CIENCIA

launion.com.mx

@uniondemorelos

El dinero que no existe: Criptomonedas y energías renovables

JESÁN VELÁZQUEZ-RESÉNDIZ Y YURI RUBO

Jesán Velázquez-Reséndiz es estudiante de la Licenciatura de Ingeniería en Energías Renovables en el Instituto de Energías Renovables, UNAM. En el 2021 y 2022 obtuvo el reconocimiento de Excelencia Cuántica otorgado por la empresa IBM por haber completado las tareas y ejercicios de la "*Qiskit Global Summer School on Quantum Machine Learning*" y la "*Qiskit Global Summer School 2022: Quantum Simulation*".

Yuri Rubo es ingeniero-físico por la Universidad Nacional de Kiev, Ucrania, y tiene doctorado en ciencias fisicomatemáticas por el Instituto de Física de Semiconductores de la Academia Nacional de Ciencias de Ucrania. Actualmente, es Investigador Titular "C" en el Instituto de Energías Renovables, UNAM, y es miembro activo de la Academia de Ciencias de Morelos.

Esta publicación fue revisada por el comité editorial de la Academia de Ciencias de Morelos

¿Antes existía el dinero?

Es bien conocido el dicho "el dinero es lo que mueve al mundo". Sin embargo, cuando queremos definir el concepto "dinero", nos damos cuenta de que es más complicado de lo que parece, puede que sean metales preciosos, papeles con cierto valor escrito o bien una abstracción de lo inexistente que se guarda en alguna parte del banco o, en los últimos años, en la red de información distribuida a lo largo del mundo.

El trueque fue la primera forma de pago en el mundo, consistía en el intercambio de dos bienes materiales entre dos personas: el comprador y el vendedor. Por ejemplo, un granjero que tenía carne de vaca o de borrego podía ir a la ciudad en búsqueda de las herramientas, ofreciendo como pago su carne. De esta manera, un martillo podía costar dos kilos de carne de vaca o un kilo de carne de borrego. No había un precio definido para los productos. Además, la persona que vendía el martillo podía no necesitar la carne, por lo que la compra de las herramientas sería muy difícil.

Debido a estos problemas, se optó por la utilización de metales preciosos como medio de pago en los comercios. podía ser en forma de polvo, pepitas, trozos, bloque, entre otras. Uno de los problemas era que el valor se medía por peso, por lo que era una tarea complicada el medir en cada instante o romper el metal en las partes deseadas. En añadidura, las falsificaciones eran sencillas de realizar, ya que no había regulación en las especificaciones que debía tener el metal. Los materiales que se utilizaban era el oro, la plata y el cobre, por lo que la actividad de extracción de estos fue importante en esta época. Además, la necesidad de transportar el polvo o los trozos del metal era muy incómodo. Se tenía que llevar en bolsas o recipientes que podían perderse o ser robados fácilmente. Con todos sus problemas, la forma de pago parecía ser la correcta, aunque no la más eficiente, pero el dinero podía guardarse y conservarse sin que perdiera su valor. Debido a esto, comenzó el proceso de acuñación de monedas.

Inicialmente, las transacciones no estaban organizadas ni escritas para llevar un registro. Así fue como el préstamo de dinero se convirtió en un mecanismo indispensable para el desarrollo, especialmente en agricultura, donde los pagos pueden ser garantizados con la cosecha en futuro. Además, no existía un registro de los préstamos y los cálculos de interés, por lo que cualquiera podía decir que se le debían 100 monedas de oro y nadie podía negarlo ni afirmarlo. Los primeros registros de este tipo datan de la época de la cultura de Mesopotamia, lugar entre los ríos Tigris y Éufrates, actual zona de Iraq y Siria. Así surgieron las matemáticas, la escritura y un conjunto de leyes que regulan las relaciones económicas (el código de Hammurabi). Las transacciones entre personas comenzaron a registrarse para el control y buen manejo de los recursos.

Las monedas ahora circulaban por las calles y paseaban de comercio a comercio; estos pequeños trozos de metal tenían un diseño distintivo en su superficie para indicar su valor y evitar falsificaciones. Pero, como ya es costumbre en la historia del dinero, había un problema: el peso de las monedas. Cuando se tenían muchas monedas, se necesitaba bastante espacio para guardarles y bastantes medios de transporte para llevarlas de un lugar a otro. En consecuencia, inició la utilización de los llamados billetes, los cuales incluían diseños distintivos únicos para evitar falsificaciones. De esta manera, se tenía un sistema económico que funcionaba en cada rincón del mundo.

Capitalismo y virtualización de dinero

Los cambios más drásticos de nuestro manejo del dinero y la virtualización profunda de los flujos monetarios aparecieron con la formación del capitalismo. Nos guste o no, eso es el sistema económico actual y sus actores principales ya no son las personas físicas sino las personas morales: las empresas. Una empresa tiene mucha más libertad que una persona física y puede incorporar más capital para su desarrollo.

Consideremos un ejemplo. Supongamos que la empresa de Emma tiene una idea de cómo crear un software de seguridad virtual para que no haya riesgo de hackeo, pero no tiene el suficiente dinero para invertir y comenzar a construir su idea, ya que cuesta $100,000. Por otro lado, está Diana que está abriendo un negocio para prestar dinero o guardarlo de forma segura (un banco), pero solo cuenta con $20,000. Luego está Cecilia, que quisiera guardar $50,000 en un lugar seguro para evitar robos, porque ya le pasó a su abuelo que por guardar el dinero debajo de la cama lo perdió todo en un robo mientras él estaba persiguiendo a un burro que se había escapado. De esta manera, Cecilia guarda su dinero con Diana y lo puede mantener alejado de robos o imprevistos, y recibir, además, los intereses.

Ahora Diana tiene la mitad del dinero que necesita Emma para emprender su idea, por lo que, aun sabiendo que no cuenta con la cantidad completa, le ofrece a Emma prestarle $100,000 MX para que su idea salga al mercado. En este momento las tres partes de esta operación salen ganando, Cecilia puede guardar su dinero y evitar robos, Diana tiene dinero para prestarle a Emma y generar ganancias a partir de este préstamo, y Emma tiene el suficiente dinero para que su idea salga al mercado. ¿Cómo es posible que Diana pueda realizar un préstamo que exceda el dinero que tiene? ¿No es una tontería? De un lado si el negocio de Emma fracasa eso va a resultar en una crisis financiera. Empero, si no permitimos a los bancos prestar más dinero, la economía se para, por lo que Emma no puede abrir su negocio, desarrollar su vida y la de otros ofreciendo nuevos trabajos. Para estimular el desarrollo, el banco Diana tiene la habilidad de prestar hasta 10 veces su capital total. En nuestro caso tenemos:

Es importante resaltar un punto de este ejemplo, Emma no está vendiendo una empresa o un producto, está vendiendo una idea. Ella vende su conocimiento y sus habilidades para desarrollar un producto y puede realizarse gracias al préstamo del banco (Diana) de dinero que no existe. Esto quiere decir que la idea de un software de seguridad virtual adquirió todo el valor en esta ocasión. La idea y la visión del futuro es lo importante y lo que se comercializa, no el dinero.

Antes de continuar, queremos hacer énfasis en un punto: la cantidad de dinero total no es definido. Hasta para una persona, la cantidad de dinero que tiene en su disposición no aparece físicamente, sino que está en cuentas de débito y/o crédito que avala el banco. De esta manera se tiene dinero que en verdad no existe pero que el banco asegura que tienes. Por otro lado, la cantidad de riqueza que se tiene no sólo depende del dinero físico o imaginario, sino que también depende de las acciones, casas, edificios, tecnología, entre otras, que se posea. Como vemos en el ejemplo anterior, el dinero aparece gracias a las necesidades del desarrollo. Es solo un mecanismo para promover las ideas del negocio.

Tu dinero dentro de una computadora

En los últimos 10 años ha surgido una nueva tecnología de cadenas de bloques de información que promete cambiar el sistema económico mundial de forma drástica. Y como resultado aparecieron *las criptomonedas*. Seguro has escuchado de personas que se hicieron millonarias de la noche a la mañana porque tenían guardadas el tipo de criptomoneda llamada bitcoin, ya que su máximo precio histórico ha sido más de 68 mil dólares [1].

¿Qué es una criptomoneda y para qué sirve? Ya discutimos que hasta en Mesopotamia antigua apareció la importancia del registro de las transacciones financieras. Técnicamente, si tenemos un registro universal, seguro y confiable para todas y todos en este mundo, ya no es necesario gastar recursos y tiempo en producción y distribución de las monedas y billetes. Ya no necesitamos dinero en su forma vulgar. La fortuna y el capital de una persona es su historia, sus transacciones financieras pasadas, y el registro de estas transacciones define la cantidad de criptomonedas que tiene. Por su parte, las criptomonedas son una representación digital del dinero, que almacena las transacciones en un registro seguro que se llama "*blockchain*" en inglés. Sin embargo, se pierde la ventaja de prestar más dinero del que se tiene. Aquí una persona o empresa no puede emitir más criptomonedas de las que tiene en su poder, aunque algunas empresas están intentando incorporar el mecanismo de préstamos de criptomonedas de manera que puedes pedir prestado hasta el 50% del valor actual de tus criptomonedas actuales.

La "*blockchain*" (cadena de bloques, por su traducción al español) es una tecnología que utiliza los métodos de seguridad computacionales de codificación y encriptación, o la criptografía electrónica, para dar seguridad a las transacciones con criptomonedas. La cadena de bloques tiene tres componentes: datos de la transacción, *hash* referido a la transacción actual y *hash* referido a la transacción pasada. El *hash* es una técnica criptográfica que provee seguridad a los datos, es una cadena de números y caracteres que asegura la veracidad de un archivo. Este *hash* pequeño, sirve como una huella digital del archivo y tiene la propiedad de que cambia drásticamente con cada elemento que se modifique en el archivo de datos. Además, cada transacción tiene un único *hash*. Cada persona que participa en una transacción tiene su *hash* privado, el cual es único para cada persona y se utiliza para autorizar las transacciones (es como una firma digital). También se tiene un *hash* público, el cual es una firma digital para guardar el rastro de la transacción y garantizar para otras personas que tienen transacción segura.

El primer componente, los datos de la transacción, se refiere a la información que describe la acción que se llevó a cabo. El *hash* referido a la transacción actual se genera al momento de realizar la transacción y es único para cada una de ellas. El *hash* referido a la transacción pasada se refiere al *hash* de la acción anterior a la actual; pero, si no se tiene ninguna acción pasada, el *hash* será una cadena de ceros.

Pongamos un ejemplo. Alice y Bob quieren realizar transferencias de criptomonedas entre ellos, así que recurren a la tecnología de la "*blockchain*". Cuando Alice paga a Bob 10 criptomonedas, se genera un bloque en la "*blockchain*" que contiene los datos de la transacción (Alice paga a Bob 10 criptomonedas), el *hash* referido a la transacción actual (por ejemplo, qwerty5116!#%) y un *hash* referido a la transacción pasada, que en este caso será una cadena ceros por no tener una acción pasada (0000000000000). Ya que Alice ha pagado a Bob, pasemos a la perspectiva de Bob. Cuando él recibe el pago se genera un nuevo bloque en la misma cadena de bloques que contiene los datos de la transacción (Bob recibe 10 criptomonedas de Alice), un *hash* referido a la transacción actual (por ejemplo hytdol5%46!#9) y un *hash* referido a la transacción pasada, que en este caso será el *hash* del bloque que se genera de Alice refiriéndose a la transacción actual (qwerty5116!#%). Estos dos bloques que se han generado están conectados entre sí, dando seguimiento y seguridad

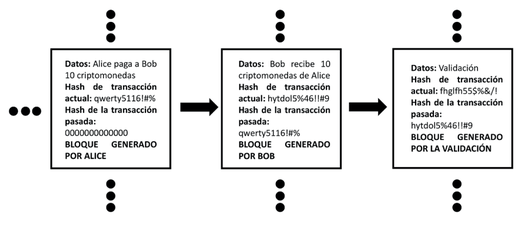

FIGURA 1: CADENA de bloques generada por la transacción entre Alice y Bob.

a la transacción; de este modo se ha creado una cadena de bloques.

Esta "*blockchain*" se encuentra en el poder de Alice y de Bob, pero no basta para que la transacción sea válida, se tiene que verificar mediante alguno de los dos siguientes procesos. El primero es el llamado la prueba de trabajo ("*proof of work*" en inglés), el cual consiste en adivinar los primeros caracteres del *hash* referido a la transacción actual mediante la resolución de problemas matemáticos complejos. Este proceso es bastante complicado y con un alto consumo de energía, ya que se necesita gran poder computacional para validar la mayor cantidad de transacciones en el menor tiempo posible. Las personas que realizan el "*proof of work*" se les llama mineros, y el primero que adivine los caracteres, valida la transacción y se lleva una comisión a su bolsillo, generando un nuevo bloque en la cadena de bloques que se refiere a la validación de la transacción, teniendo los datos de la transacción (Validación), un *hash* referido a la transacción actual (por ejemplo fhglfh55$%&/!) y un *hash* referido a la transacción pasada, el cual será el *hash* de la transacción actual del bloque que generó Bob (hytdol5%46!#9). De esta manera, la "*blockchain*" tiene tres bloques: el que generó Alice, el que generó Bob y el que generó el minero para validar la transacción; esta cadena de bloques ahora se encuentra en poder de Alice, Bob y el minero (figura 1).

La segunda manera de verificar la transacción es con el método de la prueba de participación ("*proof of stake*" en inglés), el cual consiste en que las personas que quieran realizar este proceso depositan criptomonedas que quedan bloqueadas y guardadas en la red de las criptomonedas (sistema de información a lo largo del internet creado específicamente para este tipo de criptomonedas). De este modo se pueden verificar las transacciones con solo tener las monedas digitales guardadas en la red, eliminando el gran consumo de energía que tiene el método anterior. A las personas que realizan este proceso se les llaman validadores, y la elección de quién verificará la transacción depende directamente de la cantidad de criptomonedas que tenga bloqueadas en la red; mientras más tenga, más oportunidades tiene.

Como hemos visto en este ejemplo, no se necesitan intermediarios para realizar la transacción. Los bancos no son requeridos y todos los datos y criptomonedas están guardados en la red computacional descentralizada, y así no depende de ningún gobierno. Otra ventaja que tiene esta nueva tecnología es que no permite gastar más dinero del que se tiene. Desafortunadamente, de estas dos ventajas resultan algunas restricciones. Las criptomonedas no están garantizadas por una autoridad gubernamental y por eso no todos los negocios las aceptan, y tienen la dificultad de promover el desarrollo económico. Eso tiene como consecuencia una gran volatilidad de las criptomonedas. Sin embargo, tal parece es un sistema monetario del futuro y es importante de considerar su eficiencia energética. Finalmente, la mayor preocupación del mercado de criptomonedas es que su minería, indispensable para seguridad del sistema, consume enorme cantidad de energía eléctrica.

Lo que no existe consume energía

Pongamos la energía consumida en perspectiva. El consumo de energía en el mundo en el año 2019 fue de 173,340 TWh [2] (la unidad de medida TWh se refiere a un billón, o un millón de millones de watts por hora). Según los datos de la Universidad de Cambridge, Reino Unido, la energía promedio anual que utilizó la red de la criptomoneda bitcoin en el año 2020 es de aproximadamente 25 000 TWh [3], lo que equivale al 14% de la energía total mundial consumida en 2019. Es enorme. En México se consumieron solamente 307.5 TWh en el año 2020 [4], por lo que la energía consumida por la red de bitcoin en el año 2020 es más de 80 veces lo que todo México consumió en el mismo año, ver Figura 2.

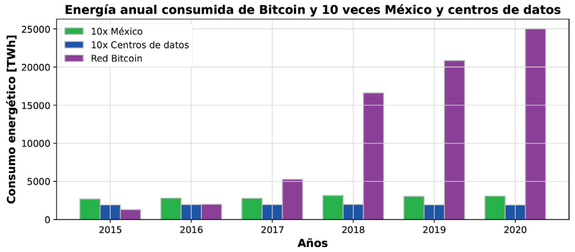

FIGURA 2: COMPARATIVA entre el consumo anual de electricidad.

Otro aspecto alarmante es que el consumo de energía eléctrica de la industria de criptomonedas crece en una forma drástica. El consumo de bases de datos electrónicas tampoco es despreciable. Podemos hablar de bases de datos tradicionales y de híper escala. Los tradicionales se caracterizan por almacenar la información de manera física, básicamente te puedes imaginar una base de datos tradicional como lo pintan en las películas, llena de máquinas gigantes y cables donde se tiene toda la información. Aunque imaginamos el almacenamiento de los datos en la nube virtualmente, en realidad, siempre hay una máquina física que resguarda la información y consume energía. Las bases de datos de híper escala ("*hyperscale*" en inglés) son, básicamente, como los tradicionales, pero a gran escala, así que solo las usan empresas gigantes digitales. La energía total consumida por las bases de datos en 2020 fue entre 200 y 250 TWh, lo que equivale al 1% de la energía consumida a nivel mundial [5], o entre 65% y 81% de la energía consumida en México en ese mismo año, ver Figura 2. Este es un problema que se tiene que afrontar, ya que las nuevas tecnologías que están surgiendo (computación cuántica y criptomonedas en algunos casos) necesitan las bases de datos.

Como resultado, la tecnología de criptomonedas y de "*blockchain*" deja una enorme huella de carbono, que es un indicador universal que refleja la cantidad de gases dañinos para el planeta emitidos por un individuo, organización, tecnología, evento o producto, y no se puede ignorar. Como hemos visto, la minería de bitcoin utiliza 144.16 TWh al año [3] por lo que el uso de combustibles fósiles como petróleo, gas natural o carbón para generación de energía eléctrica no es el método sostenible para la Tierra y sus habitantes. Expertos han propuesto la utilización de *las energías renovables* para los procesos requeridos en las criptomonedas (como minería y bases de datos donde se almacene la información), reduciendo las emisiones de gases nocivos para el ambiente y el costo de la electricidad. Hay que señalar que las fluctuaciones diarias que tienen algunas fuentes de energías renovables no son tan importantes para la tecnología de criptomonedas. Uno siempre puede hacer minería en lugares en la Tierra en donde hay sol o hay viento en el momento de minería. No solo las energías renovables pueden ayudar a la tecnología "*blockchain*", sino que puede ser al revés. Empresas de generación y distribución de energía eléctrica han comenzado a utilizar la cadena de bloques para verificar si la generación de energía es 100% renovable [6], eliminando intermediarios y garantizando la veracidad y transparencia de los datos.

Además de las energías renovables, existe otra tecnología que puede ayudar a la seguridad y rapidez de las transacciones de las criptomonedas: *la computación cuántica*. Esta tecnología tiene apenas 40 años de investigación y desarrollo, por lo que no existen aplicaciones prácticas en cuestiones de criptomonedas. Sin embargo, expertos en campos de economía, física, matemáticas, medicina, química y biología tienen altas expectativas en los logros de esta tecnología, ya que la supremacía de las computadoras cuánticas con respecto al cómputo tradicional ya fue demostrada por Google hace tres años [7].

La computación cuántica hace uso de propiedades de la física cuántica y promete reducir el consumo energético de las bases de datos alrededor del mundo y la creación de nuevas supercomputadoras, dispositivos informáticos con mayor capacidad que las computadoras normales de escritorio o laptop, que puedan realizar tareas matemáticas que hasta ahora son inviables. Además, ofrece seguridad de alta encriptación en cada una de las operaciones, por lo que su uso en la cadena de bloques podría beneficiar al consumo energético, la seguridad y rapidez de las transacciones.

Aunque el uso de energías renovables y la computación cuántica suena prometedor para las criptomonedas, primero hay que superar varias barreras. En el mundo todavía no se sabe cómo regular a las criptomonedas y cómo garantizar su eficacia, por lo que su uso cotidiano no está muy cerca. Además, la volatilidad en el precio de ellas es un problema latente que se tiene que solucionar.

Las criptomonedas son una alternativa monetaria importante para un cambio radical en el sistema económico mundial. Sin embargo, primero se tienen que superar las barreras gubernamentales y jurídicas para que sea un sistema económico viable. Simultáneamente, se tiene que trabajar en tecnologías que ayudan a reducir el impacto ambiental y aumentar la seguridad en las transacciones, siendo las energías renovables y computación cuántica opciones prometedoras.

Esta columna se prepara y edita semana con semana, en conjunto con investigadores morelenses convencidos del valor del conocimiento científico para el desarrollo social y económico de Morelos. Desde la Academia de Ciencias de Morelos externamos nuestra preocupación por el vacío que genera la extinción de la Secretaría de Innovación, Ciencia y Tecnología dentro del ecosistema de innovación estatal que se debilita sin la participación del Gobierno del Estado.

Agradecimientos

A los proyectos 251808 "*Rompimiento de simetría en condensados de bosones y láser polaritónico*" de CONACYT y IN106320 "*Condensados polaritónicos para simulación y computación cuántica*" de PAPIIT-UNAM.

Referencias

[1] CoinMarketCap. (s. f.). *Cryptocurrency Prices, Charts And Market Capitalizations*. Recuperado 7 de abril de 2022, de https://coinmarketcap.com/

[2] Ritchie, H. (2020, 28 noviembre). *Energy Production and Consumption*. Our World in Data. Recuperado 10 de abril de 2022, de https://ourworldindata.org/energy-production-consumption

[3] *Cambridge Bitcoin Electricity Consumption Index (CBECI)*. (s. f.). Cambridge Bitcoin Electricity Consumption Index. Recuperado 10 de abril de 2022, de https://ccaf.io/cbeci/index

[4] *Mexico - Countries & Regions*. (s. f.). IEA. Recuperado 10 de abril de 2022, de https://www.iea.org/countries/mexico

[5] *Data Centres and Data Transmission Networks – Analysis*. (s. f.). IEA. Recuperado 17 de julio de 2022, de https://www.iea.org/reports/data-centres-and-data-transmission-networks

[6] ¿Cómo puede el "blockchain" acreditar el origen de la energía verde? (2019, 10 octubre). Iberdrola. Recuperado 10 de abril de 2022, de https://www.iberdrola.com/innovacion/blockchain-energia

[7] F. Arute et al., *Quantum supremacy using a programmable superconducting processor*, Nature **574**, 505 (2019).

ACADEMIA DE CIENCIAS DE MORELOS, A.C.

ESTA PUBLICACIÓN FUE REVISADA POR EL COMITÉ EDITORIAL DE LA ACADEMIA DE CIENCIAS DE MORELOS

Para actividades recientes de la academia y artículos anteriores puede consultar: **www.acmor.org.mx**

¿Comentarios y sugerencias?, ¿Preguntas sobre temas científicos? CONTÁCTANOS: editorial@acmor.org.mx