El ecosistema criptográfico - Elementos clave y riesgos

Informe presentado a los ministros de Finanzas y Gobernadores de los Bancos Centrales del G20.



**BIS Otros**|**11 julio 2023**

[**PDF texto completo** (1,193kb)](https://www.bis.org/publ/othp72.pdf)|27 páginas

* **Otro informe presentado al G20:** [**Lecciones aprendidas sobre las CBDC**](https://www.bis.org/publ/othp73.htm)

Este informe revisa los elementos clave del ecosistema criptográfico y evalúa sus fallas estructurales. Hay tres conclusiones principales. En primer lugar, debido a los incentivos económicos subyacentes, el ecosistema criptográfico se caracteriza por la congestión y las altas tarifas, lo que conduce a la fragmentación. En segundo lugar, a pesar de un espíritu original de descentralización, las criptomonedas y las finanzas descentralizadas (DeFi) a menudo presentan una centralización sustancial de facto, lo que introduce varios riesgos. En tercer lugar, si bien DeFi replica principalmente los servicios ofrecidos por el sistema financiero tradicional, amplifica los riesgos conocidos. Además, como DeFi no financia la actividad en la economía real, su crecimiento está impulsado por la afluencia especulativa de nuevos usuarios, lo que plantea riesgos sustanciales para los inversores. El informe describe opciones de políticas para mitigar los múltiples riesgos que las criptomonedas representan para los inversores.

**Información relacionada**

* [Plan para el futuro sistema monetario: mejorar el antiguo, habilitar el nuevo](https://www.bis.org/publ/arpdf/ar2023e3.htm)
* [Investigación sobre tecnología financiera del BIS](https://www.bis.org/topic/fintech/research.htm)
* [El futuro sistema monetario](https://www.bis.org/publ/arpdf/ar2022e3.htm)
* [Proyecto Atlas: Mapeando el mundo de las finanzas descentralizadas](https://www.bis.org/about/bisih/topics/suptech_regtech/atlas.htm)



1. Introducción

La capitalización de mercado del ecosistema criptográfico, a pesar de una disminución significativa en 2022, se encuentra en los billones de dólares, y hay miles de monedas criptográficas en circulación. La difusión de la criptografía ha sido de naturaleza global e impulsada por una amplia gama de inversores.

En teoría, el universo criptográfico se basa en la premisa de la descentralización. En lugar de depender del dinero del banco central y de intermediarios de confianza, la criptografía prevé que el mantenimiento de registros de las transferencias sea proporcionado por una multitud de validadores anónimos. Las finanzas descentralizadas, o "DeFi", buscan replicar los servicios financieros convencionales de una manera descentralizada dentro del universo criptográfico, a menudo respaldada por el medio de intercambio de las monedas estables. DeFi incorpora innovaciones como la programabilidad y la componibilidad en blockchains. Dichos sistemas están "siempre encendidos", lo que permite transacciones en todo el mundo las 24 horas del día, los siete días de la semana.

Los acontecimientos recientes revelaron una amplia divergencia entre la visión criptográfica y la realidad. Aunque la criptografía opera bajo la bandera de la descentralización, en la práctica los nuevos intermediarios centralizados han desempeñado un papel clave en la canalización de fondos hacia el universo criptográfico e intermediación dentro de él. La implosión del intercambio de criptomonedas FTX es solo la manifestación más notable de las vulnerabilidades del sector. En lugar de proporcionar una arquitectura financiera más resistente, la criptografía mostró las mismas vulnerabilidades bien conocidas de las finanzas tradicionales, pero de manera amplificada.

Este informe revisa los elementos clave del ecosistema criptográfico y evalúa sus defectos estructurales. Luego repasa los riesgos que plantea y discute las opciones para abordarlos. También identifica las brechas de datos y discute formas de aliviarlas.

El informe tiene tres conclusiones clave. En primer lugar, el ecosistema criptográfico está sujeto a un alto grado de fragmentación y se caracteriza por la congestión y las altas tarifas. Este habría sido el caso incluso si se hubiera mantenido fiel a su espíritu descentralizado original. Estos defectos estructurales se derivan de la economía subyacente de los incentivos de los validadores más que de la tecnología. Y si bien la criptografía ha ofrecido algunos elementos de innovación genuina, estos pueden replicarse o integrarse en el sistema financiero tradicional más seguro y confiable (BIS (2023)). En segundo lugar, a pesar de un espíritu original de descentralización, crypto y DeFi a menudo presentan una centralización sustancial de facto, lo que introduce varios puntos débiles. Un buen ejemplo se refiere a las monedas estables, que aprovechan la credibilidad de la unidad de cuenta del banco central y pueden plantear riesgos para la soberanía monetaria. En tercer lugar, si bien DeFi replica principalmente los servicios ofrecidos por el sistema financiero tradicional, no financia ninguna actividad en la economía real, sino que amplifica los riesgos conocidos. Como el crecimiento está impulsado principalmente por la afluencia especulativa de nuevos usuarios que esperan altos rendimientos, la criptografía y el DeFi plantean riesgos sustanciales para los inversores (especialmente minoristas). En resumen, los defectos estructurales inherentes de la criptografía la hacen inadecuada para desempeñar un papel constructivo en el sistema monetario (BIS (2022)).

2. Los elementos clave del ecosistema criptográfico

Esta sección describe los principales componentes del ecosistema criptográfico. Comienza rastreando el desarrollo de Bitcoin y la tecnología blockchain. Luego discute el creciente papel de los intermediarios centralizados en el ecosistema. En particular, analiza las monedas estables, que con mayor frecuencia son emitidas por entidades centralizadas y pasaron de ser una solución a medida a la volatilidad inherente de los activos criptográficos a convertirse en un pilar del ecosistema criptográfico. La sección concluye con una discusión sobre los contratos inteligentes y las aplicaciones financieras descentralizadas que se basan en ellos. Los términos técnicos utilizados a lo largo de este informe se definen en el Glosario.

2.1 Criptomoneda sin respaldo

El nacimiento de las criptomonedas data de la introducción de Bitcoin en 2009: un medio descentralizado de igual a igual para transferir valor en un libro mayor público compartido (es decir, una cadena de bloques pública que utiliza tecnología de contabilidad distribuida (DLT)). En su formulación original, la criptografía se caracterizaba por no estar respaldada por ningún activo, así como por una afirmación declarada de reducir la influencia de los intermediarios a través de la descentralización (Nakamoto (2008)).

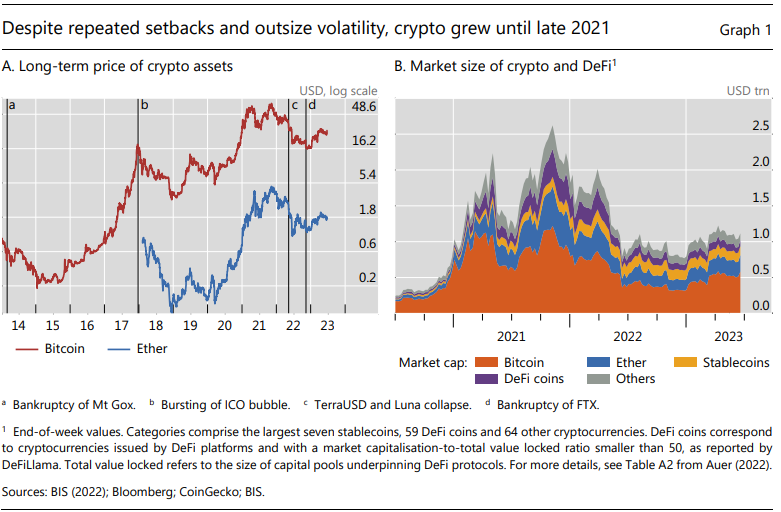
La propiedad de los criptoactivos y las transacciones con ellos son verificadas por validadores descentralizados y registradas en el libro mayor. Si un vendedor desea transferir criptoactivos a un comprador, el comprador (identificado a través de su firma digital criptográfica) transmite los detalles de la transacción, por ejemplo, las partes que realizan transacciones, el monto o las tarifas. Los validadores (en algunas redes llamadas "mineros") luego compiten para verificar la transacción, y quien es seleccionado para verificar agrega la lista de transacciones a la cadena de bloques y es compensado en tarifas pagadas en criptoactivos. La cadena de bloques actualizada se comparte entre todos los mineros y usuarios. De esta manera, el historial de todas las transacciones es públicamente observable y está vinculado a billeteras específicas, mientras que las verdaderas identidades de las partes detrás de las transacciones (es decir, los propietarios de las billeteras) permanecen sin revelar. En este sentido, las transacciones en blockchains son pseudo-anónimas. Al transmitir toda la información públicamente, el sistema verifica que cada transacción sea consistente con el historial de transferencias en la cadena de bloques, por ejemplo, que la criptomoneda realmente pertenece al vendedor y no se ha gastado más de una vez.

A medida que los criptoactivos comenzaron a atraer una mayor atención de los inversores potenciales, las entidades centralizadas desempeñaron un papel más importante en la canalización de fondos hacia las criptomonedas. En particular, los intercambios centralizados, que facilitaron la conversión entre Bitcoin, otros criptoactivos y dinero fiduciario, contribuyeron al aumento de los precios de las criptomonedas al atraer a nuevos participantes, en un bucle que se refuerza a sí mismo. Los intermediarios centralizados (especialmente plataformas como Mt Gox en los primeros días, y más recientemente Binance, Coinbase, Kraken y FTX hasta su repentino colapso a fines de 2022) han reafirmado su papel clave en el ecosistema criptográfico una y otra vez. Este sistema ha llegado a ser conocido dentro del espacio criptográfico como finanzas centralizadas (CeFi), y sus altibajos han contribuido a la volatilidad de los precios de los criptoactivos (Gráfico 1.A).

2.2 Monedas estables

Las monedas estables se han establecido como el principal medio de intercambio dentro del ecosistema criptográfico y como una puerta de entrada a él. Se llaman así porque tienen como objetivo mantener un valor estable en relación con un activo específico o conjunto de activos. Las monedas estables generalmente están vinculadas a un numerario, casi siempre el dólar estadounidense, pero también pueden apuntar al precio de otras monedas o activos (por ejemplo, oro o incluso otros criptoactivos). De esta manera, buscan superar la alta volatilidad y la baja liquidez para desempeñar el papel de un medio de intercambio en el universo criptográfico. Las monedas estables también juegan un papel clave en el ecosistema DeFi (ver siguiente sección).

Las monedas estables vienen en dos tipos principales, dependiendo de cómo intenten mantener su paridad (FSB (2022)). La mayoría de los acuerdos de monedas estables son administrados por un intermediario centralizado y están "respaldados por activos". Los activos subyacentes pueden incluir bonos del gobierno de Estados Unidos, deuda corporativa a corto plazo o depósitos bancarios. El intermediario centralizado invierte la garantía subyacente y coordina el reembolso y la creación de las monedas. Las monedas estables más destacadas son Tether, USD Coin (USDC) y Binance USD. Las "monedas estables algorítmicas", por el contrario, tienen como objetivo reequilibrar automáticamente el suministro a través del arbitraje con un token volátil emparejado para mantener la paridad. Por lo general, no están respaldados por activos del mundo real, siendo el ejemplo más destacado la fallida moneda estable TerraUSD.



2.3 Contratos inteligentes y finanzas descentralizadas

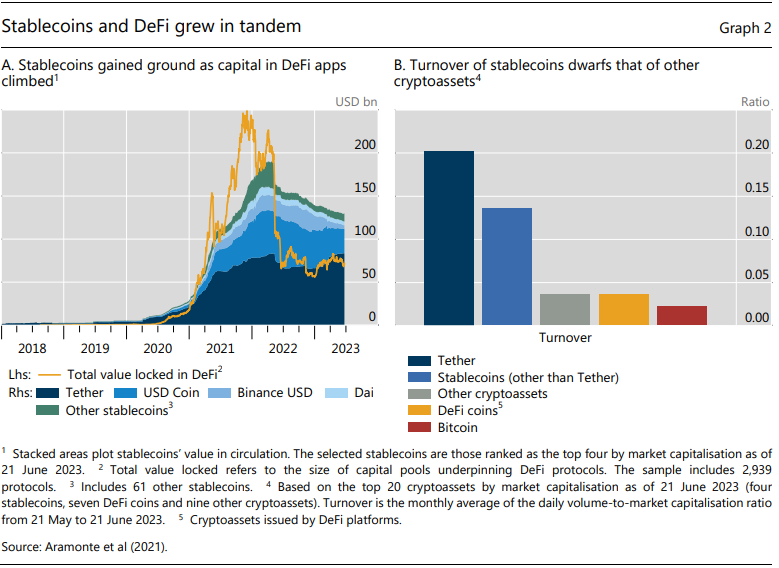
Desde el advenimiento de Bitcoin, muchas otras cadenas de bloques y monedas criptográficas asociadas han entrado en escena, especialmente Ethereum y su moneda nativa asociada Ether en 2015 (Gráfico 1.B). Ethereum y muchas de las cadenas de bloques más nuevas permiten la "programabilidad", es decir, dan a los desarrolladores la opción de crear aplicaciones sobre su cadena de bloques mediante el uso de los llamados contratos inteligentes.

Los contratos inteligentes son código autoejecutable que desencadena una acción si se cumplen ciertas condiciones preespecificadas. Pueden automatizar algunas funciones del mercado y, hasta cierto punto, obviar a los intermediarios que tradicionalmente se requieren para tomar decisiones. Por lo tanto, es mejor considerarlos como contratos desatendidos (Neilson (2021)). El código subyacente está disponible públicamente (es decir, código abierto) y puede ser examinado. Como los contratos inteligentes no pueden acceder directamente a la información que reside "fuera de la cadena", es decir, fuera de la cadena de bloques específica, requieren los llamados oráculos como mediadores para proporcionar dichos datos.

Una característica importante de los contratos inteligentes es su "componibilidad", es decir, la capacidad de combinar diferentes componentes en el sistema. Los usuarios pueden realizar transacciones complejas en la misma cadena de bloques combinando múltiples instrucciones dentro de un solo contrato inteligente, como "money lego".

La programabilidad también abrió la puerta a DeFi, un nuevo ecosistema para la prestación de servicios criptográficos. DeFi tiene como objetivo ofrecer servicios y productos financieros tradicionales en la cadena de bloques, con el objetivo declarado de una mayor transparencia y eliminar a los intermediarios para reducir los costos. Los protocolos DeFi combinan múltiples contratos inteligentes para proporcionar servicios de préstamos, préstamos y comercio dentro del ecosistema criptográfico. Las aplicaciones descentralizadas (DApps) son interfaces gráficas que permiten a los usuarios interactuar con protocolos desde sus ordenadores o smartphones. Si bien no son estrictamente necesarios para interactuar con el ecosistema DeFi, ya que los usuarios pueden configurar su propia interfaz, son el punto de entrada a DeFi para todos, excepto para los participantes más expertos.

Las monedas estables desempeñan un papel importante en el ecosistema DeFi al servir como medio de intercambio en una amplia gama de actividades (Gráfico 2.A).4 Por un lado, proporcionan liquidez al ecosistema DeFi al permitir a los usuarios entrar y salir de aplicaciones descentralizadas. Relacionadamente, las monedas estables sirven como pares comerciales para otros criptoactivos en intercambios descentralizados, lo que permite a los usuarios intercambiar criptomonedas sin tener que volver a convertir a moneda fiduciaria, lo que reduce los costos de transacción. Además, las monedas estables se utilizan ampliamente en las plataformas de préstamos y préstamos DeFi, donde los usuarios piden prestado y prestan monedas estables contra garantías en forma de otros criptoactivos. Debido a este papel clave, el volumen de negocios en monedas estables generalmente empequeñece al de otros criptoactivos (Gráfico 2.B).



Los principales tipos de actividad financiera en DeFi, como préstamos, comercio y seguros, son los mismos que los ya disponibles en las finanzas tradicionales. Las plataformas de préstamos permiten a los usuarios prestar sus monedas estables con intereses a los prestatarios que publican otras criptomonedas como garantía. Los intercambios descentralizados (DEX) representan mercados donde las transacciones ocurren directamente entre comerciantes de criptomonedas o monedas estables, y los precios se determinan a través de fórmulas matemáticas automatizadas. En las plataformas de seguros DeFi, los usuarios pueden asegurarse contra algunos riesgos dentro del sistema criptográfico, por ejemplo, el mal manejo de claves privadas, hacks de intercambio o fallas de contratos inteligentes, recibiendo criptoactivos como compensación.

Sin embargo, las actividades de DeFi implican casi exclusivamente el intercambio de una moneda estable o criptomoneda por otra, y no financian la actividad en la economía real. En este sentido, el sistema es principalmente autorreferencial y se utiliza para la especulación en monedas.5 El crecimiento está impulsado principalmente por la afluencia continua de nuevos usuarios que esperan altos rendimientos. De hecho, la evidencia reciente sugiere que el aumento de los precios de las criptomonedas es seguido por una adopción significativamente mayor de las aplicaciones de comercio de criptomonedas, ya que los nuevos usuarios se sienten atraídos por la perspectiva de nuevas ganancias.

3. Defectos estructurales y riesgos

Esta sección destaca que, a pesar del potencial para la innovación tecnológica genuina, la criptografía tiene fallas estructurales inherentes que plantean serios riesgos no solo para su propia estabilidad y seguridad, sino también para el sistema financiero tradicional. La sección primero revisa los principales defectos estructurales del ecosistema criptográfico, incluida la congestión, la fragmentación y la necesidad de pedir prestada credibilidad al dinero soberano. También discute los problemas derivados de la necesidad de centralización. La sección luego resume los principales riesgos, dividiéndolos en riesgos dentro del ecosistema criptográfico (incluidos los riesgos para la integridad del mercado, la protección del consumidor y la privacidad), riesgos específicos de DeFi y riesgos derivados de la interconexión con el sistema financiero tradicional. Luego, la sección analiza las opciones para abordar los riesgos planteados por la criptografía, antes de cerrar con una discusión de las brechas de datos que actualmente dificultan el monitoreo.

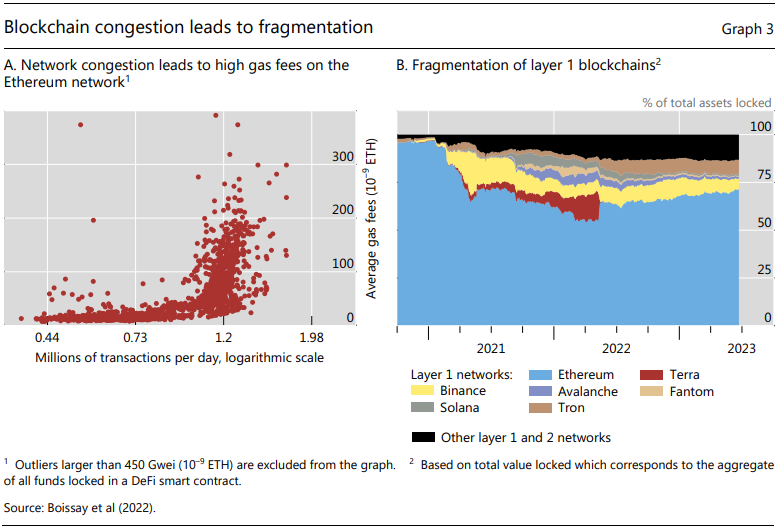
3.1 Defectos estructurales

3.1.1 Fragmentación y congestión

La criptografía, incluso en su forma original, totalmente descentralizada, sufre de limitaciones inherentes de las cadenas de bloques sin permiso que conducen a la fragmentación del sistema, acompañada de congestión y altas tarifas.7 El rastreo de las razones de la fragmentación destaca por qué las limitaciones no son tecnológicas, sino que provienen de estructuras de incentivos.

En la cadena de bloques, los validadores interesados son responsables de registrar la propiedad y las transacciones. Sin embargo, en el sistema criptográfico pseudo-anónimo, no tienen reputación en juego y el anonimato impide la rendición de cuentas. En cambio, deben ser incentivados a través de recompensas monetarias suficientemente altas para informar con veracidad y sostener el sistema de consenso descentralizado. La validación honesta debe producir rendimientos más altos que las ganancias potenciales de hacer trampa. Si las recompensas se vuelven demasiado bajas, los validadores individuales tendrían un incentivo para engañar y robar fondos, poniendo en peligro la seguridad general (Budish, 2022).

Una forma común de recompensar a los validadores para mantener los incentivos es limitar la capacidad de la cadena de bloques, manteniendo así altas tarifas sostenidas por la congestión (Huberman et al (2021)). Como los validadores pueden elegir qué transacciones se validan y procesan, los períodos de congestión hacen que los usuarios ofrezcan tarifas más altas para procesar sus transacciones (Gráfico 3.A). La congestión y las altas tarifas también significan que los sistemas de pago basados en blockchains descentralizados seguirán siendo comparativamente lentos y costosos.



El problema de la capacidad de blockchain es una manifestación del llamado trilema de escalabilidad (Buterin (2021)). Por su naturaleza, las cadenas de bloques sin permiso solo pueden lograr dos de las tres propiedades: seguridad, descentralización y escalabilidad. La seguridad, en el sentido de informes veraces y evitando la manipulación del historial de transacciones, se mejora a través de incentivos y descentralización. Pero mantener los incentivos implica congestión, lo que limita la escalabilidad. Es esta incompatibilidad entre tres atributos clave lo que perjudica la capacidad de las cadenas de bloques para servir como un sistema de pago eficiente y la capacidad de la criptografía para servir como dinero.

La escalabilidad limitada ha resultado en la fragmentación del universo criptográfico, ya que las cadenas de bloques más nuevas con más capacidad que posiblemente cortan esquinas en la seguridad entraron en la refriega. Estas nuevas cadenas de bloques a menudo apuntan a límites de transacción más altos, incluso si estos se producen a costa de una mayor centralización y una seguridad más débil. En pocas palabras, en blockchains que dependen de una red más grande de validadores y donde cada validador tiene una influencia limitada sobre el consenso, es más difícil para un validador manipular el libro mayor. Pero esto también significa que cada transacción tarda más en ser validada, lo que implica mayores costos para los usuarios y, por lo tanto, mayores recompensas requeridas. Por lo tanto, tales cadenas de bloques se congestionan más rápidamente. En blockchains con menos validadores, por otro lado, hay más potencial para que un grupo más pequeño de validadores manipule la red.

La cadena de bloques Terra fue solo el ejemplo más evidente de un gran número de nuevos participantes (Gráfico 3.B). Tan recientemente como a principios de 2021, Ethereum representó casi todo el valor total bloqueado en los protocolos DeFi. Para mayo de 2022, esta proporción se había reducido al 50%. La cuña cada vez mayor (área roja) representada por la fallida cadena de bloques Terra es particularmente sorprendente, ya que el colapso de la cadena de bloques Terra destaca la tendencia a la fragmentación a través de la vulnerabilidad de la criptografía a los nuevos participantes que priorizan la cuota de mercado y la capacidad a expensas de la descentralización y la seguridad.

Un sistema de blockchains competidoras que no son interoperables introduce nuevos riesgos de hackeos y robos. En este contexto, la interoperabilidad se refiere a la capacidad de los protocolos y validadores para acceder y compartir información, así como validar transacciones, a través de diferentes blockchains.8 La interoperabilidad de las capas de liquidación subyacentes no se puede lograr en la práctica, ya que cada cadena de bloques es un registro separado de liquidaciones. Sin embargo, los llamados puentes de cadena cruzada han surgido para permitir a los usuarios transferir monedas a través de blockchains. Sin embargo, la mayoría de los puentes dependen solo de un pequeño número de validadores, en los que, en ausencia de regulación y responsabilidad legal, los usuarios deben confiar en no participar en comportamientos ilícitos. A medida que el número de puentes ha aumentado, se han mantenido en el centro de varios hackeos de alto perfil, destacando las vulnerabilidades a las violaciones de seguridad derivadas de la debilidad en la gobernanza de blockchain. Tales hackeos podrían reducir aún más la confianza en el sector fintech más amplio, interponiéndose en el camino de una mayor adopción (Chen et al (2023), Doerr et al (2023)).

La fragmentación del universo criptográfico contrasta con los efectos de red que echan raíces en las redes tradicionales. La dependencia de Crypto en validadores descentralizados y la fragmentación concomitante no deja ningún papel para el dinero como dispositivo de coordinación, lo que hace que la criptografía sea inadecuada como sistema monetario. Las redes tradicionales, por el contrario, se caracterizan por la propiedad de "el ganador se lo lleva todo", por la cual más usuarios que acuden a una plataforma en particular engendran aún más usuarios. Tales efectos de red están en el corazón del círculo virtuoso de menores costos y mayor confianza en las plataformas tradicionales.

3.1.2 Las monedas estables y la búsqueda de un ancla nominal

Las monedas estables respaldadas por Fiat, la forma dominante de moneda estable, aprovechan la credibilidad de la unidad de cuenta del banco central. Tener una unidad de cuenta significa que todos la utilizan como una medida común del valor económico de los productos y servicios, facilitando enormemente las transacciones financieras y económicas. En el mundo real, proporcionar la unidad de cuenta para la economía es el papel principal del banco central. Si bien no existe un banco central en el universo criptográfico, necesita tener una unidad de cuenta, como cualquier sistema monetario. Las monedas estables intentan cumplir esta función de unidad de cuenta, pero lo hacen vinculando su valor a monedas fiduciarias, como el dólar, cuyo valor está garantizado por un banco central. En este sentido, las stablecoins son la manifestación de la búsqueda existencial de la criptografía de un ancla nominal.

Sin embargo, las monedas estables sufren de una serie de deficiencias que amenazan su reclamo de estabilidad. Por un lado, están sujetos a un conflicto de intereses inherente por el cual se incentiva a los emisores a invertir en activos de riesgo. Por lo tanto, la solidez de los mecanismos de estabilización de las monedas estables depende fundamentalmente de la calidad y la transparencia de sus activos de reserva, de los que a menudo carecen. Además, no se benefician ni de los requisitos reglamentarios ni de las protecciones de los depósitos bancarios y el dinero electrónico, ni de la credibilidad del banco central que defiende la paridad. Además, como las monedas estables son pasivos transferibles y las transacciones no se liquidan en el balance del banco central, su tipo de cambio puede fluctuar lejos del par.

|  |
| --- |
| Recuadro A  El colapso de la stablecoin TerraUSD  El uso de TerraUSD (UST) creció rápidamente durante 2021-22, de modo que, antes de su colapso a mediados de 2022, era la tercera moneda estable más grande, con una capitalización de mercado máxima de casi $ 19 mil millones. Una moneda estable algorítmica, UST tenía como objetivo mantener una vinculación uno por uno con el dólar estadounidense al ser convertible en el valor de un dólar de otra criptomoneda, Luna, en la cadena de bloques Terra, y viceversa. Por ejemplo, si Terra cae a 99 centavos, un usuario podría comprar UST en un intercambio por 99 centavos y luego cambiar su UST por $ 1 en nuevas unidades de Luna en la plataforma Terra. Un aspecto crucial de este acuerdo era que los usuarios estarían dispuestos a intercambiar UST por Luna solo si la capitalización de mercado de Luna excedía la de UST. Como Luna no tenía valor intrínseco, su valoración se debió principalmente a la afluencia de usuarios especulativos al ecosistema Terra. Para atraer nuevos usuarios, el protocolo de préstamo asociado Anchor ofreció una tasa de depósito de alrededor del 20% en UST. Mientras los usuarios tuvieran confianza en el valor estable de UST y la capitalización de mercado sostenida de Luna, el sistema podría mantenerse.  Sin embargo, una vez que los inversores perdieron la confianza en la sostenibilidad del sistema, el acuerdo se desmoronó. En mayo de 2022, el valor de UST se desplomó a casi cero (Gráfico A1. R). A medida que UST cayó por debajo de su paridad, una dinámica de ejecución clásica se afianzó a medida que los inversores buscaban canjear sus fondos. Los usuarios quemaron su UST a gran escala para acuñar el valor de un dólar de Luna nueva, con la esperanza de vender Luna mientras todavía tenía algún valor. Sin embargo, dado el tamaño y la velocidad del shock, la confianza se evaporó, lo que significa que no había suficientes partes dispuestas a comprar todas las monedas Luna recién acuñadas, por lo que el precio de Luna colapsó.    La implosión UST / Luna se extendió a la moneda estable más grande, Tether, que cayó a un valor de $ 0.95 antes de recuperarse. Vio salidas de más de $ 10 mil millones en las semanas posteriores (Gráfico A1. B). La desvinculación se ha relacionado con la falta de voluntad de Tether para proporcionar detalles sobre su cartera de reservas: a los inversores les preocupaba si Tether tenía suficientes activos de alta calidad que pudieran liquidarse para respaldar la paridad. Este argumento está respaldado por las entradas experimentadas por la stablecoin regulada USDC (con reservas mejor documentadas), con fondos probablemente provenientes de Tether (Gráfico A1. C) |

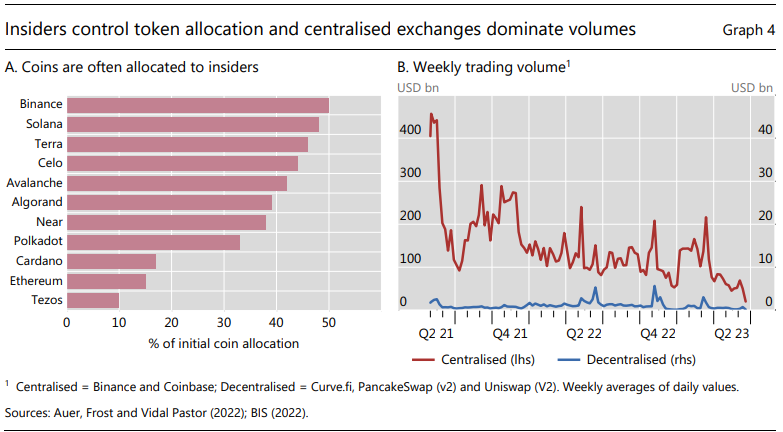
Un ejemplo de ello ha sido la implosión mencionada anteriormente de TerraUSD, que en mayo de 2022 perdió casi todo su valor en el transcurso de unos pocos días (Recuadro A). Como consecuencia, varias monedas estables respaldadas por fiat vieron reembolsos a gran escala, perdiendo temporalmente su paridad. Los reembolsos fueron más pronunciados entre las monedas estables cuyos emisores no revelaron la composición de los activos de reserva en detalle, presumiblemente reflejando las preocupaciones de los inversores de que dichos emisores podrían no ser capaces de garantizar la conversión a la par. De hecho, las monedas estables han demostrado no ser tan estables.

3.1.3 Falsas reivindicaciones de descentralización y sus consecuencias

Los defensores de las criptomonedas argumentan que la descentralización garantiza la seguridad del sistema. Sin embargo, a menudo hay una concentración de facto del poder de toma de decisiones. Si bien la centralización no es un defecto estructural per se, introduce nuevos riesgos e invalida los argumentos presentados por los defensores de la criptografía y DeFi que enfatizan su naturaleza supuestamente descentralizada.

La concentración se debe en parte a los efectos de congestión en plataformas descentralizadas con sistemas de prueba de trabajo. Para reducir la congestión, las nuevas cadenas de bloques de prueba de participación requieren que los validadores publiquen sus monedas como garantía, lo que les da una mejor oportunidad de recibir un pago por validar el siguiente bloque. Sin embargo, esto puede llevar a una concentración de poder y monedas entre un pequeño número de validadores, ya que los costos operativos son en su mayoría fijos (Auer, Frost y Vidal Pastor (2022)).

La "incompletitud del contrato", es decir, la incapacidad de redactar contratos que puedan cubrir todas las posibles eventualidades futuras, es otra razón para la centralización. Se reconoce que la centralización puede permitir a los agentes económicos superar la incompletitud de los contratos. Esto tiene un análogo en el espacio DeFi en el concepto de "incompletitud del algoritmo", a saber, la incapacidad de escribir código que cubra todas las situaciones y resultados potenciales. En consecuencia, las plataformas DeFi deben tener cierto grado de gobernanza central para abordar estas brechas en el código y delinear las prioridades estratégicas y operativas. Este elemento de centralización suele estar representado por "tokens de gobernanza", mantenidos en gran medida por desarrolladores de plataformas y primeros inversores (es decir, iniciados) que votan sobre las propuestas (Gráfico 4.A). Con la creciente centralización de los validadores, aumenta el riesgo de ataques y hacks, sobre todo porque estos nodos centralizados a menudo no están regulados.



La necesidad inherente de DeFi de obtener información del mundo real también representa un impedimento importante para la descentralización. Mientras que DeFi, en principio, se basa en la confianza descentralizada y basada en el consenso, el informe de datos que sustenta los contratos inteligentes se basa en oráculos. Los oráculos procesan y obtienen los datos, transmitiendo finalmente esta información a la cadena de bloques. Como los oráculos requieren confianza y exhiben varios grados de centralización, esto da lugar al "problema del oráculo" (Recuadro B). En el extremo, algunos utilizan una sola fuente de datos o tienen una sola persona / entidad encargada de transmitir información a la plataforma. Esto introduce un único punto de falla y deja espacio para informes falsos, ya que quienquiera que supervise el oráculo tiene la capacidad de corromper el sistema informando mal los datos. Actualmente, no existen reglas claras sobre cómo se incentiva o examina a los proveedores de oráculos, o quién es responsable si un contrato inteligente actúa sobre información incorrecta fuera de la cadena.

Finalmente, la centralización también está presente en las actividades de comercio de criptomonedas, donde los inversores dependen principalmente de intercambios centralizados (CEX) en lugar de descentralizados. Mientras que estos últimos funcionan haciendo coincidir a las contrapartes en una transacción a través de los llamados protocolos automatizados de creadores de mercado, los CEX mantienen registros fuera de la cadena de órdenes pendientes publicadas por los comerciantes, conocidos como libros de órdenes limitadas, que son familiares de las finanzas tradicionales. Los CEX atraen más actividad comercial que los DEX debido a sus menores costos (Gráfico 4.B). A pesar de que las criptomonedas CEX imitan algunas funciones de los intercambios tradicionales, no están sujetas a la misma regulación y supervisión.

La dependencia de las CEX puede poner en peligro las inversiones de los usuarios, ya que estos intercambios han demostrado repetidamente que carecen incluso de controles básicos de gestión de riesgos y estándares de gobernanza. Los ejemplos más destacados incluyen el fracaso del intercambio de bitcoins Mt Gox en 2014, que resultó en la pérdida de más de $ 400 millones en bitcoin, y la quiebra de FTX en noviembre de 2022, que causó pérdidas a sus clientes de miles de millones de dólares, entre muchos otros.

|  |
| --- |
| Recuadro B  El problema del oráculo  Las finanzas descentralizadas (DeFi) necesitan importar datos del mundo real, lo que crea un enigma práctico: es imposible importar datos a una cadena de bloques sin involucrar a un tercero (el oráculo).  El problema del oráculo surge porque los oráculos introducen la centralización en un sistema descentralizado, anulando la dependencia del consenso como mecanismo de confianza (Gráfico B1). Los oráculos con un alto grado de centralización se basan en una única fuente de datos o tienen una sola persona/entidad responsable de transmitir información a la plataforma. Esta dependencia de una fuente introduce un único punto de error y deja espacio para la manipulación cuando la fuente de datos no es confiable.  Surgen tres riesgos principales. En primer lugar, el anonimato de los agentes en un entorno DeFi puede aumentar los incentivos para el comportamiento malicioso. En las finanzas tradicionales (TradFi), cuando se detectan manipulaciones, las identidades de los manipuladores generalmente se revelan, y esas personas son responsables de las malas prácticas de las agencias de supervisión y otros. La naturaleza abierta y transparente de DeFi puede facilitar la detección de fraude, pero la incapacidad de identificar y responsabilizar a las personas responsables hace que los sistemas DeFi sean más susceptibles a la manipulación. En segundo lugar, la falta de regulación o supervisión de los proveedores de Oracle hace que el recurso sea menos claro en DeFi. Aunque existen desafíos legales en torno a la falsificación de información en TradFi, los sistemas legales establecidos proporcionan la base para asignar sanciones, compensar a las víctimas y, en algunos casos, recuperar fondos. En tercer lugar, los términos de los contratos inteligentes y las entradas de datos a las que hacen referencia en la cadena de bloques son inmutables, lo que hace que los errores o las acciones ilegales sean más costosos que en los entornos financieros tradicionales. Una vez que los datos se validan en la cadena de bloques, no se pueden corregir, y todos los contratos inteligentes que hacen referencia a esos datos continuarán haciéndolo.  Los esfuerzos tecnológicos para descentralizar los oráculos implican agregar mecanismos de consenso a los procesos de provisión de información, por ejemplo, a través de un grupo de oráculos independientes de blockchain. Estas soluciones intentan reintroducir la confianza descentralizada a expensas de la velocidad y la eficiencia, ya que cuantas más redes se agreguen para garantizar la verdad, más retrasos se introducirán a lo largo del ciclo de vida de un contrato inteligente. |

3.2 Riesgos

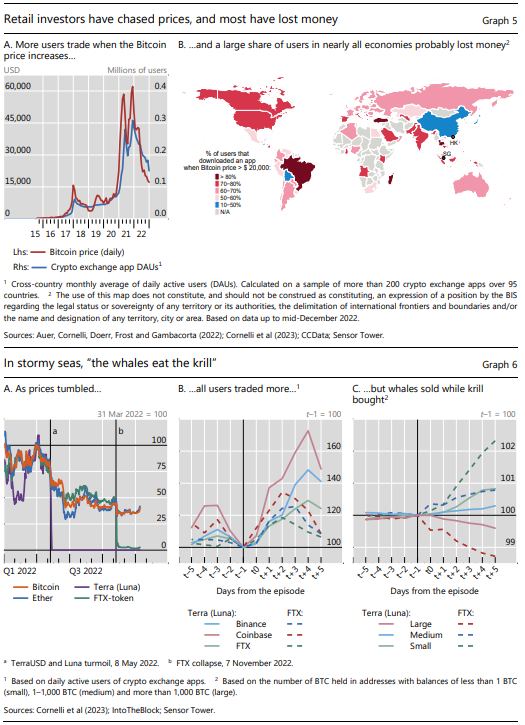
Al discutir los riesgos de la criptografía, es importante tener en cuenta que, hasta la fecha, el ecosistema es en gran medida autorreferencial. Las actividades implican casi exclusivamente el intercambio de una moneda estable o criptomoneda por otra, sin financiar ninguna actividad en la economía real. En consecuencia, la criptografía actualmente plantea riesgos significativos principalmente para los inversores en el espacio criptográfico, mientras que los enlaces al mundo real siguen siendo limitados.

3.2.1 Dentro del ecosistema criptográfico

Crypto plantea riesgos significativos para los inversores. El aumento de los precios de las criptomonedas tiende a atraer a los inversores minoristas al espacio, con la expectativa de ganancias de capital rápidas y grandes (Gráfico 5.A). Sin embargo, estas expectativas generalmente no se cumplen, ya que una gran parte de los usuarios en la mayoría de las economías tienden a perder dinero (Gráfico 5.B).

Los eventos de 2022 ilustran vívidamente los riesgos que enfrentan los inversores, especialmente los más pequeños. Las secuelas de los colapsos de TerraUSD y FTX vieron un patrón sorprendente: el número de usuarios activos diarios en las principales plataformas aumentó notablemente, lo que sugiere que los usuarios intentaron capear la tormenta cambiando sus carteras de tokens estresados a alternativas más seguras. incluidas las monedas estables respaldadas por activos (gráficos 6.A y 6.B). Sin embargo, detrás de esta ráfaga de actividad, los grandes inversores parecen haberse beneficiado a expensas de los tenedores más pequeños. De hecho, los propietarios de billeteras grandes redujeron sus tenencias de bitcoin, mientras que los propietarios medianos y especialmente los más pequeños aumentaron sus tenencias (Gráfico 6.C).

La falta de mecanismos de control en muchas empresas criptográficas implica que el dinero de los inversores está en alto riesgo si estas empresas enfrentan desafíos de financiamiento o la amenaza de bancarrota. Por ejemplo, después de su fracaso, se supo que FTX debía más de $ 3 mil millones a sus acreedores no garantizados, principalmente usuarios del intercambio que habían transferido sus fondos allí. FTX no fue el único caso en el que esto sucedió. Muchos de los clientes de otras empresas criptográficas que fracasaron en los últimos años no han podido acceder a sus fondos o han tenido que esperar mucho tiempo para hacerlo.



Crypto probablemente también se utiliza para actividades ilícitas como el lavado de dinero, el financiamiento del terrorismo y la evasión fiscal. El pseudo-anonimato y la falta de supervisión ciertamente contribuyen a estos riesgos. Por lo tanto, el uso de criptografía presenta desafíos importantes para los reguladores y las agencias de aplicación de la ley, ya que pueden tener dificultades para rastrear y rastrear las transacciones criptográficas. Para hacer frente a estos riesgos, se necesitan medidas destinadas a mejorar la gobernanza, la lucha contra el blanqueo de capitales y la financiación del terrorismo. Unos marcos de gobernanza eficaces pueden garantizar que los participantes en el mercado operen de manera transparente y responsable, promoviendo la integridad del sistema financiero. El Grupo de Acción Financiera ha desarrollado una guía sobre los requisitos de registro y licencia para los proveedores de servicios en el espacio criptográfico (GAFI (2021, 2022)).

3.2.2 Riesgos en DeFi

El ecosistema DeFi amplifica varios riesgos que también están presentes en el sistema financiero tradicional (FSB (2023)). De particular relevancia son los riesgos operacionales, su dependencia del apalancamiento y la compleja red de interconexiones dentro del sistema, que lo hacen particularmente propenso a episodios de inestabilidad.

Riesgos operacionales

Si bien todos los servicios están sujetos a riesgos operativos, una serie de características de DeFi hacen que tales riesgos sean particularmente agudos. Esto puede causar interrupciones operativas y dificultar la capacidad de ofrecer servicios y productos.

El primer tipo de riesgos operativos en DeFi son los vinculados a los marcos de gobernanza. Como estos marcos a menudo son poco claros, opacos, no probados y fáciles de manipular, pueden engañar a los usuarios sobre las afirmaciones y salvaguardas de las actividades de DeFi. Además, existe incertidumbre sobre qué protecciones correctivas ex post están disponibles para los participantes. Por ejemplo, los desarrolladores y fundadores a veces carecen de los incentivos para mantener DApps una vez que reciben la inversión inicial. Esto puede exponer a los usuarios a perder su dinero en "tirones de alfombra", un riesgo que se ve agravado por la dificultad de hacer que los desarrolladores y fundadores rindan cuentas de sus acciones, ya que sus incentivos económicos están expresados de manera poco clara y mal divulgados y el sistema presenta una estructura pseudo-anónima.

La necesidad de centralización plantea más problemas. El poder de voto en las principales organizaciones autónomas descentralizadas (DAO), que son responsables de la gestión de muchas DApps, está muy concentrado, lo que implica que, en la práctica, solo unos pocos actores de control pueden proponer, aprobar o implementar iniciativas (Feichtinger et al (2023)). Pueden ocurrir desacuerdos sobre las decisiones de gobernanza, lo que lleva a bifurcaciones y divisiones de red. Esto puede materializarse en pérdidas para los inversores y una pérdida de confianza en los protocolos DeFi, que podría extenderse a otros mercados.

El segundo tipo de riesgo operacional en DeFi está vinculado a su dependencia del buen funcionamiento de las cadenas de bloques subyacentes. Las interrupciones en la cadena de bloques causadas por interrupciones, congestión de la red o fallas de consenso pueden afectar el costo, el funcionamiento y el rendimiento de la cadena de bloques y los servicios DeFi que dependen de ella.

Una tercera fuente de riesgo operacional es el uso de contratos inteligentes. Los contratos inteligentes deben tener en cuenta muchos estados posibles del mundo antes de que se implementen, creando complejidad. A su vez, tal complejidad aumenta el potencial de errores de codificación y el consiguiente comportamiento inesperado. La inmutabilidad implica que no es posible corregir errores y restablecer el statu quo ante sin el consenso de los validadores de blockchain.

En cuarto lugar, los oráculos y puentes pueden ser una fuente adicional de riesgo operacional en DeFi. El funcionamiento de muchos protocolos DeFi depende críticamente de los oráculos. Los errores, la manipulación o los ataques a los oráculos pueden desencadenar acciones en un protocolo (por ejemplo, liquidaciones o llamadas de margen) con consecuencias negativas imprevistas en otros protocolos (por ejemplo, en activos de reserva algorítmicos o gestión de garantías). Por lo tanto, los oráculos podrían ser críticos para iniciar o propagar un choque.

Un riesgo similar está relacionado con los puentes de cadena cruzada. Las cadenas de bloques separadas no son interoperables, lo que requiere puentes que conecten protocolos a través de varias cadenas de bloques. Normalmente, un puente retendrá (recopilará) activos de una cadena o protocolo y emitirá o liberará activos en otra cadena o protocolo por el mismo valor. Esto permite a los titulares de activos realizar transacciones a través de cadenas o protocolos, pero crea repositorios que potencialmente contienen grandes cantidades de activos, convirtiéndolos en objetivos de robo y apropiación indebida.

Colateral y apalancamiento

Debido al pseudo-anonimato, la intermediación financiera en DeFi se basa en gran medida en la reutilización de garantías. La razón es que la identidad de los prestatarios y prestamistas está oculta detrás de firmas digitales criptográficas. Por lo tanto, los prestamistas no pueden acceder a información como los puntajes de crédito de los prestatarios, pero requieren garantías criptográficas para alinear los incentivos.

La presencia ubicua de garantías conduce a la prociclicidad y puede desencadenar fuertes ajustes en los precios que tienen efectos en cadena en otros segmentos del mercado. En los auges, la apreciación de los precios significa que los valores de las garantías aumentan, mientras que los coeficientes de colateralización disminuyen. En las crisis, los préstamos se liquidan a medida que los precios, y por lo tanto los valores de las garantías, disminuyen drásticamente, lo que suprime la actividad crediticia. Este mecanismo se amplifica aún más cuando los criptoactivos prestados se utilizan como garantía para préstamos adicionales (similar a la rehipotecación). Las características específicas de DeFi relacionadas con la gestión del apalancamiento, en particular, la liquidación automática de garantías, son una de las principales razones por las que la dinámica de desapalancamiento en DeFi puede ser especialmente fuerte.

Las herramientas automatizadas de gestión de riesgos sirven para proteger al prestamista, pero plantean problemas de estabilidad financiera para el ecosistema DeFi debido a sus efectos en todo el sistema. En estos protocolos, los préstamos cuyo valor de garantía cae por debajo de un cierto umbral desencadenan una liquidación automática. Si estas liquidaciones se producen en condiciones de estrés, las garantías pueden liquidarse por la fuerza en un mercado con baja liquidez, lo que hace que los precios de las garantías bajen aún más, lo que lleva al contagio. En el sistema financiero tradicional, esta dinámica que se refuerza a sí misma puede aliviarse mediante la liquidación ordenada en las contrapartes centrales o mediante la intervención humana, o puede ser detenida por los interruptores automáticos del mercado. Tales mecanismos están ausentes en DeFi.

Intra-conectividad y complejidad

Las DApps están considerablemente interconectadas entre sí. Además, el ecosistema DeFi en su conjunto está estrechamente entrelazado con otras partes del ecosistema criptográfico. Gracias a las propiedades de componibilidad de DeFi, las DApps a menudo emplean múltiples contratos inteligentes e interactúan con múltiples protocolos, lo que crea fuertes interdependencias entre los contratos inteligentes. Como resultado, los problemas en un solo contrato inteligente podrían propagarse por todo el ecosistema. Como tal, la componibilidad puede amplificar el alcance y la velocidad del contagio financiero dentro de DeFi o llevar a los contratos inteligentes a interactuar de maneras inesperadas. Para agravar este problema está el hecho de que el código de contrato inteligente se reutiliza ampliamente, de modo que los contratos aparentemente independientes pueden en la práctica estar sujetos a las mismas vulnerabilidades. En resumen, los diversos componentes de DeFi están altamente interconectados, por lo que evaluar un elemento del sistema criptográfico de forma aislada no llega a evaluar su papel en el ecosistema general.

3.2.3 Interconexión con el sistema financiero tradicional

La interacción entre el mercado criptográfico, las finanzas tradicionales y la economía real ha seguido siendo limitada hasta ahora (Auer, Farag, Lewrick, Orazem y Zoss (2022)). Como la criptografía sigue siendo un vehículo en gran medida autorreferencial utilizado principalmente para la especulación, esto quizás no sea sorprendente. De hecho, los vínculos existentes resultan en gran parte de la necesidad de la criptografía de interactuar con las finanzas tradicionales para sostener su crecimiento. Sin embargo, los inversores institucionales y los hogares continúan mostrando interés en la criptografía a pesar de los eventos del año pasado. Por lo tanto, no se puede ignorar la posibilidad de que estos vínculos crezcan aún más.

Entre estos vínculos, la relación entre la criptografía y el sector bancario central es de particular importancia. La caída de los precios de las criptomonedas que comenzó en la segunda mitad de 2022 finalmente se extendió al sistema financiero tradicional. En marzo de 2023, por ejemplo, Silvergate Bank, con sede en California, ampliamente promocionado como un "criptobanco" clave, tuvo que cesar sus operaciones después de una gran cantidad de depósitos de clientes. Del mismo modo, Signature Bank, que también se especializó en servir a la industria de la criptografía, fue liquidado por las autoridades poco después. Estos casos resaltan que un modelo de negocio que está altamente expuesto a la criptografía puede ser problemático para el sector bancario.

Los bancos también podrían aumentar las conexiones a la criptografía a través de la provisión de crédito a contrapartes con exposiciones criptográficas o mediante la custodia y otros servicios relacionados con la criptografía a sus clientes. Reconociendo esos riesgos, el Comité de Supervisión Bancaria de Basilea (CSBB) aprobó recientemente una norma prudencial global para las exposiciones de los bancos a criptoactivos (BCBS (2022)). Además, los riesgos a lo largo del nexo banco-cripto se extienden más allá de las exposiciones (directas e indirectas) debido a las posibles externalidades negativas asociadas con los bancos que canalizan fondos hacia el ecosistema criptográfico, dado su papel como pilar del sistema monetario. Junto con los bancos, otras entidades financieras como oficinas familiares, fondos de cobertura y administradores de activos también podrían aumentar sus inversiones criptográficas, atraídas por los rendimientos potencialmente altos.

La tokenización de reclamos sobre activos del mundo real, como acciones o bienes raíces, es otra forma a través de la cual podrían crecer las interconexiones entre las finanzas tradicionales y la criptografía. Esto podría resultar en el crecimiento de la criptografía en sí, ya que el nuevo dinero se canaliza hacia tales activos tokenizados. También podría generar una red más compleja de interconexiones entre la criptografía y las finanzas tradicionales a medida que las actividades de las entidades en estos dos ecosistemas se entrelazan más. En este escenario, la importancia sistémica del ecosistema criptográfico podría aumentar sustancialmente.

La creciente interconexión de Crypto con las finanzas tradicionales y la economía real también puede representar una amenaza para la soberanía monetaria. La disponibilidad de monedas estables, en particular, puede facilitar la criptoización, es decir, la sustitución de monedas locales por monedas basadas en criptomonedas.16 Durante períodos de inestabilidad macroeconómica y depreciación de los tipos de cambio, los titulares de monedas fiduciarias nacionales podrían cambiar a monedas alternativas, ejerciendo una presión adicional sobre la propia moneda nacional. Tal comportamiento puede dar lugar a la pérdida de soberanía monetaria de las autoridades monetarias nacionales, así como a la exclusión de la financiación de las instituciones financieras locales, con consecuencias a largo plazo para la estabilidad monetaria y financiera general de estos países. Sin duda, el riesgo de sustitución de moneda siempre está presente y corresponde a cada jurisdicción administrarlo adecuadamente. Sin embargo, la existencia de criptomonedas y monedas estables puede aumentar sustancialmente la probabilidad de que tales escenarios se materialicen, ya que hace que la sustitución de divisas sea mucho más fácil en la práctica. Si las grandes empresas tecnológicas emiten monedas estables, aprovechando el bucle de actividades de red de datos que se refuerza a sí mismo y que les permite explotar los efectos de red cada vez mayores (Shin (2019)), la amenaza a la soberanía monetaria puede exacerbarse enormemente.

Las interconexiones entre la criptografía y el sistema financiero tradicional pueden funcionar en ambos sentidos. Por ejemplo, como consecuencia de la agitación bancaria en marzo de 2023, algunas monedas estables perdieron su paridad, especialmente USDCoin después de revelar que una cantidad sustancial de su reserva de efectivo se depositó en Silicon Valley Bank. Las monedas estables que usaron USDCoin como activo de reserva también rompieron el par, mientras que otras monedas estables se negociaron con una prima. Estos eventos demostraron que es probable que no sea posible desarrollar monedas estables verdaderamente estables, es decir, monedas estables que puedan mantener su paridad contra todas las circunstancias, incluso si invierten principal o exclusivamente en activos seguros.

3.2.4 Riesgos para las economías de mercados emergentes y en desarrollo

Varios riesgos relacionados con las criptomonedas y las monedas estables se exacerban en las economías de mercados emergentes y en desarrollo (Feyen et al (2021), UNCTAD (2023), Prasad (2023)).

En primer lugar, las monedas estables podrían plantear graves riesgos para la integridad del sistema financiero, incluso para ALD / CFT. Si bien este riesgo está presente en todos los países, las limitaciones de recursos en las economías de mercados emergentes y en desarrollo (EMED) pueden dificultar que las autoridades mantengan el ritmo y ajusten sus marcos de supervisión, regulación y supervisión.

En segundo lugar, las monedas estables vinculadas a monedas extranjeras fluctuarían en valor frente a las monedas locales en las EMED. Si se utiliza para contratos de deuda, esta sería una nueva forma de facto de préstamos en divisas (FX), que ha estado en el centro de muchas crisis financieras en las EMED.

En tercer lugar, las monedas estables podrían importar las políticas monetarias de las monedas fiduciarias en la cesta, lo que puede no ser óptimo para la mayoría de las EMED y, por lo tanto, podría afectar su autonomía monetaria (FMI (2023a)). Los países con grandes entradas transfronterizas de monedas estables pueden tener dificultades para mantener las reservas internacionales en monedas fiduciarias fuertes. Esto tiene implicaciones para el funcionamiento de los mercados de divisas e interbancarios, que son menos profundos en las EMED. Por lo tanto, las perturbaciones de liquidez y reembolso pueden crear efectos de contagio perturbadores.

En cuarto lugar, y en relación con los puntos anteriores, los riesgos de criptoización descritos en la sección anterior son particularmente agudos para las EMED. Las monedas estables pueden facilitar la sustitución de divisas y la evasión de las medidas que las EMED pueden utilizar para defender sus monedas durante períodos de elevada volatilidad cambiaria.

En quinto lugar, dado el alcance, la escala, la red y los efectos de "el ganador se lleva todo", las EMED podrían terminar como un "anfitrión" para las entidades en un sistema de monedas estables que brindan servicios críticos como la gobernanza y la gestión de activos de reserva, que pueden tener su sede en otros lugares. Esto podría crear una desalineación de los incentivos entre los supervisores "domésticos" y "anfitriones", impidiendo una supervisión holística. Como tal, las autoridades de EMED pueden carecer de control sobre el acuerdo más amplio de monedas estables y sus operaciones que involucran a los residentes. Cuando se adopta a escala nacional, esto podría inhibir el monitoreo de riesgos y la supervisión efectiva de los pagos para prevenir el uso ilícito y salvaguardar la estabilidad financiera.

3.3 Abordar los riesgos en criptografía

Los numerosos riesgos planteados por las criptomonedas han generado naturalmente un debate sobre las estrategias políticas óptimas para mitigarlos. Un boletín del BIS (Aquilina et al (2023)) describió tres líneas de acción no mutuamente excluyentes que podrían seguirse en la política hacia la criptografía, a saber, una combinación de contención, regulación y prohibiciones. El Boletín contiene detalles de los tres enfoques, junto con ejemplos específicos.

Varias jurisdicciones ya están tomando varias medidas de política a lo largo del espectro anterior. Más concretamente, esto incluye prohibiciones, restricciones, aclaraciones, requisitos a medida e iniciativas para facilitar la innovación. La mayoría de las iniciativas adoptadas hasta ahora tienden a dirigirse a actividades gestionadas centralmente (en particular, emisores de tokens de seguridad y monedas estables) y son una función de la evolución del mercado en cada jurisdicción.

Las iniciativas multilaterales en esta área, coordinadas por el Consejo de Estabilidad Financiera (CEF), ya están tomando medidas para llegar a un consenso sobre las acciones regulatorias apropiadas. El FSB ya ha publicado un marco propuesto para la regulación internacional de las actividades de criptoactivos (FSB (2022)). Este marco contiene dos componentes principales. En primer lugar, formula recomendaciones que promueven la coherencia y la exhaustividad de los enfoques regulatorios, de supervisión y de supervisión de las actividades y los mercados de criptoactivos, y fortalecen la cooperación internacional, la coordinación y el intercambio de información. En segundo lugar, establece recomendaciones revisadas de alto nivel para la regulación, supervisión y supervisión de los acuerdos de "moneda estable global" para abordar los riesgos asociados para la estabilidad financiera de manera más efectiva. El FMI también ha publicado su opinión sobre los elementos centrales de un marco de política eficaz para abordar los riesgos planteados por los criptoactivos (FMI (2023b)).

En términos más generales, las autoridades públicas también podrían complementar las líneas de acción anteriores fomentando una innovación sólida dentro del sistema financiero tradicional o mediante el uso de monedas digitales del banco central (Aquilina et al (2023)). Mejorar la calidad y reducir los costos de los pagos sería un componente importante de esa estrategia. Esto podría lograrse mediante la introducción de sistemas de pago rápido minoristas, como la Interfaz de Pago Unificada (UPI) en India, Pix en Brasil, FedNow en los Estados Unidos o iniciativas como la Zona Única de Pagos en euros (SEPA). Otro componente importante de esta estrategia más amplia sería emitir monedas digitales del banco central que satisfagan las necesidades reales. Si se diseñan y aplican adecuadamente, esas iniciativas podrían apoyar una innovación sólida del sector privado, al tiempo que reducen el costo de los pagos, mejoran la inclusión financiera y refuerzan la integridad del sistema financiero.

3.4 Abordar las lagunas de datos: Proyecto Atlas

Los datos sobre las actividades criptográficas provienen de dos fuentes: datos en cadena de blockchains y datos fuera de la cadena informados por los actores del mercado. Los datos se distribuyen a través de una vasta red de libros de contabilidad distribuidos, intercambios y otros proveedores. Por lo tanto, las cifras sobre indicadores básicos como el tamaño del mercado y el uso de criptografía carecen de transparencia, consistencia y confiabilidad (JERS (2023)).

Las brechas de datos obstaculizan los esfuerzos para desarrollar un marco de monitoreo coherente para la criptografía en general.18 Estos problemas se derivan en gran parte de (i) la dificultad de agregar, conciliar y analizar los datos disponibles en los libros de contabilidad distribuidos; (ii) el pseudo-anonimato que inhibe la capacidad de determinar los tipos de inversores en criptoactivos que pueden ser los beneficiarios de múltiples billeteras; y iii) el gran número de transacciones fuera de la cadena. Estas lagunas de datos impiden una evaluación adecuada de los riesgos potenciales.

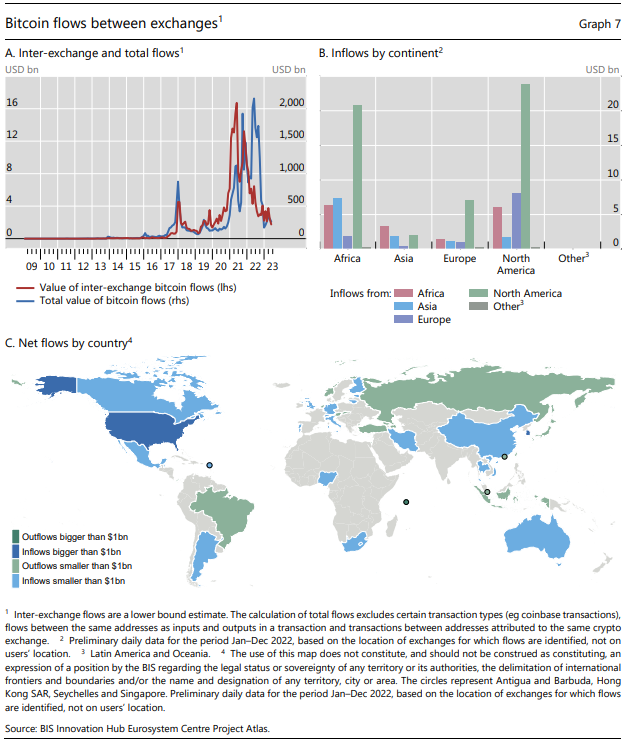
En respuesta a estos desafíos de datos, el Centro del Eurosistema del Centro de Innovación del BIS, el Deutsche Bundesbank y el De Nederlandsche Bank han iniciado el Proyecto Atlas, que arrojará luz sobre la relevancia macroeconómica de los mercados de criptoactivos y DeFi. Los datos se basarán en una metodología transparente y adaptada a las necesidades de las autoridades públicas. Combinará los datos reportados recopilados de los intercambios criptográficos y los emisores de monedas estables con datos de blockchains públicas. Al atribuir las transacciones de blockchain a los intercambios criptográficos y sus ubicaciones geográficas, Atlas podrá derivar y visualizar flujos transfronterizos en todo el mundo.

Los datos preliminares del Proyecto Atlas revelan que, aunque relativamente pequeño en comparación con el tráfico total de la red, los flujos entre los intercambios criptográficos centralizados son sustanciales (Gráfico 7.A). La atribución de ubicaciones geográficas a los intercambios (cuando sea posible) establece la estructura de los flujos transfronterizos y proporciona un punto de partida para evaluar la importancia económica relativa entre jurisdicciones (gráficos 7.A y 7.B). Esto indica un uso no despreciable, y creciente, de las criptomonedas para los flujos de capital transfronterizos.

Sin embargo, se necesitan más pasos para una evaluación holística de los criptomercados. La cooperación en la recopilación de datos y el seguimiento por parte de las distintas jurisdicciones puede facilitar la elaboración de respuestas normativas adecuadas. Esa cooperación también podría ayudar a adoptar medidas coercitivas en relación con las actividades ilícitas. Actualmente, la falta de estándares implica que los datos sobre criptografía generalmente se limitan a lo que las empresas informan voluntariamente o dependen de empresas cuyo modelo de negocio es vender datos a los participantes del mercado. Para los datos en cadena, la elección de las metodologías influye en gran medida en los números informados, mientras que la heurística y las metodologías exactas a menudo no están claras. En consecuencia, los datos a menudo son reportados de manera diferente por varias compañías de análisis y son difíciles de comparar a través del tiempo y el espacio.

Con respecto a DeFi, el FSB (2023) destaca tres tipos de indicadores que las autoridades deberían monitorear para evaluar vulnerabilidades y riesgos. En primer lugar, indicadores que pueden ayudar a medir el tamaño general y la evolución del sector. En segundo lugar, indicadores especialmente diseñados para evaluar las vulnerabilidades financieras. Y tercero, indicadores que pueden ayudar a medir el potencial de efectos de contagio mediante el seguimiento y la evaluación de las interconexiones entre DeFi, CeFi, las finanzas tradicionales y la economía real.

Desarrollar una imagen precisa de criptografía y DeFi requerirá una cantidad considerable de trabajo para estandarizar definiciones, procesos y enfoques. El trabajo sobre estos temas ya está en curso en la Iniciativa de Brechas de Datos, como acogieron con beneplácito los líderes del G20 en noviembre de 2022.



4. Conclusiones

En poco más de una década, la criptografía ha pasado de ser una actividad de nicho a algo que afecta al sistema financiero convencional. Si bien inicialmente era dominio exclusivo de un pequeño grupo de entusiastas, millones de usuarios minoristas, así como más y más inversores institucionales han ingresado al ecosistema criptográfico en los últimos años.

Crypto ofrece algunos elementos de innovación genuina, como la programabilidad y la componibilidad. Con estas nuevas funcionalidades, las secuencias de transacciones financieras podrían automatizarse e integrarse sin problemas. Junto con la tokenización, esto tiene el potencial de reducir la necesidad de intervenciones manuales que actualmente retrasan las transacciones y crean costos (Carstens (2023), Aldasoro et al (2023)).

Dicho esto, la criptografía hasta ahora no ha aprovechado la innovación en beneficio de la sociedad. Crypto sigue siendo en gran medida autorreferencial y no financia la actividad económica real. Adolece de deficiencias inherentes relacionadas con la estabilidad y la eficiencia, así como con la rendición de cuentas y la integridad. Estos defectos estructurales son el resultado de la economía subyacente de los incentivos en lugar de las limitaciones tecnológicas. Además, si bien DeFi y crypto en su mayor parte replican los servicios ofrecidos por el sistema financiero tradicional, pueden exacerbar las vulnerabilidades conocidas. En conjunto, las conclusiones clave de este informe sugieren que los defectos estructurales inherentes de la criptografía la hacen inadecuada para desempeñar un papel importante en el sistema monetario.

Glosario

Este glosario establece una lista (no exhaustiva) de términos utilizados en el informe. Las definiciones se basan principalmente en informes anteriores de organizaciones internacionales y organismos normativos.

TOKEN RESPALDADO POR ACTIVOS: un criptoactivo que representa un interés en un activo físico.

BLOCKCHAIN: Una forma de libro mayor distribuido en el que los detalles de las transacciones se mantienen en el libro mayor en forma de bloques de información. Un bloque de nueva información se adjunta a la cadena de bloques preexistentes a través de un proceso informatizado mediante el cual se validan las transacciones.

PUENTE: Una técnica utilizada para transferir criptoactivos entre ecosistemas, por lo general, creando una representación sintética de un criptoactivo específico de blockchain en una cadena de bloques diferente.

INTERCAMBIO CENTRALIZADO (CEX): Una plataforma de negociación de criptoactivos que facilita la compra y venta de criptoactivos, ya sea para monedas fiduciarias o para otro activo digital. La plataforma funciona como intermediario y, a veces, proporciona custodia y otros servicios.

FINANZAS CENTRALIZADAS (CEFI): intermediarios centralizados (por ejemplo, plataformas de préstamos o negociación) dentro del ecosistema criptográfico que pretenden ofrecer algunas de las características de DeFi con cierta facilidad de uso y seguridad de los productos de servicios financieros tradicionales.

COMPOSABILIDAD: la capacidad de reutilizar componentes de software existentes para construir nuevas aplicaciones. La industria de la criptografía se refiere a la componibilidad como similar a los bloques de Lego. Cada bloque se puede combinar con otro, lo que permite a los desarrolladores construir estructuras complejas combinando diferentes bloques.

MECANISMO DE CONSENSO: En aplicaciones DLT, el proceso por el cual los validadores acuerdan el estado de un libro mayor distribuido.

CRIPTOACTIVO: Un tipo de activo digital del sector privado que se expresa principalmente a través de la criptografía y el libro mayor distribuido o tecnología similar.

CRIPTOIZACIÓN: El riesgo de sustitución de moneda local con criptoactivos, muy probablemente monedas estables denominadas en dólares. Este es un riesgo particular para los países con monedas inestables y marcos monetarios débiles.

ORGANIZACIÓN AUTÓNOMA DESCENTRALIZADA (DAO): En teoría, una aplicación descentralizada que consiste en reglas de operación que dictan quién puede ejecutar un determinado comportamiento o realizar una actualización. El código ayuda a crear una estructura organizativa destinada a funcionar sin una estructura de gestión centralizada.

APLICACIONES DESCENTRALIZADAS (DAPPS): aplicaciones DeFi que ofrecen servicios como préstamos o comercio, predominantemente entre criptoactivos, incluidas las monedas estables.

INTERCAMBIO DESCENTRALIZADO (DEX): Mercados construidos utilizando un libro mayor distribuido o tecnología similar donde las transacciones pueden ocurrir directamente entre los comerciantes de criptoactivos.

FINANZAS DESCENTRALIZADAS (DEFI): Un conjunto de mercados financieros alternativos, productos y sistemas que operan utilizando criptoactivos y contratos inteligentes (software) construidos utilizando contabilidad distribuida o tecnología similar.

PROTOCOLO DEFI: Un sistema especializado de reglas que crea un programa diseñado para realizar funciones financieras tradicionales.

ACTIVO DIGITAL: Un instrumento digital que se emite o representa mediante el uso de un libro mayor distribuido o tecnología similar. Esto no incluye representaciones digitales de monedas fiduciarias. También se llama moneda o ficha.

TECNOLOGÍA DE CONTABILIDAD DISTRIBUIDA (DLT): Un medio para guardar información a través de un libro mayor distribuido, es decir, una copia digital repetida de los datos disponibles en múltiples ubicaciones.

TARIFAS DE GAS: Unidad que se relaciona con la cantidad de esfuerzo computacional requerido para ejecutar operaciones específicas en la red Ethereum. Gas se refiere a la tarifa requerida para realizar una transacción en Ethereum.

TOKENS DE GOBERNANZA: tokens emitidos como incentivo, lo que permite al usuario la supuesta oportunidad de convertirse en propietario parcial y tomador de decisiones en un protocolo DeFi.

MINERÍA: Uno significa crear nuevos criptoactivos, a menudo a través de un proceso matemático mediante el cual las transacciones se verifican y se agregan al libro mayor distribuido.

TOKEN NATIVO: El token base de una cadena de bloques que desempeña un papel integral en el funcionamiento del protocolo en el que se emite y que se crea en la génesis de la cadena de bloques. Por lo general, se utiliza para pagar tarifas de transacción.

ORACLE: Un servicio que permite a los contratos inteligentes acceder, en tiempo real, a datos externos o fuera de la cadena relevantes por medio de consultas generalmente a través de interfaces de programación de aplicaciones de intercambio criptográfico y que proporciona entradas para contratos inteligentes.

INTERCAMBIO DE LIBROS DE PEDIDOS: un tipo de intercambio descentralizado (DEX) que utiliza contratos inteligentes para la liquidación de transacciones y libros de pedidos, que generalmente se mantienen fuera de la cadena por un tercero, para el registro de órdenes de compra y venta.

PRUEBA DE PARTICIPACIÓN: Un mecanismo de consenso específico de blockchain para validar las entradas en una base de datos distribuida y mantener la base de datos segura en función de la promesa o "apuesta" de los validadores de una cierta cantidad de criptoactivos para tener la oportunidad de ser elegido para la creación de un nuevo bloque.

PRUEBA DE TRABAJO: Un mecanismo de consenso específico de blockchain para validar entradas en una base de datos distribuida y mantener la base de datos segura donde los validadores potenciales compiten entre sí para resolver acertijos criptográficos para poder agregar transacciones al libro mayor distribuido.

DATOS SEUDÓNIMOS: Datos que no pueden atribuirse a un individuo específico, sin el uso de información adicional.

RUG PULL: Una estafa del mercado de criptoactivos en la que un equipo de desarrollo atrae a los inversores a un proyecto antes de desaparecer con los fondos de los inversores, dejando a los inversores con un activo sin valor.

CADENA LATERAL: Un tipo de solución de escalado fuera de la cadena que ayuda a superar las restricciones de capacidad inherentes a las redes de blockchain tradicionales al aprovechar una red de blockchain separada e independiente que está conectada a la original por un puente bidireccional.

CONTRATO INTELIGENTE: un término de criptoactivo que se refiere a aplicaciones autoejecutables que pueden desencadenar una acción si se cumplen algunas condiciones preespecificadas.

STABLECOIN: Un criptoactivo que tiene como objetivo mantener un valor estable en relación con un activo específico, o un grupo o canasta de activos.

STAKING: Es el proceso de bloquear criptoactivos durante un período de tiempo determinado para ayudar a respaldar la operación de una cadena de bloques a cambio de una parte de las tarifas de transacción.

TOKENIZACIÓN: El proceso de crear una representación digital (token) de un activo y ponerlo en un libro mayor programable. La información almacenada en forma tokenizada puede incluir el tipo de activo, los detalles de propiedad, la valoración, el marco legal, la opcionalidad y los requisitos de liquidación.

VALOR TOTAL BLOQUEADO: medida informada por la industria del valor total de los activos depositados en un protocolo DeFi.

VALIDADOR: Un individuo o entidad responsable de verificar las transacciones en una cadena de bloques.

MONEDERO: Una aplicación o dispositivo para almacenar las claves privadas que proporcionan acceso al criptoactivo. Las carteras alojadas suelen estar en manos de un proveedor externo, las carteras no alojadas por el usuario.

PROVEEDOR DE BILLETERA: Una empresa que ofrece servicios de almacenamiento a inversores en criptoactivos. Estos pueden estar conectados en línea (almacenamiento "caliente") o mantenerse fuera de línea (almacenamiento "frío").