por lo que ningún gobierno puede interferir en el proceso de minado de los bitcoins.
- b) Valor. Cualquier moneda tipo *fiat* es aceptada sólo si tiene un valor. El bitcoin tiene el mismo principio, ya que es obtenido a través de un proceso llamado *minado* y este esfuerzo da valor a la moneda, mientras que la demanda y la oferta afecta la fluctuación del valor.
- c) Virtual. Las monedas tradicionales son tangibles y es lo que les da un valor; pero el bitcoin es digital y, debido a esto, se almacena usando una “cartera digital”. Por esta razón, no hay un tangible que represente al bitcoin.

- d) Seudónimo. Los propietarios de Bitcoins mantienen estos activos de forma segura en su cartera digital, por lo que la identidad del propietario se almacena en una ubicación encriptada que se puede controlar, pero no asociar con la identidad del propietario. Esta conexión entre el bitcoin y el dueño se realiza de forma seudónima, ya que el acceso a los libros contables lo tiene cualquiera.
- e) Criptografía. Es el elemento principal de Bitcoin, pues se utiliza para controlar la producción de esta moneda digital y verificar las transacciones.
- f) Escala adaptativa. El bitcoin está diseñado para que un bloque de transacciones sea minado cada 10 minutos, pero el algoritmo cambia cada que se han minado 2 mil 016 bloques. De esta manera, el minado se vuelve más difícil dependiendo del tiempo que toma minar esos bloques.

---

*La cadena de bloques se refiere al registro virtual, público y descentralizado de todas las transacciones de una criptomoneda, como el Bitcoin*

---

### **Las cadenas de bloques**

Las criptomonedas son monedas que existen de forma digital o virtual y que usan tecnología de encriptación, las cuales añaden una capa de seguridad durante el proceso de transferencia y almacenamiento de registros. La cadena de bloques o *Blockchain* es un libro contable descentralizado usado para llevar un registro de las transacciones realizadas a lo largo de la red de computadoras, por lo que estos registros no pueden ser alterados de forma retroactiva.

La cadena de bloques se refiere al registro virtual, público y descentralizado de todas las transacciones de una criptomoneda, como el bitcoin, las cuales se registran en una secuencia cronológica. Cada computadora que está conectada a la red recibirá una copia de esta cadena de bloques, la cual se descarga de forma automática. La información que se registra en la cadena de bloques estará disponible en la forma de una base de datos pública y regulada.

Incluso, ésta puede ser usada por cualquier usuario a través de internet, ya que se almacena en millones de computadoras alrededor del mundo al mismo tiempo.

Esta cadena de bloques no está almacenada en una sola ubicación, de manera que los registros son de carácter público y pueden ser verificados por cualquier persona que ingrese a la red. Por ello, es prácticamente imposible que un *hacker* pueda comprometer los datos. La red de la cadena de bloques realiza revisiones automáticas cada 10 minutos. Es importante señalar que a cada grupo de estas transacciones se le llama *bloque*, y que hay dos propiedades que resultan de esto:

- a) No es corrompible porque para realizar un cambio en la información en la cadena de bloques, se requiere sobrepasar el poder actual de la red de computadoras conectadas, lo cual es prácticamente imposible.
- b) La información está inmersa en la red como un todo, por lo que es accesible al público en general.

La revolución de la cadena de bloques ha generado que se busquen otras aplicaciones para esta tecnología, siendo algunas de ellas, las siguientes:

---

*La revolución de la cadena de bloques ha generado que se busquen otras aplicaciones para esta tecnología e implementación de monedas virtuales*

---

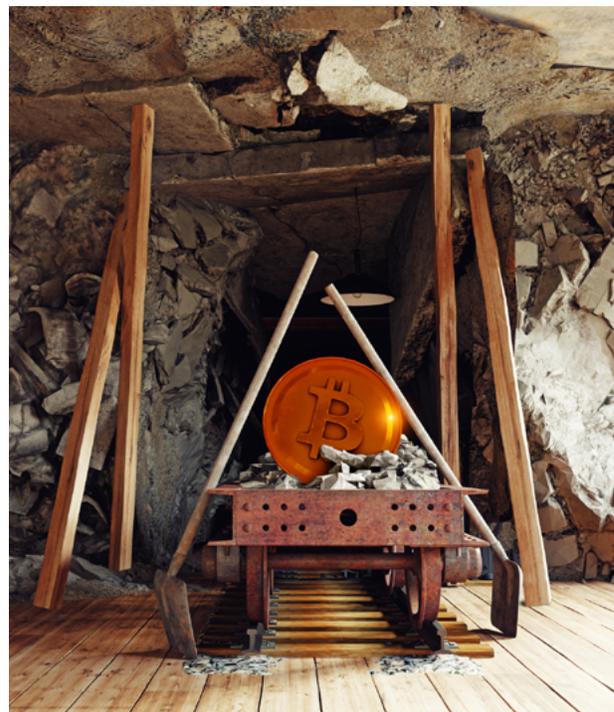
- a) Industria de compartir. El surgimiento de empresas como *Airbnb* y *Uber*, industria bajo el esquema de compartir, se ha convertido en un modelo de negocio que busca que la aplicación de la tecnología de cadena de bloques se enfoque en este modelo, a través del uso de la tecnología P2P. Esto permitiría el pago de servicios como *Uber* de forma directa entre el pasajero y el conductor.

- b) Contratos inteligentes. Se podrán diseñar para realizar funciones básicas, por ejemplo, pagar un derivado si el instrumento financiero ha cumplido con un *benchmarking* específico a través del uso de la cadena de bloques y el bitcoin para realizar el pago de forma automática.
- c) Servicios gubernamentales. Mediante la mejora de la transparencia y el acceso a la información, la tecnología de cadena de bloques puede ser una gran ventaja para los gobiernos en la administración de sus servicios, así como en los resultados electorales.
- d) Protección de la propiedad intelectual. A través del uso de los contratos inteligentes, los derechos de autor pueden ser protegidos y automatizar la venta de contenido creativo a través del internet, lo que elimina el riesgo de redistribución y replicación. Un ejemplo de esto es el sitio de música *Mycelia*, que usa la tecnología de cadena de bloques para construir un sistema de distribución de música tipo P2P.
- e) Internet de las cosas (IOT). Se refiere a todo el conjunto de dispositivos electrónicos que pueden conectarse a internet y, por lo tanto, ser manejados a través de esta red con la finalidad de facilitar la interacción entre las compañías que ofrecen productos y servicios a los usuarios. A través del uso de los contratos inteligentes, es posible administrar la automatización de sistemas remotos. Esto se realiza mediante la integración de redes, sensores y *software*, lo que resulta benéfico para la reducción de costos y los sistemas.
- f) *Crowdfunding*. Es un esquema de financiamiento de proyectos mediante la captación de pequeñas cantidades de dinero de un número

amplio de personas a través de internet. El uso de la tecnología de cadena de bloques ha incrementado el interés de crear fondos de capital a través de este esquema.

### Cómo obtener bitcoins

La manera de obtener bitcoins es mediante el minado. Este proceso añade transacciones a la cadena de bloques, así como la liberación de nuevas monedas digitales, a través de la compilación de transacciones en bloques y resolviendo problemas matemáticos muy complejos. Quien resuelva estos problemas podrá agregar el siguiente bloque a la cadena de bloques y obtener como recompensa



bits. Es trabajo del minero verificar estas transacciones y registrarlas en el libro contable y una vez que se ha generado un bloque de transacciones, los mineros lo registran a través de un proceso consistente en ingresar la información al bloque, usar una fórmula matemática y transfor-

marlo en una versión corta compuesta de números y letras denominado *hash*.

Esto sirve para verificar que ese bloque, incluyendo los siguientes, es legítimo y, si alguien intenta realizar alguna modificación no autorizada, cada integrante de la red será notificado. Los mineros usan un *software* especial para verificar los bloques y el minado de Bitcoin, por lo que, cada vez que un miembro de la red crea de forma exitosa un *hash*, obtiene como recompensa bitcoins.

Las recompensas se refieren al número de nuevos bitcoins que se liberaron cuando es minado un bloque. Sin embargo, estas recompensas disminuyen debido a que el número de bitcoins minados se reduce en 50% cada 210 mil bloques. En 2009, la recompensa empezó en 50 bitcoins; después, disminuyó a 25 para 2014 y, en febrero de 2019, esta recompensa fue de 12.5 bitcoins, la cual se mantiene hasta la fecha.



---

*Cada vez más países, negocios y personas están abiertas a recibir Bitcoin como forma de pago*

---

Una de las características más importantes del bitcoin es que cada vez más negocios y personas están abiertos a aceptarla como medio de pago. Otra forma de obtener bitcoins es comprándolos, ya sea en efectivo, transferencia bancaria o cargo a tarjeta de crédito.<sup>2</sup> Una vez comprados,

---

<sup>2</sup> Para mejorar la referencia de cómo llevar a cabo la compra de bitcoins, se recomienda revisar el siguiente video, pues explica el proceso de compra de esta moneda digital: Sizemore, Chris. (3 de marzo de 2017). *Living on Bitcoin for a week*. Recuperado de [https://www.youtube.com/watch?v=27VZ6gYYNOA&list=FLYLX-tjz2hmF-kdHZ\\_tXhpCw&index=6](https://www.youtube.com/watch?v=27VZ6gYYNOA&list=FLYLX-tjz2hmF-kdHZ_tXhpCw&index=6)

serán acreditados a una cartera digital para enviar y recibir pagos a un vendedor o comprador sin la necesidad de un intermediario como las compañías de tarjetas de crédito o bancos, o simplemente guardarlos si se quiere especular que el precio del bitcoin incrementará en un futuro o, incluso, venderlos para cambiarlos en moneda local.

---

*Las transacciones de bitcoins se realizan en poco tiempo, no son reversibles y son fáciles de transferir, incluso, a cualquier país*

---

### **Las transacciones de Bitcoin**

Las transacciones de bitcoins se realizan en poco tiempo, no son reversibles y son fáciles de transferir a cualquier país, pues se evita el pago de altas comisiones por el intercambio de monedas, debido a que no hay políticas de gobierno sobre los bitcoins; además, las cuentas no pueden ser sujetas a ser congeladas y no tienen límites. Varios factores afectan su precio; entre ellos, la oferta y la demanda, la cantidad total de bitcoins disponibles, aspectos técnicos, volatilidad, eventos políticos e incluso las noticias en redes sociales. Sin embargo, el factor principal es la oferta y la demanda, pues el código del Bitcoin está limitado a 21 millones (disponibles hasta 2140, cuando se cree que se minará el último bitcoin), de los cuales actualmente hay cerca de 18.5 millones en circulación.

Debido a que las criptomonedas como el bitcoin son consideradas instrumentos financieros, es posible obtener ganancias a través de la compraventa o inversión. Aquellos que compran bitcoins toman ventaja de las fluctuaciones en el precio para obtener ganancias, mientras que los inversionistas buscan altos retornos a lo largo de un lapso, mediante la compra y retención de esa criptomoneda. Con base en lo anterior, se puede establecer que invertir o comprar bitcoins puede ser una actividad rentable.

Para algunos, Bitcoin puede ser una mina de oro virtual mediante el minado donde se puede hacer dinero en cualquier momento desde cualquier lugar, siempre y cuando se cuente con el

*software* y *hardware* adecuado. No obstante, la realidad es que esto ha dejado de ser rentable, porque la mayoría de las personas que desean obtener bitcoins lo hacen comprando y no mediante el minado.

### **Bitcoins y criptomonedas: ¿es o no viable?**

Entonces, ¿vale la pena invertir o comprar bitcoins? La respuesta no es sencilla, pues depende del conocimiento que se tenga en relación con cómo funciona esta moneda digital, así como los recursos que se tienen para destinar una parte del dinero a la compra o inversión en bitcoins. Lo que sí es posible es invertir o comprar una pequeña cantidad e ir incrementándola a medida que se conozca más acerca de cómo obtener bitcoins. Hay que recordar que esto es una estrategia a largo plazo que puede dar grandes ganancias, pero también pérdidas.

---

*A pesar de los obstáculos a los que se enfrentan las criptomonedas, año tras año han generado más interés por la forma en que operan y por su utilidad. No obstante, tomará años percatarnos hasta dónde pueden llegar estas monedas de cambio*

---

No hay duda de que la tecnología de la cadena de bloques cambiará a gran escala la economía global en los siguientes años. Desde la forma en que la información es compartida, hasta la posibilidad de que los gobiernos emitan su propia criptomoneda, pues la fortaleza de la cadena de bloques se centraliza en la habilidad para lograr la cooperación entre las partes en conflicto. A pesar de los obstáculos a los que se enfrentan las criptomonedas, en particular, el bitcoin, año tras año ha generado más interés por la forma en que opera y por su utilidad. Pero no sólo es eso, pues diversos gobiernos han considerado crear su propia criptomoneda para usarla como medio de pago válido dentro de sus economías.

Ya se ha hablado de la innovación que ha sido la creación del bitcoin y que probablemente en un futuro podría llegar a sustituir las monedas tradicionales. Si en un futuro la gente decide confiar

más en esta criptomoneda que en el valor del dólar, sobre el cual el valor del bitcoin está establecido, realmente se podría convertir en la moneda del futuro. A pesar de que esta innovación ha sido de gran impacto para la tecnología, posiblemente tomará años o décadas antes de que podamos percatarnos hasta dónde pueden llegar las criptomonedas, sin embargo, hay una tendencia por un mayor interés hacia este tipo de monedas.

## Referencias

CoinMarketCap. (2021). *Today's Cryptocurrency Prices by Market Cap*. Recuperado de <https://coinmarketcap.com/>

Pain, George. (2018). *Cryptocurrency*. Carolina del Sur: CreateSpace Independent Publishing Platform

Satoshi Nakamoto. (2008). *Bitcoin: A peer to peer Electronic Cash System*. Recuperado de <https://bitcoin.org/bitcoin.pdf>

Satoshi, Stephen. (2017). *Cryptocurrency for beginners*. Carolina del Sur: CreateSpace Independent Publishing Platform

Sizemore, Chris. (3 de marzo de 2017). *Living on Bitcoin for a week*. Recuperado de [https://www.youtube.com/watch?v=27VZ6gYYNOA&list=FLYLXtjz2hmF-kdHZ\\_tXhpCw&index=6](https://www.youtube.com/watch?v=27VZ6gYYNOA&list=FLYLXtjz2hmF-kdHZ_tXhpCw&index=6)

Tapscott, D. y Tapscott, A. (2018). *La revolución Blockchain: Descubre cómo esta nueva tecnología transformará la economía global*. México: Paidós.

Vela, D. (2018). *Blockchain Technology*. Carolina del Sur: CreateSpace Independent Publishing Platform

