# NOTAS MONETARIAS

**BANCO DE GUATEMALA**, julio - agosto 2023, No. 182, año 25

**Contenido**



## Una breve introducción al mundo de las monedas digitales

*Sergio Javier López Toledo*[1]

El dinero ha acompañado al género humano durante la mayor parte de su milenaria evolución. Es por eso que, de acuerdo a las necesidades y a la tecnología de cada época, las personas han utilizado una gran variedad de objetos como dinero.

Las distintas civilizaciones han sustentado el funcionamiento de sus economías con diferentes formas de dinero, iniciando, por supuesto, con el trueque y posteriormente con el uso de conchas marinas, granos de cacao, monedas de plata o de oro, con el dinero *fiat* que emiten bancos centrales y en la actualidad se perfila el uso de monedas digitales.

El hecho de que diversos objetos hayan sido utilizados como dinero significa que este es un proceso de mercado, ya que ha sido utilizado como medio de intercambio, reserva de valor y unidad de cuenta, lo que en la actualidad son las funciones esenciales atribuidas al dinero.

La modernización de los sistemas financieros condujo a las economías a la adopción del actual sistema de banca central, donde la autoridad monetaria tiene la prerrogativa de ser el único emisor de moneda de curso legal, es decir, el banco central tiene el monopolio de la creación de dinero y, por ende, tiene la obligación de proveer de la liquidez adecuada para el normal funcionamiento de la economía, lo cual no debería ser diferente cuando se refiere a una moneda digital.

Es importante puntualizar que, con la creación e introducción de moneda digital, los bancos centrales no necesariamente pretenden sustituir al efectivo físico por completo, solo se desea que sea un complemento para reducir los costes de transacción y como soporte de programas específicos, tal como el de inclusión financiera.

Además, es necesario disipar la confusión tendente a considerar a las criptomonedas como sinónimos de las monedas digitales emitidas por bancos centrales. Las primeras no son dinero en el sentido técnico, únicamente son activos financieros cuya creación y administración es completamente descentralizado. Las segundas, sí son dinero en el sentido conceptual y su emisión compete exclusivamente a los bancos centrales, es decir, es un sistema totalmente centralizado.

### I. El sistema de dos tramos (*Two-Tier*)

En la mayoría de libros de texto de teoría y política monetaria, se presenta a los bancos centrales administrando la oferta monetaria a través de transferencias directas, es decir, procesando transacciones directamente con el público, tal es el caso de las operaciones de mercado abierto; sin embargo, en el caso de las monedas digitales esto es técnicamente inviable, ya que podría generar una severa desintermediación financiera.

En contraste con lo mencionado, la mayoría de bancos centrales debe operativizar su gestión con monedas digitales a través de un esquema de "dos tramos" (*two-tier*). En el primer tramo, la autoridad monetaria se relaciona con los bancos privados y estos tienen una relación directa con el público, lo que constituye el segundo tramo. Esto significa que el banco central se relaciona indirectamente con los agentes económicos.

Para implementar eficientemente la gestión monetaria digital mencionada, se ha estimado conveniente utilizar el concepto de *blockchain*, el cual, por supuesto, es una derivación del concepto utilizado en criptomonedas. El *blockchain* es un sistema de contabilidad colectiva en internet, el cual está organizado y opera en grupos de datos o bloques. Este es un código abierto, totalmente transparente, que no está controlado por ninguna persona o ente externo. La información se encuentra replicada y distribuida en la red y cada nodo u ordenador conectado tiene información idéntica y, además, participa en el proceso de validación de cada transacción. De esta forma, es la propia arquitectura de la red la que protege la transacción. En caso de que algún nodo trate de modificar o falsificar cierta información, el resto de nodos lo nota e invalida esa operación.

Otro notable mecanismo de seguridad consiste en encriptar los datos, lo que implica que solo se pueden interpretar si se dispone de su clave. Además, cada bloque acumula toda la información de los bloques anteriores, por lo que se puede considerar como un libro de contabilidad actualizado en tiempo real. Cada bloque contiene la información relativa a transacciones como: emisor, cantidad, receptor, etc.

1 Elaborado por Sergio Javier López Toledo, Especialista IV de la Sección de Investigación Económica Aplicada, Departamento de Investigaciones Económicas.

En el caso específico de las monedas digitales, los bancos centrales que deseen implementar eficientemente el modelo de dos tramos, deben adaptarse para adoptar la tecnología del *blockchain*, con el objetivo adicional de utilizarlo para crear moneda digital y no solo para monitorear las transacciones de los agentes económicos. De esto se deduce que el *blockchain* utilizado en el caso de monedas digitales es completamente centralizado, a diferencia del caso de minado descentralizado que caracteriza al esquema de criptomonedas.

## II. Monederos

Los monederos son el último componente del sistema de dos tramos, los cuales están diseñados para facilitar que los agentes económicos reciban dinero y efectúen los gastos deseados. Por otra parte, aunque las experiencias de los países que han ensayado con monedas digitales es un tema a tratar en una futura nota monetaria, en la presente nota se ilustrará, básicamente, con la evidencia emanada de los ensayos realizados en la República Popular China. En este país hay que puntualizar que la autoridad monetaria se mantuvo totalmente al margen tanto del diseño como de la elaboración de los monederos de los agentes económicos y, obviamente, fueron los bancos privados y/o compañías externas las que realizaron dicho proyecto.

En esa economía asiática se inició con pruebas piloto y se determinó que las personas que deseen hacer transacciones con moneda digital deben obligatoriamente registrar la serie y número de su teléfono móvil, así como la información personal requerida por una oficina o superintendencia creada para el efecto. Además, cada monedero, al igual que en el caso de las criptomonedas, deben tener una llave pública y una privada. La primera se utiliza para tener acceso al sistema cuando se realiza una transacción entre dos monederos, mientras que la segunda permite al usuario encriptar o desencriptar monedas, lo que debe ser utilizado para que los participantes en una transacción confirmen los montos y destinatarios de sus operaciones, lo que coadyuvaría significativamente a reducir la posibilidad de fraude.

## III. Principales plataformas operativas

En la República Popular China, como se mencionó, se inició con planes piloto con muestras de población relativamente pequeñas. Para el efecto se utilizó como plataforma operativa el código *Quick Response* (QR, por sus siglas en inglés), el cual es una evolución natural del conocido código de barras. El código QR almacena información en una matriz de datos bidimensional, la cual se lee con un dispositivo móvil que tiene escáner especial.

El inicio del ensayo consistió en difundir el código mencionado y su uso correcto, lo cual fue relativamente fácil en segmentos poblacionales pequeños y bien adiestrados; sin embargo, los problemas aparecieron cuando se amplió significativamente el número de usuarios, ya que este código es muy fácil de plagiar, por lo que el número de fraudes y estafas aumentaron ostensiblemente.

Debido a lo mencionado, se ensayó con la plataforma *Near Field Communication* (NFC, por sus siglas en inglés), la cual es una tecnología inalámbrica de corto alcance que opera en la banda de 13.56MHz, por lo que no requiere de licencia alguna. Con esta tecnología se logró reducir, no erradicar, las estafas y los fraudes; sin embargo, fue muy difícil difundirla debido a que requiere de teléfonos mucho más sofisticados, los cuales no estaban al alcance de la mayoría de población rural, lo que implicaba que no ayudaría a cumplir con la política de inclusión financiera implementada por el gobierno de ese país. Además, resultó ser una tecnología con una capacidad muy lenta para procesar información, en tiempo real, de un número significativo de transacciones.

Para subsanar los problemas mencionados, el Banco Central de la República Popular China financió el desarrollo del esquema *Unspent Transaction Output* (UTXO, por sus siglas en inglés), el cual tiene la capacidad de realizar hasta 500,000 transacciones por segundo. Asimismo, con la misma velocidad que acredita a una cuenta, tiene la capacidad de debitar el cambio, incluso cuando la transacción involucra números decimales. Esta plataforma logró minimizar la probabilidad de fraudes y ampliar la funcionalidad y la operatividad del sistema de moneda digital, aunque a un costo financiero muy alto.

## IV. Estructura básica de las monedas digitales

La creación de una moneda digital segura, eficiente y eficaz es, sin duda, el principal reto dentro de este esquema. En efecto, el diseño debe conservar la confianza absoluta de los agentes económicos, ya que esto es lo que sustenta a toda moneda *fiat* emitida por un banco central.

Las monedas digitales son simplemente *tokens* (códigos), los cuales se generan a través del uso de técnicas criptográficas. Estos *tokens*, al ser equivalentes al dinero físico, deben tener un número único de serie de emisión, la cantidad que representa, el nombre del emisor y, en este caso, el del propietario o portador.

Lo mencionado significa que cada unidad monetaria digital, independientemente de la cantidad que representa, debe estar asociada a un código criptográfico único, lo que implica que la autoridad monetaria debe tener la capacidad física de crear y destruir cientos de millones de *tokens*.

Además, como se mencionó, cada usuario de moneda digital debe registrar ante la autoridad competente, tanto su teléfono móvil como su número de identificación personal. Esta información pasa automáticamente al código de cada unidad monetaria digital al momento de ser el portador y, por supuesto, al realizar una transacción se adhiere la información del nuevo propietario de dicha moneda digital.

El registro sistemático de los diversos portadores de un *token* es una garantía de autenticidad y, sobre todo, de seguridad. Asimismo, es una herramienta sumamente eficaz contra el lavado de dinero, ya que siempre se registra la identidad de los agentes económicos involucrados en una transacción, lo que les permite a las autoridades contar con el historial de posesión del *token*.

Lo indicado explica, en gran parte, la razón por la cual ha sido extremadamente difícil implementar un esquema de monedas digitales. El costo financiero y la complejidad técnica requerida para generar cientos de miles de millones de *tokens*, seguros, eficientes y eficaces, es extremadamente alto para los países más desarrollados y está muy lejos del alcance de los países en desarrollo como Guatemala.

## V. Institucionalidad requerida

La implementación de un esquema de monedas digitales implica la creación de, al menos, tres nuevos departamentos, los cuales, aunque de carácter operativo, son de mucha importancia para el funcionamiento eficiente y eficaz de este sistema. A continuación se discuten las principales características y atributos de esos departamentos.

### a. Centro de verificación

Este centro debería ser una plataforma centralizada, ya que sus principales funciones serían, por un lado, verificar la autenticidad de la identidad de cada usuario de moneda digital y, por el otro, registrar los teléfonos celulares que se utilizarán para realizar transacciones con moneda digital.

Para armonizar y operativizar las funciones arriba indicadas, el centro de verificación deberá mantener el historial de las transacciones realizadas por los bancos con cada uno de sus usuarios, ya que deberá conciliar la información mencionada con el uso adecuado de las llaves públicas y privadas de cada usuario.

### b. Centro de registro

Este es el departamento donde se generan las monedas digitales (*tokens*) y, al final de su vida útil, se destruyen. Asimismo, es el principal centro operativo debido a que provee la energía necesaria para procesar, a velocidad colosal, las transacciones de encriptamiento y desencriptamiento de las monedas digitales. Además, en este centro se deberá monitorear el flujo de monedas digitales hacia todo el sistema, manteniendo un récord actualizado de las transacciones realizadas por cada uno de los agentes económicos.

El centro de registro no solo debe satisfacer las necesidades de energía del sistema, sino también proveer la capacidad informática para autenticar y confirmar, a través de cálculos criptográficos, las transacciones que se lleven a cabo en el mercado, lo que implica que deberá contar con la suficiente infraestructura física y técnica para identificar y autenticar, en tiempo real, cada una de las transacciones realizadas con monedas digitales.

Debido a que una persona puede tener diversas cuentas monetarias, por ende, también podrá poseer varios monederos de moneda digital, lo que implica que cada uno de esos monederos se le debe aplicar un proceso de autenticación, ya que en el sistema operarán una gran variedad de dispositivos móviles, algunos con capacidad de identificación biométrica y mucho poder operativo, mientras que otros extremadamente primitivos. Para cumplir con esta tarea, este centro deberá contar con el sofisticado y costoso programa *Message Authentication Codes* (MAC).

Además, este departamento tendrá tanto la meta, como el objetivo de que cada moneda digital sea única, confidencial y, sobre todo, a prueba de fraude. Es importante recalcar que todas las técnicas criptográficas mencionadas demandarán una cantidad considerable de energía, por lo que los especialistas encargados de diseñar esas técnicas criptográficas, tendrán que buscar el delicado equilibrio entre la necesaria velocidad operativa y la seguridad imprescindible del sistema.

### c. Centro de análisis de datos

El centro de análisis de datos es el verdadero cerebro del sistema, ya que, en tiempo real, podrá recibir y analizar las transacciones efectuadas con moneda digital. Cualquier incoherencia y/o anomalía referente a quién, cómo y dónde se realiza una determinada transacción, así como lo referente a la identidad de los propietarios de la moneda con la que se realiza una transacción, deberá ser alertada por este centro.

El departamento de análisis de datos sería equivalente al concepto de "la nube" que se utiliza regularmente, para designar a la infraestructura o plataforma que aloja una gran cantidad de programas, ofrecidos por proveedores externos y que se ponen a disposición de usuarios por medio de internet. Este departamento garantiza la prevención efectiva contra el fraude y el lavado de dinero.

## VI. Conclusiones

El dinero es un bien utilizado como medio de intercambio, reserva de valor y unidad de cuenta. A pesar de que, a través de la historia económica, muchos bienes han sido utilizados como dinero, en la actualidad son los bancos centrales los que tienen el monopolio de emitir dinero. Lo cual requiere la absoluta confianza del público para que dicho dinero cumpla con las funciones mencionadas. Esto no es distinto cuando se habla de monedas digitales creadas y emitidas por un banco central.

Es de suma importancia no confundir a las criptomonedas con las monedas digitales emitidas por un banco central, ya que las primeras solo son activos financieros y, por ende, no le permiten a la autoridad monetaria ejecutar una política monetaria fluida, eficiente y eficaz.

Respecto de la gestión monetaria con monedas digitales, esta se debe ejecutar siguiendo el esquema de dos tramos, ya que esto le permite al banco central tener una relación fluida con los bancos del sistema y estos, a su vez, con el público. Esta relación debe estar sustentada en la adaptación de los *blockchain*, lo cual es tomado de los esquemas de criptomonedas.

El esquema de monedas digitales debe contar con un sistema de monederos confiables y de fácil administración para cualquier usuario, lo que implica que cada persona debe tener acceso a una llave pública y a una privada. Además, el diseño de los monederos debe estar a cargo de entes ajenos a la autoridad monetaria, ya que cualquier tipo de fraude y/o estafa colectiva podría dañar considerablemente la reputación y credibilidad del banco central, las cuales son los principales activos con que cuenta toda autoridad monetaria seria.

Congruente con lo mencionado, el diseño de las unidades monetarias digitales debe garantizar la seguridad contra la falsificación, aunque con esto se sacrifique significativamente la privacidad de las transacciones de los agentes económicos.

Para cumplir a cabalidad con lo expuesto, la banca central debe ampliar su institucionalidad, ya que las nuevas funciones que demanda un esquema de monedas digitales implican la creación de nuevos departamentos.

Estos departamentos son de carácter operativo y deben, como en el caso del centro de verificación, garantizar la autenticidad de las transacciones, la confiabilidad de la creación y destrucción de los *token* y la disponibilidad de energía para el sistema que estaría a cargo del centro de registro y, por último, el centro de análisis de datos, el cual es el verdadero cerebro del sistema debido a que verificará datos de suma importancia como, por ejemplo, la autenticidad de las transacciones realizadas con moneda digital.

Como se puede apreciar, la creación y funcionamiento de un esquema de monedas digitales emitidas, por un banco central serio, demanda de una gran cantidad de capital tanto humano como físico. En efecto, existen varios bancos centrales que han manifestado su intención de adquirir computadoras cuánticas con el fin de poner en marcha programas de monedas digitales. Cabe puntualizar que los requerimientos de capital humano y físico para implementar un programa de monedas digitales es financieramente muy oneroso tanto para países desarrollados como en desarrollo, por lo que su implementación tomará más tiempo de lo inicialmente previsto.

## Bibliografía

Prasad, S. Eswar (2021): The Future of Money. **How the Digital Revolution is Transforming Currencies and Finance.** Cambridge, Massachusetts: The Belknao Press of Harvard University Press.

Turrin, Richard (2021): **China´s Digital Currency Revolution. Cashless.** California: Authority Publishing.

Torres, José Manuel (2022): **Criptomonedas. Qué son, cómo utilizarlas y por qué van a cambiar al mundo.** México: Ediciones Culturales Paidós.

## Directorio

**Director**
Johny Rubelcy Gramajo M.

**Consejeros**
Jorge Vinicio Cáceres Dávila
Herberth Solórzano Somoza

**Coordinador**
Ronald Vinicio Ruiz Alonzo

**Producción**
Diego Ovalle

**Edición de textos**
Juan Francisco Sagüí Argueta

**Arte y Diagramación**
Paulina Tercero

**Impresión**
Taller Nacional de Grabados en Acero

**Notas Monetarias** es un órgano divulgativo de información económico-financiera actualizada, de periodicidad bimestral y distribución gratuita. De aparecer colaboraciones especiales, sus autores serán entera y exclusivamente responsables por sus opiniones y, de consiguiente, estas no reflejarían la posición oficial del Banco de Guatemala, a menos que ello se haga constar de modo expreso. Es libre la reproducción de los artículos, gráficas y cifras que figuren en esta publicación, siempre y cuando se mencione la fuente. Toda correspondencia deberá dirigirse a: Notas Monetarias del Banco de Guatemala, 7a. avenida, 22–01, zona 1, Ciudad de Guatemala, Código Postal No. 01001.