CRIPTOACTIVOS: CONCEPTOS BÁSICOS, POSIBLES BENEFICIOS Y RIESGOS POTENCIALES*

Cristóbal Domínguez Flores

Resumen. Los avances tecnológicos de los últimos años han acelerado la adopción de los medios digitales en todo el mundo. Particularmente, los avances en informática y la fácil disponibilidad de equipos y dispositivos electrónicos han permitido el desarrollo de nuevos productos y servicios de forma descentralizada. Los criptoactivos son un ejemplo claro del impacto que pueden tener estos avances, al permitir que cualquier persona con conocimientos en programación e informática sea capaz de desarrollar productos y servicios que asemejan a los ofrecidos por el sistema financiero tradicional. El objetivo principal de este documento es ofrecer una introducción a los conceptos elementales de operación de los criptoactivos, particularmente de aquellos que fueron diseñados con la intención de operar de forma análoga al dinero. Este se centra en dos tipos principales: los no estables o sin subyacente (por ejemplo, *bitcoin*, *ether*) y los llamados estables (*stablecoins*). Adicionalmente se describen algunos de los principales beneficios y riesgos identificados en la literatura reciente. Aunque se argumenta que su uso y adopción más generalizada podría traer algunos beneficios en materia de inclusión financiera y eficiencia, también conlleva riesgos potenciales en materia de ciberseguridad, protección de la población usuaria e inversionista, prevención de lavado de dinero, e incluso en estabilidad financiera que requerirían atención de las autoridades. El documento concluye con un breve acercamiento a la discusión actual sobre mejores prácticas internacionales en materia de regulación de estos activos.

Palabras clave: Criptoactivos, criptomonedas, *stablecoins*, activos virtuales, DeFi, *Bitcoin*.

JEL: E42, E44, F55, G23, O31, O33, Y2.

**/ Esta investigación corresponde a un documento de trabajo solo con fines informativos. Las opiniones vertidas en el corresponden únicamente al autor y no necesariamente reflejan la postura institucional de la CNBV. No constituye una recomendación de inversión.*

CRYPTOASSETS: BASIC CONCEPTS, POSSIBLE BENEFITS AND POTENTIAL RISKS*

Cristóbal Domínguez Flores

Abstract. Technological advances in the last years have sped up the adoption of digital means worldwide. Recent advances in computing and the availability of electronic devices have allowed the development of new products and services in a decentralized way. Cryptoassets are a clear example of the impact of these improvements by letting any person with programming skills to develop products and services similar to the ones offered by traditional financial intermediaries. The main objective of this paper is to offer a primer on the basic concepts of cryptoassets operation, particularly on those designed to work in a similar way as money. The document focuses on two main types: nonstable cryptoassets (e.g. bitcoin, ether, XRP) and the so-called stablecoins. In addition, some of the main potential benefits and risks identified in recent literature are described. Although it is argued that the widespread adoption and use of these assets could bring benefits in financial inclusion and efficiency, it could also bring potential risks related to cybersecurity, protection of users and investors, anti-money laundering and financial stability that would need attention from financial authorities. This paper concludes with a brief introduction to the current discussion on best international practices on regulation of cryptoasssets.

Keywords: Cryptoassets, cryptocurrencies, stablecoins, virtual assets, DeFi, Bitcoin.

JEL: E42, E44, F55, G23, O31, O33, Y2.

**/ This document represents a working paper. The opinions expressed in it are responsibility to the author and do not necessarily reflect the institutional position of the CNBV. This document does not represent an investment advice.*

CRIPTOACTIVOS: CONCEPTOS BÁSICOS, POSIBLES BENEFICIOS Y RIESGOS POTENCIALES*

Cristóbal Domínguez Flores°

I. Introducción

Las últimas décadas se han visto enmarcadas en un acelerado avance tecnológico, que ha llevado a una adopción veloz de medios digitales alrededor del mundo. El sistema financiero no ha estado exento de esta transformación. Los servicios financieros se han digitalizado rápidamente aprovechando el acceso más generalizado al internet y la mayor adquisición de teléfonos inteligentes y computadoras entre la población.

La innovación no ha sido exclusiva de las grandes corporaciones y las autoridades. El acceso inmediato a herramientas e información, además de la facilidad y alcance de las comunicaciones a través de redes sociales han contribuido al desarrollo de sistemas descentralizados y conglomerados de individuos capaces de utilizar las ventajas de las nuevas tecnologías para diseñar productos y servicios que han llegado a ser considerados, por algunas personas, como alternativas reales a los tradicionales. El sistema financiero actual, que se destaca por la fusión de tecnologías que han borrado las líneas entre las esferas físicas y digitales,[1] está experimentando cambios importantes que en muchos casos parecen querer superar las líneas definidas por los

**/ Esta investigación corresponde a un documento de trabajo solo con fines informativos. Las opiniones vertidas en el corresponden únicamente al autor y no necesariamente reflejan la postura institucional de la CNBV. No constituye una recomendación de inversión.*

°Agradezco los valiosos comentarios y revisiones detalladas de Damián Urbina, Alejandro Rodríguez y Eduardo Bello durante la elaboración de este documento. Asimismo, agradezco a todas las personas integrantes de la Dirección General de Estudios Económicos y de la Vicepresidencia de Política Regulatoria de la CNBV que participaron en las presentaciones internas. Particularmente, agradezco a Daniel Miranda cuyo diálogo constante conmigo respecto a este tema fue esencial para definir el contenido y rumbo de este documento. Sus comentarios detallados a varias versiones de este evitaron muchos errores y mejoraron la claridad de la exposición. José Daniel Gutiérrez, Sofía Huidobro, Daniela Moreno, Katia Negrete y Alejandra Pacheco ofrecieron su apoyo en la revisión de la redacción y versión final de este documento, lo que agradezco enormemente. Las traducciones incluidas fueron realizadas por mí y, por ende, son interpretaciones propias de los textos citados. Por supuesto, cualquier error, omisión u opinión es mi completa responsabilidad y no necesariamente reflejan la de alguno de los comentaristas, de los revisores o de la CNBV.

[1] Esta fusión de tecnologías es comúnmente característica de lo que se ha llamado la cuarta revolución industrial (Schwab, 2016).

marcos de supervisión y regulación establecidos después de muchas décadas de esfuerzos y actualizaciones.

Tal vez uno de los ejemplos más característicos de esta situación la representan los denominados criptoactivos. Aunque no existe una definición globalmente aceptada, un criptoactivo puede entenderse como un activo digital cuyo funcionamiento depende de un protocolo soportado por herramientas criptográficas[2] y tecnologías de registro que permiten la validación de sus operaciones, el acceso a sus registros históricos y la actualización de éstos de forma descentralizada y generalmente abierta. Aunque existe una enorme variedad de activos virtuales que podrían cumplir con esta definición, este trabajo se concentra en los que comúnmente se conocen como "criptomonedas". En términos muy simplificados, estos activos pueden entenderse como productos diseñados para tratar de cumplir funciones similares al dinero, con la salvedad de que son netamente digitales y que no dependen de una autoridad central que las garantice u opere.

El primer ejemplo de una de estas "criptomonedas" completamente funcionales es el *bitcoin*, la cual fue diseñada por Satoshi Nakamoto (Nakamoto, 2008) y cuya red homónima fue lanzada de forma completamente independiente en 2010.[3] Desde su aparición, el mercado de criptoactivos ha tenido un crecimiento importante, con una enorme variedad de "criptomonedas" inspiradas en el diseño original de Nakamoto que han sido adoptadas por una parte del mercado financiero.

Ante el dinamismo del mercado, las autoridades financieras requieren comprender la forma en que este tipo de activos operan, entender cómo interactúan con el sistema financiero y la economía en su conjunto, e identificar los riesgos y beneficios potenciales que conlleva su adopción. Por ello, este trabajo busca hacer una revisión de cómo han evolucionado los principales criptoactivos, ofreciendo los conceptos y explicaciones básicas de su operación. El análisis se concentra en dos grupos de criptoactivos diseñados para operar como "criptomonedas":[4] 1) los no estables, que corresponden a aquellos que no están respaldados por alguna moneda

[2] La criptografía es la técnica para proteger comunicaciones, documentos y datos a través de la creación y utilización de códigos que aseguren que la información sólo sea descifrable para quién está dirigida.

[3] La identidad real de Satoshi Nakamoto nunca ha sido revelada públicamente, pero el consenso es que se trata de una persona o grupos de individuos especialistas en informática y criptografía ligados a foros de entusiastas en estas materias (Mehta et al. 2021). Satoshi Nakamoto desapareció completamente pocos años después del lanzamiento de la red *Bitcoin*. Los escritos atribuidos a su persona, que pueden reducirse al *white paper* de *bitcoin*, publicaciones en foros y listas públicas, además de algunos emails pueden consultarse en Champagne (2014).

[4] Debe enfatizarse que no todos los criptoactivos pueden definirse como criptomonedas. En este documento, no se consideran a detalle otro tipo de criptoactivos como los NFTs (*Non-fungible tokens*), los tokens de valores (*security tokens*) o los tokens de utilidad (*utility tokens*).

fiduciaria o activo, siendo el ejemplo más famoso el *bitcoin*, y 2) los llamados estables o *stablecoins*, que buscan mantener un valor estable en el tiempo.

Además de ofrecer una explicación sencilla de su operación, el documento también busca presentar un resumen informado de los riesgos y beneficios potenciales de su adopción. Si bien las "criptomonedas" se desarrollan en el mundo digital y operan primordialmente a través de entidades especializadas como *exchanges*, existe un interés reciente y creciente entre algunos participantes del mercado por intensificar su interacción con el sistema financiero tradicional, lo que puede materializar algunos de los riesgos asociados con su uso en áreas como la Prevención del Lavado de Dinero y Financiamiento del Terrorismo (PLD/FT), la protección de la población usuaria y la estabilidad del sistema en su conjunto.

Este documento no busca ser una guía, ni un estudio exhaustivo de los riesgos y beneficios, pero constituye una introducción amplia que aborda los criptoactivos desde los elementos más básicos de operación hasta algunas de las discusiones sobre las consecuencias de su adopción. Con este documento se busca abonar a la discusión informada sobre un sector que ha despertado interés y ganado popularidad entre una parte relevante de la población, parte de la cual puede no estar plenamente informados sobre los riesgos y beneficios que puede conllevar su adopción. El documento se desarrolló manteniendo lo más posible una línea didáctica y representa únicamente mi opinión, basada en una revisión bibliográfica. Por supuesto, el documento no representa la opinión o postura de la Comisión Nacional Bancaria y de Valores (CNBV) en esta materia.

Este texto está organizado de la siguiente forma. En la primera sección se analizan los criptoactivos no estables, iniciando con los conceptos básicos de la operación de sus redes, así como instituciones participantes como las plataformas de intercambio o *exchanges*. Basado en el entendimiento obtenido sobre su operación, se analiza algunos de los beneficios y riesgos potenciales relacionados con estos activos. Aunque los criptoactivos no estables podrían tener impactos positivos en materia de pagos e inclusión financiera de acuerdo con sus proponentes, presentan también una enorme volatilidad que dificulta su uso como medio de pago y podrían tener implicaciones en la estabilidad financiera de las instituciones en caso de una adopción generalizada. Además, su naturaleza netamente digital presenta riesgos relevantes de ciberseguridad, protección de usuarios y prevención de lavado de dinero que requieren atención.

La segunda sección analiza las llamadas *stablecoins* o criptoactivos estables. En primer lugar, se discute su funcionamiento, que presenta diferencias importantes respecto a otros activos virtuales y ha fomentado el desarrollo de las llamadas finanzas descentralizadas (DeFi). Este tipo de

activos digitales solucionan hipotéticamente el problema de volatilidad de los criptoactivos no estables, aunque para lograrlo requieren mecanismos de estabilización que pueden traer riesgos particulares. Aunque los criptoactivos estables comparten en general la mayoría de los riesgos detectados para los no estables, su adopción y uso presentan riesgos particulares relacionados con el manejo de las reservas y otros mecanismos de estabilización, la posible criptoización de las economías y los impactos monetarios de una adopción generalizada.

La última sección concluye con una discusión sobre el estado actual del mercado de criptoactivos, se comentan brevemente algunos de los esfuerzos internacionales para establecer principios y estándares para su operación entre la población usuaria y las instituciones, y se analizan algunos de los enfoques que han tomado diversas jurisdicciones a nivel global en esta materia.

II. Criptoactivos no estables

Los criptoactivos no estables o sin subyacente, a los que llamaremos de esta forma para diferenciarlas de las llamadas *stablecoins* o de los activos tradicionales tokenizados,[5] se caracterizan por el hecho de que su valor no está respaldado por otros activos y no son redimibles. En su lugar, su valor radica en la confianza que tienen sus tenedores de que éstas continuarán siendo aceptadas por otros. Estos son netamente digitales, y carecen de cualquier institución centralizada que controle su distribución y operación.

Los criptoactivos convencionales combinan tres características principales (BIS, 2018):

i) tienen un protocolo o conjunto de reglas establecidas en su código que determina cómo se realizan transacciones con ellas, y buscan alinear los incentivos de todos los participantes a través de lo que se conoce como mecanismo de consenso.

ii) cuentan con un registro (*ledger*) histórico de todas sus transacciones.

iii) están soportadas en una red descentralizada de participantes que actualizan, almacenan y acceden al registro de transacciones bajo las reglas del protocolo.

Estas características los diferencian de los depósitos en una institución financiera ya que permiten, en principio, que estos activos puedan transferirse en un marco descentralizado, es decir, sin la necesidad de que una contraparte (por ejemplo, un banco), ejecute y valide la transacción.

[5] En este caso, nos ceñimos a la clasificación propuesta por FMI (2021c). Las *stablecoins* se detallan en la sección III.

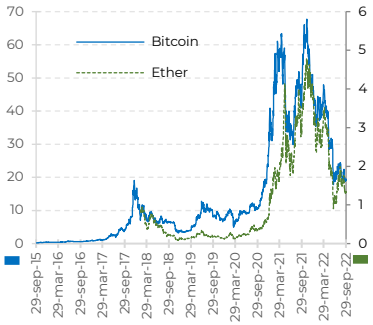
El ejemplo pionero de una "moneda" digital completamente descentralizada es el *bitcoin*, el criptoactivo diseñado por Satoshi Nakamoto en 2008 y soportado en la tecnología *blockchain*, una clase particular de registro distribuido descentralizado (DLT).[6] La llegada de *bitcoin* ha dado como resultado la aparición de un enorme número de activos digitales similares en los últimos años. CoinGecko, uno de los principales agregadores independientes de datos de criptoactivos, ha rastreado la cotización de más de 10 mil de estos en circulación, aunque solo un número muy reducido tiene un volumen de operaciones relevante. Además del *bitcoin*, que continúa siendo el de mayor circulación del mundo, otros criptoactivos han mostrado una circulación relevante como es el caso del *ether*, la "criptomoneda" nativa de la red *Ethereum*, o XRP (antes *ripple*), el activo virtual nativo de la red homónima.

Figura 1. Principales criptoactivos no virtuales en circulación

A. Cotización y valor de capitalización de los principales activos virtuales

Activo	Valor de capitalización (mMdd)	Cotización (Dólares por unidad)
Bitcoin (BTC)	384.9	20,078.4
Ether (ETH)	165.7	1,367.7
Binance Coin(BNB)	47.8	293.2
XRP (XRP)	24.8	0.50
Cardano (ADA)	14.5	0.43
Solana (SOL)	12.0	33.8

B. Precios del *bitcoin* y *ether* (miles de dólares)



Fuente: Elaboración propia con datos de Bloomberg y CoinGecko. Actualización: octubre 2022.

En particular, tanto el *bitcoin* como el *ether* han mostrado episodios de enorme volatilidad y crecimiento de su cotización, alcanzado máximos históricos a finales de 2021 (figura1B). Esto les ha permitido tener valores de capitalización comparables con algunas de las empresas más reconocidas en el mundo. Como se muestra en la tabla 1A, con cifras al cierre de octubre de 2022, el valor de capitalización total de *bitcoin* era ligeramente mayor al de Meta, la empresa matriz de Facebook, que se ubicaba en alrededor de 370 mil millones de dólares (mMdd), mientras que el valor conjunto de las 6

[6] Un DLT es un conjunto de tecnologías que permiten diseñar una estructura de sistemas que pueden operar como una base de datos descentralizada. En principio, son sistemas más seguros que los tradicionales centralizados, ya que carecen de un servidor central que concentre toda la información.

principales "criptomonedas" era cercano al valor de Tesla (700 mMdd). Si bien los principales criptoactivos se encuentran lejos del valor de algunas de las empresas más grandes del planeta como Apple (2.2 Bdd), Microsoft (1.8 Bdd) o Alphabet-Google (1.3 Bdd), sus valores de capitalización están lejos de ser despreciables.

Funcionamiento y operación de los criptoactivos no estables

Los criptoactivos son en su forma más elemental códigos de computadora, y como tales viven netamente en un marco digital. Esto ha ocasionado que el conocimiento detallado sobre su funcionamiento se haya concentrado más en los programadores y científicos informáticos, que en los especialistas económicos y financieros. No obstante, su integración cada vez mayor a los mercados financieros tradicionales y la aparición de los proyectos de finanzas descentralizadas hacen necesario tener un conocimiento básico de la operación de esta clase de activos.

Para fines prácticos, esta sección se concentrará en las dos principales redes: *Bitcoin* y *Ethereum*. La red *Bitcoin*, su "criptomoneda" nativa del mismo nombre y la tecnología *blockchain*, que le da origen y sustento, son conceptos esenciales para entender la operación del mercado de criptoactivos en general. La mayoría de los activos virtuales en circulación operan actualmente, salvo ciertas particularidades, en un entorno inspirado en el diseño pionero de esta red.

Por su parte, la red *Ethereum*, cuya "criptomoneda" *ether* es la segunda de mayor circulación a nivel mundial, presenta una operación más compleja, debido a que permite la creación de contratos inteligentes. Estos hacen posible automatizar algunas operaciones con estos activos y han facilitado que, entre otras cosas, nuevos participantes diseñen sus propios criptoactivos y ofrezcan "servicios financieros alternativos" a través de esta red. Entender su funcionamiento es esencial para comprender cómo operan otros activos como las llamadas *stablecoins* y el surgimiento de las llamadas finanzas descentralizadas (DeFi).

Finalmente, se incluye una explicación de la operación de las plataformas de intercambio o *exchanges*. Si bien los criptoactivos pueden operar completamente a través de sus redes digitales nativas, las plataformas de intercambio se han vuelto el punto focal de gran parte de las transacciones. Los *exchanges* se han convertido en el principal vínculo entre estos activos y el sistema financiero, y su expansión a otras áreas del mercado los han transformado en un elemento básico de su ecosistema. Como resultado de estos desarrollos, los *exchanges* deben ser considerados como de interés prioritario para cualquier autoridad del sistema financiero.

La red *Bitcoin*

Al discutir sobre la red *Bitcoin*, nos estaremos refiriendo al protocolo (reglas codificadas en su programación) y al conjunto de participantes que permiten la operación del *bitcoin* de forma puramente digital. Una descripción completa de su operación requiere cierto grado de conocimiento técnico en programación e informática.[7] No obstante, una explicación de los términos básicos permite discernir y evaluar las posibles implicaciones económicas, regulatorias y de supervisión que entraña, al menos someramente.

La red *Bitcoin* es completamente abierta y no requiere de permisos: cualquier persona puede participar en ella mientras cuente con un dispositivo electrónico y con alguno de los softwares abiertos que permiten el acceso.[8] Cada computadora o dispositivo que participa en la red se convierte en un nodo, es decir, se vuelve parte de una red de computadoras que siguen el protocolo de la red y son esenciales para mantener su integridad.

La estabilidad y seguridad de la red *Bitcoin* se basa en la existencia de la *blockchain*. Conocida en español como cadena de bloques, esta es un tipo particular de tecnología de registro distribuido (DLT) abierto, disponible en cada uno de los nodos de la red *Bitcoin*, y dónde cada bloque de información es referenciado criptográficamente a su antecesor. La cadena de bloques es un registro histórico de todas las operaciones realizadas en la red, la cual puede ser consultada por cualquier nodo sin restricciones. El hecho de que los bloques de información estén ligados entre sí asegura que, por un lado, el registro sea prácticamente inalterable, lo que ofrece confianza de que las operaciones registradas son auténticas y, por otro lado, permite mantener un orden cronológico de las operaciones, ya que cada bloque depende de la información del bloque anterior para su construcción. Los nodos pueden ser completos, al albergar una copia íntegra de la *blockchain*, o ligeros (*light*), al únicamente conectarse con alguno de los nodos completos. Al momento de la redacción, se estima que existen más de 40 mil nodos activos con diferente dirección IP en la red *Bitcoin*.[9]

Al contrario que en los sistemas de pago digitales convencionales, el usuario puede realizar operaciones a través de la red *Bitcoin* sin la necesidad de ofrecer información de identificación directa. En su lugar, se necesita una

[7] Para una explicación detallada de los elementos de programación relacionados con la red *bitcoin* puede consultarse en Antonopoulos (2017).

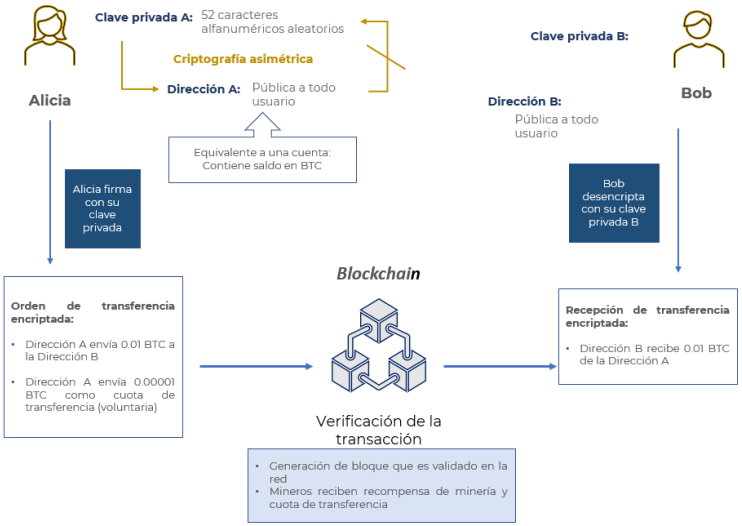
[8] Aunque existen una multitud de programas para acceder a *Bitcoin*, el software más comúnmente utilizado es *Bitcoin Core*, con alrededor de 97% de los nodos activos utilizándolo (Mehta et al., 2021).

[9] La identificación de los nodos depende de la dirección IP, que es una dirección única que identifica a un dispositivo en internet o una red local que permiten el envío de información entre estos (https://latam.kaspersky.com/resource-center/definitions/what-is-an-ip-address). El dato proviene de https://bitnodes.io/, accedido el 27 de septiembre de 2022. Aunque el número de nodos registrados es mucho mayor, solo 14.7 mil nodos son alcanzables de acuerdo con la estimación de la página.

clave privada, que permite generar una dirección que funciona como un identificador seudónimo del cliente. La clave privada es una secuencia completamente aleatoria de 52 caracteres alfanuméricos que, por seguridad, debe ser conocida únicamente por el propietario. Para realizar transacciones, se debe tener al menos una dirección, la cual se genera a partir de la clave privada a través de herramientas de criptografía asimétrica. La dirección funciona tanto como un identificador seudónimo como un equivalente a una cuenta de depósito, que es pública para todo nodo de la red. Debido al uso de procesos criptográficos, no existe ningún proceso de ingeniería en reversa que posibilite obtener la clave privada a través de la dirección, lo que permite realizar una transacción segura sin la necesidad de revelar información adicional de identificación de las personas participantes.[10]

El manejo de los *bitcoins* se diseñó para ser autogestionado: la persona poseedora de la clave privada tiene control único y completo sobre los criptoactivos contenidos en las direcciones asociadas a ésta, y puede disponer de ellos discrecionalmente. El resguardo de las claves privadas es responsabilidad total de las y los usuarios. Éstas son inmodificables e irrecuperables, por lo que, en caso de extravío, los *bitcoins* en las direcciones ligadas a ella quedarían bloqueadas permanentemente.

Figura 2: Transferencia en la red *Bitcoin*

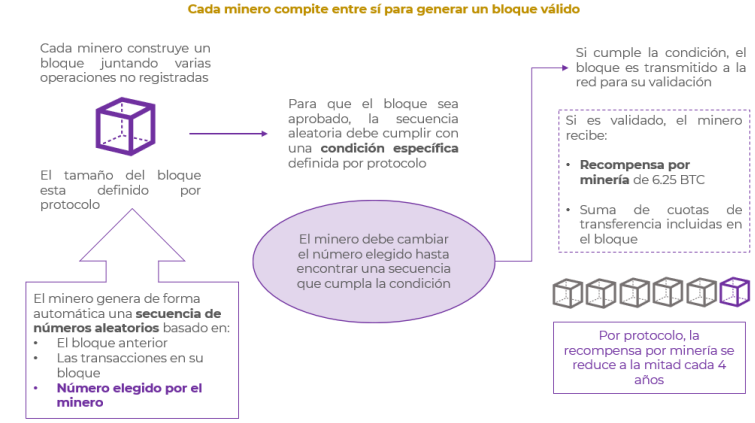


Fuente: Elaboración propia.

[10] Una explicación sencilla de la criptografía asimétrica que permite el funcionamiento descentralizado de la red *Bitcoin* puede leerse en (Lewis, 2018).

Un ejemplo básico de una operación con *bitcoins* se presenta en la figura 2. Para realizar una operación, el emisor debe firmar el movimiento de *bitcoins* de su dirección utilizando la clave privada ligada a ésta. La orden se transmite a los diversos nodos de la red *Bitcoin*, los cuáles pueden verificar si la operación es válida accediendo a la *blockchain*. Para controlar el lapso en que ocurre una transacción y construir un orden cronológico de éstas, las operaciones son agrupadas en bloques de información. La creación de bloques implica trabajo para los nodos, ya que deben comprobar que cada operación incluida sea válida. Para asegurar que los incentivos para construirlos sean los adecuados, la red *Bitcoin* utiliza un mecanismo de consenso llamado prueba de trabajo (*proof-of-work*, PoW). Una explicación sencilla del proceso se presenta en la figura 3. Éste consiste en que participantes voluntarios, conocidos comúnmente como mineros, agrupan un conjunto de operaciones aún no registradas en la *blockchain* en un bloque verificando que éstas sean válidas. El tamaño del bloque está definido por el protocolo, lo que asegura control en el número de operaciones que pueden procesarse en un tiempo determinado.

Figura 3: Prueba de trabajo (*Proof-of-work*, PoW)

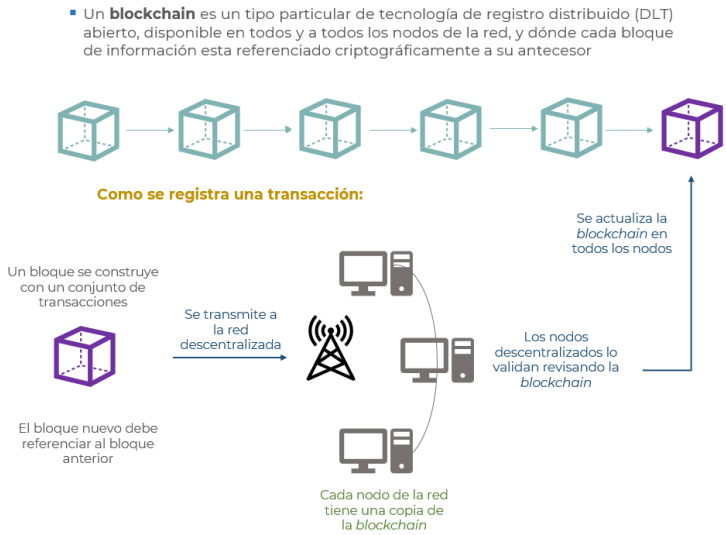


Fuente: Elaboración propia.

Para que el bloque sea sujeto a la validación de la red, el minero necesita proveer de una secuencia de caracteres que cumpla con una condición específica cuya dificultad es definida de forma automática por el protocolo. Esta secuencia se genera automáticamente con herramientas criptográficas utilizando la información del bloque inmediatamente anterior, de las transacciones en el bloque construido y un número elegido por el minero. Cumplir con la condición es computacionalmente costoso. La solución sólo

puede encontrarse de forma aleatoria a través del proceso iterativo de probar diferentes números seleccionados por el minero hasta cumplirla. La condición, que no requiere habilidad al ser netamente aleatoria, y su dificultad, que se ajusta en función de la cantidad de participantes y el número de operaciones en espera de ser registradas, aseguran que los mineros compitan entre sí para crear el bloque y que el tiempo para realizarlo sea generalmente estable.

Figura 4: Definición y operación de la *blockchain*



Fuente: Elaboración propia.

Cuando algún minero cumple con la condición específica, su bloque es transmitido a la red y, en caso de ser validado por ésta, agregado a la *blockchain* (véase figura 4). En promedio, toma alrededor de 10 minutos incluir un nuevo bloque al registro.[11] El minero recibe un pago por su trabajo consistente en una emisión de *bitcoins*, de ahí el nombre común de minería para este proceso, y la suma de las cuotas voluntarias incluidas en las transacciones en su bloque. Puede darse la situación en que múltiples mineros cumplan casi simultáneamente con la condición específica para agregar un bloque, lo que generaría varias cadenas diferentes. En esos casos, el protocolo define que sólo la cadena de bloques más larga se considera válida.

[11] En algunos casos el proceso puede tardar un mayor tiempo bajo condiciones de congestionamiento como se discute posteriormente.

La ganancia por minería está definida por protocolo y se ubica al momento de la redacción en 6.25 *bitcoins* por bloque agregado al *blockchain*. De hecho, el proceso de minería es la única forma de agregar nuevos *bitcoins* a la oferta global. El protocolo establece que la ganancia por esta actividad vaya decreciendo a la mitad cada cuatro años. Bajo este esquema, las ganancias por minería se reducirían a prácticamente cero en las próximas décadas y la oferta de estos activos quedaría definida permanentemente en alrededor de 21 millones (Mehta et al., 2021).[12]

Una vez que la operación se encuentra en la *blockchain*, ésta es prácticamente irreversible en condiciones normales.[13] El registro incluye el monto de operación y las direcciones del emisor y receptor. El tiempo en que ocurrió la transacción está definido por el bloque al que pertenece. Estos datos son actualizados simultáneamente en todos los nodos de la red y, combinado con la naturaleza abierta de su acceso, ofrecen transparencia sobre las operaciones realizadas.

La red *Ethereum*

Al contrario que la red *Bitcoin*, construida con la intención de funcionar directamente como la plataforma de pago descentralizada de una "moneda digital", la red *Ethereum* es una *blockchain* programable de propósito general (Antonopoulos & Gavin, 2018). La red permite, entre otras varias aplicaciones, establecer contratos inteligentes, es decir, programas que permiten almacenar y transmitir activos virtuales de acuerdo con reglas preestablecidas en su código. Su "criptomoneda" nativa, llamada *ether*, fue diseñada primordialmente como un token de utilidad, cuya función es permitir la operación de la red y mantener su integridad, incluyendo el cumplimiento de estos contratos.

En *Ethereum*, la persona usuaria puede enviar *ether* a un contrato inteligente para invocarlo. Todas las transacciones y contratos inteligentes son operados por los nodos participantes a través de un sistema operativo llamado Máquina Virtual de *Ethereum* (EVM). Al momento de la redacción, se estima que existen alrededor de 8.7 mil nodos activos.[14] Cada uno de ellos opera como una EVM independiente, lo que permite que puedan llevar a cabo cualquier tipo de operación de forma individual, desde una transferencia de

[12] El *bitcoin* no es perfectamente divisible. La menor fracción de la criptomoneda es el satoshi, que equivale a una diezmillonésima parte de un *bitcoin*. Al año 2140, la ganancia por minería se ubicaría en un nivel que requeriría una división menor a un *satoshi*. No obstante, considerando el decaimiento exponencial de las ganancias por minería, estas se ubicarán en niveles cercanos a cero con antelación.

[13] En el apartado siguiente se discutirán las ventajas y desventajas de la irreversibilidad, y los casos particulares en los cuales se puede revertir una operación.

[14] El dato proviene de https://www.ethernodes.org/ , accedido el 27 de septiembre de 2022.

ethers hasta el más sofisticado contrato inteligente.[15] Al ser una computadora virtual, es posible utilizar *Ethereum* para operar otros activos virtuales programados dentro de la red, como es el caso de los NFT (tokens no fungibles por sus siglas en inglés)[16] y la mayoría de las llamadas *stablecoins* (véase Sección III).

Al igual que la red *Bitcoin*, la red *Ethereum* es una red abierta y sin permisos, a la que cualquier persona con un dispositivo electrónico con acceso a internet puede conectarse. Ambas redes ofrecen la misma transparencia, al registrar sus operaciones en una *blockchain* abierta que puede ser consultada por cualquier nodo participante. No obstante, cambios recientes en la operación de la red la han diferenciado más de la red *Bitcoin*. Originalmente, ambas utilizaban el mismo mecanismo de consenso para validar las operaciones: la prueba de trabajo (PoW). Bajo este esquema, de forma similar a lo que ocurre en la red *Bitcoin*, los mineros obtenían una recompensa de 3 *ethers* por cada bloque validado y agregado a la *blockchain*. La recompensa en *Ethereum* era constante por protocolo, en lugar de reducirse a la mitad cada 4 años, lo que aseguraba que la oferta de *ethers* creciera a una tasa estable y conocida.

En septiembre de 2022, el mecanismo fue reemplazado por la prueba de participación (*proof-of-stake*, PoS) en lo que fue popularmente conocido como el *Merge*.[17] Al contrario que la red *Bitcoin*, *Ethereum* ya no requiere de mineros para generar bloques (véase figura 5). En su lugar, la red requiere de la presencia de validadores, los cuales se encargan de verificar las operaciones. Para ser un validador, el usuario debe depositar 32 *ethers* en un contrato inteligente que le permite darse de alta como tal, lo que comúnmente se llama *staking*. Este depósito actúa como una reserva, ya que no puede ser comprado o vendido, al menos inicialmente.[18] Para crear un bloque, el protocolo elige al azar a uno de estos participantes para construirlo, por tanto, la probabilidad de ser elegido depende de la cantidad de ETH puesta en reserva (número de cuentas de validador en posesión). Los encargados de

[15] El lenguaje de programación utilizado en *Ethereum* es *Solidity* y fue diseñado por los programadores originales de la red con el objetivo de construir contratos inteligentes.

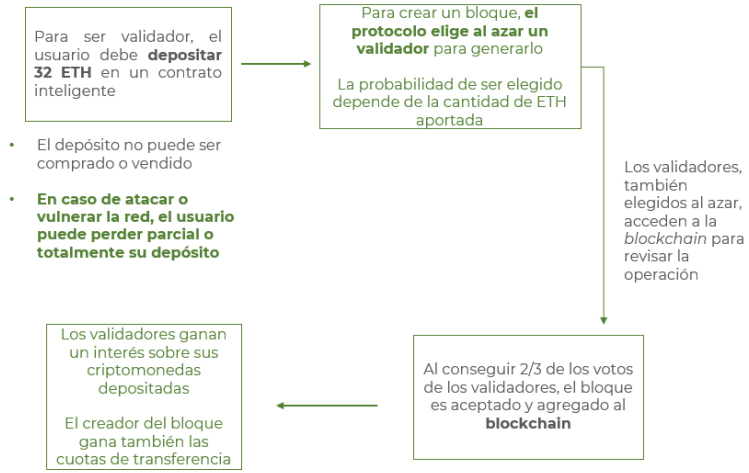
[16] En términos muy simples, un NFT puede definirse como un coleccionable digital cuya verificación de autenticidad se logra a través de su registro en el *blockchain* (Véase https://latam.kaspersky.com/blog/que-es-un-nft/22918/). Al contrario que las "criptomonedas", que se consideran fungibles ya que todas las unidades son idénticas e intercambiables entre sí, los NFT son únicos e irrepetibles y por ende pueden tener valores diferenciados. Este tipo de activos se han vuelto populares primordialmente en el mundo del arte digital.

[17] Véase ethereum.com/en/developers/docs/consensus-mechanism. Al contrario que el PoW, el PoS no requerirá la minería de bloques ya que los usuarios son asignados de forma aleatoria para crear un bloque, o en caso contrario, para comprobar su validez. Buterin (2022) recopila algunos de los principales *white papers* y publicaciones en blogs de Vitalik Buterin, el principal programador detrás de la red *Ethereum*, lo que permite hacer un rastreo de cómo fue planteada y planeada la transición de PoW a POS.

[18] La red *Ethereum* lanzó en abril de 2023 la actualización Shanghái que permite el retiro de las ganancias derivadas de la validación de bloques e incluso retirarse de ser validador al incluirse en una lista de espera para este fin. Véase https://www.binance.com/en/ethereum-upgrade.

verificar la validez de los bloques también son elegidos aleatoriamente y, al igual que en la red *Bitcoin*, acceden a la *blockchain* para cumplir con este fin. Al conseguir al menos dos terceras partes de los votos de los validadores, el bloque se considera válido y es incluido a la *blockchain*. Al contrario que en la prueba de trabajo, tanto los validadores como los creadores del bloque obtienen recompensas en forma de un interés sobre su posición de reserva. El creador del bloque obtiene las cuotas de transferencias incluidas. Para asegurarse que los incentivos se alineen de forma adecuada, el protocolo castiga a los validadores que vulneren la red con la pérdida parcial o total del depósito ofrecido de acuerdo con la gravedad de la conducta infractora.[19]

Figura 5: Prueba de participación (*Proof-of-stake*, PoS)



Fuente: Elaboración propia

Además del nuevo mecanismo de consenso, existen diferencias importantes en el funcionamiento entre *Ethereum* y *Bitcoin*. En primer lugar, los bloques en *Ethereum* se construyen a un ritmo mayor en comparación con la red *Bitcoin*, 12 segundos en contra de 10 minutos promedio, por lo que las transacciones con *ether* son por diseño más veloces.[20] En segundo lugar,

[19] Esto incluye desde cosas simples como desconectarse temporalmente de la red, hasta construir bloques con operaciones no válidas.

[20] Originalmente, la mayor velocidad en construcción de bloques también generaba que existiera una mayor probabilidad de que se generen bloques válidos de forma simultánea. Para asegurar que los mineros se mantuvieran incentivados para generar bloques, a pesar de que es muy probable que estos queden fuera de la *blockchain*, *Ethereum* premiaba con una recompensa de entre 0.624 y 2.625 *ethers* por cada bloque válido fuera de la *blockchain* que hayan sido referenciados por otro minero. Actualmente, el mecanismo de prueba de participación no parece sufrir de esta debilidad.

debe enfatizarse que *Ethereum* es una computadora virtual, por lo que los validadores no sólo están registrando operaciones de transferencia sino también corriendo programas en sus propias computadoras. La posibilidad de crear contratos inteligentes ocasiona que existan múltiples tipos de operaciones en la red, cada una de ellas con complejidad diferente y por tanto con un costo computacional variable. Para captar estas diferencias, se han establecido unidades de medida de este costo, conocidas comúnmente como Gas. Cada tipo de operación tiene un costo definido similar a un catálogo de precios: las operaciones simples requieren una menor cantidad de Gas para ser realizadas, mientras que las más complejas podrían requerir una cantidad mucho mayor.

Al realizar una orden en *Ethereum*, sea una transferencia de *ethers* o lanzar un contrato inteligente, el usuario debe definir un precio que está dispuesto a pagar por unidad de Gas, y el límite de Gas que está dispuesto a consumir para llevar a cabo su operación.[21] El validador que crea el bloque recibe por su trabajo la cuota de Gas cobrada en las operaciones realizadas, adicional a su recompensa por protocolo.

Un punto final que debe recalcarse es que la versatilidad de la red *Ethereum* y otras redes que han surgido a su imagen ha sido la punta de lanza de diversos desarrollos con probabilidad de ser disruptivos en los mercados financieros. Uno de ellos es la aparición de nuevos criptoactivos desarrollados utilizando la capacidad de programación en la red, la mayoría de las cuales han comenzado su circulación a través de las llamadas ICOs (Ofertas iniciales de monedas, por sus siglas en inglés). Éstas pueden definirse como la creación de tokens[22] por parte de privados que se distribuyen a usuarios o inversionistas, a cambio de retornos o la promesa de un producto o servicio en el futuro (OECD, 2019). Igualmente, también han surgido las llamadas *stablecoins*, activos virtuales que buscan mantener una paridad con algún activo o conjunto de ellos.

Al ser operadas dentro de redes programables, los movimientos tanto de los tokens como de las *stablecoins* son registrados en la *blockchain* y son comerciables dentro de estas redes y en *exchanges*. Estos avances han dado origen a las finanzas descentralizadas (DeFi), es decir, a la provisión de servicios financieros sin intermediarios centralizados, ya que las operaciones de intercambio, crédito e inversión pueden realizarse a través de protocolos automatizados a través de contratos inteligentes en *blockchains*

[21] Establecer un límite al Gas dispuesto a consumir es particularmente importante en el caso de contratos inteligentes. Por ejemplo, un error de programación podría llevar al contrato a un *loop* perpetuo, lo que llevaría a una cuota de operación igualmente infinita. Si una operación supera el límite de Gas propuesto, ésta se detiene y el creador del bloque recibe la recompensa de Gas pactada.

[22] Un token puede definirse como un objeto físico o digital que representa un valor o derecho dentro de un contexto.

programables (Aramonte et al, 2021). Todos estos desarrollos se revisarán en mayor medida en la sección III.

Las plataformas de intercambio de criptoactivos (*exchanges*)

Las "criptomonedas" pueden transaccionarse en sus propias plataformas par-a-par (*peer-to-peer*) sin la necesidad de un tercero que valide y garantice las operaciones. No obstante, al menos en el caso de las principales en circulación, es imposible obtener una unidad de estos en la red sin recibirla de alguien que ya la posee.[23] Igualmente, no es posible intercambiar diferentes tipos de criptoactivos entre sí, al menos de forma directa, ya que generalmente las redes no están integradas.[24] Aunque es posible negociar la compraventa *over-the-counter*,[25] ya sea con moneda fiduciaria o con otra "criptomoneda", esto requiere conjuntar de forma independiente a compradores y vendedores, además de enfrentar el riesgo de tratar con individuos sin algún intermediario que garantice el cumplimiento de las condiciones pactadas.

Estas necesidades han dado origen a las plataformas de intercambio o *exchanges*. Las plataformas, en su forma más tradicional, son entidades privadas, que operan de forma equivalente al mercado de valores, al conectar a compradores y vendedores de criptoactivos y funcionar como cámara de compensación.

Estas plataformas, de forma simplificada, operan cumpliendo cuatro pasos básicos (Lewis, 2018). En el primer paso, el cliente debe generar una cuenta en la plataforma de intercambio, lo que en la mayoría de las jurisdicciones requiere cumplir con requisitos de identificación similares a los solicitados en un banco para abrir una cuenta de depósito. En segundo lugar, una vez que la cuenta ha sido aprobada, el usuario debe depositar fondos antes de comenzar un intercambio. Estas pueden ser fondeadas tanto con moneda fiduciaria como con criptoactivos, dependiendo de las políticas del *exchange*. El tipo de monedas fiduciarias (dólares, euros, pesos) y "criptomonedas" (*bitcoin*, *ether*, o *stablecoins*) aceptadas es establecido por cada plataforma. En tercer lugar, una vez que la cuenta tiene los recursos requeridos, es posible realizar intercambios de cualquier tipo de activos a través de ofertas de compra o de venta, y esperando a que otros clientes las acepten. En la mayoría de los casos, los *exchanges* tienen las llamadas *hot wallets*, es decir cuentas con recursos propios de la plataforma que se utilizan

[23] También es posible obtenerlos a través del proceso de minería en el caso del *bitcoin*.

[24] Esto ha cambiado en los últimos años con el surgimiento de los llamados bridges (puentes), que permiten intercambiar criptoactivos de redes diferentes a través de la generación de un token que represente el criptoactivo que se desee intercambiar en una red programable, haciendo que el intercambio sea indirecto. Estos desarrollos se discutirán con más detalle en capítulos posteriores.

[25] Una operación *over-the-counter* se refiere a aquella realizada fuera de bolsas o mercados organizados.

generalmente para atender órdenes de menor monto rápidamente. En cuarto lugar, una vez que se ha aceptado un intercambio, el *exchange* realiza la transferencia asegurándose de que las condiciones de intercambio se cumplan cabalmente.

En su forma más tradicional, las plataformas de intercambio generan ingresos a través de cobrar comisiones por cada transacción. Para asegurar que las operaciones de compraventa se lleven a cabo, los *exchanges* deben tener forma de acceder a los fondos de los clientes, lo que en caso de los criptoactivos podría requerir que los clientes den acceso, aunque sea indirecto, a sus claves privadas. Toda operación con criptoactivos se realiza a través de su plataforma propia, por lo que parte de la labor del *exchange* es realizar estas operaciones en las plataformas par-a-par a nombre de sus clientes sin revelar información privada de cada contraparte. Una forma en que clientes y *exchanges* lidian con esta situación es a través de los proveedores de monederos digitales, o *wallet providers*. Estos son servicios privados donde una empresa custodia las claves privadas de los clientes y realiza la gestión de sus direcciones a su nombre. En muchos casos, los *exchanges* ofrecen estos servicios a través de sus propios proveedores, con lo que simplifican sus operaciones.

En los casos en que los *exchanges* operan con moneda fiduciaria, es necesario cumplir con protocolos de identificación de clientes (*Know-your-customer*, KYC) para la Prevención del Lavado de Dinero y Financiamiento al Terrorismo (PLD/FT), dependiendo de la regulación vigente en la jurisdicción de operación de la plataforma. Debe enfatizarse que en toda jurisdicción que siga los estándares internacionales en materia prudencial, las operaciones de captación están restringidas únicamente a entidades financieras autorizadas, las cuales están fuertemente reguladas y supervisadas. Por esta razón, los *exchanges* generalmente deben operar a través de instituciones financieras autorizadas para manejar indirectamente los recursos de sus clientes. En contraste, los que intercambian únicamente con criptoactivos pueden operar en un área legal gris, ya que en la mayoría de los países no existen marcos que regulen la captación y compraventa de esta clase de activos.

Los *exchanges* son el medio más comúnmente utilizado para hacer transacciones con criptoactivos. Por dar un ejemplo, estimaciones recientes sugieren que alrededor del 60% del volumen real de operaciones con *bitcoin* en el mundo está relacionado con ellos. Esto, además de destacar la importancia de estos en el ecosistema, sugiere que mantener los criptoactivos para realizar transacciones de compra de bienes y servicios no es el principal objetivo de los usuarios de estos activos.

Otro factor relevante en materia regulatoria es que el negocio de las plataformas se ha expandido a diferentes actividades en el mercado de

activos virtuales. Muchos de ellos ofrecen, además de las operaciones básicas de compraventa y conversión de criptoactivos, servicios de custodia, manejan *pools* de mineros y validadores, generan y dirigen sus propios criptoactivos estables y no estables, integran en sus sistemas el intercambio de criptoderivados y otorgan servicios CeFi, es decir, operaciones de inversión y crédito con activos puramente digitales, pero realizadas por un agente centralizado (Aramonte et al, 2021). Estas características hacen de los *exchanges* uno de los puntos focales del mercado de criptoactivos a nivel mundial y un punto de particular atención de los esfuerzos en materia de regulación y supervisión de los mercados.

Beneficios y riesgos de los criptoactivos no estables

Los activos virtuales, particularmente las "criptomonedas" como el *bitcoin* o *ether*, han sido sujetos a un interés creciente por parte de las autoridades, empresas privadas, entidades financieras y de una proporción relevante del público en general desde su aparición. El interés ha estado impulsado principalmente por su masificación en medios y sus elevados rendimientos durante algunos años. Aunque persiste el entusiasmo en redes sociales y foros virtuales alrededor del mundo, es importante recalcar que el entendimiento sobre sus beneficios potenciales y, sobre todo, de sus riesgos inherentes no es tan detallado como sería adecuado para activos que pretenden ser utilizados como medios de pago e inversión. [26] Al entender el funcionamiento de estos activos, algunos de los posibles desafíos que podría traer su adopción generalizada resultan más evidentes. En esta sección se presenta una revisión de las principales ventajas que se han propuesto y, posiblemente más importante, de los riesgos que podría traer su adopción más generalizada.

Uso transaccional de los criptoactivos no estables

Los criptoactivos sin subyacente como el *bitcoin* fueron diseñados originalmente con la intención de funcionar de forma análoga al dinero en efectivo (Nakamoto, 2008). El mecanismo de consenso en las redes y la existencia de una *blockchain* descentralizada de acceso abierto, permite a cualquier persona con un dispositivo digital realizar operaciones con ellos de forma relativamente segura a través de la plataforma par-a-par sin la necesidad de cumplir con requisitos estrictos de identificación.

Quienes proponen su adopción han argumentado que estos tienen beneficios potenciales en varias áreas. En primer lugar, su uso generalizado podría tener un impacto positivo en la adopción de los servicios financieros digitales, particularmente entre la población con menores ingresos. Este impacto podría ser mayor en economías emergentes, donde el acceso a

[26] Esta situación no es exclusiva de los criptoactivos, pero se vuelve especialmente relevante en ellos al operar en muchos casos fuera del marco institucional tradicional del sistema financiero.

servicios y medios digitales de pago a través de instituciones financieras tradicionales continúa rezagado y enfrenta varios obstáculos. Estos incluyen, entre otros, la obligatoriedad de abrir una cuenta con una institución financiera, la lejanía de los canales financieros físicos y la necesidad de amplia documentación para cumplir con los requisitos de identificación y debida diligencia, lo que afecta desproporcionadamente a la población con menos recursos (Feyen et al., 2021). Por supuesto, este potencial requiere que los individuos tengan acceso a dispositivos digitales con las capacidades adecuadas, algo que bien puede no ocurrir en hogares de bajos ingresos. A pesar de esto, el acceso a pagos digitales a través del uso de criptoactivos podría presentar requisitos menores y más sencillos que el acceso a los canales digitales tradicionales.

Por otro lado, quienes apoyan su adopción consideran que su uso puede ser particularmente eficiente para realizar transferencias transfronterizas, lo que es importante para países de bajo y mediano ingreso que tienen una mayor dependencia en las remesas. Las transferencias realizadas a través de bancos o de transmisores de dinero requieren convertir de una divisa a otra en ambos lados de la transacción, además de que generalmente no son inmediatos debido a los tiempos para compensación. En contraste, las realizadas con criptoactivos generalmente toman un tiempo muy reducido (alrededor de 10 minutos en la red *Bitcoin*) y tienen una disponibilidad más inmediata al no requerir conversiones.

Además, al momento de redacción, el costo de realizar una transferencia de criptoactivos puede considerarse bajo. Al cierre de 2022, las ganancias que reciben los mineros por validar operaciones consisten en una nueva emisión de 6.25 *bitcoins* definidas por el protocolo y de las cuotas de transferencia voluntarias incluidas en las operaciones del bloque validado. Considerando el valor en mercado de la ganancia por minería, el costo marginal de agregar una operación sin cuota de transacción a un bloque es prácticamente nulo. Como resultado, los mineros generalmente incluyen cualquier operación válida en los bloques, lo que ha permitido que, en la mayoría de los casos, los usuarios hagan transferencias par-a-par con costos ínfimos. En el entorno actual, la cuota de transferencia funciona más como un mecanismo para obtener prioridad entre aquellas personas usuarias que desean que sus transacciones se incluyan en la *blockchain* más rápidamente (Huberman et al., 2021).

Los proponentes del uso de los criptoactivos han argumentado también que las redes como *Bitcoin* y *Ethereum* han mostrado ser seguras y transparentes, aunque esto requiere ignorar en cierto grado la seudonimidad de sus usuarios. En el caso de las redes par-a-par, no existe un accidente

reportado de vulneración directa de sus protocolos de validación[27] y la transparencia en el acceso a la *blockchain* ofrece confianza en que las operaciones son definitivas e inmodificables. Adicionalmente, en países donde los corresponsales de remesas han enfrentado problemas de *de-risking*,[28] poder transferir recursos de forma digital sin ningún intermediario puede resultar particularmente atractivo (Feyen et al., 2021).

Aunque en principio pareciera existir un enorme potencial para utilizar los criptoactivos como herramientas para favorecer la digitalización e inclusión financiera de la población, parte primordial de esto depende de que sean adoptados de forma generalizada y aceptados como medio de pago. La evidencia empírica sugiere que la capacidad de los criptoactivos no estables para operar como "moneda" sufre de serios inconvenientes en la práctica. Su aceptación como medio de pago ha sido muy limitada en el ambiente comercial. De acuerdo con información de *Coinmap*, sólo cerca de 30 mil establecimientos en el mundo reportan aceptar pagos con criptoactivos, primordialmente *bitcoin*,[29] una proporción ínfima de los establecimientos a nivel mundial.[30]

La baja adopción de estos activos como medio de pago puede explicarse por diversos factores, aunque sin duda uno de los principales es su volatilidad. Al operar de forma descentralizada, no existe una autoridad (banco central) que tenga el mandato de mantener la estabilidad de su valor en el tiempo. Considerando que su oferta está definida por sus protocolos y no existe un activo de referencia, fluctuaciones en la demanda conllevan invariablemente a cambios en su valuación, lo que deriva en una elevada volatilidad (BIS, 2018). Se ha observado que las criptomonedas no estables son particularmente sensibles a las noticias (por ejemplo, cambios regulatorios hipotéticos o reales, su adopción o rechazo por algunas empresas), lo que puede llevar a crecimientos o caídas inusitadas de forma casi inmediata (FSB, 2021).

Otro de sus principales desafíos es la escalabilidad.[31] En el caso de la red *Bitcoin*, su propio mecanismo de consenso limita esta capacidad ante el

[27] El único evento de vulneración directa al protocolo de la red *Bitcoin* se detectó en agosto de 2010, cuando una vulnerabilidad en un bloque permitió generar miles de millones de *bitcoins* ilegalmente. La operación fue detectada y la red fue bifurcada, bajo consentimiento de la mayoría de las personas usuarias corrigiendo el error de programación (Lewis, 2018, p. 213). Ningún evento similar se ha presentado desde entonces hasta la fecha de redacción.

[28] El *de-risking* se define como el proceso en el cual las instituciones financieras abandonan o reducen significativamente ciertas líneas de negocio para evitar riesgos regulatorios y de cumplimiento (ASBA, 2017).

[29] La información está disponible en https://coinmap.org/view/#/world/50.09996918/14.46910948/2. Cifras al 25 de octubre de 2022.

[30] Para referencia, suponiendo que estos 30 mil establecimientos se ubicaran en México, representarían alrededor del 1.3% de los negocios dedicados a actividades comerciales en el país (2.25 millones de establecimientos dedicados a actividades comerciales, de acuerdo con datos de los Censos Económicos 2019, véase https://www.inegi.org.mx/programas/ce/2019/).

[31] Este concepto puede definirse como la capacidad de expandir la adopción de un medio de pago sin que esto genere un incremento desproporcionado en el costo de las transacciones.

elevado costo de generar confianza sin contar con una autoridad de contraparte. Por ejemplo, para mantener el control del flujo de transacciones, se requiere un tiempo de espera promedio de 10 minutos, lo que podría ser considerado muy largo para compras de mercancías de bajo costo o de consumo rápido. Por supuesto, esta espera podría ser perfectamente aceptable para transacciones de alto costo, aunque serían más susceptibles de enfrentar mayor vigilancia para evitar el lavado de dinero y el financiamiento al terrorismo.

También se ha observado que un flujo constante de operaciones puede llevar a períodos de congestionamiento. Por dar un ejemplo, un período de alta transaccionalidad en la red *Bitcoin* en diciembre de 2017 derivó en esperas de alrededor de 16 horas para confirmar una operación e incrementos en las cuotas por transacción ofrecidas, que superaron en su momento más álgido los 55 dólares promedio por transacción, ante la impaciencia de los clientes para que sus operaciones fueran registradas en la *blockchain* (Mehta et al., 2021; pp. 67-68).

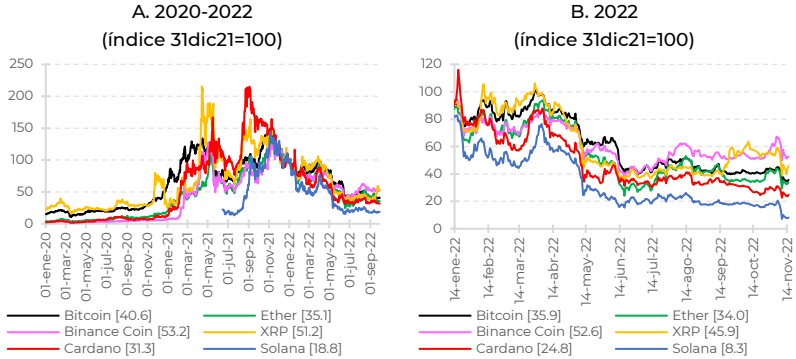
Además de esto, asegurar la validez de las operaciones realizadas con *bitcoin* o *ether* requiere la constante actualización de la *blockchain* en múltiples nodos descentralizados, lo que conlleva un creciente costo en memoria computacional para lograrse. Por ejemplo, hospedar un nodo completo para la plataforma *Bitcoin* requería en 2021, un mínimo de 440 GB de memoria libre, 2 GB de memoria operativa, y una conexión de banda ancha mínima de 400 kb por segundo. Los nodos deben correr por un mínimo de 6 horas diarias y podría requerir días para sincronizarse con la versión completa de la historia del *blockchain* la primera vez que se hospeda el nodo (WEF, 2021a. 2021b). Aunque es posible mantener solo nodos ligeros, la integridad de la red podría verse comprometida ante un número reducido de nodos completos.

El uso de criptoactivos como instrumentos de inversión

Como se comentó anteriormente, aunque las "criptomonedas" fueron diseñadas para operar como medio de pago, varios inconvenientes parecen haber limitado de forma importante su uso para este fin. Aunque algunos usuarios utilizan estos activos para realizar pagos, su volatilidad parece haber propiciado que su uso principal sea como activo de inversión. Por ejemplo, previo a 2022, el *bitcoin* había tenido rendimientos generalmente positivos e incluso mayores a los de los principales índices accionarios. Adicionalmente, estos activos virtuales habían mostrado baja correlación con otros activos tradicionales o índices bursátiles, lo que hace que algunos inversionistas los consideraran buenos valores en estrategia de inversión (FMI, 2021a). En 2022, esta apreciación parece haberse modificado, considerando que el incremento generalizado de la inflación, que llevó a un ciclo alcista en las tasas de interés

a nivel global que se reflejó en un mayor rendimiento de los bonos públicos, parece estar relacionado con una caída significativa en la cotización de los principales criptoactivos en circulación (figura 6).

Figura 6. Evolución de los principales criptoactivos no estables en circulación



Fuente: Elaboración propia con datos de Bloomberg.

A pesar de los choques que ha enfrentado el mercado de criptoactivos, el uso de estos como instrumento de inversión no se ha frenado. Sus principales adoptantes tienen un perfil más cercano a un inversionista regular que al carácter libertario de Satoshi Nakamoto y los primeros participantes de la red *Bitcoin* (Auer & Tercero-Lucas, 2021). De hecho, la mayor importancia relativa de los *exchanges*, por naturaleza centralizados y en muchos casos supervisados, sobre los canales netamente par-a-par sugiere que los usuarios están más interesados en la posibilidad de trasladar sus ganancias por valuación en criptoactivos hacía el mercado financiero tradicional que contar con un medio de pago efectivo y descentralizado, sin vigilancia de las autoridades.

El creciente interés en esta clase de activos, no sólo de inversionistas particulares sino también de institucionales en algunas economías, ha llevado en los últimos años al surgimiento de criptoderivados, es decir activos financieros cuyo valor está respaldado en la cotización de criptoactivos. Los primeros criptoderivados se diseñaron e intercambiaron de forma descentralizada a través de *exchanges* o en plataformas como *Ethereum*. Estudios recientes estiman que el tamaño del mercado de criptoderivados ha explotado en los últimos años, incluso rivalizando con el volumen diario transaccionado en la New York Stock Exchange en días de alta operación (Soska et al., 2021). Actualmente, existen múltiples fondos cotizados

(*exchanged traded funds*, ETFs),[32] es decir, fondos que no tienen exposición directa en criptoactivos, sino que buscan replicar el comportamiento de futuros en estos o de compañías que trabajan en el ecosistema. Varios de ellos operan en bolsas internacionales, por ejemplo, el *Proshares Bitcoin Strategy* (BITO) y el *Valkyrie Bitcoin Fund* (BTFD) en Estados Unidos; el *Purpose Bitcoin ETF* (BTC), el *Evolve Bitcoin ETF* (EBIT) y el *Cryptocurrencies ETF* en Canadá, y el *Nasdaq Crypto Index ETF* (HASH11) en Brasil.

A pesar de esta mayor participación en los mercados de derivados, debe tenerse en cuenta que los usuarios continúan expuestos a riesgos similares a los que tendrían con una exposición directa a los criptoactivos. El hecho de que estos ETFs cotizan en bolsas establecidas no debe interpretarse como una "marca de seguridad", ya que un colapso en el sector de criptoactivos podría arrastrar a las empresas en el ecosistema a una caída similar en sus cotizaciones. Por esta razón, es importante que los usuarios sean conscientes de los posibles riesgos que conllevan las operaciones con estos activos en general.

Protección de la población usuaria

La masificación en medios de los criptoactivos y su desempeño los ha convertido en materia de interés no sólo de inversionistas especializados, sino también de la población en general. No obstante, su operación descentralizada y el conocimiento financiero y tecnológico que requieren para su operación los hace frágiles en materia de protección de usuarios, especialmente si se considera que algunos de los usuarios podrían tener bajos niveles de alfabetización digital y financiera. Aunque los proponentes han argumentado que las personas no incluidas en el sistema financiero tradicional podrían beneficiarse de adoptar estos activos, no debe obviarse que parte importante de los participantes podrían no comprender plenamente los riesgos asociados con los criptoactivos (WEF, 2021b), algo que ya ocurre con los productos financieros tradicionales, pero que podría intensificarse ante las características particulares de estos activos.

Realizar operaciones con *bitcoins* o *ethers*, incluso si se hacen a través de *exchanges*, requiere de la clave privada. Debe enfatizarse que estas claves son autogestionadas por el cliente: su resguardo y seguridad dependen únicamente del usuario y no son recuperables. Los recursos dentro de una dirección están tan seguros como lo esté su clave privada. Si el usuario la extravía, los recursos dentro de las cuentas asociadas quedarían bloqueados permanentemente. Si bien no es posible saber el número de personas que podrían haber perdido acceso a sus activos virtuales, existe una tasa

[32] Un ETF es un fondo de inversión, un vehículo que concentra aportaciones de varios inversionistas para invertirlos en otros activos, que cotiza en bolsa de valores, lo que permite que se puedan comprar y vender fácilmente como si fueran acciones individuales.

importante de recursos que han permanecido inmóviles por años. Un estudio reciente sugiere que alrededor del 60% de los *bitcoins* minados pasaron más de un año sin movimiento, mientras que 20% no se ha movido en cinco años (Mehta et al., 2021).

En caso de robo de la clave, el ladrón tendrá acceso total a los recursos dentro de la dirección sin posibilidad de que el dueño legítimo pueda evitarlo en condiciones normales. Es probable que muchos clientes incluso ignoren el hecho de que, al entregar su clave privada a alguna plataforma de intercambio o algún proveedor de monederos para activos virtuales para resguardo, podrían estar dando acceso completamente discrecional a sus recursos si los proveedores de servicios de criptoactivos no ofrecen protección adecuada o actúan de forma deshonesta.

Adicional a estos posibles problemas derivados de la autogestión, debe también considerarse la irreversibilidad de las operaciones, uno de los temas más controversiales en materia de criptoactivos. Al contrario que en transacciones realizadas a través de medios tradicionales, donde se pueden recurrir al intermediario financiero y/o una autoridad en casos en que se necesite anular una operación, el mecanismo de consenso de las criptomonedas hace relativamente imposible revocar una transacción una vez que esta se ha incluido en la *blockchain*, indistintamente de su naturaleza. En caso de realizar una operación por error, sufrir un robo o ser víctima de extorsión o fraude en operaciones con criptoactivos, no existe ningún mecanismo intrínseco de protección que permita la recuperación de los recursos dentro de la red.

Este inconveniente es aún más serio en el caso de contratos inteligentes, donde los riesgos o fraudes pueden gestarse desde su programación. En algunos casos, las oportunidades de abuso surgen de forma no intencionada cuando existen errores en el código de contrato y quienes lo programaron son incapaces de identificarlos en la aplicación descentralizada (WEF, 2021a). En otros, las personas programadoras pueden diseñar contratos inteligentes abusivos aprovechando la elevada complejidad de estos productos y la falta de conocimientos digitales y financieros de sus posibles víctimas.

Algunos *exchanges* han sido utilizados para defraudar a sus usuarios, algo que fue particularmente común en las primeras etapas de desarrollo del mercado. Aprovechándose del acceso a las claves privadas que resguardan, la irrevocabilidad de las operaciones y la seudonimidad de la población usuaria de criptoactivos, los *exchanges* fraudulentos pueden desaparecer con facilidad, llevándose consigo los recursos de sus clientes (Moore & Christin, 2013). A pesar de que muchas de estas plataformas ya son entidades autorizadas e incluso reguladas, con una estructura organizacional sólida, el hecho de que operan con recursos virtuales excluye a sus usuarios de las

protecciones que tienen los ahorros en entidades financieras. En muchos casos, los *exchanges* han establecido políticas de "seguros de depósito", comprometiéndose a devolver la totalidad o una parte de los recursos en caso de un robo o hackeo, aunque lo hacen de forma voluntaria, ya que no hay regulación en la materia en la mayoría de las jurisdicciones.

La generación de nuevos criptoactivos también puede presentar riesgos importantes para los usuarios. Las ICOs se han caracterizado por la alta discrecionalidad en su creación y manejo. Generalmente, las nuevas "criptomonedas" o tokens se presentan a través de un *white paper*, un documento que describe las características del activo lanzado, similar en naturaleza a un prospecto de inversión de una emisora en bolsa. Considerando que son lanzados de forma independiente, los *white papers*, en la mayoría de los casos, carecen de exactitud, transparencia o claridad. Incluso, pueden ser muy complejos técnica o tecnológicamente para ser entendidos por la mayoría de los usuarios (Bains et al. 2022a).

La falta de regulación en estos documentos posibilita que sean utilizados como una herramienta mercadológica, permitiéndose exagerar las bondades o beneficios del producto sin sustento. Esto hace de las ICOs campo fértil para operaciones fraudulentas como los *wash trades*, una forma de manipulación de mercado donde un inversionista compra y vende simultáneamente un mismo activo para inflar su volumen de operación. Una ICO fraudulenta podría inflar la cotización de su propio activo artificialmente a través de *wash trades*, para después vender sus propias posiciones en masa cuando su cotización en mercado es alta, lo que se conoce comúnmente como un *whale trade*, eliminando en instantes el valor de mercado del activo y dejando a usuarios que lo adoptaron con pérdidas significativas. En conjunto, la posible falta de conocimiento de algunos de sus participantes, la falta de protecciones a los inversionistas y la irrevocabilidad de las operaciones en las plataformas pueden llevar a una crisis de confianza especialmente si el uso de estos activos se expande rápidamente al público usuario (FSB, 2022).

Ciberseguridad

Al operar a través de plataformas digitales, los riesgos más comunes para asegurar la operación adecuada de los criptoactivos son de ciberseguridad. Los mecanismos de consenso utilizados han probado ser resilientes ante posibles ataques cibernéticos. Incluso si los protocolos pudieran ser violados, el impacto monetario podría ser limitado.[33] Esto ha hecho que los criminales

[33] Incluso la posibilidad de una vulneración de gran escala como sería un ataque del 51% podría tener impactos limitados. Un ataque de este tipo reemplaza bloques recientes de la blockchain permitiendo al agregar sustituir transacciones en el muy corto plazo, absorber las ganancias de minería y realizar gastos dobles. No obstante, estos ataques no permiten crear nuevas transacciones que gasten las "criptomonedas" de otros participantes (Budish, 2018). Una mayor explicación de estos ataques se discute en la sección de riesgos de centralización.

no concentren sus esfuerzos en romper el mecanismo de consenso de las redes, sino en encontrar vulnerabilidades que les permitan abusar de errores de programación u omisiones de seguridad de la clientela y *exchanges* para acceder a sus recursos.

La sofisticación tecnológica de estos productos puede llevar a abusos, especialmente en el caso de los contratos inteligentes, cuya automatización e irreversibilidad los hace campo abierto para comportamientos no éticos. Tal vez el ejemplo más representativo de esa clase de problemas sea el hackeo de La DAO en la plataforma *Ethereum* en 2016 (Lewis, 2018).[34] Esta fue un proyecto privado diseñado para financiar *startups* utilizando "criptomonedas" a través de contratos inteligentes en *Ethereum*. La idea era que los inversionistas transfirieran *ether* al contrato inteligente del proyecto, por los qué recibirían, de forma automatizada, tokens DAO en su lugar. Estos tokens podían ser utilizados como votos para decidir qué startups recibirían financiamiento y, al final del proceso, el más votado recibiría una transferencia de criptoactivos.

En su primer mes activo, La DAO había captado alrededor del 15% del total de *ethers* en circulación. Desafortunadamente, poco después de alcanzar este logro, un hacker encontró un error en el código del contrato inteligente que le permitió transferir alrededor de un tercio de los fondos del proyecto a una de sus cuentas. El descubrimiento del hackeo envió el precio del *ether* en caída libre, perdiendo casi 50% de su valor.

El problema de La DAO requirió de una respuesta dentro de la propia plataforma. Debe recordarse que aún ahora no existe forma inmediata y efectiva de lidiar con transacciones realizadas por error, fraudes, extorsiones o robos de forma interna en cripto-redes. Tampoco existe una caracterización legal del protocolo que registra y afecta operaciones con criptomonedas, por lo que no necesariamente existen mecanismos legales para atender de forma inmediata un crimen en la red. Además, deben considerarse las dificultades de regular espacios sin jurisdicción evidente como lo es el ciberespacio. Estas condiciones reducen en gran medida la capacidad de las autoridades para atender esta clase de situaciones.

En casos como éste, la única solución factible ha sido recurrir a la coordinación social de los usuarios de la red de criptoactivos (Auer, 2019a). En el caso de La DAO, regresar los recursos a sus clientes requirió bifurcar la red *Ethereum*, lo que se llama comúnmente un *fork*. Este proceso consiste en crear una nueva versión de una "criptomoneda" copiando la *blockchain* de la

[34] "La DAO" no debe confundirse con el resto de las organizaciones descentralizadas autónomas, también abreviadas como DAOs, las cuales son estructuras comunes en las finanzas descentralizadas. "La DAO" era en si un ejemplo de una DAO, ya que se esperaba que funcionara de forma autónoma.

anterior hasta un bloque específico. Un *fork* no elimina la *blockchain* anterior: para ser efectivo requiere que los usuarios de la criptomoneda original acepten el cambio y comiencen a operar en la nueva versión como la legítima.

En julio de 2016, de forma coordinada, un grupo importante de usuarios de *Ethereum* bifurcaron la red a un bloque previo al hackeo, lo que regresó retroactivamente los recursos perdidos a sus dueños originales. La nueva red conservó el nombre *Ethereum* y fue adoptada como la red principal (Lewis, 2018; Mehta et al., 2021). No obstante, la red con la *blockchain* inalterada, y que por tanto incluye el hackeo de La DAO, se ha mantenido en operación regular bajo el nombre de *Ethereum Classic*. Es interesante observar que todos los usuarios de *Ethereum* previo al *fork* mantienen recursos en ambas redes. En forma muy básica, la bifurcación duplicó los *ethers* de todos los participantes de la red original, aunque en redes incompatibles entre sí y con un valor reducido debido a la pérdida de confianza, al menos en el mediano plazo.

Adicional a las propias redes y contratos inteligentes, uno de los puntos históricamente más débiles en materia de ciberseguridad en el mercado de criptoactivos han sido los *exchanges*. Como se mencionó anteriormente, las plataformas de intercambio mantienen generalmente en resguardo claves privadas de sus clientes, tanto directa como indirectamente, así como las propias que utilizan para realizar operaciones rápidas. Si la ciberseguridad de la plataforma de intercambio es inadecuada, es posible para un cibercriminal acceder a éstas y hacerse de los recursos de la plataforma con nula oposición.

El caso más representativo de un hackeo a un *exchange* es Mt. Gox, en su momento el mayor *exchange* de criptoactivos en el mundo (Mehta, et al., 2021). Esta plataforma de intercambio había logrado acumular el 70% de los intercambios con *bitcoins* a nivel global en 2013. A pesar de su tamaño, Mt. Gox tenía prácticas inadecuadas de ciberseguridad como el hecho de guardar las claves privadas de sus clientes sin alguna clase de encriptación en un servidor compartido. Esto permitió que un agente criminal tuviera acceso a las claves sin que Mt. Gox se percatara desde 2011. Entre este año y 2014, el criminal fue vaciando de forma discreta las cuentas del *exchange*. El manejo deficiente de la plataforma, tanto en el ámbito financiero como en materia de ciberseguridad, lo llevó a su quiebra. Para febrero de 2014, Mt. Gox se declaró en bancarrota y anunció que había perdido alrededor de 750 mil *bitcoins* de su clientela y alrededor de 100 mil *bitcoins* propios (Lewis, 2018).

Si bien este hackeo tuvo un impacto severo en el mercado *bitcoin*, con una caída de más de 20% al momento del anuncio de Mt. Gox, el mercado se mantuvo operando incluso cuando la clientela defraudada no había podido recuperar sus recursos satisfactoriamente. Parte de esta "recuperación rápida" parece haberse debido a que el tamaño del mercado era muy reducido en 2014, por lo que la población afectada fue poca. Al momento de

la redacción, los mayores *exchanges* en operación superan por mucho el tamaño de Mt. Gox, por lo que una afectación similar tendría un impacto mucho mayor en el mercado, además de que el golpe a la confianza en una entidad en el sector podría contagiarse a otras entidades del ecosistema.

Riesgos de lavado de dinero, financiamiento al terrorismo y evasión de sanciones

Desde la aparición del *bitcoin*, las autoridades se han preocupado por la naturaleza seudónima de los criptoactivos. La facilidad con la cuál es posible realizar transacciones con ellos sin tener un medio de identificación directa en las plataformas par-a-par los hace un factor de riesgo, ya que podrían ser utilizadas para financiar actividades ilícitas o mover recursos generados en estas. En la medida en que estos activos se integren a los mercados financieros tradicionales, mayor será el riesgo que podrían presentar para la integridad de los recursos relacionados.

La naturaleza seudónima de los clientes en redes como *Bitcoin* y *Ethereum* hace que, en condiciones normales, no se cuente con medios para realizar una identificación directa del propietario de cada dirección en las redes de "criptomonedas". No obstante, las características del *blockchain* permiten que cualquier persona pueda acceder a la historia completa de transacciones realizadas. Esto permite rastrear cualquier movimiento realizado en cualquier momento de la historia: no existe operación, sin importar su origen, que no quede registrada para la posteridad en las redes cripto. No es gratuito que el BIS haya propuesto utilizar supervisión incorporada del mercado cripto (*embedded supervision*), es decir, un marco que permita vigilar el cumplimiento regulatorio a través de monitoreo y verificación por medio de la *blockchain* u otro tipo de registro distribuido de la propia "criptomoneda" (Auer, 2019b).

Esta transparencia ha llevado a que los cibercriminales utilicen diversos medios para intentar dificultar el rastreo de sus operaciones por parte de las autoridades. El método más sencillo es a través de la pulverización de sus posiciones de criptoactivos, lo que se puede lograr depositando los recursos en múltiples direcciones ligadas a diferentes cuentas privadas, pero propiedad del mismo grupo criminal. Un método más sofisticado es a través del uso de los servicios de mezcladores o *tumblers* digitales. Estos servicios, ofrecidos de forma informal y muchas veces *over-the-counter*, consisten en depositar criptoactivos de diversas direcciones, que pueden provenir de actividades legales o ilegales, y concentrarlas en una única bolsa (dirección), la cuál es posteriormente depositada en direcciones nuevas generadas con claves privadas también nuevas, lo que dificulta identificar a los dueños originales. Otros criminales han transitado hacía el uso de criptoactivos "confidenciales", los que, aunque se registran en una *blockchain* como el

bitcoin o los *ethers*, no permiten identificar las direcciones y montos de las transacciones.

Actualmente no existen estimaciones ampliamente aceptadas del tamaño de las transacciones ilegales con activos virtuales, debido a la dificultad de identificar la naturaleza de los clientes y operaciones en redes seudónimas. Algunas estimaciones consideran que alrededor del 46% de las operaciones con *bitcoin* estaban relacionadas con actividades ilegales (Foley et al., 2019), aunque cálculos más detallados lo ubican en alrededor del 3% del volumen total real (Makarov & Schoar, 2021).[35] El *Crypto Crime Report* de Chainalysis (2021) estima que, en 2020, sólo el 0.34% del volumen total de operaciones con criptoactivos pueden ligarse con este tipo de actividades, lo que representaría alrededor de 10 mil millones de dólares.

Aunque el volumen de criptoactivos relacionados con actividades ilegales no es despreciable, existen condiciones de mercado que podrían estar limitando su adopción mayor por parte de criminales. Es importante tener en cuenta la limitada adopción de los pagos con criptoactivos en la mayor parte del mundo, lo que dificulta su uso directo en operaciones de compraventa en establecimientos formales. Además, aún entre aquellos que los aceptan, existen pocos que permitan realizar compras de bienes físicos con estos sin protocolos de identificación previa, particularmente cuando los montos involucrados son elevados. Para poder obtener ganancias de actividades ilegales a través de activos virtuales, es muy probable que los criminales requieran convertirlos en moneda fiduciaria.

Es en este punto que los *exchanges* juegan un papel relevante en la lucha contra el lavado de dinero a través de criptoactivos. En la mayoría de las jurisdicciones, las plataformas de intercambio que operan con moneda fiduciaria están obligados a cumplir con protocolos de identificación de clientes. Considerando que las cuentas de los *exchanges* legítimos son públicas e identificables para la mayoría de las autoridades y los recursos relacionados con operaciones ilegales pueden ser rastreados en la *blockchain*, existe una clara oportunidad de identificar a los criminales una vez que intentan convertir criptoactivos en moneda fiduciaria.

Esta capacidad de rastrear e identificar operaciones en las redes han permitido combatir la proliferación de mercados negros operados con criptoactivos. Estos mercados se han reportado desde el surgimiento de las redes de criptoactivos y continúan apareciendo primordialmente en la *dark*

[35] Esta discrepancia pueden ser resultado de que los criminales realizan un número mucho más elevado de operaciones que los usuarios legales, en un intento de dificultar su rastreo. Esto genera que el volumen real de operaciones sea mucho menor, ya que la mayoría de los movimientos son entre direcciones asociadas al mismo grupo criminal.

web.[36] Un caso emblemático es el Silk Road, un mercado negro virtual en Estados Unidos que se dedicaba a la venta de contrabando, particularmente de drogas y pasaportes falsos. Durante su período de actividad entre 2011 y 2013, Silk Road movilizó un estimado de 1.2 mil millones de dólares en contrabando (Mehta, etal., 2021). Los clientes utilizaban como medio de pago el *bitcoin*, suponiendo que podría ser un medio para evitar el rastreo de las autoridades. Cuando las autoridades arrestaron a su fundador se hicieron de las claves privadas ligadas a sus posiciones de *bitcoin* y pudieron ligar sus operaciones a las cuentas del Silk Road utilizando la *blockchain*.

Aunque este caso refleja las posibilidades que existen de usar las cualidades de transparencia de los registros *bitcoin* para rastrear actividades criminales, la realidad es que los cibercriminales se han vuelto mucho más sofisticados en los últimos años. Los cibercriminales que utilizan ataques de *ransomware*[37] para obtener criptoactivos en extorsiones han abandonado el uso de criptoactivos más comunes por los "confidenciales" como Monero, una tendencia que se ha observado en los últimos años (CipherTrace, 2021). Por supuesto, la existencia de *exchanges* ilegítimos y/o netamente digitales dificultan el actuar de las autoridades para frenar este tipo de operaciones. Además, siempre existe el riesgo de las operaciones *over-the-counter*, donde un criminal puede pagar con criptoactivos mercancía o servicios ilegales y después utilizar prestanombres o negocios fantasma para convertirlos en moneda fiduciaria.

Finalmente, no debe olvidarse la facilidad que existe para operar criptoactivos de forma transnacional, particularmente a través de plataformas de intercambio par-a-par, lo que los hace factores de riesgo multijurisdiccional. Considerando que diferentes países están aplicando marcos diferentes, es factible que los operadores de criptomonedas realicen arbitraje regulatorio, ubicándose legalmente en países con marcos más laxos sin restringir sus operaciones en países más estrictos aprovechando las ventajas tecnológicas. Existe el riesgo incluso de que la naturaleza seudónima de las "criptomonedas" permita que sean utilizadas para evadir sanciones a nivel internacional. Por ejemplo, el gobierno de Estados Unidos ha mostrado preocupación de que Rusia podría utilizar activos virtuales como un medio para evitar las sanciones internacionales después del inicio de su conflicto con

[36] La *dark web* es el conjunto de sitios ocultos de internet a los cuales sólo se puede acceder a través de software de navegación especializados. Esto permite mantener su actividad privada y anónima, lo que permite a criminales realizar operaciones ilegales con menor riesgo de ser identificados por autoridades.

[37] Un ataque de *ransomware* consiste en infectar una computadora con un programa malicioso para encriptar su contenido, haciendo que la información en ella sea inaccesible para sus usuarios legítimos. El cibercriminal exige el pago de una extorsión para desbloquear la información y/o amenaza con la destrucción o la difusión de esta en caso de no hacerlo. Véase https://www.kaspersky.com/resource-center/threats/ransomware.

Ucrania.[38] Un estudio reciente (Makhlouf & Selmi, 2022) sugiere que la población rusa se ha vuelto más activa en el uso de criptoactivos desde del inicio del conflicto, aunque el mercado podría no ser lo suficientemente líquido para permitir que los activos virtuales sean usados como medio de evasión de sanciones.

Centralización de las redes

En adición de los riesgos antes mencionados, los protocolos bajo los cuales operan las redes de criptoactivos pueden traer algunos riesgos que pueden considerarse no intencionados. El mecanismo de consenso para la creación de bloques en la red *Bitcoin*, la prueba de trabajo (PoW), genera costos elevados de validación. Recordemos que el protocolo requiere que el minero resuelva un problema matemático cuya solución práctica solo puede hallarse a través de millones de iteraciones con números aleatorios. El esquema se diseñó con el objetivo de evitar que un individuo o grupo de individuos fueran capaces de abusar la red y realizar pagos dobles, ya que para tener posibilidad de hacerlo deberían controlar al menos más del 50% de la capacidad computacional de la red, lo que comúnmente se ha llamado un ataque del 51%.[39]

Aunque el mecanismo se había creado originalmente para permitir que cualquier individuo pudiera participar en la creación de bloques, la situación actual dista mucho del "ideal democrático" planteado por Satoshi Nakamoto. La capacidad de generar un bloque y obtener una ganancia de este depende tanto del número de computadoras a disposición del minero como de la capacidad operativa de cada equipo, lo que en conjunto suele llamarse *hashrate*.

La búsqueda de los mineros de obtener las mayores ganancias posibles ha llevado al establecimiento de estrategias para maximizar la *hashrate* a través de dos mecanismos que surgieron naturalmente del mercado. Por un lado, la PoW ha impulsado la creación de *pools* de mineros, es decir, organizaciones que conjuntan una enorme cantidad de equipos de cómputo con el objetivo de incrementar su probabilidad de crear el mayor número de bloques y, con ello, obtener las mayores ganancias posibles (figura 7A). Se estima que alrededor de 15 *pools* controlan más de 95% de capacidad de minería de la red, y el top 4 controla habitualmente más del 50% de la capacidad total (Mehta et al., 2021, pp. 98-99; Baines, 2022).

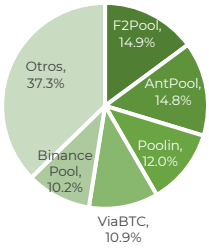
[38] Véase https://www.whitecase.com/insight-alert/us-regulators-seek-prevent-use-crypto-circumvent-russia-sanctions.

[39] Aunque éste es el término común utilizado para referirse a esta clase de ataques, la definición más correcta sería un ataque de "50%+1", ya que sólo se necesita un nodo más allá del 50% para que fuera factible.

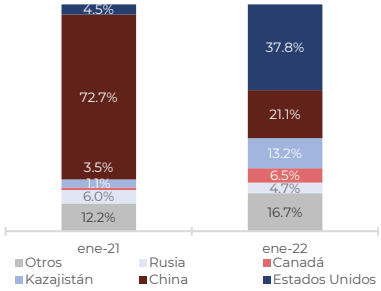
Por otro lado, algunas empresas de cómputo se han especializado en el diseño de equipos construidos específicamente para la minería. Para ser competitivo en la red *Bitcoin*, los equipos requieren de chips ASIC (*Application Specific Integrated Circuits*), que son muy eficientes en realizar procesos iterativos (Budish, 2018). Los *pools* de mineros generalmente ocupan cientos de estos equipos, cuyos costos de adquisición son muy elevados y su consumo de energía es igualmente alto.

Figura 7. Concentración de la actividad de minería en la red *Bitcoin*

A. Distribución del *hashrate* en *pools* de mineros
(Porcentaje del *hashrate* estimado total)



B. Distribución geográfica del *hashrate*
(Porcentaje del *hashrate* estimado total)



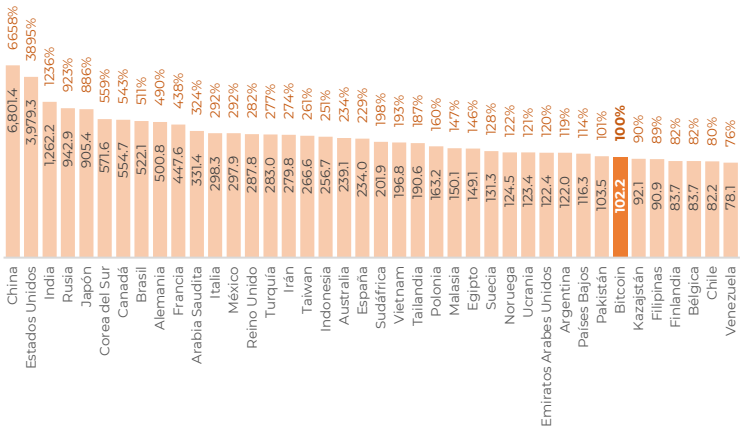
Fuente: Panel A proviene de Baines (2022) con información de BTC.com de enero de 2020 a enero de 2021. Panel B: Elaboración propia con datos de CCAF. Los datos se estiman con una muestra recolectada con varios *pools* de minería.

En la situación actual, es casi imposible que un minero solitario sea capaz de obtener un beneficio de participar en la minería. En su lugar, con el crecimiento de la concentración de las operaciones en los *pools*, existe la posibilidad real de que el protocolo de prueba de trabajo pueda ser capturado por un conglomerado de grandes empresas, particularmente aquellas que producen equipos de cómputo para minería y manejen *pools* de mineros de forma simultánea (Ferreira et al., 2019). Esto pondría en tela de juicio la independencia de la red y la haría susceptible a los ataques de 51%. Además, existe el riesgo de concentración geográfica de los *pools*, lo que los podría hacer vulnerables a presiones políticas o sabotajes concentrados (figura 7B). De acuerdo con cifras del *Cambridge Centre for Alternative Finance* (CCAF), en enero de 2021 alrededor del 72% de la *hashrate* estaba ubicada en China. No obstante, después de la prohibición de las actividades de minería de criptoactivos por parte de su gobierno, su participación se redujo a menos del 40% un año después.

Otro factor que podría estar limitando la viabilidad de la red *Bitcoin* en el mediano plazo es su dependencia en las ganancias generadas por protocolo sobre las cuotas de transferencia. La reducción de la recompensa

cada cuatro años se había diseñado como un mecanismo para transitar hacía una economía asentada en las cuotas y al mismo tiempo mantener una oferta de monedas controlada. Se ha argumentado que el protocolo actual no puede generar tarifas de transacción alineadas con la garantía de generar pagos seguros (Auer, 2019a). Existe el riesgo real de que la reducción de las ganancias lleve a un abandono generalizado de la actividad minera al volverse significativamente menos rentable. Este abandono de la red cuando el valor del *bitcoin* cae o cuando las ganancias de minería son cortadas a la mitad por protocolo se ha reflejado en un incremento en el riesgo de ataques cibernéticos, al reducir el número de nodos verificadores de la red (Makarov & Schoar, 2021).

Figura 8: Costo eléctrico anual promedio de la red *Bitcoin*



Fuente: *Cambridge Centre for Alternative Finance. Cambridge Bitcoin Electricity Consumption Index*. Los datos se presentan en escala logarítmica por fines de presentación.

Adicionalmente, el costo energético de la prueba de trabajo hace de la actividad minera de criptoactivos un factor de riesgo climático relevante. De acuerdo con estimaciones del *Cambridge Centre for Alternative Finance* (CCAF), el costo eléctrico del protocolo *Bitcoin* se ubica en alrededor de 102 TW/hora al año, a la par del gasto eléctrico anual de economías completas de tamaño medio como Filipinas o Pakistán. Este costo fue una de las razones que llevó a *Ethereum* a plantearse un cambio hacia un mecanismo de consenso basado en la prueba de participación. De acuerdo con estimaciones de la propia red, la transición de la prueba de trabajo a la de participación

implicó una reducción en el costo eléctrico de la red en 99.95%, lo que representó un cambio significativo en materia de impacto climático.[40]

A pesar de esto, la prueba de participación (PoS) no está alejada de problemas de centralización. Si bien la prueba de trabajo es relativamente costosa, ésta ha probado su efectividad considerando que, al momento, la red *Bitcoin* no ha sufrido de un ataque directo exitoso. La PoS requiere por diseño menos recursos para su operación, pero debe tenerse en cuenta que no ha sido probada en una red tan extensa. En particular, se ha argumentado que no existe una forma clara de seleccionar bloques validados de forma simultánea bajo este mecanismo (Auer, 2019a), lo que podría llevar a problemas de consenso y hacer a las redes más vulnerables a ataques cibernéticos.

De la misma forma que en la PoW, un validador solitario podría tener poca posibilidad de beneficiarse de participar en el esquema. La PoS podría ser tan antidemocrática como la PoW: el mismo mecanismo puede llevar fácilmente a la concentración del proceso de validación en pocos participantes, ya que la mayor posesión de criptoactivo se relaciona directamente con la probabilidad de ser seleccionado. El costo de registrarse como validador en la red *Ethereum* (32 *ethers*) podría ser muy elevado para inversionistas minoristas, lo que favorece la creación de *pools* que controlen múltiples cuentas de validador a través de ofrecer rendimientos en proporción con su participación en los recursos de reserva para la cuenta (*pool staking*). De hecho, la aparición en el mercado de *ethers* del *staking* y del *pool staking* no ha estado libre de escrutinio. Algunas autoridades han impulsado la discusión sobre si las criptomonedas que utilizan la PoS deberían ser consideradas valores, al requerir depósitos de la clientela bajo la promesa de un rendimiento en el futuro.[41]

La situación de los dos protocolos de validación más comunes en el ecosistema muestra que, lejos del ideal democrático de los primeros diseñadores de las redes, estos podrían estar fomentando la aparición de oligopolios. A pesar de los esfuerzos de los proponentes de los criptoactivos por enfatizar las diferencias de estos activos con respecto a los convencionales, la forma en que opera el ecosistema se asemeja cada vez más al mercado financiero tradicional, incluyendo su estructura de mercado concentrada.

En esta línea de pensamiento, la participación de los *exchanges* en los procesos de validación merecen una mención aparte. Actualmente, estas plataformas no sólo concentran la mayor parte de las transacciones con

[40] Véase https://blog.ethereum.org/2021/05/18/country-power-no-more.
[41] Véase, por ejemplo, https://www.bloomberg.com/news/articles/2023-03-15/sec-s-gary-gensler-signals-tokens-like-ether-are-securities.

criptoactivos, sino que han expandido sus operaciones hacía la minería de *bitcoins* y el *staking* para validar operaciones en *Ethereum*. Por dar un ejemplo, las actividades de minería de *Binance Pool*, el *pool* de mineros del mayor *exchange* de criptoactivos en el mundo, concentra alrededor del 10% de la *hashrate* estimada a nivel mundial. En el caso de la prueba de participación, la necesidad de mantener una reserva importante de criptoactivos en reserva para ser un validador puede llevar a que los *exchanges* con grandes posiciones en estos puedan beneficiarse desproporcionalmente al contar con los medios para generar múltiples cuentas y centralizar el proceso de validación (Bains, et al. 2022a). Estas situaciones podrían ocasionar que los *exchanges* concentren poder sobre los procesos de intercambio y validación de operaciones, convirtiéndolos en infraestructura crítica para la operación de todo el ecosistema.

III. Criptoactivos estables o *stablecoins*

Las llamadas *stablecoins* surgieron como respuesta al desafío más apremiante de los criptoactivos sin subyacente para su uso como medio de pago: la volatilidad. Al prometer paridad constante con otros activos, como monedas fiduciarias, pero permitiendo que sus transacciones se realicen de forma descentralizada, como el *bitcoin* o el *ether*, las *stablecoins* mantienen los beneficios de acceso y disponibilidad inmediata de los criptoactivos no estables, pero hipotéticamente sin los riesgos derivados de la volatilidad que reducen su utilidad como medio de pago.

Si bien no existe una definición globalmente aceptada, los llamados criptoactivos estables o *stablecoins* pueden definirse como activos digitales que buscan mantener un valor estable relativo a un activo tradicional o una canasta de estos. Al igual que los no estables, son registros electrónicos, pueden transferirse a través de plataformas par-a-par y no son emitidas por ninguna autoridad como un banco central (Auer et al., 2021). De acuerdo con algunos investigadores, para que una *stablecoin* represente un arreglo exitoso, se espera que cumpla con tres propiedades principales (Mell & Yagu, 2022):

1) Deben ser fungibles, es decir, las unidades de la *stablecoin* deben ser completamente idénticas e intercambiables.

2) Deben representar unidades con valor financiero dentro de la *blockchain*, y operar como depósito de valor y medio de cambio en la red donde se hayan generado.

3) Deben presentar mínima volatilidad con respecto al valor de su bien o canasta de bienes de soporte.

Las llamadas *stablecoins* no son necesariamente una propuesta nueva, algunas tienen paralelismos con productos financieros conocidos como los fondos mutuos de dinero (*money market mutual funds*) o los monederos electrónicos, ya que muchos de los diseños dependen de la inversión en activos altamente líquidos. Incluso, han sido comparados con la operación del Banco de Amsterdam en el siglo XVIII, que emitió depósitos respaldados en monedas de oro y plata, y liquidó pagos a través de transferencias entre estos (Frost et al., 2020). La principal diferencia radica en que, al contrario de los anteriores, las llamadas *stablecoins* pueden aprovecharse de las tecnologías DLT y de su compatibilidad con otros criptoactivos. Estas operan en redes abiertas y programables, la mayoría a través de la red *Ethereum*, lo que les permite funcionar como medios de liquidación para contratos inteligentes, y utilizarse como instrumentos de cobertura entre otros criptoactivos y monedas fiduciarias.

Funcionamiento y operación de los criptoactivos "estables"

Operación de las stablecoins

Al contrario que en el caso del *bitcoin* y el *ether*, las *stablecoins* no son las "criptomonedas" nativas de sus redes. En su lugar, son tokens secundarios generados a través de contratos inteligentes en redes programables como *Ethereum*, por lo que requieren generalmente de la "criptomoneda" nativa para ser operados. Al ser producto de contratos inteligentes, estos activos están registrados en las *blockchains* de estas redes, lo que les permite ser transferidos de forma completamente descentralizada (Bullmann et al., 2019) y son también susceptibles a ser comerciados a través de *exchanges* tradicionales o digitales.

Una vez la *stablecoin* ha sido emitida y registrada en la *blockchain* de la red, el usuario puede realizar transacciones con ella de forma completamente descentralizada, es decir, de forma idéntica a una transacción con *ethers* u otras "criptomonedas" no estables.[42] De hecho, al ser en su mayoría tokens secundarios de *Ethereum*, la operación con ellas debe cumplir el protocolo de la red, por lo que requiere de *ethers* para pagar por los costos de transacción.

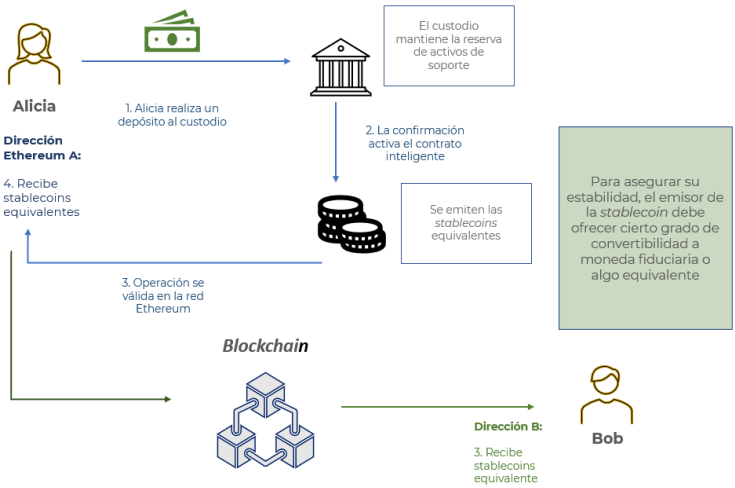
La diferencia radical entre las *stablecoins* y los criptoactivos no estables es su promesa de mantener un valor fijo en el tiempo. En la mayoría de los casos, se comprometen a mantener un valor uno-a-uno con alguna divisa, aunque algunas buscan replicar el comportamiento de canastas de activos o índices. Esta necesidad de mantener un valor objetivo es la causa de que, en muchos casos, requieran de un agente centralizado que las emita y controle. Uno de los factores más relevantes es que, al operar en redes abiertas y sin permisos, cualquier entidad privada puede diseñar y lanzar su propia

[42] Véase la sección II.

stablecoin, lo que abre la posibilidad de que cualquiera pueda ofrecer "servicios financieros alternativos" de forma virtual.

Para lograr que una *stablecoin* mantenga su valor en el tiempo, es necesario establecer un mecanismo de estabilización, el cual depende del tipo de activo subyacente y determina su proceso de creación y destrucción. Uno de los más comúnmente utilizados es la colateralización completa, el cual es usado por arreglos de stablecoins que buscan mantener su valor con moneda fiduciaria. La figura 9 esquematiza la operación de este tipo de arreglos. Para obtener una stablecoin bajo este esquema, el usuario inicia una transferencia de fondos en moneda fiduciaria a una cuenta del emisor bajo control de un custodio. Una vez que el custodio confirma la recepción del depósito, el emisor cobra una comisión y procede a "acuñar" la cantidad equivalente de criptoactivos estables a través de un contrato inteligente en alguna red programable.

Figura 9: Operación de un fondo tokenizado



Fuente: Elaboración propia

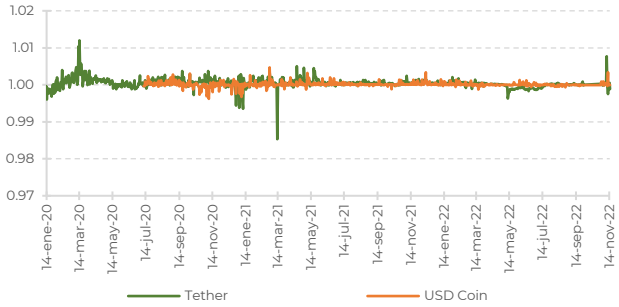
Para asegurar que la *stablecoin* mantenga el valor en el tiempo, el emisor mantiene una reserva de la moneda fiduciaria y promete algún grado de convertibilidad de la *stablecoin* a esta última, lo que podríamos llamar un derecho de canje. Este tipo de arreglos son comúnmente conocidas como fondos tokenizados, ya que representan en sí una reclamación sobre un depósito en moneda fiduciaria que puede ser redimida, en teoría, en cualquier momento (Bullmann et al., 2019). Por tanto, en la colateralización completa, la

estabilidad del precio depende de la transferibilidad entre el criptoactivo estable y sus colaterales (Pernice et al., 2019).

El derecho de canje varía de arreglo a arreglo, incluso entre fondos tokenizados con colateralización completa. La mayoría de las emisoras ofrecen convertir las *stablecoins* en moneda fiduciaria al recibirlas de vuelta en el contrato inteligente, aunque con restricciones de monto mínimo, tiempo de respuesta y/o horarios de atención que dependen del agente central que las controla. En otros casos, los *exchanges* pueden ser los agentes controladores o mantener acuerdos de operación con alguna emisora de éstas. En estos casos, los *exchanges* se compromete a cumplir con el derecho de canje, aunque en su mayoría ejerciendo también ciertas restricciones. Considerando que operan en redes descentralizadas, algunos arreglos cumplen el derecho de canje a través del envío del valor equivalente de ésta en la "criptomoneda" nativa de la red, eliminando la *stablecoin* de circulación de forma automatizada y retirando de la reserva la moneda fiduciaria a través del custodio.

Los fondos tokenizados requieren necesariamente de una entidad central que controle las reservas que soportan al criptoactivo "estable" fuera de la red, lo que comúnmente se conoce como un arreglo de custodia centralizado o CeFi. Esto permite que el agente sea capaz de cumplir con el derecho de canje que mantiene la estabilidad del criptoactivo. En general, las emisoras de *stablecoins* son entidades privadas no financieras, por lo que no están autorizadas para mantener depósitos de su clientela en moneda fiduciaria. Por tanto, la emisora opera como custodio a través de cuentas a su nombre en alguna institución financiera. Las reservas son generalmente invertidas en los mercados financieros tradicionales, pero considerando la promesa de convertibilidad, requieren mantener una liquidez elevada.

Figura 10: Evolución de las cotizaciones de *Tether* y USDCoin

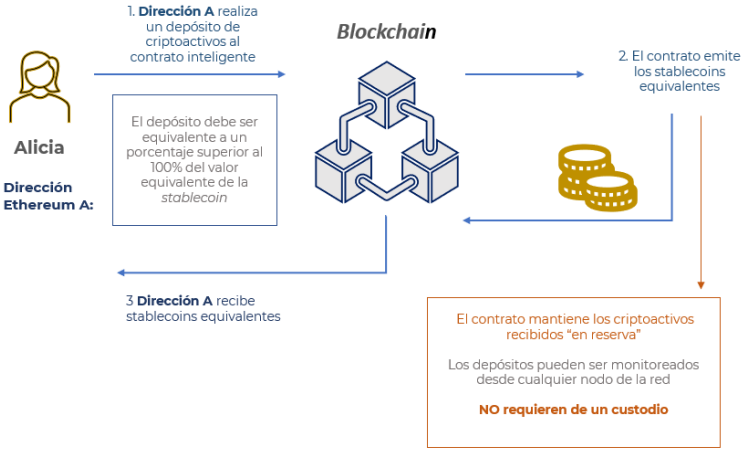


Fuente: Elaboración propia

Las principales *stablecoins* en circulación, como son los casos de *Tether* y USDCoin, son colateralizadas. Ambas han establecido una meta de valor uno a uno con el dólar, y son clasificadas comúnmente como fondos tokenizados. En general, aunque presenta cierto grado de volatilidad, *Tether* ha sido exitoso en mantener su paridad con el dólar, mostrando variaciones máximas que no superan los dos centavos con respecto a su valor objetivo. USDCoin incluso ha mostrado aún menor volatilidad (figura 10).

Algunas *stablecoins* están soportadas por una canasta de activos virtuales, y no necesariamente en el activo sobre el que se fija el precio. Por ejemplo, es posible tener una *stablecoin* que prometa un valor 1 a 1 con el dólar, pero cuyas reservas estén conformadas por *ethers*. Este tipo de criptoactivos requieren de arreglos diferentes de estabilización ya que los activos subyacentes son en sí mismos vulnerables a cambios en valuación, algo que no ocurre con las soportadas puramente en moneda fiduciaria. El esquema más común es la sobrecolateralización, es decir, se requiere un depósito de activos con un valor superior al establecido de la *stablecoin*. Este tipo de arreglos son especialmente comunes en aquellas soportadas en criptoactivos no estables y son la base primordial de los esquemas de finanzas que buscan ser totalmente descentralizados (Aramonte et al., 2022).

Figura 11: Operación de una *stablecoin* soportada en criptoactivos



Fuente: Elaboración propia.

Un diagrama de cómo opera este tipo de *stablecoins* se presenta en la figura 11. En estos esquemas, un usuario puede obtener una a través de realizar un depósito de estos a un contrato inteligente. El monto necesario por

depositar, siempre superior al 100% del valor de la *stablecoin* por unidad, está definido en el contrato. De forma automática, el cliente recibe *stablecoins* equivalentes al monto enviado menos comisiones, lo que hace que el proceso de emisión sea similar a un préstamo con garantía (Mell & Yaga, 2022). Al contar únicamente con reservas en activos virtuales, todas las operaciones con ellas son visibles y verificables en la *blockchain* de la red programable, lo que ofrece transparencia sobre su estado. Cuando la cotización de la reserva depositada cae por debajo de un límite, superior al 100% pero menor al requerido para su emisión, el contrato inteligente liquida de forma inmediata la posición de reserva, lo que le permite mantener el valor prometido.

Existen otros mecanismos de estabilización que no requieren necesariamente de un agente central o de algún grado de colateralización (Pernice et al., 2019). Algunos criptoactivos estables presentan un mecanismo automático de ajuste, programado en el contrato inteligente que la emite, con la intención de que éste realice los movimientos necesarios para evitar la volatilidad sin intervención de un emisor. Estas *stablecoins*, conocidas comúnmente como algorítmicas, tienen la ventaja de responder de forma inmediata a cambios en factores observables que afectan la valuación del criptoactivo, aunque la efectividad depende de que el programador haya sido capaz de considerar todos los factores relevantes para evitar una fluctuación.

Uno de los esquemas más comunes de estabilización en *stablecoins* algorítmicas es el señoreaje. En éste, el contrato inteligente utiliza un criptoactivo complementario como mecanismo de estabilización, el cual se genera sin la necesidad de un colateral y cuya oferta manipula con el objetivo de mantener el valor de la *stablecoin* (Mell & Yang, 2022). El contrato inteligente está programado para emitir estos activos complementarios o destruirlos periódicamente en línea con cambios en la oferta y demanda de la *stablecoin*. Otro método de estabilización común es el rebase (*rebasing*). En este método, el contrato inteligente ajusta regularmente la oferta total de la *stablecoin* en respuesta a cambios en el precio. En términos simples, crea más "monedas" cuando el precio está por arriba de su objetivo, y las destruye en caso contrario. Una particularidad de este método es que las *stablecoins* son agregadas o eliminadas directamente de las cuentas de los usuarios.

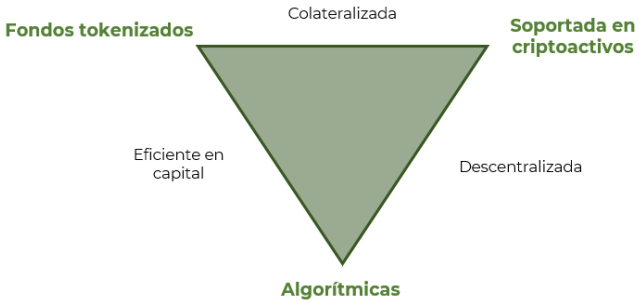
En resumen, la operación de una *stablecoin* puede presentar algunas características particulares de acuerdo con el tipo de activo o mecanismo de soporte que posea (figura 12). Los arreglos de *stablecoins* pueden ser:

1) colateralizados, es decir, mantener una reserva de activos de soporte, sean tradicionales o virtuales,

2) eficientes en capital, es decir, requerir en reservas sólo la cantidad mínima que permite mantener su valor (no están sobrecolateralizados), o

3) descentralizados, es decir, son independientes de un emisor centralizado que controle el mecanismo de estabilización fuera de la red.

Figura 12: Taxonomía de *stablecoins* basadas en tipo de activo de soporte



Fuente: Elaboración propia.

En general, ninguno de los tres tipos discutidos es capaz de ofrecer las tres características al mismo tiempo, aunque existen arreglos híbridos que dicen hacerlo, aunque con mayores dudas sobre su funcionamiento y seguridad.

Protocolos de finanzas descentralizadas

La llegada de las redes de criptoactivos, particularmente aquellas con capacidad programable como *Ethereum*, ha dado pasó a la aparición de "servicios financieros alternativos" que pueden realizarse sin la necesidad de recurrir a la estructura tradicional del sistema financiero. El concepto de finanzas descentralizadas o DeFi puede definirse como la capacidad de proveer servicios financieros sin intermediarios centralizados, operando a través de protocolos automatizados en redes descentralizadas programables (Aramonte et al., 2021).

Los protocolos DeFi están sustentados en dos desarrollos principales. Por un lado, los contratos inteligentes, los cuales permiten el intercambio, inversión y préstamo de criptoactivos sin la necesidad de un agente central que ejecute la orden. En segundo lugar, la aparición de las *stablecoins*, tanto las soportadas en activos tradicionales como en activos virtuales ofrecieron cobertura y liquidez a los protocolos y han funcionado como el vínculo

principal entre los criptoactivos estables y los no estables. Los protocolos DeFi tiene tres características definitorias (OCDE, 2022):

1) Naturaleza no custodial, ya que los recursos son autogestionados y son generalmente visibles para todos a través de los registros de las redes donde operan.

2) Se manejan de forma comunitaria. Generalmente los participantes pueden recibir tokens de gobernanza, que les permiten tener voz y voto sobre los cambios que pueden realizarse sobre el protocolo.

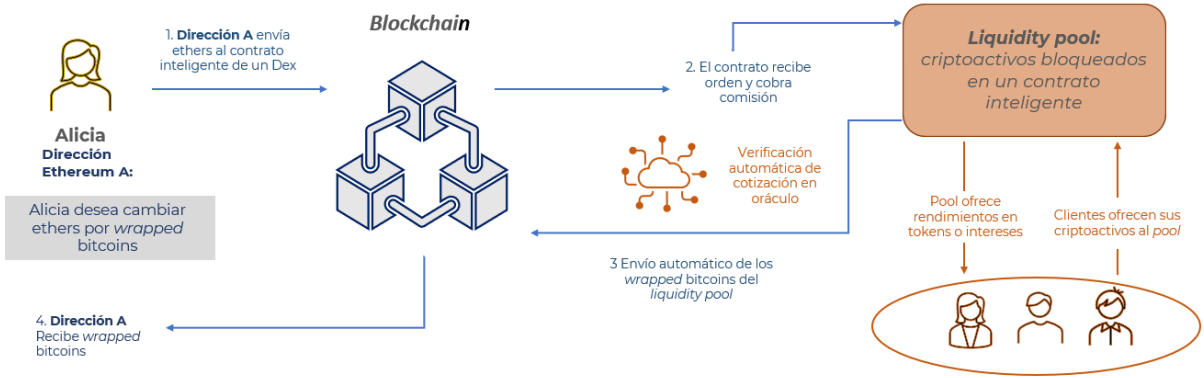
3) *Componibilidad*, ya que los componentes DeFi diseñados en una red programable pueden juntarse para crear nuevos productos.

Los servicios DeFi más comunes incluyen a los *exchanges* descentralizados, es decir, aquellos que permiten el intercambio de algún activo virtual por otro sin la necesidad de que un agente opere como cámara de compensación. Al estar enfocados en el intercambio de activos virtuales, los *exchanges* descentralizados o Dex generalmente carecen de los controles en materia de PLD/FT que deben implementar las plataformas de intercambio físicas, ya que no incluyen operaciones con moneda fiduciaria.

La figura 13 muestra en forma simplificada la operación de un Dex. Para obtener la liquidez necesaria para responder a cualquier intercambio, los *exchanges* descentralizados requieren de los llamados *liquidity pools*, es decir una cantidad de criptoactivos bloqueados en un contrato inteligente, los cuales provienen mayoritariamente de usuarios. Para esto, estos esquemas prometen incentivos a los depositantes, que pueden ser intereses, tokens de gobernanza u otros tokens intercambiables en *exchanges* centralizados o descentralizados. Esto permite que las operaciones se realicen de forma automática y expedita, sin la necesidad de que el agente central construya una reserva para realizar los intercambios.

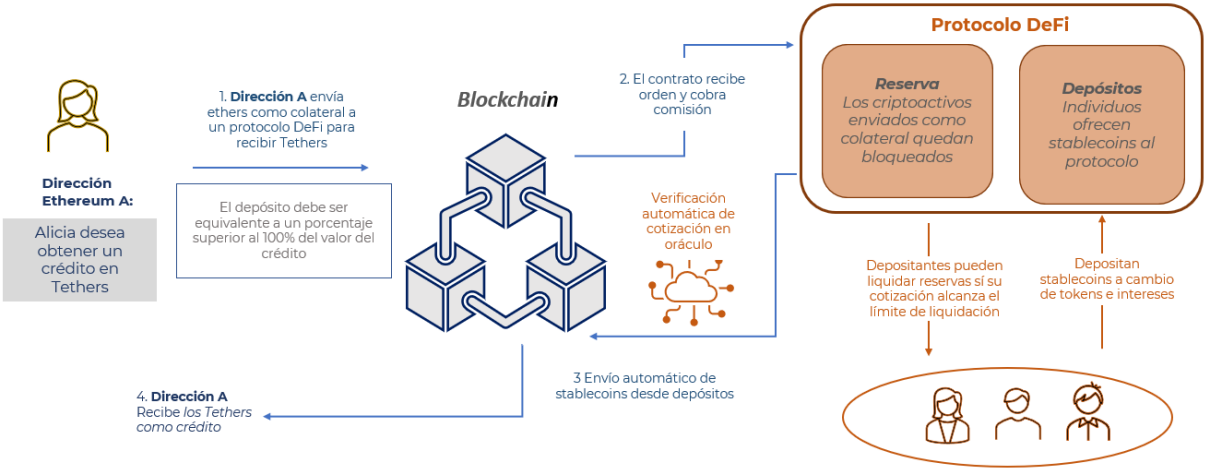
La persona encargada del diseño del contrato inteligente del Dex, y de casi cualquier otro protocolo DeFi, obtiene ganancias a través de cobrar comisiones programadas directamente en este. La mayoría de estos esquemas están gobernados por una DAO (Organización Autónoma Descentralizada, por sus siglas en inglés), que representa un conjunto de reglas definidas en código y por tanto es, en principio, transparente para todos los participantes. Para realizar cambios en el protocolo, la DAO está programado para permitir votaciones. Para su aprobación, un cambio requiere que la mayoría de los tokens de gobernanza, que no necesariamente representan usuarios únicos, vote a favor.

Figura 13: Operación de un *exchange* descentralizado (Dex)



Fuente: Elaboración propia.

Figura 14: Operación de una plataforma de crédito DeFi



Fuente: Elaboración propia.

Otros esquemas que han tomado mayor relevancia han sido las plataformas de crédito DeFi. Los criptoactivos relacionados con estos protocolos alcanzaron una cotización de alrededor de 50 mil millones de dólares en 2022, después de ser casi inexistentes a inicio de 2020 (Aramonte et al., 2022). Estos esquemas requieren de participantes externos para construir una reserva de activos virtuales, generalmente *stablecoins*. Con este fin, el contrato inteligente del protocolo DeFi ofrece rendimientos por los depósitos, ya sea en tokens de gobernanza, tokens comerciables o en intereses para tener una reserva. Los acreditados potenciales obtienen recursos de esta reserva, la cual no requiere de un agente que la gestione.

En estas plataformas, un acreditado puede obtener un préstamo a través de realizar un depósito en criptoactivos no estables al contrato del protocolo, por los cuales reciben una cantidad de *stablecoins* en préstamo. Cómo ejemplifica la figura 14, el protocolo opera de forma similar a los mecanismos de estabilización de las *stablecoins* soportadas en criptoactivos, ya que los créditos son siempre sobrecolateralizados para evitar posibles pérdidas por cambios en la valuación de los activos de soporte. Para asegurar que los participantes en las reservas no pierdan recursos, el esquema permite la liquidación del colateral cuando su valor se reduce por debajo de un umbral definido. Como tales, estos mecanismos ofrecen *stablecoins* que pueden ser utilizados en otros protocolos DeFi, lo que genera un efecto similar al multiplicador de crédito bancario. No obstante, al estar soportados en la sobrecolateralización por criptoactivos, son esquemas con poco impacto en materia de inclusión financiera: para ser sujeto de crédito, el usuario debe contar de inicio con recursos cuya valuación debe ser incluso mayor al valor de las *stablecoins* que va a adquirir. Además, sufren del problema de ser claramente procíclicos, ya que, en períodos de caída en la valuación de criptoactivos, estos protocolos caen en ciclos de liquidación constante de su colateral.

Los protocolos DeFi tienen dos ventajas importantes. En primer lugar, presentan costos de operación menores, ya que no requieren de un intermediario financiero. Además, al realizarse de forma automatizada a través de contratos inteligentes, presentan una mayor velocidad de ejecución. Es importante recalcar que al operar en redes programables con *blockchains*, existe transparencia sobre las posiciones y estado de las reservas y los fondos involucrados. A pesar de esto, los protocolos DeFi también presentan riesgos y desventajas importantes. Además de su impacto muy limitado en la inclusión financiera, la utilización de los contratos inteligentes supone riesgos de abusos y errores de programación que los hacen proclives a fraudes y hackeos. Además, la seudonimidad de las redes hace de los protocolos actividades vulnerables en materia de prevención de lavado de dinero y financiamiento al terrorismo. Debe recordarse que, al operar únicamente a

través de redes digitales, los protocolos carecen de cualquier protección a los usuarios, cuyos riesgos se elevan debido a la autogestión e irreversibilidad de los contratos.

Un posible riesgo del protocolo DeFi es que muchos de estos esquemas podrían tener una gobernanza débil o fácilmente controlable por pocos individuos. Como se comentó anteriormente, la mayoría de los esquemas DeFi operan a través de DAOs, que permiten realizar cambios en el protocolo siempre que se cuente con una mayoría de los tokens de gobernanza. En muchos casos, estos tokens son comerciados en *exchanges* y pueden ser adquiridos en masa por cualquier individuo o grupo, lo que les permitiría realizar cambios discrecionales. Esto eleva la posibilidad de que participantes de uno de estos esquemas sufran de pérdidas de recursos ante cambios en las reglas.

Un factor para considerar es que la participación de entidades financieras en este tipo de esquemas es muy limitada. La mayoría de los involucrados participan con el objetivo de recibir ganancias con otros criptoactivos, sean propios u obtenidos a través de algún protocolo DeFi, o generar retornos al prometerlos como colateral o en los llamados *liquidity pools*. Una parte importante de ellos podrían participar con el objetivo de posponer la monetización de las ganancias para escapar de la fiscalización (OCDE, 2022). Esto supone que, al menos en materia de estabilidad financiera, los esquemas DeFi no presentan aún un desafío apremiante. No obstante, su mayor adopción podría suponer la necesidad de mantener un enfoque cauto que evite que sus riesgos comiencen a filtrarse al sistema financiero y generen riesgos a la población usuaria.

Beneficios y riesgos de los criptoactivos "estables"

Al ser activos virtuales capaces de transferirse de forma completamente descentralizada, las llamadas *stablecoins* comparten en gran medida las ventajas y desventajas de las "criptomonedas" no estables. No obstante, sus características particulares hacen que presenten riesgos particulares. Estas incluyen su proceso de emisión, mayormente centralizado entre las principales *stablecoins* en el mercado, y la necesidad de mecanismos de estabilización, que podrían vincularlos directamente con el mercado financiero tradicional o muy frágiles a choques de confianza. Con el fin de no repetir lo discutido la sección II, y siendo conscientes de que la mayoría de los riesgos entre criptoactivos estables y no estables son compartidos, esta sección se concentra primordialmente en aquellos que aplican principalmente a los *stablecoins*.

Uso transaccional de las *stablecoins*

Los proponentes de los llamados criptoactivos estables argumentan que los pagos con esta clase de activos son más adecuados para generar un acceso generalizado a una plataforma de pagos digitales sin la necesidad de recurrir al sistema financiero tradicional. Su estabilidad, en claro contraste con el *bitcoin* o el *ether*, las hace un mejor sustituto del dinero fiduciario en operaciones digitales. Cualquier persona con un dispositivo digital puede acceder a plataformas par-a-par o *exchanges* y realizar transferencias con *stablecoins*. Si bien carecen de las protecciones habituales de los medios de pago tradicionales, las transferencias par-a-par no requieren de una cuenta bancaria, lo que puede hacerlas útiles como medios de pago y transferencia para la población no bancarizada.

Se ha argumentado que esto podría ser particularmente beneficioso en el caso de los envíos de remesas. Un trabajador en el extranjero podría adquirir *stablecoins* y transferirlos a sus dependientes en el país de origen sin la necesidad de que estos tuvieran una cuenta bancaria. Además, si la *stablecoin* funciona adecuadamente, los depósitos estarían protegidos de la volatilidad, algo que evidentemente no ocurre con las transferencias con otro tipo de criptoactivos. Adicionalmente, estas transferencias podrían ser mayores y con mayor inmediatez que las realizadas por medios tradicionales, considerando que los costos y tiempos de transacción en los mercados de criptoactivos son habitualmente menores.

Si bien los criptoactivos estables muestran beneficios en comparación con los no estables, el mercado de pagos con *stablecoins* está poco desarrollado. Actualmente, existen pocos proveedores de servicios de pago operando con ellas, lo que puede deberse a que las posiciones de estos criptoactivos están concentradas en inversionistas de gran tamaño, con sólo el 3% de los tenedores con posiciones menores a los 10 mil dólares (ECB, 2022). Esta concentración hace suponer que pertenecen a cripto-inversionistas institucionales, como podrían ser fondos cripto o incluso *exchanges*, que parecen más interesados en su uso como cobertura en inversiones especulativas en otros criptoactivos.

Esto no quiere decir que el uso transaccional de las *stablecoins* sea una imposibilidad. Algunas empresas de tecnología como Meta consideraron en su momento integrar *stablecoins* propias a sus sistemas de pago soportados en sus redes sociales.[43] Por supuesto, como se ha discutido en secciones anteriores, su uso conlleva riesgos importantes en materia de protección de usuarios. Al funcionar a través de redes abiertas programables, las operaciones con ellas son irrevocables y sufren de los problemas generados

[43] Esto se describe con más detalle en la subsección de Criptoización y riesgos monetarios.

por la autogestión de cuentas. Además, al emitirse a través de contratos inteligentes, existe el riesgo de abusos y fraudes derivados de su misma complejidad.

Mecanismos de emisión y estabilización

Si bien los criptoactivos estables parecen tener mayores beneficios en comparación de los no estables, esto es completamente dependiente de su capacidad para cumplir con su promesa de estabilidad. Históricamente, las *stablecoins* han tenido un grado variable de éxito para mantener estable su valor en el tiempo, siendo los más estables los fondos tokenizados (Bullmann et al., 2019; Jarno y Kołodziejczyk, 2021). Las *stablecoins* son mucho menos volátiles que el *bitcoin* o el *ether*, pero lo son más que las monedas fiduciarias o el oro al analizar información de alta frecuencia. Esto puede deberse a una correlación elevada entre los flujos de operaciones de *stablecoins* contra criptomonedas no estables derivado de su uso común en transferencias entre éstas (Hoang & Baur, 2020). No obstante, también puede deberse a una incapacidad del emisor de mantener su compromiso en todo momento, lo que abre espacio para el arbitraje y la especulación.

Debe tenerse en cuenta que, incluso con un cierto grado de volatilidad, las *stablecoins* podrían seguir siendo un medio de pago adecuado para gran parte de su población usuaria. Su practicidad general, su disponibilidad casi inmediata, su seudonimidad y su integración con otros criptoactivos, pueden ser considerados beneficios suficientes para continuar utilizándolas aún con volatilidad presente. La población usuaria puede soportarla en cierto grado mientras esta no sea elevada o recurrente. No obstante, una *stablecoin* con un episodio relevante de volatilidad podría generar la señal de que sufre dificultades para mantener su compromiso, lo que podría derivar en una respuesta severa de sus usuarios e incluso en riesgo de contagio hacía otros arreglos de *stablecoins*.

Uno de los riesgos más importantes de los criptoactivos estables se encuentra en la resiliencia de sus mecanismos de estabilización, particularmente en momentos de estrés. Existen varias situaciones que podrían llevar a un emisor a ser incapaz de respaldar su compromiso, incluso en casos en los cuales parecía tener un manejo adecuado de sus reservas. Esto ocurre tanto en las soportadas en activos tradicionales o virtuales como en las algorítmicas, aunque las razones de este incumplimiento pueden ser muy diferentes.

En el caso de arreglos como los fondos tokenizados controlados por un agente central, su desempeño adecuado dependerá no sólo de la solvencia financiera sino moral de su emisora. Como se comentó con anterioridad, la colateralización con monedas fiduciarias u otros activos muy líquidos es el

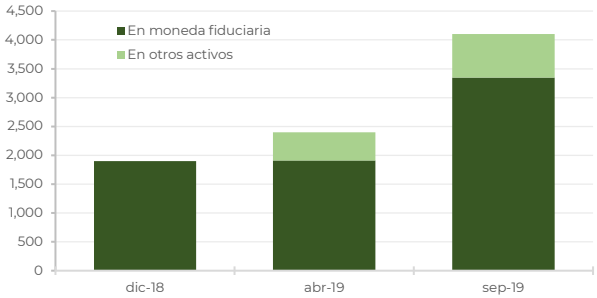
principal mecanismo de estabilización utilizado por las principales *stablecoins* en circulación. Aunque éste parece ofrecer un alto grado de seguridad, también puede ser muy ineficiente. Conservar reservas en moneda fiduciaria uno a uno en todo momento puede resultar impráctico y costoso, ya que mantener un depósito no es necesariamente el medio más efectivo para generar ingresos.

Además, considerando que la mayoría de las emisoras de *stablecoins* no están autorizadas para operar como custodios de las reversas, mantener grandes depósitos en canales tradicionales podría poner los fondos en riesgo. Por un lado, estos podrían perderse en caso de que la institución de depósito quebrara, considerando que es muy probable que las reservas superen por mucho el límite del seguro de depósito en cualquier jurisdicción. Por otro lado, existe la posibilidad de que las instituciones lleven a cabo prácticas de *de-risking*, particularmente si hay una pérdida de confianza en el mercado de criptoactivos o se establecen requisitos más estrictos a las entidades que ofrezcan servicios a los proveedores de servicios cripto.

Estas situaciones pueden generar incentivos para reducir las reservas; no obstante, sin una cobertura al 100%, los fondos tokenizados podrían correr el riesgo de ataques especulativos o ataques de arbitraje (Calcaterra et al., 2019). Una posible solución es desviarse de la cobertura completamente en moneda fiduciaria, y recurrir a otros activos, preferiblemente muy líquidos, en sustitución. Esto genera nuevas dificultades para garantizar el derecho de canje, ya que se abre la posibilidad de variaciones importantes en el valor de los activos de reserva y hace generalmente necesario mantener activos con valor superior a la emisión de la *stablecoin* para asegurar la convertibilidad. Esta sobrecolateralización puede hacer que las reservas en otros activos diferentes sean incluso más costosas que las reservas en efectivo.

No es posible descartar que las emisoras de criptoactivos estables, en búsqueda de mayores ganancias, puedan tener el incentivo perverso de invertir en activos riesgosos, no necesariamente muy líquidos, o prestar los activos en reserva para generar retornos. Esto puede intensificarse si se considera que estas tienen fuentes de ingreso limitadas, podrían estar sujetas a una limitada supervisión por parte de su clientela y autoridades, y que en pocas jurisdicciones se ha implementado un régimen de autorización o licencia para estas actividades. En el marco internacional actual, existe poca transparencia en la información divulgada sobre la composición de reservas y están aún en discusión las prácticas globalmente aceptadas de revelación de información para emisoras de *stablecoins*. En la mayoría de los casos, son las emisoras las que la revelan voluntariamente, como fue el caso de *Tether* (Moore Cayman, 2021), e incluso en estos casos resulta notoria la dificultad para mantener reservas puramente en moneda fiduciaria (figura 15).

Figura 15: Composición de las reservas de *Tether*



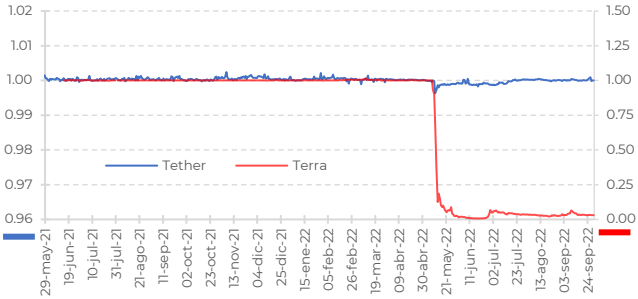
Fuente: Arner et al. (2020).

Sin esquemas de transparencia, las llamadas *stablecoins* pueden ser especialmente vulnerables a pérdidas de confianza. Alguna falla, o incluso la mera expectativa de una, puede llevar a corridas donde los usuarios busquen canjear rápidamente sus *stablecoins* por moneda fiduciaria u otros activos, similar a lo que ha ocurrido históricamente con las salidas de depósitos en crisis bancarias. Esto puede ocasionar "ventas en caliente" de los activos en reserva, lo que puede llevar a perdidas severas tanto para las emisoras como para algunas de las personas usuarias. La pérdida de confianza puede extenderse rápidamente hacía otras criptomonedas, otras *stablecoins*, e incluso a empresas cercanas o relacionadas si se considera que mantienen un perfil de riesgo similar, algo análogo a lo que ocurre entre jurisdicciones diferentes durante una crisis de deuda. Una de las características más riesgosas de estos activos virtuales es que su naturaleza digital hace que transferirlos sea rápido, lo que precipita un deterioro veloz y acelera el contagio en episodios de crisis.

Adicionalmente, existe el riesgo de que la caída de una *stablecoin* se contagie al sistema financiero en general, tanto directa como indirectamente. Por ejemplo, las ventas de activos puedan disrumpir los mercados de fondeo, especialmente cuando el volumen de *stablecoins* relacionados es muy alto (PWWFM, FDIC & OCC, 2021). Un custodio podría enfrentar un problema serio de liquidez si la salida de reservas alcanza un nivel crítico, lo que podría ocasionarle problemas de inviabilidad del negocio. Adicionalmente, si una institución financiera presenta dificultades relacionados con su exposición al mercado de criptoactivos, es muy probable que se generen episodios de contagio entre instituciones que sean percibidas como cercanas al mismo mercado o a entidades financieras relacionadas con estas.

Finalmente, las *stablecoins* algorítmicas presentan desafíos específicos. Al operar de forma automatizada a través de un contrato inteligente, estas *stablecoins* no requieren de una reserva de soporte. En su lugar, necesitan que el programador haya sido capaz de considerar todos los factores relevantes para evitar una fluctuación, algo poco probable si se considera que la mayoría de estas opera a través del señoreaje. Las *stablecoins* algorítmicas son capaces de mantener su objetivo sólo a través de 1) un nivel de demanda de soporte continuo, 2) las acciones de actores independientes que realicen arbitraje estabilizador de precios y 3) la determinación de precios rápida y exacta, particularmente en tiempos de crisis (Mell & Yaga, 2022). El caso del colapso de TerraUSD, una *stablecoin* algorítmica cuyo esquema de señoreaje se soportaba en el criptoactivo Luna, es el ejemplo más claro de las dificultades que tienen estos activos para mantener su promesa de estabilidad.

Figura 16: Evolución de *Tether* y TerraUSD



Fuente: Elaboración propia con información de Bloomberg.

TerraUSD era un arreglo de *stablecoin* algorítmico dirigida por Terraform Labs, una empresa con domicilio en Singapur. Previo a su crisis, la *stablecoin* había mostrado éxito en mantener su promesa de estabilidad, incluso presentando una volatilidad menor que *Tether*, la principal *stablecoin* en circulación (figura 16). Su criptoactivo de soporte Luna tenía una cotización y volumen de operación altos y varios fondos cripto habían tomado posiciones elevadas en el activo. Cuando uno de estos fondos, Pantera Capital, realizó un *whale trade* sobre su posición en Luna, el valor del criptoactivo de soporte cayó de forma dramática y generó que múltiples inversionistas se deshicieran de sus posiciones. Como resultado, el valor de Luna se desplomó haciendo imposible que TerraUSD mantuviera su promesa. En menos de un día, el valor de la *stablecoin* había caído de 1 dólar por unidad a relativamente cero.

Criptoización y riesgos monetarios

Un foco de atención para las autoridades monetarias es el hecho de que la adopción generalizada de las "criptomonedas" podría llevar a la pérdida de soberanía monetaria, afectando los canales de transmisión de la política monetaria sobre los precios. Si bien este riesgo es menos relevante en el contexto de "criptomonedas" no estables, cuya utilización como medio de pago es limitada, éste podría ser determinante en el caso de monedas con valores más estables.

Las autoridades y organismos internacionales han mostrado mayor preocupación por las que han llamado comúnmente *stablecoins* globales, es decir, aquellos criptoactivos estables con un alto potencial de alcance y adopción, además de una probabilidad elevada de alcanzar un volumen de operaciones sustancial (FSB, 2020). En particular, grandes empresas tecnológicas podrían establecer *stablecoins* aprovechando su amplia base de usuarios y su presencia en múltiples jurisdicciones para integrarlas en sus plataformas de comunicación ya existentes.

El ejemplo más claro fue el proyecto Diem de Meta, anteriormente conocido como proyecto Libra de Facebook (Jafari & Gruber, 2021). Originalmente, el proyecto, introducido en 2019, tenía la intención de proveer servicios financieros de forma transfronteriza a través de tecnología DLT. La red de soporte tendría una gobernanza a través de la Libra Association, una asociación no lucrativa de membresía independiente formada por varias empresas privadas incluida Facebook (Libra Association, 2019). El proyecto se sustentaba en la *stablecoin* Libra, que estaría soportada por depósitos y bonos de gobierno de corto plazo, los cuales serían administrados por la Libra Association y sus subsidiarias.

El proyecto generó gran inquietud, particularmente en Estados Unidos y los países europeos. La preocupación principal se relacionaba con la participación de Facebook, ya que al momento la red social y sus subsidiarias, como WhatsApp y Messenger, tenían un alcance de alrededor de 3.21 mil millones de personas, lo que representa alrededor de 25% de la población mundial. Esto pondría a Facebook en posición de ser parte crítica del sistema de pagos a nivel mundial en caso de que el proyecto fuera ampliamente adoptado. Las constantes comparecencias de sus directivos en la Cámara de Representantes de Estados Unidos requirieron que sus promotores repensaran el proyecto, lo que llevó al cambio hacía el proyecto Diem de Meta.

En la nueva propuesta, se introducirían múltiples *stablecoins*, cada una soportada por una única moneda fiduciaria. A partir de ellas, se generaría una *stablecoin* compuesta, el Diem, que sería utilizada para transferencias transfronterizas en jurisdicciones donde no se hubiera introducido una

stablecoin en su moneda local. La idea básica era que la combinación de una plataforma DLT sin permisos, pero gobernada de forma descentralizada por un conglomerado de empresas privadas, con aplicaciones de contrato inteligente integradas y *stablecoins* soportadas por diferentes divisas deberían evolucionar hacia un ecosistema de sector financiero, accesible a través de cualquier dispositivo digital (Jafari & Gruber, 2021).

Aunque el proyecto Diem fue cancelado y sus activos intelectuales fueron vendidos a Silverlight, aún existe la posibilidad de la aparición futura de una *stablecoin* con capacidad de ser ampliamente adoptada. El surgimiento de una *stablecoin* global soportada en monedas fiduciarias como el dólar, el euro o el yuan podría llevar a un proceso de sustitución de moneda fiduciaria por *stablecoins*, principalmente en el caso de países con elevada inestabilidad económica (Foster et al., 2021). Este proceso de criptoización puede detonarse por causas como la baja credibilidad del banco central, ineficiencias en el sistema de pagos y acceso limitado a servicios financieros (FMI, 2021). Igualmente, existen incentivos para criptoizar una economía en casos donde sanciones económicas podrían dificultar el uso de la moneda de curso legal y/o limitar la capacidad de recibir transferencias en otras divisas.

La aparición de una *stablecoin* de estas características podría tener impactos sistémicos, ya que podría llevar a que una parte significativa de la oferta de dinero en la economía quede fuera del control de la banca central y del sector bancario, además de retirar un volumen significativo de activos de bajo riesgo del sistema (Arner et al., 2020).

IV. Consideraciones finales

Los avances tecnológicos de los últimos años han acelerado la adopción de los medios digitales en todo el mundo. Particularmente, los avances en informática y la fácil disponibilidad de equipos y dispositivos electrónicos han permitido el desarrollo de nuevos productos y servicios de forma descentralizada. Los criptoactivos son un ejemplo claro del impacto que pueden tener estos avances, al permitir que cualquier persona con conocimientos en programación e informática sea capaz de crear productos y servicios que asemejan e incluso podrían llegar a competir con los ofrecidos por el sistema financiero tradicional. Además, la presencia de dispositivos digitales a todo nivel hace posible que potencialmente cualquiera pueda participar de estos productos. Su aparición y adopción, aunque podría traer algunos beneficios, también conlleva riesgos potenciales en materia de ciberseguridad, protección de usuarios, y prevención de actividades ilícitas. Incluso, en el caso de una adopción generalizada, podrían poner en riesgo la estabilidad financiera de las instituciones cuando se manejan de forma inadecuada.

A pesar de haber aparecido por primera vez hace más de una década, el interés del público general por los criptoactivos comenzó apenas hace algunos años. La primera ola de interés generalizado puede rastrearse a 2017, cuando el *bitcoin* experimentó su primer ciclo de crecimiento acelerado. Esta ola se caracterizó por un aumento elevado de su valor, períodos de congestionamiento y una mayor proliferación de fraudes. El segundo ciclo puede identificarse con el choque de la pandemia de la COVID-19, que impulsó el uso generalizado de medios digitales ante las restricciones a la movilidad a nivel global. La exposición mediática solo ha incrementado tanto el entusiasmo como el escrutinio de este mercado, que ha presentado una elevada volatilidad desde 2022.

A pesar de este mayor interés general, la integración del mercado de criptoactivos con el sistema financiero tradicional puede considerarse aún incipiente en la mayoría de las economías. No obstante, episodios recientes como las quiebras en 2023 de los bancos Silvergate y Signature, cuyo negocio incluía la prestación de servicios a proveedores de servicios cripto, muestran la necesidad de mantener un enfoque cauto y una vigilancia atenta. Aunque puede argumentarse que la caída de estos bancos no estuvo completamente relacionada a su negocio cripto (FDIC, 2023), esto no implica que situaciones similares no podrían llevar a episodios de contagio e inestabilidad. Como ha ocurrido en crisis financieras anteriores, "una pequeña exposición conocida no necesariamente implica una pequeña cantidad de riesgo" (FSB, 2022, p. 5).

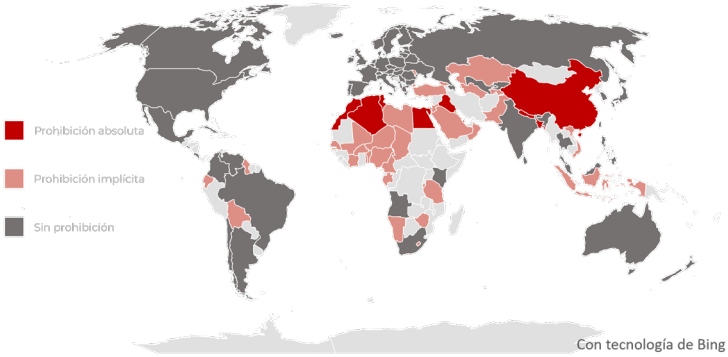
Los últimos años han dado un nuevo ímpetu a los esfuerzos internacionales para generar una respuesta coordinada a la aparición y posible adopción de los criptoactivos, aunque la posibilidad de establecer un marco regulatorio y de supervisión globalmente aceptado está aún en discusión. Las dificultades para establecer un marco común se derivan de sus características particulares y su tecnología subyacente, que han complicado la aplicación automática de definiciones legales y marcos regulatorios existentes (WEF, 2021b). Igualmente, no existe un consenso para una terminología o taxonomía global (Allen et al., 2020), ya sea porque estos activos tienen múltiples usos, lo que hace difícil construir una definición apropiada y definir competencias entre autoridades, o porque una definición acotada podría no contener todas las características relevantes, permitiendo cierto grado de arbitraje.

Esto no quiere decir que la coordinación internacional sea inexistente. Por dar solo algunos ejemplos, las primeras propuestas para establecer estándares y prácticas internacionales en la materia, liderados por el Grupo de Acción Financiera Internacional (GAFI) iniciaron poco después de que el *bitcoin* alcanzará volúmenes de operación relevantes, y se concentraron particularmente en mitigar los riesgos que presentaban en materia de

prevención de lavado de dinero y financiamiento al terrorismo (GAFI/FATF, 2014; 2015, 2019 y 2021). De forma complementaria, la Organización Internacional de Comisiones de Valores (IOSCO, por sus siglas en inglés) ha establecido guías y principios básicos para la protección y educación de inversionistas minoristas en criptoactivos (OICV-IOSCO, 2020a), así como principios para la regulación de plataformas de intercambio (OICV-IOSCO, 2020b).

En materia de estabilidad financiera, el Comité de Supervisión Bancaria de Basilea (BCBS, por sus siglas en inglés) ha propuesto principios guía para cualquier diseño de un marco prudencial sobre exposiciones en criptoactivos (BCBS, 2019)[44] y ha sido enfático en el riesgo potencial que representan para la estabilidad financiera. El Comité ha publicado varios documentos (BCBS, 2021, 2022a), incluyendo la versión final del estándar para la exposición en criptoactivos (BCBS, 2022b), diferenciando entre los fondos tokenizados, y los criptoactivos sin soporte o no estables. Sobre las *stablecoins*, el *Financial Stability Board* (FSB) generó su primer reporte sobre el tema y ofreció recomendaciones en materia de regulación y supervisión de los arreglos de *stablecoins* globales (FSB, 2020).

Figura 17: Estado del uso legal de criptoactivos a nivel mundial (estatus legal por país)



Fuente: Elaboración propia con información de Library of Congress (2021). "Regulation of cryptocurrencies around the world". La base de datos fue actualizada en noviembre de 2021. Los países sin información disponible aparecen en gris claro.

[44] Los tres principios corresponden a:
1) Mismo riesgo, misma actividad, misma regulación: en términos prácticos, un criptoactivo que tiene las mismas funciones y plantea los mismos riesgos que un activo tradicional debe cumplir con los mismos requisitos que este, incluyendo aquellos relacionados con liquidez y capital.
2) Simplicidad: existe merito en iniciar con un tratamiento cauto y simple, que pueda modificarse en línea con la evolución del mercado.
3) Estándares mínimos: cualquier tratamiento prudencial de criptoactivos debe constituir un estándar mínimo para bancos activos internacionalmente. Una jurisdicción que prohíba a un banco tener exposición a criptomonedas se consideraría que cumple con un estándar prudencial global.

Los estándares internacionales, que continúan en discusión, no han frenado los trabajos independientes de varias jurisdicciones para lidiar con el creciente interés y adopción de los criptoactivos. Algunas han actuado de forma más rápida y con grados diversos de apertura a estos. De acuerdo con un estudio de la Library of Congress (2021) de Estados Unidos, la mayoría de las economías en el mundo tienen al menos algún tipo de regulación relacionada con el uso de estos activos. En la mayoría de los países, su utilización por el público en general es legal, aunque a excepción de El Salvador, en ninguno se consideran como moneda de curso legal (figura 17).

El ejemplo más característico de un veto al uso de criptoactivos ha sido China, que realizó cambios regulatorios que detuvieron de facto las operaciones con estos en el país (Borri & Shakhnov, 2020). En contraste, países como Suiza han construido un marco amistoso a estos activos (Borri & Shakhnov, 2020), siendo de los primeros en definirlos legalmente como activos o propiedad y establecer un marco legal específico para la provisión de servicios de *exchange* de criptoactivos y brindar licencias a instituciones financieras para ofrecer servicios con activos virtuales. El país europeo es el hogar del Crypto Valley, considerado el ecosistema más grande de empresas de *blockchain* en el mundo.[45] El Salvador merece una mención aparte. El país centroamericano publicó en su Diario Oficial el 8 de junio de 2021 la llamada Ley Bitcoin, que estableció la capacidad de utilizar este criptoactivo como moneda de curso legal en el país, [46] algo que fue considerado un paso demasiado lejos por el Fondo Monetario Internacional (FMI) (Adrian & Weeks Brown, 2021).

La Unión Europea aprobó en abril de 2023 su regulación MiCA (*Markets in Crypto Assets*) que establece el primer marco integral para la operación de criptoactivos en uno de los principales mercados del mundo, incluyendo el establecimiento de un régimen de licencias para proveedores de criptoservicios y definiendo claramente el tratamiento regulatorio de las "criptomonedas" y otros activos virtuales. [47] Estados Unidos ha estado activo en la evaluación de una posible regulación del mercado de criptoactivos, particularmente en el caso de las *stablecoins*. Las autoridades del país publicaron su primer reporte inter-agencias relacionado con los criptoactivos estables en 2021 (PWWFM, FDIC & OCC, 2021). En abril de 2023, el Comité de Servicios Financieros de la Cámara de Representantes publicó el borrador

[45] Véase https://cryptovalley.swiss/about-the-association/
[46] Véase https://www.asamblea.gob.sv/node/11282.
[47] Un resumen de la regulación puede consultarse en https://oeil.secure.europarl.europa.eu/oeil/popups/printsummary.pdf?id=1632639&l=en&t=E. La versión íntegra de la regulación está disponible en https://www.europarl.europa.eu/RegData/docs_autres_institutions/commission_europeenne/com/2020/0593/COM_COM(2020)0593_EN.pdf

para discusión de la primera regulación específica en materia de *stablecoins*.[48]

En el caso de México, la regulación actual sobre el uso de criptoactivos se encuentra principalmente en la Ley para Regular las Instituciones de Tecnología Financiera, conocida comúnmente como Ley Fintech, publicada en 2018.[49] El Banco de México, la Secretaría de Hacienda y Crédito Público (SHCP) y la Comisión Nacional Bancaria y de Valores (CNBV) se han expresado de forma conjunta sobre los riesgos de utilizar activos virtuales y han sido enfáticos en la prohibición actual que tienen las instituciones financieras para celebrar y ofrecer operaciones con criptoactivos a sus clientes.[50] Las autoridades mexicanas han mantenido un enfoque cauto en la materia, y llevan a cabo una vigilancia y evaluación constantes de los desarrollos en el ecosistema cripto y su interacción con los mercados tradicionales para asegurarse que estos no representen un riesgo tanto para las personas usuarias, actuales y potenciales, como para las instituciones financieras.

Eventos recientes han mostrado que un enfoque cauto podría ser el más adecuado, considerando los riesgos que podría conllevar la adopción generalizada de estos activos. Probablemente el episodio que mayor repercusión ha tenido sobre la percepción reciente de los mercados de criptoactivos ha sido la quiebra de FTX, uno de los *exchanges* más importantes del planeta, en noviembre de 2022. El colapso de esta plataforma no se relacionó originalmente por un problema de ciberseguridad, sino con un uso inadecuado de recursos de la clientela para financiar a otras compañías relacionadas. En específico, una investigación periodística reveló que FTX había utilizado recursos de su clientela, específicamente aquellos en FTT, la "criptomoneda" nativa del *exchange*, para financiar a su empresa hermana Alameda Research.[51] La publicación de la nota ocasionó una crisis de confianza en la institución, lo que tiró el valor del token FTT hasta niveles cercanos a cero. El colapso generó una crisis de liquidez en FTX, que se contagió rápidamente a empresas relacionadas con la plataforma y ocasionó la quiebra de varios *exchanges*, fondos cripto y otras empresas relacionadas que contaban con posiciones altas en FTT. La intervención de las autoridades tanto de Estados Unidos como de Bahamas, el domicilio legal de la plataforma reveló una completa falta de controles corporativos que se reflejó en una administración de riesgos inexistente y la concentración del poder de decisión

[48] La versión puede consultarse en https://docs.house.gov/meetings/BA/BA21/20230419/115753/BILLS-118pih-Toproviderequirementsforpaymentstablecoinissuersresearchonadigitaldollarandforotherpurposes.pdf

[49] Puede consultarse en https://www.diputados.gob.mx/LeyesBiblio/pdf/LRITF_200521.pdf.

[50] Comunicado No. 39, 28 de junio de 2021, disponible en https://www.gob.mx/cms/uploads/attachment/file/648832/Comunicado_No._039.pdf.

[51] Véase https://www.coindesk.com/business/2022/11/02/divisions-in-sam-bankman-frieds-crypto-empire-blur-on-his-trading-titan-alamedas-balance-sheet/.

en un pequeño grupo de individuos que parecen haber tenido pocos escrúpulos para manejar los recursos de sus clientes.

Es importante que las autoridades mantengan los esfuerzos de cooperación internacional para enfrentar los riesgos que representan los activos virtuales, y que sus potenciales beneficios puedan ser capitalizados. Los esfuerzos por establecer principios guías y estándares serán beneficiosos para evitar el arbitraje multijurisdiccional y permitirán establecer medidas que mitiguen los riesgos que pueden presentar en materia de estabilidad financiera, protección de usuarios, ciberseguridad y prevención del lavado de dinero y financiamiento al terrorismo.

Las experiencias individuales de diversos países y la constante evolución en el desarrollo basados en criptoactivos muestran la necesidad de mantener un enfoque cauto y continuar evaluando los desarrollos del mercado. Es importante que las autoridades financieras mexicanas continúen dando seguimiento oportuno al desarrollo de la regulación y supervisión de los criptoactivos a nivel internacional, tanto a los acuerdos globales como a los esfuerzos individuales de diversas jurisdicciones. Esto permitirá afinar el marco actual y evitar que los riesgos potenciales de estos productos permeen en las instituciones financieras. Finalmente, es relevante que las autoridades se mantengan a la vanguardia de los desarrollos en el sector de criptoactivos. La versatilidad que ofrecen las nuevas tecnologías hace posible la innovación constante en el sector, lo que se refleja en el surgimiento de nuevos productos y esquemas que podrían tener efectos disruptivos en los mercados financieros. Espero que este documento funcione como una base que permita a las personas interesadas conocer los conceptos básicos de operación de los criptoactivos, y permitan facilitar la comprensión de los desarrollos recientes.

Referencias

Abadi, J., & Brunnermeier, M. (2018). Blockchain economics. NBER Working Paper No. 25407. Retrieved from https://www.nber.org/system/files/working_papers/w25407/w25407.pdf

Adrian, T., & Weeks-Brown, R. (2021, Julio 26). Cryptoassets as national currency? A step too far. IMF Blog. Retrieved from https://www.imf.org/en/Blogs/Articles/2021/07/26/blog-cryptoassets-as-national-currency-a-step-too-far

Allen, J. G., Rauchs, M., Blandin, A., & Bear, K. (2020). Legal and regulatory considerations for digital assets. Cambridge Centre for Alternative Finance. Cambridge University. Retrieved from https://www.jbs.cam.ac.uk/wp-content/uploads/2020/10/2020-ccaf-legal-regulatory-considerations-report.pdf

Antonopoulos, A. M. (2017). Mastering Bitcoin: Programming the open blockchain (2° ed.). Sebastapol, California, EUA: O'Reilly.

Antonopoulos, A. M., & Wood, G. (2018). Mastering Ethereum. Sebastopol, California, EUA: O'Reilly.

Aramonte, S., Huang, W., & Schrimpf, A. (2021). DeFi risks and the decentralisation illusion. BIS Quaterly Review, Diciembre 2021, 21-36. Retrieved from https://www.bis.org/publ/qtrpdf/r_qt2112b.htm

Arnet, D., Auer, R., & Frost, J. (2020). Stablecoins: risks, potential and regulation. BIS Working Papers No. 905. Retrieved from https://www.bis.org/publ/work905.htm

Auer, R. (2019a). Beyond the doomsday economics of "proof-of-work" in cryptocurrencies. BIS Working Paper No.765. Retrieved from https://www.bis.org/publ/work765.htm

Auer, R. (2019b). Embedded supervision: how to build regulation into blockchain finance. BIS Working Paper No. 811. Retrieved from https://www.bis.org/publ/work811.pdf

Auer, R., & Claessens, S. (2020). Cryptocurrency market reactions to regulatory news. Globalization Institute Working Paper 381. Federal Reserve Bank of Dallas. Retrieved from https://www.dallasfed.org/~/media/documents/institute/wpapers/2020/0381.pdf

Auer, R., & Tercero-Lucas, D. (2021). Distrust or speculation? The socioeconomic drivers of US cryptocurrency investments. BIS Working Papers No.951. Retrieved from https://www.bis.org/publ/work951.pdf

Bains, P., Ismail, A., Melo, F., & Sugimoto, N. (2022a). Regulating the crypto ecosystem: The case of unbacked crypto assets. IMF. Fintech Notes. Retrieved from https://www.imf.org/en/Publications/fintech-notes/Issues/2022/09/26/Regulating-the-Crypto-Ecosystem-The-Case-of-Unbacked-Crypto-Assets-523715

Bains, P., Ismail, A., Melo, F., & Sugimoto, N. (2022b). Regulating the crypto ecosystem: The case of stablecoins and arrangements. IMF. Fintech Notes. Retrieved from https://www.elibrary.imf.org/view/journals/063/2022/008/article-A001-en.xml

BCBS [Basel Committee for Banking Supervision]. (2021). Consultative document: Prudential treatment of cryptoasset exposures. BIS. Retrieved from https://www.bis.org/bcbs/publ/d519.htm

BCBS [Basel Committee on Banking Supervision]. (2022a). Consultative document: Second consultation on the prudential treatmeant of cryptoasset exposures. BIS. Retrieved from https://www.bis.org/bcbs/publ/d533.pdf

BCBS [Basel Committee on Banking Supervision]. (2022b). Prudential treatment of cryptoasset exposures. BIS. Retrieved from https://www.bis.org/bcbs/publ/d545.pdf

BCBS [Basel Committtee for Banking Supervision]. (2019). Discussion document - Designing a prudential treatment for cryptoassets. BIS. Retrieved from https://www.bis.org/bcbs/publ/d490.pdf

BIS [Bank of International Settlements]. (2018). Cryptocurrencies: looking beyond the hype. BIS Annual Economic Review 2018, 91-114. Retrieved from https://www.bis.org/publ/arpdf/ar2018e5.pdf

Blandin, A., Cloots, A. S., Hussain, H., Rauchs, M., Saleuddin, R., Allen, J. G., . . . Cloud, K. (2019). Global cryptoasset regulatory landscape study. Cambridge Centre for Alternative Finance. Cambridge University. Retrieved from https://www.jbs.cam.ac.uk/wp-content/uploads/2020/08/2019-04-ccaf-global-cryptoasset-regulatory-landscape-study.pdf

Blandin, A., Pieters, G., Eisermann, T., Dek, A., Taylor, S., & Njoki, D. (2020). 3rd Global cryptoasset benchmarking study. Cambridge Centre for Alternative Finance. Cambridge University. Retrieved from https://www.jbs.cam.ac.uk/wp-content/uploads/2021/01/2021-ccaf-3rd-global-cryptoasset-benchmarking-study.pdf

Borri, N., & Shakhnov, K. (2020). Regulation spillovers across cryptocurrency markets. Finance Research Letters, 36(2020), 1-6.

Budish, E. (2018). The economic limits of bitcoin and the blockchain. NBER Working Paper Series No. 24717. Retrieved from https://www.nber.org/system/files/working_papers/w24717/w24717.pdf

Bullman, D., Klemm, J., & Pinna, A. (2019). In search of stability in crypto-assets: Are stablecoins the solution? Ocassional Paper Series No. 230. European Central Bank. Retrieved from https://www.ecb.europa.eu/pub/pdf/scpops/ecb.op230~d57946be3b.en.pdf

Buterin, V. (2022). Proof of Stake: The making of Ethereum and the philosophy of blockchains. Nueva York, EUA: Seven Stories Press.

Calcaterra, C., Kaal, W. A., & Rao, V. (2019). Stable cryptocurrencies - First order principles. Stanford Journal of Blockchain Law & Policy, 2019, 1-30.

Chainalysis. (2021a). The 2021 Crypto Crime Report. Retrieved from https://go.chainalysis.com/rs/503-FAP-074/images/Chainalysis-Crypto-Crime-2021.pdf

Chainalysis. (2021b). The 2021 Geography of cryptocurrency report. Retrieved from https://go.chainalysis.com/2021-geography-of-crypto.html

Champagne, P. (2014). The book of Satoshi: The collected writings of Bitcoin creator Satoshi Nakamoto. EUA: e53 Publishing LLC.

CipherTrace. (2021). Current trends in Ramsomware with special notes on Monero usage. Mastercard. Retrieved from https://4345106.fs1.hubspotusercontent-na1.net/hubfs/4345106/Content/Current%20Trends%20in%20Monero%20Usage%20and%20Ransomware_FINAL.pdf

Coelho, R., Fishman, J., & Garcia Ocampo, D. (2021). Supervising cryptoassets for anti-money laundering. BIS. FSI insights on policy implementation No 31. Retrieved from https://www.bis.org/fsi/publ/insights31.htm

De Filippi, P., & Wright, A. (2019). Blockchain and the Law: The rule of code. Cambridge, Massachusets, EUA: Harvard University Press.

ECB [European Central Bank]. (2022). Stablecoins' role in crypto and beyond: functions, risks and policy. ECB. Macroprudential Bulletin. Retrieved from https://www.ecb.europa.eu/pub/financial-stability/macroprudential-bulletin/html/ecb.mpbu202207_2~836f682ed7.en.html

FDIC [Federal Deposit Insurance Corporation]. (2023). FDIC's supervision of Signature Bank. Disponible en https://www.fdic.gov/news/press-releases/2023/pr23033a.pdf.

Ferreira, D., Li, J., & Nikolowa, R. (2021). Corporate capture of blockchain governance. European Corporate Governance Institute. Working Paper Series in Finance No. 593. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3320437

FMI [Fondo Monetario Internacional]. (2021a). The rise of digital money - A strategic plan to continue delivering on the IMF's mandate. FMI. Retrieved from https://www.imf.org/-/media/Files/Publications/PP/2021/English/PPEA2021054.ashx

FMI [Fondo Monetario Internacional]. (2021b). The crypto ecosystem and financial stability challenges. In FMI, Global Financial Stability Report: COVID-19, crypto and climate: navigating challenging transitions (pp. 41-57). Retrieved from https://www.elibrary.imf.org/view/books/082/465808-9781513595603-en/ch002.xml

FMI [Fondo Monetario Internacional]. (2021c). Global Financial Stability Report Chapter 2. Online Annex 2.1 Technical Note. In FMI, Global Financial Stability Report: COVID-19, crypto and climate: navigating challenging transitions (pp. A1-4).

Foley, S., Karlsen, J. R., & Putnins, T. J. (2019). Sex, drugs and bitcoin: How much illegal activity is financed through cryptocurrencies? The Review of Financial Studies, 32(5), 1798-1853.

Frost, J., Shin, H. S., & Wierts, P. (2020). An early stablecoin? The Bank of Amsterdam and the governance of money. BIS. Retrieved from https://www.bis.org/publ/work902.htm

FSB [Financial Stability Board]. (2019). Crypto-assets: Work underway, regulatory approaches and potential gaps. FSB. Retrieved from https://www.fsb.org/2019/05/crypto-assets-work-underway-regulatory-approaches-and-potential-gaps/

FSB [Financial Stability Board]. (2020). Regulation, supervision and oversight of "global stablecoin" arrangements. Final report and high-level recommendations. FSB. Retrieved from

https://www.fsb.org/2020/10/regulation-supervision-and-oversight-of-global-stablecoin-arrangements/

FSB [Financial Stability Board]. (2022). Assessment of risks to financial stability from crypto-assets. FSB. Retrieved from https://www.fsb.org/wp-content/uploads/P160222.pdf

GAFI/FATF [Grupo de Acción Financiera Internacional / Financial Action Task Force]. (2014). Virtual currencies: Key definitions and potential AML/CFT Risks. FATF/OECD. Retrieved from https://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf

GAFI/FATF [Grupo de Acción Financiera Internacional / Financial Action Task Force]. (2015). Guidance to a risk-based approach to virtual currencies. París: FATF/OECD.

GAFI/FATF [Grupo de Acción Financiera Internacional / Financial Action Task Force]. (2019). Guidance for a risk-based approach to virtual assets and virtual asset service providers. Paris: FATF/OECD. Retrieved from http://www.fatf-gafi.org/media/fatf/documents/recommendations/RBA-VA-VASPs.pdf

GAFI/FATF [Grupo de Acción Financiera Internacional / Financial Action Task Force]. (2020). FATF report to the G20 Finance Ministers and Central Bank Governors on so-called stablecoins. París: FATF/OECD. Retrieved from http://www.fatf-gafi.org/publications/virtualassets/documents/report-g20-so-called-stablecoins-june-2020.html

GAFI/FATF [Grupo de Acción Financiera Internacional / Financial Action Task Force]. (2021). Virtual assets and virtual asset service providers: Updated guidance for a risk-based approach. París: FATF. Retrieved from https://www.fatf-gafi.org/media/fatf/documents/recommendations/Updated-Guidance-VA-VASP.pdf

Hoang, L. T., & Baur, D. G. (2020). How stable are stablecoins? University of Western Australia. Retrieved from https://www.researchgate.net/publication/338739334

Huberman, G., Leshno, J. D., & Moallemi, C. (2021). Monopoly without a monopolist: An economic analysis of the bitcoin payment system. Review of Economic Studies, 2021(88), 3011-3040.

Jafari, G. A., & Gruber, M.-C. (2021). The case of Diem: a distributed ledger technology-based alternative financial infrastructure built by a centralised multisided platform. JIPITEC 301. Retrieved from https://www.jipitec.eu/issues/jipitec-12-4-2021/5402/gruber_pdf.pdf

Jarno, K., & Kolodziejczyk, H. (2021). Does the design of stablecoins impact their volatility? Journal of risk and financial management, 14(42), 1-14.

Kahn, C. M., Long, C., & Alwazir, J. (2020). Privacy provision, payment latency, and role of collateral. IMF Working Papers No. 20/148. Retrieved from https://www.elibrary.imf.org/view/journals/001/2020/148/article-A001-en.xml

Lewis, A. (2018). The basics of bitcoins and blockchains: An introduction to cryptocurrencies and the technology that powers them. Coral Gables, Florida, EUA: Mango Publishing.

Libra Association. (2019). An introduction to Libra. Libra Association. Retrieved from https://sls.gmu.edu/pfrt/wp-content/uploads/sites/54/2020/02/LibraWhitePaper_en_US-Rev0723.pdf

Makarov, I., & Schoar, A. (2020). Trading and arbitrage in cryptocurrency markets. Journal of Financial Economics, 135(2), 293-319.

Makarov, I., & Schoar, A. (2021). Blockchain analysis of the bitcoin market. NBER Working Paper Series No. 29396. Retrieved from https://www.nber.org/system/files/working_papers/w29396/w29396.pdf

Mehta, N., Agashe, A., & Detroja, P. (2021). Bubble or revolution? The present and future of blockchain and cryptocurrencies (2° ed.). North Chelmsford, MA, EUA: Paravane Ventures.

Mell, P., & Yaga, D. (2022). Understanding stablecoin technology and related security considerations. Initial public draft. U.S. Department of Commerce - National Institute of Standards and Technology. Retrieved from https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8408.ipd.pdf

Moore Cayman. (2021). Independent accountant's report Tether Holdings Limited.

Moore, T., & Christin, N. (2013). Beware the middleman: empirical analysis of Bitcoin-exchange risk. In A.-R. Sadeghi (Ed.), Financial cryptography, volume 7858 of Lecture notes in computer science (pp. 25-33). Springer.

Moore, T., Christin, N., & Szurdi, J. (2018). Revisiting the risk of bitcoin currency exchange closure. ACM transactions on internet technology, 18(4), Artículo 50, 1-18.

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. Retrieved from https://bitcoin.org/bitcoin.pdf

Nelson, B. (2018). Financial stability and monetary policy issues associates with digital currencies. Journal of Economics and Business, 100(2018), 76-78.

OCDE [Organización para la Cooperación y el Desarrollo Económicos]. (2022). Why Decentralised Finance (DeFi) matters and the policy implications. OCDE. Retrieved from https://www.oecd.org/finance/why-decentralised-finance-defi-matters-and-the-policy-implications.htm

OICV-IOSCO [International Organization of Securities Commisions]. (2020a). Investors education on crypto-assets. IOSCO. Retrieved from https://www.iosco.org/library/pubdocs/pdf/IOSCOPD668.pdf

OICV-IOSCO [International Organization of Securities Commisions]. (2020b). Issues, risks and regulatory considerations relating to crypto-asset trading platforms (Final Report). IOSCO. Retrieved from https://www.iosco.org/library/pubdocs/pdf/IOSCOPD649.pdf

Pernice, I. G., Henningsen, S., Proskalovich, R., Florian, M., Elendner, H., & Scheuermann, B. (2019). Monetary stabilization in cryptocurrencies - Design approaches and open questions. 2019 Crypto Valley Conference on Blockchain Technology (pp. 1-13). IEEE. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3398372

PWWFM, FDIC & OCC [President's Working Group on Financial Markets, the Federal Deposit Insurance Corporation, & the Office of the Comptroller of the Currency]. (2021). Interagency Report on Stablecoins. Gobierno de los Estados Unidos. Retrieved from

https://home.treasury.gov/system/files/136/StableCoinReport_Nov1_508.pdf

Ríos, M. D. (2013). Technological neutrality and conceptual singularity. SSRN. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2198887

SHCP [Secretaría de Hacienda y Crédito Público]. (20202). Evaluación Nacional de Riesgos 2020, Versión pública. Disponible en https://www.pld.hacienda.gob.mx/work/models/PLD/documentos/enr2020.pdf

Schwab, K.. (2016). The Fourth Industrial Revolution: what it means, how to respond. World Economic Fourm. Disponible en https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond/

Soska, K., Dong, J.-D., Khodaverdian, A., Zetlin-Jones, A., Routledge, B., & Christin, N. (2021). Towards understanding cryptocurrency derivatives: A case study of BitMex. The Web Conference. Carnegie Mellon University CyLab. Retrieved from https://www.cylab.cmu.edu/_files/documents/towards-understanding-cryptocurrency.pdf

VISA. (2021). The crypto phenomenon: consumer attitudes & usage. VISA, LRW, a Material Company. Retrieved from https://usa.visa.com/content/dam/VCOM/regional/na/us/Solutions/documents/visa-crypto-consumer-perceptions-white-paper.pdf

Watorek, M., Drozdz, S., Kwapien, J., Minati, L., Oswiecimka, P., & Stanuszek, M. (2021). Multiscale characteristics of emerging global cryptocurrency market. Physics Report, 901(2021), 1-82.

WEF [World Economic Forum]. (2021a). Cryptocurrencies: A guide to getting started. WEF. Global Future Council on Cryptocurrencies. Community Paper. Retrieved from https://www3.weforum.org/docs/WEF_Getting_Started_Cryptocurrency_2021.pdf

WEF [World Economic Forum]. (2021b). Navigating cryptocurrency regulation: An industry perspective on the insights and tools needed to shape balanced crypto regulation. Genova, Suiza: WEF. Retrieved from https://www3.weforum.org/docs/WEF_Navigating_Cryptocurrency_Regulation_2021.pdf

White, R., Marinakis, Y., Islam, N., & Walsh, S. (2020). Is Bitcoin a currency, a technology-based product, or something else? Technological Forecasting & Social Change, 151(2020), 1-13.