EL NUEVO RETO DE CIBERSEGURIDAD DE LOS BANCOS CENTRALES

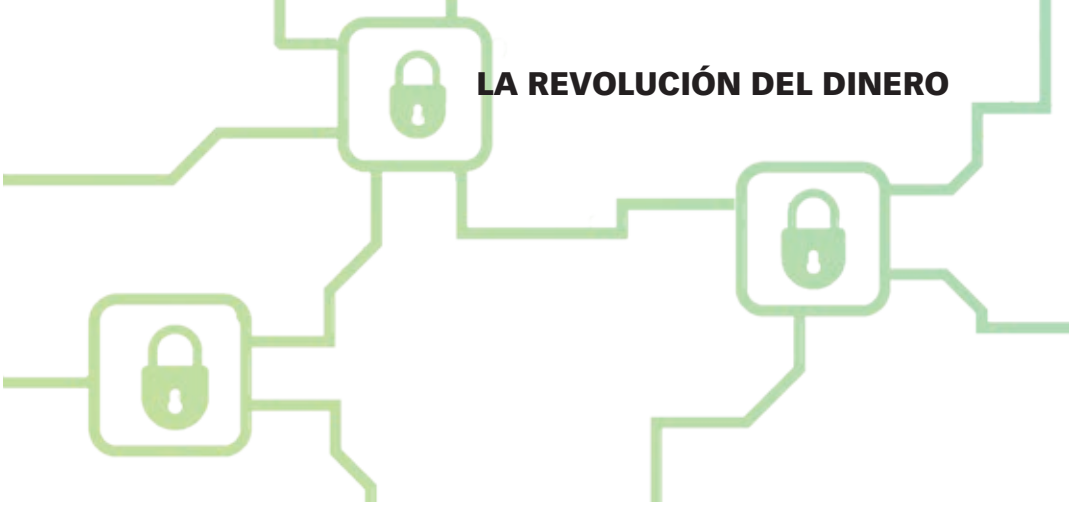
Las monedas digitales de los bancos centrales pueden plantear riesgos de seguridad, pero si están bien diseñadas también pueden generar oportunidades

Giulia Fanti, Josh Lipsky y Ole Moehr

En el mundo habitualmente cauto de los bancos centrales, la idea de las monedas digitales de los bancos centrales (MDBC) está avanzando a un ritmo vertiginoso. Según una investigación del Atlantic Council GeoEconomics Center, 105 países y uniones monetarias están pensando en lanzar una MDBC minorista (emitida para el público general) o mayorista (utilizada principalmente para transacciones interbancarias). Se estima que en 2020 solo unos 35 países tenían tales planes. Y el interés no se limita a las economías pequeñas: 19 países del Grupo de los Veinte (G-20) están pensando en emitir MDBC, y la mayoría ya han superado la fase de investigación.

Pero a medida que más países experimentan con MDBC, acechan temores relativos a la ciberseguridad y la privacidad. Jerome Powell, presidente de la Reserva Federal, dijo recientemente que el "ciberriesgo" era su principal temor en relación con la estabilidad financiera, y un informe reciente de la Cámara de los Lores del Reino Unido cita en concreto los riesgos de ciberseguridad y privacidad como posibles motivos para no desarrollar una MDBC.

No son temores infundados. Las vulnerabilidades de las MDBC podrían poner en riesgo el sistema financiero de un país. Las MDBC podrían acumular datos confidenciales sobre pagos y usuarios a una escala jamás vista. En las manos equivocadas, esos datos permitirían espiar transacciones privadas, obtener



La tecnología permite que los bancos centrales incorporen la protección de la ciberseguridad y la privacidad en el diseño de cualquier MDBC.

detalles confidenciales sobre personas y organizaciones, e incluso robar dinero. Si se adopta sin los debidos protocolos de seguridad, una MDBC podría ampliar el alcance y la escala de muchas amenazas a la seguridad y la privacidad que ya existen en el sistema financiero.

Hasta no hace mucho, era poco lo que se había hecho en el ámbito público para comprender los riesgos específicos de ciberseguridad y privacidad asociados con las MDBC. Pocos habían analizado si el diseño de estas monedas podía mitigar los riesgos o incluso mejorar la ciberseguridad de un sistema financiero.

Nuestro nuevo estudio, publicado en el informe reciente del Atlantic Council sobre el problema de la ciberseguridad y las MDBC ("Missing Key—The Challenge of Cybersecurity and CBDCs"), analiza los nuevos riesgos de ciberseguridad que esas monedas podrían implicar para los sistemas financieros y sostiene que las autoridades disponen de numerosas opciones para introducir las MDBC de forma segura. Las MDBC presentan muchas variantes de diseño, que van desde bases de datos centralizadas hasta registros distribuidos y sistemas basados en tókenes. Cada diseño debe analizarse antes de sacar conclusiones sobre los riesgos de ciberseguridad y privacidad. Además, deben compararse con el sistema financiero actual —el que inquieta a Powell— para determinar si la nueva tecnología puede ofrecer opciones más seguras.

¿Cuáles son los principales riesgos de ciberseguridad a los que podría dar lugar una MDBC? Y, lo que es más importante: ¿qué se puede hacer para mitigarlos?

Recopilación de datos centralizada

Muchas de las variantes de diseño propuestas para las MDBC (en especial las minoristas) implican la recopilación centralizada de datos de transacciones, lo que supone importantes riesgos de privacidad y seguridad. En términos de privacidad, esos datos podrían usarse para vigilar las actividades de pago de los ciudadanos. Acumular tantos datos confidenciales en un solo lugar también agrava el riesgo de seguridad, ya que el botín que podrían llevarse los posibles intrusos es mucho más valioso.

Sin embargo, los riesgos vinculados a la recopilación centralizada de datos pueden mitigarse ya sea no recopilándolos u optando por una arquitectura de validación en la que cada componente acceda solo a la información que necesita para funcionar. Para esto último, algo que puede ayudar son las herramientas criptográficas, como las pruebas de conocimiento cero, que autentican información privada sin revelarla ni permitir que se vulnere, o técnicas de cifrado criptográfico. Por ejemplo, el Proyecto Hamilton (una iniciativa conjunta de la Reserva Federal de Boston y el Instituto Tecnológico de Massachussetts para analizar una MDBC de Estados Unidos) diseñó un sistema que separa en fases la validación de transacciones, y cada fase necesita acceso a una parte distinta de los datos de la transacción.

Estas técnicas criptográficas pueden ampliarse más para crear sistemas que comprueben la validez de la transacción solo con acceso cifrado a detalles como el emisor, el receptor o el importe. Suena a algo demasiado bueno para ser real, pero estas herramientas se han probado exhaustivamente en criptomonedas que preservan la privacidad, como Zcash, y que se basan en importantes avances logrados en el ámbito de la criptografía. Lo importante es que la tecnología permite que los bancos centrales incorporen la protección de la ciberseguridad y la privacidad en el diseño de cualquier MDBC.

Transparencia o privacidad

Algo que suele preocupar de los diseños que velan por la privacidad (incluidos los que usan técnicas criptográficas especializadas) es la menor transparencia frente a los entes reguladores. En general, los reguladores tienen que poder acceder a información que les permita percatarse de transacciones sospechosas y detectar casos de lavado de dinero, financiamiento del terrorismo y otras actividades ilícitas.

Pero aun así lo uno no excluye lo otro. Es posible usar técnicas criptográficas para diseñar MDBC

FOTO: FUNTAP A TRAVÉS DE GETTY IMAGES

Es fundamental contar con normas internacionales y más intercambio de conocimientos entre bancos en este momento de rápida evolución y adopción.

que ofrezcan un nivel de privacidad similar al del efectivo hasta un umbral determinado (por ejemplo, USD 10.000) y que permitan al mismo tiempo una supervisión suficiente por parte de las autoridades. Este tipo de umbrales no difiere mucho del sistema actual de Estados Unidos, que establece requisitos de información menos estrictos para las transacciones por debajo de los USD 10.000. Lo cierto es que, en muchos sentidos, un nuevo sistema de MDBC no tendría que reinventar los protocolos de seguridad, sino que podría mejorarlos.

Muchos países se comprometieron a adoptar, o incluso llegaron a adoptar, MDBC minoristas con una infraestructura basada en la tecnología de registro distribuido. La eNaira de Nigeria, lanzada en octubre de 2021, es un buen ejemplo. Esos diseños exigen la participación de terceros como agentes de validación de las transacciones. Esto crea una nueva función para estos terceros (por ejemplo, instituciones financieras y no financieras) en las operaciones monetarias del banco central. Algo de suma importancia es que las garantías de seguridad de los registros dependerían de la integridad y la disponibilidad de agentes de validación externos, sobre los que el banco central no puede ejercer control directo. (Si bien es posible adoptar una tecnología de registro distribuido en la que todos los agentes de validación están controlados por el banco central, eso desbarataría el propio fin de esta tecnología). Los riesgos conexos podrían mitigarse con mecanismos normativos, como requisitos de auditorías y la obligación de denunciar infracciones. Sin embargo, no existe un plan claro para diseñar esas normas en un sistema tan sujeto a plazos y estrechamente interconectado como el de una MDBC basada en un registro distribuido. Es por eso que es fundamental contar con normas internacionales y más intercambio de conocimientos entre bancos en este momento de rápida evolución y adopción.

¿Amenaza u oportunidad?

En los últimos 18 meses, algunos bancos centrales se han apresurado a decidir que una MDBC implica demasiados riesgos. Queríamos determinar qué constituye realmente una amenaza y qué es en efecto una oportunidad. La conclusión es que los gobiernos tienen muchas opciones a la hora de diseñar una MDBC, incluidas algunas variantes nuevas aún no probadas cabalmente en los actuales proyectos experimentales de los bancos centrales. Esas variantes presentan diversas disyuntivas en cuanto a resultados, seguridad y privacidad. Los gobiernos deben elegir el diseño en función de sus necesidades y prioridades en materia de políticas. Según nuestra evaluación, las MDBC no son inherentemente más o menos seguras que los sistemas actuales. Ineludiblemente, un diseño prudente debe tener en cuenta la ciberseguridad, pero no a tal punto que eso niegue de entrada la posibilidad de diseñar MDBC y someterlas a prueba.

Nuestra investigación deja algo muy en claro. Si no hay coordinación, es probable que las iniciativas internacionales den lugar a problemas de interoperabilidad y riesgos de ciberseguridad transfronterizos. Lógicamente, los países se concentran en el uso interno, sin prestar demasiada atención a la normativa internacional, la interoperabilidad y el establecimiento de normas. Ya sea que Estados Unidos decida o no adoptar una MDBC, la Reserva Federal, como emisor de una moneda de reserva mundial importante, debe impulsar la elaboración de reglas mundiales para las MDBC en los organismos normativos. Los foros financieros internacionales, como el Banco de Pagos Internacionales, el FMI y el G-20 han de cumplir un papel igualmente importante.

Los riesgos de ciberseguridad y privacidad de las MDBC son reales. Pero las soluciones están al alcance de los tecnólogos y las autoridades responsables de las políticas. Sería una lástima que se decida que los riesgos son demasiado altos antes de desarrollar soluciones que, en realidad, podrían ayudar a crear un sistema financiero mundial más moderno y estable. FD

GIULIA FANTI es investigadora principal en el Atlantic Council GeoEconomics Center y profesora adjunta de ingeniería eléctrica e informática en la Universidad Carnegie Mellon.
JOSH LIPSKY es Director principal del Atlantic Council GeoEconomics Center y exfuncionario del FMI.
OLE MOEHR es investigador en el Atlantic Council GeoEconomics Center.