Finanzas descentralizadas en México

¿Advertencia u oportunidad?

Israel Cedillo Lazcano
y Miguel Hakim Simón

UNIVERSIDAD DE LAS AMÉRICAS PUEBLA

Finanzas descentralizadas en México

¿Advertencia u oportunidad?

Israel Cedillo Lazcano
y Miguel Hakim Simón

UDLAP®

D. R. © 2026 Fundación Universidad de las Américas, Puebla
Ex hacienda Santa Catarina Mártir s/n, San Andrés Cholula,
Puebla, México, 72810
Tel.: +52 222 229 20 00
www.udlap.mx
editorial.udlap@udlap.mx

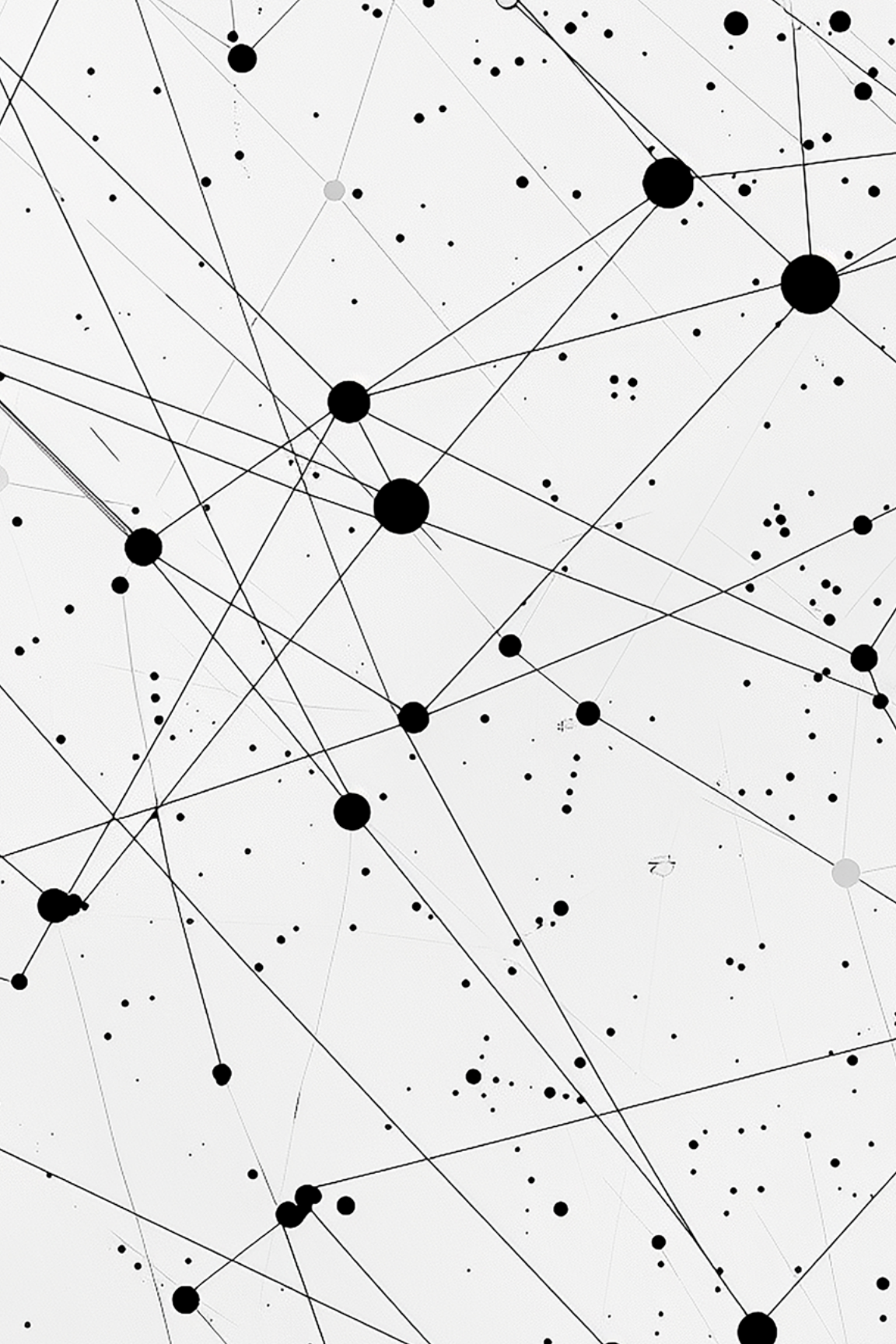
Primera edición: mayo de 2026
ISBN: 978-607-69316-5-3

Diseño editorial y portada: Willy Daniel Sepúlveda Juárez
Corrección de estilo: Andrea Garza Carbajal, Román Esaú Ocotitla Huerta y Beatriz del Carmen Ramírez Berttolini
Coordinación editorial: Rosa Quintanilla Martínez

Este libro se publica bajo licencia de Creative Commons Atribución-No comercial-Compartir Igual 4.0 Internacional. CC BY-NC-SA 4.0» https://creativecommons.org/licenses/by-nc-sa/4.0/deed.es

Queda prohibida la reproducción parcial o total, por cualquier medio, del contenido de la presente obra, sin contar con autorización por escrito de los titulares de los derechos de autor.
El contenido de este libro, así como su estilo y las opiniones expresadas en él, son responsabilidad de los autores y no necesariamente reflejan la opinión de la UDLAP.

Editado en México | Edited in Mexico



Índice

Introducción *7*

Capítulo 1 ..... *11*
Monedas, registros y finanzas

Capítulo 2 ..... *71*
Las finanzas descentralizadas (DeFi) y más allá

Capítulo 3 ..... *113*
Ver, advertir, regular o prohibir

Capítulo 4 ..... *141*
Grupos, conjeturas y recomendación

Epílogo *171*

Referencias *177*

Páginas web consultadas *189*

Glosario *193*

Anexo 1 ..... *203*
Bitcoin y bitcoin

Anexo 2 ..... *217*
Ethereum y ether

Anexo 3 ..... *227*
Solana y SOL

Anexo 4 ..... *233*
Tecnología de registros distribuidos (TRD)
y cadenas de bloques

Introducción

La primera transacción en criptomonedas a través de internet, por un monto de diez bitcoins, se realizó en 2009. Desde entonces, esta primera criptomoneda ha mantenido una política monetaria fija (limitada) y predeterminada, acompañada de una tecnología de registros distribuidos (cadena de bloques) *especializada* que le ha conferido altos niveles de seguridad. En 2015 surgió Ethereum, con una cadena de bloques *general* que ha logrado una gran cantidad de aplicaciones descentralizadas, respaldadas por una política monetaria sin límite máximo para su moneda, el ether. Este proyecto ha servido de base para una serie de aplicaciones que imitan e innovan numerosos productos y servicios financieros. A este conjunto de programas informáticos es al que, desde 2018, un grupo de desarrolladores ha denominado *finanzas descentralizadas*, concepto que la gran mayoría de los estudios abrevian como DeFi, sigla formada a partir de las dos primeras palabras del término en inglés *descentralized finance*.

Todo esto se desarrolló en Estados Unidos. Bitcoin transmitía el mensaje de que su moneda (el bitcoin) tenía la intención de sustituir al dólar estadounidense, mientras que Ethereum planteaba la sustitución de los intermediarios financieros tradicionales, particularmente en el contexto de aversión pública que definió al mundo que emergió de la crisis financiera occidental de 2007 a 2009, comúnmente asociada al colapso del banco de inversión Lehman Brothers y a movimientos sociales como la «toma de Wall Street» (*occupy Wall Street*).

Uno de los símbolos más reconocidos de la moneda de curso legal de Estados Unidos es el billete de un dólar, cuyo reverso lleva la inscripción *In God We Trust* (en Dios confiamos). Antes del predominio del dólar, se solía decir *In gold we trust* (confiamos en el oro). Hoy resulta evidente que el Bitcoin es un activo virtual y no una moneda de pago capaz de escalar a nivel global; aun así, muchas de las personas que lo respaldan emplean el lema

«en Bitcoin creemos». Otros, retomando planteamientos de autores como el abogado y político estadounidense Lawrence Lessig, argumentan que es más apropiado decir «confiamos en los códigos del ciberespacio», «nos fiamos de las matemáticas», «en la criptografía confiamos» o «en el *software* y el internet». Los autores de este libro confían en que el lector cuente con los elementos necesarios para formarse su propio criterio, en el entendido de que estas posturas no son necesariamente excluyentes entre sí.

Ya sea mediante encuestas o a través de herramientas actuales de minería de datos, puede corroborarse que, tanto en Estados Unidos como en México y en muchos otros países, la gran mayoría de las personas ha oído hablar de Bitcoin; aproximadamente la mitad conoce Ethereum, y prácticamente nadie está familiarizado con el concepto de finanzas descentralizadas. Esto nos ha convencido de que es necesario un manuscrito que explique las DeFi y que, además, esté enfocado en el contexto mexicano.

Los servicios financieros disponibles en México son variados y, en su mayoría, son ofrecidos por empresas *reguladas de manera integral* dentro de un sistema en el que predominan las instituciones bancarias. Recientemente, también se ha tenido acceso a aplicaciones informáticas que ofrecen servicios financieros sin contar con licencia para operar en el país, pero que son *regulados parcialmente* al clasificarse como actividades vulnerables. De las 16 actividades existentes, el intercambio de activos virtuales fue, durante el primer semestre de 2025, la más vulnerable.

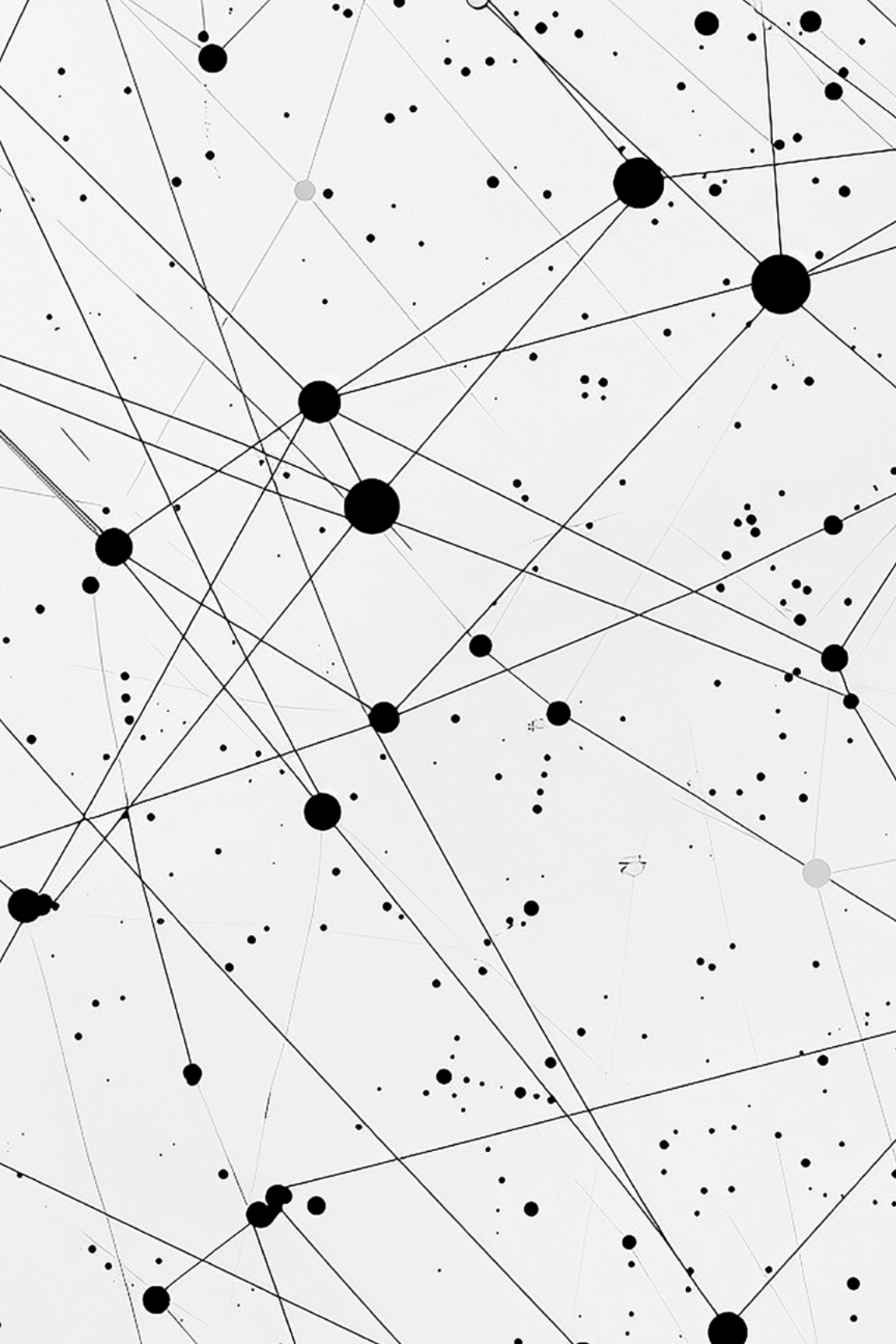
Al menos en teoría, algunos de estos servicios descentralizados han experimentado un proceso de recentralización formal a partir de 2018, con la promulgación de la Ley para Regular las Instituciones de Tecnología Financiera (Ley Fintech) y con las adiciones a la Ley Federal para la Prevención e Identificación de Operaciones con Recursos de Procedencia Ilícita (Ley Antilavado).

Cada una de estas opciones presenta ventajas y desventajas, por lo que corresponde al usuario decidir si combina ambos tipos de servicios o si se concentra en uno de ellos. Independientemente de la decisión que se adopte, resulta fundamental promover la educación financiera desde la escuela primaria hasta la universidad, con el fin de facilitar la toma de decisiones fundamentadas.

Este volumen busca mantener un equilibrio razonable entre la teoría y la práctica de los servicios financieros; por ello, describe tanto las bases tecnológicas que los sustentan como las aplicaciones informáticas que utilizan los usuarios.

En el primer capítulo, el lector encontrará material para comprender las características del sistema financiero mexicano formal, así como el entorno de los servicios descentralizados y el concepto de monedas estables (*stablecoins*). El segundo capítulo no solo presenta la definición y alcance de las finanzas descentralizadas, sino que también las distingue de las instituciones de tecnología financiera (*fintech*) y de las grandes empresas que encabezan las tecnologías de la información y la comunicación (*bigtech*). En el tercer capítulo se analiza la situación normativa, tanto en el ámbito nacional como en el internacional. Finalmente, en la cuarta parte se describen los principales grupos de interés, se plantean algunas conjeturas y se reitera la recomendación de que es necesaria más y mejor educación para tomar decisiones. Los aspectos más técnicos son descritos en los cuatro anexos incluidos al final del volumen. El contenido se complementa con un glosario de términos, diseñado para facilitar la comprensión.

Advertencia: en este documento se hace referencia a instituciones e instrumentos financieros específicos, así como a activos virtuales, criptomonedas o criptoactivos. Se aclara que dichas menciones tienen exclusivamente fines educativos o académicos y no deben interpretarse como respaldo, apoyo, aprobación o asesoría para realizar inversión alguna. Este volumen no incluye ejercicios al final de cada capítulo y, en sentido estricto, no se considera un libro de texto. El manuscrito se concluyó el 8 de enero de 2026.



Capítulo 1

Monedas, registros y finanzas

La *base monetaria* en México está compuesta por dos partes. En primer lugar, contiene los billetes y monedas en circulación que están en poder del público, así como los que se ubican en las cajas de los bancos. En segundo lugar, se encuentran los depósitos en cuenta corriente que los bancos múltiples y de desarrollo tienen en el Banco de México (Banxico). Toda esta base opera en pesos, que son considerados como nuestra moneda de curso legal. En este proceso participa tanto el sector público —representado por el Banco de México (Banxico) y la Secretaría de Hacienda y Crédito Público (SHCP)— como el sector privado a través de los bancos múltiples, que se encuentran altamente regulados.

Desde hace poco más de quince años circulan en internet, en formato digital, otras formas de monedas virtuales, que no son consideradas de curso legal. Su objetivo original es eliminar intermediarios, ya que operan entre pares y usan criptografía para funcionar de manera anónima. Sus creadores las llaman *criptomonedas*; no obstante, las autoridades las clasifican como activos virtuales o criptoactivos y, debido a los riesgos asociados a su operación, han emitido advertencias reiteradas sobre su uso.

Históricamente, los registros —ya sea mediante sistemas de partida simple o doble— se han realizado de forma centralizada, como puede corroborarse a través de la credencial del Instituto Nacional Electoral (INE), la expedición del acta de nacimiento, el título universitario o el expediente de salud del doctor u hospital que se frecuente.

En este contexto, el dinero actúa como facilitador de las operaciones comerciales, es decir, de las negociaciones mediante las cuales las personas intercambian bienes y servicios. Esta función resulta fundamental para comprender las finanzas, entendidas como el intercambio de distintas formas de dinero. Sin ello, las finanzas no existirían.

En este primer capítulo se analizan tanto los sistemas de servicios centralizados como los descentralizados, así como las combinaciones y relaciones que actualmente existen entre estos dos mecanismos diametralmente opuestos.

El sistema financiero formal o tradicional de México

En la actualidad, los servicios financieros predominantes son aquellos que se obtienen a través de alguna de las 53 instituciones privadas de banca

múltiple autorizadas en México. El número de cuentas de captación supera ampliamente al de créditos, y la operación bancaria se realiza mediante miles de sucursales físicas, cuyo número continúa disminuyendo como consecuencia de la digitalización de los servicios financieros. Algunas de estas instituciones cuentan con una trayectoria que se remonta a siglos atrás y cuyos modelos han evolucionado a partir de regulaciones como las impulsadas por José Yves Limantour, titular de la Secretaría de Hacienda y Crédito Público entre 1893 y 1911. Otras, en cambio, se han constituido recientemente como bancos íntegramente digitales, sin sucursales físicas.

Como se muestra en la tabla 1, la banca múltiple representaba el 41.32 % del total de los activos del sector financiero a finales de septiembre de 2025. Existe una elevada concentración en este subsector, ya que cinco de las 53 instituciones representan el 60 % de dicho 41.32 %. De estos cinco bancos, solo uno es considerado totalmente mexicano; los cuatro restantes forman parte de conglomerados financieros con sede en Estados Unidos, Inglaterra y España. En cualquier caso, los cinco son considerados bancos sistémicamente importantes conforme a los criterios establecidos por el Banco de Pagos Internacionales (BIS, por sus siglas en inglés), y por ello, algunos reguladores e investigadores los califican como «demasiado grandes para caer». Estas cinco instituciones cuentan con infraestructura física en gran parte del territorio nacional y forman parte de los 21 grupos financieros autorizados por la Ley para Regular las Agrupaciones Financieras de 1990, reformada en enero de 2014. Conforme al artículo 12 de dicha ley, cada grupo financiero está integrado por una sociedad controladora y al menos dos entidades adicionales, provenientes de un listado que incluye bancos múltiples, casas de bolsa, instituciones de tecnología financiera, sociedades financieras populares, sociedades operadoras de fondos de inversión, administradoras de fondos para el retiro o sociedades financieras de objeto múltiple.

Asimismo, existen seis instituciones de banca de desarrollo, propiedad del Estado, constituidas como sociedades nacionales de crédito conforme al modelo introducido durante el periodo de la banca nacionalizada, entre 1982 y 1991. El tercer párrafo del artículo 30 de la Ley de Instituciones de Crédito de 2025 establece que

> *Las instituciones de banca de desarrollo tienen como objetivo fundamental facilitar el acceso al crédito y los servicios financieros a personas físicas y morales, así como proporcionales asistencia*

técnica y capacitación en términos de sus respectivas leyes orgánicas con el fin de impulsar el desarrollo económico. (p. 39)

Para los autores de este texto, dicho objetivo debería instrumentarse a través del otorgamiento de créditos contracíclicos a la banca múltiple, así como mediante la provisión de financiamiento de largo plazo. Al cierre del tercer trimestre de 2025, este grupo de instituciones —sin considerar los fideicomisos de fomento FIRA, FOVI y FIFOMI— representaba el 8.12 % del total de los activos del sistema financiero.

Desde principios de este siglo, México cuenta con una Ley de Ahorro y Crédito Popular, de la cual derivan 33 Sociedades Financieras Populares (Sofipo) y 153 Sociedades Comunitarias, también llamadas Cooperativas de Ahorro y Préstamo (Socap). Estas instituciones cumplen una función social importante; sin embargo, hasta la fecha representan una proporción reducida del total de activos del sector financiero (1.39 %).

La suma de la banca múltiple, la banca de desarrollo y las instituciones derivadas de la Ley de Ahorro y Crédito Popular representa el 50.83 % del total de activos, lo que permite afirmar que el sector bancario mantiene una posición mayoritaria dentro del sistema financiero mexicano. El Banco de México, al igual que muchos bancos centrales del mundo occidental, también forma parte del sector; no obstante, no se incluye en esta sección y será discutido en la siguiente.

En segundo lugar se encuentran los servicios vinculados con los sistemas de ahorro para el retiro de los trabajadores, tanto del sector privado (IMSS) como del sector público (ISSSTE). Actualmente operan diez Administradoras de Fondos para el Retiro (AFORE), apoyadas por numerosas Sociedades de Inversión Especialidades de Fondos para el Retiro (SIEFORE). Este sistema administra más de 76 millones de cuentas, con activos netos de las SIEFORE de 8.06 billones de pesos, lo que equivale al 21.68 % del total de los activos del sistema financiero.

Este panorama se complementa con los fondos de inversión y las casas de bolsa. Los primeros tienen como objetivos principales la adecuada diversificación del riesgo y el acceso al mercado de valores para inversionistas pequeños y medianos. Se constituyen como sociedades anónimas cuyas acciones representan su capital social y, aunque no cotizan en bolsa, deben estar inscritas en el Registro Nacional de Valores que administra la Comisión Nacional Bancaria y de Valores (CNBV). Por esta razón, la Ley del Mer-

cado de Valores los considera valores. Estos fondos se enfocan en instrumentos de deuda o de renta variable y, en algunos casos, en el financiamiento de empresas con alto potencial de crecimiento. Son administrados por 31 sociedades operadoras de fondos de inversión, cuya función es mitigar posibles conflictos de interés entre accionistas y administradores. En total, existen 631 fondos cuyos activos representan el 13.18 % del total del sector financiero mexicano. Desde diciembre de 2023, tras las reformas legales correspondientes, también se permite la operación de fondos de inversión de cobertura (*hedge funds*), los cuales pueden asumir posiciones largas o cortas y están dirigidos a inversionistas sofisticados.

El subsector bursátil incluye 36 casas de bolsa, que son el conducto para que los inversionistas puedan acceder a las dos bolsas de valores que operan en México: la Bolsa Mexicana de Valores (BMV) y la Bolsa Institucional de Valores (BIVA). Históricamente, el número de cuentas administradas por las casas de bolsa era reducido y requería montos mínimos elevados; sin embargo, en años recientes su crecimiento ha sido notable, principalmente por las aplicaciones digitales y regulaciones más favorables para los inversionistas minoristas. Entre marzo de 2022 y septiembre de 2025, el número de cuentas pasó de 3.7 a 22.4 millones. Los activos administrados por las casas de bolsa representaban el 3.23 % del total del sector.

Es importante mencionar el caso de Mercado Libre y su brazo financiero, Mercado Pago, que en asociación con la casa de bolsa GBM permitieron la apertura de cuentas de inversión desde montos tan bajos como cien pesos a partir de 2020. De los 22.4 millones de cuentas reportadas en septiembre de 2025, 21.5 millones —equivalentes al 96 %— correspondían a GBM. Hay que felicitar a GBM por democratizar el mercado bursátil, pero al mismo tiempo hay que notar que, pese a administrar el 96 % de las cuentas, solo obtuvo el 1.9 % de las utilidades totales durante el primer semestre de 2025. En contraste, la casa de bolsa Inversora Bursátil (Inbursa), con 9,580 cuentas —el 0.05 % del total—, concentró el 11.2 % de las ganancias.

En tercer lugar se sitúan los servicios de seguros y fianzas. A través de las compañías aseguradoras y mediante el pago de una prima, las personas pueden transferir riesgos asociados a su integridad física o a sus bienes materiales, los cuales pueden o no materializarse. De igual forma, las instituciones de fianzas permiten contratar pólizas que garantizan el pago o el cumplimiento de determinadas obligaciones. En conjunto, existen 113

instituciones de seguros y fianzas, cuyos activos representan el 8.02 % del total del sistema financiero.

También es necesario mencionar los servicios derivados de la Ley General de Organizaciones y Actividades Auxiliares del Crédito (LGOAAC). Los almacenes generales de depósito y las uniones de crédito constituyen las dos organizaciones contempladas en este marco normativo y representan el 0.08 % y el 0.19 % de los activos totales del sistema financiero. Las actividades auxiliares están representadas por tres categorías. La primera, y la de mayor relevancia, corresponde a la realización habitual y profesional de operaciones de crédito, arrendamiento o factoraje financiero. Para ello se requiere establecer una sociedad financiera de objeto múltiple (Sofom), la cual debe contar con registro ante la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (Condusef). Algunas de estas sociedades se consideran reguladas por mantener vínculos de carácter patrimonial con bancos múltiples, sociedades financieras populares o sociedades de ahorro y préstamo (Socap). La tabla 1 muestra que existen 21 sociedades que no consolidan con sus respectivos grupos financieros o que emiten deuda en los mercados de valores; en conjunto, sus activos representan el 0.95 % del total del sistema. Las Sofom que no cumplen con dichos criterios se clasifican como no reguladas. No obstante, estas entidades están sujetas a la inspección y vigilancia de la Comisión Nacional Bancaria y de Valores (CNBV) exclusivamente para verificar el cumplimiento de las disposiciones en materia de prevención de lavado de dinero y financiamiento al terrorismo. El conjunto de las 2,145 Sofom no reguladas concentra el 1.72 % del total de activos del sistema financiero.

La segunda actividad auxiliar del crédito corresponde a los servicios prestados por las casas de cambio autorizadas, las cuales registraban activos por 943 millones de pesos al cierre del tercer trimestre de 2025, equivalente al 0.003 % del total. El hecho de que la tabla 1 exprese los activos en billones de pesos y que la columna de porcentajes incluya únicamente dos decimales provoca que estos valores aparezcan redondeados a cero.

La tercera y última actividad auxiliar del crédito requiere solo del registro de la sociedad ante la CNBV para operar como transmisor de dinero o centro cambiario. Los transmisores de dinero reciben recursos en moneda nacional o extranjera para su transferencia electrónica, ya sea al extranjero o dentro del territorio nacional, o bien para su entrega en una sola exhibición al beneficiario designado en un lugar específico. Por estos servicios reciben, como contraprestación, una comisión, beneficio o ganancia. Algo similar ocurre con los centros cambiarios que operan de manera física y no

Tabla 1. Estructura del sistema financiero de México (al 30 de septiembre de 2025)

Instituciones	Número	Activos totales (billones de pesos)	% del total
Banca múltiple	53	15.36	41.32
Banca de desarrollo	6	3.02	8.12
Soc. coop. de ahorro y préstamo	153	0.31	0.83
Soc. fin. populares (Sofipo)	33	0.21	0.56
Subtotal bancos + ahorro y préstamo	**245**	**18.90**	**50.83**
Fondos de pensiones (SIEFORE)	118	8.06	21.68
Fondos de inversión	631	4.90	13.18
Casas de bolsa	36	1.20	3.23
Subtotal de fondos + bursátil	**785**	**14.16**	**38.09**
Subtotal de seguros y fianzas	**113**	**2.98**	**8.02**
Almacenes generales de depósito	14	0.03	0.08
Uniones de crédito	62	0.07	0.19
Sofomes reguladas	21	0.35	0.95
Sofomes no reguladas	2,145	0.64	1.72
Casas de cambio	7	0.00	0.00
Centros cambiarios	695	0.00	0.00
Transmisores de dinero	88	0.00	0.00
Subtotal LGOAAC	**3,032**	**1.09**	**2.94**
Instituciones de tecnología financiera	88	0.04	0.10
Total	**4,263**	**37.17**	**100.0**

Fuente: elaboración propia con datos y reportes de Banxico, SHCP, CNBV, CNSF, CONSAR y Condusef.

Nota: en algunos casos, no se encontraron disponibles los datos correspondientes a finales de septiembre de 2025; por ello, se consideraron los más próximos a esta fecha. En otros casos —como en el de las instituciones de tecnología financiera— se usaron datos de diciembre de 2023. Un billón de pesos mexicanos es igual a un millón de millones; es decir, un uno seguido de doce ceros. Las sumas no necesariamente coinciden con el total por efectos del redondeo.

electrónica. No se han identificado datos sobre los activos de los transmisores de dinero ni de los centros cambiarios; por ello, se asume que no superan los de las casas de cambio y, en consecuencia, también se reflejan como ceros en la tabla.

Por su importancia, conviene retomar la primera actividad auxiliar de crédito prevista en la LGOAAC (el otorgamiento de crédito, el arrendamiento y el factoraje financiero) para reiterar que dichas operaciones pueden realizarse de manera habitual y profesional a través de cualquier Sofom que cuente con registro vigente ante la Condusef. Una vez constituidas como sociedades anónimas ante notario, las Sofom deben especificar si se trata de una entidad regulada (ER) o de una entidad no regulada (ENR). Cabe señalar que las ER suelen obtener sus recursos mediante la emisión pública de valores de deuda inscritos en el Registro Nacional de Valores, conforme a la Ley del Mercado de Valores. En contraste, las ENR se financian principalmente con el capital inicial de sus fundadores y mediante financiamiento privado, a través de pagarés quirografarios de corto plazo que pagan una tasa de interés específica. En el caso de una Sofom no regulada dedicada al otorgamiento de crédito, se esperaría que la tasa pagada a sus acreedores fuera inferior a la tasa promedio que cobra a las pequeñas y medianas empresas; de lo contrario, su modelo de negocio resultaría insostenible en el mediano plazo.

Lo anterior es importante, ya que en 2025 se registraron numerosos casos de Sofom no reguladas que incumplieron con el pago de interés y capital, cuyos propietarios o administradores desaparecieron con los recursos captados, o que operaron con esquemas de tipo piramidal con funcionamiento temporal.

Si una Sofom no regulada ofrece una tasa del 28 % anual mediante un pagaré quirografario, cuando la tasa libre de riesgo —representada por los certificados de la Tesorería de la Federación— se sitúa en torno al 7 %, resulta evidente que a mayor tasa de interés corresponde un mayor riesgo esperado. Si la inversión fracasa y no se recupera el capital, conviene recordar la máxima de la sabiduría convencional: si la tasa de interés o de rendimiento financiero parece ser demasiado buena para ser verdad, existe una alta probabilidad de que sea un engaño o una estafa. En términos coloquiales, «todo iba bien hasta que algo salió mal», ya sea porque la empresa entró en concurso mercantil o porque sus dueños desaparecieron. Los autores de este libro consideran que las autoridades financieras deben establecer reglas más estrictas y una supervisión más eficaz para minimizar este tipo de situaciones, tanto en las entidades no reguladas o sujetas

únicamente a registro, como en el ámbito de las criptomonedas que se analizan en esta obra.

El penúltimo renglón de la tabla 1 incluye 88 instituciones de tecnología financiera autorizadas por la CNBV, previo acuerdo del comité interinstitucional integrado por dos representantes de la SHCP, dos de Banxico y dos de la CNBV. Con base en información del Banco de México de diciembre de 2025, existen 61 instituciones de fondos de pago electrónico (IFPE) y 27 instituciones de financiamiento colectivo (IFC). El último reporte disponible de la CNBV, correspondiente a diciembre de 2023, señala que los activos de estas instituciones de tecnología financiera ascendían a 36,445 millones de pesos, lo que representaba el 0.10 % del total general. Resulta relevante destacar que la iniciativa de Ley de Ingresos de la Federación para 2026, presentada al Congreso de la Unión el 8 de septiembre de 2025, propone que las instituciones de financiamiento colectivo cumplan con la obligación de retener y enterar el impuesto sobre la renta y el impuesto al valor agregado, correspondientes a las operaciones en las que participan como intermediarias. Esta propuesta busca eliminar el trato diferenciado que han tenido respecto de sus competidores en los mercados de ahorro e inversión, con el objetivo de establecer condiciones de competencia equitativas entre las instituciones de tecnología financiera y las entidades tradicionales que realizan funciones similares.

Los rubros y datos presentados en la tabla 1 pueden complementarse con las actividades de supervisión que realiza la CNBV. Esto resulta particularmente relevante en el sector bursátil, donde no se incluyen las dos bolsas de valores que operan en el país —la BMV y la BIVA— ni el Mercado Mexicano de Derivados (MexDer). La omisión obedece a que estas entidades se consideran organismos autorregulatorios, encargados de establecer estándares de operación y conducta entre sus miembros, mientras que la CNBV se limita a emitir disposiciones de carácter general y, en su caso, a otorgar reconocimiento oficial. Lo mismo sucede con las contrapartes centrales de valores y de derivados (CCV y Asigna).

Tampoco se incluyen las más de 500 emisoras listadas en ambas bolsas, los asesores en inversiones (153), las instituciones calificadoras de valores (seis), los participantes en redes de medios de disposición (142), las sociedades de información crediticia (tres), ni la Institución para el Depósito de Valores (Indeval). Si estas entidades, junto con otras como los proveedores de precios, se sumaran a las 4,263 instituciones que figuran en la tabla 1, podría afirmarse que la CNBV supervisa, ya sea de manera integral o úni-

camente en materia de prevención de lavado de dinero, cerca de 5,000 instituciones, agrupadas en más de 70 figuras jurídicas.

En resumen, el sistema financiero mexicano está dominado por intermediarios, entre los que destacan los bancos múltiples y las compañías de seguros; sin embargo, también cuenta con diferentes mercados, especialmente los accionarios, los de deuda y los de derivados. Es decir, México cuenta con un sistema financiero integral, con intermediarios y mercados orientados a captar el ahorro de las personas y canalizarlo hacia inversiones productivas.

Como se desprende de la tabla 1, las autoridades financieras suelen evaluar el peso relativo de cada institución con base en sus activos en un momento determinado, lo cual equivale a tomar como referencia su balance general. Si bien este enfoque es válido, no constituye la única alternativa de análisis. Para obtener una visión más completa, es necesario complementar esta perspectiva con información proveniente del estado de resultados, en particular las utilidades o pérdidas netas de las instituciones y los mercados. Dicho enfoque permitiría aproximarse al valor agregado de los servicios financieros dentro del cálculo de la producción de bienes y servicios del país.

Finalmente, resulta llamativo que, de acuerdo con datos del Instituto Nacional de Estadística y Geografía (INEGI), el producto interno bruto (PIB) de México, anualizado al tercer trimestre de 2025 y a precios corrientes, haya ascendido a 35.19 billones de pesos. Esta cifra es porcentualmente cercana a los 37.17 billones del total de los activos financieros consignados en la tabla 1, lo que significa que el sistema financiero mexicano equivale a un porcentaje ligeramente superior (alrededor del 5 %) del PIB. Esto sitúa a México en una posición relativamente baja en el contexto internacional. Basta mencionar el caso de Estados Unidos, cuyo sistema financiero alcanza un tamaño cercano a cinco veces el valor de su PIB. Además de ser uno de los sistemas financieros más grandes y líquidos del mundo, se apoya principalmente en los fondos de inversión y no en las instituciones bancarias, como ocurre en México. En este sentido, puede afirmarse que el país cuenta con un sistema financiero de dimensiones relativamente reducidas.

Las autoridades financieras en México

Algunas de las fuentes de las que emanan las autoridades financieras mexicanas tienen su origen en el siglo pasado, mientras que otras surgieron después de la crisis financiera de 2008. Entre estas últimas destaca el Consejo de Estabilidad Financiera (FSB, por sus siglas en inglés), de alcance internacional creado en la Cumbre del G20 celebrada en Londres en 2009, con una secretaría de dimensiones reducidas ubicada en la sede del Banco de Pagos Internacionales (BIS, por sus siglas en inglés). Esta configuración ha dado lugar a una red de seguridad financiera y monetaria que, en gran parte del mundo occidental, incluye un regulador, un supervisor, un prestamista de última instancia, un liquidador y una entidad encargada de garantizar los depósitos.

Estos elementos han moldeado la regulación prudencial del sistema financiero nacional, cuya arquitectura se ha estructurado en torno al modelo conocido como torres o picos gemelos (*twin peaks plus*), acompañado de la creación, en 2010, de un Consejo de Estabilidad Financiera (CEF) de carácter nacional, cuyo objetivo es coordinar esfuerzos para prevenir interrupciones y alteraciones en el funcionamiento del sistema.

En México, de manera directa o indirecta, todos los servicios financieros mencionados son autorizados, regulados, supervisados, vigilados y, en su caso, sancionados por dos entidades del Estado mexicano: (a) la autoridad financiera, representada por la Secretaría de Hacienda y Crédito Público, y (b) la autoridad monetaria, representada por el Banco de México.

La SHCP, como su nombre lo indica, se encarga del crédito del Gobierno federal, pero también de los asuntos relacionados con el sistema financiero, como la autorización de la entrada de instituciones, la delimitación de sus actividades, su regulación prudencial y su posible salida del mercado. Estas funciones se ejercen de manera directa a través de sus unidades administrativas, entre las que destacan la Unidad de Banca, Valores y Ahorro (UBVA), la Unidad de Banca de Desarrollo (UBD), la Unidad de Seguros, Pensiones y Seguridad Social (USPSS) y la Unidad de Inteligencia Financiera (UIF). Asimismo, la SHCP se apoya de forma directa en sus organismos desconcentrados e indirectamente en organismos descentralizados de la Administración Pública Federal.

La diferencia fundamental entre los organismos descentralizados y los desconcentrados radica en que los primeros cuentan con personalidad jurídica y patrimonio propios. La SHCP tiene cuatro entes desconcentrados:

la Comisión Nacional Bancaria y de Valores (CNBV), la Comisión Nacional del Sistema de Ahorro para el Retiro (Consar), la Comisión Nacional de Seguros y Fianzas (CNSF) y el Servicio de Administración Tributaria (SAT). Además, ejerce una influencia significativa sobre dos organismos descentralizados de la Administración Pública Federal: la Comisión Nacional para la Defensa de los Usuarios de los Servicios Financieros (Condusef) y el Instituto para la Protección al Ahorro Bancario (IPAB). Dicha influencia es más marcada en la Condusef, donde la SHCP participa en la Junta de Gobierno con cuatro o más miembros de un total de ocho, y menor en el IPAB, donde, en teoría, ocupa dos de siete posiciones, aunque en la práctica ejerce dos de cinco, debido a que no se han designado dos de los cuatro vocales independientes.

Siguiendo el ejemplo de otros bancos centrales, como el Banco de Suecia (1668) y el Banco de Inglaterra (1694), el Banco de México inició operaciones en 1925 como una sociedad anónima con mayoría estatal y participación privada, con el propósito de cumplir lo dispuesto en el artículo 28 de la Constitución de 1917, que establecía la existencia de un banco único de emisión de moneda. Con ello se puso fin a la diversidad de instituciones privadas emisoras de billetes, consolidada bajo el modelo impulsado por José Yves Limantour en la Ley General de Instituciones de Crédito de 1897, y se reservó la facultad de emisión a una entidad bajo control estatal. En sus primeros años, el Banco de México combinó la función emisora con el otorgamiento de crédito, como cualquier banco comercial. Con el tiempo, dejó de conceder crédito al público y evolucionó hacia una institución plenamente pública, concentrada solo en la emisión de moneda, con autonomía, mandato, y funciones bien definidas. La Ley Monetaria de los Estados Unidos Mexicanos estableció en 1931 que la unidad del sistema monetario sería el peso y que las únicas monedas circulantes serían los billetes del Banco de México y las monedas metálicas acuñadas por la Casa de Moneda de México.

Desde 1905, el gobierno desmonetizó la plata y, en 1931, hizo lo mismo con el oro, por lo que la emisión de monedas y billetes en México dejó de tener equivalencia con metales preciosos. En consecuencia, el peso no cuenta con respaldo metálico, sino con el sustento jurídico de la Constitución y con las reservas internacionales de Banxico. El peso es la moneda oficial de México y tiene curso legal, es decir, de manera oficial, el pago de impuestos y deudas solo se puede llevar a cabo con el mismo. Al haber sido establecida por decreto, se le denomina *dinero fíat* (del latín *fiat*, 'hágase'), aunque también se utiliza el término *dinero fiduciario* (del latín *fides*, fe o confianza). En cualquier escenario, nuestro sistema monetario es el peso

y, al igual que todas las monedas del mundo, no tienen respaldo alguno, más que la promesa de pago de las entidades emisoras.

El México independiente heredó un sistema monetario bimetálico, basado en monedas de oro y plata y en billetes respaldados por dichos metales. Este sistema desapareció a principios de la década de 1930 y, desde entonces, el peso opera como moneda fíat. No se considera conveniente llamarla fiduciaria debido a los episodios de alta inflación que hemos vivido en el pasado, aunque este fenómeno ha mejorado desde que Banxico obtuvo su autonomía en 1994. Esto significa que ninguna autoridad puede ordenar al banco conceder financiamiento, lo que reduce la posibilidad de que intereses políticos interfieran con el interés público. La reforma al artículo 28 constitucional también estableció con claridad su objetivo primario: procurar la estabilidad del poder adquisitivo de la moneda, así como un esquema de nombramiento por periodos escalonados de personas designadas por el presidente de la República y aprobados por el Senado. Hasta la fecha, prevalece la emisión exclusiva de billetes por parte del Banco de México y de acuñación de monedas por parte de la Casa de Moneda de México, organismo descentralizado de la Administración Pública Federal, que actúa conforme a las órdenes de Banxico.

La Ley del Banco de México vigente (2014), en su segundo artículo, establece como finalidad:

> *proveer a la economía del país de moneda nacional. En la consecución de esta finalidad tendrá como objetivo prioritario procurar la estabilidad del poder adquisitivo de dicha moneda. Serán también finalidades del Banco promover el sano desarrollo del sistema financiero y propiciar el buen funcionamiento de los sistemas de pago. (p. 1)*

Para analizar si el Banco de México ha cumplido con su función prioritaria entre 1994 y 2025, se compara la tasa de inflación fijada como meta cada año con la realmente obtenida. De los 32 años transcurridos, Banxico ha cumplido con la meta en 15 ocasiones y ha fallado en los 17 restantes. Corresponde al lector valorar si una efectividad del 47 % amerita una calificación aprobatoria. Más allá de esta valoración, la presidenta de México, Claudia Sheinbaum, señaló en su conferencia matutina del 28 de julio de

2025 que «vale la pena discutir si el Banco de México debe ampliar su visión hacia el desarrollo económico», además de cumplir con su mandato constitucional de estabilidad de precios. De manera llamativa, un mes después, en la conferencia matutina del 28 de agosto de 2025, fue nuevamente cuestionada sobre la posibilidad de un objetivo dual para Banxico y contestó: «No estamos pensando en ello», aunque manifestó su interés en un mayor acceso al crédito y en condiciones de financiamiento más favorables para las empresas. Los autores de este libro consideran acertado este repliegue, pues si al banco central le resulta complejo cumplir con un solo mandato, asignarle uno adicional podría resultar contraproducente.

Tabla 2. La inflación desde la autonomía del Banco de México

Año	% de inflación	Meta (%)	Evaluación
1994	7.05	5.00	No cumplió
1995	51.97	42.00	No
1996	27.70	20.50	No
1997	15.72	15.00	No
1998	18.61	12.00	No
1999	12.32	13.00	Sí cumplió
2000	8.96	10.00	Sí
2001	4.40	6.50	Sí
2002	5.70	4.50	No
2003	3.98	3 ± 1	Sí
2004	5.19	3 ± 1	No
2005	3.33	3 ± 1	Sí
2006	4.05	3 ± 1	No
2007	3.76	3 ± 1	Sí
2008	6.53	3 ± 1	No
2009	3.57	3 ± 1	Sí
2010	4.40	3 ± 1	No
2011	3.82	3 ± 1	Sí
2012	3.57	3 ± 1	Sí
2013	3.97	3 ± 1	Sí

Tabla 2. La inflación desde la autonomía del Banco de México (continuación)

Año	% de inflación	Meta (%)	Evaluación
2014	4.08	3 ± 1	No
2015	2.13	3 ± 1	Sí
2016	3.36	3 ± 1	Sí
2017	6.77	3 ± 1	No
2018	4.83	3 ± 1	No
2019	2.83	3 ± 1	Sí
2020	3.15	3 ± 1	Sí
2021	7.36	3 ± 1	No
2022	7.82	3 ± 1	No
2023	4.66	3 ± 1	No
2024	4.21	3 ± 1	No
2025	3.69	3 ± 1	Sí

Fuente: elaboración propia con datos de Banxico y el INEGI.

El Banco de México pone en circulación los billetes y monedas principalmente a través de las instituciones de banca múltiple, las cuales son reguladas y supervisadas por el Estado mediante la SHCP y el propio banco central, conforme a la Ley de Instituciones de Crédito. Este mecanismo constituye un ejemplo claro de colaboración público-privada en el funcionamiento del sistema financiero.

La emisión de moneda es un prerrequisito fundamental para los servicios financieros en particular y para las finanzas en general, ya que, en la actualidad, sin moneda o dinero no hay finanzas (dinero por dinero). En este libro se consideran sinónimos los términos *moneda* y *dinero*. Los antecedentes legales que sustentan esta afirmación se detallan en el capítulo 3.

Como es sabido, las monedas y los billetes en circulación constituyen la forma primaria del dinero y se utilizan para realizar operaciones en efectivo dentro de la economía. Una de sus principales ventajas es que permiten efectuar transacciones de manera anónima, lo que las distingue de otras formas de dinero basadas en depósitos bancarios: a la vista (M1), a plazo (M2), en reportes con valores públicos (M3, véase el glosario) y en

operaciones con no residentes (M4). En resumen, los billetes y monedas puestos en circulación, junto con los depósitos a la vista, conforman el primer agregado monetario (M1), que se define como dinero. Para ubicarlos dentro del conjunto de agregados monetarios —ordenados según su grado de liquidez—, los datos del Banco de México muestran que, en septiembre de 2025, estos sumaron 21.11 billones de pesos, lo que representaba el 39 % del M1, el 37 % del M2, el 15 % del M3 y el 9 % del M4.

Los sistemas de pagos están estrechamente vinculados con los sistemas financieros, por lo que pueden considerarse conceptos afines; no obstante, conviene reiterar que estos últimos dependen de los primeros para su operación. En términos generales, los instrumentos monetarios se utilizan para el pago de bienes y servicios, mientras que los instrumentos financieros se usan para ahorrar o invertir, ya sea en el corto o en el largo plazo. Desde 2016, el Fondo Monetario Internacional (FMI) diseñó un nuevo manual de estadísticas monetarias y financieras que ha sido adoptado por el Banco de México. Dicho manual no solo presenta los agregados monetarios, sino que, a partir de ellos, construye los activos financieros internos, los cuales incluyen fondos de inversión, acciones bursátiles e instrumentos híbridos en poder de los residentes.

Para dimensionar la importancia del dinero en efectivo en las transacciones, se recurre a los datos trienales de la Encuesta Nacional de Inclusión Financiera (ENIF) 2025. Esta reporta que el 94 % de la población adulta (18 años o más) utilizó efectivo para realizar pagos en establecimientos y plataformas en línea, seguido de las tarjetas físicas (34 %) y de las transferencias o aplicaciones móviles (22 %).

Con excepción de los pagos en efectivo, todos los servicios financieros privados mencionados hasta ahora se consideran centralizados, convencionales, tradicionales o habituales. Estos se realizan siempre a través de una institución financiera altamente regulada y supervisada, la cual funge como un intermediario «confiable». Todas las operaciones se llevan a cabo con las características principales descritas en los siguientes incisos:

a) Se realizan en moneda de curso legal (fíat), y cada uno de los usuarios es identificado mediante nombre y apellidos.

b) Los horarios de operación en formato presencial son limitados: la mayoría de las instituciones abren de lunes a viernes, de 9:00 a 15:00 horas. Con el surgimiento de la banca completamente digital y la incorporación de servicios financieros digitales en la banca con sucursales, una parte de la población puede operar mediante aplicaciones móviles las 24 horas del día, los siete días de la semana, durante todo el año.

c) Los intermediarios pueden negar el servicio financiero a quienes no cumplan con una serie de requisitos, por lo que, en casos necesarios, pueden ser bloqueados o censurados.

d) La custodia del dinero o de los activos financieros de los usuarios es mantenida, en la gran mayoría de los casos, por los intermediarios.

e) Existen ciertos mecanismos de protección al cliente cuando las instituciones intermediarias enfrentan problemas financieros. Destaca el seguro de depósitos bancarios, que cubre hasta 400,000 unidades de inversión (UDI), equivalentes, al momento de redactar estas líneas, a aproximadamente 3.4 millones de pesos.

f) En el caso de que los usuarios no logren resolver de manera bilateral sus diferencias o reclamos con las instituciones proveedoras de servicios, pueden presentar sus quejas ante la Condusef. Finalmente, si estas instancias resultan insuficientes, pueden contratar a un abogado para hacer valer las cláusulas de los contratos o las múltiples leyes que hay en el proceso.

Algunos problemas de los servicios monetarios y financieros formales

La politización del dinero puede provocar hiperinflaciones

Durante la década de 1980, México registró inflaciones muy altas, en tres ocasiones superiores al 100 %. La recurrencia de estos eventos obligó a las autoridades monetarias y financieras a sustituir, entre 1993 y 1996, el peso por el llamado nuevo peso, cuya equivalencia representaba miles de unidades de la moneda anterior. Es decir, en este periodo se eliminaron tres ceros al peso que continúa vigente, aunque con un poder adquisitivo considerablemente menor. Adicionalmente, con el objetivo de eliminar el conflicto de interés que implicaba que el banco central fuera simultáneamente el emisor único de dinero y la instancia encargada de difundir las estadísticas de inflación, esta última función fue transferida al INEGI en 2011.

Inclusión financiera muy limitada

El acceso y uso de los servicios financieros convencionales no ha logrado una inclusión financiera amplia entre la población mexicana. Como se mencionó en la sección anterior, el quinto levantamiento de la Encuesta

Nacional de Inclusión Financiera (ENIF), publicado en 2025 por el INEGI y la CNBV, presenta información correspondiente a la situación prevaleciente en 2024. Al igual que la cuarta edición, este levantamiento amplía el rango de la población objetivo. Mientras que en ediciones anteriores se consideraba a la población de entre 18 a 70 años, la quinta edición incorpora también a las personas de 18 años y más. Por ello, el lector debe tener cautela al interpretar las estadísticas, ya que en algunos casos se emplean datos del grupo de 18 a 70 años y, en otros, del conjunto de 18 años y más.

El principal resultado de la quinta edición indica que el 77 % de las personas de entre 18 a 70 años reportó contar con al menos un producto financiero formal, como cuentas de ahorro, crédito, seguros o fondos de pensiones. Si bien esta cifra supera el 68 % reportado en 2015, aún deja fuera del sistema formal al 23 % de ese grupo poblacional, lo que, según estimaciones de los autores, equivale a aproximadamente 22 millones de personas. Esta falta de acceso refleja una infraestructura financiera limitada, que se traduce en un número insuficiente de sucursales bancarias, cajeros automáticos, terminales, puntos de venta y aplicaciones móviles. Se espera que las oportunidades derivadas de las finanzas digitales puedan acelerar el proceso de inclusión financiera, como ya ha ocurrido con la apertura de cuentas para inversionistas minoristas por parte de algunas casas de bolsa.

La presidenta de México, Claudia Sheinbaum, abordó el tema de la baja inclusión financiera durante su discurso de inauguración de la 88ª Convención Bancaria, celebrada el 8 de mayo de 2025 en Nuevo Vallarta, Nayarit, ante representantes de la Asociación de Bancos de México (ABM). En su exposición presentó una lámina con datos del Banco Mundial que mostraban que, a finales de 2024, el crédito al sector privado no financiero representaba el 33 % del producto interno bruto (PIB) de México. Subrayó que este porcentaje se encontraba por debajo del observado en otros países con niveles de desarrollo similares, como Chile (110 %), Brasil (72 %), Perú (46 %) y Colombia (42 %). Al señalar esta oportunidad de expansión del crédito, exhortó a las instituciones bancarias a reducir las tasas de interés que cobran a las micro y pequeñas empresas, lo que derivó en la firma de un convenio orientado a impulsar este objetivo. Al mismo tiempo, reconoció la fortaleza de la banca múltiple mexicana, caracterizada por altos niveles de capitalización y utilidades, tema que se aborda en la próxima sección.

El 26 de noviembre de 2025, el Consejo Nacional de Inclusión Financiera (CONAIF), integrado por altos funcionarios de las autoridades financieras y del Banco de México, presentó la tercera edición de la Po-

lítica Nacional de Inclusión Financiera (PNIF) 2025-2030. El documento, de aproximadamente 120 páginas, plantea una visión centrada en que

> *las mujeres, las poblaciones que habían sido históricamente excluidas y las empresas de menor tamaño participen plenamente en los beneficios del sistema.*
> *Que, en México, se fortalezca el bienestar a través de la inclusión financiera, para que nadie se quede atrás, y nadie se quede afuera. (p. 3)*

Más allá del lema con el que concluye el fragmento citado, la PNIF establece objetivos, estrategias, líneas de acción e indicadores de seguimiento. En el acto de presentación participó el secretario de la SHCP, Edgar Amador, quién reconoció que persiste una desconfianza significativa hacia el sistema financiero, incluso entre la población que ya utiliza alguno de sus servicios. Su intervención ofreció un diagnóstico realista y subrayó que aún queda un largo camino por recorrer, aunque destacó la importancia de dar seguimiento a las acciones planteadas para los próximos años.

Las dos caras de las altas utilidades de los bancos múltiples

De acuerdo con los datos agregados de la CNBV, resumidos en la tabla 3, la tasa de rendimiento sobre el capital contable del sistema de banca múltiple de 2024 fue del 18 %, resultado de una utilidad neta de 291,593 millones de pesos. Se trata de beneficios y tasas atractivas en el escenario macroeconómico nacional.

Estos resultados se explican, en gran medida, por el diferencial entre los ingresos generados por los préstamos y los gastos asociados al pago de intereses sobre los depósitos de los clientes. En 2024, la tasa promedio de los préstamos (ingresos sobre cartera) fue del 23 %, mientras que la tasa de los depósitos (gastos sobre captación) se situó en el 10 %, lo que arrojó un diferencial de 13 puntos porcentuales. Como consecuencia, el margen financiero se consolidó como la principal fuente de ingresos, con un total de 854,741 millones de pesos.

La segunda fuente relevante de ingresos provino de las comisiones y tarifas cobradas por los bancos a los usuarios que contrataron y operaron

servicios financieros. El resultado neto de esta partida ascendió a 171,674 millones de pesos, cifra equivalente al 20 % del margen financiero.

Tanto el margen financiero como las comisiones y tarifas aplicadas en México se sitúan por encima de los promedios internacionales, lo que ha permitido que la tasa de rendimiento sobre el capital se mantenga en niveles de dos dígitos durante los últimos años. El reporte de banca global de McKinsey (2023) señala una tasa promedio del 9 %, entre 2009 y 2023. Asimismo, el reporte de 2021 estima que dicha tasa ha sido de un solo dígito en regiones como Estados Unidos, Europa, África y Medio Oriente.

En conjunto, estos factores han dado lugar a un sistema bancario sólido, integrado por instituciones bien capitalizadas, lo que contribuye a la estabilidad financiera. Sin embargo, la contracara de este escenario es que las comisiones y los intereses representan una carga significativa para los usuarios, lo que limita el acceso a los servicios financieros. Por un lado, existe una banca bien capitalizada y estable; por otro, se prestan servicios costosos para los usuarios. Alcanzar un mayor equilibrio entre ambos aspectos sigue siendo un desafío pendiente.

Tabla 3. Estados financieros del sistema de banca múltiple (millones de pesos, 2024)

	Balance general	**Estado de resultados**	
Activo	15,211,645	Ingreso por intereses	1,794,087
(-) Pasivo	13,557,394	(-) Gastos por intereses	939,346
= Capital	1,654,251	(=) Margen financiero	854,741
		Comisiones y tarifas	171,674
		Utilidad neta	291,593

Fuente: Boletín estadístico de la CNBV (2024).

La presidenta de México, Claudia Sheinbaum, dio a conocer el 5 de septiembre de 2025 un adelanto del contenido del paquete económico para el próximo año. Anunció que, a partir de 2026, los bancos múltiples ya no podrían deducir como gastos las aportaciones que realizan al Instituto para la Protección al Ahorro Bancario (IPAB), y estimó que cerca de 10,000 millones de pesos serían recuperados por el Sistema de Administración Tribu-

taria (SAT). Tres días después, Edgar Amador, secretario de la SHCP, presentó el Paquete Económico 2026 ante la Cámara de Diputados. En su discurso reiteró que este contenía disposiciones extrafiscales orientadas a garantizar que los contribuyentes realicen una aportación justa y equitativa. Entre las medidas para ampliar la base tributaria, confirmó que las cuotas pagadas al IPAB por las instituciones de banca múltiple no serían deducibles; no obstante, precisó que la medida aplicaría únicamente a tres cuartas partes de dichas aportaciones. Un día después, en una conferencia de prensa, declaró que la no deducibilidad de las cuotas al IPAB tiene como objetivo homologar el tratamiento fiscal con el de otros países, como Canadá y Estados Unidos.

La presidenta Sheinbaum declaró que este tema fue previamente conversado con los propietarios de algunos bancos, por lo que confió en que no se presenten resistencias ni acciones legales —como amparos— para frenar la medida. El Congreso ya autorizó la implementación de esta política en un 75 %, por lo que algunos analistas consideran que las utilidades netas mostradas en la tabla 3 serán menores, mientras que otros estiman que estos nuevos gastos serán trasladados a los usuarios, lo que podría encarecer el crédito. Ya veremos lo que sucede.

Lentitud en las transferencias bancarias internacionales

Las transferencias electrónicas realizadas por los bancos múltiples en México, bajo la supervisión y apoyo del Banco de México, han experimentado una rápida evolución en el siglo XXI. Desde 2004, el banco central diseñó —y continúa operando— el Sistema de Pagos Electrónicos Interbancario (SPEI), utilizado para la liquidación de operaciones en tiempo real. Actualmente, no solo participan los bancos múltiples, sino también sus clientes, una amplia gama de entidades reguladas en el ámbito federal y dependencias del gobierno central. El requisito fundamental para utilizar este servicio es contar con una cuenta en un banco múltiple que ofrezca servicios de banca electrónica, ya sea a través de computadoras o teléfonos inteligentes. Los pagos realizados mediante SPEI pueden ser de cualquier monto y el sistema opera las 24 horas del día, los siete días de la semana. En teoría, las transferencias no deberían tardar más de 30 segundos; sin embargo, en la práctica, pueden demorar desde algunos minutos hasta una hora. El servicio no tiene costo, salvo que el usuario acuda físicamente a una sucursal, llene una solicitud y sea atendido por un cajero o cajera.

Desde 2019, el SPEI tiene una nueva funcionalidad denominada cobro digital (CoDi), la cual opera principalmente a través de dispositivos

móviles, también en un esquema 24/7 y sin costo alguno. La aplicación utiliza tecnología QR (código de respuesta rápida) y NFC (comunicación de campo cercano), e incorpora a empresas no financieras, cadenas comerciales, pequeños comerciantes y al público en general. El monto máximo por operación es de 8,000 pesos y la liquidación se realiza en tiempo real. Las transacciones se efectúan mediante la clave bancaria estandarizada (CLABE) de 18 dígitos de los comercios y tienen como objetivo principal reducir el uso de efectivo en operaciones de bajo monto. A finales de 2024, tras casi cinco años de operación, CoDi superaba los 20 millones de usuarios.

A finales de 2023, el Banco de México amplió el uso del SPEI mediante el lanzamiento de un nuevo servicio que vincula las cuentas bancarias con el número de teléfono celular —de diez dígitos— de los usuarios para realizar transferencias. Este servicio, conocido como DiMo (dinero móvil), puede ser utilizado por cualquier persona que cuente con la aplicación móvil de su banco y tenga activada esta opción. Un mismo número telefónico puede asociarse a cuentas en diversos bancos, aunque solo a una por institución. En diciembre de 2024, DiMo registraba más de 11 millones de usuarios y mostraba un crecimiento más acelerado que CoDi.

El Banco de México argumenta que DiMo y CoDi son herramientas diseñadas para facilitar las transferencias electrónicas: el primero resulta más adecuado para pagos de personas a empresas, mientras que el segundo se orienta a transferencias entre personas. Asimismo, reconoce que el uso del número telefónico es más sencillo que el de la CLABE bancaria. En noviembre de 2025, la Asociación de Bancos de México (AMB) propuso al Banco de México la fusión de CoDi y DiMo con el fin de simplificar el acceso para los usuarios y escalar el sistema de pagos instantáneos. Al cierre de este texto, no existía aún una respuesta de la autoridad monetaria.

Estos avances en materia de transferencias electrónicas contrastan con la lentitud que persiste en el subsector bursátil, particularmente en la Contraparte Central de Valores (CCV, véase glosario), donde durante décadas el plazo de liquidación de valores se realizaba dos días hábiles después de concretadas las operaciones de compraventa (T+2). Desde mayo de 2024, este plazo se redujo a T+1 exclusivamente para el mercado accionario local, en parte para armonizar el proceso con los cambios implementados en Estados Unidos y Canadá, y en parte para mejorar la eficiencia de la liquidación de valores.

La velocidad alcanzada en los sistemas de pago nacionales contrasta de manera significativa con las transferencias bancarias electrónicas internacionales o transfronterizas. En este caso, el tiempo de procesamiento depende del

par de divisas involucrado. No es lo mismo convertir pesos mexicanos a dólares estadounidenses que convertir pesos mexicanos a pesos bolivianos. El primer caso es relativamente sencillo debido al elevado volumen de remesas y al comercio bilateral entre dos países con un tratado de libre comercio; el segundo resulta más complejo, dado el reducido intercambio comercial y el bajo volumen de remesas entre ambos países. Otros factores que influyen son el día en que inicia la transferencia —no es igual realizarla un un viernes o en día festivo—, las diferencias horarias entre los países y el monto enviado. Por estas razones, una transferencia de este tipo puede tardar entre uno y siete días en completarse. La mayoría se procesa a través de la red denominada Sociedad para las Telecomunicaciones Financieras Interbancarias Mundiales (SWIFT, por sus siglas en inglés), un sistema de mensajería y rastreo. Aunque el proceso puede ser lento, las instituciones bancarias argumentan que es seguro.

Como consecuencia de estas limitaciones, han surgido numerosos transmisores de dinero no bancarios que ofrecen servicios más rápidos, aunque a un costo mayor. Asimismo, desde 2009, las criptomonedas, las monedas estables y las finanzas descentralizadas se han propuesto como alternativas para resolver la lentitud de las transferencias bancarias transfronterizas, los elevados costos de las comisiones de la banca múltiple, así como para promover la democratización financiera y la despolitización del dinero. La capitalización agregada de las plataformas que prestan estos servicios ha mostrado una elevada volatilidad, aunque con una tendencia histórica positiva. Diversos reguladores han intentado someter estos sistemas a reglas similares a las de los servicios centralizados. Paralelamente, tres bancos centrales ya ofrecen la emisión de monedas digitales (CBDC, por sus siglas en inglés), mientras que muchos otros se encuentran en fase de experimentación, con el objeto de mantener vigente el sistema de servicios formales. Surge entonces la pregunta: ¿podrán coexistir los servicios tradicionales con los descentralizados?, ¿cuál de ellos será predominante? Para abordar estas cuestiones, se presentará un análisis detallado del funcionamiento y de las características del ecosistema cripto.

Servicios descentralizados

Desde hace algunos años es posible realizar pagos y operaciones financieras sin utilizar el peso mexicano ni recurrir a intermediarios, ya sean bancarios o de otro tipo. ¿Cómo? Mediante el uso de criptomonedas, que permiten efectuar transacciones monetarias o financieras entre pares a través de programas informáticos automatizados, de manera cuasianónima. Estas operaciones se realizan por internet, en tiempo real, las 24 horas del día, los siete días de la semana, durante todo el año.

Cripto es un prefijo, no una palabra autónoma. Proviene del griego *kryptós*, que significa «encubierto» u «oculto», y se emplea siempre para formar voces compuestas, como criptografía, criptomoneda, criptodivisa, criptoactivo o kryptonita (material ficticio presente en las historias de Superman).

La Real Academia Española (RAE) incorporó al *Diccionario de la lengua española* el término *criptomoneda* (del inglés *cryptocurrency*) desde 2021 y lo define como una «moneda virtual gestionada por una red de computadoras descentralizadas que cuenta con un sistema de encriptación para asegurar las transacciones entre usuarios». Esta definición admite al menos dos observaciones. En primer lugar, ¿cuándo puede considerarse que una red es realmente descentralizada? Bitcoin, la primera criptomoneda, surgida en 2008, cuenta actualmente con 21,119 computadoras como nodos completos visibles en su red; Ethereum supera los 11,000 validadores; Solana dispone de 1,502, y XRP tiene 35. No existe un criterio unívoco: algunos consideran que la descentralización inicia con redes de dos dígitos, mientras que otros exigen cifras de cinco dígitos. En segundo lugar, la RAE define *encriptación* como la acción y el efecto de encriptar, verbo que reconoce como sinónimo de *cifrar*, entendido este último como la transcripción de un mensaje mediante una clave.

La RAE también reconoce el término *bitcóin*, que define como una «moneda digital». A esta breve definición añade que se trata de una marca registrada y que procede del inglés, formada por *bit* (la unidad mínima de información en el sistema binario, representada por 0 o 1) y *coin,* que significa moneda. En un primer momento se registró sin acento gráfico, pero posteriormente se le incorporó la tilde. En este documento, por razones históricas y de simplicidad, se empleará la forma bitcoin, sin acento.

Una definición anterior y de carácter divulgativo fue propuesta por John Oliver, comediante británico conocido por el uso de la sátira para ex-

plicar temas complejos. En su programa televisivo del 11 de marzo de 2018, emitido por HBO, se refirió a las criptomonedas como «todo aquello que no entiende usted del dinero combinado con todo aquello que no entiende usted de las computadoras». A ello podría añadirse todo lo que tampoco se comprende plenamente de las matemáticas —en particular de la criptografía—, de internet, de las leyes, de las regulaciones y de la economía financiera.

Resulta difícil determinar cuántas criptomonedas existen en la actualidad. La información disponible presenta grandes discrepancias y genera desconfianza, debido a la falta de datos completos y homogéneos en este ámbito. Algunos proveedores de precios y clasificaciones enfrentan conflictos de interés, y sus criterios de inclusión varían considerablemente. Así, messari.io reporta 38,287 activos; crypto.com, 27,369 monedas; coingecko.com, 18,563; coinmarketcap.com, 20,540 criptomonedas, mientras que studio.glassnode.com lista 1,700 activos. Estas clasificaciones incluyen una amplia variedad de proyectos. Existen criptomonedas orientadas a los pagos, algunas son descentralizadas, otras semidescentralizadas y otras centralizadas. También se encuentran las denominadas estables (*stablecoins*), casas de intercambio, aplicaciones financieras descentralizadas (DeFi), tókenes —fungibles y no fungibles (NFT)—, así como criptomonedas basadas en memes, algunas de las cuales han alcanzado valoraciones inesperadas, como Dogecoin u Official Trump. Se trata de un ecosistema fragmentado que vive una etapa naciente y con escasa regulación. Pocos proyectos parecen sólidos y bien fundamentados, mientras que la mayoría responde a dinámicas especulativas o está vinculada con fraudes, estafas, lavado de dinero, secuestro de datos (*ramsomware*), códigos maliciosos (*malware*) y otras actividades ilícitas propias del internet profundo. Todo ello, sumado a la intensa publicidad de los proyectos y a la cobertura mediática constante, permite aplicar el conocido proverbio «mucho ruido y pocas nueces». Por esta razón, resulta indispensable realizar un análisis riguroso y una debida diligencia antes de decidir participar en alguno de estos proyectos.

Como se muestra en la tabla 4, Bitcoin, la primera moneda descentralizada, también es la primera en valor de capitalización y concentra el 57.3 % del valor total del ecosistema.

Tabla 4. Los siete grandes (28 de diciembre de 2025)

Nombre	Símbolo	Año de creación	Valor de capitalización (billones de dólares)	% del mercado
Bitcoin	BTC	2009	1,755	57,3
Ethereum	ETH	2015	355	11,6
Tether	USDT	2014	186	6,1
BNB	BNB	2017	118	3,9
Ripple	XRP	2011	113	3,7
USD Coin	USDC	2018	76	2,5
Solana	SOL	2020	70	2,3
Total			3,061	100

Fuente: CoinGecko (2025).
Nota: en Estados Unidos un trillón de dólares es igual a un millón de millones (un uno seguido de doce ceros). Equivale a un billón en español.

Gráfica 1. Valor de capitalización total (28 de diciembre de 2025)

Fuente: CoinGecko.

El valor total de capitalización del mercado de las criptomonedas —3.06 trillones de dólares— puede analizarse desde distintas perspectivas. Una de ellas consiste en compararlo con el total de activos financieros globales que, de acuerdo con *The Banker*, ascendieron a 487.6 trillones de dólares en 2021. Desde esta óptica, el mercado cripto representa el 0.6 % del sistema financiero mundial. Por esta razón, la mayoría de los organismos internacionales, entre los que destacan el Fondo Monetario Internacional (FMI) y el Banco de Pagos Internacionales (BIS), han reiterado en diversas publicaciones que, en la actualidad, las criptomonedas no representan un riesgo sistémico.

La situación cambia parcialmente si nos concentramos en las personas que utilizan criptomonedas, en lugar de su valor de capitalización. De acuerdo con Triple-A (triple-a.io), en 2024 existían 562 millones de propietarios de criptomonedas, cifra que representa al 6.9 % de la población mundial. México se sitúa por encima de la media global, ya que el 9.7 % de su población posee algún tipo de criptomoneda. Los datos del número de usuarios varían según la fuente, el método de cálculo y la fecha de corte; sin embargo, permiten establecer rangos aproximados.

Otro indicador para estimar el número de usuarios de criptomonedas en México es recurrir a los informes de datareportal.com, que ofrecen datos sobre el comportamiento de los usuarios de internet. En su reporte digital para México, publicado en marzo de 2025, se señala que el 8.1 % de los consumidores de internet de 16 años o más es propietario de algún tipo de criptomoneda. El mismo informe indica que, a febrero de 2025, la población total de México ascendía a 131 millones de personas, de las cuales, el 76 % tenía 16 años o más. Asimismo, reporta la existencia de 110 millones de usuarios de internet en el país.

Con todo lo anterior y bajo el supuesto de que el rango de edad es similar para la población total y para los usuarios de internet, puede estimarse que el número de propietarios de criptomonedas de 16 años o más es de 6.8 millones de personas (110 millones de usuarios de internet x 76 % de mayores de 16 años x 8.1 % de propietarios de criptomonedas).

La estimación más baja sobre el número de propietarios de criptomonedas en México proviene de la Encuesta Nacional de Inclusión Financiera (ENIF) 2025, cuyos resultados indican que:

> *a pesar de su presencia mediática, la penetración de estos es incipiente. A nivel nacional, solo el 2 % de la población ha comprado o invertido en activos virtuales siendo más común entre la población más joven y quienes tienen educación superior. (p. 64)*

La misma encuesta señala que las personas de 18 años o más asciende a 94.2 millones de personas, lo que permite estimar que el número de propietarios de criptomonedas en este grupo etario es de 1.9 millones.

Con la información presentada en los cuatro párrafos anteriores, el lector puede formarse una idea de los valores máximos y mínimos del nú-

mero de personas que son propietarias de al menos una criptomoneda en México. Conviene aclarar que la profundidad y el criterio de medición del uso difieren según la fuente: algunas estimaciones se basan en la población total, otras en los usuarios de internet de 16 años o más, y otras en rangos etarios específicos, como el de 18 a 70 años.

Desde el inicio de operaciones de Bitcoin en 2009 y con la posterior aparición de otras criptomonedas de características similares, quienes defienden la descentralización como una herramienta de la libertad —comúnmente asociados a una postura libertaria— han sostenido debates con las autoridades financieras, las instituciones tradicionales y los organismos internacionales, que representan una visión más formal o institucional. Estas diferencias siguen abiertas y se articulan en torno a una serie de interrogantes relacionadas con las criptomonedas: ¿son dinero desde una perspectiva económica?, ¿lo son desde el punto de vista legal?, ¿son un valor o instrumento financiero?, ¿deben considerarse activos virtuales, criptoactivos, bienes mercantiles, materias primas o activos intangibles?

En las siguientes secciones se tratará de responder brevemente algunas de estas interrogantes, no sin antes mencionar que ambos grupos discrepan incluso en la terminología utilizada. El término *criptomoneda* tiene su origen en el grupo libertario que trata de resaltar tanto el medio de pago de carácter privado como el uso de la criptografía que usa a su alrededor. Por su parte, el grupo formal suele emplear las denominaciones *activo virtual* o *criptoactivo*. El término *activo virtual* es más frecuente en Norteamérica; prueba de ello es que la Ley para Regular las Instituciones de Tecnología Financiera (2018) de México lo define en su artículo 30 como:

> *la representación de valor registrada electrónicamente y utilizada entre el público como medio de pago para todo tipo de actos jurídicos y cuya transferencia únicamente puede llevarse a cabo a través de medios electrónicos. En ningún caso se entenderá como activo virtual la moneda de curso legal en territorio nacional, las divisas ni cualquier otro activo denominado en moneda de curso legal o en divisas. (p. 16)*

El término *criptoactivo*, en cambio, es ampliamente utilizado en los países de la Unión Europea. El Reglamento de la Unión Europea 2023/1114

(MiCA) lo define en su artículo 3 como «una representación digital de un valor o de un derecho que puede transferirse y almacenarse electrónicamente, mediante la tecnología de registro distribuido o una tecnología similar» (p. 63).

Tanto en el pasado como en el presente, el dinero puede ser «cualquier cosa» que la gente esté dispuesta a aceptar en el pago de bienes, servicios o deudas. Esto significa que uno de los tres requisitos económicos que debe cumplir esa «cosa», para que se la considere dinero, es ser generalmente aceptada como medio de cambio.

La segunda condición es la unidad de cuenta, es decir, el patrón que permite denominar los precios de los bienes, los servicios y los activos. Esto facilita la contabilidad, herramienta fundamental de las finanzas.

La tercera exigencia consiste en servir como depósito de valor, lo cual representa una de las formas en que las personas pueden conservar su riqueza o patrimonio; para ello, el control de la inflación es de vital importancia.

Que la «cosa» utilizada como dinero tenga o no valor por sí mismo ha dejado de ser relevante en la actualidad; lo importante es que se cumplan los tres requisitos mencionados. La gran mayoría de los economistas y los bancos centrales consideran como dinero, básicamente, los billetes y monedas, los depósitos bancarios y las inversiones en bonos gubernamentales. Sin embargo, no reconocen a las criptomonedas en ninguna de sus clasificaciones oficiales. Es posible adoptar la perspectiva de los libertarios y argumentar que las criptomonedas, en general, y el bitcoin, en particular, son aceptadas por los 562 millones de usuarios en el mundo y por cerca de 20,000 establecimientos que las reciben. Esto puede interpretarse como una aceptación generalizada de su uso como medio de pago. Asimismo, también pueden sostenerse que, pese a la alta volatilidad del precio del bitcoin en periodos cortos, su tenencia a largo plazo ha funcionado como un depósito de valor. Es justo reconocer que estos argumentos tienen cierta solidez; no obstante, en última instancia, no son aceptados por los bancos centrales. Por esta razón, se evita denominarlos monedas o divisas y se prefiere el uso de términos como *activos virtuales* o *criptoactivos*. Este desacuerdo lleva ya diecisiete años y probablemente persistirá durante muchos más. Por ahora, cada postura continúa desarrollándose en su propio ámbito, y el debate ha adquirido un carácter predominantemente académico o conceptual. Aunque al momento de escribir estas líneas, ningún país del mundo utiliza el bitcoin u otro activo virtual como moneda de curso legal, resulta pertinente mencionar dos experimentos fallidos.

Desde el punto de vista jurídico, puede afirmarse que tanto El Salvador como la República Centroafricana fueron los únicos países en el mundo que adoptaron oficialmente el bitcoin como moneda de curso legal. El Salvador lo reconoció en 2021 junto con el dólar estadounidense; sin embargo, a principios de 2025 revirtió esta decisión, por lo que su uso quedó limitado a intercambios privados y su aceptación pasó de ser obligatoria a voluntaria. Esta decisión estuvo influida por un préstamo de 1.4 billones de dólares del FMI, que estableció como una de sus condiciones la mitigación de los riesgos asociados al bitcoin. La República Centroafricana, por su parte, también adoptó el bitcoin como moneda de curso legal en 2022, junto con el franco CFA de África Central. Sin embargo, el hecho de que solo el 10 % de sus habitantes tenga acceso a internet, aunado a malas condiciones macroeconómicas y a problemas sociales y políticos, la obligó a revertir esta decisión. Actualmente, ya no existe la convertibilidad automática entre el franco CFA y el bitcoin, aunque la población tiene la libertad de usarlo para pagos de bienes y servicios.

La definición de si las criptomonedas son un valor o un instrumento financiero depende del régimen legal vigente en cada país. En el caso de México, la Secretaría de Hacienda y Crédito Público, el Banco de México y la Comisión Nacional Bancaria y de Valores, en un comunicado del 13 de diciembre de 2017, alertaron al público sobre su uso y la posible participación en esquemas de inversión conocidos como ofertas iniciales de monedas (ICO, por sus siglas en inglés). En dicho comunicado se señala que «algunas ICO que, en su caso se originen y emitan en México podrían violar la Ley del Mercado de Valores y constituir un delito financiero». Asimismo, se aclara que, dependiendo de las características de cada caso, las fichas o tókenes pueden constituirse como valores conforme la Ley del Mercado de Valores (LMV), siempre que su oferta al público cumpla con las condiciones y limitaciones establecidas. A continuación, se realiza una digresión para explicar esta última parte.

La Ley del Mercado de Valores, en su artículo segundo, fracción XXIV, no define lo que son los valores, pero sí específica cuáles están autorizados para su oferta pública. En este sentido, incluye:

> *las acciones, partes sociales, obligaciones, bonos, títulos opcionales, certificados, pagarés, letras de cambio y demás títulos de crédito, nominados o innominados, inscritos o no en el Registro Nacional*

> *de Valores, susceptibles de circular en los mercados de valores a que se refiere esta Ley. (p. 5)*

Posteriormente, el artículo octavo permite la oferta privada de valores que no requieren inscripción en el registro, siempre que se oferten exclusivamente a inversionistas institucionales o calificados, y que no exceda un límite de cien personas. Los valores pueden considerarse como hermanos de los instrumentos financieros que permiten a las personas intercambiarlos por dinero en los mercados de capital y de deuda, tanto públicos como privados.

En resumen, en México las criptomonedas no se encuentran incluidas en la lista oficial de valores que pueden ofrecerse al público en general, ni en la Ley de Mercado de Valores ni en la Ley General de Títulos y Operaciones de Crédito. Sin embargo, en caso de cumplir una serie de requisitos, las criptomonedas sí pueden ser ofertadas de manera privada. El Banco de México, en su comunicado del 10 de marzo de 2014, las clasifica como activos virtuales y deja claro que no son monedas de curso legal ni divisas extranjeras. Además, señala que las instituciones reguladas del sistema financiero mexicano no están autorizadas para utilizarlas ni para efectuar operaciones con ellas. Posteriormente, en un comunicado conjunto con la SHCP y la CNBV, se definen los activos virtuales o criptoactivos como mecanismos de almacenamiento e intercambio de información electrónica. Más recientemente, en el *Reporte de Estabilidad Financiera* de junio de 2025, el Banco de México identifica otro riesgo asociado a los activos virtuales (AV). De manera literal, señala que:

> *la concentración de AV en manos de grandes tenedores, comúnmente denominados ballenas, plantea riesgos significativos de manipulación de mercado. Se ha observado que estos inversionistas, aunque representan solo el 1 % de las direcciones con al menos 1,000 tokens, poseen el 37 % del total de la tenencia. (p. 109)*

Más allá del caso mexicano, en la actualidad las criptomonedas ya cotizan en diferentes regiones del mundo de manera regulada, incluido Es-

tados Unidos, a través de fondos de inversión negociados en bolsa (ETF). Más adelante, al final de la sección titulada «la centralización de lo descentralizado», se ofrece información sobre los ETF de contado de bitcoin y ether. Aunque, en teoría, sería posible que en el futuro estos instrumentos se negociaran también a través de la Bolsa Mexicana de Valores o la Bolsa Institucional de Valores, su probabilidad de que ello ocurra es baja.

Tres ejemplos de lo descentralizado

Si el lector tiene interés en conocer el funcionamiento técnico de Bitcoin (primer caso), puede encontrar información adicional en el anexo 1. El segundo modelo está representado por Ethereum, cuyos detalles se presentan en el anexo 2. Por su parte, quienes deseen profundizar en Solana (tercer ejemplo) pueden consultar el anexo 3.

Los tres protocolos tienen en común una serie de características, entre las que destacan las siguientes:

(a) operan de manera descentralizada o distribuida;
(b) su *software* es de código abierto;
(c) son globales, es decir, no reconocen fronteras;
(d) son resistentes a la censura;
(e) recompensan a mineros, validadores o líderes, y
(f) utilizan directa o indirectamente criptografía, algoritmos y funciones *hash* (funciones resumen).

Sin embargo, también presentan diferencias relevantes, sobre todo en términos de visión y prioridades. En términos generales, Bitcoin tiene como objetivo primordial la creación de una moneda global descentralizada y, para ello, se apoya en una plataforma que garantiza la seguridad de los pagos entre pares. En cambio, Ethereum y Solana buscan principalmente desarrollar una plataforma capaz de ejecutar programas de cómputo conocidos como contratos inteligentes (véase su definición en el glosario complementario y los aspectos técnicos en el anexo 2), así como permitir la construcción de aplicaciones descentralizadas. Para lograrlo, ambos protocolos se apoyan en sus monedas nativas, que permiten cobrar el uso de dichas plataformas.

La tabla 5 presenta algunas diferencias entre Bitcoin, Ethereum y Solana, de las cuales se destacan tres. En primer lugar, Ethereum y Solana sí tienen desarrolladores con nombre y apellidos reales, como es el caso de Vitálik Buterin y Anatoly Yakovenko. Esta identificación facilitó la obten-

ción de financiamiento de terceros mediante las denominadas ofertas públicas iniciales. En contraste, Bitcoin fue desarrollado por alguien que usó un seudónimo y después desapareció de la vida pública.

En segundo lugar, los protocolos de Ethereum y Solana son generales y Turing completos, en el sentido de que permiten bucles o ciclos (*loops*), es decir, instrucciones que permiten repetirse más de una vez. De igual forma, son capaces de manejar instrucciones condicionales del tipo «si ocurre esto, entonces haz aquello» (*if-then*). Esto representa una diferencia sustancial con respecto a Bitcoin, cuya cadena de bloques está especializada en la realización de pagos entre iguales. Como se detallará más adelante, Ethereum y Solana permiten que terceros utilicen sus plataformas para crear fichas (tókenes), así como para su operación y almacenamiento.

En tercer lugar, el mecanismo de consenso de los nodos que participan en la operación de la base de datos de Ethereum se basa en la prueba de participación (POS, por sus siglas en inglés), mientras que Solana combina este mecanismo con la prueba de historia (POH, por sus siglas en inglés). Ambos sistemas consumen una cantidad considerablemente menor de energía eléctrica que la prueba de trabajo (POW, por sus siglas en inglés) utilizada por Bitcoin.

La prueba de trabajo de Bitcoin quedó establecida en el libro blanco de Satoshi Nakamoto, quien, en la cuarta sección del documento (p. 3), explicó que dicho mecanismo permite alcanzar decisiones mayoritarias entre los participantes en el registro de las transacciones. Para entender la prueba de trabajo, es necesario distinguir entre los nodos completos y los nodos ligeros que operan en la red de Bitcoin. Los nodos completos validan las transacciones de manera independiente y almacenan toda la cadena de bloques. En cambio, los nodos ligeros dependen de los nodos completos para verificar las transacciones y únicamente descargan o almacenan los encabezados de los bloques.

Dentro de los nodos completos se encuentran los denominados nodos mineros (véase el glosario), que, además de validar y almacenar, crean nuevos bloques al resolver problemas matemáticos con alto grado de dificultad. Por esta labor reciben una recompensa en bitcoins, así como las comisiones asociadas a las transacciones. En esencia, este mecanismo constituye un sistema de votación en el que cada nodo completo especializado —el minero— emite un voto a través de su capacidad de cómputo.

Como se muestra en la tabla 5, existen más de 21,000 nodos completos, de los cuales solo una parte corresponde a nodos mineros que compiten por resolver un acertijo criptográfico con el fin de obtener las comisiones

de las transacciones y una recompensa de 3.125 nuevos bitcoins para su beneficio. En consecuencia, para ser un minero competitivo es necesario invertir en equipos computacionales de alto costo, los cuales, además, consumen grandes cantidades de energía eléctrica.

Los mineros se encuentran distribuidos en diversas regiones del mundo, entre las que destacan Estados Unidos, Kazajistán, Rusia, Alemania, Canadá y Paraguay. Aunque el portal bitnodes.io indica que en México existen 24 nodos completos verificados, los autores de este libro solo han identificado un minero que operó hasta enero de 2025. En ese mes se descubrieron granjas de minería de Bitcoin en Nuevo Necaxa, Puebla, vinculadas al Sindicato Mexicano de Electricistas (SME), las cuales obtenían de manera ilegal la energía de la Comisión Federal de Electricidad (CFE). Dichas instalaciones fueron desarticuladas por las autoridades tras haber operado por más de un año. Nadie fue detenido en este proceso, que diversos medios denominaron *huachicoleo* (robo) *eléctrico* en Puebla.

La ley mexicana no prohíbe ni la compra de bitcoins ni el establecimiento de mineros, por lo que con frecuencia se interpreta que dichas actividades están permitidas, lo cual puede ser válido hasta cierto punto.

Tabla 5. Las tres principales plataformas descentralizadas

Concepto	**Bitcoin**	**Ethereum**	**Solana**
Fundador	¿Satoshi Nakamoto?	Vitalik Buterin+	Anatoly Yakovenko+
Inicio de operaciones	2009	2015	2020
Libros	Blanco	Blanco, Amarillo y Beige	Blanco
ICO	Familia y amigos	18.3 mdd (2013)	25.6 mdd (2018)
Software	Código abierto	Código abierto	Código abierto
Instituciones	Fundación (2012)	Fundación	Fundación + Solana Lab Inc.
Moneda nativa	BTC	ETH	SOL
Unidad mínima	1 BTC = 10^8 satoshis	1 ETH = 10^{18} weis	1 SOL = 10^8 lamports
Protocolo	Especializado (Turing incompleto)	General (Turing completo)	General (Turing completo)
Lenguajes	Bitcoin Core + Script	Solidity + bytecode	Rust + bytecode
Nodos activos	21,000 + nodos completos	11,000 + validadores	1,502 validadores

Tabla 5. Las tres principales plataformas descentralizadas (continuación)

Concepto	Bitcoin	Ethereum	Solana
Invierten en	Computadoras y energía eléctrica	Requieren 32 ETH	Sin mínimo
Política monetaria	Máximo 21 millones	Sin límite	Sin límite
Consenso	POW (mineros)	PoS (sept. 2022; validadores)	PoS + POH (líderes y validadores)
Emisión de monedas	Recompensa a mineros por nuevos bloques	Recompensa a validadores por nuevos bloques (-) quema	Incremento anual del 1.5 % en el L. P. (-) quema
Recompensa por bloque	Resolver acertijo (3.125 BTC)	Lotería ponderada; usuarios pagan por uso	Lotería ponderada proporcional
Tamaño del bloque	Límite de 4 MB	Límite de 30 millones de unidades de gas	Límite de 128 MB
Direcciones	Varias	Una	Una
Tiempo promedio por bloque	10 minutos	12 segundos	500 ms
Transacciones por segundo	7	29	3,610
Fichas (tókenes)	Muy pocos	Muchos ERC-20 (fungibles) y ERC-721 (NFT); Ether+	Muchos SOL+
Sistema de registro	UTXO	Cuentas (saldos)	Cuentas (saldos)
Inmutabilidad	Total	Parcial	Parcial
Bifurcaciones	Múltiples	Ethereum Classic (2016)	Serum (2021) + 7 interrupciones

Fuente: elaboración propia con el uso de diversas fuentes (junio de 2025).

Para establecer una comparación entre Ethereum y Solana puede recurrirse al trilema de las cadenas de bloques públicas y descentralizadas, término acuñado por el cofundador de Ethereum, Vitálik Buterin, en 2018. Dicho trilema plantea que las tres principales características de una red pública deberían ser la descentralización, la seguridad (la protección de los datos y la información) y la escalabilidad (transacciones por segundo). Buterin afirma que para el diseño de la red solo se pueden lograr dos de las

tres propiedades, por lo que necesariamente debe renunciarse a la tercera. De este modo, se presentan tres alternativas:

(a) una red segura y descentralizada, pero no escalable;

(b) una red escalable y descentralizada, pero no segura; o

(c) una red escalable y segura, pero no descentralizada.

Al lector interesado en profundizar en los conceptos de redes y registros se le remite al anexo 4. Se trata, por tanto, de decisiones mutuamente excluyentes. En este contexto, resulta claro que Ethereum optó por privilegiar la descentralización y la seguridad, con la desventaja de una baja escalabilidad en términos de velocidad, ya que procesa 29 operaciones por segundo, cifra que, si bien supera a la de Bitcoin —siete transacciones por segundo—, continúa siendo limitada. No obstante, Buterin ha señalado que su trilema es una hipótesis válida bajo la tecnología actual, pero que se trata de una cuestión abierta susceptible de modificarse con los avances tecnológicos.

Por su parte, en 2017 Anatoly Yakovenko decidió desarrollar Solana como una cadena descentralizada con contratos inteligentes capaz de alcanzar velocidades comparables a las de los sistemas centralizados tradicionales. Gracias a diversas innovaciones —entre las que destaca la prueba del historial (PoH)—, Solana logra un mayor rendimiento mediante el procesamiento de transacciones agrupadas en lotes en tiempo real. Actualmente procesa 3,610 transacciones por segundo y afirma que, al menos desde un punto de vista técnico, podría alcanzar hasta 710,000 transacciones por segundo. Además, Solana lo hace con una comisión promedio por transacción de 0.00064 dólares, muy por debajo de las comisiones de Ethereum, que pueden oscilar entre 50 y 100 dólares. Desde la perspectiva de la escalabilidad, no cabe duda de que Solana, mediante un enfoque de cambio horizontal aplicado en su mecanismo de consenso de primera capa (véase la figura 1), supera a Ethereum, el cual ha recurrido a soluciones en la segunda capa (figura 1). Estas soluciones implican delegar —o subcontratar— el registro de las transacciones a plataformas como Arbitrum, que las procesan fuera de la cadena de bloques, las empaqueta y las regresa para su finalización. Esto es producto de la descentralización de las redes, ya que Ethereum cuenta con más de 11,000 nodos validadores, mientras que Solana apenas supera los 1,500. El tercer pilar del trilema es la seguridad, ámbito en el que todas estas redes han experimentado bifurcaciones (véase el glosario); sin embargo, hasta el momento, solo Bitcoin ha sido inmutable en sus registros (véase el glosario).

Solana afirma que su tecnología ha logrado resolver el trilema de las cadenas de bloques. Eteherum, en contraste, continúa argumentando lo contrario, al señalar que constituye una red descentralizada con más de 11,000 validadores, mientras que Solana parece ser una red centralizada, con solo 1,502 nodos.

Ante este panorama, ¿qué postura resulta más convincente? Independientemente de la respuesta, el debate seguirá abierto mientras no se pueda definir cada uno de los tres pilares del trilema de manera objetiva. Lo que sí puede afirmarse, con base en los datos disponibles al momento de escribir estas líneas y en las estadísticas de la tabla 4, es que Ethereum ocupa el segundo lugar dentro del universo cripto, mientras que Solana se sitúa en la séptima posición.

Un tema estrechamente relacionado con el trilema es el caso de Ripple (XRP), que aparece en el quinto renglón de la tabla 4. Ripple constituye, en realidad, un modelo híbrido entre cadenas de bloques públicas (de permiso abierto) y privadas (de acceso restringido). Su historia inicia en 2011, cuando tres ingenieros, David Schwartz, Jed McCaleb y Arthur Britto, desarrollaron lo que consideraron un libro de registros superior al de Bitcoin, denominado XRPL, basado en *software* de código abierto. A esta propuesta la describieron como «Bitcoin sin mineros». XRPL es una cadena de bloques descentralizada, pública y abierta con un nuevo mecanismo de consenso, distinto tanto de la prueba de trabajo de Bitcoin como de la prueba de participación de Ethereum y Solana. La red opera con aproximadamente 150 nodos especiales (validadores) en los que participan empresas financieras, casas de intercambio (*exchanges*), universidades e individuos. De este conjunto, existe un subconjunto de 35 nodos incluidos en las denominadas listas de nodos únicos (LNU), que actúan como servidores de confianza. Estos nodos no reciben compensación económica por su labor de validar transacciones, sino beneficios no financieros y reconocimiento reputacional cuando desempeñan correctamente su función. Cada participante puede seleccionar su LNU; de no hacerlo, el sistema asigna una por defecto. El consenso se alcanza cuando al menos el 80 % de las LNU aprueba un conjunto de transacciones. Cabe señalar que, de los 35 nodos de estas listas, aproximadamente dos están vinculados a los fundadores de la compañía Ripple, descrita más adelante.

En 2012, XRPL crea su moneda nativa, XRP, con un límite máximo de 100 billones de unidades. En ese momento la promocionaban como la moneda nativa más rápida (con tiempos de liquidación de entre tres y cinco segundos), la más económica (0.0003 por transacción), la más escalable

(hasta 1,500 transacciones por segundo) y la más ecológica, debido a su bajo consumo energético, comparable al envío de un correo electrónico. Todas las monedas fueron emitidas de manera simultánea mediante un proceso de preacuñación. El 20 % de la emisión fue donado a los desarrolladores originales, mientras que el 80 % restante se entregó a una empresa, que se describe en el siguiente apartado. En la actualidad circulan 58 billones de XRP, en tanto que el resto permanece bajo custodia o depósito en el libro contable de XRPL.

La compañía que recibió los 80 billones de monedas ha cambiado de nombre tres veces. En 2012 inició como New Coin y se incorporó en California, para después llamarse Open Coin, y en 2013 pasó a denominarse Ripple Labs, incorporándose en 2014 en Delaware. Se presenta como una empresa de tecnología que tiene el control del protocolo de Ripple (XRPL) y cuya función principal es facilitar pagos dentro de la red de nodos entre pares. Ripple Labs ha recaudado más de 700 millones de dólares en rondas iniciales de financiamiento. Se trata de una empresa privada que obtiene ingresos tanto de las ventas de monedas que le fueron donadas como por la comercialización de *software* y, de manera más relevante, de la prestación de servicios profesionales a diversas instituciones financieras en el mundo. Al tratarse de una compañía privada, no da a conocer sus estados financieros al público en general. Lo que sí se sabe es que sus fundadores son Britto, Larsen y McCaler.

Uno de los servicios profesionales que Ripple presta a las instituciones financieras es la realización de pagos transfronterizos (de alcance global) de forma económica y eficiente con su moneda, XRP. La empresa se presenta como una alternativa al sistema SWIFT, utilizado por los bancos. De igual forma, ha sido contratada por la casa de intercambio centralizada Bitso —que opera en México con licencia de Gibraltar— para facilitar el envío rápido de remesas con el apoyo de algunos bancos favorables a las criptomonedas en Estados Unidos. En este esquema, los depósitos en dólares se emplean para comprar XRP, que posteriormente se transfiere a México, donde Bitso lo recibe, lo convierte a pesos mexicanos y lo entrega al destinatario final.

La historia de Ripple ha estado marcada por diversos problemas en Estados Unidos. En 2015, Fincen —organismo equivalente a la UIF en México— la multó en varias ocasiones por violar el secreto bancario y por incurrir en publicidad engañosa. Sin embargo, en diciembre de 2020, la Comisión de Valores y Bolsa (SEC, por sus siglas en inglés) presentó una demanda civil contra Ripple, su CEO, Brad Garlinghouse, y su cofundador,

Chris Larsen, al considerar que la venta de la moneda XRP constituía la colocación de un valor no registrado. En particular, a la empresa se le acusó de violar la sección quinta de la Ley de Valores. El caso acumuló miles de fojas, así como múltiples testimonios de expertos, y obligó a la compañía a contratar equipos legales y a destinar millones de dólares a su defensa. Por lo anterior, XRP fue retirado temporalmente de algunas de las casas de intercambio.

El 13 de julio de 2023, la jueza Analisa Torres dio a conocer las conclusiones de su fallo sumario, en el que determinó que las ventas originales de XRP realizadas por Ripple a fondos e inversionistas sí constituían contratos de inversión (valores), y por tanto, valores no registrados ante la Comisión de Valores y Bolsa. No obstante, también resolvió que las ventas de XRP efectuadas a través de casas de intercambio descentralizadas, así como las distribuciones otorgadas como incentivos a sus empleados o utilizadas como pago por servicios, no podían considerarse valores y, en consecuencia, no requerían registro ante la SEC.

Esta decisión fue interpretada como un triunfo para ambas partes y aportó mayor claridad al marco regulatorio de las criptomonedas en Estados Unidos, donde se intentó aplicar legislación de la década de 1930 a un nuevo fenómeno surgido en 2009. El fallo dejó claro que XRP, en particular, y las criptomonedas, en general, no son valores en sí mismos, aunque pueden ser vendidos mediante esquemas, transacciones o contratos que sí sean considerados como tales.

El final de este caso se produjo en octubre de 2024, cuando la jueza Torres multó a Ripple con 125 millones de dólares por haber recaudado 1,300 millones de dólares mediante la venta de XRP. Una vez más, la decisión fue interpretada por ambos lados como favorable. Por un lado, el CEO de Ripple expresó satisfacción debido a que el monto de la multa fue considerablemente menor al solicitado inicialmente por la SEC (2,000 millones de dólares). Por otro lado, la SEC sostuvo que la resolución reafirmaba su capacidad para hacer cumplir la legislación vigente.

Ripple se considera un caso híbrido, ya que cuenta con un libro contable descentralizado (XRPL), al que cualquier usuario puede acceder sin necesidad de autorización; es decir, su cadena de bloques es descentralizada, púbica y abierta. Sin embargo, para participar en la operación de su moneda (XRP) o en su compañía (Ripple) se requiere del permiso de un grupo reducido. Como ya se mencionó, la moneda es operada básicamente por 35 nodos, dominados por bancos e instituciones financieras, y el acceso a la compañía exige la aprobación de sus propietarios. Esto implica una centra-

lización tanto en la operación de la moneda como en el control de la compañía privada, lo que explica el carácter híbrido del proyecto.

Este caso se circunscribe a Estados Unidos. Sin embargo, la Unión Europea publicó el 9 de junio de 2023 su reglamento 1114 relativo a los mercados de criptoactivos (MICA, por sus siglas en inglés), que establece normas claras para la emisión y operación de las criptomonedas mediante diversos prestadores de servicios. Estas disposiciones entraron en vigor desde el 30 de diciembre de 2024, adelantándose a la regulación estadounidense, donde la Comisión de Valores y Bolsa, encargada de los valores, y la Comisión de Futuros de Materias Primas (CFTC, por sus siglas en inglés), que establece las normas de las mercancías o materias primas (*commodities*), competían por aplicar las reglas antiguas a este nuevo espacio. El debate ha llegado al Congreso, donde algunos miembros han propuesto nuevos proyectos y, con el nombramiento del presidente Trump, se produjo la renuncia del presidente de la SEC, en medio de las críticas por las múltiples demandas interpuestas contra la nueva industria cripto.

Con la segunda llegada del presidente Trump al poder en 2025, marcada por una postura abiertamente favorable al ecosistema de las criptomonedas y por el control de su partido en el Congreso, se ha logrado modificar o actualizar las leyes del siglo pasado. Un avance regulatorio relevante inició el 17 de junio de 2025, cuando la Cámara de Representantes aprobó la ley destinada a regular las monedas estables, conocida como GENIUS (*Guiding and Establishing National Innovation for U. S. Stablecoins*, por sus siglas en inglés). La iniciativa fue enviada al Senado, que la aprobó el 17 de julio y fue firmada por el presidente un día después en la Casa Blanca.

Las monedas estables serán estudiadas en las siguientes secciones de este capítulo; no obstante, conviene exponer aquí, de manera sintética, los principales alcances de la ley GENIUS. Esta norma exige a las entidades y bancos con depósitos no asegurados que emitan monedas estables de pago para mantener un colateral equivalente al cien por ciento del dólar estadounidense. Dicho respaldo puede consistir en inversiones en activos líquidos, como letras, notas o bonos del Tesoro, reportos que tengan un periodo máximo de 93 días, o con los mismos dólares. Además, exige que los emisores den a conocer de manera mensual la composición de sus reservas. La ley busca proteger a los consumidores, ya que, en caso de que los emisores quiebren, los tenedores de las monedas estables tendrían prioridad de cobro frente a otros acreedores. Asimismo, los emisores deberán cumplir las reglas del Grupo de Acción Financiera Internacional (GAFI), incluidas aquellas relacionadas con la prevención del lavado de dinero y el

financiamiento al terrorismo. Sin embargo, podrán conservar íntegramente el rendimiento de los bonos, notas o letras del Tesoro, que actualmente se sitúan entre el cuatro y el cinco por ciento. Esta ley incrementará la demanda de las emisiones del Tesoro, por lo que el gobierno podrá emitir una mayor cantidad de deuda adquirida por los emisores, reduciendo la necesidad de que el banco central la compre y, con ello, mitiguen el incremento de la emisión de dinero.

Ya se han apuntado varias entidades, entre ellas J. P. Morgan, Citigroup, Amazon, Walmart y distintas cámaras de compensación. La ley asigna la supervisión de las monedas estables a la Oficina del Contralor de la Moneda (OCC, por sus siglas en inglés), dependiente del Departamento del Tesoro, siempre que se trate de emisiones de diez billones de dólares o más. Los emisores de menor tamaño serán responsabilidad de los reguladores estatales. Esta ley entrará en vigor 18 meses después de su promulgación o cuatro meses después de que los reguladores emitan las reglas secundarias, lo que ocurra primero. De igual manera, ordena la realización de un estudio para explorar el tratamiento regulatorio de las monedas estables que no sean de pago, cuyo reporte deberá concluirse en el plazo de un año.

Conviene informar al lector que el presidente Trump y su familia, a través de World Liberty Financial, lanzaron en marzo de 2025 la moneda estable USD1, cuyo valor de capitalización asciende a 3.3 billones de dólares, lo que la ubica en el lugar 45 de CoinGecko. World Liberty Financial Inc. fue constituida en Delaware como una empresa que no tiene acciones, aunque con un protocolo de finanzas descentralizadas, y es propietaria de la marca USD1. También es operadora de la gobernabilidad de la plataforma de su empresa controladora, WLF Holdco LLC, la cual tiene derecho a todos los ingresos que provengan de los tókenes de gobernanza $WLFI.

Las reservas de la moneda estable USD1 son administradas por BitGo Trusted Company, incorporada en Dakota del Sur, Estados Unidos, o por BitGo Technologies LLC, ambas con múltiples licencias para operar como transmisores de dinero o como proveedores globales de infraestructura. Las monedas son acuñadas en las cadenas de bloques de Ethereum, BSC y Tron, y negociadas en varias plataformas de finanzas descentralizadas, entre las que destacan Uniswap y Pancakeswap. Se deja aquí expuesta esta compleja estructura legal, y corresponde al lector valorar si representa o no un conflicto de interés para el presidente Trump y su familia.

El periodo comprendido entre el 14 y el 18 de julio de 2025 fue conocido como la «semana cripto», no solo por la ley GENIUS, sino también porque la Cámara de Representantes aprobó dos iniciativas más que fueron

enviadas al Senado. La primera, conocida como ley CLARITY (*Digital Asset Market Structure Clarity Act*), define las diferentes clasificaciones (o taxonomía) de los activos digitales, como tókenes de instrumentos financieros, de materias primas, de uso comercial o consumo. Además, establece la obligatoriedad del registro de los intermediarios y propone reglas claras para la custodia y operación de las fichas. La segunda iniciativa, denominada CBDC *Anti-Surveillance State Act*, prohíbe la creación de una moneda digital del banco central, con el objetivo de salvaguardar la privacidad de las personas. Estas dos iniciativas serán consideradas por el Senado en 2026.

Las criptomonedas y su ecosistema surgieron y se desarrollaron en Estados Unidos, pero la falta de claridad regulatoria provocó que los proyectos y las empresas migraran a lugares más favorables. En este contexto, estas tres leyes pretenden crear un marco adecuado para que retornen.

Al retomar la única ley aprobada, es importante considerar que el mercado de las monedas estables ronda en los 260 billones de dólares; ante ello, el secretario del Tesoro, Scott Bessent, explicó en el Congreso que, al considerar esta nueva ley, el mercado podría crecer a dos trillones de dólares en los próximos años. Adicionalmente, los congresistas consideran que este escenario económico podría generar certidumbre para que el ámbito cripto crezca con seguridad. Con lo anterior dicho, Trump ha dado un primer paso para tratar de cumplir su promesa de convertir a Estados Unidos en el país líder de activos digitales, así como transformarse en la capital cripto del mundo. En el capítulo 3 se abordarán las distintas perspectivas mundiales y la regulación de las criptomonedas en México.

La centralización de lo descentralizado

Con el paso del tiempo se ha demostrado que la gran mayoría de los precios de mercado de las criptomonedas son altamente volátiles, con variaciones por día, hora o minuto, que fácilmente pueden alcanzar cambios de dos dígitos. Esta característica las vuelve inviables para cumplir funciones monetarias básicas, ya sea como medio de intercambio o como de unidad de cuenta. Más allá del tema especulativo y del riesgo tecnológico, esta inestabilidad impide la existencia de una base monetaria estable para la oferta de servicios financieros. Conviene recordar que sin dinero estable no hay anclaje monetario y, por ende, no hay finanzas. De esta necesidad surgen las denominadas monedas estables (*stablecoins*), ya mencionadas en párrafos anteriores.

Aunque existen diversos tipos de monedas estables, en primer lugar destacan aquellas que tienen un respaldo, colateral o reserva que está fuera de la cadena de bloques (*off-chain*), es decir, de inversiones centralizadas en cualquiera de las principales monedas oficiales (fíat) de las economías del mundo, particularmente el dólar de Estados Unidos.

El funcionamiento de este tipo de monedas estables inicia con su depósito de dinero fíat en la cuenta bancaria de una compañía centralizada, la cual lo recibe e invierte en diversos instrumentos financieros, como bonos del Tesoro. Esta compañía está plenamente identificada en el mundo físico y recaba sus datos personales con el fin de cumplir con las reglas del conocimiento del cliente (KYC, por sus siglas en inglés). Si el usuario deposita 100 dólares, la empresa crea (emite) 100 monedas virtuales en una cadena de bloques de su propiedad o rentada y se la enviará a su monedero (*wallet*). Alternativamente, si la moneda estable se adquiere en el mercado secundario, tiene la opción de dejarla en custodia de la casa de intercambio centralizada (CEX) utilizada para la compra o transferirla a su propio monedero. Suponiendo que no hay ningún tipo de comisiones, la compañía gana intereses o ganancias de capital derivado de sus inversiones, mismas que deberán ser suficientes para compensar sus gastos operativos. La persona física o moral que la recibe está en posesión de una criptomoneda cuyo precio se mantiene cercano a la unidad fíat (paridad uno a uno), y puede utilizarla para sus consumos o efectuar transferencias internacionales rápidas y de bajo costo. También tiene la opción de mantenerla en su cuenta y devolverla a la compañía para obtener de regreso su dinero fíat.

En la mayoría de los casos, la moneda estable recibida no es una ficha (token) nativa, lo que significa que no tiene una cadena de bloques propia que la respalda. Aun así, al usar una cadena de bloques rentada, se considera que las monedas estables funcionan como un puente entre las finanzas centralizadas y las descentralizadas, lo que le da sentido al título de esta sección.

Debe advertirse al lector que el uso de este tipo de monedas estables implica asumir el riesgo de la contraparte, es decir, el riesgo asociado a la compañía en la que se depositó el dinero fíat. De ahí la importancia de exigir plena transparencia respecto de las inversiones que garantizan la paridad y la posibilidad de redimir el depósito original en cualquier momento. Adicionalmente, se corre el riesgo tecnológico asociado al uso de criptomonedas.

La más popular de estas monedas estables es tether, surgida en 2014, que mantiene una paridad uno a uno con el dólar estadounidense (USDT)

y ocupa el tercer lugar en la tabla 4, con un valor de capitalización de 186 billones de dólares. Sus cofundadores son Brock Pierce, Craig Sellars y Reeve Collins. Al menos en teoría, tether mantiene en sus cuentas bancarias el equivalente de un dólar por cada unidad en circulación. A pesar de todo, desde 2019 existe controversia en torno a dicha paridad, luego de que sus abogados afirmaran que solo el 74 % de las reservas estaba respaldado por efectivo, cuentas bancarias e inversiones financieras en dólares, mientras que el resto correspondía a cuentas por cobrar a empresas afiliadas. Esta controversia parece haberse atenuado en años recientes, dado que la empresa ha comenzado a publicar la composición de sus reservas. Sin embargo, en abril de 2025 concretó un acuerdo con la empresa Adecoagro, que cotiza en el NYSE (AGRO), para adquirir el 70 % de sus acciones por un monto cercano a los 600 millones de dólares. Esta operación ha sido posible debido a que tether no está constituida en los Estados Unidos y a la aparente obtención de utilidades que ha acumulado, derivada de las altas tasas de interés de los bonos del Tesoro del gobierno estadounidense. Actualmente, la empresa afirma que sus reservas superan el 100 % de sus emisiones.

Originalmente, USDT se emitió como un token de la segunda capa de Bitcoin (véase la figura 1), con la particularidad de utilizar un esquema de prueba de trabajo para lograr consenso. Posteriormente, se implementó como token estandarizado ERC-20 en Etherum, así como en EOS, Tron y otras plataformas en las que actualmente se negocia.

Originalmente los tókenes de tether eran emitidos y gestionados por Tether Limited, empresa que, de acuerdo con su libro blanco, estaba incorporada en Hong Kong, mantenía cuentas en Taiwán y contaba con algún registro administrativo en Estados Unidos. Su empresa controladora, Tether Holding Limited, estaba incorporada en las Islas Vírgenes Británicas, donde posee diversas subsidiarias. Tether Limited tiene vínculos con la casa de intercambio de criptomonedas Bitfinex, propiedad de iFinex, también registrada en las Islas Vírgenes Británicas. Bitfinex ha enfrentado diversos incidentes cuya explicación no siempre ha sido del todo clara. Desde 2025, una parte importante del conglomerado relocalizó su negocio en El Salvador, donde opera a nivel global con una licencia para proveer activos digitales otorgada por el gobierno local. La compañía ha anunciado, además, su intención de establecerse en territorio estadounidense, cumplir con la nueva ley GENIUS y emitir otra moneda estable para competir localmente con USDC y conservar su liderazgo mundial.

Las inversiones de tether se han incrementado de manera exponencial mediante la adquisición de más de cien empresas, lo que la ha convertido en uno de los principales mineros de Bitcoin a escala global. Recientemente, logró recaudar 500 millones de dólares en cuestión de minutos con el objetivo de crear su propia cadena de bloques especializada en monedas estables, denominada Plasma, para no depender de terceros. En otras palabras, busca complementar la distribución de sus tókenes mediante el uso de infraestructura propia, que también ofrecerá en renta a terceros. A pesar de ello, su principal problema continúa siendo la escasa —o nula— transparencia en el uso de sus reservas y una administración opaca, facilitada por su registro en jurisdicciones que tienen reglas débiles para la protección de los usuarios.

Desde hace algunos años, tether publica documentos sobre sus reservas que son «certificados suavemente» por la empresa BDO Italia. Con base en esta información, S&P ha elaborado reportes periódicos no solicitados para evaluar su paridad con el dólar (*stablecoin stability assesment*). Las evaluaciones se estructuran en cinco estratos: uno (paridad muy fuerte), dos (fuerte), tres (adecuada), cuatro (apretada) y cinco (paridad débil). La última evaluación preparada por S&P el 26 de noviembre de 2025, con resultados al tercer trimestre, muestran que las reservas han disminuido en el último año de 105 % a 103.9 %. Asimismo, revela que su composición actual consiste en 76 % de instrumentos del banco central estadounidense y el resto con activos de mayor riesgo y baja transparencia, como bonos corporativos, Bitcoin y metales preciosos. Como consecuencia, S&P modificó la calificación de las reservas de tether de apretadas (nivel 4) a débiles (nivel 5). El lector tiene la última palabra para evaluar la solidez de la plataforma de monedas estables con mayor capitalización a escala mundial. Cabe recordar que tether no cuenta con el seguro de depósitos equivalente al de los bancos tradicionales, ni dispone de un banco central que actúe como prestamista de última instancia.

Continuamos con el grupo empresarial Binance, que aparece en el cuarto lugar de la tabla 4. La empresa principal inició en 2017 con el establecimiento casi simultáneo de una casa de intercambio centralizada de criptomonedas en Estados Unidos y el lanzamiento de una criptomoneda (token ERC-20), desarrollada sobre la cadena de bloques de Ethereum, a la que denominó originalmente Binance (BNB). Para este propósito, realizó una oferta inicial de monedas entre el 26 de junio y el 3 de julio de 2017. El objetivo original consistía en utilizar su criptomoneda como medio para facilitar las transacciones dentro de su casa de intercambio. Casi dos años

después, en 2019, Binance creó su propia cadena de bloques, hoy llamada *Binance Smart Chain* (BSC), y decidió emitir su moneda nativa con sus propios estándares (*Binance Evolution Proposal* 2, BEP2). Para ello, los tókenes de Ethereum fueron intercambiados uno a uno por la nueva moneda nativa (BNB). Ese mismo año, en colaboración con Paxos, creó una moneda estable respaldada uno a uno por dólares estadounidenses, denominada Binance USD (BUSD), la cual obtuvo la validación del Departamento de Servicios Financieros del Estado de Nueva York (NYDFS, por sus siglas en inglés). Para tratar de diferenciarse de otras monedas estables, Binance destacaba tanto dicha validación como su compromiso de publicar mensualmente en su sitio web un informe de auditoría sobre las inversiones financieras realizadas. Al momento de escribir estas líneas, BUSD ocupaba la posición 205 en Geicko, con un valor de capitalización de 313 millones de dólares, mientras que BNB —la moneda nativa y su cadena de bloque— se ubicaba en el cuarto lugar, con un valor de 118 billones de dólares.

Binance ofrece servicios de infraestructura en prácticamente todo el ecosistema cripto, a través de una red de más de doce empresas centralizadas localizadas en distintas jurisdicciones, entre las que destacan las Islas Caimán. Todas ellas están lideradas por Changpeng Zhao (conocido como CZ), principal accionista y primer director general (CEO) del grupo. Tras casi seis años de operación en Estados Unidos, el 27 de marzo de 2023 la Comisión de Futuros de Materias Primas (CFTC, por sus siglas en inglés) demandó a la casa de intercambio Binance por operar ilegalmente en Estados Unidos y a Changpeng Zhao por evadir de manera premeditada la ley federal. Ese mismo día, el expresidente de la CFTC, Rostin Behnam, declaró:

> *Por años, Binance sabía que estaba violando las reglas de la Comisión, trabajando activamente tanto para mantener el flujo de dinero como para evadir el cumplimiento de las reglas. Esto debería ser un aviso para cualquiera del mundo digital de que la CFTC no tolerará la evasión de la ley de los Estados Unidos. (CFTC, 2023)*

Adicionalmente, el 5 de junio de 2023, la Comisión de Valores y Bolsa de Estados Unidos interpuso trece denuncias contra diferentes enti-

dades de Binance y contra Changpeng Zhao, entre las que destacan la operación de su casa de intercambio con activos virtuales sin registro alguno, falsear los controles de operación y vigilancia de la plataforma Binance.US, y el ofrecimiento y venta de valores no registrados. El 21 de noviembre de 2023, Zhao se declaró culpable, y el monto total de penalizaciones superó los cuatro billones de dólares. Como parte de las medidas correctivas, se le obligó a abandonar la dirección de su conglomerado y se nombraron supervisores y nuevos miembros del consejo; aun así, las empresas continuaron operando.

De igual manera, se demostró que más de cien mil operaciones ilícitas fueron realizadas a través de Binance, relacionadas con lavado de dinero, financiamiento al terrorismo, narcotráfico y abuso de menores. Posteriormente, el 30 de abril de 2024, Zhao fue sentenciado a cuatro meses de prisión, tras admitir que no implementó adecuadamente los controles contra el lavado de dinero. El resultado final fue de una multa histórica para Binance, mientras que la sanción personal para CZ fue limitada en términos de la privación de su libertad. En este contexto, cobra relevancia la frase «más vale pedir perdón que pedir permiso».

En la actualidad, Binance continúa trabajando en Estados Unidos de manera supervisada, y aunque ha perdido clientes, mantiene un crecimiento sostenido en el resto del mundo. *The Wall Street Journal*, en su edición del 10 de marzo de 2025, publicó que «representantes de la familia del presidente Trump han mantenido conversaciones para adquirir una participación financiera en la filial estadounidense de la casa de cambio centralizada Binance». En consonancia con lo anterior, la revista semanal *The Economist* dedicó su portada del 15 de mayo de 2025 a la estrecha relación entre el gobierno del presidente Trump y el sector de las criptomonedas. El título original puede consultarse en la bibliografía; en este trabajo se ha traducido como «Cripto se junta con el gobierno federal: por qué no terminará bien». Los dos artículos que integran dicha edición exponen diversos conflictos de interés entre los negocios de la familia del presidente Trump (World Liberty Financial y su token de gobernanza $ WLFT, la moneda estable USD1, la criptomoneda $TRUMP y Trump Media) y el ecosistema de las criptomonedas. Se destacan dos ejemplos principales. El primero se relaciona con las altas donaciones, directas o indirectas, de empresas como Ripple a campañas políticas, así como el retiro de numerosos casos que la Comisión de Valores y Bolsa ha desechado o congelado. El segundo escándalo alude a la inversión cercana a dos billones de dólares que la empresa MGX del gobierno de Abu Dabi inyectó a Binance mediante el uso de la moneda estable USD1,

emitida por World Liberty Financial. Estos casos evidencian que el apoyo financiero del sector cripto a los negocios de la familia presidencial se ha traducido en un mayor acceso al poder gubernamental. Los artículos advierten que esta relación difícilmente tendrá un desenlace favorable, al quedar sujeta a las fluctuaciones políticas de su benefactor.

Los autores de este libro complementan la información anterior con tres datos adicionales vinculados con la familia Trump. En primer lugar, resaltamos que World Liberty Financial (WLF) ha celebrado tratos formales con lo más altos niveles del gobierno de Pakistán para auxiliarlos en la implementación de todo lo relacionado con las criptomonedas, en general, y con la minería de Bitcoin, en particular. En este marco, el gobierno pakistaní se comprometió a cambiar las leyes necesarias y a proveer la energía eléctrica necesaria para su implementación. De la misma forma, el gobierno de Pakistán también ha involucrado al fundador de Binance (CZ), ante la ambición de convertir al país en el centro principal de criptomonedas del sur de Asia. En segundo lugar, destacamos que el presidente Trump, un día después de su segunda toma de posesión, indultó a Ross Ulbricht, creador de Silk Road, el mayor mercado del internet oscuro, que utilizaba Bitcoin para facilitar la venta de drogas por millones de dólares y que había sido condenado a cadena perpetua en 2015. En tercer lugar, el 23 de octubre de 2025, el presidente Trump ejerció su autoridad constitucional para indultar a Changpeng Zhao, cuya trayectoria se abordó anteriormente. Esta decisión abrió las puertas para que CZ regrese a operar en Estados Unidos y reasuma la dirección del grupo Binance. Tras el indulto, CZ escribió en su cuenta de X que estaba «profundamente agradecido por el indulto de hoy y al presidente Trump por defender el compromiso de Estados Unidos con la equidad, la innovación y la justicia. Haremos todo lo posible para ayudar a que América sea la capital cripto del mundo, así como avanzar la web3». Entre este y otros factores, el precio de BNB se incrementó de manera significativa, hasta ocupar temporalmente la cuarta posición en la tabla 4. Resulta llamativo que esto se produjera después del apoyo de CZ para posicionar a WLF en el espacio cripto.

La ironía radica en que el objetivo original de las criptomonedas era eliminar a los intermediarios gubernamentales para permitir transacciones entre particulares. A pesar de ello, tanto en Estados Unidos como en Pakistán, el sector cripto ha decidido integrarse al gobierno, permitiendo que los políticos y sus familiares también operen en la creación y operación de estos servicios.

En la tabla 4 también se encuentra USD Coin (USDC), moneda estable lanzada en 2018 con el apoyo de Coinbase —casa de cambio de criptomonedas centralizada que cotiza en el Nasdaq y tiene sede en San Francisco—, y de Circle Internet Group, empresa global de tecnología financiera para servicios de pagos entre pares, que cotiza sus acciones en el NYSE. Ambas empresas formaron el consorcio The Center, con sede en Estados Unidos. USDC trata de mantener la paridad con el dólar estadounidense y se promociona como una moneda más transparente, ya que ha contratado a una empresa auditora que verifica los niveles de efectivo y otros saldos que se mantienen en reserva, así como su correspondencia con el número de criptomonedas en circulación. Esta auditoría se da a conocer al público de manera periódica. Actualmente se ubica en la sexta posición con un valor de capitalización de 76 billones de dólares. Desde sus inicios, USDC se diseñó como un token ERC-20 de Ethereum, a través de la implementación de un contrato inteligente sobre la base de la cadena de bloques que usa programas de computación que son Turing completos.

Respecto de las empresas que integran The Center, se señala que Coinbase lanzó, en noviembre de 2025, una plataforma para la colocación de ofertas públicas iniciales (ICO) dirigida a inversionistas de menudo. El esquema contempla una oferta mensual y utiliza la moneda estable USDC para los pagos correspondientes. Se aclara que Coinbase no emite ni vende los tókenes ofrecidos, sino que únicamente provee la plataforma sin costo para los compradores y con una comisión para los colocadores, quienes suelen establecerse legalmente en las Islas Caimán o en las Islas Vírgenes Británicas.

Por su parte, Circle ha realizado más de cuarenta operaciones de fusiones y adquisiciones en los últimos años y se mantiene como un referente para proveer de infraestructura a los emisores de monedas estables con respaldo de moneda fíat en Brasil, Japón, Canadá y México. En este último caso, desde 2024 existe una moneda estable respaldada uno a uno con el peso mexicano, mediante depósitos en las empresas Nvio —institución financiera de fondos de pago electrónico que es parte de Bitso—, Banco Ualá y Hey Banco. El proyecto inició con el apoyo de Circle, mediante un cambio de su protocolo (*fork*) de su repositorio de contratos inteligentes, y se implementó como un token ERC-20 en Ethereum y Arbitrum. Es emitido por Juno (EM EX CI, S. de R. L. de C. V.), subsidiaria de Bitso, que opera con un registro obtenido en El Salvador. La moneda estable MXNB está listada en CoinGecko y ocupa la posición 3,126, con un precio de 0.05387 dólares y un valor de capitalización de 1.95 millones de dólares.

La filial mexicana de BDO —empresa de contadores públicos y consultores de negocios— da a conocer de manera trimestral un informe de valuación financiera. En su reporte del 30 de septiembre de 2025 describe que existían en circulación 30.5 millones de fichas de MXNB y que los depósitos en las cuentas bancarias ascendían a 30.6 millones de pesos mexicanos. Se precisa que dicha información no fue obtenida directamente de las instituciones financieras, sino de los documentos entregados por Juno. Se trata de un proyecto de escala reducida, con bajos volúmenes de operación, que no ha podido consolidarse, entre otros factores, debido a la falta de claridad de las regulaciones en México.

Más allá de las monedas estables, existe un segundo ejemplo en los mercados de valores que ha servido de puente entre el mundo cripto y el sector bursátil tradicional: los fondos de inversión cotizados en las bolsas de valores (ETF, por sus siglas en inglés). Normalmente los fondos de inversión se establecen para lograr un portafolio diversificado y están dirigidos a los inversionistas de menudeo. Sin embargo, también existen fondos que tratan de replicar el rendimiento de un índice (como el S&P 500), de un activo (como el oro) o de una estrategia de inversión (como la de Warren Buffett). El 10 de enero de 2024, la Comisión de Bolsa y Valores de Estados Unidos aprobó el listado y la negociación de once fondos (ETF) de contado de bitcoin. La SEC ha considerado tanto a bitcoin como a ether como mercancías o materias prima (*commodities*), y no como un valor. De hecho, durante la administración de Biden se consideró que la gran mayoría de los criptoactivos eran un valor (instrumento financiero) sujeto a regulación. Aunque en 2021 se aprobó un ETF de futuros de Bitcoin, la Comisión se mostró renuente a aceptar cualquier ETF de contado del Bitcoin, hasta que la Corte de Apelaciones del Distrito de Columbia devolvió una demanda del fideicomiso Grayscale que contenía bitcoins, lo que finalmente la presionó a conceder dichas autorizaciones.

Hoy en día, usted puede invertir su dinero en cualquiera de los fondos listados en la Bolsa de Nueva York (NYSE) y el Nasdaq de manera más simple. Las acciones de estos fondos ofrecen un rendimiento similar al de cambio de precios del bitcoin. Se habla de una similitud y no de una equivalencia exacta, porque es necesario cubrir una pequeña comisión por su negociación y por su custodia. Al invertir, usted será poseedor de una acción del fondo de inversión y la custodia de los bitcoins las tendrá un tercero, entre los que destacan Coinbase y Gemeni. Por lo general, los custodios son una entidad distinta de los promotores o emisores del fondo, como BlackRock, Fidelity y GrayScale. Al usar un ETF, usted no necesitará

contar con un monedero basado en criptografía ni memorizar su clave privada, compuesta por 12 o 24 palabras, conocidas como semilla. Como se detalla en el anexo 1, para poseer bitcoins de manera directa es indispensable contar con dicha semilla. Andrea Antanopoulos resume esta idea en la frase: «Si no tienes tu semilla, no tienes tus monedas». Con la introducción de los ETF de contado de Bitcoin, usted puede, de manera indirecta, tener sus monedas sin tener su semilla. Solo requiere de una cuenta con una casa de bolsa y adquirir acciones de alguno de los fondos de inversión autorizados para cotizar en las bolsas de valores. Esta vía ofrece mayor transparencia y evitará posibles fraudes. El 23 de julio de 2024, la SEC también aprobó múltiples ETF de contado para ether. De este modo, actualmente en Estados Unidos existen dos fichas que pueden ser negociadas mediante fondos de inversión cotizados en las bolsas de valores. A ello se suma la aprobación, a principios de 2025, para que los ETF puedan ofrecer una mezcla o combinación entre bitcoin y ether.

Durante la primera semana de agosto de 2025, el total de activos bajo administración de los ETF de contado del bitcoin superó los 162 billones de dólares, cifra que representaba el 7.4 % de su valor de capitalización de 2.19 trillones de dólares. Esta adopción del bitcoin por parte de inversionistas del sistema financiero tradicional ha crecido rápidamente y supera el valor de los ETF de contado de ether, cuyos activos netos rondan los 20 billones de dólares. Sin embargo, los ETF de bitcoin solo representan cerca de la mitad de los ETF de oro, que en la misma fecha ascendían a 325 billones de dólares, con un valor de capitalización de 23.5 trillones de dólares. Tanto el bitcoin como el oro tienen aplicaciones financieras, pero el segundo también se utiliza para joyería y en usos industriales. Para los inversionistas que consideran al bitcoin como el «nuevo oro» o el «oro digital», los autores de este libro recuerdan que el valor de capitalización del oro es diez veces mayor y que sus ETF duplican los activos bajo administración. Ante este panorama, ¿usted prefiere un ETF del oro o uno de bitcoin?

Es importante añadir que J. P. Morgan ya acepta los ETF como garantía para otorgar préstamos a sus clientes institucionales y tiene planeada su extensión para aceptar bitcoin y ether en los próximos meses. Al igual que en el caso de los ETF, la institución se apoyará en empresas independientes para custodiar los criptoactivos, lo que debería de incrementar la confianza en el proyecto.

En la misma línea, Vanguard, la segunda empresa de administración de fondos a escala global, con 50 millones de clientes que manejan más de once trillones de dólares, ha cambiado radicalmente su estrategia.

Desde el 3 de diciembre de 2025 permite que sus clientes puedan negociar en su plataforma algunos fondos de inversión cotizados en bolsa (ETF) de criptomonedas.

También Citi, Schwab y otras instituciones financieras han anunciado planes para ofrecer ETF de criptomonedas a partir de 2026. Todo ello apunta a una creciente adopción institucional, que podría mejorar la credibilidad y madurez del espacio de las criptomonedas, al menos de activos virtuales como bitcoin, ether y SOL.

La Bolsa Mexicana de Valores y la Bolsa Institucional de Valores no solo cotizan las acciones de las empresas residentes en nuestro país, sino que también cuentan con una sección denominada Mercado Global o Sistema Internacional de Cotizaciones (SIC), en la que se cotizan más de 1,500 ETF de Estados Unidos, Europa, Asia, Sudamérica y otras regiones. Hasta el momento de escribir estas líneas, ni la BMV ni la BIVA habían recibido la autorización de las autoridades mexicanas para listar los nuevos fondos de inversión cotizados en las bolsas de valores de bitcoin y ether en el SIC. Sin embargo, en México ya se pueden adquirir algunos de estos ETF de bitcoin cotizados en Estados Unidos mediante las plataformas de la casa de bolsa GBM (GBM+ y su nueva aplicación), a través de la sección Trading Global. GBM tiene una asociación con Mercado Pago, que a su vez tiene una alianza con Paxos.

Esta centralización para negociar bitcoin y ether a través de ETF ha crecido de manera exponencial, y el volumen diario de operación supera los billones de dólares en las diferentes bolsas estadounidenses. Los seguidores del bitcoin original, que buscaban eliminar intermediarios y realizar solo pagos en efectivo entre pares, han sufrido un duro golpe, aunque continúan su operación. En última instancia, negociar criptomonedas de manera descentralizada no es incompatible con hacerlo a través de un intermediario regulado o no. De hecho, el tercer ejemplo de la centralización de lo descentralizado se materializó desde 2010 con las casas de intercambio centralizadas (*centralized exchanges* o CEX), que actualmente compiten con las casas de intercambio descentralizadas (*decentralized exchanges* o DEX). Si el lector tiene interés en profundizar en su funcionamiento y diferencias, lo referimos al segundo capítulo, en la sección titulada «Otro sistema financiero alternativo».

De las monedas estables a las finanzas descentralizadas (DeFi)

En el mismo nivel de las monedas estables que tienen como reserva a una o varias monedas fíat que se encuentran fuera de la cadena de bloques (*off-chain*), se incluyen las que tienen como colateral a materias primas, como el oro o el petróleo. Aun así, es necesario agregar otras dos categorías en función de su mecanismo de estabilización. El primer grupo lo constituyen aquellas que tienen como colateral otras criptomonedas que se encuentran en la cadena de bloques (*on-chain*). En el segundo, se ubican aquellas que no se basan en reservas, pero que implementan un algoritmo útil para influir en la oferta y en la demanda de la moneda estable. Un ejemplo de lo anterior es la creación de Terra (UST), a finales de 2020, que buscaba mantener la paridad con un dólar estadounidense mediante la emisión de la criptomoneda Luna —su token hermano— usando el protocolo algorítmico Anchor. A pesar de que tuvo un inicio exitoso, los usuarios perdieron la confianza en su operación, ya que pagaba tasas de interés insostenibles —de dos dígitos— que le provocaron pérdidas enormes. Como consecuencia, la *stablecoin* colapsó en mayo de 2022. En la actualidad, la mayoría de los inversionistas que perdieron su dinero opinan que se trató de una estafa y no de un algoritmo. Con el ejemplo anterior, se advierte al lector que es responsable de revisar con cuidado el libro blanco si quiere invertir en estos mecanismos sin respaldo alguno y que, además, debe dar seguimiento a la información de las operaciones —que son públicas— en la cadena de bloques.

El proyecto DAI permite explicar de manera integrada tanto las monedas estables que tienen como colateral a otras criptomonedas, como aquellas que, sin reservas, buscan influir en la oferta y la demanda mediante algoritmos computacionales. Es decir, DAI nos permite explicar de manera conjunta las dos categorías, con el objetivo de conservar algunas de las principales virtudes de las criptomonedas: la descentralización, la transparencia de sus operaciones y la apertura (resistencia a la censura). Así como las monedas estables con respaldo de una moneda fíat pueden considerarse una condición necesaria, aunque no suficiente, de las finanzas descentralizadas, el protocolo DAI puede analizarse también como una de las primeras aplicaciones representativas de este ecosistema.

El comienzo de DAI se remonta a 2014, cuando el danés Rune Christensen inició MakerDAO como un proyecto de código abierto en la cadena de bloques de Ethereum. Las últimas tres letras del nombre corresponden a las iniciales de *Decentralized Autonomous Organization* (DAO), que se traduce como organización autónoma descentralizada. Este tipo de organización no guarda similitud con las formas corporativas tradicionales —como las sociedades anónimas, sociedades de responsabilidad limitadas o sociedades cooperativas—, las cuales se constituyen ante fedatarios públicos y se inscriben en los registros públicos de comercio. Todas estas estructuras legales tienen una personalidad jurídica distinta de la de sus socios. MakerDAO, en cambio, se creó de forma íntegramente digital, opera en línea y está registrada mediante un contrato inteligente hospedado en Ethereum. En este sentido, más que una empresa convencional, puede considerarse un ente digital.

MakerDAO representa una comunidad ubicada en distintas partes del mundo, unida por el interés común de desarrollar una moneda estable ligada al dólar estadounidense, cuyo colateral original es el ether, la criptomoneda nativa de Ethereum. En 2015, inició operaciones únicamente entre sus desarrolladores, quienes, desde distintas partes del mundo, definieron el código, la documentación y la arquitectura. Para 2017 se finalizó el libro blanco, en él se describió un colateral único —el ether— para la emisión de la moneda estable DAI, vinculada al dólar de los Estados Unidos. A diferencia de USDT, USDC y BUSDM que tienen una vinculación fuerte con el dólar, DAI posee una fijación suave o débil. Lo anterior se debe a que los participantes depositan ether en los contratos inteligentes denominados bóvedas o cajas fuertes (*maker vaults*), que funcionan como garantía para la emisión de un número menor de DAI, la cual se entrega al depositante original.

En la actualidad, DAI puede adquirirse directamente en mercados secundarios, como Uniswap o Coinbase y utilizarse como cualquier otra criptomoneda: se puede intercambiar, transferir o emplearse para comprar bienes y servicios. Sin embargo, en la mayoría de los casos, se hace a través del mercado primario, donde el usuario deposita ether como garantía en la misma plataforma y obtiene, a cambio, una tasa de interés flexible. En este último caso, la emisión y la administración de DAI se llevan a cabo mediante el protocolo Maker que usa los contratos inteligentes (*maker vaults*). Es decir, el proceso inicia con el depósito de alguna cantidad específica de ether que se realiza en las supuestas bóvedas o cajas fuertes del contrato inteligente de MakerDAO hospedado en Ethereum. Por ejemplo,

si un usuario deposita 100 ether, estos quedan en custodia como garantía y permiten la emisión de 60 DAI, que se transfieren a su monedero a modo de préstamo de duración indefinida. Lo anterior ha dejado en claro que usted es libre de usar o consumir los 60 DAI; alternativamente, puede dejarlos en la misma plataforma para ahorrarlos y obtener una tasa de interés.

Como puede observarse, el monto recibido como préstamo (60 DAI) es inferior al valor del colateral aportado (100 ether), lo que equivale a un préstamo del 60 % del valor de la garantía. Esto es semejante a tener un préstamo equivalente al 60 % de su garantía. O a la inversa, su garantía representa 1.67 veces el préstamo recibido (100/60 = 1.67). Si el precio de ether aumenta de forma significativa y el usuario conserva los 60 DAI, puede intercambiarlos por ether para recuperar su garantía y obtener una utilidad. En cambio, si el precio de ether disminuye y el valor de la garantía pierde valor y se aproxima al valor del préstamo, el contrato inteligente vende automáticamente los ether para liquidar su posición.

Por un lado, los 60 DAI recibidos pueden invertirse en el mismo protocolo y generar una tasa de interés flexible (tasa de ahorro). Por otro, el préstamo en DAI, como cualquier obligación crediticia, tiene que pagar intereses sobre el saldo de esta. En este último caso, el protocolo establece una tasa de interés denominada comisión de estabilidad, y se calcula como una tasa compuesta que tiene que ser pagada al liquidar la deuda y cuyos ingresos van directamente al protocolo.

DAI utiliza un algoritmo para mantener su fijación suave con el dólar estadounidense. El objetivo fundamental es que el precio de un DAI sea igual al precio de un dólar. Para ello, se utiliza un mecanismo automático que ajusta el precio de un DAI para poder mantener la paridad en contextos de alta volatilidad. Por ejemplo, si el precio de un DAI es menor al de un dólar, el algoritmo incrementa la tasa de ahorro para estimular la demanda. En cambio, si el precio supera al dólar, se reduce dicha tasa para desincentivar la demanda. De manera complementaria, también puede ajustarse la comisión de estabilidad.

Existen otros factores que influyen en el resultado final de la oferta y demanda, como la definición de la política que establece los cambios máximos de precios en un periodo determinado. Esto es el equivalente a la puja (véase glosario) de los precios de las acciones cotizadas en bolsa y, en el caso de DAI, se conoce como parámetro de sensibilidad.

En paralelo al proyecto digital, Rune Christensen constituyó dos fundaciones con reconocimiento legal. En Dinamarca creó la Fundación Dai, encargada de la gestión de los activos digitales, como el registro de la mar-

ca comercial y los derechos de propiedad intelectual. De manera independiente, y junto con desarrolladores y socios externos, en 2018 se creó la Fundación Maker para el lanzamiento del protocolo descrito en los párrafos anteriores. Así, el proyecto combinó una estructura centralizada en el mundo jurídico con una arquitectura descentralizada en el ámbito digital. Tras varios incidentes y una demanda colectiva, se decidió que la Fundación Maker cediera el control a la comunidad del proyecto. Para ello, se emitieron fichas (tókenes) denominadas Maker (MKR), cuyos titulares, distribuidos globalmente, participan mediante votación en las decisiones clave relacionadas con el protocolo y la organización autónoma descentralizada MakerDAO. En este sentido, MakerDAO representa a la comunidad de desarrolladores, mientras que el token MKR constituye el mecanismo mediante el cual dicha comunidad se organiza y toma decisiones.

De esta manera, en 2019, la comunidad aceptó que DAI pudiera respaldarse con otras criptomonedas, además de ether, entre las que destaca wBTC (*wrapped bitcoin*). Los wbitcoins son tókenes (fichas) fungibles creados en Ethereum que están respaldados uno a uno por bitcoins depositados y bloqueados en otra unidad administrativa. El objetivo de esta operación es integrar el bitcoin en el espacio de las finanzas descentralizadas.

La mayoría de las veces, el precio de DAI se ha mantenido muy cercano al del dólar estadounidense, aunque el rango ha variado desde un punto mínimo de 0.88 dólares en marzo de 2023 hasta un máximo de 1.22 dólares en marzo de 2020. Cabe destacar que, durante la primera quincena de marzo de 2020, ether sufrió una caída de 47 % en cuestión de días, y el mecanismo de desconexión de emergencia de Maker (*emergency shutdown*) estuvo a punto de activarse. Los acontecimientos de esos días críticos de la pandemia por COVID-19 obligaron al algoritmo a liquidar una gran cantidad de posiciones para mantener la paridad de DAI con el dólar. Derivado de esta experiencia, y desde entonces, DAI también ofrece como garantía en los depósitos no solo ether y wbitcoin, sino también USDC.

Es importante hacer un paréntesis para subrayar que el hecho de que estas monedas se denominen estables no quiere decir que su precio se mantenga en el mismo nivel todo el tiempo. Como ya se mencionó en el párrafo anterior, los precios cambian y, en ocasiones, se alejan del objetivo paritario por un margen amplio. Por esta razón, algunos investigadores e inversionistas consideran que, con mayor propiedad, podrían denominarse monedas inestables.

A la fecha de elaboración de este texto, la moneda estable DAI —actualmente denominada USDS— ocupa la posición número 38 en cuanto a valor

de capitalización con 4.3 billones de dólares. Por su parte, el token (ficha) de gobierno corporativo de MakerDAO, MKR —hoy renombrado Sky—, se sitúa en el lugar número 73, con un valor de 1.5 billones de dólares.

El proyecto DAI se puede comparar con el funcionamiento de un criptobanco, donde los depósitos de sus cuentahabientes —denominados en ether, wbitcoin o USDC— pueden ser usados como garantía para obtener préstamos denominados en DAI. En este caso el intermediario no es una institución bancaria tradicional, sino el denominado contrato inteligente. Es una plataforma abierta, por lo que cualquier persona puede depositar las monedas autorizadas, así como todos tienen el derecho de obtener un préstamo en DAI, con la posibilidad de ganar intereses en sus ahorros y la obligación de pagar intereses en su préstamo recibido. Por lo mismo, DAI ha sido considerada como la primera aplicación de las finanzas descentralizadas cuyos pilares serán descritos en el siguiente capitulo. Es una aplicación descentralizada en la cadena de bloques de Ethereum con el uso de su moneda nativa ether.

En una primera instancia, la plataforma de contratos inteligentes genera dos tókenes: (a) MakerDAO, que representa a la comunidad interesada en el proyecto, y (b) su mecanismo de toma de decisiones o de gobernabilidad, basado en el token MKR. Posteriormente se desarrolla el protocolo Maker, el cual permite la creación de la moneda estable DAI mediante un algoritmo que la vincula al valor de un dólar estadounidense. En la actualidad, este protocolo también se conoce como un sistema múltiple de depósitos —o garantías— de diversas criptomonedas que genera la moneda estable DAI, misma que se apalanca con criptomonedas que son aprobadas por su gobierno corporativo (MKR).

A partir de lo anterior, se creó la aplicación de la plataforma oasis.app, en la que los usuarios pueden acceder de forma directa. El proceso es sencillo: si el usuario solicitó un préstamo en DAI, selecciona la criptomoneda que dejará como garantía y automáticamente genera los DAI correspondientes. Posteriormente, la plataforma ofrece la oportunidad de ahorrar sus DAI en el mismo entorno digital; si el usuario acepta, debe seleccionar la opción de depósito e indicar la cantidad que desea destinar para el ahorro. En caso contrario, es libre de usar sus DAI para cualquier otro fin. Con ello se concluye la descripción del proceso, dejando claro que tanto ether como DAI son ampliamente utilizadas dentro de las aplicaciones que componen las finanzas descentralizadas.

En septiembre de 2024, la comunidad de este ecosistema se actualizó y fortaleció con el objeto de consolidar una participación más relevante

dentro del ámbito de las finanzas descentralizadas. En este contexto, MakerDAO fue renombrado como Sky; la moneda DAI pasó a denominarse USDS, y la ficha Maker (MKR) se transformó en Sky token.

Una de las desventajas a las que se enfrentan los usuarios de las monedas estables es el denominado riesgo de la contraparte, que alude a la posibilidad de que la entidad que recibe el activo colateral haga un uso indebido de este y no se mantenga la paridad entre las reservas y las criptomonedas emitidas. Existen, además, otros riesgos que pueden provocar pérdidas económicas para los usuarios de las monedas estables. Por esta razón, en los bancos centrales de los tres países que han lanzado o implementado su moneda digital de menudeo —Bahamas, Jamaica y Nigeria— el riesgo de la contraparte es menor o no existiría, lo que podría disminuir el atractivo de muchas monedas estables privadas que actualmente ocupan lugares destacados en las listas de los valores de capitalización.

De acuerdo con cbdctracker.org, en septiembre de 2025, además de los tres países anteriormente mencionados, existían 97 naciones en la etapa de investigación (entre ellas México), 23 con pruebas piloto (como Rusia), 30 países en etapa de desarrollo y construcción (*proof of concept*), así como nueve que han cancelado su proyecto (entre ellos Estados Unidos).

En el caso de México, el informe anual del Banco de México sobre el ejercicio de las atribuciones conferidas por la Ley para Transparencia y Ordenamiento de los Servicios Financieros, publicado el 22 de noviembre de 2021, dio a conocer su trabajo y las etapas del proyecto. A continuación, se transcriben dos párrafos: el primero corresponde a la página 66 del reporte y el segundo al folio 67:

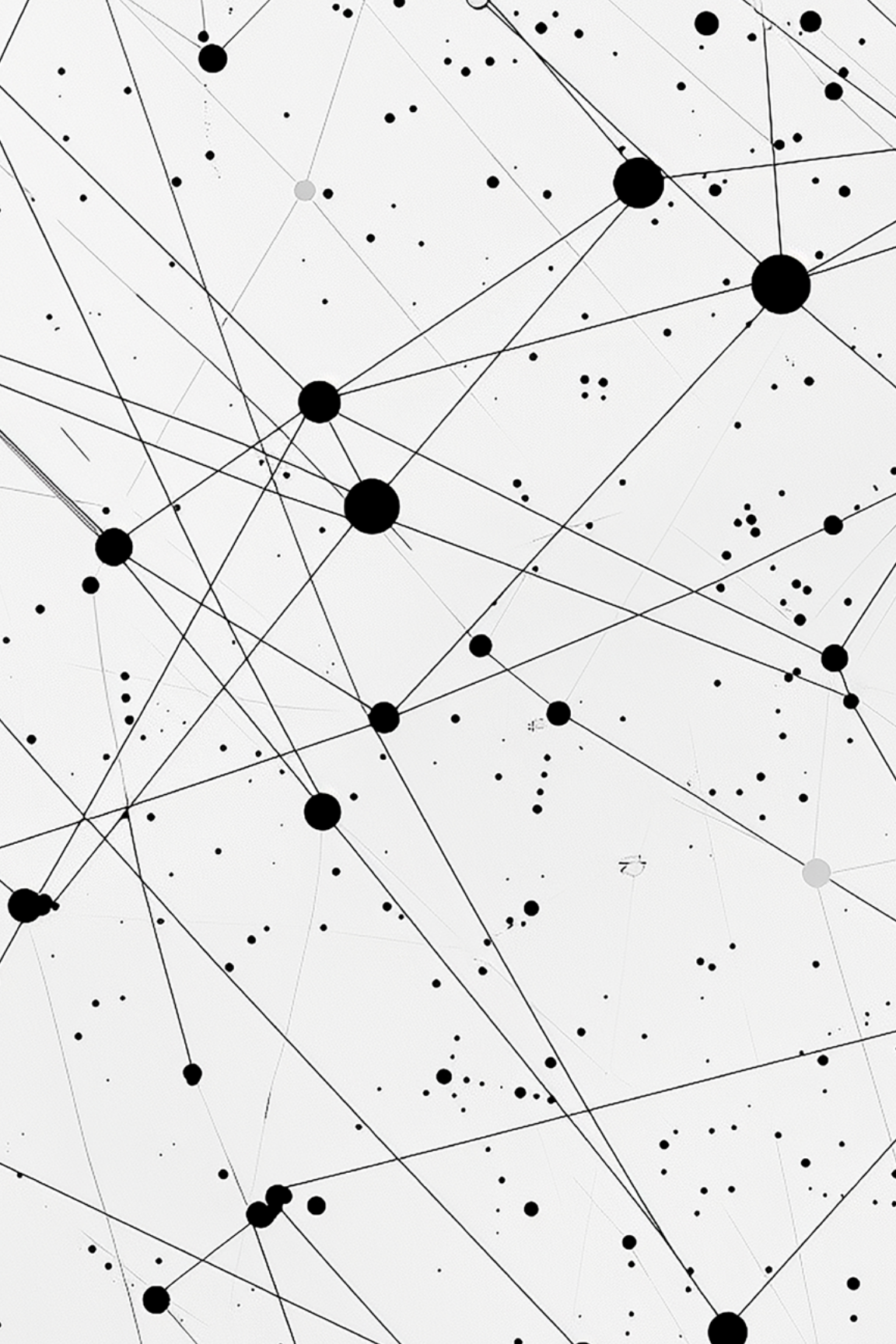
> *El Banco de México trabaja en el estudio y desarrollo de una plataforma encaminada a la implementación de una moneda digital tomando como base las características que hoy ya posee la infraestructura de compensación y liquidación del SPEI. Esto es, operatividad 24/7, pagos instantáneos, alta disponibilidad, estandarización de procesos y medidas robustas para administración de riesgos y ciber-resiliencia.*
>
> *El desarrollo de este proyecto se ha concebido en tres etapas, recurriendo en primera instancia al ecosistema CoDi a fin de permitir la realización de transferencias indicando únicamente el dato del beneficiario, como es el caso de un número celular, así como el mantenimiento temporal de saldos a favor de un usuario*

no bancarizado. En una etapa posterior, esta funcionalidad podrá evolucionar a un esquema de órdenes de pago tokenizadas, de modo que una transferencia pueda ser posteriormente redimida.

Finalmente, y a partir de los elementos desarrollados en las dos etapas previas, se contempla el desarrollo de funcionalidades para construir registros de moneda digital a favor de usuarios directa o indirectamente en el banco central.

En esas fechas, el Banco de México, a través del exdirector general de pagos, dio a conocer de manera informal que se tenía la intención de implementar la moneda digital (CBDC) en 2024. Sin embargo, en septiembre de 2022, la subgobernadora Galia Borja señaló que no existía una fecha definida para que la moneda virtual estuviera lista. Textualmente afirmó: «Estamos en el plan de estudio, de análisis. El Banco debe estar listo para cuando se requiera. No me puedo comprometer a que sea en 2024». A diciembre de 2025, se puede afirmar que no se implementó y que no parece estar en la agenda ni en el presupuesto del Banco de México. Lo cierto es que México no es un caso aislado a escala global, y que los posibles riesgos tecnológicos de su implementación parecen ser mayores a los beneficios de ayudar a resolver parcialmente el tema de la inclusión financiera.

A pesar de lo anterior, el Banco de México sí tiene dos asesores, Andrea Pérez de Celis y Carlos Vélez, que participan con los centros de innovación del BIS y del Banco de la Reserva Federal de Nueva York, dentro del proyecto denominado PINE. Este ejercicio tiene como objetivo utilizar contratos inteligentes para implementar la política monetaria de manera más ágil, eficiente y flexible en un mundo tokenizado del dinero de mayoreo que emiten. Se trata de un primer modelo que teóricamente relaciona las diferentes herramientas que actualmente tienen los bancos centrales con los bancos comerciales, tales como el pago de intereses sobre sus reservas y la compra o venta de valores gubernamentales. Aunque el modelo ha sido probado con éxito en diferentes escenarios hipotéticos basados en los datos de eventos anteriores, su experimentación técnica se encuentra en su etapa temprana.



Capítulo 2

Las finanzas descentralizadas (DeFi) y más allá

En el primer capítulo hemos visto los principios básicos de las finanzas formales o tradicionales, así como el origen de las criptomonedas que vino no solo con dinero privado, sino también con la nueva tecnología de registros distribuidos (TRD). Desde entonces se pueden llevar a cabo anotaciones descentralizadas. También se habló de las denominadas monedas estables (*stablecoins*), que en algunos casos representan un puente entre lo nuevo y lo tradicional.

Dado que las finanzas descentralizadas (DeFi) pueden operar tanto con criptomonedas —introducidas en 2009— y estar caracterizadas por una alta volatilidad, como con monedas estables —surgidas en 2014 y con menor variabilidad en sus precios—, en este capítulo exploramos la tercera etapa de este ecosistema. En él se definen las DeFi, se analizan los estratos que las sustentan y se dimensiona su tamaño.

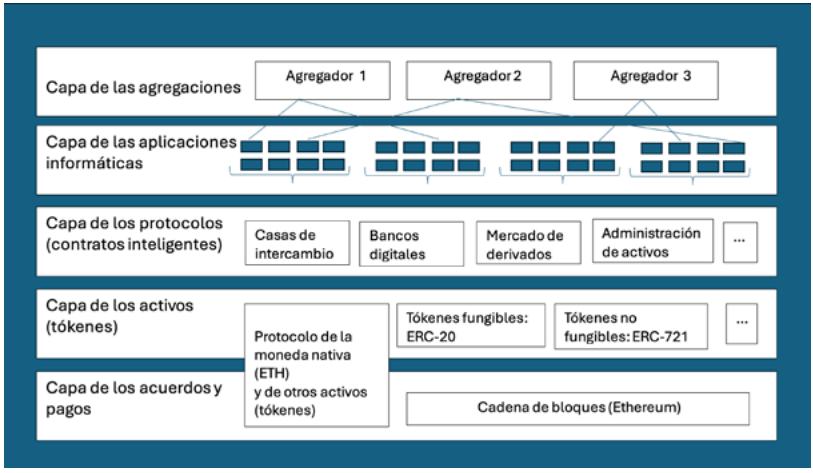
El conjunto de aplicaciones descentralizadas que conforman las DeFi fue nombrado como tal en 2018 por un grupo de desarrolladores. En esta sección se estudian dichas aplicaciones, las cuales puede constituir un sistema alternativo al formal. Finalmente, esta sección va más allá de una descripción general y busca facilitar la comprensión de los distintos conceptos que integran este espacio emergente, además de establecer una comparación entre las finanzas descentralizadas, las instituciones de tecnología financiera (*fintech*) en México y las grandes empresas de las tecnologías de la información y la comunicación (*bigtech*).

Los pilares de las finanzas descentralizadas (DeFi)

El profesor de la Universidad de Basilea, Fabian Schär señala, en su publicación de 2021, que las finanzas descentralizadas suelen referirse a una pila (*stack*) de protocolos abiertos, públicos y generalmente interoperables, construidos en plataformas de contratos inteligentes, como la cadena de bloques de Ethereum. Se trata de una estructura ordenada de información que contiene cinco capas (*layers*) que se muestran en la figura 1. Para efectos ilustrativos, se trata de una abstracción y se aclara que, objetivamente, las barreras o líneas entre los niveles no siempre son bien definidas. Un esquema similar de estratos se usó anteriormente para describir el funcionamiento de internet. La explicación de esta pila de las finanzas descentralizadas se desarrolla desde la capa de la parte inferior de la figura 1 (C1)

hasta la capa superior (C5). Así, puede afirmarse que la pila de las finanzas descentralizadas basada en Ethereum tiene cinco capas.

Figura 1. El apilado de las finanzas descentralizadas de Schär



Nota: este diagrama es una reproducción y traducción del publicado en 2021 por Schär en Federal Reserve Bank St. Louis Review.

En la primera capa (C1) se finalizan las transacciones; es decir, se ejecutan operaciones que son pagadas, liquidadas o saldadas. Este nivel también puede entenderse como aquel en el que se logran acuerdos o consensos. Está integrado por la cadena de bloques y el protocolo para crear su moneda nativa. Esta capa posibilita que la red almacene de manera segura información de la propiedad y garantiza que cualquier cambio de estado se ajuste al conjunto de reglas establecidas. La cadena de bloques puede considerarse como la base para la ejecución de transacciones sin que los miembros tengan confianza alguna entre ellos y funciona como medio para lograr consensos, mayorías y resolver disputas.

Las cadenas de bloques constituyen solo una de las formas posibles de implementar la tecnología de los registros distribuidos (véase anexo 4). Aquellas que pueden ser la base de las finanzas descentralizadas utilizan un lenguaje de programación completo de Turing. Por lo mismo, Bitcoin no es estrictamente necesario para las finanzas descentralizadas.

En la actualidad, Ethereum, creado por Vitálik Buterin, continúa siendo la principal cadena de bloques en el mundo de las finanzas descentra-

lizadas, aunque tiene competencia de Solana, BSC, Tron y muchas más. De acuerdo con coingecko.com, actualmente existen 224 cadenas de bloques.

Según Schär, la segunda capa (C2) constituye el estrato de los activos. En ella se incluye tanto la moneda nativa (ether) como otros activos no nativos, generalmente conocidos como tókenes (fichas). Algunos académicos consideran que las monedas nativas son también un token especial, llamado ficha de pago; bajo esta perspectiva, la segunda capa podría denominarse estrato de los tókenes. Hasta marzo de 2025 existían muchas clasificaciones diferentes. Algunas distinguen los tókenes según la plataforma en la que se originan o se implementan; así, las fichas de Ethereum y Solana son consideradas como tókenes de consumo. Otras clasificaciones se basan en el acceso digital a un servicio o a una plataforma (*utility tokens*), entre los que se encuentra FunFair, utilizado en apuestas en línea. Existen también clasificaciones que los dividen en función del instrumento financiero o del activo que se busca negociar. En estas últimas categorías se distingue entre tókenes fungibles y no fungibles. Los primeros son valores, datos o activos que son idénticos, por lo que se pueden sustituir unos por otros. Un ejemplo cotidiano es el de las monedas de diez pesos, que son intercambiables entre sí. En cambio, los tókenes no fungibles (NFT, por sus siglas en inglés) poseen características únicas, por lo que no se pueden replicar ni dividir. Los NFT pueden aplicarse a activos externos a la cadena de bloques, tanto intangibles —como el arte digital— como tangibles —por ejemplo, bienes raíces— los cuales, si bien no son divisibles, en ciertos casos permiten la fragmentación de su propiedad. El mercado de los bienes raíces, tanto comercial como residencial, es parte vital de los activos del mundo real (RWA, por sus siglas en inglés). Aunque este mercado es de gran magnitud en numerosos países, aún presenta un amplio potencial de crecimiento. Por ello, algunos investigadores opinan que pueden llegar a ser la aplicación más grande de las cadenas de bloques.

Aunque ya existían tókenes antes de 2015, fue Ethereum el primero en introducir un estándar técnico para tókenes fungibles y no fungibles, lo que dio origen a una gran expansión en todo el ecosistema cripto. Además, la empresa facilitó el funcionamiento, ya que solo se tiene que construir un contrato inteligente (programa de computadora) que, una vez implementado en la cadena de bloques, se encarga automáticamente de los accesos, las transferencias y su propiedad.

El primer estándar para tókenes fungibles surgió en Ethereum en 2015, a partir del intercambio de información entre la comunidad de usuarios. Inicialmente fue abreviado como ERC-20 (*Ethereum Request for Com-*

ments) y, posteriormente, se convirtió en EIP-20 (*Ethereum Improvement Proposal*). Como se observa en la figura 1, también existe un estándar para tókenes no fungibles (NFT), identificado como ERC-721. Para actualizar el diagrama de Schär en este nivel, cabe señalar la incorporación del ERC-1155, un estándar que permite la emisión y gestión de tókenes fungibles, no fungibles y semifungibles mediante un conjunto único de reglas. Además, se cuenta ya con el ERC-3643, estándar utilizado para la tokenización de activos del mundo real (RWA).

En relación con la segunda capa y con el estándar ERC-20, la empresa estadounidense Robinhood, listada en el Nasdaq (HOOD) y con licencias para llevar a cabo corretaje de acciones y de criptomonedas —además de formar parte del índice accionario S&P 500—, lanzó el 30 de junio de 2025 un servicio de tokenización de más de 200 acciones y ETF de Estados Unidos, construido sobre Arbitrum (C2 de Ethereum). En la actualidad, este servicio solo está disponible para usuarios europeos, ya que utiliza como base el avanzado marco establecido en la reglamentación de la Unión Europea (véase el capítulo 3). El proceso inicia con la compra de acciones —por ejemplo, de Apple—, las cuales se depositan en custodia dentro de una entidad con propósito especial (SPE, por sus siglas en inglés). Dicha entidad emite, a su vez, un token correspondiente por cada acción, que posteriormente se ofrece a usuarios europeos de menudeo de manera instantánea, con disponibilidad 24/5 y con comisiones y costos mínimos. El usuario no posee una acción de Apple, sino un token de Apple. Cuando decide vender el token, el fidecomiso correspondiente liquida la acción subyacente y transfiere el importe al usuario. Al respecto, Vlad Tenev, cofundador, principal accionista y director general de Robinhood, declaró en la edición agosto-septiembre de 2025 de la revista *Forbes* que el espacio cripto «tiene el potencial de convertirse en la columna vertebral del sistema financiero».

En el caso mexicano, la plataforma Bitso comunicó a sus clientes el 10 de agosto de 2025 que próximamente podrían negociar fracciones de miles de acciones y fondos de Estados Unidos, con una ejecución casi instantánea durante un horario extendido que va del domingo a las 19:00 h (CST) al viernes a las 19:00 h (CST). No obstante, la empresa no ha proporcionado detalles sobre el mecanismo de implementación, y queda pendiente conocer la postura de las autoridades y de las casas de bolsa.

Para no quedarse atrás, el Nasdaq, una de principales bolsas de valores de Estados Unidos, solicitó formalmente el 8 de septiembre de 2025 a la Comisión de Valores y Bolsa (SEC) la autorización para tokenizar cada una de las acciones que tiene cotizadas y otros productos que negocia en su

plataforma (ETF o ETP) a partir de 2026. Esta solicitud no eliminaría el esquema digital de operación vigente, sino que lo complementaría mediante una versión basada en tókenes derivados de una cadena de bloques operada por un grupo de empresas, entre las que destacan Citi, Santander, Visa, Mastercard, Consensys y Accenture. Los usuarios podrían elegir entre la modalidad tradicional o la tokenizada. Esto va más de allá del modelo adoptado por Robinhood, que básicamente empaqueta y usa derivados sin otorgar la totalidad de los derechos a los compradores. En el caso de Nasdaq, se negociarían las acciones originales en una cadena de bloques común, y los adquirentes tendrán todos los derechos, tanto patrimoniales como los que definen la gobernabilidad de las empresas.

De manera paralela, BlackRock, el mayor administrador de fondos del mundo, ha manifestado su intención de tokenizar internamente la totalidad de sus productos financieros con el fin de integrarlos en su propia plataforma de negociación. El 14 de octubre de 2025, su presidente, Larry Fink, al presentar los resultados del tercer trimestre, señaló que «necesitamos tokenizar todos los activos, especialmente aquellos que tienen distintos niveles de intermediación». Esta estrategia contempla la migración de bonos, acciones y activos reales a una cadena de bloques desarrollada por la propia firma. Por el momento, se trata únicamente del anuncio de un plan ambicioso de largo plazo, cuyo desarrollo futuro queda abierto al seguimiento del lector.

Finalmente, con el propósito de complementar y actualizar lo relativo a las dos primeras capas de la figura 1, resulta pertinente mencionar que el Grupo Intersecretarial de Trabajo sobre las Cuentas Nacionales, coordinado por la Comisión Estadística de la Organización de las Naciones Unidas (ONU), culminó el 20 de marzo de 2025 la quinta actualización del Sistema de Cuentas Nacionales (SCN). En esta revisión se incorporan de manera explícita los temas relacionados con la digitalización en general, y el de los criptoactivos fungibles y no fungibles en particular. Las discusiones del grupo se concentraron principalmente en decidir si los criptoactivos deben considerarse activos financieros, así como en precisar las definiciones que delimitan la frontera de la producción de bienes y servicios.

Se recuerda al lector que el SCN distingue dos tipos de activos: los no financieros, que incluyen activos fijos, inventarios y objetos de valor, y los activos no producidos, como la tierra. Por su parte, los activos financieros abarcan las posesiones de dinero en efectivo, los depósitos bancarios, las propiedades de acciones y préstamos. Cabe destacar que todo activo financiero tiene un pasivo igual y opuesto, con la única excepción

del oro que mantienen los bancos centrales como reserva internacional. Estas definiciones son fundamentales para comprender los siguientes párrafos.

Aunque la implementación está prevista para que 190 países y sus agencias de estadísticas —entre ellas el INEGI, en el caso de México— la concluyan entre 2029 y 2030, es importante resaltar algunos detalles. El primero es que ya se cuenta con un conjunto de definiciones comunes y con una clasificación (taxonomía) mundial de los criptoactivos fungibles, que comprende tres grandes categorías:

I. Aquellos diseñados para actuar de manera general como medio de cambio. Esta categoría se subdivide en dos grupos: los que no cuentan con un pasivo correspondiente, como el bitcoin, y los que sí lo tienen, como las monedas estables respaldadas por una o varias monedas fíat, así como por oro. En este rubro también pueden incluirse las monedas estables de los bancos centrales (CBDC), siempre que utilicen tecnología de registros distribuidos.

II. Los que actúan como medio de cambio en una plataforma o red, también conocidos como fichas de pago (*payment tokens*). Al igual que en la primera categoría, existen criptoactivos fungibles con pasivo correspondiente —como las monedas estables basadas en algoritmos— y otros que no tienen su contraparte. El manual no menciona ejemplos concretos de este último grupo.

III. Los que funcionan como instrumentos financieros o valores (*security cripto-assets*), que pueden representar reclamos de deuda (pasivo), de capital (acción) o sus derivados. Son similares a los valores del sistema financiero formal, pero se negocian entre pares mediante criptografía. Siempre tienen un pasivo correspondiente; por ello, en esta categoría se incluyen también las fichas que otorgan a sus tenedores de cualquier bien o servicio (*utility tokens*).

Mientras que las dos primeras categorías (I y II) explican los dos primeros niveles de la figura 1, la tercera (III) se refiere al desarrollo de protocolos y aplicaciones descentralizadas que son descritas en las tres capas superiores, mismas que serán explicadas en las próximas páginas de esta misma sección dedicada a las bases de las finanzas descentralizadas.

El segundo aspecto se refiere a las cuentas específicas en las que se registran estos activos digitales. Así, todos los criptoactivos fungibles que tienen su pasivo correspondiente se consideran activos financieros y se contabilizan en la cuenta financiera del sistema. En contraste, aquellos que no tienen su correspondiente contraparte son clasificados como activos no financieros, fuera de la frontera de producción, y son reportados en la cuenta de capital.

Las transacciones que se realizan para validar los criptoactivos son registradas en la cuenta de producción de bienes y servicios; es decir, en ella se registra el valor agregado que realizan los mineros de bitcoin, y las empresas o personas de otras criptomonedas, que incluyen el pago de sus comisiones y recompensas.

En cuanto a los criptoactivos o fichas no fungibles (NFT), el manual del SCN de 2025 los considera como registros digitales que existen en una cadena de bloques, son únicos y no pueden intercambiarse por otros activos de su misma clase. Algunos otorgan derechos integrales de propiedad, mientras que otros se consideran únicamente servicios de uso personal. Entre ambos extremos se encuentran fichas que otorgan derechos de propiedad limitados y puede ser usados con propósitos comerciales. Según el caso, se clasifican en la cuenta de bienes y servicios o de capitales. Por lo general, se pagan con las monedas nativas de las cadenas de bloques en donde están alojados. Por esta razón, este libro le dedica un espacio reducido y se concentra en los criptoactivos fungibles que sí pueden intercambiarse por fichas de la misma clase.

En la misma fecha en donde se acordó la actualización del SCN (20 de marzo de 2025), el Fondo Monetario Internacional dio a conocer la séptima edición del *Manual Integral de Balanza de Pagos y Posición de Inversión Internacional* (BPM7, por sus siglas en inglés), lo que garantizó la armonización de los estándares estadísticos macroeconómicos. Este hecho demuestra la estrecha cooperación entre la ONU y el FMI y permite a los usuarios contar con una adecuada articulación entre las cuentas nacionales (entre residentes) y las cuentas externas (entre residentes y no residentes).

Una muestra de esta sincronización es que ambos manuales establecen que las clasificaciones relativas a los criptoactivos con pasivo correspondiente (monedas estables), así como aplicables a los que no tienen esa contraparte (como el bitcoin), podrán revisarse en el futuro si existen cambios significativos en el mercado, en las regulaciones o en la contabilidad.

Tras este paréntesis, se retoma la figura 1 para analizar la tercera capa (C3), en la que se ubican los protocolos mediante los cuales sus desarrolladores (ingenieros electrónicos o informáticos) implementan contratos inteligentes. Esta capa proporciona estándares para casos de uso específicos, como criptobancos, casas o centros de intercambio descentralizados (DEX), mercados de derivados y administración de activos en la cadena de bloques. Estos modelos suelen implementarse mediante conjuntos de contratos inteligentes que son fácilmente interoperables. Se puede decir que en esta capa reside el núcleo de la funcionalidad de las finanzas descentrali-

zadas. Conviene aclarar, además, que los dos primeros niveles tienen otros protocolos particulares.

En el cuarto nivel (C4) se sitúan las aplicaciones informáticas a través de las cuales la mayoría de los usuarios no especializados interactúa con los contratos inteligentes mediante internet, ya sea por medio de navegadores web2, que convierten los datos en una interfaz amigable para relacionarse con el servicio financiero, o mediante aplicaciones diseñadas para los dispositivos móviles inteligentes. Estos desarrollos conectan a los usuarios con los contratos inteligentes de manera individual y permiten conectar el monedero o llavero digital del usuario con los contratos inteligentes individuales de una manera relativamente sencilla, lo que facilita el envío y firma de transacciones válidas.

En términos generales, es un diseño «amigable» que emplea texto, imágenes o recursos multimedia para que el usuario interactúe con los contratos inteligentes a través de desarrollos web o móviles construidos sobre una red abierta y descentralizada de pares. Un ejemplo destacado es uniswap.org, del cual se hablará más adelante.

La última capa (C5) puede considerarse una extensión de la capa anterior (C4), en la que es posible conectar varias aplicaciones en un solo lugar. Por lo general se trata de herramientas que permiten a los usuarios realizar tareas complejas de manera «amigable», fácil y concisa. Estas aplicaciones agrupan varios contratos inteligentes, por lo que, en realidad, la capa C5 se conecta directamente con la C3. Un ejemplo es 1inch, que permite realizar transacciones en más de trece cadenas de bloques y funciona como un agregador de bolsas de criptomonedas descentralizadas que opera en el sitio 1inch.io.

A esta capacidad de integración se le denomina componibilidad (*composability*), también conocida como los legos del dinero (*money legos*). Se trata, en esencia, de una forma de «dinero privado». Mediante el uso de estas agregaciones, se transita de la web2 (basada en lectura y escritura) a la web3, que incorpora además la propiedad. Mientras que en la web2 no es posible acceder a plataformas como X (antes Twitter) y Linkedin, en la web3 sí es factible interactuar al mismo tiempo con varias bolsas de valores descentralizadas y mantener la propiedad directa de los activos.

El término de la web3 fue acuñado por el cofundador de Ethereum, Gavin Wood, mientras escribía su libro amarillo en 2014. Afirmó que la cadena de bloques de Ethereum era segura, descentralizada y general, lo que representaba una visión alternativa de la web. Este hecho antecedió por cuatro años a la acuñación (DeFi) que fue definida por un grupo de inno-

vadores a través de un mensaje de Telegram en 2018. Por esa razón, las finanzas descentralizadas, así como otras aplicaciones no financieras (DAO, NFT, juegos o entretenimientos interactivos y el metaverso descentralizado) pueden ser estudiadas en lo individual o a través del concepto general de la web3.

El creador de la World Wide Web (www o red mundial), Timothy Berners-Lee, declaró en una conferencia organizada por Wired el 22 de diciembre de 2022 que le resultaba penoso que el nombre web3 hubiera sido apropiado por un grupo de personas del espacio cripto. Berners opinó que «los protocolos de las cadenas de bloques son muy lentos, caros y demasiado públicos». Desde 2016 impulsa el proyecto Solid, cuyo protocolo permite que los usuarios almacenen todos sus datos con seguridad en una red descentralizada de billeteras denominados *pods*. Posteriormente, junto con Rudina Seseri y su fondo de inversión Glasswing, creó la empresa Inrupt con el objetivo de desarrollar los estándares requeridos para este ecosistema. En 2024 cedió el control del proyecto a la entidad sin fines de lucro Open Data Institute. Todo este planteamiento se integra en lo que denomina web 3.0, una propuesta orientada a modificar el modelo de negocio dominante, en el que empresas como Facebook y X ofrecen el uso gratuito de sus plataformas a cambio de la recolección y centralización de datos personales. Sus ingresos provienen de la publicidad y, en algunos casos, de la venta de información personal a terceros.

En septiembre de 2025, Tim Berners-Lee publicó *This is for everyone: the unfinished story of the World Wide Web*, en el que comparte su autobiografía y describe su proyecto actual. En el capítulo 15 aborda el papel de la empresa Inrupt, en la que funge como responsable del área tecnológica (CTO), y expone el análisis de la competencia realizado por Glasswing, en el cual se incluye la tecnología basada en cadenas de bloques. A continuación, se presenta la traducción de sus comentarios relacionados con el tema:

> *Yo era escéptico de la tecnología basada en las cadenas de bloque que el científico computacional y cofundador de Ethereum, Gavin Wood haya agrupado bajo la rúbrica de Web3. Para mi este término era una palabra de moda sin sentido de unas pocas iniciativas que no tenían nada que ver con la web per se (el apodo también estaba en conflicto con la creación de mi marca Solid, que separadamente había llamado la Web versión 3.0). Mi sentir era que la cadena de bloques, la tecnología subyacente que impulsó*

> *Bitcoin, era buena para hacer transacciones públicas identificables, pero un mal almacenamiento para los datos personales. No solo porque es costosa y lenta, sino porque cualquier información que pones en la cadena de bloques se convierte inmediatamente en pública lo que no es nada bueno para los datos personales, que por defecto deberían ser privados. (p. 303)*

Con el proyecto Solid, el usuario puede almacenar todos sus datos en la nube y decidir libremente a quién otorga permisos para utilizarlos o, en su caso, mantener un control absoluto sobre ellos. Es una plataforma abierta, accesible y sin límites. Actualmente, el usuario debe optar entre web3 y web 3.0 para mantener el control de sus datos o sus activos.

Para terminar con el apilado de Schär, se presentan tres observaciones. En primer lugar, se debe recordar que las aplicaciones descentralizadas se derivan de los contratos inteligentes que tienen un código abierto, lo que permite que numerosos usuarios intenten identificar vulnerabilidades; en ciertos casos, ello puede incrementar las probabilidades de un ataque informático (hackeo). En segundo lugar, es importante señalar que algunos libros y cursos que están en el mercado se concentran en aplicaciones que abarcan los niveles tres al cinco del apilado, mientras que otros se concentran en la tecnología de registros distribuidos (cadenas de bloques) que cubren las dos primeras capas. Lo ideal sería cubrir todos los niveles, pero no siempre es posible debido a las limitaciones de tiempo. Este volumen aborda, en mayor o menor medida, a todas las capas y centra su análisis en el caso mexicano, donde la literatura especializada es escasa, lo que le confiere un valor agregado. En tercer lugar, se aclara que las monedas estables cuya garantía se encuentra fuera de la cadena de bloques (*off-chain*) no constituyen aplicaciones (C4) ni agregaciones (C5); aunque sí son fichas (tókenes) centrales en la operación de las finanzas descentralizadas.

El apilado de las finanzas descentralizadas propuesto por Schär fue publicado en 2021 y se ha convertido en uno de los documentos académicos más usados en diversas universidades y foros de discusión. Sin embargo, algunos investigadores y organismos cuestionan que el modelo se haya construido solo en Ethereum, aun cuando esta cadena represente la principal subcategoría de las finanzas descentralizadas. Existen otras cadenas de bloques con monedas nativas que son Turing completas, pero todas pueden explicarse mediante la estructura presentada en la figura 1. No obstante,

debe reconocerse que existe muy poca interoperabilidad entre ellas, a pesar de los esfuerzos por construir puentes, como en los casos de Polkadot y Cosmos. La tercera capa es la que permite a los desarrolladores de protocolos apilar, superponer o amontonar los contratos inteligentes para ubicarlos en la capa cuatro o cinco. Finalmente, todas las operaciones realizadas en las aplicaciones descentralizadas — de forma individual o compuesta—regresan a la primera capa para ser liquidadas y finalizadas.

Con el fin de superar la limitación de asignar un único nombre en la capa uno, el Banco de Pagos Internacionales, mediante el documento de trabajo núm. 1066 de enero de 2023, propuso una arquitectura general que describe el apilado de las finanzas descentralizadas a partir de un nuevo modelo de referencia (*DeFi Stack Reference*, DSR, por sus siglas en inglés). En este se precisa que las DeFi solo incluyen la actividad que se realiza en las cadenas de bloques (*on-chain*), por lo que las operaciones efectuadas en casas de intercambio centralizados (CEX) no caben en el modelo. Este desarrollo se forma por tres capas. La primera corresponde a la compensación y liquidación de pagos o valores (*settlement layer*), que se lleva a cabo a través de la tecnología de registros distribuidos (TRD). La segunda capa se refiere a las aplicaciones de las TRD relativas a criptoactivos, protocolos y composiciones (agregadores) DeFi, implementadas a través de contratos inteligentes. La tercera capa comprende las interfaces que conectan los contratos inteligentes con aplicaciones destinadas a los usuarios finales. Cada capa se vincula con una entidad externa a la cadena de bloques: la primera con los mineros o validadores que operan las TRD, la segunda con los desarrolladores y la tercera con usuarios finales. Al utilizar esta estructura, se puede afirmar que la última capa puede denominarse el tercer piso de la transformación digital descentralizada. Es probable que, con el tiempo, este apilado general del BIS alcance una relevancia igual o mayor a la del apilado particular de Schär.

Es importante resaltar que las finanzas descentralizadas no solo tratan de replicar las funciones del sistema financiero, sino que han creado innovaciones interesantes, como los proveedores de liquidez, los hacedores automáticos de mercado (AMM, por sus siglas en inglés), los préstamos relámpago y los derivados a perpetuidad. Con todo lo anterior, se pueden definir a las finanzas descentralizadas como una plataforma alternativa para estudiar las instituciones y mercados del sistema financiero formal, ya que no solo emulan los productos y servicios financieros, sino que también aportan ideas innovadoras para el sector.

El Observatorio y Foro de la Unión Europea para las Cadenas de Bloques, en su informe sobre finanzas descentralizadas de 2022, las define como un término paraguas para referirse a los «productos financieros que se basan en contratos inteligentes y cadenas de bloques que habilitan servicios financieros abiertos entre pares, automatizando sus procedimientos específicos» (p. 6).

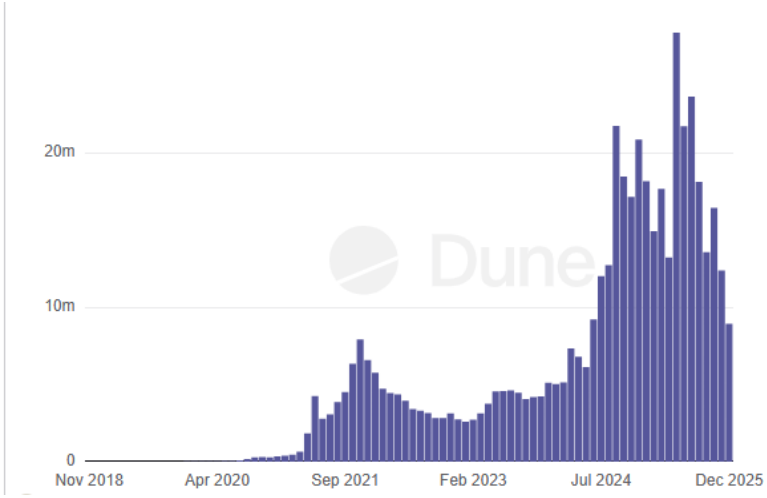
En términos generales, puede afirmarse que las finanzas descentralizadas surgieron en Ethereum. También puede afirmarse que usan «dinero privado» y sustituyen a las instituciones tradicionales por programas computacionales (contratos inteligentes). Permiten transacciones globales las 24 horas del día, los siete días de la semana. En conjunto, las criptomonedas, las monedas estables y las finanzas descentralizadas han creado un sistema financiero basado en internet, diseñado para evitar al máximo la regulación de las autoridades financieras. En las finanzas descentralizadas nadie puede ser vetado, y los titulares de los monederos mantienen la custodia de sus activos.

El tamaño de las DeFi

Existen varios parámetros utilizados para dimensionar los protocolos de las finanzas descentralizadas. Uno de los indicadores más usados es el número de usuarios de este espacio. La gráfica 2 muestra el crecimiento mensual de usuarios, medido a partir de las direcciones activas únicas en la totalidad de los protocolos, entre agosto de 2020 y diciembre de 2025. El valor mínimo registrado fue de 175,912 en agosto de 2020, mientras que el máximo alcanzó los 27.72 millones en mayo de 2025. Es importante mencionar que estos números están sobreestimados, ya que un usuario puede tener varias direcciones para operar.

La gráfica 2 también nos muestra el número de usuarios activos en cada uno de los meses del periodo reportado. En diciembre de 2025, por ejemplo, solo se registró actividad en 8.9 millones de direcciones. Sin embargo, si sumamos cada uno de ellos a lo largo tiempo, encontramos que el total de personas que han utilizado los servicios de las finanzas descentralizadas ya sobrepasaron los 313 millones.

Gráfica 2. Número de usuarios de las finanzas descentralizadas (cifras en millones)



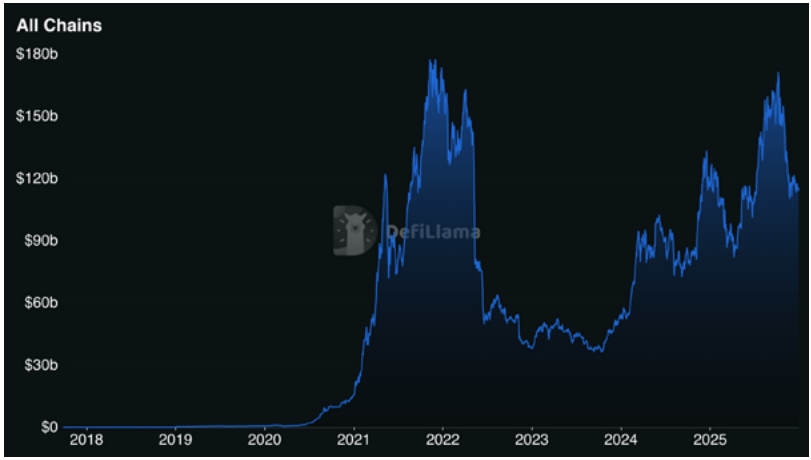
Fuente: Dune.com

Desde una perspectiva relativa, el espacio de las finanzas descentralizadas sigue siendo reducido dentro del conjunto del mercado de las criptomonedas. Si comparamos el valor máximo registrado en mayo de 2025 (27 millones de usuarios) con los 562 millones de propietarios de criptomonedas que reporta triple-a.io, se observa que este segmento representa apenas el 4.8 % del total.

Otro parámetro ampliamente utilizado es el valor total bloqueado (TVL, por sus siglas en inglés), que representa el número total de fichas (tókenes) que han sido empeñadas o arriesgadas en los protocolos de las finanzas descentralizadas. Cada una de las fichas involucradas se multiplica por el precio de mercado correspondiente a cada una de ellas. La gráfica 3 muestra la evolución del TVL desde 2018, año en que comenzaron a adoptarse las aplicaciones financieras descentralizadas. Se observa un crecimiento pronunciado que alcanza su punto máximo en noviembre de 2021, con un valor de 176 billones de dólares, nivel que no se ha recuperado hasta finales de diciembre de 2025, último periodo considerado. En esa fecha, el TVL de los protocolos DeFi ascendió a 118.4 billones de dólares, cifra que, al compararse con el valor total de capitalización del sector de las criptomonedas (3.06 trillones de dólares), representa solo el 3.9 % del espacio

total. Cabe señalar que, aunque no se refleja en la gráfica, el volumen de operaciones presenta un comportamiento distinto, con su punto máximo registrado en el año 2025.

Gráfica 3. Valor total bloqueado (TVB) en las DeFi



Fuente: Defillama.com

Resulta pertinente analizar el desglose del TVL por cada una de las cadenas de bloques que alojan las aplicaciones de las finanzas descentralizadas. El domino de Ethereum es ampliamente significativo, ya que concentra el 68.2 % del total, seguido a considerable distancia por Solana, con 8.3 %; Bitcoin, con 6.8 %; y BSC, con 6.5 %. A partir de estos datos, el lector puede constatar la hegemonía de Etherum y la limitada participación de Bitcoin en las finanzas descentralizadas.

Un tercer indicador se obtiene al calcular el valor de capitalización de las monedas en circulación dentro del espacio de las finanzas descentralizadas. Para ello, se recurre a coingecko.com como fuente de referencia, que reporta una capitalización de 104 billones de dólares al 28 de diciembre de 2025, cifra que representa el 3.4 % del total global. Algunos analistas comparan este tercer indicador con el segundo mediante una relación matemática, con el fin de estimar si el mercado se encuentra sobrevalorado o subvaluado.

Para terminar esta sección, es necesario subrayar que Ethereum se considera como la cadena dominante en las finanzas descentralizas. Por su

parte, Bitcoin aparece en el tercer lugar del espacio DeFi, con una participación reducida, aun cuando su moneda continúa siendo predominante en el espacio global de las criptomonedas.

Otro sistema financiero alternativo

Desde el siglo pasado, el sistema financiero tradicional o formal de la mayoría de los países del mundo occidental ha estado integrado por bancos, casas de bolsa, compañías de seguros, así como por otras instituciones o mercados regulados y supervisados por autoridades gubernamentales. Por lo general, los usuarios pueden tener acceso a información relevante y a los estados financieros, lo que proporciona un grado razonable de transparencia. Sin embargo, desde hace décadas este sistema ha coexistido con uno informal, en el que destacan los derivados de mostrador y algunos fondos de inversión privados, que generalmente tienen una menor regulación y suelen operar de manera opaca. Este sistema informal se conoce comúnmente como sistema financiero en la sombra o, cuando predominan las instituciones de crédito, como bancos en la sombra (*shadow banking*), y supera al sistema formal en términos del monto nominal de las operaciones realizadas.

No se requiere un análisis particularmente sofisticado para advertir que muchos propietarios de instituciones financieras y grandes inversionistas prefieren usar el sistema informal, lo que ha dado lugar al arbitraje regulatorio. Durante la primera década de este siglo, dicho sistema se caracterizó por un notable grado de innovación mediante la creación de nuevos productos y servicios, entre los que destacan las entidades o fideicomisos con propósitos especiales (SPE, por sus siglas en inglés), establecidos en paraísos fiscales; los instrumentos de deuda respaldados por créditos hipotecarios (CDO, por sus siglas en inglés), y los seguros por falta de pago (CDS, por sus siglas en inglés) para proteger posibles incumplimientos. Estas innovaciones fueron adoptadas también por el sistema financiero formal y, de manera conjunta, ambos provocaron la gran crisis financiera de 2008.

De manera paralela a dicha crisis surgieron las criptomonedas y su tecnología de registros distribuidos (TRD), orientadas a eliminar o, al menos, a competir con los intermediarios del sistema tradicional. A partir de ello se desarrollaron las finanzas descentralizadas, que pueden considerarse un segundo sistema financiero informal. Se le denomina así porque,

aunque su volumen diario de operaciones —expresado en dólares estadounidenses— representa solo una fracción del correspondiente al sistema formal, comparte con aquel ciertos rasgos estructurales. Con estos antecedentes, procede analizar las coincidencias y diferencias entre las finanzas formales, también llamadas finanzas centralizadas, y este segundo sistema financiero informal representado por las finanzas descentralizadas.

Tanto el sistema financiero privado tradicional o centralizado como la mayor parte del sistema descentralizado compiten por ofrecer servicios similares a los usuarios, aunque mediante mecanismos radicalmente diferentes. Eso sí, ambos lo hacen con fines de lucro. Se resaltan cuatro diferencias entre los dos sistemas. La primera tiene que ver con la identidad de las personas. Mientras que el sistema tradicional opera a través de intermediarios que identifican a cada uno de los usuarios con nombres y apellidos, el sistema descentralizado (DeFi) conecta directamente a los usuarios, quienes se identifican de manera cuasianónima mediante una cadena de números y letras. En el caso de Ethereum, la mayoría de las direcciones comienzan con 0x, seguido de cuarenta caracteres hexadecimales que incluyen los dígitos del cero al nueve y letras de la A la F. Quien desee pasar de la cuasianonimidad al anonimato puede utilizar alguna de las denominadas criptomonedas privadas, como Monero y Zcash, diseñadas para dificultar el rastreo del historial de operaciones mediante el uso de varias herramientas criptográficas. Según datos de CoinGecko, Zcash ocupa el lugar 23 con un valor de capitalización de 8.7 billones de dólares, mientras que Monero se sitúa en la posición 25, con un valor de 7.8 billones de dólares.

La segunda diferencia radica en la custodia de los activos. En las finanzas centralizadas, los intermediarios también son custodios de los activos negociados; en cambio, en las finanzas descentralizadas son los mismos usuarios quienes conservan la propiedad o tenencia de sus activos. La tercera diferencia se refiere al marco regulatorio: el sistema financiero tradicional está regulado con leyes y reglamentos, lo que contrasta con el sistema descentralizado que solo es regulado por los códigos computacionales de los contratos inteligentes, así como por los acuerdos entre desarrolladores y la comunidad de usuarios. La cuarta y última diferencia se refiere al hecho de que cualquier operación dentro del sistema tradicional puede ser revertida, ya sea por errores de los intermediarios o por mandato judicial, cuestión que normalmente no sucede en las finanzas descentralizadas, cuyas operaciones difícilmente se pueden revertir y se consideran inmutables.

Este apartado tiene la intención de exponer los aspectos más relevantes de los distintos componentes de este sistema financiero alternativo que opera a través de internet. Cabe destacar que, tal como se ha establecido en la obra de uno de los autores de este libro, titulada Teoría del dinero socio-jurídica para una sociedad comercial digital (*Socio-legal theory of money for the digital commercial society*, 2024), nos encontramos ante una criptoparadoja. Como se ha planteado en secciones anteriores, DeFi surge a partir de una demanda endógena social orientada a eliminar a los intermediarios tradicionales para devolver a las personas el control sobre su dinero, sus valores y su destino financiero. A pesar de ello, de manera paradójica, estos esfuerzos iniciales han dado lugar al surgimiento de nuevos intermediarios que actualmente configuran una suerte de banca en la sombra digital, cuyo tamaño, como se ha visto en la sección anterior, sigue siendo reducido en el espacio de las criptomonedas. En consecuencia, se analizarán los principales protocolos y aplicaciones que ofrecen servicios equivalentes a los de un banco comercial, una bolsa de valores, de los derivados, los seguros y la administración de activos, correspondientes a las capas tres (C3) a cinco (C5) del apilado de Schär (véase la figura 1).

El equivalente descentralizado de un banco tradicional puede denominarse criptobanco, en el que no existe intermediación directa entre depositantes y acreedores. Lo único que separa a estos participantes es un contrato inteligente y no una entidad bancaria. En el capítulo anterior se describió el proyecto DAI (actualmente Sky), que ilustra el funcionamiento de un criptobanco en el que los depósitos de los usuarios, denominados principalmente en ether o USDC, se utilizan como garantía para obtener préstamos denominados en DAI. Cabe señalar que todos los préstamos realizados por los criptobancos deben estar respaldados por garantías que oscilan entre 1.5 y 2.0 veces el monto de los depósitos originales de los cuentahabientes. Es decir, los préstamos tienen un colateral que puede llegar a duplicar el monto depositado. Lo anterior contrasta con los préstamos de los bancos comerciales, que en muchos casos son quirografarios —es decir, sin garantía— o cuentan con respaldo cuyo valor no sobrepasa el monto de lo prestado. Otro ejemplo se encuentra en las tarjetas de crédito que los bancos, en conjunto con Visa o Mastercard, otorgan a las personas físicas, cuyas tasas de interés promedio se encuentran 40 puntos porcentuales por arriba de la tasa de interés interbancaria de equilibrio (TIIE), actualmente ubicada en 7.0 %. Para concluir este apartado sobre los criptobancos (*DeFi lending and borrowing*), conviene señalar que existen nu-

merosas plataformas adicionales, como Aave, Compound y Curve, que compiten con DAI.

En noviembre de 2025, Aave lanzó una nueva aplicación para teléfonos móviles autorizada por la Unión Europea conforme al marco regulatorio MICA, cuyo objetivo es permitir a los consumidores transferir euros directamente a las finanzas descentralizadas de manera sencilla. A través de esta aplicación, los usuarios pueden obtener una tasa mínima de rendimiento del 5 %, mientras el funcionamiento subyacente de la cadena de bloques queda oculto al usuario final. Este modelo opera mediante la identificación formal de cada cliente (KYC, por sus siglas en inglés) y la gestión del riesgo a través de altos niveles de colateral con los que presta. Con esto, se confirma que todos los préstamos ofrecidos por los llamados criptobancos exigen algún tipo de colateral de criptomonedas. Este proyecto se encuentra en una fase inicial y, por el momento, solo está disponible para usuarios europeos, quienes pueden acceder a las finanzas descentralizadas sin conocimientos técnicos de criptografía ni el uso de largas direcciones alfanuméricas. En términos prácticos, Aave ha logrado presentar al usuario una plataforma similar a la utilizada por las instituciones formales, mientras que la operación en cadena de bloques se mantiene en segundo plano. En resumen, Aave pone al frente del usuario a las finanzas tradicionales y ubica en la parte trasera el uso de las finanzas descentralizadas (*TradFi in the front, DeFi in the back*). En caso de éxito, es previsible que surjan competidores de mayor escala.

Para describir el funcionamiento de las casas o bolsas de criptomonedas (DEX), sus derivados y los seguros descentralizados, resulta conveniente comenzar con las casas de intercambio centralizadas. Las plataformas centralizadas de negociación de criptomonedas (CEX, por sus siglas en inglés) actúan como intermediarios que facilitan tanto el canje de criptoactivos por dinero fíat como intercambio de criptoactivos por otros activos virtuales. De cierta forma, es comparable a lo realizado por las casas de bolsa en México con las operaciones de compra y venta de acciones cotizadas en la Bolsa Mexicana de Valores (BMV) o en la Bolsa Institucional de Valores (BIVA).

El primer paso consiste en depositar dinero fíat, que posteriormente se utiliza para la adquisición de criptomonedas. En esta etapa, el intermediario exige la recopilación de datos personales —nombre, apellidos y otra información relevante— que permitan identificar plenamente al comprador (*know your customer*). La solicitud de compra se registra en un libro electrónico de órdenes que concentra las posturas de compra y venta de las

distintas criptomonedas negociadas. Una vez adquirida la criptomoneda, esta queda depositada con el intermediario o puede intercambiarse por otros activos digitales. Cuando el usuario desea convertir sus criptomonedas por dinero fíat, solo tiene que solicitarlo al intermediario.

Es importante resaltar que la administración y custodia de las criptomonedas las mantiene el intermediario. El usuario no posee directamente los activos, sino una anotación del libro electrónico asociado a su cuenta o monedero. En este contexto, las claves privadas del monedero (*wallet*) no las tiene el usuario, sino la CEX. El intermediario suele cobrar comisiones relativamente altas por las operaciones y bajas o inexistentes por la custodia.

La gran mayoría de las operaciones gestionadas por las CEX se tramitan en libros electrónicos de órdenes, es decir, fuera de la cadena de bloques (*off-chain*). Los clientes que normalmente recurren a estas plataformas son principiantes o inversionistas de menudeo. Las CEX surgieron en 2010, poco después de la aparición del bitcoin, y desde entonces han crecido de manera exponencial en todo el mundo. Las autoridades de los países miembros del GAFI exigen que estos intermediaros identifiquen a sus clientes y adopten medidas para prevenir el lavado de dinero y el financiamiento al terrorismo. Algunos ejemplos de CEX son Binance, Coinbase, Cryto, Kraken y Bitso. Binance continúa siendo la plataforma dominante a nivel mundial, a pesar de los problemas legales que ha enfrentado en Estados Unidos.

Estas plataformas operaron prácticamente sin competencia hasta 2018, cuando surgieron las plataformas descentralizadas de negociación de criptomonedas (DEX, por sus siglas en inglés), en las que no existen intermediarios para realizar los canjes. En las DEX, los intercambios se hacen de manera directa entre pares mediante la implementación de contratos inteligentes creados en una cadena de bloques (*on-chain*), los cuales replican las funciones de las plataformas centralizadas. En este caso no interviene el dinero fíat y solo se permiten canjes entre criptomonedas o monedas estables.

Las DEX pueden entenderse como la eliminación de las casas de bolsas y la operación directa en las bolsas de valores que usan otros mecanismos más allá de los libros de órdenes electrónicas, entre los que destacan los proveedores de liquidez y los hacedores automáticos de mercado (AMM, por sus siglas en inglés), que utilizan diferentes algoritmos para la determinación de precios. Algunos ejemplos de DEX son Uniswap (2018), PancakeSwap, Hyperliquid y Balancer, siendo Hyperliquid la plataforma dominante.

En las DEX no existe la obligación de identificar al cliente. Dado que las operaciones se realizan en una cadena de bloques, los participantes se presentan de manera anónima o cuasianónima mediante direcciones generadas por monederos (*wallets*), que usan criptografía. Estas plataformas permiten a los usuarios mantener la custodia de las criptomonedas, lo que reduce ciertos riesgos frente a las CEX. Desde la perspectiva de un atacante, resulta más atractivo vulnerar una CEX —donde se concentran grandes volúmenes de activos— que atacar a un usuario individual en una DEX. Un ejemplo ilustrativo es el ciberataque a la CEX ByBit, ocurrido en Dubái el 21 de febrero de 2025, que provocó la pérdida aproximada de 1,500 millones de dólares en ether. El ataque ha sido atribuido presuntamente al grupo Lazarus, vinculado a Corea del Norte que, al parecer, tiene apoyo del gobierno y ha operado desde hace muchos años a nivel internacional.

En general, las DEX presentan comisiones más bajas y un mayor grado de transparencia que las CEX, ya que el código de los contratos inteligentes es público. Sin embargo, para los inversionistas minoristas, la comprensión de estos códigos resulta compleja, lo que explica que las DEX estén dominadas por inversionistas sofisticados.

En las CEX, el intermediario puede negar el acceso a la plataforma si la información proporcionada por el cliente es incompleta o genera sospechas, lo que implica un grado de censura. En contraste, las DEX son de acceso libre y no requieren autorización previa. Inicialmente, las DEX operaban con un nivel de liquidez o bursatilidad baja, pero con el tiempo se ha incentivado a numerosos grandes proveedores y se han mejorado los algoritmos que utilizan los hacedores automáticos de mercado. En la actualidad, la mayoría de las DEX ya no operan con libros de órdenes electrónicos, sino a través de proveedores de liquidez que depositan sus criptomonedas en los contratos inteligentes para fungir como hacedores de mercado en los intercambios de fichas (tókenes), y obtener una utilidad en el proceso. Este modelo ha sustituido eficazmente a los libros de órdenes y se ha extendido a todo el ecosistema de las finanzas descentralizadas.

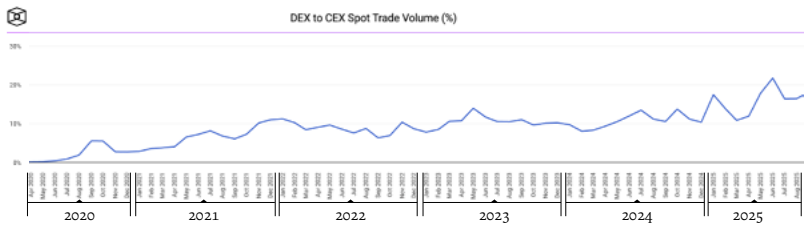
Las DEX no custodian las criptomonedas de sus clientes. La propiedad de los activos es de cada uno de los negociantes, no de la plataforma. Además, todas sus operaciones son atómicas (*atomic transactions*), lo que implica que los intercambios se realizan en su totalidad o no se realizan en absoluto. El intercambio (*swap*) entre dos criptomonedas se concreta de manera íntegra o se cancela.

Tanto las plataformas descentralizadas (DEX) como las centralizadas (CEX) tienen riesgos. Destacan aquellos relacionados con la contraparte (el intermediario) en las CEX y los riesgos de posibles errores en los códigos de los contratos inteligentes o la falta de liquidez en las DEX. Las primeras son tan seguras como lo sean sus intermediarios y las segundas son tan seguras como sus programas informáticos (códigos).

Las CEX operan primordialmente fuera de las cadenas de bloque (*off-chain*) y usan monedas fíat para las entradas y salidas. Las DEX, por su parte, funcionan dentro de la cadena de bloques (*on-chain*) y solo permiten el intercambio de criptomonedas y monedas estables. En la práctica, ambos modelos terminan interactuando: los usuarios de DEX que obtienen ganancias necesitan convertirlas en dinero fíat mediante CEX, mientras que los intermediarios centralizados requieren de las DEX para operar posiciones dentro de las cadenas de bloques.

Actualmente, las DEX se consolidan como una de las principales aplicaciones de las finanzas descentralizadas y compiten de manera creciente con las CEX. Como se observa en la gráfica 4, en julio de 2020 el volumen de operación de las DEX solo representaba el 0.8 % del correspondiente al de las CEX. No obstante, en junio de 2025 alcanzó un máximo de 23.4 %, lo que permite afirmar que las DEX negocian aproximadamente una transacción por cada cuatro realizadas en las CEX. Aunque el volumen ha disminuido entre junio y agosto de 2025, los analistas del grupo libertario (optimistas) consideran que se trata de una tendencia que continuará en los próximos años, e incluso décadas.

Gráfica 4. Volumen mensual de operaciones al contado (DEX/CEX) x 100



Fuentes: The Block y Defillama.com

Algunos investigadores y empresas de consultoría consideran que el análisis anterior equivale a comparar peras con manzanas, ya que las

CEX realizan fundamentalmente operaciones entre dinero fíat y criptomonedas fuera de las cadenas de bloques, mientras que las DEX se centran en intercambios de activos virtuales dentro de estas. Para solucionar dicha situación, proponen comparar el volumen de las CEX y las DEX considerando únicamente a las operaciones que se realizan dentro de las cadenas de bloques.

El reporte del estado de la web3, elaborado por Chainalysis en junio de 2022, representa una comparación entre las plataformas centralizadas y descentralizadas utilizando el volumen de transacciones *on-chain* expresado en porcentajes. La gráfica 5 muestra que, desde 2017, prácticamente todas las operaciones de este tipo eran realizadas por las CEX, y que no fue sino hasta 2022 cuando las DEX empezaron a despegar y a ganar participación. En abril de ese año, el volumen de las DEX ya superaba ligeramente al de las CEX.

Gráfica 5. Porcentaje del volumen de transacciones en las cadenas de bloques (*on-chain*). CEX vs. DEX (enero de 2017-abril de 2022)

Fuente: The Chainalysis state of web3 report (2022).

El reporte también ofrece datos del volumen de transacciones expresado en dólares. Entre abril de 2021 y abril de 2022, 175 billones fueron enviados a las CEX, cifra notablemente inferior a los 224 billones enviados a las DEX. Este fenómeno está estrechamente relacionado con el auge de las DEX como componente central de las finanzas descentralizadas. Aunque el reporte del estado de la web3 de 2025, primera parte, ya fue publicado, no incluye una actualización de esta comparación. Sin embargo, el portal de-

fillama.com muestra que, al 2 de septiembre de 2025, la razón entre el volumen de las DEX y las CEX era del 45 %, lo que sugiere que, desde mediados de 2022, el volumen de operaciones en las cadenas de bloques se reparte prácticamente a partes iguales.

En diciembre de 2022, Lin W. Cong (Universidad de Cornell de los Estados Unidos), Xi Li (Reino Unido), Ke Tang y Yang Yang (Universidad Tsinghua en China), publicaron un documento de trabajo en el National Bureau of Economic Research (NBER) titulado *Cripto-operaciones simuladas o falsas* (*Crypto wash trading*). En este estudio comparan el comportamiento de 26 casas de intercambio no reguladas y tres reguladas. En las primeras se incluyen, entre otras, Binance, KuCoin y Bgogo; las segundas corresponden a Bitstamp, Coinbase y Gemini. El análisis se basa en datos de las transacciones diarias que se realizaron en estas casas entre el 9 de julio y el 3 noviembre de 2019. Se trata del primer estudio académico sobre operaciones simuladas (*wash trading*) en el espacio cripto con una muestra representativa de toda la industria. Los autores encuentran que, en las casas de intercambio no reguladas, estas operaciones falsas representan en promedio cerca del 70 % del volumen, lo que revela manipulaciones generalizadas en todas ellas. Asimismo, concluyen que las casas de intercambio reguladas tienen características muy similares a las de los mercados financieros tradicionales. En esencia, el mensaje principal es que las CEX tienen menos operaciones simuladas que las DEX.

Para complementar el análisis y demostrar que las CEX también manipulan, otros investigadores han utilizado directamente el libro de operaciones de la casa de intercambio centralizada Mt. Gox, que fue hackeada en 2011, tras lo cual se filtró su base de datos completa, incluida la de identificación de compradores y vendedores. En un primer estudio (Gandal *et al*., 2018) se documentó la manipulación del precio del bitcoin mediante transacciones iniciadas por un robot sin fondos reales, que compraba bitcoin a un vendedor legítimo y, casi de inmediato, realizaba la operación inversa a un precio más alto. Se demostró que, en los días en que las operaciones sospechosas se realizaron, el tipo de cambio entre el bitcoin y el dólar subió en promedio el 4 %, frente a un ligero descenso cuando no se efectuaban. Posteriormente, A. Allosh y J. Li (2024) se centraron en cuantificar las operaciones simuladas o falsas (manipulación del volumen), definidas como aquellas en las que el comprador y el vendedor eran la misma persona, realizando la operación de ida y vuelta de manera simultánea. Sus resultados indican que algo más del 2 % del total de las operaciones eran simuladas. En suma, el usuario

debe ser consciente de que, al operar tanto en CEX como en DEX, es probable que los precios, el volumen de operaciones y la volatilidad estén inflados.

Al 28 de diciembre de 2025, CoinGecko reportaba un total de 1,444 casas de intercambio, de las cuales 1,127 corresponden a DEX, 194 a CEX y 123 se especializan en productos derivados. Estas últimas operan de manera descentralizada a través de contratos inteligentes que se concentran en dos grandes rubros. El primero abarca futuros, opciones y *swaps* sobre criptomonedas, donde activos como bitcoin y ether funcionan como subyacentes para derivados considerados como clásicos, con innovaciones como los contratos de futuros a perpetuidad. El segundo grupo consiste en generar fichas (tókenes) sintéticas utilizando contratos inteligentes (*on-chain*), que sirven como subyacente para los derivados. Los activos o fichas sintéticas representan la exposición a otro activo subyacente, y permiten a los usuarios asumir su riesgo sin la necesidad de poseerlos.

Aunque las aplicaciones financieras descentralizadas solo operan con los datos derivados de la cadena de bloques, las DEX especializadas en derivados requieren, en algunos casos, información externa, como índices bursátiles, precios de materias primas, tipos de cambio, tasas de interés o incluso resultados deportivos. El proceso de incorporar estos datos a los contratos inteligentes se conoce como problema del oráculo. Actualmente, el oráculo más utilizado es Chainlink, una red descentralizada de nodos que provee este servicio. El funcionamiento resulta más simple en las DEX especializadas en derivados que no dependen de información externa, ya que los activos sintéticos pueden ser cualquier cosa, y son creados por cualquier persona que deposite una ficha como colateral, los cuales son negociados libremente en la cadena de bloques. Un ecosistema destacado es synthetix.io, que usa su propia moneda SNX para emitir activos sintéticos llamados synths vinculados a criptomonedas, materias primas, monedas fíat, acciones —como Tesla— y diversos índices accionarios.

Un caso particular de los activos sintéticos es el de las fichas envueltas (*wrapped tokens*), creadas en una cadena de bloques y utilizadas en otra con el fin de lograr interoperabilidad. En este capítulo se mencionó el WBTC, emitido en Ethereum con respaldo uno a uno de bitcoins que fueron depositados y bloqueados. Se pueden considerar como una ficha derivada, pero en este caso la relación entre el depósito de la criptomoneda y la emisión de la nueva ficha es de uno a uno. El problema de la envoltura es que requiere de algún custodio que bien puede ser centralizado. La principal diferencia entre las monedas envueltas y los activos sintéticos es que en

las primeras sí se requiere tener posesión de activos subyacentes para hacer derivados, y en la segundas no es necesario.

A continuación, se describen brevemente los seguros descentralizados, tema incipiente dentro del espacio de las DeFi. Los riesgos en este espacio son mayores que en las finanzas tradicionales, aunque algunos usuarios deciden asumirlos con la expectativa de obtener tasas de rendimiento más elevadas. Además de los riesgos propios de las finanzas centralizadas, en el entorno DeFi existen contingencias técnicas relacionadas con el funcionamiento de las cadenas de bloques, errores en el *software* de los protocolos y ciberataques. También existen peligros en su gobernabilidad, fraudes, robos, estafas, mercados negros, lavado de dinero y manipulación de precios. Los usuarios e intermediarios del ecosistema cripto ya tienen opciones para protegerse frente a estos escenarios. Existen alternativas en las que los solicitantes deben identificarse con nombre y apellidos para obtener un seguro, como Nexus Mutual, y otras en donde se puede operar de manera cuasianónima, como Opyn.

Nexus Mutual es tanto una empresa registrada en el Reino Unido (LLC) como una organización autónoma descentralizada (DAO) que opera con su protocolo implementado en la cadena de bloques de Ethereum y con su token de gobernanza NXM. Se trata de una plataforma de carácter mutualista en la que el usuario que adquiere un seguro realiza un pago para recibir NXM, lo que le otorga derecho a la póliza y a participar en las votaciones de la DAO. Para obtener fichas de seguro NXM, las personas se tienen que registrar como miembros de Nexus Mutual —la entidad legal—, proporcionar sus datos personales (KYC) y cumplir con las directrices del GAFI relacionadas con la prevención del lavado de dinero y el financiamiento al terrorismo. En la actualidad, NXM está ubicada en la posición número 344 de la clasificación de CoinGecko con una capitalización de mercado de 138 millones de dólares. En la sección anterior, se mencionó que el valor total bloqueado (TVL) en el espacio de las finanzas descentralizadas se ubicaba en 118.4 billones de dólares. Cuando se habla de las plataformas de seguros en DeFi, tenemos que pasar de los billones a los millones de dólares. Todo esto para que el lector observe que el valor de capitalización de NXM es reducido.

Opyn, por su parte, es una sociedad incorporada en Delaware, con oficinas centrales en California, Estados Unidos. Su protocolo, desarrollado en Ethereum, ofrece protección contra la volatilidad de precios de las fichas (tókenes), así como seguros para contratos inteligentes. Utiliza opciones y *swaps*, acuña su propia moneda (oToken) y usa casas de cambio descentra-

lizadas (DEX) como Uniswap para lograr que las transacciones se realicen entre pares que operan de manera cuasianónima. No obstante, el 7 de septiembre de 2023 la Comisión de Futuros de Materias Primas de Estados Unidos (CFTC, por sus siglas en inglés) emitió una orden en contra de los operadores del protocolo de Opyn al considerar que no estaban registrados y que ofrecían transacciones ilegales en activos digitales a consumidores minoristas de Estados Unidos, sin exigirles su identificación necesaria para combatir el lavado de dinero. Como consecuencia, se impuso una multa de 250,000 dólares y se ordenó el cese de dichas actividades. Dos meses después, dos de sus fundadores anunciaron su salida de la sociedad y dejaron el liderazgo a Andrew Leone. Aunque se trató de un golpe significativo, no resultó fatal, debido al arbitraje regulatorio existente entre diferentes países del mundo y a la facilidad de crear nuevos proyectos en las finanzas centralizadas. Hoy existen diversas plataformas descentralizadas de menor tamaño, como InsurAce y Tidal Finance.

Para los usuarios, es fundamental definir con precisión el tipo de seguro descentralizado que desean contratar, el tiempo de cobertura, la plataforma, la cadena de bloques y la forma en que se toma la decisión de aceptar o negar los reclamos (la gobernabilidad). En el caso de quienes mantienen sus criptomonedas custodiadas por una casa de intercambio centralizada (CEX), se debe tomar en cuenta que, a pesar de que algunas de estas plataformas afirman contar con seguros o coberturas, suele existir poca transparencia y una regulación limitada. En México, por ejemplo, estas entidades solo tienen la obligación de estar registradas en el Sistema de Administración Tributaria (SAT), organismo cuyo interés principal es cobrar impuestos y no la protección de los usuarios financieros. Un caso representativo es el de Bitso International, que opera en México con una licencia financiera de Gibraltar a nombre de The Badger Technology Company Limited y que publicita contar con una póliza contra robo emitida por CoinCover. Sin embargo, para un usuario resulta difícil verificar el valor de su capital contable asegurado en el sitio web de dicha empresa (coincover.com) o confirmar si esta se encuentra listada en CoinGecko. Aún falta mucho por hacer en la implementación de seguros en el ámbito de las finanzas descentralizadas. Cabe añadir que el 13 de agosto de 2025 Bitso reconoció que, entre abril de 2021 y diciembre de 2022, no siguió los procedimientos internos de reportes de actividades sospechosas, por lo que tuvo que pagar a la Comisión de Servicios Financieros de Gibraltar una penalización de 263,822 libras esterlinas.

Para completar este sistema alternativo, es necesario referirse al equivalente de los asesores en inversión que atienden a los clientes con patrimonios elevados. Algunos de ellos trabajan como apoderados del intermediario financiero y otros lo hacen de manera independiente. También hay clientes que optan por no utilizar a ninguno de estos y establecen oficinas propias para administrar sus activos. En todos estos casos se habla de la administración de la riqueza (*wealth management*), de la gestión de activos (*asset management*) o de sus fondos (*fund management*). En contraste, en las finanzas tradicionales los inversionistas de menudeo no tienen esta oportunidad y, en muchas ocasiones, solo son atendidos por *chatbots* o, más recientemente, por plataformas gratuitas de inteligencia artificial.

Las finanzas descentralizadas sustituyen a los asesores financieros por protocolos que usan contratos inteligentes para ejecutar automáticamente estrategias de inversión. Existen cientos de plataformas que ofrecen servicios de administración, ya sea mediante fondos de inversión de criptomonedas o de inversiones individuales. Si el usuario opta por una estrategia pasiva de comprar y conservar, puede hacerlo directamente o a través de protocolos que manejan fondos indexados. Para quienes prefieren estrategias activas, con entradas y salidas frecuentes, puede acceder a agregadores (C5 de la figura 1) que permiten seleccionar estrategias predeterminadas, ejecutadas de manera automática por el protocolo. Un ejemplo de este tipo de agregadores lo puede encontrar en yearn.fi.

Por un lado, las comisiones totales promedio en las finanzas descentralizadas pueden ser menores si se comparan con la regla del «2 y 20» aplicada en muchos fondos de cobertura tradicionales, donde se cobra un 2 % de gestión administrativa y el 20 % como comisión de éxito. Sin embargo, también existen riesgos adicionales, como errores en los códigos de los contratos inteligentes, ataques a la plataforma de operación o problemas de liquidez en la operación. En última instancia, la decisión recae en el usuario: a mayor riesgo, cabría esperar un mayor rendimiento, aunque el futuro no puede predecirse de manera consistente.

Hilary J. Allen (2022) plantea en su artículo *DeFi: Shadow banking 2.0*? la pregunta de si las finanzas descentralizadas pueden considerarse una segunda versión de la banca en la sombra. Retoma la crisis de 2008 y sostiene que el sistema financiero en la sombra —al que denomina banca en la sombra 1.0— contribuyó de manera decisiva a sus efectos negativos que hasta el día de hoy impactan en la sociedad. Señala que los reguladores siguieron una estrategia de «esperar y ver» y que solo después de la crisis implementaron medidas limitadas. Según la autora, esta tarea inconclusa

se ve hoy acompañada por las innovaciones de las finanzas descentralizadas, que podría evolucionar hacia una banca en la sombra 2.0, como indica el signo de interrogación de su título. Allen argumenta que las finanzas descentralizadas tienen las mismas tendencias a las de la banca en la sombra 1.0, entre ellas el apalancamiento, las rigideces y las corridas bancarias. Por ello, propone establecer una regulación preventiva para limitar su crecimiento y aislarla del sistema financiero formal. Asimismo, sostiene que las innovaciones de las finanzas descentralizadas tienen un beneficio limitado para la sociedad, ya que no aspiran a proveer nuevos servicios y productos, sino duplicarlos sin el uso de intermediarios. Apoya su argumento en investigaciones del Banco de Pagos Internacionales (BIS), que señalan que la descentralización es, en gran medida, una ilusión, debido a la necesidad ineludible de tener una gobernanza centralizada y a la tendencia de los mecanismos de consenso de la cadena de bloques a concentrar el poder. Allen concluye que «el trabajo de los hacedores de políticas no es promover la innovación a cualquier costo, sino la de considerar los aspectos negativos de la innovación para justificar su intervención» (2022, p. 966). El único punto que no menciona es que el sistema financiero también fue uno de los causantes de la crisis de 2008, mediante el uso de innovaciones asociadas a la banca en la sombra 1.0.

Sopa de letras (TradFi, CeFi, DeFi, CeDeFi)

Este libro inicia con un análisis de las denominadas finanzas formales o tradicionales (TradFi), caracterizadas por la existencia de instituciones y mercados altamente regulados por diversas autoridades, cuyo objetivo es la protección de los participantes, que llevan a cabo operaciones con la moneda oficial de México. Las transacciones entre usuarios se concretan a través de algún intermediario considerado «tercero de confianza», tales como bancos comerciales, casas de bolsa, aseguradoras y mercados de valores o de derivados. Por lo anterior, muchos investigadores consideran que, en un sentido amplio, se trata de un sistema centralizado.

La Organización de Cooperación y Desarrollo Económico (OCDE), con sede en París, en su reporte de 2022 sobre la importancia de las finanzas descentralizadas (DeFi) y sus implicaciones para el diseño de políticas, señala con claridad que las finanzas centralizadas se refieren a las finanzas

tradicionales (TradFi). Para dicho organismo, TradFi es equivalente a CeFi. A partir de esta premisa, se debe estudiar cuáles son los canales de comunicación entre ambos tipos de finanzas. El tener solo dos de las cuatro sopas de letras hace mucho más fácil el análisis. Por un lado, tenemos el espacio formal y, por el otro, el ecosistema de las criptomonedas, para analizar las conexiones entre ambos grupos. Este documento considera que los custodios de las finanzas formales o tradicionales no deberían limitarse a las autoridades financieras, sino incluir también a las plataformas centralizadas de criptomonedas y a los proveedores de pagos, como Visa y PayPal, en tanto que constituyen la rampa de acceso y la vía de salida cuando el dinero fíat se convierte en activos virtuales, o viceversa. Asimismo, se señala que la interconexión entre CeFi y DeFi no es particularmente fuerte; sin embargo, destacan dos empresas cuyas acciones cotizan en las bolsas de valores de los Estados Unidos —MicroStrategy (hoy Strategy) y Square— que mantienen indirectamente (en custodia) altas inversiones de criptomonedas, principalmente bitcoin, en sus estados financieros.

A pesar de lo anterior, en 2023 la Federación Mundial de Bolsas de Valores (WFE, por sus siglas en inglés) con sede en Londres, advirtió la existencia de una falta de entendimiento entre Tradi, CeFi y DeFi, por lo que procedió a establecer definiciones precisas. A continuación, se transcribe el concepto que la WFE utiliza para referirse a las finanzas centralizas (CeFi):

> *se refieren a las entidades de la esfera cripto que facilitan la ejecución de los intercambios de cripto-activos en un sistema que en términos generales replica el sistema financiero tradicional. Un ejemplo de esto podría ser Binance que opera una plataforma de negociación de cripto-activos, que, entre otras cosas, es similar en forma a una bolsa. (p. 5)*

Esta definición deja claro que, para la WFE, las finanzas centralizadas (CeFi) constituyen una categoría distinta de las finanzas tradicionales (TradFi); es decir, CeFi no equivale a TradFi. El reporte va más allá e incluye a las finanzas descentralizadas (DeFi) dentro del mismo espacio cripto en el que sitúa a las CeFi. De esta manera, la WFE considera tres de las cuatro sopas de letras para su planteamiento: a saber, inicia con las finanzas tradicionales

(TradFi), que operan con las monedas oficiales de cada país; el entorno de las criptomonedas; y, dentro de este último, tanto a las CeFi como a las DeFi. Como ejemplos de plataformas DeFi se mencionan a Uniswap y Synthetix, ya abordadas previamente en este capítulo. Una de las conclusiones de su estudio es que las plataformas de negociación de criptoactivos deberían estar sujetas a las mismas reglas que las bolsas de valores y de derivados del sistema financiero tradicional. En otras palabras, se propone el principio de que una misma actividad, con riesgo equivalente, debe contar con la misma regulación, independientemente de si se trata del sistema tradicional o el de los criptoactivos. Cabe señalar que este principio no se aplica en México, donde las plataformas de negociación de criptomonedas solo deben registrarse ante la Secretaría de Hacienda y Crédito Público, mientras que las bolsas de valores requieren autorización previa y el cumplimiento de numerosos requisitos que, en algunos casos, tardan años.

Aunado a lo anterior, ahora existe la intención por parte de algunos operadores de las CeFi de incorporar servicios propios de las DeFi, actividad que ha sido denominada con el término de CeDeFi, que puede traducirse como la centralización de las finanzas descentralizadas. Este acrónimo fue acuñado originalmente por el entonces CEO de Binance, Changpeng Zhao (CZ), cuya trayectoria controvertida se describió en el primer capítulo de este libro. El concepto fue presentado en septiembre de 2020, con el lanzamiento de la cadena de bloques Binance Smart Chain (BSC). Su principal objetivo consistía en promover tanto a su casa de intercambio de criptomonedas como su nueva cadena de bloques para ofrecer servicios descentralizados, pero bajo esquemas de identificación del cliente y cumplimiento regulatorio, además de proporcionar custodia de los activos de los usuarios. El resultado final de toda esta sopa de letras es que, en la actualidad, existe una distancia cada vez menor entre las finanzas tradicionales, las finanzas descentralizadas y las finanzas centralizadas. En realidad, el concepto CeDeFi refleja un pleito de negocios entre quienes buscan obtener utilidades en el espacio de las criptomonedas de manera centralizada y descentralizada. Por esta razón, el término solo se menciona de manera marginal en el presente libro, ya que no se considera útil para este volumen cuyo propósito es la formación integral de los usuarios. Además, actualmente, las DeFi también buscan incorporar servicios propios de la CeFi, lo que ha dado lugar al término DeFiCEX, que contribuye a una mayor complejidad conceptual.

Como el lector habrá advertido, en esta obra hemos decidido adoptar la recomendación de la Federación Internacional de Bolsas de Valores. En

consecuencia, el capítulo anterior se inició con el énfasis en las finanzas formales o tradicionales (TradFi). En este segundo capítulo se aborda el extremo opuesto: las finanzas descentralizadas, que operan en el espacio de las criptomonedas mediante protocolos que permiten las transacciones entre pares y que, en general, no se encuentran reguladas por las autoridades. Uno de los ejemplos utilizados dentro de las DeFi es el de las plataformas descentralizadas de negociación de criptomonedas (DEX). De manera paralela, se analizan las finanzas centralizadas a través de las casas de intercambio centralizadas, las cuales permiten tanto el intercambio entre activos virtuales como la conversión de criptomonedas en dinero fíat. La regulación de estas entidades o plataformas varía según el país; sin embargo, en el caso mexicano, únicamente se exige su registro ante las autoridades, por lo que se puede decir que tienen una regulación laxa.

Para terminar esta sección, se subraya que siempre será más sencillo regular actividades centralizadas que aquellas descentralizadas. La Unión Europea, pionera en la búsqueda de claridad normativa en este ámbito, publicó en su Diario Oficial del 9 de junio de 2023 el reglamento relativo a los mercados en criptoactivos (MICA, por sus siglas en inglés), con la finalidad de adaptar sus servicios financieros a la era digital. A continuación, se reproduce el párrafo 22 de su introducción:

> *El presente reglamento debe aplicarse a las personas físicas y jurídicas y a determinadas otras empresas, así como a los servicios y actividades de cripto-activos que realicen, presten o controlen, directa o indirectamente, también cuando parte de dichas actividades o servicios se lleven a cabo de forma descentralizada. Cuando los servicios de cripto-activos se presten de manera totalmente descentralizada sin recurrir a un intermediario, no deben entrar en el ámbito de aplicación del presente reglamento.*

DeFi vs. fintech vs. bigtech

Estrictamente hablando, las entidades que prestan servicios financieros —ya sea de manera centralizada o descentralizada— mediante el uso de alguna tecnología (de la información, de la comunicación o de registros

distribuidos) pueden agruparse en la misma categoría. Libros como Fintech y el ecosistema emergente (*Fintech and the emerging ecosystems*) publicado en 2025, incluyen en un solo volumen tanto temas relacionados con el espacio de las criptomonedas como con el de la inteligencia artificial (véase la bibliografía).

A pesar de lo anterior, en el caso mexicano es necesario explicar las diferencias entre las finanzas descentralizadas, las instituciones de tecnología financiera (*fintech*) y los denominados gigantes tecnológicos (*bigtech*). La razón fundamental de esta sección es reiterar que las DeFi operan mediante intercambios entre criptomonedas y monedas estables, mientras que las *fintech* —tanto en su sentido amplio como en el restringido— y las *bigtech* realizan operaciones con monedas fíat.

Desde hace aproximadamente una década, en particular en el contexto de la denominada nueva primavera de la inteligencia artificial —que ha permitido potenciar el uso de la tecnología de registros distribuidos—, numerosos países han establecido un marco jurídico para autorizar, regular y supervisar las nuevas empresas o emprendimientos de tecnología financiera. Una definición general de *fintech* la proporciona el Consejo de Estabilidad Financiera (FSB, por sus siglas en inglés) en marzo de 2022, que considera como aquellos «servicios financieros con innovación tecnológica aplicada que pueden resultar en nuevos modelos de negocio, aplicaciones, procesos o productos, y que, junto con un material asociado, logran su prestación».

En México, en 2018 se promulgó la Ley para Regular las Instituciones de Tecnología Financiera, conocida como Ley Fintech, denominación que resulta de la asociación de los términos *finanzas* y *tecnología*. Las autorizaciones para operar las otorga un comité compuesto por el Banco de México, la Secretaría de Hacienda y Crédito Público, y la Comisión Nacional Bancaria y de Valores. Este marco normativo se limitó a dos actividades: los financiamientos colectivos (*crowdfunding*) y los fondos de pago electrónico.

La primera actividad está definida en el artículo 15 de la ley y su objetivo es poner en contacto a personas del público en general para que, entre ellas, se otorguen financiamientos mediante aplicaciones informáticas, interfaces, páginas de internet o de cualquier otro medio de comunicación electrónica o digital. El artículo 16 delimita las operaciones que pueden efectuar las instituciones de financiamiento colectivo, las cuales puede ser de deuda, de capital y de copropiedad o regalías.

La segunda actividad se establece en el artículo 22 e incluye la emisión, administración, redención y transmisión de fondos de pago electrónico a través de aplicaciones informáticas, interfaces, páginas de internet o cualquier otro medio de comunicación electrónica o digital. Es importante resaltar que las instituciones de fondos de pago electrónico (IFPE) no pueden pagar a sus clientes intereses ni ningún otro rendimiento o beneficio monetario por el saldo mantenido en el tiempo. Es decir, esta ley en su artículo 29 establece que en ningún caso se consideran depósitos bancarios de dinero. Esto permite que muchas IFPE ofrezcan a sus clientes transferencias sin costo alguno.

Las institucionales de tecnología financiera (ITF) operan en pesos mexicanos (moneda fíat); sin embargo, la ley prevé la posibilidad de realizar transacciones en monedas extranjeras (divisas) o en activos virtuales, siempre que se obtenga la autorización del Banco de México. Hasta la fecha de redacción de este texto, el banco central no ha concedido autorización alguna y ha asegurado blindar tanto a los bancos múltiples como a las propias ITF, especialmente frente a los riesgos asociados con los activos virtuales.

Para diciembre de 2025, las autoridades mexicanas habían autorizado a 88 ITF para operar, de las cuales 27 correspondían a instituciones de financiamiento colectivo (IFC) y 61 a instituciones de fondos de pago electrónico (IFPE). Al menos en términos numéricos, México tiene más instituciones de tecnología financiera que bancos múltiples. Estas entidades requieren un capital contable reducido y el monto de las operaciones que tienen autorizado realizar también es limitado; por ello, su tamaño relativo frente a la banca múltiple resulta modesto. En otras palabras, se puede decir que su peso en el espacio financiero y de pagos es marginal (véase la tabla 1).

Dado que las instituciones de tecnología financieras solo contemplan dos grandes actividades, el Banco de México las adopta con la definición de *fintech* en sentido estricto. En su *Reporte de Estabilidad Financiera* de diciembre de 2021, aclara que:

> *existen otras entidades que otorgan servicios financieros con base en tecnología, pero que no solicitaron autorización para operar como ITF, toda vez que operan bajo la figura de Sociedades Anónimas de Capital Variable u otras modalidades dentro del sistema financiero (Sofom ENR y Sofipo). Las licencias de este tipo de*

> *entidades se han vuelto atractivas para las instituciones que usan tecnología financiera (denominadas empresas Fintech en el sentido amplio), por la capacidad de captar depósitos del público, por lo cual es importante dar seguimiento a su evolución. (p. 93)*

El informe menciona los casos de Credijusto Sofom ENR, especializada en financiamiento a pymes, que compró Banco Finterra, así como a la *fintech* brasileña Nubank, que adquirió la Sofipo Akala para poder captar ahorros del público en general y que recientemente obtuvo una licencia para operar su banco cien por ciento digital.

La noción *fintech* en sentido amplio debe incluir muchas de las 2,145 Sofomes no reguladas que aparecen en la tabla 1, así como a los emprendimientos (*startups*) relacionados con los servicios financieros. En lugar de hacer un análisis detallado de las Sofomes y de los emprendimientos, puede adoptarse como referencia la definición del *Financial Stability Board* de marzo de 2022 y combinarla con la estimación del reporte elaborado por *Finnovista*, que calcula la existencia de 803 *fintech* fundadas y en operación en México. La tabla 6 muestra cada uno de los diferentes segmentos en donde operan.

En resumen, se puede decir que el número de las *fintech* mexicanas, en su sentido estricto, asciende a 88 empresas autorizadas para operar como ITF, y en su sentido amplio hay que sumar otras 803 instituciones o emprendimientos. Las primeras están completamente reguladas por las autoridades financieras mexicanas y pueden consultarse en www.gob.mx/cnbv/entidades-autorizadas/paginas/default.aspx. En el caso de los emprendimientos e instituciones, se debe aclarar que la gran mayoría no están reguladas y que solo están sujetas a una supervisión parcial, relacionada con el lavado de dinero y el financiamiento al terrorismo. Dicho lo anterior, a continuación se abordarán las grandes compañías tecnológicas (GCT), también denominadas «gigantes tecnológicos» (*bigtech*).

El término *bigtech* lo estableció Goldman Sachs para referirse a las empresas que se dedican principalmente a las tecnologías de la información y la comunicación que han logrado un gran impacto social y un elevado valor de capitalización en los mercados donde cotizan sus acciones. Pero, ¿qué se entiende por un valor de capitalización elevado? A partir de la información presentada en la tabla 7, puede observarse que las nueve empresas con mayor capitalización en el mundo pertenecen al sector tecno-

lógico y registran valores que oscilan entre 1.570 trillones de dólares (TSMC) y 4.638 trillones de dólares (Nvidia).

Tabla 6. Número de *fintech* por segmento (México, 2024)

Segmento	Número de empresas
Préstamos	174
Pagos y remesas	134
Administración financiera de empresas	109
Infraestructura financiera para bancos	95
Administración financiera de personas	64
Servicios para bienes raíces (*proptech*)	59
Servicios de seguros (*insurtech*)	55
Gestión empresarial (*wealth management*)	31
Banca digital	29
Finanzas abiertas (*open finance*)	22
Cripto	18
Financiamiento colectivo (*crowdfunding*)	13
Total	803

Fuente: *Finnovista Fintech Radar México* (2025).
Nota: también se reportan 301 empresas extranjeras que operan en México.

Tabla 7. Valor de capitalización; trillones de dólares (1 seguido de doce ceros); 28 de diciembre de 2025

Puesto	Empresa	Valor	Puesto	Empresa	Valor
1	Nvidia	4.638	11	Berkshire Hathaway	1.074
2	Apple	4.057	12	Eli Lilly	0.966
3	Alphabet (Google)	3.802	13	J. P. Morgan	0.901
4	Microsoft	3.625	15	Tencent	0.705
5	Amazon	2.485	16	Visa	0.685
Puesto	**Empresa**	**Valor**	**Puesto**	**Empresa**	**Valor**

Tabla 7. Valor de capitalización; trillones de dólares (1 seguido de doce ceros); 28 de diciembre de 2025 (continuación)

6	Meta Platforms (Facebook)	1.671	19	Mastercard	0.523
7	Broadcom	1.669	30	Alibaba	0.363
8	Tesla	1.580	205	Mercado Libre	0.101
9	TSMC	1.570			
10	Saudi Aramco	1.527			

Fuente: companiesmarketcap.com

A partir de lo anterior, una posible forma de definir a los gigantes tecnológicos es que ofrecen sus servicios en prácticamente todos los continentes, cuentan con millones de usuarios y presentan valores de capitalización de sus acciones que alcanzan billones o trillones de dólares. Como se observa en la tabla 7, incluso J. P. Morgan Chase, que ocupa la posición 13 con un valor de 901 billones de dólares, resulta pequeña en comparación con Nvidia, cuya cifra asciende a 4.638 trillones de dólares.

No existe una definición consensuada del concepto *bigtech*; sin embargo, la Nota/2022/002 del FMI, elaborada por Bains, Sugimoto y Wilson, propone la siguiente definición:

> *es un modelo de negocios basado en una plataforma enfocada en maximizar la interacción entre un gran número de usuarios, especialmente de menudeo. BigTechs son usualmente grandes conglomerados de tecnología con una red de clientes muy amplia y con negocios principales a través de muchos mercados, por ejemplo, en redes sociales, búsquedas en internet, y comercio electrónico. (p. 3; traducción de los autores)*

Dado que esta definición no establece rangos específicos sobre el número de usuarios, conviene precisar que estos pueden variar desde millones de personas —como en el caso de Alibaba— hasta miles de millones, como ocurre con Apple o Tencent. También es importante agregar a los ne-

gocios que son primordialmente de mayoreo, en especial los servicios de computación en la nube. Estos servicios son ampliamente utilizados por bancos y otras entidades financieras para almacenamiento y análisis de datos, aplicaciones de inteligencia artificial y acceso a *software*. En la actualidad, las empresas dominantes en este segmento son Google Cloud, Microsoft Azure y Amazon Web Services (AWS).

En el caso mexicano, resulta pertinente señalar que, en junio de 2025, Amazon obtuvo la primera autorización de la CNBV para ser comisionistas de base tecnológica. Además, estableció una alianza con el banco Invex y Mastercard para implementar Amazon Access. Con esta iniciativa, los usuarios pueden abrir una cuenta mediante la aplicación móvil de compras de Amazon y obtener una tarjeta digital emitida por el Banco Invex, sin requisito de saldo mínimo, costos anuales ni comisiones por transferencia. De igual manera, los clientes pueden comprar fuera de Amazon, ya sea con su tarjeta digital o solicitando una tarjeta física Invex-Mastercard sin costo adicional. Este caso ilustra una de las múltiples formas de conexión entre las instituciones financieras y los gigantes tecnológicos.

Las *bigtech* pueden aprovechar la gran cantidad de datos que poseen sobre sus clientes para prestar servicios monetarios y financieros, los cuales, combinados con sus algoritmos, permiten diseñar productos personalizados de manera más rápida y a menor costo. Una primera opción consiste en la provisión directa de servicios, como pagos electrónicos, financiamientos, seguros y fondos de inversión. En estos casos, los proyectos pueden ser disruptivos, como es el caso del intento fallido de Facebook de crear una moneda estable (libra) respaldada por dinero fíat denominado en distintas monedas e invertido en depósitos bancarios, valores gubernamentales y bonos corporativos. Lo anterior estaba acompañado por una billetera (calibra) para guardar su moneda. Debido al impacto potencial sobre los sistemas monetarios mundiales y en los bancos comerciales, se ejercieron fuertes presiones políticas que evitaron su implementación. La justificación era evidente: en un terreno de juego en el que las *bigtech* son más poderosas que las entidades financieras, no era viable un proyecto que profundizara aún más dicha asimetría.

La segunda opción es la más común y consiste en la asociación entre las *bigtech* y entidades financieras para prestar un servicio. Este esquema se ha consolidado tanto en regiones donde las *bigtech* son predominantes —como Estados Unidos y China— como en otras partes, incluida América Latina. Más allá del caso mexicano mencionado en párrafos anteriores, es

importante mostrar dos ejemplos adicionales: uno de alcance regional y otro de carácter global.

En el ámbito regional destaca Mercado Libre, cuyas acciones están listadas en el Nasdaq (MELI) y que opera en prácticamente toda la región latinoamericana. Aunque su origen es argentino, la empresa tiene su domicilio en Montevideo, Uruguay. Como se muestra en la tabla 7, está clasificada en el lugar 205, con un valor de capitalización de 101 billones de dólares. Una de sus divisiones es Mercado Pago, dedicada al procesamiento de cobros o pagos en línea y presenciales. Esta ofrece una cuenta digital de manera gratuita, tarjetas de crédito y débito, así como seguros. Si bien el segmento *fintech* genera menores ingresos que el comercio electrónico, en México Mercado Pago obtuvo su autorización para operar como institución de fondos de pagos electrónicos y firmó un convenio con Grupo Bursátil Mexicano (GBM) que permite a los usuarios obtener rendimientos, invertir en bonos y acceder al mercado accionario con saldos desde 100 pesos mexicanos. Este acuerdo contribuyó a que GBM se consolidara como líder en cuanto al número de cuentas bursátiles: en marzo de 2021 contaba con un poco más de un millón de cuentas y, para septiembre de 2025, ya superaba los 21.5 millones. Hoy, GBM posee el 96 % del total de cuentas del mercado (22.4 millones), y ha permitido la entrada de inversionistas de menudeo en México. Esto ha favorecido la inclusión financiera, principalmente en el mercado accionario, históricamente reservado a inversionistas institucionales y gente con altos niveles de recursos.

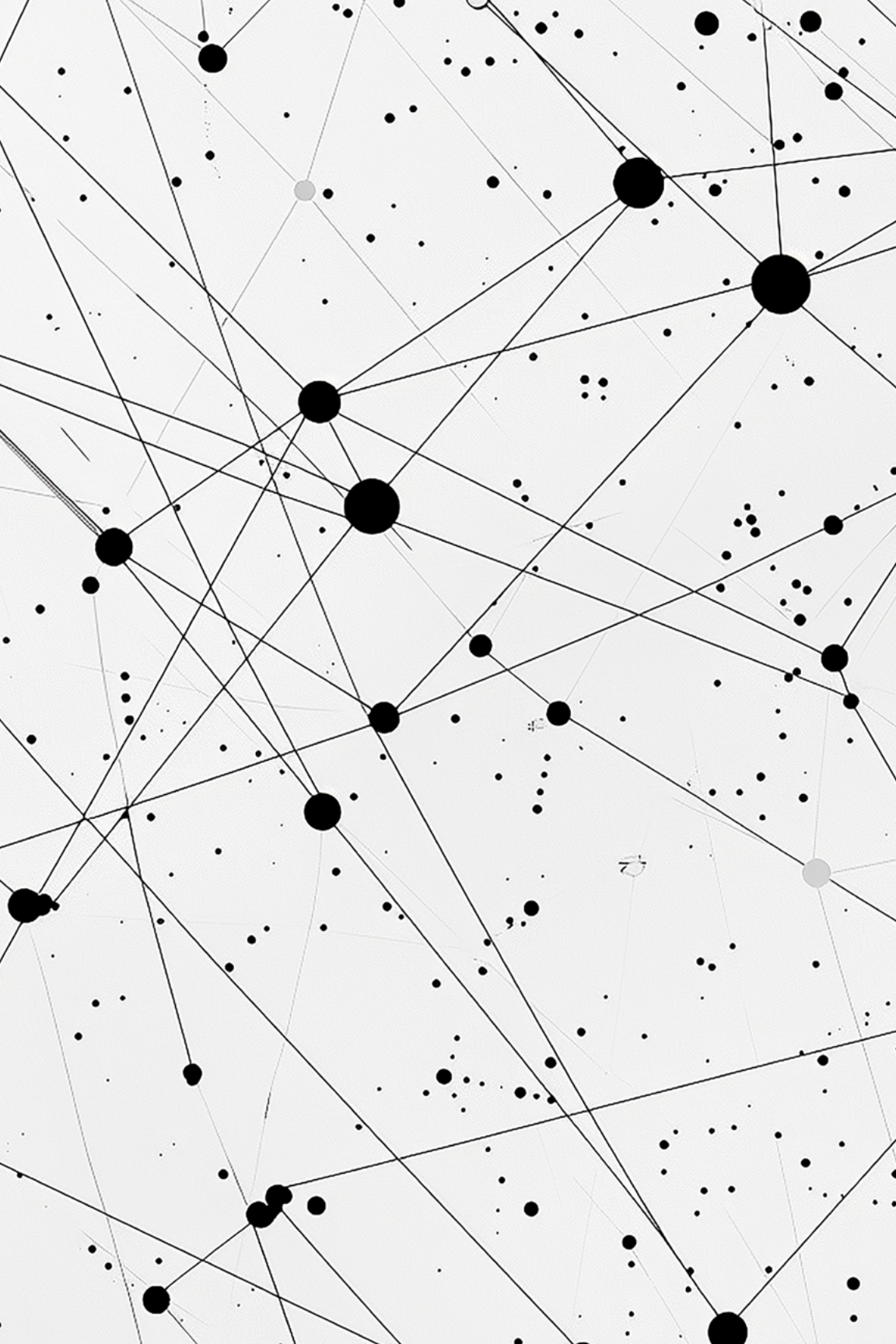
En el plano global, nos concentramos en Google, que a principios de noviembre de 2025 anunció la integración de datos de la plataforma Polymarket en su motor de búsqueda, en combinación con el uso de inteligencia artificial. Polymarket opera el mayor mercado de predicciones del mundo mediante la tecnología de registros distribuidos (*on-chain*) y, en julio de 2025, adquirió por 112 millones de dólares a QCEX, compañía que tiene una licencia de la Comisión de Futuros de Materias Primas de Estados Unidos (CFTC, por sus siglas en inglés). Los usuarios acceden a pronósticos políticos, económicos y deportivos a través de su plataforma polymarket.com, donde realiza depósitos en la moneda estable USDC. Polymarket opera sobre Polygon, una solución que fue construida en la segunda capa de Ethereum. En octubre de 2025, Intercontinental Exchange (ICE), propietaria de diez bolsas de valores en mundo —incluida la de Nueva York (NYSE)—, invirtió de manera estratégica dos billones de dólares en Polymarket. De este modo, se configura una asociación entre Google (una *bigtech*), Polymarket (una compañía del espacio cripto) e ICE (una organi-

zación central en las finanzas tradicionales). Esta triple asociación ilustra con claridad el enfoque DeFi vs. *fintech* vs. *bigtech*, aunque, en este caso, no se trata de una confrontación, sino de una colaboración directa o indirecta. Diversos investigadores consideran que este fenómeno constituye un cambio radical en los mercados financieros: si históricamente estos han servido para fijar los precios de mercados de las acciones, los bonos y las materias primas, a partir de 2026 tendremos la valuación no solo de activos financieros, sino también la determinación de los precios de cualquier tipo de información. Pasaremos de valuar activos a evaluar información.

Continuamos con el plano global para afirmar que resulta innegable la incursión de las *bigtech*, ya sea de manera directa o mediante asociaciones, en la provisión de servicios financieros. Se resalta que los servicios financieros de las *bigtech* solo representan una parte de sus ingresos totales, a diferencia de las *fintech*, cuyo modelo de negocios genera prácticamente todos sus ingresos de la prestación de servicios financieros. En consecuencia, se trata de dos modelos de negocios que son diferentes. Aunque el número de empresas *fintech* es mayor a las de *bigtech*, cuando se usa como indicador de comparación el monto operado de financiamiento, sucede lo contrario.

La incursión de las *bigtech* en las finanzas tiene beneficios y riesgos. Dentro de los primeros se encuentran la inclusión financiera de sectores no atendidos por el sistema financiero formal, así como costos más accesibles y servicios más eficientes. Sin embargo, el principal riesgo está relacionado con la estabilidad financiera del sistema. Se ha señalado la estrecha conexión entre las *bigtech* y los bancos múltiples, lo que conduce a que existan entidades excesivamente grandes; algunos autores incluso las califican como «demasiado grandes para quebrar». Por lo anterior, diversos gobiernos, bancos centrales y organismos como el Banco de Pagos Internacionales (BIS), han solicitado mayor regulación y supervisión. Incluso se ha planteado la implementación de esquemas regulatorios apoyados en nuevas tecnologías (*regtech*), acompañados de mecanismos avanzados de supervisión (*suptech*). Debido a las características de operación de las *bigtech* —particularmente su alcance global y su funcionamiento continuo, las 24 horas del día— esta tarea resulta compleja. Sin duda, se trata de un esfuerzo que solo mediante la cooperación internacional podría generar resultados en el largo plazo. En el corto plazo, las autoridades financieras de algunos países intentan que las comisiones de competencia económica ejerzan cierto control sobre los gigantes tecnológicos que operan en sus respectivos territorios.

Para terminar esta sección y el segundo capítulo, se presenta una comparación parcial entre la tabla 4, que muestra el valor de capitalización de las siete primeras criptomonedas en el mundo, y la tabla 7, que expone el valor de capitalización de las principales diez empresas cotizadas en las bolsas de valores. En particular, se busca ubicar a Bitcoin dentro de la tabla 7, aun cuando este ejercicio no sea estrictamente correcto, ya que Bitcoin no es una empresa, sino un sistema electrónico de pagos en efectivo entre pares, gobernado por un protocolo y por diversos programas informáticos. De manera sorprendente para muchos, este ejercicio situaría a Bitcoin como la sexta empresa con mayor valor del mundo. Queda a juicio del lector determinar si este resultado obedece a la relevancia de su tecnología especializada, a los elevados niveles de especulación o a una combinación de las dos.



Capítulo 3

Ver, advertir, regular o prohibir

Desde 2009, año en que se realizó la primera operación de Bitcoin, y hasta 2013, cuando el valor de las criptomonedas aún era modesto, la gran mayoría de los países, a través de sus autoridades monetarias y financieras, decidieron ser simples observadores de un fenómeno que representaba un desafío menor y que, en muchos casos, no entendían del todo. A partir de 2014, algunas autoridades —entre ellas el Banco de México— empezaron a emitir advertencias para comunicar a los inversionistas que estos activos virtuales no eran monedas de curso legal ni divisas. De igual forma, avisaron a los usuarios que no estaban reguladas y que podían sufrir pérdidas importantes.

En una tercera etapa, cercana a 2018, cuando los precios de las criptomonedas se dispararon, los países empezaron discusiones de alto nivel sobre la posibilidad de regular esta actividad que se desarrolla a través de internet y opera de manera continua. Pronto resultó evidente que las reglas solo tendrían resultados si se implementaban a nivel global. Ante esto, el único organismo internacional dispuesto a coordinar esfuerzos fue el Grupo de Acción Financiera Internacional, cuya intervención se limitó al combate del lavado de dinero y del financiamiento al terrorismo. No se identificó ninguna otra instancia internacional que pudiera liderar los esfuerzos de los gobiernos, y que, además, se enfocara en la protección del consumidor y abordara el problema de las negociaciones con información privilegiada.

Como consecuencia, hoy tenemos un sistema fragmentado. Algunos países, como China, han prohibido el uso de estos activos; otros, como la Unión Europea, han decidido establecer nuevas reglas para facilitar su operación; y Estados Unidos que, desde julio de 2025, cuenta con un nuevo marco para el espacio de las monedas estables con reservas en dólares estadounidenses. En contraste, varias naciones han decidido no actuar al respecto y ser simples observadores que se limitan a publicar avisos o sugerencias generales. En este grupo se encuentran países que solo exigen que las plataformas se inscriban con alguna instancia gubernamental que las supervise, así como otros que expiden licencias para operar si se cumplen ciertos requisitos. En cualquiera de los casos, esta diversidad de esquemas nos ha llevado a la existencia de un arbitraje regulatorio, en el que los nuevos negocios se constituyen en los países con menores barreras normativas y, desde ahí, tratan de operar a nivel internacional.

La discusión permanente gira en torno a la búsqueda de un equilibrio adecuado entre la protección a los inversionistas y la innovación de los desarrolladores. También es importante mencionar que, en la mayoría de los

casos, los innovadores avanzan varios pasos por adelante de los reguladores, tanto en las finanzas centralizadas como en las descentralizadas.

En este capítulo, el lector recorrerá el panorama de la regulación y la supervisión en México, así como un contraste de lo que sucede en la Unión Europea. Finalmente, se abordará el tema de la computación cuántica y su potencial para poner en riesgo, en el futuro, la seguridad de las cadenas de bloques.

México: plataformas CEX (35) vs. modelos novedosos (0)

En el caso de México, los activos virtuales, también llamados criptoactivos o criptomonedas, han experimentado tres advertencias de las autoridades y una gran complacencia. Poco después de que comenzaran a operar las primeras casas de intercambio de criptomonedas, en 2014, el Banco de México publicó su primer comunicado, en el que definió a los activos virtuales como «mecanismos de almacenamiento e intercambio de información electrónica sin respaldo de institución alguna, por lo que no son una moneda de curso legal». La publicación deja en claro que tampoco son divisas, ya que ninguna autoridad monetaria extranjera las emite ni respalda. Además, advirtió que el Banco de México no los regula ni supervisa y que no existe autorización para que las instituciones reguladas del sistema financiero mexicano las utilicen o realicen operaciones con ellas. Finalmente, señaló que los precios de los activos virtuales son altamente volátiles y especulativos, y que no existe ninguna garantía de que quienes los adquieran puedan recuperar su dinero.

Conviene hacer una pausa para formular dos comentarios en torno a dicho comunicado. El primero se refiere al sistema monetario desde el punto de vista legal, en el que aparecen los términos de moneda nacional, divisas (moneda extranjera) y dinero. Hasta la fecha, continúa el debate entre abogados mexicanos sobre si el derecho monetario es una disciplina autónoma o si debiera integrarse al derecho financiero. Con independencia de lo anterior, las normas jurídicas monetarias nacionales se encuentran principalmente en cuatro leyes vigentes: la Constitución Política de los Estados Unidos Mexicanos, la Ley Monetaria de los Estados Unidos Mexicanos, la Ley del Banco de México y la Ley de la Casa de Moneda de México. En todas ellas se establece que la unidad monetaria del sistema es el peso, así

como las diferentes monedas que pueden circular —metálicas y billetes—, su poder liberatorio (curso legal) y el objetivo principal del banco central, que es la estabilidad del poder adquisitivo de la moneda nacional.

Si bien el término *moneda* es el que aparece con mayor frecuencia, en algunas disposiciones también se hace referencia a los depósitos bancarios de dinero y a la moneda extranjera. En relación con esta última, se establece con claridad que no tiene curso legal en el país; no obstante, si aparece en determinados contratos financieros o mercantiles, estos podrán liquidarse mediante la entrega del equivalente en moneda nacional, al tipo de cambio que rija en el lugar y fecha en que se haga el pago. En todo este proceso queda implícito que *moneda* y *dinero* son términos legales sinónimos.

A pesar de lo anterior, la Suprema Corte de Justicia de la Nación ha establecido jurisprudencia (tesis 224, 227 y 239858) en la que sostiene que la moneda extranjera es, genéricamente, dinero, y que el dólar estadounidense puede ser una especie dentro del género dinero. Esta postura coincide con las visiones teóricas de abogados que sostienen que los términos *moneda* y *dinero* no son sinónimos. Para ellos, el dinero es el género y la moneda es la especie. El dinero es un concepto abstracto y la moneda es una cuestión práctica o una forma de materialización del dinero.

¿Cómo resolver este dilema? La jerarquía legal mexicana sitúa a las leyes primarias y supletorias —el Código de Comercio y el Código Civil Federal— por encima de la jurisprudencia. Por ello, en este libro los términos *moneda* y *dinero* son utilizados de manera intercambiable. Lo anterior significa que los jueces de los tribunales inferiores tendrán que decidir en cada caso si aplican la jurisprudencia existente o las leyes en vigor.

El segundo comentario tiene como propósito contrastar el ejemplo mexicano, que establece una barrera entre las instituciones reguladas del sistema y el espacio de los activos virtuales, con una visión completamente opuesta que se observa en Estados Unidos. En ese país, la Oficina del Contralor de la Moneda (OCC, por sus siglas en inglés), que es parte del Departamento del Tesoro, autorizó el 12 de diciembre de 2025 de manera condicional dos nuevos bancos nacionales fiduciarios. Resulta llamativo que esta aprobación se otorgó a dos empresas de la industria de los activos virtuales, ambas mencionadas en los dos primeros capítulos de este libro. Una de ellas corresponde a Ripple Labs, que operará el Ripple National Trust Bank; la otra, a Circle Internet Group, que manejará el First National Digital Currency Bank NA(National Association). En Estados Unidos no existe una barrera entre los bancos tradicionales y las empresas del ecosistema de las cripto-

monedas. Se aclara que los bancos nacionales fiduciarios se concentran en servicios relacionados con el manejo de fideicomisos, como custodia de activos, gestión de patrimonios y otras actividades afines. No reciben depósitos, no hacen préstamos, pero sí reciben comisiones de los servicios fiduciarios. En consecuencia, no están sujetos al mismo nivel de supervisión que las autoridades imponen a las compañías tenedoras bancarias, es decir, a los bancos tradicionales que pueden hacer funciones completas de banca múltiple aunado a los servicios financieros.

La interacción mencionada en el párrafo anterior es de ida y vuelta. La OCC emitió el 9 de diciembre de 2025 la carta interpretativa número 1188, en la que dejó en claro que los bancos nacionales pueden participar en transacciones de criptoactivos sin riesgo, por cuenta propia o en nombre de sus clientes. Estas operaciones incluyen la compra de un activo a una contraparte para su venta inmediata a una segunda contraparte. Esto ha sido aprovechado por J. P. Morgan, que ya opera depósitos tokenizados y un fondo de mercado de dinero en Ethereum, además de haber lanzado la primera emisión de papel comercial negociado en USDC sobre la cadena de bloques de Solana. Para no quedarse atrás, Bank of America anunció, a principios de diciembre de 2025, que cambiará su estrategia pasiva de operar los ETF de contado de bitcoin. A partir de enero de 2026, sus asesores de gestión de patrimonios recomendarán activamente a sus clientes que inviertan en su portafolio entre el 1 y el 4 % en activos virtuales a través de ETF. ¿Se trata de una convicción genuina o de la búsqueda de las elevadas comisiones de entrada y salida de los fondos de inversión cotizados en bolsa?

Regresando al caso mexicano, conviene retomar las advertencias de las autoridades nacionales y centrarse en el segundo comunicado de prensa que realizaron el Banco de México, la Secretaría de Hacienda y Crédito Público y la Comisión Nacional Bancaria y de Valores en diciembre de 2017. En dicho comunicado, las autoridades advierten sobre los riesgos asociados al uso de activos virtuales y a la participación en esquemas de inversión conocidos como oferta inicial de monedas (*initial coin offerings*, ICO). Se señala que algunas de estas emisiones, cuando se originan en México, podrían violar la Ley del Mercado de Valores y constituir un delito financiero. A las personas interesadas en invertir se les recomienda que tengan experiencia, que consideren el alto riesgo —incluida la posibilidad de tener pérdidas totales— y que deben estar atentas a señales de fraude. La tercera advertencia fue publicada el 28 de junio de 2021 por el Banco de México, la SHCP y la CNBV, en la que nuevamente se enfatizan los riesgos de utilizar

los activos virtuales. En esta ocasión, el alcance se amplía para incluir a las monedas estables y se explica lo siguiente:

> *En México no se ha autorizado la oferta del servicio de manejo de saldos denominados en pesos o divisas derivados de la captación de recursos a través de depósitos del público en general, a través de esquemas tecnológicos relacionados con cadenas de bloques o registros distribuidos, denominados monedas estables (en inglés, stablecoins). Las instituciones financieras que realicen y ofrezcan operaciones con los denominados activos virtuales sin una autorización incurrirán en infracciones a la normativa y serán sujetos a las sanciones aplicables. (p. 1)*

Es importante destacar que este comunicado reconoce, por primera vez y de manera explícita, que los activos virtuales o criptoactivos sí pueden ser intercambiados, aunque no cumplen las funciones de dinero de curso legal. Para analizar las reglas y a los reguladores de las operaciones con activos virtuales en México, es necesario remitirse a las leyes que fueron expedidas en 2018. El 9 de marzo de ese año se publicaron en el Diario Oficial de la Federación (DOF) tanto la nueva Ley para Regular las Instituciones de Tecnología Financiera (Ley Fintech) como las reformas a la Ley Federal para la Prevención e Identificación de Operaciones con Recursos de Procedencia Ilícita (Ley Antilavado). Ambas disposiciones incorporan referencias expresas a los activos virtuales. En la primera se contempla la posible operación con activos virtuales por parte de instituciones financieras reguladas, sean o no tecnológicas. Su título IV regula las autorizaciones temporales para los denominados modelos novedosos, cuya aprobación requiere, en términos generales, el visto bueno del Banco de México y de la SHCP. Los productos o servicios deben probarse en un entorno controlado, con un número limitado de clientes, y la autorización no puede exceder un plazo de dos años. Este tipo de pruebas o experimentos ya se han realizado en otros países y son conocidos como *sandbox*, término que puede traducirse como «arenero» o «caja de arena». Hasta la fecha de redacción de estas líneas, no existe una sola autorización de modelos novedosos en México.

Para quienes deseen profundizar en la Ley Fintech, se recomienda leer las disposiciones de carácter general publicadas el 10 de septiembre de 2018 por la SHCP y CNBV, así como la circular 4/2019 del Banco de México. Entre las adiciones a la Ley Antilavado en 2018 destaca la inclusión del intercambio de activos virtuales como una actividad vulnerable. El artículo 17 amplía el catálogo a dieciséis actividades vulnerables y, en su sección XVI, incorpora textualmente lo siguiente:

> *El ofrecimiento habitual y profesional de intercambio de activos virtuales por parte de sujetos distintos a las Entidades Financieras, que se lleven a cabo a través de plataformas electrónicas, digitales o similares, que administren u operen, facilitando o realizando operaciones de compra o venta de dichos activos propiedad de sus clientes o bien, provean medios para custodiar, almacenar, o transferir activos virtuales distintos a los reconocidos por el Banco de México en términos de la Ley para Regular las Instituciones de Tecnología Financiera. (p. 14)*

Asimismo, se establece que las personas clasificadas en la sección anterior deberán reportar a la SHCP cuando el monto de la operación de compra o venta realizada por un cliente sea igual o superior al equivalente de 645 Unidades de Medida y Actualización (UMA). Con base en los datos del INEGI para 2025, este umbral equivale a 113.14 pesos diarios. Esto significa que si el usuario ha comprado o vendido una criptomoneda (activo virtual) por una cantidad igual o mayor a 72,975 pesos, es casi seguro que aparecerá en la base de datos de la SHCP. Los informes de actividades de la Unidad de Inteligencia Financiera (UIF) de la SHCP evidencian el crecimiento sostenido en el número de avisos relacionados con operaciones de activos virtuales desde que se tienen registros.

Tabla 8. Avisos recibidos por operaciones de activos virtuales

Año / periodo	Número de avisos
2020	1,554
2021	4,199

Tabla 8. Avisos recibidos por operaciones de activos virtuales (continuación)

Año / periodo	Número de avisos
2022	4,939
2023	284,771
2024	2,819,101
enero-junio de 2025	4,073,212
enero-julio de 2025	100,187
enero-agosto de 2025	241,971
enero-septiembre de 2025	824,348
enero-octubre de 2025	1,002,154
Total 2020-octubre 2025	4,116,718

Fuente: Unidad de Inteligencia Financiera (UIF), distintos informes de actividades.

Aunque no se muestra en la tabla 8, las operaciones con activos virtuales, tanto en 2024 como en los primeros seis meses de 2025, ya se habían convertido en la primera actividad vulnerable en términos de avisos recibidos por la UIF. Solo en el primer semestre de 2025 representaban el 48 % del total de avisos. En agosto de ese mismo año, la presidenta Claudia Sheinbaum nombró al especialista en seguridad Omar Reyes Colmenares como nuevo titular de la UIF, en sustitución del político Pablo Gómez. En septiembre de ese año, el nuevo titular presentó el informe de actividades correspondientes al periodo de enero a julio de 2025. En dicho documento se reporta un total de 100,187 operaciones con activos virtuales. Esta cifra carece de continuidad con los datos reportados en la tabla 8, que mostraban un acumulado superior a cuatro millones de avisos entre enero y junio del mismo año. Para explicar esta notable diferencia, los autores de este libro recurrieron a la letra chiquita del informe, donde se detalla que las 100,187 operaciones de enero a julio se contabilizaban de la siguiente forma:

> *Para estas estadísticas no se consideran aquellos avisos enviados por un sujeto obligado del sector de Activos Virtuales, cuyos montos*

reportados en las operaciones se encuentran por abajo del umbral de 645 UMAS. Este umbral es señalado por la Ley Federal para la Prevención e Identificación de Operaciones con Recursos de Procedencia Ilícita vigente hasta el 16 de julio de 2025. Los avisos que se han excluidos representan el 97.9 % del total de avisos emitidos por este sector. (Nota 1 de la página 4)

Como se detalla en las siguientes páginas, en la última reforma a la Ley Antilavado de 2025 se redujo el umbral para la presentación de avisos de 645 a 210 UMA. Sin embargo, esto implica que el número de operaciones debería incrementarse y no disminuir. Además, la reforma incluyó avisos para las operaciones con activos virtuales que se generaran por una contraprestación de cuatro UMA. Otra posibilidad es que, con anterioridad, la ley no se hubiera aplicado de manera estricta y se reportaran todos los avisos recibidos, independientemente de su monto. Queda claro que la serie histórica ya no será comparable y que se inicia una nueva etapa estadística.

Bajo este nuevo esquema, la UIF ya reportó los meses de agosto, septiembre y octubre, con un acumulado de poco más de un millón de avisos en los primeros diez meses de 2025. Hasta el momento, ha eliminado la letra chiquita de sus reportes sin dar ninguna explicación convincente sobre el cambio de metodología. Lo que no es creíble es que, con este cambio del umbral, dicha actividad haya pasado de ser la principal actividad vulnerable a ocupar el cuarto lugar. Es un hecho que existen consideraciones técnicas y políticas que desconocemos; sin embargo, para los usuarios de la información, el resultado es una confusión generalizada. Este caso es solo un ejemplo de una creciente opacidad en la generación de estadísticas oficiales, al menos en los últimos cinco años.

Desde 2018, la supervisión de las operaciones con activos virtuales se le asignó al SAT, órgano desconcentrado de la SHCP, cuya responsabilidad principal es aplicar la legislación fiscal y aduanera. Esto proviene del hecho de que, desde 2013, el artículo 14 del Reglamento de la Ley Antilavado ya había encargado al SAT mantener actualizado el padrón de todas las actividades vulnerables, recibir los avisos correspondientes y realizar visitas de verificación. En consecuencia, el SAT supervisa no solo a las plataformas que custodian y administran las criptomonedas por cuenta de clientes, sino también a otros proveedores de servicios, entre los que destacan los

criptocajeros automáticos y los proveedores de monederos, billeteras o llaveros (*wallets*). En esta labor, el SAT es auxiliado por la UIF de la SHCP, que desde 2004 funge como organismo coordinador para el cumplimiento de los estándares internacionales establecidos por el Grupo de Acción Financiera Internacional (GAFI). La UIF recibe los reportes de operaciones y los avisos de las actividades vulnerables, los cuales procesa y combina con modelos estadísticos que sirven para la toma de decisiones. Los avisos de las operaciones con activos virtuales a la UIF se realizan a través del SAT desde abril de 2020. Aunque en teoría la UIF es parte de la SHCP, en la práctica se encuentra más cercana en su operación a la Secretaría de Seguridad y Protección Ciudadana de México, lo que contribuye a una mayor confusión institucional.

Aunque el GAFI será abordado en el último capítulo, se adelanta que México cumple —de manera completa, parcial o a secas— con 39 de sus 40 recomendaciones. La única partida que no satisface es la relativa a las actividades y profesiones no financieras designadas (APNFD), en la que abogados, notarios y contadores deberían reportar operaciones sospechosas cuando participan en la compraventa de bienes inmuebles, creación de empresas o administración de activos de clientes (recomendación 23). En adición a lo anterior, hay otras dos recomendaciones que están altamente relacionadas con los temas de este manuscrito: la recomendación 15, que se refiere a la regulación y supervisión de las nuevas tecnologías, especialmente a la de los activos virtuales y a sus proveedores de servicios, en donde México cumple completamente. Por su parte, la recomendación 16 exige que se identifique plenamente al que envía y al que recibe las transferencias electrónicas de fondos, conocida como la «regla del viajero». En la última evaluación, nuestro país cumplía a secas con este estándar.

Para mejorar estas evaluaciones era necesaria una reforma legal que, en primera instancia, fue presentada en el Senado de la República en 2018. Dicha iniciativa proponía modificaciones tanto a la Ley Antilavado como a la Ley General del Sistema Nacional de Seguridad Pública. Entre otros aspectos, planteaba trasladar la supervisión de las actividades vulnerables del SAT a la CNBV, establecer mecanismos de coordinación entre la federación y las entidades federativas, otorgar mayor autonomía técnica y de gestión a la UIF y crear una guardia financiera. Actualmente, esta iniciativa se encuentra archivada, y los legisladores han diseñado un nuevo proyecto que, si bien busca cumplir con los estándares del GAFI, excluye tanto el cambio de supervisor como la creación de la guardia financiera.

En octubre de 2024, el senador Javier Corral presentó una iniciativa, la cual fue analizada en un parlamento abierto celebrado en enero de 2025. Entre las modificaciones propuestas se establecen facultades para que la CNBV, la Comisión Nacional de Seguros y Finanzas (CNSF) y la Comisión Nacional del Sistema de Ahorro para el Retiro (Consar) participen también en la supervisión de las actividades vulnerables. En el caso de los activos virtuales, se adicionan las operaciones realizadas por ciudadanos mexicanos desde otras jurisdicciones y se reduce el umbral para presentar los avisos de 645 a 210 UMA. Este proyecto se aprobó en el Senado el 25 de junio de 2025 y fue turnado a la Cámara de Diputados para su siguiente etapa constitucional. Resulta llamativo que ese mismo día el Departamento del Tesoro de Estados Unidos emitiera órdenes en las que identificó a los bancos mexicanos CI e Intercam, así como a la casa de bolsa Vector, como facilitadores financieros de las organizaciones terroristas extranjeras, en operaciones de lavado de dinero relacionadas con el tráfico ilícito de opioides (fentanilo), y prohibiera sus transferencias de fondos desde o hacia ese país. Este episodio evidencia que la coordinación entre la UIF de la SHCP y la Financial Crimes Enforcement Network (FinCEN) del Departamento del Tesoro estadounidense no está funcionando de manera adecuada, lo que ha representado un duro golpe tanto para el gobierno de nuestro país como para su sistema financiero. Paradójicamente, quienes parecen capitalizar esta situación son los sectores libertarios de las criptomonedas, que hoy argumentan que el lavado de dinero también se presenta en las finanzas tradicionales.

Retomando la reforma autorizada por el Senado, el 30 de junio de 2025 la Cámara de Diputados avaló rápidamente las reformas a la Ley Antilavado y al Código Penal Federal, las cuales fueron turnadas al Ejecutivo federal para su firma y publicadas el 16 de julio en la edición vespertina del *Diario Oficial de la Federación*. Seguramente esto logrará reducir el riesgo de que el GAFI coloque a México en la lista gris en la evaluación de marzo de 2026, cuyos resultados se darán a conocer en octubre de 2026. No obstante, más allá de la adecuación normativa, lo fundamental es la aplicación efectiva de las leyes en la práctica. Mientras tanto, Elisa de Anda, de nacionalidad mexicana, preside el GAFI de manera eficiente, al tiempo que el gobierno de México —como ya fue mencionado— realizó un cambio en la titularidad de la UIF.

Más allá del GAFI, la consultora estadounidense Chainalysis, en su *Reporte Cripto del Crimen 2025*, detalla cómo los cárteles mexicanos usan las criptomonedas para pagar a los vendedores de China por los pre-

cursores químicos destinados a la producción de fentanilo. En dicho informe se señala:

> *El comercio global de fentanilo ha dependido desde hace mucho tiempo de la secrecía financiera, con la utilización que hacen los carteles mexicanos de sistemas bancarios opacos y con redes de dinero clandestinos, para poder pagar a los proveedores chinos de los precursores necesarios. (p. 118)*

Para corroborar esta situación, el Departamento del Tesoro de Estados Unidos, a través de la FinCEN, emitió el 28 de agosto de 2025 una advertencia en la que exhorta a las instituciones de su país a extremar la vigilancia para detectar el uso de redes chinas de lavado de dinero empleadas por los cárteles mexicanos, incluidos aquellos designados como organizaciones terroristas. Estos reportes también incluyen el tráfico de personas, los fraudes médicos, las actividades de los casinos y la compra de bienes inmuebles.

Regresando al SAT, es necesario mencionar al extitular de la Administración Central de Asuntos Jurídicos de Actividades Vulnerables, cargo que desempeñó entre 2019 y 2021. Tras su salida por pérdida de confianza, el SAT mencionó que:

> *Como servidor público tenía un evidente conflicto de interés ya que es socio y fundador de García Gibson Consultores, S. C. que ofrece servicios de asesoría en materia de lavado de dinero y recursos de procedencia ilícita, áreas en las que contaba con información privilegiada cuando se desempeñaba como Administrador Central de Asuntos Jurídicos de Actividades Vulnerables del SAT. (Quinto Elemento Lab, 2021)*

EL SAT fundamentó su decisión en el informe del Senado de los Estados Unidos titulado *Vulnerabilidades de los Estados Unidos al lavado de dinero, las drogas y el financiamiento al terrorismo: historia del caso de HSBC*, en el que el

extitular aparece en múltiples ocasiones como participante de un esquema que permitió a los cárteles de Sinaloa y del Norte del Valle de Cali usar la infraestructura de HSBC en México para lavar millones de dólares desde principios de este siglo, cuando era responsable del tema. La situación resulta irónica: ¿quién supervisaba al supervisor mexicano? Está claro que en el periodo de 2019 a 2021, el inspector mayor fue el Senado de los Estados Unidos. Finalmente, el caso se cerró en México con una multa impuesta por la CNBV a HSBC México por 379 millones de pesos, mientras que el extitular de la Administración Central (2019-2021) salió indemne, ya que ni el SAT ni la SHCP decidieron judicializar sus posibles irregularidades.

Otro tema relacionado con el SAT y la UIF se vincula con lo que podría denominarse el secreto mejor guardado. En la conferencia de prensa en la que se presentó el tercer Informe de Seguimiento Intensificado de México ante el GAFI, celebrada el 28 de junio de 2021, el entonces titular de la UIF, Santiago Nieto, declaró lo siguiente:

> *Respecto al tema criptomonedas, lo único que diría es que tenemos registro de 23 plataformas que operan en el país y que presentan sus Avisos ante la UIF; y sí, tenemos tres casos de irregularidades; una banda de nigerianos, un tema de trata de personas y otro tema de hackers, en donde la operación de lavado de dinero se efectúa a través de criptomonedas. Todo se ha denunciado ante la Fiscalía General de la República.*

Poco después, Santiago Nieto complementó la información declarando que, además de las 23 plataformas mencionadas, existían al menos otras doce que no estaban registradas ante la autoridad. Con el interés de conocer el nombre de las 23 plataformas registradas, el 17 de octubre de 2022 uno de los autores de este libro envío una solicitud al Instituto Nacional de Transparencia y Acceso a la Información (INAI), entonces organismo autónomo del gobierno federal. La solicitud fue turnada al comité de transparencia del SAT, el cual respondió meses después que la información solicitada «resulta inexistente en los términos solicitados». Ante ello, se interpuso un recurso de revisión, cuya respuesta fue que la información estaba clasificada como reservada, con fundamento en diversas disposiciones legales. Posteriormente, se enviaron otras solicitudes tanto a la SHCP como al Banco

de México, las cuales no atendieron los cuestionamientos y recomendaron revisar la información en la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (Condusef). Se inspeccionó el sitio electrónico de esta última, se encontró información general sobre la actividad de las criptomonedas, pero no sobre los nombres de las plataformas que operan en México. El último intento se realizó el 31 de enero de 2023, cuando el presidente de la Condusef, Óscar Rosado Jiménez, acudió a la Universidad de las Américas Puebla (UDLAP) para dar una plática. Al finalizar, se le preguntó a quién podía recurrir un inversionista que hubiera tenido un problema con alguna de las plataformas que operan criptomonedas en México. Su respuesta fue que solamente podía recurrir «a la Virgen María».

Es increíble que las autoridades mexicanas resguarden la información relativa a las plataformas y corredores (*brokers*) que operan en el país. La gran mayoría de la comunidad cripto las conoce, y entre ellas se encuentran Bitso (con licencia para operar en Gibraltar) y su afiliada Juno (El Salvador), ChangeNOW (incorporada en San Vicente y las Granadinas), KuCoin (Seychelles), OKX (Seychelles), DitoBanx (El Salvador), Kraken, Binance y CoinFlip (Estados Unidos). El caso de la última plataforma mencionada es un ejemplo de que en México podemos obtener información sin recurrir al SAT. CoinFlip es una empresa que, entre otras actividades, instala y opera criptocajeros automáticos en diversos lugares del mundo. En México, los llama Bitcoin ATM y, en su página web, informa que cuenta con 35 cajeros distribuidos en todo el territorio nacional, con la localización física de cada uno de ellos. Estos cajeros reciben dinero fíat en efectivo y tarjetas de débito para comprar varias criptomonedas, y ofrecen la creación rápida de un monedero (*wallet*), asistiendo al usuario en la generación de una dirección autoalojada, con lo cual obtiene su llave privada y semilla, lo que le da posesión y custodia directa de todas las operaciones. El uso del cajero exige la aceptación de los términos del servicio, que incluyen el nombre completo de las personas, su fecha de nacimiento y el número de teléfono, al cual se envía un código QR que debe escanearse. En Estados Unidos cuenta con más de 4,400 criptocajeros, por lo que la conexión entre estos equipos y los de México puede facilitar el envío de remesas.

Hoy en día, el INAI ha dejado de ser un organismo autónomo y ha sido sustituido por la entidad denominada Transparencia para el Pueblo, que depende directamente del gobierno federal. Surge entonces la duda de si valdría la pena intentar nuevamente conseguir información sobre el nú-

mero y los nombres de las plataformas que operan en México. ¿Es razonable pensar que, esta vez, se recibiría una respuesta positiva?

En resumen, el proceso de regulación de las criptomonedas en México inició con advertencias, continúo con la Ley Fintech, la Ley Antilavado y el registro de las plataformas en el SAT, registro que, por diversos motivos, no se ha hecho público. Desde esta perspectiva, ha prevalecido la indefinición de las autoridades y una enorme complacencia. El mejor ejemplo de esto lo dio el exsubsecretario de Hacienda y Crédito Público, Gabriel Yorio, durante el cierre de la Semana Fintech, el 30 de agosto de 2023, cuando afirmó:

> *México ya tiene actualmente operando en la jurisdicción algún tipo de criptoactivos, pero no tenemos todavía una regulación clara, ni una definición de política pública de qué vamos a hacer con respecto a estos activos. Entonces, creo que, en el grupo de innovación financiera, tal vez pueda ser un muy buen espacio para pensar, y en algún momento definir entre autoridades y gremio qué vamos a hacer con los criptoactivos. O los prohibimos o los regulamos, pero ya tenemos que tomar una decisión.*

Han pasado dos años y cuatro meses desde entonces sin que exista una definición al respecto. Corresponde al nuevo gobierno tomar una postura en esta materia.

Normas mexicanas para el intercambio de información y datos

La Ley Fintech, publicada en marzo de 2018, puso a México a la vanguardia en la regulación de las instituciones de tecnología financiera en América Latina. Sin embargo, con el paso del tiempo el país se ha rezagado, principalmente porque no se han expedido muchas de las regulaciones secundarias para la implementación de diversos aspectos clave. Entre ellos destaca el intercambio de información, no solo entre las autoridades financieras, sino también entre las diversas entidades o instituciones financieras. El artículo

76 de la Ley para Regular las Instituciones de Tecnología Financiera determina que todas las entidades financieras estarán obligadas a establecer interfaces de programación de aplicaciones informáticas estandarizadas que posibiliten la conectividad y acceso de otras interfaces desarrolladas o administradas por ellas o por terceros especializados en tecnologías de la información. Dicho artículo define tres niveles para compartir los datos. El primero corresponde a los datos financieros abiertos, los cuales no contienen información confidencial e incluyen, entre otros, los relacionados con los productos y servicios ofrecidos al público en general, así como la ubicación de sus oficinas y sucursales. El segundo nivel se refiere a los datos agregados, que comprenden información estadística sobre las operaciones realizadas, presentada de forma tal que no permita la identificación de personas. El tercer nivel incluye los datos transaccionales relacionados con el uso de un producto o servicio contratado por los clientes de las instituciones financieras. Estos últimos constituyen datos personales y solo pueden compartirse previa autorización expresa de los usuarios.

El mismo artículo establece que los detalles para el intercambio de información quedarán sujetos a las disposiciones de carácter general que emita el Banco de México o cualquiera de las comisiones supervisoras competentes (CNBV, Consar, CNSF y Condusef).

Dos años después de la publicación de la Ley Fintech, el 10 de marzo de 2020, el Banco de México emitió la Circular 2/2020, publicada en el *Diario Oficial de la Federación* (DOF) en la misma fecha. Esta disposición está dirigida solo para las Sociedades de Información Crediticia y a las Cámaras de Compensación, y establece los estándares en materia de interfaces de programación de aplicaciones informáticas estandarizadas (API, por sus siglas en inglés). Por su parte, la CNBV publicó en el DOF, el 4 de junio de 2020, las disposiciones de carácter general relativas a las interfaces de programación de aplicaciones informáticas estandarizadas a las que hace referencia la Ley Fintech. Las disposiciones detallan los lineamientos de seguridad que deben observar proveedores y solicitantes de datos abiertos, definen la arquitectura para su intercambio y proporcionan un diccionario técnico de códigos para los datos abiertos de cajeros automáticos.

Hasta el momento de redactar estas líneas, las autoridades solo han emitido la regulación secundaria para los datos abiertos. Aún faltan las disposiciones generales para los datos agregados y transaccionales. El avance ha sido limitado y, aun en esta etapa temprana, la CNBV ya ha sancionado a instituciones financieras con multas millonarias por no haber establecido API en sus cajeros automáticos.

La mayor parte de la banca múltiple de México, que constituye la columna vertebral del sistema financiero, ha optado por no actuar hasta que se publique la regulación secundaria completa. Algunos bancos, como BBVA y HSBC, decidieron crear nuevas estructuras en su organigrama para abordar este tema y, con ello, generar la infraestructura técnica para estar preparados. Otros grupos han decidido obtener nuevas licencias bancarias para operar entidades cien por ciento digitales. Hasta ahora, la CNBV ha otorgado siete licencias, y ya se encuentran en operación Bineo, de Banorte; Hey, de Banregio; y Openbank, de Santander. Próximamente entrarán en operación Revolut de Reino Unido, Banca Plata, Nu México y Mercado Pago, del que se habló al final del capítulo anterior.

Se contrastan un par de ejemplos de la evolución de los bancos cien por ciento digitales. Por un lado, Bineo inició operaciones el 29 de enero de 2024 con solo dos productos: una cuenta de depósito y préstamos personales. La institución estimó alcanzar su punto de equilibrio financiero en tres años, por lo cual aportó un capital social considerablemente superior al mínimo requerido. Sin embargo, en septiembre de 2025, el Grupo Financiero Banorte anunció la venta de Bineo a Clearscope, subsidiaria de Klar USA, empresa que a su vez controla a la Sofipo mexicana Klar. Esta operación de venta ya fue autorizada por los reguladores mexicanos y demuestra un proyecto que no logró consolidarse. Por el otro lado, Openbank, el banco digital del Grupo Santander, informó en la misma fecha que había alcanzado 300,000 clientes durante sus primeros seis meses, con resultados altamente favorables. Se aclara que estos bancos cien por ciento digitales tienen una operación limitada y no tienen sucursales físicas, aunque algunos de ellos utilizan la infraestructura del banco múltiple que les dio origen.

La operación de los bancos cien por ciento digitales es diferente del concepto de banca abierta (*open banking*). En México, la banca abierta es una posibilidad contemplada de manera indirecta en el artículo 76 de la Ley Fintech, el cual establece que el intercambio de datos transaccionales estará sujeto a las disposiciones de carácter general para su autorización e implementación. Sin embargo, dichas disposiciones no se han publicado, por lo que, de manera oficial, México todavía no cuenta con un sistema de banca abierta. La ley no hace referencia explícita a este concepto, pero tampoco establece que está prohibida.

Todo esto ha provocado que numerosos inversionistas recurran a otros entes regulados y no regulados para ofrecer servicios de forma digital. Tal es el caso de la empresa brasileña Nubank, que inicialmente

compró una Sofipo establecida en México para operar cuentas de ahorro, tarjetas de débito que ganan intereses y otorgamiento de crédito. Existen muchos otros casos que operan de manera similar en México a través de Sofomes no reguladas. A estas entidades suelen denominárseles neobancos; sin embargo, en sentido estricto, no cuentan con una licencia bancaria, sino que se trata de empresas *fintech* en su sentido amplio (*startups*), que forman parte del denominado ecosistema financiero digital. La tabla 6 del capítulo anterior muestra que, a finales de 2024, en México existían 29 entidades *fintech* consideradas como bancos digitales. Se precisa que no se trata propiamente de bancos, ni tradicionales ni nuevos, sino de empresas que han emprendido procesos de innovación con la expectativa de consolidarse en el mediano y largo plazo.

La banca abierta es una parte importante de las finanzas abiertas (*open finance*) tanto en México como en el mundo, aunque no necesariamente involucra a todo el universo de instituciones o entidades financieras. La Ley Fintech también incluye, entre otros, a los grupos financieros, las bolsas de valores, las casas de bolsa, las uniones de crédito, las casas de cambio y las sociedades operadoras de fondos de inversión. Las finanzas abiertas son un ecosistema que también requiere del consentimiento explícito de los usuarios para que segundos o terceros interesados puedan acceder a sus datos, con el fin de ofrecer productos y servicios hechos a la medida. Su principal base tecnológica es el uso de la API, que permite conectar y explorar las diferentes bases de datos de los participantes.

El IV Informe Fintech en América Latina y el Caribe, publicado por el Banco Interamericano de Desarrollo (BID), BID Invest y Finnovista, agrupa a las finanzas abiertas en cinco categorías:

(a) los servicios de iniciación de pagos (PISP, por sus siglas en inglés), que permiten realizar transacciones en línea sin intermediarios de pago convencionales;

(b) los proveedores de servicios de información de cuentas (AISP, por sus siglas en inglés), que facilitan el acceso a datos bancarios esenciales para la personalización de productos financieros por parte de terceros;

(c) los proveedores de infraestructura, que son el soporte tecnológico necesario para la implementación de soluciones;

(d) el subsegmento de los datos abiertos, que abarca a otro grupo de habilitadores dedicados al procesamiento, análisis y disponibilidad de cifras y transacciones que alimentan API diseñadas para conectarse con cuentas bancarias; y

(e) las finanzas embebidas, que agrupan soluciones dentro de productos no financieros y constituyen una fuente significativa de ingresos para nuevos actores.

En suma, aunque México fue pionero en América Latina al publicar la Ley Fintech en 2018, actualmente se encuentra rezagado en la construcción de un sistema monetario y financiero ágil, transparente, accesible, seguro y abierto. Esto se debe, por un lado, a la falta de regulación secundaria que permita implementar plenamente un sistema de finanzas abiertas y, por otro, a la ausencia de una colaboración integral y sostenida con el sector privado para definir objetivos específicos e implementarlos. Hoy el liderazgo lo tiene Brasil, donde las autoridades, en conjunto con el sector privado, han definido un modelo de sistema financiero programable, capaz de incorporar de manera progresiva nuevos productos y servicios. El primer paso en ese proceso ha sido la adopción masiva de los pagos instantáneos. Mientras que el Banco de México ha lanzado DiMo (Dinero Móvil), que a diciembre de 2024 contaba con 11 millones de usuarios —equivalentes al 9 % de su población— registrados a través de más de 20 instituciones, Brasil cuenta con PIX, utilizada por el 80 % de su población. En ese país se realizan actualmente más de 250 millones de transacciones diarias, lo que ha reducido el uso de cajeros automáticos, pues los usuarios pueden retirar dinero en cualquier tienda de conveniencia, siempre y cuando la caja registradora esté conectada a PIX.

Con esta base, Brasil cuenta con una reglamentación clara y específica en materia de finanzas abiertas, desarrollada en colaboración con los bancos comerciales, que persigue dos objetivos básicos: la comparabilidad e interoperabilidad en tiempo real. Para ello, han desarrollado una aplicación en la que los usuarios pueden acceder a todos los productos y servicios de los bancos e instituciones financieras individuales con los que tienen cuentas. No es lo mismo operar con tres aplicaciones distintas —por ejemplo, las de un banco, una casa de bolsa y una aseguradora— que disponer de una sola plataforma en la que se concentre toda la información de manera integral. Además, el usuario puede, cuando lo desee, cotizar productos y servicios en este mismo lugar y concretar las operaciones que quiera de manera instantánea. Quien esté interesado en analizar los pagos instantáneos y la inclusión financiera en la región de América Latina y el Caribe puede consultar el documento 153 (marzo de 2025) del Banco de Pagos Internacionales, citado en la bibliografía.

Algunos participantes del ecosistema *fintech* en México consideran que el aspecto positivo del rezago nacional radica en la posibilidad de aprender

tanto de los aciertos como de los errores de países como Brasil, India, Reino Unido y la Unión Europea. Desde esta perspectiva, sostienen que, si se aprovecha esa experiencia, al momento de elaborar las disposiciones secundarias estas podrían alinearse con las mejores prácticas, lo que permitiría retomar el crecimiento con mayor rapidez. La presidenta de México respaldó lo anterior, ya que el 2 de septiembre de 2025 anunció una revisión del sistema financiero que contempla la digitalización de los sistemas de pagos en línea con modelos aplicados en otros países. En sus palabras: «Brasil e India, por ejemplo, tienen esquemas de pagos digitales muy avanzados. En México, todavía no avanzamos lo suficiente en eso y queremos avanzar más para el beneficio de la gente» (*La Jornada*, 2025).

Como cierre de esta sección y de la anterior, resulta pertinente complementar el análisis con una evaluación general de los siete años de vigencia de la Ley Fintech. Tiene dos aspectos positivos y dos negativos. Entre los primeros destaca la operación regulada de 61 instituciones de fondos de pagos electrónicos y 27 instituciones de financiamiento colectivo. Entre los segundos sobresale la ausencia de modelos novedosos autorizados (*sandbox*) y la falta de reglamentación secundaria para implementar las finanzas abiertas.

Regulación en la Unión Europea

Tras un proceso de negociación exitoso, el 9 de junio de 2023 se publicó en el *Diario Oficial de la Unión Europea* el Libro 150 (L 150), que contiene tanto el Reglamento 1113 del Parlamento Europeo y del Consejo, relativo a las transferencias de fondos y de determinados criptoactivos, como el Reglamento 1114, referente a los mercados de criptoactivos. El objetivo de la presente sección es resaltar cuatro aspectos de cada uno de estos instrumentos.

El Reglamento 1113 tiene como objetivo cumplir con los estándares del GAFI en general, y en particular, de las Recomendaciones 15 (regulación y supervisión de las nuevas tecnologías) y 16 (identificación plena de los participantes en una transacción). A continuación, se destacan los siguientes temas:

(a) Antes de la entrada en vigor de este reglamento, solo se supervisaban dos categorías de proveedores de servicios: aquellos que custodiaban monederos electrónicos y los que prestaban servicios de cambio de monedas virtuales por monedas fíat. Con el fin de subsanar las lagunas existen-

tes en el marco del combate al lavado de dinero y el financiamiento al terrorismo, la normativa reconoce ahora diez proveedores de servicios y actividades de criptoactivos. La lista incluye a quienes custodian y administran por cuenta de terceros; gestionan una plataforma de negociación; canjean criptoactivos por fondos; intercambian criptoactivos por otros criptoactivos; ejecutan las órdenes por cuenta de clientes; colocadores; los que reciben y transmiten órdenes por cuenta de clientes; asesores; gestores; y los que hacen transferencias de criptoactivos por cuenta de clientes. Esta ampliación supone un reto para los supervisores de la Unión Europea.

(b) El reglamento reconoce que las transferencias relacionadas con tecnologías diseñadas para mejorar el anonimato —en particular los monederos privados y los mezcladores de criptoactivos— son factores de alto riesgo para el lavado de dinero y el financiamiento del terrorismo. En este contexto, encomienda a la Autoridad Bancaria Europea (ABE) que publique las directrices que se deben aplicar para mitigar estos riesgos.

(c) Se explica cómo, en algunas instancias, los criptocajeros automáticos permiten a los usuarios realizar transferencias de criptoactivos a una dirección mediante depósitos en efectivo, sin ninguna forma de identificación ni verificación del cliente. El efectivo puede ser de origen desconocido y, por lo tanto, ser un vehículo ideal para actividades ilícitas, por lo que pasa a formar parte de esta regulación.

(d) El reglamento establece que los proveedores de servicios de criptoactivos deben evaluar el riesgo cuando realicen trasferencias hacia o desde direcciones autoalojadas (véase el glosario de este libro). Cuando proceda, deberán aplicar medidas reforzadas de diligencia debida para gestionar y mitigar los riesgos adecuadamente. Cualquier operación que considere inusual deber ser informada a la Unidad de Inteligencia Financiera.

Por su parte, el Reglamento 1114 para los mercados de criptoactivos (MiCA, por sus siglas en inglés), muestra el interés estratégico de la Unión Europea por facilitar el uso de tecnologías innovadoras en el sector financiero. Dentro de este objetivo se incluye a la tecnología de registros distribuidos (TRD) y su aplicación en el espacio de los criptoactivos. Los cuatro temas que se subrayan son:

(1) El reglamento introduce una taxonomía para estudiar con claridad los criptoactivos a través de tres categorías: fichas referenciadas a dinero electrónico; fichas referenciadas a activos (monedas estables), y un ente residual que engloba aquellos que no corresponden a dinero electrónico ni fichas referenciadas a activos, entre las que se encuentran las fichas de consumo.

(2) El dinero electrónico es diferente a los criptoactivos referenciados a una moneda oficial. En el primer caso, es emitido por un banco y hay un crédito ante el emisor. En el segundo, es expedido por otras entidades que no tienen crédito ante el emisor y limitan el periodo de reembolso.

(3) Para lograr una supervisión adecuada, se requiere que los servicios de criptoactivos sean prestados por personas morales que estén domiciliadas en un Estado miembro de la Unión Europea, en el que lleven a cabo actividades empresariales sustantivas.

(4) Los emisores de ofertas públicas distintas de las fichas referenciadas a activos o a dinero electrónico deben elaborar un documento de información obligatoria, equivalente a un libro blanco de criptoactivos o a un prospecto de colocación con todos los detalles pertinentes. Dicho documento debe incluir el material publicitario, el cual deberá ser imparcial, claro y no engañoso.

Ambos reglamentos excluyen los servicios prestados de manera completamente descentralizada (DeFi). Tampoco abarcan los proyectos actuales o futuros relacionados con las monedas digitales de los bancos centrales (CBDC, por sus siglas en inglés). Asimismo, al priorizar los criptoactivos financieros, dejan fuera de su ámbito de aplicación a las fichas no fungibles (NFT).

Este breve análisis concluye señalando que ambos reglamentos garantizan el principio de neutralidad tecnológica, en tanto no regulan la tecnología subyacente, sino sus aplicaciones y actividades. La legislación se basa en los principios de «misma actividad, mismos riesgos, mismas normas». Los reglamentos entraron en vigor en diciembre de 2024, por lo que se necesita más tiempo para hacer una evaluación seria de su implementación. Es un hecho que se adelantaron a Estados Unidos, en donde la única ley aprobada en julio de 2025 (GENIUS Act), probablemente entrará en vigor en 2026. Por su parte, tanto la ley que definirá la estructura de mercado de los activos virtuales (CLARITY Act) como la ley que prohíbe al banco central la emisión de moneda digital y busca proteger la seguridad financiera de los ciudadanos frente a la vigilancia gubernamental (CBDC Anti-Surveillance State Act) fueron aprobadas en julio por la Cámara de Representantes y se espera que sea discutida por el Senado en 2026.

Computación cuántica y las cadenas de bloques

Los computadores actuales que utilizan el sistema binario (bits conformados por 0 y 1) han sido capaces de resolver, uno por uno, la gran mayoría de los problemas matemáticos mediante algoritmos seguros, entre los que destaca el SHA-256 (*Secure Hash Algorithm*).

En 2025 se conmemoró el centenario de la teoría cuántica que impactó la física y provocó grandes discusiones científicas y filosóficas. Una de sus aplicaciones prácticas inició en la década de 1980, con el surgimiento de un área conocida como computación cuántica, basada en cúbits, que pueden ser cero, uno o ambos a la vez, que tratan de resolver problemas probabilísticos y matemáticos de manera simultánea o paralela de forma más eficiente y rápida. En la siguiente década se desarrollaron técnicamente diversos algoritmos, entre los que destacan el de Peter Shor (1994), que permite calcular de manera probabilística los factores primos de números a una velocidad más rápida que cualquier computadora clásica o tradicional, y el algoritmo de Lov Grover (1996), que busca la mejor secuencia de datos para describir la inversa de una función. Desde 2011 existen computadoras cuánticas comerciales desarrolladas por empresas como D-Wave, IBM, Google y Honeywell International, que compiten activamente en esta primera etapa, a la cual también se han sumado China y la Unión Europea. Se estima que el número de computadores cuánticos existentes en el mundo oscila entre 100 y 200. Sin embargo, no se ha logrado escalar el número de cúbits necesarios para sustituir o complementar a los computadores clásicos. Tampoco existe un acuerdo del número exacto de cúbits necesarios para romper cifrados, aunque en la actualidad nos encontramos lejos de sus rangos de operación. La Organización de la Naciones Unidas (ONU) declaró 2025 como el Año Internacional de la Ciencia y de las Tecnologías Cuánticas. En este contexto, la edición especial de primavera-verano de 2025 de la revista *Scientific American* está dedicada completamente al mundo cuántico y menciona que, más allá de los temas físicos de la materia y sus componentes, así como de la posibilidad de espacios y tiempos alternativos, es probable que la aplicación tangible más relevante de sus descubrimientos sea la computación cuántica, por lo que le dedica tres artículos destacados, altamente recomendables para los lectores de este texto.

Los computadores cuánticos necesitan una mayor capacidad computacional que los clásicos, por lo que usan transistores (chips) especializados que puedan manejar ceros y unos, y requieren de enfriadores (refrigerados) de gran escala, cuyo costo es elevado.

Algunos desarrolladores consideran que los computadores cuánticos alcanzarán su objetivo en cinco años, mientras que otros estiman que serán necesarios al menos cinco lustros. En lo que sí están de acuerdo es que, cuando esto suceda, todo cambiará para bien o para mal. Si la computación cuántica se utiliza adecuadamente ayudará en el campo de la medicina —con diagnósticos más rápidos y personalizados—, la meteorología, el medioambiente, las comunicaciones, las finanzas y las criptomonedas. No obstante, si se utiliza para mal, puede abrir la puerta para todo tipo de robos (*hacks*) tanto en el sistema financiero formal como en el espacio cripto. En resumen, la computación cuántica puede ser una magnífica oportunidad para cambiar de forma progresiva las funciones resumen (*hash*) y la criptografía asimétrica que actualmente utilizamos con seguridad en los ordenadores clásicos; alternativamente, su uso irresponsable podría facilitar prácticas maliciosas con fines personales.

Estados Unidos ha sido uno de los primeros países en reconocer que se necesitan nuevos estándares para una transición adecuada. En agosto de 2024, a través del Instituto Nacional de Estándares y Tecnología (NIST, por sus siglas en inglés), dependiente del Departamento de Comercio, finalizó un conjunto de cuatro algoritmos destinados a la nueva encriptación resistente a ataques cuánticos. El primero, CRYSTALS-Kyber, define en lo general la estandarización de la encriptación pública. Los tres restantes se orientan a las firmas digitales: uno para las claves o llaves generales de cifrado (FIPS 203), otro para la protección de firmas digitales (FIPS 204) y un tercero para respaldar la autenticación de identidades (FIPS 205). Este resultado fue fruto de un esfuerzo público y privado, con la participación de criptógrafos de todo el mundo y de grandes empresas tecnológicas como IBM.

Pasamos ahora a la relación entre la computación cuántica y las cadenas de bloques (TRD), uno de los principales temas de interés de este manuscrito. Hoy existe una considerable especulación, ya que muchos desarrolladores e inversionistas consideran que se aproxima un peligro para la seguridad de las cadenas de bloques y de las criptomonedas. A continuación se presentan algunos ejemplos de cómo la computación cuántica podría poner en peligro a Bitcoin, la criptomoneda con mayor capitalización del mercado.

Tanto en el primer capítulo como en el anexo 1 se abordan algunas características generales de Bitcoin, pero es necesario volver a distinguir entre el algoritmo SHA-256 (función resumen), que se utiliza para la minería, y la encriptación de curva elíptica (véase el glosario) que usan los monederos (*wallets*) para relacionar la clave privada con las públicas y sus múltiples direcciones. Ambos son algoritmos, pero cumplen funciones distintas: el primero es para hacer funciones resumen, pero no es un algoritmo de cifrado. Algunos los nombran «algoritmos criptográficos», pero esto puede confundir, ya que en realidad son funciones *hash*, ya sea de datos, bits o texto. El segundo es un algoritmo de firmas digitales de curva elíptica (ECDSA, por sus siglas en inglés) que sí usa encriptaciones.

La clave privada es un número aleatorio de 256 bits que es factible usar en cualquier monedero. Puede ser cualquier número entre 1 y 2^{256}, lo que en el sistema decimal es aproximado a 10^{77}, es decir, una cantidad de opciones y combinaciones extremadamente amplia. La clave pública es derivada de la privada usando una encriptación de curva elíptica, un proceso que, en teoría, es irreversible. Las claves privadas y públicas pueden representarse en diferentes formatos, entre los que destaca el sistema hexadecimal que utiliza 64 dígitos, cada uno con cuatro bits. Con la clave pública se pueden generar múltiples direcciones mediante una función resumen (*hash*) que tiene una base 58 para hacerlas más compactas. El creador de Bitcoin recomendó desde el inicio cambiar la dirección en cada transacción realizada, consejo que sigue siendo útil hasta la fecha. Si se asume que Satoshi Nakamoto desapareció conservando una gran cantidad de bitcoins que nunca se han movido, significa que su monedero contiene las direcciones originales. Igualmente, muchas otras direcciones fueron creadas en la primera etapa de su lanzamiento y de manera explícita su clave pública fue almacenada en la cadena de bloques, lo que las hace más vulnerables frente a los computadores cuánticos. En estos casos, el atacante no necesita vulnerar el SHA–256, sino solo encontrar la clave privada con la clave pública que está en la cadena de bloques. Más allá de estos casos particulares, en el caso de las direcciones modernas, cuando las computadoras cuánticas alcancen un mayor grado de madurez y aumenten su número de cúbits, podrían descifrar la encriptación de curva elíptica. Es decir, derivado de las direcciones, podrían obtener las claves públicas y después las claves privadas para transferir los bitcoins no gastados a cualquier otra cuenta.

De manera alternativa, las computadoras cuánticas podrían intervenir durante el proceso de minería, cuando los mineros trabajan en su bloque candidato. Dado que todos los nodos que ejecutan el *software* completo de

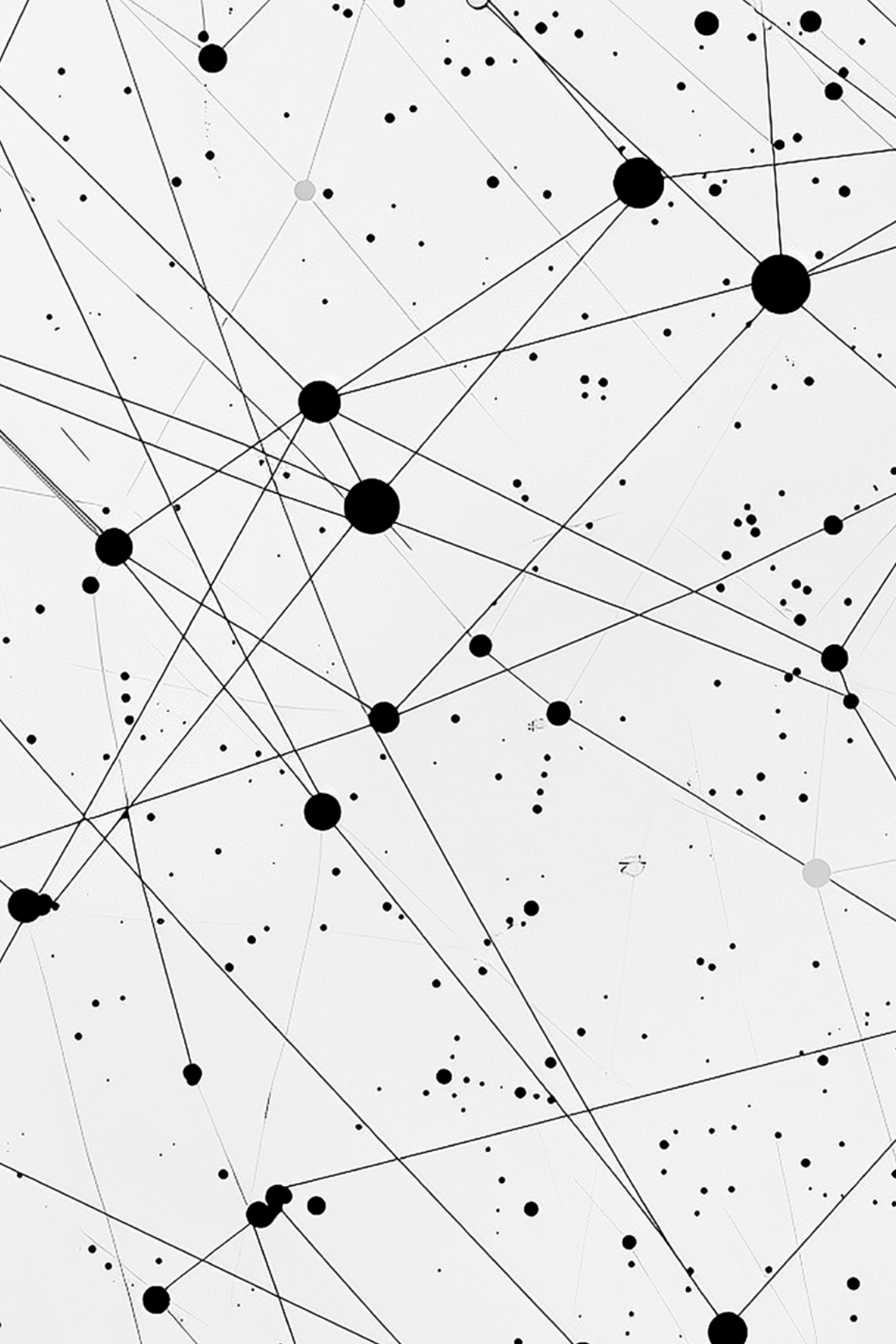
Bitcoin pueden observar las transacciones de pago solicitadas por los usuarios, los computadores cuánticos podrían interferir para realizar un ataque, cambiando las direcciones de destino, y descubrir la función resumen que ligue este bloque con el anterior. Este proceso se puede considerar como el ataque del 51 %, en el que el control mayoritario del poder computacional permitiría alterar las transacciones del bloque.

La transición que Bitcoin debe realizar para prepararse ante las computadoras cuánticas se ve dificultada no solo por lo mencionado previamente, sino también por una comunidad históricamente conservadora respecto a las actualizaciones de su protocolo de consenso o mayoría. Por ello, actualmente hay un silencio en relación con la bifurcación necesaria para enfrentar este riesgo. Una perspectiva diferente se nota en Ethereum y Solana, cuyos equipos trabajan activamente en las etapas necesarias para llevar a cabo una transición gradual y segura.

El cofundador de Ethereum, Vitálik Buterin, participó activamente en la reunión anual organizada por la Fundación Ethereum en Buenos Aires, Argentina, durante la segunda quincena de noviembre de 2025. En dicho evento abordó el tema de la computación cuántica y afirmó que la encriptación de curva elíptica podría ser vulnerada por computadores cuánticos en los próximos cuatro años. En consecuencia, ya está trabajando en la actualización de la tecnología de Ethereum, un proceso que requiere de la coordinación de validadores, desarrolladores y usuarios corporativos e individuales. Esta fase de actualización, conocida como el capricho o el lujo (*the splurge*), está prevista entre 2027 y 2030 y busca que Ethereum sea más segura, simple y óptima, priorizando los cambios no solo en la primera capa, sino en los estratos superiores y en las billeteras.

Solana, por su parte, ha dado a conocer que también trabaja en la implementación de algoritmos resistentes a los computadores cuánticos y ha expresado que este proceso no requiere rehacer la red completa de operación. Una de las actualizaciones más importante es la de firmas digitales y en innovaciones en la segunda capa.

Para terminar esta sección, se reitera que los computadores cuánticos aún se encuentran en una etapa experimental. Los autores de este manuscrito confían en que, antes de que sucedan los primeros ataques, se implementen los nuevos estándares que garanticen la seguridad del espacio cripto y del sistema financiero formal. Aunque el objetivo es claro, su ejecución será compleja, al requerir voluntad política y un proceso planificado.



Capítulo 4

Grupos, conjeturas y recomendación

En los tres primeros capítulos se han medido los servicios descentralizados mediante indicadores como el valor de capitalización de las criptomonedas (activos virtuales o criptoactivos) y el número de usuarios que han adoptado esta opción, la cual no requiere de los intermediarios tradicionales. Los resultados obtenidos a partir de las dos medidas muestran grandes cantidades absolutas, pero porcentajes reducidos cuando se comparan con los servicios formales o centralizados. Sin embargo, más allá de estos datos, se ha creado una industria que agrupa a diversos proveedores de estos servicios, entre los que destacan los facilitadores de monederos (*wallets*), los desarrolladores de *software*, los criptocajeros automáticos, los proveedores de liquidez, los corredores (*brokers*), las plataformas que listan y comunican precios, los denominados oráculos —que conectan las cadenas de bloques con el mundo exterior—, así como los que custodian, administran y contabilizan las operaciones.

En el caso mexicano, la actividad se concentra más en el uso de los servicios descentralizados que en la creación de empresas y plataformas. En consecuencia, existe una mayor cantidad de despachos de asesoría (económica, fiscal y contable) que de emprendedores interesados en constituirse legalmente en el territorio nacional. Esto se puede observar en las reuniones anuales de los foros relacionados con las cadenas de bloques, la tecnología financiera y la inteligencia artificial generativa.

No puede omitirse la labor de quienes se dedican a la alfabetización ni la de quienes nos enfocamos en la educación universitaria. Los primeros suelen evitar el término *industria* y prefieren decir que se trata de un *ecosistema cripto*, en el que también incluyen pláticas y videos producidos por influyentes (*influencers*) que realizan publicidad masiva. Los segundos, en cambio, procuramos rescatar la parte tecnológica como un elemento neutral y documentar, con revistas académicas arbitradas, la evidencia teórica y empírica de los riesgos y beneficios de invertir en estos instrumentos. En relación con el uso de la estadística para obtener resultados prácticos, se sugiere al lector asegurarse de que los datos de precios del mercado de las criptomonedas provengan de proveedores confiables y sin conflicto de interés, así como ser consciente de la posibilidad de que sean manipulados.

En este capítulo se presentan las principales posturas de los distintos grupos que participan en el espacio (o ecosistema) de las criptomonedas, en contraste con las posiciones de las autoridades y de los organismos internacionales. Tras este panorama general, el texto se aventura a plantear cuatro conjeturas sobre las tendencias actuales y concluye recomendando una educación más sólida y de mayor alcance en finanzas tradicionales, centralizadas y descentralizadas.

Un panorama general de los grupos de interés

Este compendio ha dejado claro que existen diferentes puntos de vista entre los principales actores del espacio de los servicios financieros formales y descentralizados. Entre los principales grupos se encuentran: (a) los desarrolladores y usuarios originales de criptomonedas; (b) las autoridades monetarias y financieras de los países o jurisdicciones, así como algunos organismos intergubernamentales o internacionales; (c) abogados y expertos legales; (d) las autoridades tributarias; (e) los legisladores; y, finalmente, (f) las asociaciones de contadores públicos. No solo existen puntos de vista diferentes entre los grupos en general, sino también posturas divergentes al interior de cada uno de ellos.

(a) *Los desarrolladores y usuarios originales de criptomonedas* (los libertarios) que buscan evitar el uso de cualquier intermediario monetario o financiero a través de la descentralización han perdido influencia, debido a que numerosos participantes han decidido manifestar su disposición de ser regulados, supervisados e integrarse con el sistema financiero tradicional.

El presidente Trump, durante los primeros once meses de su segundo mandato presidencial que inició el 20 de enero de 2025, ha sido un factor decisivo para apoyar al espacio de las criptomonedas. Ya se mencionó en el primer capítulo la promulgación de la ley relacionada con las monedas estables (GENIUS Act), así como del avance de otras dos leyes importantes, en las que falta la aprobación del Senado. A ello se suma el lanzamiento de su moneda estable, USD1, y otra de sus empresas, Media & Technologies Group Corp, cuyas acciones son cotizadas en el Nasdaq (DJT), que ha invertido una cantidad considerable de sus recursos en bitcoin y otras criptomonedas. Asimismo, el 3 de septiembre de 2025, Erick Trump y sus asociados listaron las acciones de su empresa American Bitcoin en el Nasdaq (ABTC), con el objetivo de minar bitcoin a gran escala y con costos reducidos, además de acumular una reserva de largo plazo para dar mayor acceso a los consumidores. Estos hechos de 2025 contrastan con lo que opinaba Trump durante su primer mandato (2017-2021), cuando calificó al bitcoin como «una estafa» y afirmó no ser aficionado ni a esta, ni a otras criptomonedas, al considerarlas altamente volátiles y ca-

rentes de sustento. Por tanto, surge la pregunta: ¿qué fue lo que le hizo cambiar de opinión?

En el caso de México, uno de los representantes del grupo libertario es el empresario Ricardo Salinas Pliego, que no solo acepta el bitcoin en algunos de sus establecimientos, sino que también ha publicado el libro *La iluminación de bitcoin: el final de la edad oscura del dinero fíat* (*The bitcoin enlightenment: ending the fiat dark age*), junto con Pascal Hügli y Daniel Jungen. En la publicación menciona que el dinero fíat es un fraude y, durante la presentación virtual del libro llevada a cabo el 30 de mayo de 2025, reiteró que su portafolio preferido es invertir 80 % en bitcoin y en sus empresas mineras, y 20 % en oro o en sus mineros.

En el ámbito de los desarrolladores de cadenas de bloques existe una división interna. La mayoría se enfoca en resultados de corto plazo mediante la creación de fichas especulativas; por el otro lado, una minoría piensa en el largo plazo, concentrándose en la creación de tókenes que tienen una utilidad social, además de buscar una descentralización escalable, sin sacrificar la seguridad. En este último grupo sobresale el cofundador de Ethereum, Gavin Wood, quien escribió su libro amarillo. Dejó la Fundación Ethereum en 2016 al no coincidir con la decisión de que la plataforma perdiera su inmutabilidad y se concretara la bifurcación de Ethereum Classic.

Wood ha continuado su carrera con el establecimiento de la Fundación Web3, con sede en Suiza, desde la cual ha colaborado en la creación de la cadena de bloques Polkadot (2021), orientada a lograr la interoperabilidad entre varias cadenas de bloques sin usar puentes. Su misión consiste en promover una web descentralizada en la que los usuarios puedan ser parte fundamental de la gobernabilidad de la plataforma. Su token es DOT, que actualmente CoinGecko ubica en el lugar 35 por valor de capitalización, superior a los 6.1 billones de dólares.

En las últimas apariciones públicas de 2025, Gavin Wood expresó que en el fondo no se considera parte del ecosistema cripto. Al referirse a las criptomonedas en general, las identifica como algo parecido a las finanzas de Mickey Mouse y, en particular, ha calificado a las criptomonedas meme —basadas en bromas— como casinos no autorizados, aunque después matizó esta postura al describirlas como escenarios propicios para la negociación con información privilegiada. También ha hecho explícito que las criptomonedas constituyen solo una fracción de la web3, pero no su totalidad. Wood se define como un científico informático con una visión de largo plazo, interesado en desarrollar proyectos de utilidad social dentro

de la web3, para que los usuarios puedan confiar sus datos y lograr controlar su propio destino, es decir, su soberanía.

Es interesante analizar el punto de vista de Wood, en el que considera a la web3 y a la inteligencia artificial en posiciones diametralmente opuestas. Opina que esta última es una tecnología centralizada en la que los usuarios no tienen por qué confiar en las fuentes de datos usadas y donde muchas de las plataformas son opacas. En contraste, la web3 es descentralizada y logra eliminar al intermediario que controla los datos, y facilita la soberanía de los usuarios.

En este contexto, es importante mencionar que uno de los principales proyectos que ha utilizado la cadena de bloques de Polkadot y su plataforma experimental es Bittensor. Este proyecto fue lanzado en 2021 por Jacob Steeves y Ala Shaabana, y funciona, simultáneamente, como una plataforma para la producción de bienes y servicios digitales y como una cadena de bloques que los sustenta mediante su moneda nativa TAO, cuya política monetaria es similar a la de bitcoin. Uno de los principales bienes y servicios digitales es la inteligencia artificial, desarrollada a través de modelos para el aprendizaje de máquinas. Se trata de un desarrollo descentralizado de inteligencia artificial en el que participan mineros, validadores, creadores y proveedores de liquidez, quienes colaboran de manera coordinada para que las máquinas aprendan y generen información de mayor calidad. Esta colaboración se lleva a cabo tanto dentro como fuera de la cadena de bloques, y, cuando las contribuciones son evaluadas positivamente, los participantes son recompensados. A diferencia de la inteligencia artificial generativa centralizada —como OpenAI, Claude o Google—, en la que el usuario que quiere un mejor servicio tiene que pagar una cantidad mensual, en Bittensor la participación es abierta y quienes aportan resultados valiosos obtienen un pago. De este modo, Bittensor ha logrado implementar un mercado para la inteligencia artificial descentralizada, que actualmente tiene un valor de capitalización de 3.2 billones de dólares y ocupa la posición 47 en el listado de CoinGecko. En este escenario, cabe preguntarse: ¿se prefiere un modelo de inteligencia artificial centralizada o uno descentralizado?

(b)*Las autoridades monetarias y financieras de los distintos países* han adoptado posturas muy diversas frente a las criptomonedas, que van desde la prohibición hasta la complacencia total o parcial de su operación, pasando por esquemas de reglamentación —nuevos o antiguos— y por acciones de represión que desalientan su operación. Algunas de estas decisiones se basan en priorizar la protección de los usuarios de servicios, otras se enfocan

en la estabilidad del sistema financiero, y unas pocas más en el fomento de la innovación. Existe, además, un reconocimiento generalizado de que cualquier esfuerzo individual no resuelve el problema de la implementación global de las criptomonedas y su operación continua (24/7), por lo que algunos países han optado por una cooperación regional.

Prevalece el hecho de que los proyectos de operación de las plataformas electrónicas descentralizadas recurran al arbitraje regulatorio y se ubiquen en países o jurisdicciones más flexibles. En este sentido, las instituciones financieras tradicionales reguladas consideran que no hay equidad cuando se trata de competir con las criptomonedas, las cuales pueden obtener licencias de manera rápida y sin muchas complicaciones. Se destacan esfuerzos del GAFI, del FMI y del BIS como mecanismos de cooperación internacional que intentan nivelar el terreno de juego.

El GAFI es un organismo intergubernamental que establece estándares para la adopción de medidas legales destinadas a combatir el lavado de dinero, el financiamiento al terrorismo y otras amenazas a la integridad del sistema financiero internacional. De manera periódica, elabora dos listas de países o jurisdicciones que no cumplen con sus consejos. La llamada lista negra incluye a aquellas naciones que tienen deficiencias estratégicas para cumplir con los mandatos mencionados y no tienen voluntad política para hacerlo. La lista gris, por su parte, agrupa a las entidades vulnerables que colaboran activamente con el GAFI en la implementación de reformas conforme a un calendario determinado, motivo por el cual quedan sujetas a un monitoreo reforzado. En 2025, el GAFI reportó la evaluación de 108 países y jurisdicciones: dos se encuentran en la lista negra (Corea del Norte e Irán), y 21 en la lista gris (Haití, Mónaco, Siria y Venezuela, entre otros). Los 85 restantes han hecho las reformas necesarias para combatir el lavado de dinero y el financiamiento al terrorismo. México forma parte del GAFI desde el año 2000 y actualmente cumple, de manera total, mayoritaria o parcial, con 39 de sus 40 recomendaciones. Como se mencionó en el capítulo 3, la única recomendación pendiente es la número 23, relacionada con los sujetos obligados por actividades vulnerables (actividades y profesiones no financieras designadas). Para su cumplimiento se requería una reforma legal cuyo primer intento, entre 2018 y junio de 2025, fracasó; sin embargo, una nueva reforma ya fue aprobada y publicada en el DOF el 16 de julio de 2025.

El FMI ha ampliado este análisis al abordar los centros financieros extraterritoriales (*off-shore financial centers*). Dado que no existe una defini-

ción consensuada, el organismo ofrece, a través del documento de trabajo elaborado por Ahmed Zoromé (2007), la siguiente definición:

> *un centro financiero extraterritorial es un país o jurisdicción que provee servicios financieros a no residentes en una escala que es enorme (inconmensurable) en relación con el tamaño y el financiamiento de su economía doméstica. (p. 7)*

Las razones que llevan a los empresarios a optar por estas jurisdicciones son diversas: algunos buscan una carga fiscal nula o reducida; otros, una regulación más laxa, y otros más se basan en razones climatológicas o culturales. Las actividades financieras que establecen en estos centros abarcan desde operaciones bancarias y bursátiles hasta, más recientemente, el ámbito de las criptomonedas. Los huéspedes los reciben para generar ingresos y especializarse en una economía que exporta servicios financieros. El estudio citado utiliza la razón entre la exportación neta de servicios financieros y el PIB, e identifica 22 centros.

Por su parte, el BIS se basa en los centros financieros transfronterizos (*cross-border financial centers*) y, en su documento de trabajo núm. 1035, escrito por Pamela Pogliani y Philip Wooldridge en julio 2022, los define como: «un país o jurisdicción cuyos activos y pasivos externos son excepcionalmente altos comparados con el tamaño de la economía doméstica» (p. 6).

Reconocen que el trabajo de Ahmed Zoromé (2007) representó un paso en la dirección correcta, aunque proponen capturar la intermediación financiera a partir de activos y pasivos mediante varios indicadores estadísticos. Con esta nueva metodología identifican 21 centros financieros transfronterizos. Con la lectura de estos tres párrafos, se podrá notar que en la actualidad cada organismo tiene objetivos diferentes, así como definiciones y metodologías que no siempre concuerdan.

Los organismos mencionados han liderado la defensa del sistema monetario y financiero tradicional o centralizado. El FMI ha seguido de cerca el ecosistema de las criptomonedas, concentrándose en lo que sucede en los países en desarrollo. En su *Reporte global de estabilidad financiera* publicado en octubre de 2021, dedicó un capítulo completo a evaluar los desafíos

que las criptomonedas imponían a la estabilidad de la economía monetaria y las finanzas tradicionales. Menciona que:

> *en los mercados emergentes, la aparición de los cripto-activos tiene algunos beneficios, pero puede eludir las restricciones de los tipos de cambio y los controles de capital. Un incremento en la negociación de los cripto-activos en estas economías puede desestabilizar los flujos de capital. (p. 41)*

En ese momento, el valor de capitalización de las criptomonedas se aproximaba a los tres trillones de dólares y el reporte reiteró la postura que el FMI venía sosteniendo desde 2018: los criptoactivos no constituían un riesgo sistémico para la estabilidad monetaria y financiera tradicional. Como se mostró en la tabla 4 del primer capítulo, el valor de capitalización a finales de diciembre de 2025 se encontraba prácticamente en el mismo nivel (3.06 trillones de dólares), lo que permite deducir que el FMI mantiene su opinión de que el espacio cripto no representa un riesgo relevante ni para el sistema monetario ni para el sistema financiero internacional.

Una de las formas de sustentar esta conclusión consiste en comparar el valor de capitalización de las criptomonedas con el valor total de los activos de las instituciones financieras a nivel mundial, que en 2021 ascendía a 468 trillones de dólares (Statista). El cociente resultante es menor al 1 %, lo que evidencia que el espacio cripto es reducido y, por tanto, no se considera como un riesgo sistémico en el aspecto monetario ni financiero.

Otros investigadores prefieren realizar la comparación con el producto interno bruto (PIB) global, aunque para muchos resulta inapropiado mezclar un acervo —como el valor de capitalización de las criptomonedas— con un flujo, como el PIB. Si se efectuara este ejercicio en la actualidad, el resultado indicaría que el espacio cripto representa el 2.5 % del PIB global. Al igual que en el párrafo anterior, el resultado final es un porcentaje reducido que sustenta la posición del FMI. En esencia, el mensaje que el FMI envía al espacio cripto es que, pese a su innovación y a la magnitud de inversión en publicidad, su dimensión sigue siendo limitada.

El *Reporte global de estabilidad financiera* del FMI, presentado el 14 de octubre de 2025, aborda la rapidez con la que están creciendo las monedas estables (*stablecoins*) respaldadas por el dólar estadounidense. Considera

que, si su adopción continúa a este ritmo, puede tener tres implicaciones para la estabilidad del sistema financiero formal. A saber:

> *(1) las economías más débiles podrían enfrentar sustitución de monedas y una reducción en la efectividad de las herramientas de política, (2) la estructura del mercado de bonos puede modificarse con implicaciones potenciales en la desintermediación del crédito, y (3) las salidas en masa de los inversionistas de las criptomonedas podrían forzar la venta de los activos en reserva. Los efectos sistémicos potenciales podrían condicionar el crecimiento continuo de las monedas estables. (pp. xiv-xv)*

El BIS dedicó un capítulo entero de su *Reporte económico anual* 2023 para dar a conocer su modelo para el futuro del sistema monetario, con el objetivo de mejorar lo existente y facilitar lo nuevo. Propone transitar de los registros contables digitales actualmente utilizados por los bancos a sistemas basados en fichas (tókenes), dejando claro que «las criptomonedas y las finanzas descentralizadas han ofrecido una visión de la promesa de la tokenización, pero las criptomonedas son un sistema fallido que no pueden cubrir el futuro del dinero» (p. 86).

Los elementos principales de su modelo están constituidos por las monedas digitales de los bancos centrales (CBDC), los depósitos de los bancos comerciales que son tokenizados y otros reclamos o derechos sobre activos financieros o reales. La propuesta consiste en utilizar un registro unificado (*unified ledger*) para conectar todos los elementos. Este registro unificado se materializa en una plataforma digital programable cuyo protocolo asegura la interoperabilidad de los elementos y la finalidad (*finality*) de las transacciones que se realizan entre ellos. Se aclara que el término de finalidad se refiere al momento en que los fondos o los activos son transferidos de una cuenta a otra, y oficialmente se convierten en propiedad legal del que los recibe. Se puede resumir como la liquidación de operaciones en firme.

El BIS deja claro que quiere mantener el sistema actual, en el que participan los bancos centrales en combinación con los bancos privados autorizados, pero también manda el mensaje de que desea utilizar la tecnología de registros distribuidos (TRD) e innovaciones como el uso de fichas o tó-

kenes. Su propuesta toma como base el uso de monedas digitales de los bancos centrales (CBDC) de mayoreo, ya que ello garantiza la participación de los bancos privados. Solo recomienda el uso de CBDC al menudeo en casos especiales que cada país debe evaluar. También prefiere la tokenización de los depósitos en bancos privados (dinero privado) frente al uso de monedas estables (*stablecoins*), debido a su variabilidad y a que no concretan la función de unidad de cuenta monetaria. Finalmente, propone el uso de interfaces de programación de aplicaciones informáticas estandarizadas (API) para conectar los diferentes sistemas y lograr la interoperabilidad. Aunque se habla de un registro unificado, en la práctica se trata de múltiples registros conectados entre sí.

A principios de abril de 2024, el BIS dio a conocer un proyecto experimental denominado Agorá, mediante el cual siete bancos centrales, junto con el sector bancario privado, usan la tokenización para realizar pagos transfronterizos de manera más rápida, económica e integral. Posteriormente, se prevé utilizar el dinero digital mayorista de los bancos centrales y depósitos comerciales en plataformas programables ejecutadas por contratos inteligentes. Entre los siete bancos centrales se encuentran la Reserva Federal de Nueva York, el Banco de México y el Banco de Inglaterra. Los bancos múltiples y otras empresas privadas financieras fueron convocados por el Instituto de Finanzas Internacionales (IIF, por sus siglas en inglés) en mayo de 2024. Este proyecto mantiene el sistema tradicional de dos niveles —público y privado— y utiliza el registro unificado (*unified ledger*) mencionado en párrafos anteriores. Resulta evidente que los banqueros tradicionales tratan de recuperar terreno en el tema de las remesas y los pagos internacionales, donde el uso de las criptomonedas y las monedas estables ha ganado ventaja.

En 2024, el BIS pasó de delinear su visión de futuro monetario a abordar el ámbito financiero. Para ello, acuñó el término *finternet* para explicar el sistema financiero del futuro. Agustín Carstens y Nandan Nilekani (2024) publicaron un documento de trabajo (*BIS Working Paper 1178*) en el que proponen un ecosistema financiero múltiple interconectado, tal como lo es hoy internet. De aquí se deriva el título en donde anteponen la F de finanzas a la palabra internet. Introducen el término como una visión del futuro del sistema financiero que:

> *implica una red de ecosistemas financieros interoperables, en donde las personas y las empresas son colocadas en el centro de la*

> *interacción financiera. El sistema se basa en tres pilares fundamentales. Estos son: (i) una arquitectura económica sólida; (ii) la integración de tecnologías avanzadas; y (iii) una estructura regulatoria y de gobierno robusta. (p. 10)*

Este modelo concibe un sistema financiero basado en tókenes y apoyado por registros unificados. Asimismo, identifica como administradores de dichos tókenes a bancos, sociedades operadoras de fondos de inversión y otras compañías financieras y no financieras, como los organismos de registros prediales. En el ámbito de las tecnologías avanzadas, no solo incluye los registros distribuidos, la criptografía, los contratos inteligentes, las firmas digitales y la componibilidad, sino también los avances en la inteligencia artificial. Se subraya que la incorporación de estas tecnologías no implica que todo debe de cambiar, y se reafirma, como principio central, la asociación público-privada de los sistemas monetarios y financieros.

En el marco de las reuniones de primavera del Fondo Monetario Internacional y del Banco Mundial, el 23 de abril de 2025 se realizó el panel titulado la «Tokenización y el sistema financiero: adaptándose al nuevo panorama». En él, los autores Agustín Carstens y Nandan Nilekani informaron que la tecnología necesaria para su implementación ya estaba lista y que los conceptos necesarios para los monederos (*wallets*) y los registros distribuidos habían sido definidos. De igual forma, reiteraron su expectativa de entregar una demostración de su funcionamiento en un entorno real hacia finales de 2025. En el mismo evento participó Piero Cipollone, miembro del Consejo Ejecutivo del Banco Central Europeo, quien delineó dos dimensiones clave de la posible tokenización del sistema financiero. La primera se refiere a lograr una mayor eficiencia del sistema actual, con operación continua (24/7), menores costos y el uso de una sola plataforma para unificar los procesos de negociación, compensación y liquidación de pagos y valores. La segunda se relaciona con la posibilidad de ofrecer nuevos servicios, como monedas estables de los bancos centrales, la tokenización de los depósitos bancarios y de la emisión de bonos del gobierno. En este caso, existiría un cambio radical en la naturaleza del dinero, ya que estaríamos hablando de un archivo (*file*) digital como su nueva definición. En esencia, la propuesta de *finternet* busca aprovechar la tecnología de registros distribuidos para incrementar la eficiencia del sistema financiero, utilizando como ancla una moneda di-

gital de los bancos centrales, preferentemente en su modalidad de mayoreo. Con esto, se retoma el concepto de cadena de bloques de los activos, pero se aplica con dinero fíat de cada uno de los países. Se puede decir que *finternet* conserva la estructura fundamental de las finanzas tradicionales, pero las trata de hacer más eficientes e innovadoras. Las propuestas operan con dinero fíat —real o digital— y no guardan relación directa con las múltiples criptomonedas existentes, aunque sí incorporan las tecnologías de registros distribuidos (TRD) descritas en el anexo 4.

Más allá del liderazgo del BIS y del FMI para defender el sistema monetario y financiero tradicional —adoptando solo la tecnología que pueda ser útil para una mayor eficiencia—, es importante dar a conocer la posición de Christine Lagarde, quien preside el Banco Central Europeo. El 22 de mayo de 2022, en una entrevista con emisoras de los Países Bajos, dijo textualmente: «Mi humilde opinión es que las criptomonedas no valen nada, no se basan en nada, y no hay ningún activo subyacente que actúa como ancla de seguridad». De igual forma, solicitó su regulación, al advertir que muchas personas no entienden los riesgos implicados: «Lo perderán todo y se sentirán decepcionados». Lo que llama la atención es que, pese a estas advertencias, su hijo no siguiera sus consejos e invirtiera en criptomonedas, con resultados negativos, perdiendo una parte importante de sus inversiones.

Para terminar esta sección, se hace referencia al seminario titulado «El futuro de las finanzas», realizado el 14 de octubre de 2025 como parte del programa de las reuniones anuales del FMI y del Banco Mundial. Por un lado, participaron representantes de alto nivel del FMI (Kristalina Georgieva) y del Banco Mundial (Ajay Banga), así como el responsable de la autoridad monetaria de Singapur (Chia Der Jiun). Por otro, estuvieron presentes el codirector de pagos globales de J. P. Morgan (Umar Farooq) y el director de estrategia y operación de Circle (Jeremy Allaire). Todos coincidieron en que el futuro de las finanzas será digital; sin embargo, mientras los primeros subrayaron que continuará dominado por las monedas fíat, los segundos sostuvieron que estará basado en la tecnología de registros distribuidos en general y en las monedas estables que tienen como reserva las principales monedas fíat. De sus intervenciones se desprende que la colaboración pública y privada continuará con una estructura diferente a la actual, que incorpora innovaciones y, en algunos casos, la tecnología de registros distribuidos. Al final del evento, la moderadora pidió a los asistentes que levantaran la mano quienes fueran los propietarios de bitcoin, ether, alguna criptomoneda, mone-

da estable o CBDC. Lo curioso fue que los titulares del FMI y del BM dieron una respuesta positiva y el representante de J. P. Morgan una negativa.

(c) *Los abogados y expertos legales*. En el marco del mundo jurídico, los activos virtuales han sido objeto de miles —si no millones— de discusiones en foros académicos, legislativos y regulatorios desde el surgimiento de bitcoin. El primer punto controvertido lo encontramos en la propia definición de dinero. Ciertamente, esta pregunta no es novedosa en la historia monetaria y financiera del mundo, pero periódicamente se le han agregado elementos originales que invitan a la reflexión académica y, en algunas ocasiones, a la acción normativa y regulatoria.

La argumentación para considerar los términos moneda y dinero como sinónimos en el caso mexicano ya fue explicada en el tercer capítulo. En esta sección se agrega que, a pesar de que la Ley Fintech establece que los criptoactivos son medios de pago válidos para satisfacer obligaciones contractuales en contextos aislados, uno de los autores de este libro ha conversado con múltiples colegas —principalmente entusiastas— que sostienen que dichos activos deberían ser considerados medios de curso legal (en específico, bitcoin), sin entender el alcance completo del concepto. Algunos incluso han intentado promover amparos contra el artículo 28 constitucional y la Ley Monetaria de los Estados Unidos Mexicanos, con resultados no satisfactorios, como era de esperarse. Por tal motivo, puede afirmarse que existe un consenso en torno a que estos activos son medios de pago legalmente válidos para satisfacer obligaciones contractuales; algunos de ellos podrían, potencialmente, fungir como dinero en el marco de una comunidad con liquidez interna, mientras que, por el momento, ninguno puede ser considerado moneda perteneciente al agregado monetario M1.

En última instancia, México se rige por el derecho civil de tradición romana, heredado históricamente, en el cual las normas jurídicas son creadas principalmente por los legisladores, a diferencia de los países que usan el derecho común, como Reino Unido y Estados Unidos, donde los jueces, a través de la jurisprudencia, desempeñan un papel central en la creación de la mayoría de las normas legales.

En Estados Unidos, los economistas John G. Gurley y Edward S. Shaw expandieron la definición de dinero. En su libro *Dinero en la teoría de finanzas* (1960), partieron de la moneda fíat emitida por el banco central, a la que denominaron dinero externo, por proveer de liquidez exógena a la actividad económica en general. Posteriormente, en un segundo círculo concéntrico, incorporaron el dinero privado, con fuentes de liquidez en-

dógena, destinados a mercados específicos. Finalmente, en un tercer círculo, incluyeron todos los satisfactores contractuales o medios de pago. En resumen, hablan de los conceptos de moneda, dinero y medios de pago. Estos últimos incluyen todos los activos o pasivos presentes en el mercado que pueden actuar como un medio para satisfacer obligaciones contractuales, siempre que medie el consentimiento en transacciones aisladas. Tal es el caso mexicano de la tesis aislada publicada el viernes 15 de noviembre de 2019 en el *Semanario Judicial de la Federación*, emitida por el Tercer Tribunal Colegiado en Materia Civil del Primer Circuito, la cual establece con claridad:

> *La moneda extranjera puede contemplarse desde dos puntos de vista funcionales. Uno es como moneda propiamente dicha con el valor que le da la ley por conducto del Banco de México para generar el cumplimiento de derechos y obligaciones; y otro, como mercancía susceptible de ser intercambiada, al precio que libremente pacten las partes, supuesto en el cual se rige conforme a la regla del mercado (oferta y demanda). (Tesis I.3o.C.382 C [10a.])*

Con base en ello, el tribunal resolvió que las transferencias electrónicas interbancarias realizadas desde cuentas en moneda extranjera con destino a cuentas en moneda nacional debían ser entregadas en la moneda objeto de la transferencia. En términos técnicos, dispuso que en estas transferencias de fondos no se aplique el primer párrafo de la Ley Monetaria de los Estados Unidos Mexicanos, pero sí el tercer párrafo. Cabe señalar que una tesis aislada sirve de guía para que los jueces puedan realizar una mejor interpretación de cada caso, pero no adquiere el carácter de jurisprudencia sino hasta que se acumulen cinco casos votados por unanimidad o por resolución de la Suprema Corte de Justicia de la Nación.

En Inglaterra también se han llevado a cabo discusiones que giran en torno a si el dinero, en general, y el bitcoin, en particular, deben considerarse propiedad o encajar en una categoría distinta de las clasificaciones tradicionales planteadas por el jurista William Blackstone (1723-1780). Este autor distinguió los bienes personales entre las cosas en acción (*chose in action*) y las cosas en posesión (*chose in possession*). Las primeras corresponden a activos intangibles —como deudas, derechos de autor o paten-

tes— cuyos derechos pueden adquirirse en el futuro a través de una acción o demanda legal. Las segundas tratan de activos tangibles —como casas, vehículos o maquinaria— sobre las cuales se tiene posesión física y control absoluto. En términos generales, se es propietario de las primeras y tiene la posesión de las segundas. En la actualidad, estas clasificaciones tienden a superarse, y el análisis se orienta en buscar una respuesta adecuada en los derechos de propiedad intelectual. Los sistemas de propiedad de los países que se rigen por el derecho común son distintos de los que usan el derecho civil. Además, no solo existen diferencias entre los dos grupos, sino también variaciones al interior de cada uno de ellos.

(d) Las posiciones de *las autoridades fiscales* de los países o jurisdicciones están altamente correlacionadas con las listas del GAFI, así como con las evaluaciones del FMI y del BIS. Seguramente un alto porcentaje de las listas o de los centros financieros extraterritoriales o transfronterizos está compuesto por entidades en las que no se paga impuesto sobre la renta o se paga una tasa muy baja. México no tiene una lista de los antes denominados paraísos fiscales; sin embargo, esta puede inferirse a partir del artículo 176 de la Ley del Impuesto sobre la Renta, que obliga a los residentes mexicanos o del extranjero a pagar por los ingresos que obtengan en regímenes fiscales preferentes. Dichos regímenes se definen como aquellos en los que los ingresos no están gravados en el extranjero o lo están con un impuesto sobre la renta inferior al 75 % del que se pagaría en México.

En el caso de las criptomonedas, la mayoría de las plataformas tienen una licencia para operar de manera global en paraísos fiscales o centros financieros extraterritoriales; por ello, los residentes en México deben pagar impuestos sobre las ganancias de capital que deriven de operar en estos sitios web. Si lo hacen a través de plataformas electrónicas que están registradas ante el Sistema de Administración Tributaria, la Ley del Impuesto sobre la Renta establece implícitamente la obligación de pagar impuestos, aunque bajo un régimen diferente al del artículo 176.

Es importante distinguir entre las ganancias o pérdidas de capital derivadas de comprar y vender criptomonedas —que están regidas por el impuesto sobre la renta— y el impuesto al valor agregado que se tendría que pagar en el caso de que los activos virtuales se usen para pago de bienes y servicios. Al menos en teoría, también se tendría que pagar esta partida; no obstante, la realidad mexicana evidencia la falta de reglas claras para el pago de los impuestos. Esta situación, aunada a la complacencia regulatoria de las autoridades financieras, ofrece un panorama favorable

para los prestadores de servicios (plataformas), pero sumamente incierto para los usuarios de las criptomonedas.

En la práctica, la gran mayoría de los mexicanos involucrados en las criptomonedas no pagan ni el impuesto sobre la renta ni el impuesto al valor agregado. Los legisladores han evitado abordar estos temas, por lo que se recomienda a los inversionistas cumplir con sus pagos de impuestos utilizando las leyes vigentes, aun cuando parte de estas datan del siglo anterior.

(e) *Los legisladores* han tomado decisiones políticas divergentes. Algunos argumentan que fomentar la innovación tecnológica es más relevante que diseñar una nueva regulación para proteger los datos de los usuarios o consumidores. Un contraste evidente es el caso de la Unión Europea con sus reglamentos del mercado de criptoactivos (MiCA) y sobre las transferencias de dinero electrónico y de determinados criptoactivos, que han establecido reglas claras para su operación, siempre y cuando exista un establecimiento local que opere de manera fácil de autenticar (véase capítulo 3).

Estados Unidos inició con el liderazgo de las criptomonedas, pero lo perdió por falta de reglas claras y actualmente intenta recuperarlo. Mantiene sin actualizar la legislación de la década de 1930, y durante la administración del expresidente Biden se permitió que las autoridades reguladoras supervisaran el sector de las criptomonedas de una manera poco favorable. Esta situación cambió tras la segunda victoria electoral de Donald Trump. Tres días después de su toma de posesión, el 20 de enero de 2025, firmó la orden ejecutiva 14178, en la que propone estudiar la posibilidad de apoyar las cadenas de bloques públicas y descentralizadas, así como favorecer a las personas para que puedan tener custodia directa de sus activos digitales. La orden también contempla evaluar la creación potencial y el mantenimiento de un inventario nacional de activos digitales, que podrán derivarse de las criptomonedas legalmente decomisadas por el gobierno federal. La orden ejecutiva, titulada *Fortaleciendo el liderazgo de los Estados Unidos en la tecnología financiera digital*, dio a conocer la creación de un grupo de trabajo que entregó su reporte el 30 de julio de 2025. En él se destaca la promulgación, el 18 de julio, de la ley para regular las monedas estables (GENIUS Act). El reporte menciona que, para fortalecer aún más el papel del dólar estadounidense, se requiere que el Senado apruebe la propuesta que prohibiría la creación de una moneda digital del banco central para salvaguardar la privacidad de las personas (CBDC anti-surveillance state Act). En la misma situación se encuentra otra iniciativa (CLARITY Act), cuyo objetivo es dar cla-

ridad a los participantes del mercado para el registro de intermediarios, custodia de activos y negociación de las operaciones. Asimismo, se recomienda modernizar la regulación para permitir que los bancos comerciales accedan a los servicios derivados de la tecnología de registros distribuidos, así como establecer un marco actualizado para el combate al lavado de dinero y un procedimiento para el pago de impuestos accesible para el ecosistema de las finanzas descentralizadas. Finalmente, se propone que el inventario de activos digitales sea administrado por el Departamento del Tesoro, capitalizado con criptomonedas incautadas y que su custodia la definan conjuntamente los departamentos de Comercio y del Tesoro.

El mismo día en que se entregó el reporte del grupo presidencial de trabajo, el nuevo responsable de la Comisión de Valores y Bolsa, Paul S. Atkin, dio a conocer a los medios su proyecto cripto, en el que destacó que, pese a lo sostenido en el pasado, la mayoría de los activos cripto no son valores. Este segundo gobierno del presidente Trump ha cambiado radicalmente la forma y el fondo del espacio de las criptomonedas respecto del utilizado por el expresidente Biden.

Las dos leyes mencionadas (CBDC y CLARITY) ya fueron autorizadas por la Cámara de Representantes y ahora se encuentran en el Senado de los Estados Unidos para su discusión y votación. Lo más probable es que se tome una decisión en el transcurso de 2026.

(f) *El mundo de los contadores públicos* se encuentra hoy dividido entre aquellos adscritos al Consejo de Estándares de la Contabilidad Financiera (FASB, por sus siglas en inglés) y aquellos que siguen al Consejo de Estándares de la Contabilidad Internacional (IASB, por sus siglas en inglés). El primero se concentra en los principios de contabilidad generalmente aceptados, bajo el liderazgo de Estados Unidos (GAAP), mientras que el segundo se basa en normas de información contable (*international financial reporting standards*), aceptadas en aproximadamente 140 países.

México se adhirió al FASB hacia finales del siglo anterior; no obstante, a principios de este siglo cambió de enfoque y hoy sigue las normas del IASB. Para tal efecto, en 2002 se estableció el Consejo Mexicano de Normas de Información Financiera A. C., encargado de elaborar las reglas aplicables en el país.

En materia de criptomonedas, existe actualmente la Norma de Información Financiera C-22 (NIF C-22), que abre una nueva partida de los estados financieros para orientar el registro de operaciones con los activos virtuales. En contraste, el FASB ofrece reglas más amplias en el tema de las criptomonedas: en ciertos casos pueden registrarse como activos intan-

gibles; en otros, de manera similar a los inventarios, o incluso como activos financieros. En diciembre de 2023, el FASB emitió una actualización de sus estándares contables y anunció que, para el caso específico de los activos intangibles, publicará disposiciones más adelante.

Cuatro conjeturas

A diferencia de los pronósticos cualitativos y cuantitativos elaborados tanto por el BIS como por el FMI, los autores de este texto consideran que nadie sabe lo que nos depara el futuro. A pesar de ello, es posible formular algunas hipótesis.

• Las divisiones y la competencia entre reguladores e innovadores continuarán. Sin embargo, es un hecho que la parte tecnológica de las criptomonedas (TRD) puede ayudar a resolver algunos de los problemas asociados con la baja inclusión financiera, así como con la lentitud y el alto costo de las transferencias transfronterizas. Al mismo tiempo, consideramos que existirá una mayor regulación de los criptoactivos con el fin de proteger a los usuarios minoristas.

La tecnología de registros distribuidos (TRD) es útil, aunque no ha sido tan disruptiva como la inteligencia artificial generativa surgida en 2022, dentro de la cual tan solo ChatGPT registraba 900 millones de usuarios activos semanales en diciembre de 2025. Hoy existen pocas aplicaciones de la TRD más allá de todo lo relacionado con las finanzas descentralizadas que, como se mostró en la gráfica 2, alcanzaron un máximo de 27 millones de usuarios activos en mayo de 2025. Hay casos aplicables a otros temas, entre los que destacan los NFT para la tokenización de activos que están fuera de la cadena de bloques, el desarrollo de videojuegos, su aplicación en la operación del comercio internacional mediante sensores del internet de las cosas, la implementación en elecciones electrónicas, así como la utilización en los registros prediales y educativos.

• En el ámbito económico y financiero, las criptomonedas no han cumplido con sus promesas originales, ya que no han logrado desplazar ni a los bancos centrales ni a los intermediarios financieros formales. Aunque, en teoría, las redes son descentralizadas o distribuidas, en la práctica existen altos niveles de concentración en su gobernanza. Es decir, tenemos redes descentralizadas, pero con un poder distribuido de manera asimétrica. En definitiva, las criptomonedas y las finanzas descentralizadas han avanzado, pero el sistema tradicional seguirá siendo dominante y continuará

apropiándose de aquellos elementos que considere necesarios para volverse más lucrativo, eficiente e inclusivo, siempre operando con dinero fíat de manera física y digital.

Existen al menos dos ejemplos que ilustran el liderazgo del sistema financiero. Estados Unidos no solo ha autorizado el uso de ETF de bitcoin y ether, así como la ley que regula las monedas estables, sino que, además, el 7 de agosto de 2025 el presidente Trump firmó una orden ejecutiva para democratizar el acceso a las inversiones alternativas en los planes de ahorro para el retiro 401(k). Esta medida permitirá que más de 90 millones de personas puedan invertir en fondos de inversión privados, bienes raíces y activos digitales. Asimismo, se instruyó al Departamento de Trabajo y a la Comisión de Valores y Bolsa para que implementen esta decisión en los próximos seis meses. El impulso a la demanda de criptomonedas derivado de esta política podría ser mayor al de los ETF. Todo ello evidencia que el sistema financiero ha regulado y dominado el espacio de las criptomonedas, principalmente al trasladar una parte del negocio de las casas de intercambio centralizadas (CEX) a las instituciones financieras tradicionales en general.

En el caso de México, las autoridades han blindado al sistema financiero para impedir su operación con activos virtuales y, al mismo tiempo, han advertido a los inversionistas sobre los riesgos asociados. Esto ha derivado en una adopción modesta de las criptomonedas y en el predominio de las instituciones tradicionales. En otras palabras, se puede dominar con una adopción masiva —como ocurre en Estados Unidos— o se puede conservar el liderazgo del sistema financiero con murallas y advertencias para una baja adopción de las criptomonedas, como sucede en nuestro país. La gran interrogante es si el nuevo gobierno federal continuará con esta situación o la transformará. Los autores de este texto consideramos que no existirán cambios de postura en 2026.

• La web3, que mucha gente relaciona con el internet de la confianza o el internet de la propiedad, provocará algo muy similar a lo ocurrido con el internet de la información (web 2.0). Es decir, algunos intermediarios serán sustituidos por otros, lo que implicará diferentes niveles de centralización. A pesar de lo anterior, las aplicaciones financieras descentralizadas podrán constituir una primera etapa de la web3. En este contexto también participarán las organizaciones autónomas descentralizadas (DAO) y sus fichas de gobernanza. En cualquier escenario final se conservará la asociación público-privada. Como se mencionó en el capítulo 2, el concepto de la web3 difiere del de web 3.0, cuyo objeti-

vo es una red mundial menos centralizada con usuarios que puedan ser propietarios de sus activos.

• El *Panorama económico mundial* publicado por el Fondo Monetario Internacional en octubre de 2025 reporta 42 economías avanzadas a nivel global, de las cuales 20 forman parte de la eurozona. En ese mismo mes, el Banco Central Europeo anunció su intención de lanzar el euro digital para 2029, siempre y cuando la autoridad política —compuesta por el Eurogrupo y la Comisión Europea— decida darle su apoyo en 2026. Más allá de este caso, consideramos que serán escasos los ejemplos, entre las 22 economías avanzadas restantes, en los que las monedas digitales de sus bancos centrales (CBDC) puedan servir como anclaje para incorporar algunas de las diferentes formas de la tecnología de registros distribuidos con el uso de tókenes. Numerosos países han evaluado los costos y beneficios de implementar CBDC, y todo indica que los primeros superan a los segundos, especialmente por las preocupaciones relacionadas con la ciberseguridad.

Las monedas estables pueden competir o coexistir con las CBDC. Consideramos que, en la mayoría de los casos, coexistirán, ya que cada una de ellas encontrará su segmento de mercado o casos de uso específicos. Las monedas estables siempre serán emitidas en cadenas de bloques (*on-chain*), a diferencia de las monedas digitales de los bancos centrales (CBDC) en su versión de mayoreo, que no necesariamente se tienen que emitir en cadenas de bloques públicas.

Una recomendación

Más y mejor educación en TradFi, DeFi y CeFi para que usted pueda decidir de manera racional. Los temas relacionados con la moneda fíat y los servicios financieros —ahorros, inversiones y deuda— son interdisciplinarios u horizontales y nos afectan a lo largo de la vida. Por ello, cuanto más temprano se adquiera educación monetaria y financiera, mejores serán los resultados.

Es importante iniciar señalando que los conceptos de educación y alfabetización están correlacionados y que diversas autoridades e investigadores los consideran sinónimos. Tal es el caso de la OCDE, de la CNBV y del INEGI, que los utilizan de manera intercambiable en los resultados que presentan cada tres años en la Encuesta Nacional de Inclusión Financiera (ENIF). Sin embargo, existen diferentes definiciones oficiales de lo que se

entiende por educación financiera como las propuestas por Banxico, el Comité de Educación Financiera (CEF) y la de la Secretaría de Educación Pública (SEP).

Para los autores de este manuscrito es importante hacer la distinción, ya que la educación se asocia con la creación —usando el método científico— y la difusión del conocimiento —a través de la pedagogía y docencia— con el fin de formar alumnos y profesionistas en escuelas y universidades. La alfabetización, en cambio, suele desarrollarse fuera de estos ámbitos institucionales y se concentra tanto en la provisión de información como en el desarrollo de competencias y habilidades prácticas. La educación financiera en nuestro país es responsabilidad directa o indirecta del gobierno federal y de las autoridades estatales, mientras que la alfabetización financiera es responsabilidad primaria del sector privado.

En lo que respecta a la educación en finanzas formales o tradicionales (TradFi), los gobiernos federales van y vienen con diferentes ideologías y perspectivas; sin embargo, actualmente en México la educación financiera no existe para la educación primaria. A pesar de lo anterior, muchos consideramos que niñas y niños deberían adquirir sus primeros conocimientos en los asuntos relacionados con el dinero desde el nivel básico. Para lograrlo, se necesitaría de voluntad política al más alto nivel, así como una adecuada coordinación entre las autoridades educativas, monetarias, los supervisores financieros y las familias. Habría un conflicto de interés si se utilizaran documentos elaborados por instituciones financieras privadas con fines de lucro en escuelas primarias, secundarias y de bachillerato. El Banco de México, nuestro banco central, ha declarado que este tema no se encuentra en sus mandatos, por lo que no tienen una justificación legal para destinar recursos a una actividad no contemplada en su ordenamiento jurídico. Aun así, mantiene una sección dedicada a educación (educa.banxico.org.mx), cuyo contenido no es suficiente para un curso académico.

Una señal alentadora se mencionó durante la 17ª Semana de la Educación Financiera en México, celebrada el 5 de septiembre de 2024. En su inauguración, el presidente de la Condusef, Oscar Rosado Jiménez, señaló que una educación financiera a lo largo de la vida requiere de la participación de las personas, la familia, el gobierno, el sistema financiero y las universidades públicas y privadas. Al referirse al tercer actor, explicó:

el gobierno tiene la asignatura pendiente para la otra administración, de sí o sí, incluir contenidos de educación financiera en la educación básica; pero los gobiernos tienen sus tiempos y sus dinámicas. Aquí hay otros responsables desde las áreas públicas y de la educación privada.

Para el tema de las universidades públicas y privadas, recomendó incorporar las ciencias del comportamiento y la psicología en sus cursos de finanzas. Además, destacó que la Condusef, en colaboración con el Tecnológico Nacional de México, lanzó el curso titulado «Educación financiera: construye tu futuro financiero». Este curso no solo está disponible para los más de 568,000 estudiantes de dicho instituto en sus 248 planteles, sino también a través de un curso masivo abierto en línea (MOOC), accesible para cualquier joven interesado en desarrollar habilidades financieras. Se imparte desde 2022, tiene una duración de 40 horas cubiertas en ocho semanas, no tiene prerrequisito y aborda diez temas, entre ellos el sistema financiero mexicano, presupuestos, ahorros, créditos, inversiones, seguros y tecnología financiera. Es gratuito y quienes lo concluyen satisfactoriamente obtienen una constancia emitida por el Tecnológico Nacional de México.

Cabe mencionar también que la Condusef lanzó el 6 de febrero de 2024 un sitio de educación financiera para niñas, niños, jóvenes y adolescentes. El sitio web, denominado «Escuadrón billete», cuenta con nueve secciones que, mediante juegos y actividades divertidas, ayudan a entender temas como el ahorro, el crédito y los fraudes financieros. Los videos, audios y cuentos pueden ser encontrados en la página webappsos.condusef.gob.mx/escuadronbillete/home.html.

Durante el cierre de la 17ª Semana de Educación Financiera, el exsubsecretario de Hacienda y Crédito Público, Gabriel Yorio, mencionó dos proyectos que han desarrollado en colaboración con la CAF-Banco de Desarrollo de América Latina y el Caribe. El primero consiste en un repositorio digital que centraliza todos los contenidos educativos financieros disponibles, para que todas las personas puedan acceder al mismo desde cualquier lugar. El segundo es una plataforma de aprendizaje en línea dirigida a estudiantes de primaria y secundaria, con el objetivo de que las generaciones más jóvenes adquieran, desde temprana edad, las habilidades necesarias para gestionar sus finanzas.

La inauguración de la 18ª Semana de Educación Financiera tuvo lugar el 23 de octubre de 2025, con la participación inicial del presidente de la Condusef, Oscar Rosado Jiménez. En su discurso señaló:

> *durante años se habló de la educación financiera como un tema académico exclusivamente. Hoy sabemos que esto es notoriamente insuficiente, por lo que realmente importa es cómo logramos que las personas vivan con menos preocupaciones por el dinero.*

Con una mirada prospectiva, utilizó la frase: «La educación financiera será conductual o no será». Afortunadamente, aclaró que estas afirmaciones las hacía a título personal y no como una postura institucional de la Condusef. El cierre del evento estuvo a cargo de la nueva subsecretaria de Hacienda y Crédito Público, María del Carmen Bonilla Rodríguez, quien recordó que la Condusef mantiene hoy un enfoque más práctico, aunque subrayó que el Comité de la Educación Financiera (CEF), coordinado por la SHCP, es el ente responsable de coordinar los esfuerzos de los sectores público, privado y educativo. La subsecretaria acertó en esta apreciación, por lo que es importante compartir los antecedentes del CEF.

El CEF fue creado por la SHCP en mayo de 2011 como un grupo de coordinación de las políticas públicas en materia de educación financiera. En el año 2014 quedó formalizado en la Ley para Regular las Agrupaciones Financieras, donde se le asignó realizar la Estrategia Nacional de Educación Financiera (ENEF), con el fin de evitar la duplicidad de esfuerzos y propiciar la maximización de recursos (artículos 188-192). Así, en 2017 se elaboró la primera ENEF, cuya principal línea de acción consistía en «fomentar el desarrollo de competencias financieras en la educación obligatoria, desde edades tempranas». Dicha estrategia contenía indicadores de seguimiento y un calendario para los próximos cuatro años. Desafortunadamente, el gobierno federal del periodo 2018 a 2024 no la asumió como propia y solo incrustó una parte mínima dentro de su Política Nacional de Inclusión Financiera (PNIF).

Una noticia relevante fue dada a conocer por la SHCP del nuevo gobierno el 18 de diciembre de 2025, cuando presentó la ENEF 2025-2030, estructurada en seis objetivos estratégicos. En este texto solo nos enfocamos en dos de ellos. El primero tiene como propósito impulsar la educación finan-

ciera en el sistema escolarizado y no escolarizado. En este sentido, la Secretaría de Educación Pública concibe y define la educación financiera como un proceso pedagógico formativo y gradual, alineado con los principios de la Nueva Escuela Mexicana. Este objetivo contempla cinco líneas de acción e identifica a las instancias responsables de cada una. La Subsecretaría de Educación Básica de la SEP (SEB) es responsable de los libros de texto gratuitos y de la generación de sinergias con otros programas federales. La Subsecretaría de Educación Media Superior de la SEP (SEMS) debe incorporar contenidos en los libros usados en esos niveles. Al Banco de México le corresponde ampliar los materiales creados para los grados tercero, sexto y noveno, tanto para estudiantes como para docentes. Por su parte, la Condusef debe elaborar los contenidos y plataformas para comunidades indígenas.

El segundo objetivo estratégico busca desarrollar y fomentar las capacidades financieras, incluidas las digitales. Una de sus líneas de acción consiste en promover la formación de facilitadores y del personal operativo en educación financiera, considerando especializaciones como el sector agroalimentario, los emprendedores y las pequeñas empresas. En todo este proceso son responsables la Unidad de Banca, Valores y Ahorro (UBVA) de la SHCP, la Condusef, los Fideicomisos Instituidos en Relación con la Agricultura (Fira) y Nacional Financiera (Nafin).

Consideramos de gran relevancia que se haya retomado esta iniciativa y que, para los próximos cinco años, tengamos una ENEF que esté complementada con la PNIF. Daremos seguimiento a estas estrategias con la expectativa de que en esta ocasión sí se cumplan sus objetivos. Mientras tanto, existe suficiente material para estructurar diversos cursos de primaria relacionados con la moneda y las finanzas. El problema actual ya no radica en la falta de contenidos —que pueden cubrirse con los repositorios y herramientas antes mencionados del Banco de México, de la Condusef y la SHCP—, sino en los obstáculos institucionales que han existido en la SEP. Todo indica que, en el pasado, esta dependencia no había aceptado que la SHCP fungiera como coordinadora del Comité de Educación Financiera (CEF).

El plan muestra que la situación actual es diferente, como lo evidencian también los trabajos de otras áreas de la SEP. Se menciona, por ejemplo, el caso de la Subsecretaría de Educación Superior en la conferencia matutina de la presidenta Claudia Sheinbaum del 21 de noviembre de 2025, en la que, junto con su titular, se presentó el proyecto Saberes MX (saberes.gob.mx). Se trata de una plataforma pública, gratuita y abierta a

todas las personas mayores de edad. Se presenta como una plataforma de plataformas, ya que mediante el uso de interfaces de programación de aplicaciones informáticas (API) se conecta con los cursos que ofrecen las universidades de nuestro país. Las personas interesadas deben registrarse, obtener una contraseña y, posteriormente, seleccionar el curso deseado e inscribirse. Veremos si esta plataforma puede utilizarse para la educación financiera a través de certificaciones, cursos cortos o microcredenciales acumulables.

Reiteramos que no se considera oportuno usar los materiales de alfabetización que hacen las instituciones financieras, los cuales suelen estar dirigidos a sectores específicos —como las mujeres o personas adultas mayores— bajo el argumento de mejorar su cultura financiera y calidad de vida. Si se pretende complementar la educación con alfabetización, sería preferible utilizar los documentos producidos por asociaciones como la Asociación de Bancos de México (ABM), la Asociación Mexicana de Instituciones Bursátiles (AMIB), la Asociación Mexicana de Administradoras de Fondos para el Retiro (Amafore) y la Asociación Mexicana de Instituciones de Seguros (AMIS).

En lo que respecta a la educación relacionada con las finanzas descentralizadas, se deben incluir los dos puntos de vista que actualmente coexisten en el tema. Por un lado, están los desarrolladores originales de las cadenas de bloques; por otro, la posición de las autoridades de cada país. Esto sucede en prácticamente todos los países, aunque algunos, como El Salvador, tuvieron que capacitar a miles de funcionarios en estos temas. En Argentina, debido a inflaciones severas, se ha recurrido al uso de criptomonedas, y en la provincia de Buenos Aires ya se imparten contenidos sobre cadenas de bloques en Ethereum en el bachillerato.

En México, la versión oficial de las autoridades está documentada en la página web de Banxico (banxico.org). En dicho portal se podrá encontrar la definición de los activos virtuales, sus características generales, origen, funcionamiento y tratamiento internacional, así como su posicionamiento compartido por la SHCP y la CBNV.

La posición de quienes buscan utilizar las criptomonedas para prescindir, al menos parcialmente, de los intermediarios monetarios y financieros puede encontrarse en los libros blancos de los principales proyectos listados en la tabla 4 o en documentos elaborados por consultores (como *Chainalysis*) o libros escritos por administradores de fondos (*Crypto decrypted*, 2023), inversionistas (*Investing in cryptocurrencies and digital assets*, 2024),

profesores (*Todo vuelve a cambiar*, 2023), o una combinación de ellos (*DeFi and the future of finance*, 2021).

Se recomienda al lector acercarse a las nuevas revistas académicas relacionadas con las cadenas de bloques y evitar los materiales difundidos por un gran número de personas influyentes (*influencers*) en redes sociales. Actualmente existen diplomados, licenciaturas y maestrías en diversas universidades; destaca la Universidad de Nicosia (UNIC), en Chipre, pionera en la materia y que ofrece también varios MOOC de manera gratuita.

En 2024, el Instituto Mexicano de Contadores Públicos (IMCP) publicó el libro *Criptoactivos: aspectos financieros, contables, fiscales y de PLD*. Esta obra está dirigida principalmente a contadoras y contadores mexicanos y constituye una excelente guía en materia de contabilidad de los criptoactivos, así como en el tratamiento fiscal de las operaciones realizadas con estos activos. Sin embargo, en los temas relativos a las finanzas descentralizadas y a la prevención de lavado de dinero (PLD) presenta deficiencias: carece de contextualización, confunde términos informáticos, utiliza datos desactualizados y no da a conocer la recomendación del GAFI incumplida por México. A pesar de lo anterior, y limitando los temas a los aspectos contables y fiscales, puede considerarse un complemento útil del presente texto. Quien quiera diseñar e impartir un curso completo de activos virtuales para enseñar en programas de licenciaturas en México, debería incluir los dos libros como parte fundamental de la bibliografía.

Existen otros académicos que se concentran en organizar cursos relacionados únicamente con la tecnología de registros distribuidos, generalmente ingenieros en computación que dejan deliberadamente de lado el tema de las criptomonedas para concentrarse en las cadenas de bloques. La Iniciativa del Inventario de Estándares Globales del Consejo Global de Negocios de la Cadena de Bloques publica periódicamente los cursos relacionados con las cadenas de bloques que ofrecen las instituciones educativas acreditadas en gran parte del mundo. En su quinta edición, de diciembre de 2024, publicó un repositorio de 1,575 cursos para ayudar a los profesores e investigadores a compartir el conocimiento. La mayoría de los cursos están enfocados en programas de licenciatura y se concentran en el área de ingeniería, específicamente en la licenciatura de Ciencias de la Computación. Para el caso de México, aparecen 14 cursos relacionados con la cadena de bloques impartidos en diversas instituciones, entre las que se encuentran la UNAM, el ITESM, la UAM y el IPN. En esta plataforma se puede acceder a los contenidos de materia o a información relevante para su registro.

En menor cantidad también se ofrecen cursos de posgrado, así como diplomados y certificados profesionales.

La Organización Internacional de las Comisiones de Valores (IOSCO, por siglas en inglés) con sede en Madrid y conformada por 133 miembros ordinarios, publicó en 2024 un reporte sobre la educación del inversionista en criptoactivos. Se trata de un documento de alto valor académico, basado en experiencias internacionales y encuestas a usuarios. Destaca que una proporción significativa de inversionistas obtiene información para invertir en esta clase de activos virtuales especulativos a través de amistades, personas influyentes o celebridades remuneradas que se dedican a promover y explicar el funcionamiento de estos espacios en redes sociales. La mayoría carece de formación adecuada y no verifican si las plataformas cuentan con licencia de las autoridades. El informe ofrece también tanto material de estudio como recomendaciones para decidir si su perfil es adecuado para este tipo de inversiones especulativas.

También es importante mencionar que la Organización de Cooperación y Desarrollo Económicos (OCDE), con sede en París, creó en 2008 la Red Internacional de Educación Financiera (INFE, por sus siglas en inglés), integrada por 130 economías, con el objetivo de facilitar la cooperación entre las autoridades políticas y otras partes interesadas en el tema. Su enfoque principal ha sido la alfabetización financiera, como se puede deducir de la Encuesta Nacional de Inclusión Financiera (ENIF) 2025, presentada por la CNBV en colaboración con el INEGI. En ella, el concepto de educación financiera se relaciona con el índice de alfabetización financiera (o índice de competencias económico-financieras), obtenido a partir de 21 preguntas aplicadas a personas de 18 años y más. Este índice se compone, por un lado, de conocimientos (comprensión básica de conceptos financieros); es en este punto en el que existe confusión, ya que los consideran como sinónimo de su educación financiera. Por otro, los comportamientos (evitar el estrés) y las actitudes (hacia el dinero y la planificación). La ENIF 2025 muestra que el índice de alfabetización en México es del 58 %, cifra que no ha cambiado desde 2018. Si bien los reportes de la OCDE son válidos y aportan insumos importantes para los cursos de educación financiera en las primarias en México y para la alfabetización financiera de los adultos, lo primero debería planteare como una meta a largo plazo y lo segundo, a corto plazo.

En el caso de las finanzas centralizadas (CeFi), la educación debería alinearse con el principio «misma actividad, mismos riesgos, mismas normas». Esto debe combinarse con el reconocimiento de que las tecnologías son neutrales y que pueden usarse tanto para fines legítimos como ilícitos.

Así, las reglas de las finanzas centralizadas deberán ser similares a las de las finanzas tradicionales, regulando funciones más que instrumentos, instituciones o plataformas.

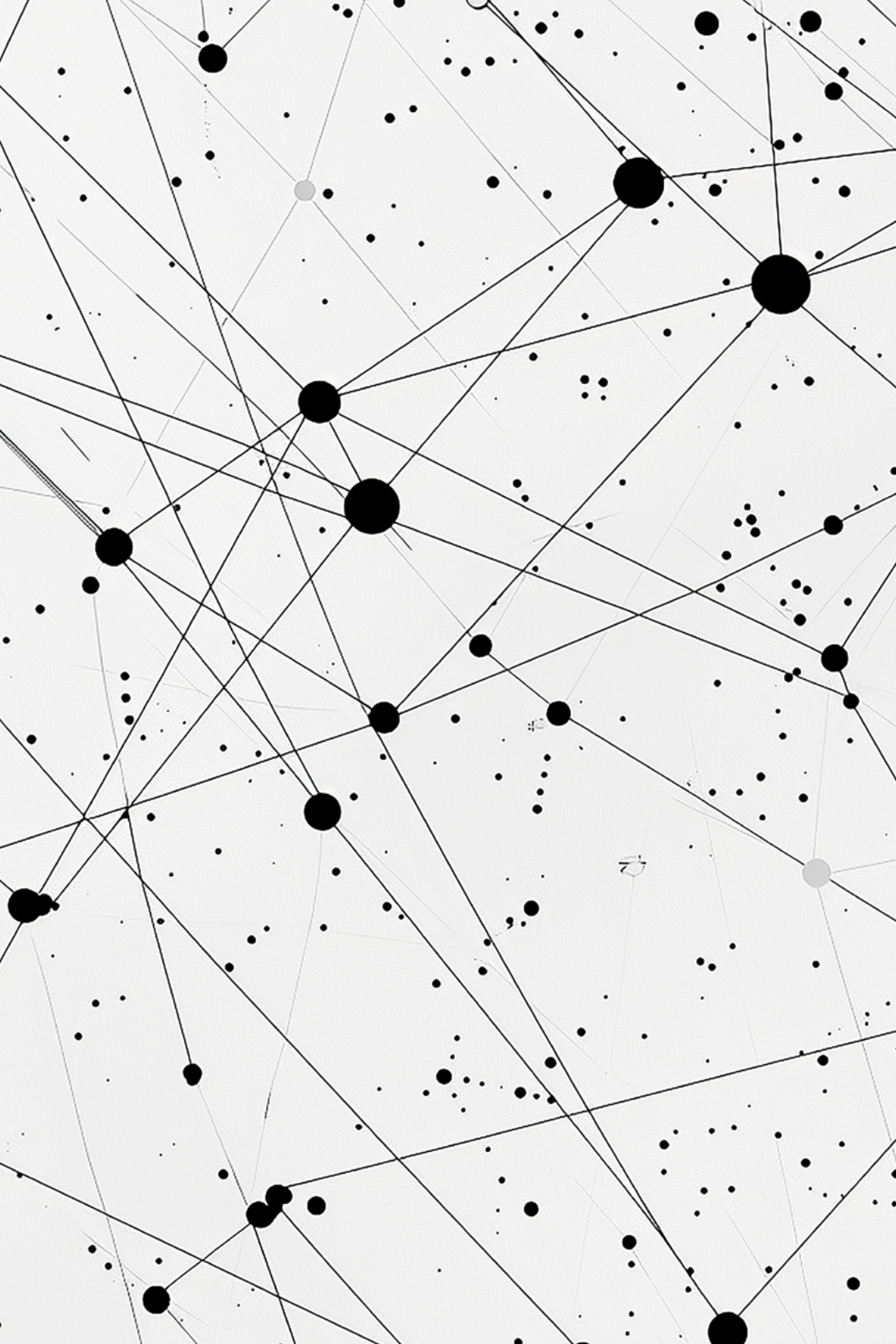
Este texto concede prioridad a la educación financiera y subraya la importancia de promoverla desde las escuelas primarias hasta la educación superior. En este último nivel, es pertinente recordar lo expuesto por José Ortega y Gasset en *Misión de la universidad* (1930), donde señala tres funciones: (a) la enseñanza de las profesiones intelectuales, (b) la investigación científica, así como la preparación de futuros investigadores, y (c) la transmisión de la cultura general referida al espíritu humano. Estos principios siguen vigentes en 2025, aunque es necesario incorporar, con las debidas cautelas, el uso de internet, la inteligencia artificial generativa y las tecnologías de registros distribuidos.

La aplicación de estas funciones en las instituciones privadas de educación superior en México puede entenderse como un convenio social con estudiantes, padres de familia y la sociedad. Este compromiso adquiere relevancia en un entorno donde, cada vez con mayor frecuencia, la educación superior se concibe como una transacción comercial y las universidades se asumen como empresas con fines de lucro y, además, los alumnos se convierten en sus clientes.

Desde hace varias décadas, los autores de este manuscrito han contribuido con materiales orientados a esta tarea. En 2013, uno de ellos publicó *Finanzas: vestidas por unos y alborotadas por otros*, donde advertía que «el problema al que nos enfrentamos los estudiosos de las finanzas es que nos concentramos en el sistema formal, aun cuando el sistema en la sombra es mucho más grande, y al mismo tiempo mucho menos transparente» (Hakim, p. 342). Esta reflexión sigue siendo válida en 2025, aunque hoy resulta imprescindible incorporar el estudio de las finanzas centralizadas y las descentralizadas, aun reconociendo su menor peso relativo frente al sistema formal. Ello ha vuelto la disciplina más compleja e interesante, tanto para la teoría como para la práctica.

Esta sección concluye enfatizando la relevancia de la educación financiera a partir de la reflexión del educador venezolano Simón Rodríguez (1769-1854): «Al que no sabe, cualquiera lo engaña». No obstante, la educación y la alfabetización financiera son condiciones necesarias, pero no suficientes. Tanto en las finanzas tradicionales como en los ecosistemas cripto (centralizados y descentralizados) resulta indispensable la protección de las personas usuarias, especialmente de los pequeños inversionistas o de menudeo. En el sistema formal, esta protección se ejerce a través

de instituciones como el IPAB, la CNBV, la CNSF, la Consar y la Condusef. Estas entidades regulan y supervisan el sistema financiero con el propósito de lograr un equilibrio entre la seguridad y la innovación. Asimismo, supervisan a los prestadores de servicios y, en última instancia, aplican las leyes correspondientes. En contraste, la protección de los usuarios en el sistema centralizado o descentralizado del espacio cripto se limita, en gran medida, al registro de las plataformas ante el SAT y su obligación de presentar avisos de operaciones relacionadas con el lavado de dinero y el financiamiento al terrorismo. Cabe señalar que el riesgo financiero en el sistema formal es menor que en el espacio de los criptoactivos, caracterizado por una alta volatilidad en los precios, ya sea derivada de las dinámicas del mercado o de posibles manipulaciones. No obstante, este entorno también conlleva riesgos no financieros (legales, técnicos y operativos) cuya cuantificación resulta compleja. El usuario es libre de decidir si utiliza una de las tres opciones o las combina según sus necesidades. En cualquier escenario, la educación financiera es una condición necesaria; por ello, se espera que este texto haya resultado de utilidad.



Epílogo

La evolución de la gobernanza que da forma al mercado de las criptomonedas (activos virtuales o criptoactivos) en México inició en 2014 a partir de las múltiples advertencias emitidas por las autoridades monetarias y financieras de nuestro país. Continuó en 2018 con la entrada en vigor de la Ley para Regular las Instituciones de Tecnología Financiera (Fintech) que blinda a las instituciones del sistema financiero de realizar operaciones con criptomonedas, pero deja abierta la posibilidad de otorgar a otras empresas autorizaciones temporales para que, mediante modelos novedosos, lleven a cabo actividades con dichos activos. Sin embargo, hasta el mes de abril de 2026, el Banco de México (Banxico) junto con la Comisión Nacional Bancaria y de Valores (CNBV) no han expedido autorización alguna de esta naturaleza. En armonía con dichos esfuerzos, en 2018 se realizaron modificaciones a la Ley Federal para la Prevención e Identificación de Operaciones con Recursos de Procedencia Ilícita (Antilavado) que desde entonces considera el tratamiento de activos virtuales como una actividad vulnerable.

A pesar de lo anterior, los «inversionistas al menudeo» mexicanos pueden acceder a este mercado compuesto por criptomonedas, monedas estables, acciones, fondos cotizados en bolsa y otras opciones a través de tres canales:

(1) Intermediarios que están establecidos en México y se encuentran regulados y supervisados de manera integral por la CNBV. Tal es el caso del Grupo Bursátil Mexicano (GBM), que posee el liderazgo de «contratos de intermediación» bursátil o cuentas de inversión.

(2) Mediante una plataforma informática que tiene licencia en alguno de los países o jurisdicciones extraterritoriales (*off-shore*) y está registrada ante el Sistema de Administración Tributaria (SAT) de México. El número y nombre de estas plataformas no es del conocimiento público debido a que el SAT y otras autoridades consideran que se trata de «información clasificada». Sin embargo, casi todos conocemos sus nombres: Bitso y Binance, entre otras. Algunas de estas empresas han complementado su operación en México con el establecimiento de instituciones de fondos de pago electrónico (IFPE) autorizadas por Banxico y la CNBV, como Nvio y Medá.

(3) Otras plataformas con licencia del exterior que no tienen registro en México y operan a través del internet o de alguna aplicación informática (por ejemplo, Uniswap y 1Inch).

Las dos primeras opciones, al menos en teoría, cumplen con la recomendación 16 del Grupo de Acción Financiera Internacional (GAFI) que exige que los intermediarios identifiquen plenamente quién envía y quién recibe las transferencias electrónicas de fondos, que es conocida coloquialmente como la «regla del viajero». La tercera opción se refiere a operaciones entre pares que funcionan de manera cuasi anónima en internet, por lo que es casi imposible seguir la regla del viajero y generan problemas de jurisdicción.

Los autores de este volumen consideran que existe una enorme indefinición de las autoridades mexicanas, así como una gran complacencia. En el cierre de la Semana Fintech de 2023, el exsubsecretario de Hacienda y Crédito Público Gabriel Yorio comentó:

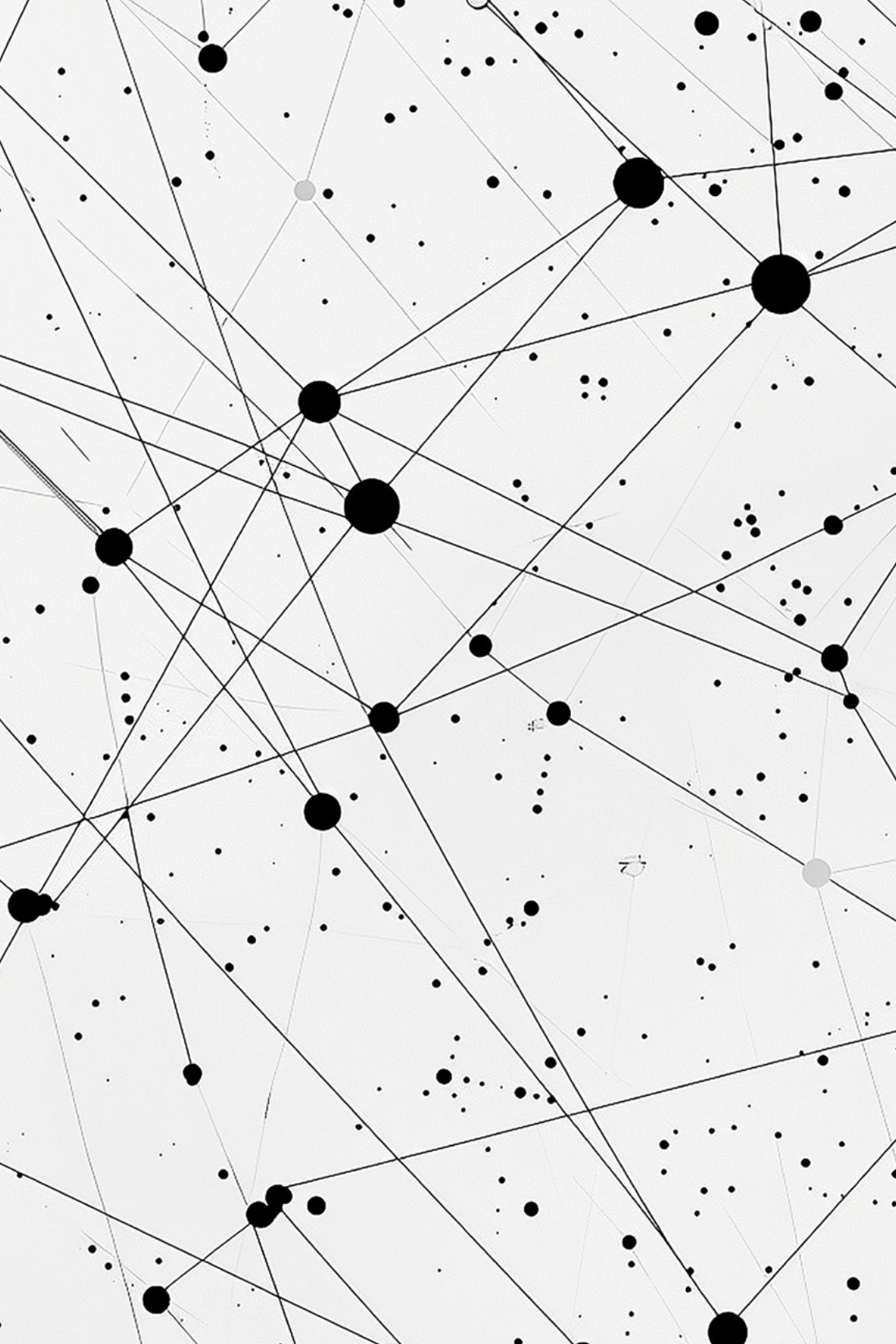
> *México ya tiene actualmente operando en la jurisdicción algún tipo de criptoactivos, pero no tenemos todavía una regulación clara, ni una definición de qué vamos a hacer con respecto a estos activos. Entonces, creo que, en el grupo de innovación financiera, tal vez pueda ser un muy buen espacio para pensar, y en algún momento definir entre autoridades y gremio qué vamos a hacer con los criptoactivos. O los prohibimos o los regulamos, pero ya tenemos que tomar una decisión.*

Hoy, Gabriel Yorio es el vicepresidente de Finanzas y Administración del Banco Interamericano de Desarrollo (BID) con sede en Washington D. C., y no ha existido definición alguna de este nuevo Gobierno federal. Así lo demuestran los discursos de la gobernadora de Banxico y del secretario de Hacienda y Crédito Público en la 89 Convención Bancaria de ABM celebrada en Cancún entre el 18 y el 20 de marzo de 2026, en donde no hubo una sola mención a los activos virtuales.

En el contexto global resaltan los casos de China, que ha prohibido el uso de criptomonedas, pero ya experimenta con el yuan digital diseñado y probado por su banco central (e-CNY), y la Unión Europea, que cuenta con reglas claras a nivel normativo y judicial para la operación de criptoactivos y sus proveedores, garantizando la neutralidad tecnológica, es decir, no regula la tecnología subyacente de los activos virtuales, sino sus aplicaciones o actividades. Finalmente, Estados Unidos (nuestro vecino del norte) em-

pezará a usar muy pronto un marco preciso para el espacio de las monedas estables con reservas en dólares estadounidenses a través de su GENIUS Act, y El Salvador (un país cercano del sur) ha dejado de usar el bitcoin como moneda de curso legal, pero mantiene una regulación amigable para el desarrollo de las criptomonedas.

Para el caso de México, los autores de este libro sostienen la hipótesis de que ni los activos virtuales ni su tecnología subyacente serán prohibidos por las autoridades, como se verifica en el régimen introducido en el marco de los últimos dos años para los certificados de los almacenes generales de depósito y la legislación general en materia de títulos de crédito, pero tampoco serán regulados de manera integral en los dos próximos años, por lo que se mantendrá la situación actual de indefinición y complacencia. Todo esto tiene ventajas y desventajas que solo pueden ser entendidas con más y mejor educación financiera, tanto acerca de los activos virtuales como del sistema tradicional.



Referencias

Agenda Financiera. (2025). *Compendio de disposiciones bancarias, bursátiles y financieras*. Editorial ISEF.

Allen, H. J. (2022). *DeFi: Shadow banking 2.0?* Washington College of Law Research Paper No. 2022-2. American University.

Aloosh, A. y Li, J. (2024). Direct evidence of bitcoin wash trading. *Management Science*, 70(12), 8875-8921.

Antonopoulos, A. M. (2014). *Mastering bitcoin. Unlocking digital cryptocurrencies*. O´Reilly.

Antonopoulos, A. M. y Wood, G. (2018). *Mastering ethereum. Building smart contracts and DApps.* O´Reilly.

Aramonte, S., Huang W. y Schrimp, A. (2021). DeFi risk and the decentralization illusion. *BIS Quartely Review*, 21-36.

Auer, R., Haslhofer, B., Kitzler, S., Saggese, P. y Victor, F. (2023). *The technology of decentralized finance (DeFi)* (*BIS* Working Papers No. 1066). Bank for International Settlements.

Aurazo, J., Franco, C., Frost, J. y McIntosh, J. (2025). Fast payments and financial inclusion in Latin America and the Caribbean. *BIS Papers*, 153.

Banco de México. (2000). *Circular 37/2000. Modificaciones a la circular 4/2019.*

Banco de México. *(2019). Circular 4/2019. Disposiciones de carácter general aplicables a las instituciones de crédito e instituciones de tecnología financiera en las operaciones que realicen con activos virtuales.*

Banco de México. (2021a). *Informe anual sobre el ejercicio de las atribuciones conferidas por la Ley para la Transparencia y Ordenamiento de los Servicios Financieros: julio 2020 a junio 2021.*

Banco de México. (2021b). *Reporte de estabilidad financiera. Segundo semestre 2021.*

Banco de México. (2023). *Informe anual sobre el ejercicio de las atribuciones conferidas por la Ley para la Transparencia y Ordenamiento de los Servicios Financieros: julio 2021 a junio 2022.*

Banco de México. (2024a). *Informe anual sobre el ejercicio de las atribuciones conferidas por la Ley para la Transparencia y Ordenamiento de los Servicios Financieros: julio 2022 a junio 2023.*

Banco de México. (2024b). *Reporte de estabilidad financiera. Primer semestre 2024.*

Banco de México. (2025a). *Reporte de estabilidad financiera.*

Banco de México. (2025b). *Agregados monetarios y actividad financiera.*

Banco de México. (2025c). *Reporte de estabilidad financiera.*

Bank for International SettIements. (2022). Chapter III. The future monetary system. *En Annual economic report.*

Bank for International SettIements. (2023). Chapter III. Blueprint for the future monetary systems: improving the old, enabling the new. En *Annual economic report*.

Bank for International SettIements. (2024). Chapter III. Artificial intelligence and the economy: implications for central banks. En *Annual economic report*.

Bank for International Settlements Innovation Hub. (2023). *Project Atlas: Mapping the world of decentralized finance.*

Bank for International Settlements Innovation Hub y Federal Reserve Bank of New York. (2025). *Project Pine: Central bank open market operations with smart contracts.*

Baran, P. (1964). On distributed communications networks. *IEEE transactions on communication systems, 12*(1), 1-9. https://doi:10.1109/TCOM.1964.1088883

Berners-Lee, T. (2025). T*his is for everyone. The unfinished story of the world wide web*. Farrar, Starus and Giroux.

BID, BID Invest y Finnovista. (2024). *Fintech en América Latina y el Caribe. Un ecosistema consolidado con potencial para aportar a la inclusión financiera regional* (IV Informe).

Black, K. (2025). *Investing in cryptocurrencies and digital assets. A guide to understanding technologies, business models, due diligence, and valuation.* Wiley.

Born A., Gschossmann I., Hodbod A., Lamert C. y Pellicani A. (2022). Decentralized finance: a new unregulated non-bank system? ECB *Macroprudential bulletin.*

Buterin, V. (2014a) *DAOs, DACs, DAs, and more. An incomplete terminology guide.* Ethereum Foundation Blog.

Buterin, V. (2014b). *Ethereum: a next-generation smart contract and decentralized application platform.*

Carstens, A. (2018, 26 de septiembre). *Technology is no substitute for trust.* [Discurso]. Borsen-Zeitung.

Carstens, A. (2020). Shaping the future of payments. *BIS Quartely Review,* 17-20.

Carstens, A. (2022, 25 de octubre). *Digital currencies and the soul of money* [Discurso]. Goethe University, Frankfurt.

Carstens A. y Nilekani, N. (2024). *Finternet: the financial system for the future* (BIS Working Papers No. 1178). Bank for International Settlements.

Cecchetti, S. G. y Schoenholtz. K. L. (2019). Finance and blockchain. In A. Fatás (ed.), *The economics of fintech and digital currencies,* 7-13. CEPR Press.

Cedillo, I. (2024). *A socio-legal theory of money for the digital commercial society: A new analytical framework to understand cryptoassets.* Hart Publishing.

Center for Strategic and International Studies. (2025). *The ByBit heist and the future of U. S. crypto regulation.*

Chainalysis. (2022, junio). *The Chainalysis state of web3 report. Your guide to how blockchains are changing the internet.*

Chainalysis. (2023, julio). *The Chainalysis crypto myth busting report. 33 cryptocurrency myths refuted.*

Chainalysis. (2024, febrero). T*he 2024 crypto crime report. The latest trends in ransomware, scams, hacking, and more.*

Chainalysis. (2025, febrero). *The 2025 crypto crime report. The rising role of cryptocurrency in all forms of crime and how its transparency is creating unique opportunities for investigation.*

Comité de Educación Financiera. (2017, septiembre). *Estrategia Nacional de Educación Financiera (ENEF).*

Commodity Futures Trading Commission (CFTC). (2023). *CFTC Charges Binance and Its Founder, Changpeng Zhao, with Willful Evasion of Federal Law and Operating an Illegal Digital Asset Derivatives Exchange*. Press release number 8680-23. https://www.cftc.gov/PressRoom/PressReleases/8680-23

Cong, L., Li, X., Tang, K. y Yang Y. (2022, septiembre). *Crypto wash trading*. (NBER Working Paper No. 30783). National Bureau of Economic Research.

Dameron, M. (2019). *Beigepaper: An ethereum technical specification* (versión v0.8.5).

Dans, E. (2023). *Todo vuelve a cambiar: Cómo la web3 revolucionará el mundo tal y como lo conocemos* (edición Kindle). Deusto.

Diffie, W. y Hellman, M. E. (1976). New directions in cryptography. *IEEE Transactions on information theory*, 22(6).

Diario Oficial de la Unión Europea. (2023a, 9 de junio). Reglamento 2023/1113 del Parlamento Europeo y del Consejo, relativo a la transferencia de fondos y de determinados cripto-activos.

Diario Oficial de la Unión Europea. (2023b, 9 de junio). Reglamento 2023/1114 del Parlamento Europeo y del Consejo, relativo a los mercados de cripto-activos.

European Union Blockchain Observatory & Forum. (2022, mayo). *Decentralized Finance (DeFi).* A Thematic report.

Financial Stability Board. (2022, 21 de marzo). *Fintech and market structure in the Covid-19 pandemic.*

Financial Stability Board. (2023, 16 de febrero). *The financial stability risks of decentralized finance.*

Finnovista. (2024). *Fintech Radar México 2024.*

Forbes. (2025, agosto/septiembre). Crypto's second revolution.

Gandal N., Hamrick J. T., Moore, T. y Oberman, T. (2018). Price manipulation in the bitcoin ecosystem. *Journal of Monetary Economics, 95, 86-96.* Global Blockchain Business Council. (2024). *Global standards mapping initiative 5.0. Courses from accredited educational institutions.*

Gobierno de México, SHCP, SEP, Banxico, CNBV, CNSF, Consar e IPAB. (2025, 18 de diciembre). *Estrategia Nacional de Educación Financiera (ENEF) 2025-2030.*

Gurley, J. C. y Shaw, E. S. (1960). *Money in a theory of finance.* Brookings Institution.

Haber, S. y Stornetta, W. S. (1991). How to time-stamp a digital document. *Journal of Cryptology*, *3,* 99-111.

Hakim, M. (2013). *Finanzas: vestidas por unos y alborotadas por otros*. EDAF y UDLAP.

Harvey, C. R., Ramachandran, A. y Santoro J. (2021). *DeFi and the future of finance.* Wiley.

Horne, I. (2023). *Why DeFi matters. What cryptoassets, web3 and the metaverse really mean for finance.* Kogan Page.

INEGI y CNBV. (2025). *Encuesta Nacional de Inclusión Financiera (ENIF) 2025.*

Instituto Mexicano de Contadores Públicos. (2024, mayo). *Criptoactivos. Aspectos financieros, contables, fiscales y PLD* (1° ed.).

International Monetary Fund. (2016, enero). Virtual currencies and beyond: initial considerations. (Staff Discussion Note SDN/16/03).

International Monetary Fund. (2019, julio). *The rise of digital money*. Fintech Note/19/01. T. Adrian y T. Mancini-Griffoli (eds.).

International Monetary Fund. (2020, agosto). *United States: FSAP-financial system stability assessment.*

International Monetary Fund. (2021, octubre). Chapter 2. The crypto ecosystem and financial stability challenges. *Global financial stability report.*

International Monetary Fund. (2022, 4 de noviembre). *Mexico: FSAP-financial system stability assessment.*

International Monetary Fund. (2022). BigTech in financial services: Regulatory approaches and architecture (Fintech note 2022/002). Parma Bains, Nobayasu Sugimoto y Christipher Wilson (eds.).

International Monetary Fund. (2025, 23 de abril). *Tokenization and the financial system*: *Adapting to the new landscape* [video]. Spring Meeting.

International Monetary Fund. (2025, octubre). *Global financial stability report. Shifting ground beneath the calm.*

International Monetary Fund. (2025, 14 de octubre). *The future of finance* [video]. Seminar, October Meeting.

International Monetary Fund, Statistical Department. (2025). *Integrated balance of payments and international investment position manual (BPM7)* (White cover pre-edited version).

International Organization of Securities Commissions. (2024). *Investor education on crypto-asstes* (Final report).

La Jornada. (2025, 2 de septiembre). Sheinbaum garantiza autonomía del Banxico en revisión del sistema financiero. https://www.jornada.com.mx/noticia/2025/09/02/economia/sheinbaum-garantiza-autonomia-del-banxico-en-revision-del-sistema-financiero

Lessig, L. (1999). *Code: And other laws of cyberspace.* Basic Books.

Lessig, L. (2000). *Code is law: On Liberty in cyberspace.* Harvard Magazine.

Martins, R. (2024). Web3 *in financial services: How blockchain, digital assets and crypto are disrupting traditional finance.* Kogan Page.

Merkle, R. C. (1979, 5 de septiembre). United States patent documents. (U. S. Patento Application No. 72,363).

Nadler M. y Schar, F. (2020). *Decentralized finance, centralized ownership? An iterative mapping process to measure protocol token distribution.* https://doi.org/10.48550/arXiv.2012.09306

Nakamoto, S. (2008). *Bitcoin: a peer-to-peer electronic cash system.*

OECD. (2022). *Why decentralized finance (DeFi) matters and the policy implications.*

OECD/INFE. (2023). I*nternational survey of adult financial literacy.*

Ortega y Gasset, J. (2024). *Misión de la universidad* (3ª ed.). Ediciones Cátedra. (Trabajo original publicado en 1930).

Pogliani, P. y Wooldrige, P. (2022). *Cross-border financial centres* (BIS Working Papers No. 1035).

Quinto Elemento Lab. (2021, 3 de febrero). *El SAT despide a funcionario implicado en tolerar lavado de dinero en HSBC*. https://quintoelab.org/project/sat-despide-garcia-gibson-lavado-dinero-hsbc

Romero, J. L. (2018, 16 de octubre). Tecnología de registros distribuidos (DLT): una introducción. *Boletín Económico del Banco de España*, 4/2018.

Ronco, V. (2023). *Criptomonedas: La revolución de los activos digitales.* Deusto.

Ryan, J. y Diorio, J. (2023). *Crypto decrypted: Debunking myths, understanding breakthroughs, and building foundations for digital asset investing.* Wiley.

Salinas, R., Hugil, P. y Jungen, D. (2025). *The bitcoin enlightenment: Ending the fiat dark age.* The Saif House.

Schär, F. (2021). Decentralized finance. On blockchain-and smart contracts-based financial markets. *Federal Reserve Bank of St. Louis Review, 103*(2), 153-74.

Scientific American. (2025, primavera/Verano). Into the quantum realm. Special edition.

SHCP, CNBV, CNSF, Condusef, Consar, IPAB, Tesofe y Banxico. (2025, 26 de noviembre). *Política Nacional de Inclusión Financiera (PNIF) 2025-2030.* Consejo Nacional de Inclusión Financiera.

SHCP, CNBV e INEGI. (2022, 11 de mayo). Encuesta Nacional de Inclusión Financiera (ENIF) 2021 (Comunicado de prensa 256).

Silver, N. (2025). *Al límite: Conoce a jugadores de póquer, apostadores profesionales, cryptobros, genios del venture capital y otros personajes capaces de arriesgarlo todo y ganar*. Debate.

The Economist. (2025, 15 de mayo). *Crypto meets the swamp: Why it won´t end well.*

The White House. (2025, 23 de enero). *Strengthening american leadership in digital financial technology* (Executive order 14178).

The White House. (2025, 20 de julio). *White House digital assets report: Strengthening american leadership in digital financial technology. Recommendations of the President´s working group.*

Unidad de Inteligencia Financiera. (2025). *Informe de actividades: enero-junio 2025, enero-julio 2025, enero-agosto 2025, enero-septiembre 2025, enero- octubre 2025.* SHCP.

United Nations, International Monetary Fund, The World Bank Group, European Commission y Organisation for Economic Co-operation and Development. (2025, marzo). *System of national accounts* 2025 (Pre-edited version).

Wharton School. (2021, mayo). *DeFi beyond the hype. The emerging world of decentralized finance.* University of Pennsylvania.

Wood, G. (2022). Ethereum: *A secured decentralized generalized transaction ledger.*

World Bank Group. (2017). *Distributed ledger technology (DLT) and blockchain* (Fintech note No. 1).

World Economic Forum. (2020, diciembre). *Crypto, what is it good for? An overview of cryptocurrency use cases.*

World Economic Forum. (2021, junio). *Decentralized finance (DeFi) policy-maker toolkit* (White paper).

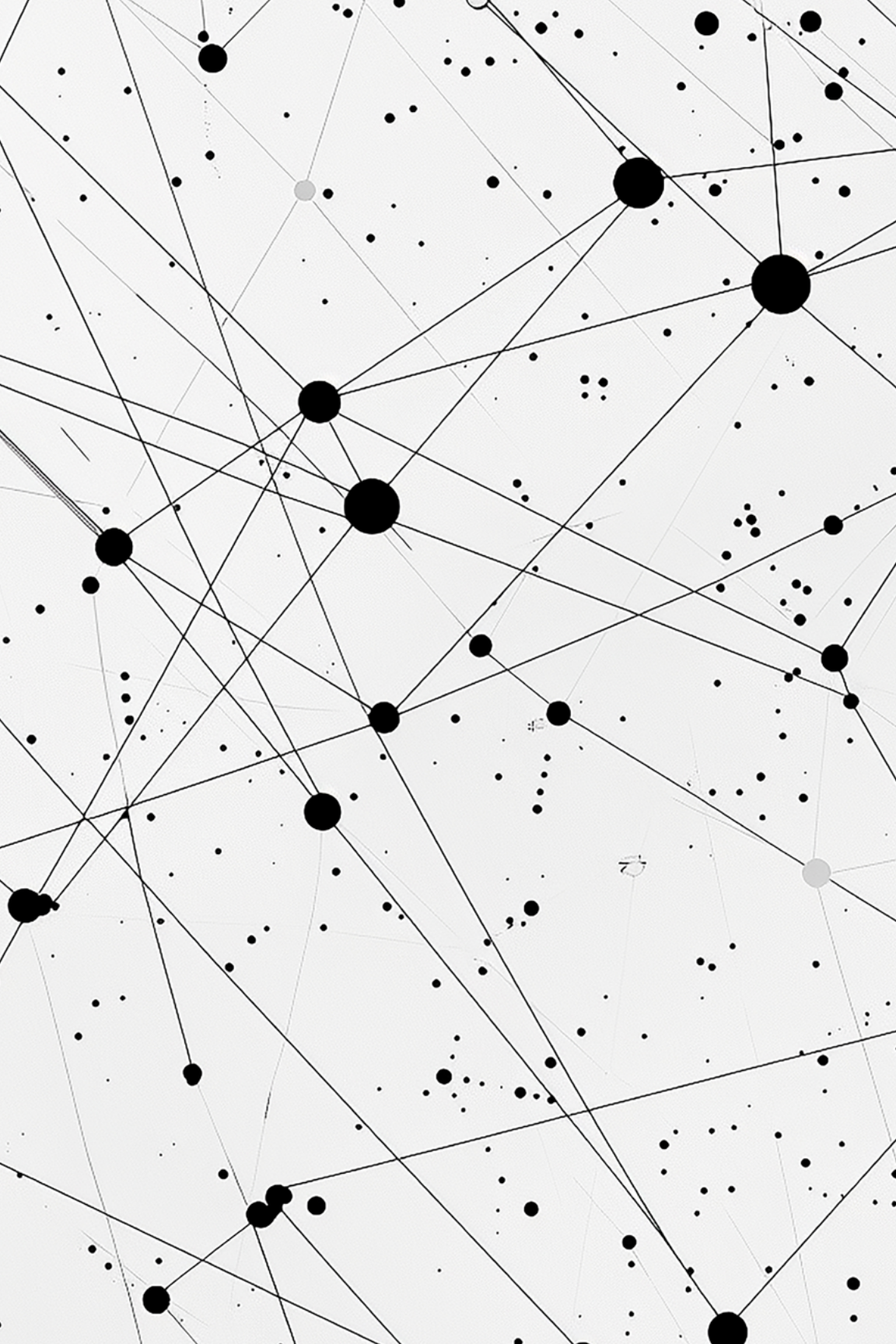
World Federation of Exchanges. (2023, 28 de septiembre). *Promoting sound marketplaces: DeFi/CeFi, crypto platforms & exchanges.*

Wust, K. y Gervais, A. (2018, junio). Do you need a blockchain? En *Crypto valley conference on blockchain technology*, 45-54. IEEE.

Yakovenko, A. (s. f.). *Solana: A new architecture for a high perfomance blockchain* (version V0.8.13).

Zarifis, A. y Cheng, X. (eds.). (2025). *Fintech and the emerging ecosystems: Exploring centralized and decentralized financial techonologies*. Springer.

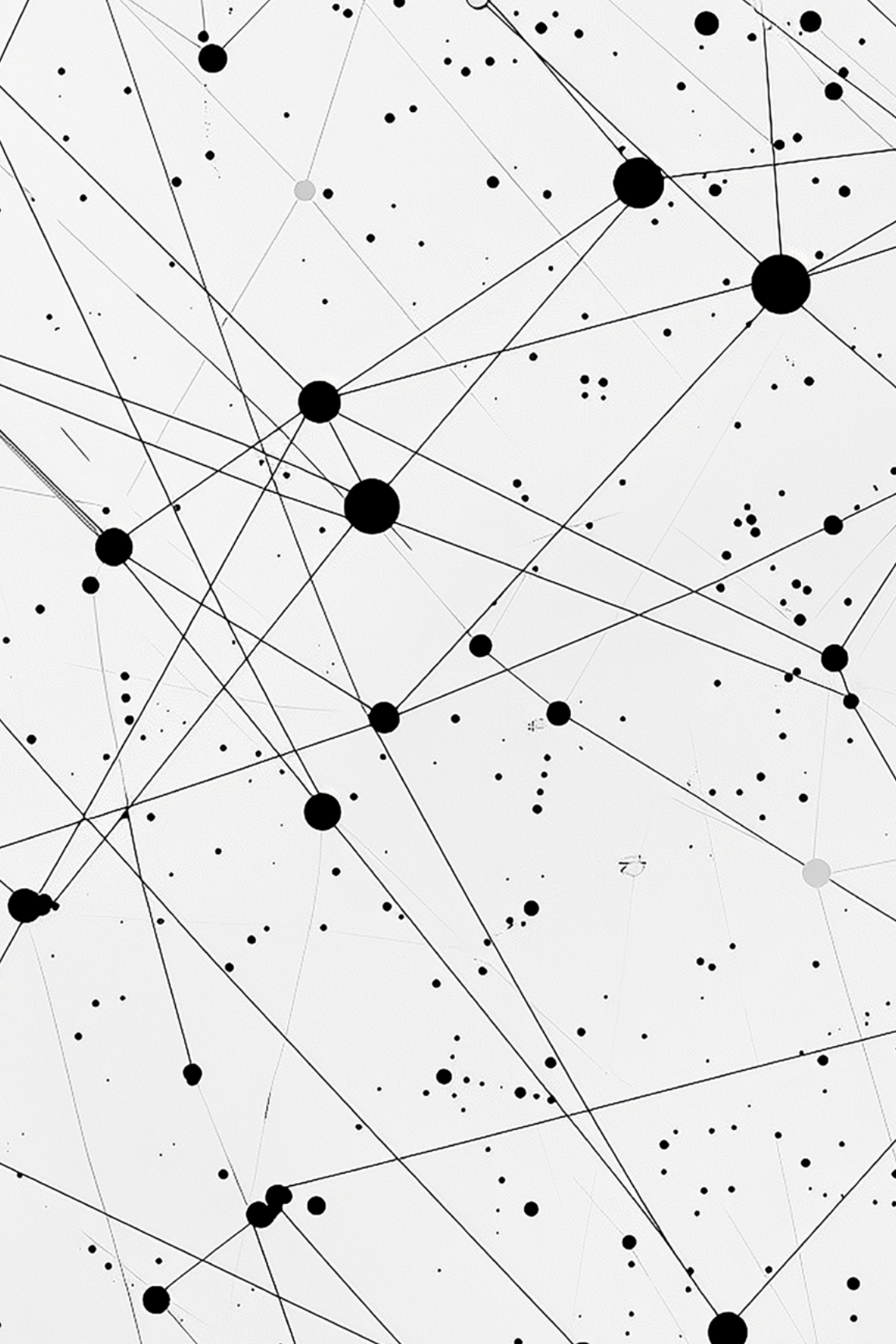
Zoromé, A. (2007, abril). *Concept of off-shore centers: In search of an operational definition*. IMF working papers.



Páginas web consultadas

www.banxico.org.mx
www.bitbo.io
www.bitso.com.mx
www.bitcoin.org
www.bitcointalk.org
www.bitgo.com
www.bitnodes.io
www.bittensor.com
www.buybitcoinworldwide.com
www.cbdctracker.org
www.chainalysis.com
www.csis.org
www.coincover.com
www.coinflip.tech
www.coinmarketcap.com
www.coingecko.com
www.companiesmarketcap.com
www.congress.gov
www.contraparte-central.com.mx
www.crypto.com
www.datareportal.com
www.datareportal.com/reports/digital-2023-mexico
www.docs.solanalabs.com
www.dof.gob.mx
www.dune.com
www.dw.com/es/
lagarde-dice-que-las-criptomonedas-no-valen-nada/a-61901672
www.educa.banxico.org.mx
www.ethereum.org
www.explore.solana.com
www.fatf-gafi.org
www.finance.yahoo.com
www.fincen.gov
www.fsb.org

www.fsc.gi
www.gavwood.com
www.gbbc.io
www.gob.mx/cnbv
www.gob.mx/cnsf
www.gob.mx/condusef
www.gob.mx/consar
www.gob.mx/shcp
www.hash.online-convert.com
www.imf.org
www.inegi.org.mx
www.investinelsalvador.gob.sv
www.investor.gov
www.iosco.org
www. messari.io
www.mxnb.mx
www.nakamotoinstitute.org
www.1inch.io
www.rae.es
www.ralphmerkle.com
www.solana.com
www.solana.org
www.solanabeach.io
www.solidproject.org
www.statista.com
www.studio.glassnode.com
www.synthetix.io
www.theblock.co
www.triple-a.io
www.uniswap.org
www.web3.foundation
www.world-exchanges.org
www.worldlibertyfinancial.com
www.yearn.fi



Glosario

Algoritmo: conjunto de reglas o instrucciones que se utilizan para resolver un problema y producir un resultado específico. El orden de los pasos es vital. Le indica al sistema qué acciones ejecutar.

Aplicación informática (*app*): se trata de una conexión (interfaz gráfica) entre un programa de computación completo (*software*) y el usuario final, a través de su computadora, tableta o teléfono móvil. Es importante diferenciarla de otras conexiones que usan los desarrolladores, especialmente de las interfaces de programación de aplicaciones informáticas (*application programming interfaces*), abreviadas como API. Estas permiten que distintos programas se comuniquen entre sí de forma remota, generalmente mediante comandos. En este caso no se trata de la interacción entre usuario y *software* completo, sino de conexiones entre diferentes programas de cómputo.

Bifurcación (*fork*): división definitiva de una cadena de bloques causada por la falta de consenso o mayoría respecto del protocolo vigente o de posibles mejoras, como en escalabilidad o privacidad. Normalmente, una cadena continúa con las reglas originales y surge otra con un nuevo protocolo y comunidad. Son poco frecuentes las bifurcaciones amigables.

Cadena de bloques: aplicación común de la tecnología de registros distribuidos (TRD) en la que los datos (transacciones) se almacenan en bloques, lotes o agrupaciones enlazados mediante funciones resumen (*hash*). Pueden ser públicas (sin permiso de acceso), privadas (requieren permiso) o híbridas.

Cifrar: ocultar datos o textos originales mediante algoritmos criptográficos. Puede emplear llaves (claves) simétricas o asimétricas para la encriptación. El descifrado transforma los datos encriptados en los datos primarios. Su objetivo es proteger el mensaje enviado entre dos partes. El resultado final en cada caso puede variar dependiendo del algoritmo que se utilice. Aunque la Real Academia Española (RAE) admite su uso como sinónimo de *codificar*, muchos investigadores resaltan sus diferencias en aspectos técnicos.

Codificar: transformar información para representarla en otro formato, ya sea con fines de protección, compresión o transmisión. Requiere de un libro de códigos que especifique las reglas empleadas. El proceso inverso se conoce como decodificación. Las transformaciones entre sistema decimal

y sistema binario es una forma de codificación. Siempre dan el mismo resultado final.

Código abierto: *software* cuyo código fuente está disponible para todos, por lo que puede utilizarse por cualquier persona para algún fin. No todo el *software* de código abierto es necesariamente libre o permisivo de forma que pueda copiarse o modificarse con previa autorización, ya sea que tenga costo o no. Lo contrario del código libre permisivo es el privado, cuyos derechos de autor están restringidos.

Código fuente: programa inicial escrito por el desarrollador en un lenguaje de programación, generalmente de alto nivel y acompañado de comentarios explicativos para otras personas. Debe compilarse o ensamblarse de acuerdo con los sistemas operativos particulares, para convertirse en un programa ejecutable.

Componibilidad (*composability*): posibilidad de integrar una ficha (token) o protocolo de finanzas descentralizadas (DeFi) con otras fichas o protocolos. Facilita las tareas de los usuarios y mejora la eficiencia operativa. El término *componibilidad* proviene del verbo «componer» y no es reconocida por la RAE.

Contraparte Central de Valores (CCV): empresa que forma parte del Grupo de la Bolsa Mexicana de Valores que actúa como intermediaria en transacciones de valores, facilita su liquidación y garantiza el cumplimiento de las obligaciones de las partes.

Contratos inteligentes (*smart contracts*): programas almacenados en una cadena de bloques, como Ethereum, que permiten convertir acuerdos tradicionales entre personas o partes en sus paralelos digitales. Están vinculados a una cuenta o dirección y se ejecutan en una computadora virtual (VM) descentralizada cuando alguien los invoca.

Criptoactivo: activo digital del sector privado que emplea criptografía y tecnología de registros distribuidos o similares.

Dirección: equivalente de una cuenta asociada a una clave pública, que permite enviar o recibir transacciones de criptomonedas.

Dirección autoalojada: dirección derivada de la tecnología de registros distribuidos, compuesta por letras y números, que pertenece a una persona. En su operación puede estar vinculada —o no— con un proveedor de servicios de criptomonedas. Sin embargo, en cualquier escenario, la persona mantiene la posesión y el control de su clave privada.

Encriptación de curva elíptica: tipo de criptografía asimétrica o de clave pública basada en el problema del logaritmo discreto, que se expresa por suma y multiplicación sobre puntos de una curva elíptica (tomado del libro *Mastering Bitcoin* de Andreas Antonopoulos quien lo llama criptografía de curva elíptica).

ERC-20: uno de los estándares técnicos más usados en el ecosistema de las criptomonedas que se utiliza para crear fichas (tókenes) fungibles intercambiables entre sí, en la cadena de bloques, debido a que no hay diferencias significativas entre cada una de ellas. Los activos fungibles también son divisibles. El término proviene de *Ethereum Request for Comments*.

Ficha (token): representación digital de un activo, valor (instrumento financiero) o derecho en una plataforma tecnológica de registros distribuidos; puede o no ser programable. Si la ficha se crea en una plataforma propia que usa tecnología de registros distribuidos, suele denominarse moneda o activo nativo; si se emite en una plataforma rentada, se denomina token. Algunos autores usan el término token como sinónimo de criptoactivo.

Fichas envueltas (*wrapped tokens*): fichas creadas en una cadena de bloques y utilizadas en otra(s) cadena(s) para facilitar la interoperabilidad. Por ejemplo, los wBTC (*wraped bitcoins*) en Ethereum representan bitcoins respaldados en proporción uno a uno, concebidos en su propia cadena, y depositados o bloqueados en Ethereum.

Firma digital (*digital signature*): usa la huella digital de una transacción y la acompaña de otra función resumen (*hash*) derivada de su clave privada, con el objeto de autorizarla y autenticarla. Una vez firmada la operación, nadie la puede cambiar, lo que garantiza su integridad.

Función resumen (*hash*): uso de algoritmos para reducir entradas de datos de diferentes longitudes en una salida de longitud fija. A diferencia del

cifrado y codificación, el *hash* no es reversible con el uso de las computadoras convencionales actuales. Puede emplearse con fines criptográficos (por ejemplo, en firmas digitales) o no criptográficos (organización de datos y creación de índices).

Futuros a perpetuidad: contrato derivado sin fecha de vencimiento. En el espacio de las criptomonedas, es común realizar contratos de bitcoin a perpetuidad en los que los participantes mantienen sus posiciones abiertas, siempre que exista margen o colateral suficiente. Permiten apalancamientos promedio de 40 a 1. Son diferentes de los contratos de futuros tradicionales, que tienen fecha de vencimiento y permiten apalancamientos mucho menores.

Gas: unidad que mide el esfuerzo computacional necesario para ejecutar operaciones específicas en Ethereum. También se refiere a las comisiones que son necesarias para completar esas operaciones en Ethereum.

Hacedores automáticos de mercado (AMM): protocolos utilizados por las casas de intercambio descentralizas (DEX) que usan los contratos inteligentes para establecer los precios de los activos digitales mediante fórmulas matemáticas preestablecidas; varía en cada una de las plataformas de las finanzas descentralizadas, cuyo objetivo es proporcionar liquidez al ecosistema.

Huella digital (*digital fingerprint*): aplicación de una función resumen (*hash*) a una transacción de bitcoin u otra criptomoneda contenida en la cadena de bloques. Por lo general utiliza el algoritmo SHA-256.

Inmutabilidad: capacidad de una cadena de bloques para evitar cambios no autorizados en los datos (registros). Implica que las transacciones ya registradas no han sido alteradas ni eliminadas. Constituye un elemento esencial para la seguridad de las cadenas de bloques.

Minero: nodo completo especializado que opera con una copia completa del bitcoin y crea nuevos bloques de transacciones que añade a la cadena de bloques, por lo que recibe una recompensa. Además, almacena, verifica y distribuye transacciones en la cadena de boques.
Los nodos completos de bitcoin son actualizados por el sitio web bitnodes.io. Al 29 de noviembre de 2025 reportaba 24,673 nodos completos accesi-

bles o públicos, es decir, que sí aceptaban conexiones entrantes externas. Sin embargo, no desglosa cuántos de ellos se dedican específicamente a la minería. Además, es imposible conocer los nodos ocultos que únicamente establecen conexiones salientes a otros nodos. Más allá de las grandes empresas de minería —algunas de las cuales cotizan en los mercados de valores de Estados Unidos—, existen también mineros individuales que usan sus computadoras personales o participan en grupos de minería. Por estas razones, es sumamente difícil estimar el número total de mineros de bitcoin a escala mundial, aunque algunas fuentes sostienen que supera el millón.

Nodo: en el espacio de las criptomonedas, se trata de una computadora conectada por internet que participa en una red distribuida o descentralizada.

Nodo completo de bitcoin: descarga la cadena de bloques íntegra y verifica las transacciones de manera independiente. Algunos nodos completos también realizan minería.

Nodo ligero de bitcoin: no tiene una copia completa de la cadena de bloques y depende de los nodos completos para verificar transacciones. Solo descarga o almacena los encabezados de las cadenas de bloques. También se conoce como nodo de verificación de pago simplificado (SPV, por sus siglas en inglés).

Organización autónoma descentralizada (DAO): en términos generales, es una aplicación descentralizada que define las reglas de operación que dictan quién puede ejecutar una determinada conducta o realizar una mejora. Un libro de códigos ayuda a crear una estructura organizacional que tiene la intención de funcionar sin estructura administrativa.

Préstamo relámpago (*flash loan*): innovación de las finanzas descentralizadas que se implementa para proveer de liquidez en casas de cambio descentralizadas (DEX), en donde todas sus operaciones son atómicas (*atomics*), es decir, se ejecutan en su totalidad o no se concretan. Por ejemplo, si se detectan diferencias de precio de una criptomoneda en dos plataformas distintas, puede solicitarse un préstamo relámpago en una de ellas para comprar la misma en otra plataforma y obtener una utilidad. Si el préstamo es pagado, se termina con éxito la transacción y se agrega a la cadena

de bloques. En caso de que no sea pagado, toda la transacción se revierte en su totalidad.

Programa: secuencia de instrucciones escritas en un lenguaje de programación. Puede clasificarse en programas base, de programación o de aplicación. Asimismo, se distingue entre código fuente (texto), objeto (binario o intermedio) y ejecutable.

Protocolo: conjunto de reglas que permiten la comunicación y el intercambio de información entre sistemas informáticos. Gobierna la operación de un sistema y le indica cómo debe funcionar. Casi todos los protocolos se encuentran estandarizados. En el caso de las criptomonedas, se refiere a la estructura de la cadena de bloques que permite que sean intercambiadas de manera segura en internet. El internet tiene sus propios protocolos (http). En otro contexto, los diplomáticos también tienen su propio protocolo.

Proveedores de liquidez: usuarios que depositan, prestan o bloquean sus criptomonedas en protocolos de finanzas descentralizadas con el fin de obtener la mayor tasa de rendimientos posible (*yield farming*). Otros usuarios inmovilizan sus criptomonedas para apoyar a cadenas de bloques específicas en su operación, convirtiéndose en validadores que identifican recompensas importantes (*staking*). Ambos buscan lucro; sin embargo, los validadores obtienen sus ganancias en la misma criptomoneda que aportan.

Puja: unidad mínima de variación en el precio de una acción negociada en la bolsa de valores, respecto del precio de mercado de la última operación. En las bolsas mexicanas suele equivaler a un centavo (0.01).

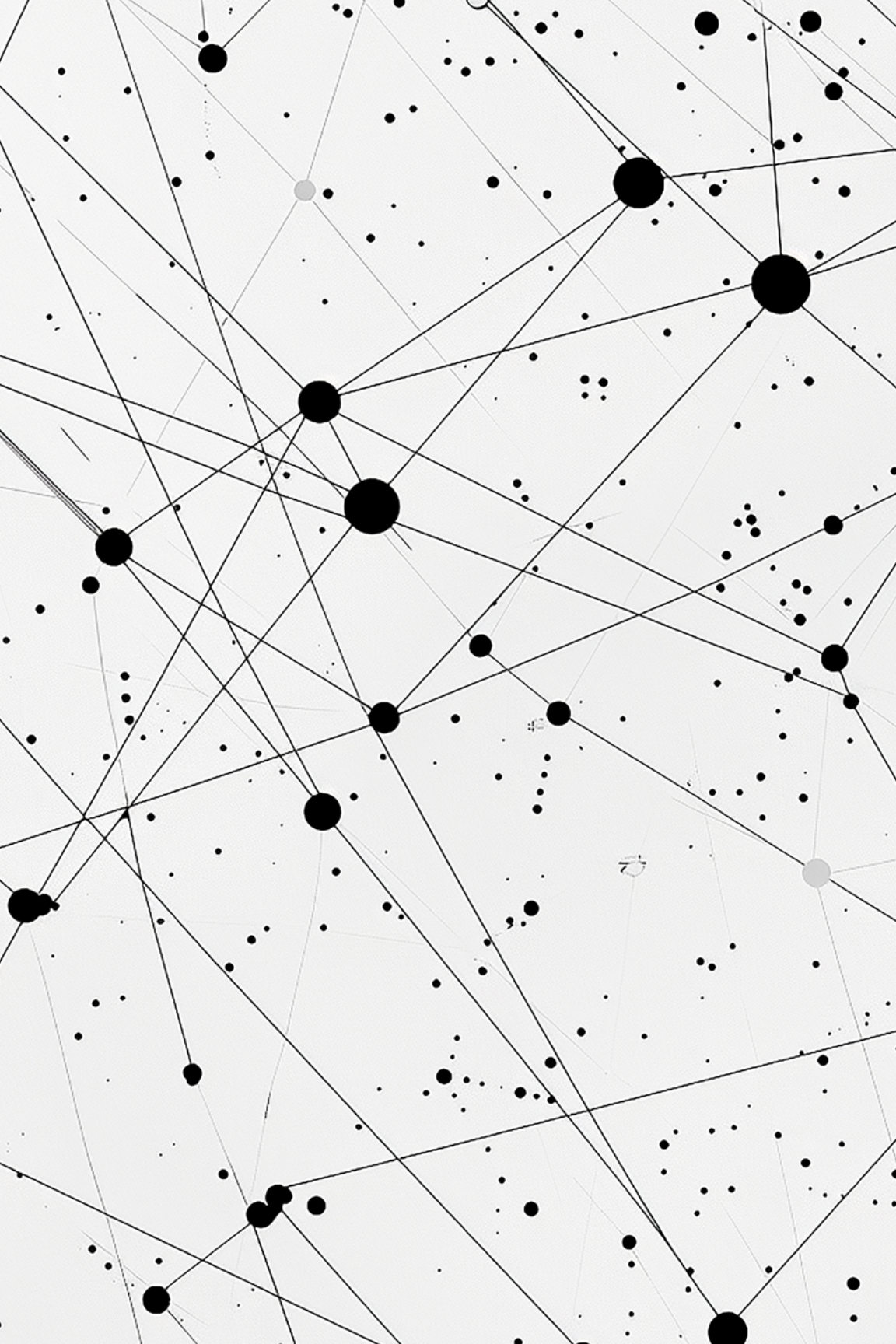
Reporto: de acuerdo con el artículo 259 de la Ley General de Títulos y Operaciones de Crédito (2024), se trata de una operación mediante la cual

> *el reportador adquiere por una suma determinada de dinero la propiedad de títulos de crédito, y se obliga a transferir al reportado la propiedad de otros tantos títulos de la misma especie, en el plazo convenido y contra reembolso de mismo precio más un premio. El premio queda en beneficio del reportador, salvo pacto en contrario. (p. 53)*

Semilla: frase mnemotécnica que contiene una secuencia de 12 o 24 palabras que permite a los usuarios de criptomonedas acceder o recuperar sus llaves (privada y pública), así como sus direcciones. También se denomina clave maestra o única.

***Wallet* (1):** puede traducirse como monedero o billetera electrónica. Una primera definición es que sirve para conectar a los usuarios de criptomonedas con las cadenas de bloques respectivas, ya sea mediante un programa computacional (*software*) o un dispositivo físico. No almacena monedas ni billetes, sino claves o llaves privadas; por ello, es mejor nombrarlos como llaveros. Se distingue entre *wallets* calientes (conectados permanentemente a internet [*software*]) y *wallets* fríos (que no están enlazados permanentemente a internet [dispositivo físico]).

***Wallet* (2):** término empleado por la Condusef en México para referirse a las operaciones que realizan los usuarios identificados con nombres y apellidos mediante instituciones de fondos de pago electrónico (monedero electrónico).



Anexo 1

Bitcoin y bitcoin

En 2008, un programador o grupo de programadores que escribió en inglés bajo el seudónimo de Satoshi Nakamoto publicó un documento técnico-científico que hoy se conoce como *libro blanco*. Este texto fue enviado por correo electrónico a un grupo de amigos. Contiene solo nueve páginas y su título puede traducirse como «Bitcoin: un sistema electrónico de pagos en efectivo entre pares».

La lectura del documento no es fácil, pues exige conocimientos generales de economía monetaria y financiera, nociones de matemáticas y criptografía, así como formación en informática o lo que algunos llaman ciencias de la computación, incluido internet. En particular, es necesario comprender los siguientes conceptos: (a) funciones resumen (*hash*), (b) criptografía asimétrica, (c) árboles *hash* de Merkle y (d) sellos de tiempo en documentos digitales. Aunque el libro no pretender desarrollar a fondo estos cuatro temas, dedica un párrafo a cada uno de ellos.

Hans Peter Luhn fue uno de los pioneros en el estudio de las funciones resumen durante la década de 1950. Desarrolló algoritmos capaces de convertir y reducir entradas de datos de diferentes longitudes en una salida de datos de longitud fija. Estas salidas, conocidas como valores o códigos resumen (*hash*), permiten construir tablas que almacenan información de forma eficiente y facilitan su recuperación. Se trata de funciones unidireccionales: trabajan en un solo sentido, a diferencia de las funciones matemáticas tradicionales, que trabajan en cualquier dirección, de ida y vuelta, entre dos variables. Por ello, también se denominan funciones irreversibles, al menos con la tecnología computacional existente. Bitcoin emplea la familia de algoritmos de resumen seguros (SHA, por sus siglas en inglés), en particular del bloque de salida de 256 bits. Existen convertidores en línea para la transformación de las entradas flexibles en salidas uniformes. Un ejemplo es hash.online-convert.com.

La criptografía tradicional simétrica o de clave secreta fue superada en 1976 por los trabajos de Whitfield Diffie y Martin E. Hellman. Estos investigadores diseñaron un sistema en el que cada usuario dispone de una clave pública (conocida por todos) y una clave privada (que solo conoce su dueño y que debe ser mantenida en secreto). En resumen, se puede decir que este diseño usa claves asimétricas, donde cada persona tiene un par de claves, una pública y otra privada, que son creadas en conjunto y están vinculadas con una función resumen (*hash*); por esta razón, es posible obtener una clave pública si se conoce la privada, pero no al revés. Este mecanismo permite cifrar (encriptar) un mensaje con la clave pública del receptor, de modo que únicamente quien posea la clave privada asociada a esa clave pú-

blica lo puede descifrar (desencriptar). Además, la clave privada posibilita la creación de una firma digital que, en teoría, logra la autenticación del verdadero contenido del mensaje. La criptografía asimétrica o de clave pública se emplea de forma esencial en los monederos (*wallets*) de bitcoin, ya que permite compartir las claves públicas y sus direcciones con seguridad en la red de computadoras descentralizadas y abiertas. No obstante, el modelo original de Diffie y Hellman representaba limitaciones teóricas que lo hacían vulnerable a ciertos ataques en su implementación práctica.

Ralph Merkle presentó en 1979 su tesis doctoral en ingeniería electrónica en la Universidad de Stanford, con el título *El secreto, la autenticación y el sistema de clave pública*, bajo la supervisión de Martin E. Hellman. En su trabajo mejoró la labor de su maestro e ideó un método para producir firmas digitales seguras basado en árboles que hoy llevan su nombre. Este esquema propone una estructura tipo árbol para manejar una gran cantidad de datos organizados, desde la parte baja hacia arriba, hasta llegar a un nodo raíz único. Los datos se agrupan en pares para ser agregados a una nueva rama del árbol (capa superior), a través de un *hash* que los conecta o encadena con el bloque anterior. El proceso se repite produciendo otras ramas que son ligadas hasta el final, en un único valor *hash* que es el resumen del nodo único del árbol. Dado que el método de Merkle es repetitivo, el nodo único también es llamado nodo raíz. A este último, Merkle lo acompaña de una firma digital para hacer el proceso más seguro y fiable, con la finalidad de que los datos no sean alterados a medida que son propagados en la red de computadoras. En 1982, Merkle obtuvo una patente en Estados Unidos por este método de firma digital basada en árboles. Bitcoin utiliza esta estructura para resumir todas las transacciones contenidas en un bloque y agregar el *hash* de la raíz en la estructura de la cabecera del bloque.

En la actualidad, la mayoría de los textos, audios, imágenes y videos están disponibles en forma digital. Dado que muchas de estas bases de datos pueden modificarse con relativa facilidad, resulta necesario certificar cuándo fueron creadas o modificadas por última vez. El problema consiste en sellar la hora, el día y el año de los datos, no de los medios. En 1991, Stuart Haber y W. Scott Stornetta publicaron el artículo «Cómo sellar el tiempo de los documentos digitales» en la *Revista de Criptología* (*Journal of Cryptology*). En él propusieron procedimientos de certificación basados en funciones *hash*, firmas digitales y enlaces o encadenamientos que son confiables y seguros. Sostenían que cualquiera de sus algoritmos computacionales provee de mayor credibilidad a un documento que la certificación

realizada por un proveedor físico. Dos de sus aportaciones fueron incorporadas a Bitcoin. En primer lugar, codifica el tiempo usando la época UNIX, que contabiliza los segundos transcurridos desde la medianoche del 1 de enero de 1970, según el tiempo universal coordinado (UTC, por sus siglas en inglés), uno de los sucesores del tiempo medio de Greenwich. Por ejemplo, si usted vive en Puebla y observa el número 1,743,851,304 registrado en la cabecera de una cadena de bloques de Bitcoin, significa que este fue creado (minado) aproximadamente a las 5 horas con 8 minutos y 24 segundos del día 5 de abril de 2025. En segundo lugar, los enlaces o encadenamientos han inspirado el funcionamiento de la cadena de bloques.

Con la aparición de Bitcoin, se integraron los desarrollos conceptuales previos y, por primera vez en la historia, se logró resolver el problema del doble uso de las monedas (doble gasto), y la aplicación práctica de un mecanismo de acuerdos mayoritarios (prueba de trabajo), que permitió garantizar que los registros contables fueran irreversibles y que la red fuera segura. Todo ello ocurrió en el contexto de la crisis del sistema financiero occidental y la caída de Lehman Brothers, momento en el que la confianza en los bancos privados y centrales disminuyó significativamente. Al menos en teoría, surgió así la primera criptomoneda global ligada a un sistema descentralizado o distribuido, como los registros de sus transacciones que se agrupan en bloques para su manejo contable.

En el correo electrónico que Satoshi Nakamoto envió el 31 de octubre de 2008 expuso las principales propiedades de Bitcoin: (a) el doble gasto se previene en una red entre pares; (b) no existe una ceca de acuñación o un intermediario de confianza; (c) los participantes pueden ser anónimos; (d) las nuevas monedas se generan mediante pruebas de trabajo al estilo Hashcash —propuesto en 1997 por Adam Black para combatir el correo basura—; y (e) la prueba de trabajo de una nueva generación de monedas también empodera a la red para prevenir el doble gasto.

El 8 de enero de 2009, Nakamoto envió un nuevo correo a su lista de amigos criptógrafos para anunciar la primera emisión de su moneda y compartir públicamente el *software* de código abierto, escrito en C++ (Bitcoin v0.1 Alpha). Describió dos formas de enviar dinero, entonces complejas, ya que todavía no existían empresas dedicadas a proveer el servicio de monederos (*wallets*). Asimismo, estableció que la circulación total de bitcoins en el tiempo tiene un límite de 21 millones de monedas, distribuidas entre los nodos de las redes que contribuyeran a completar los bloques de las transacciones, con una cantidad que se reducirá a la mitad cada cuatro años (*halving*). Durante los primeros cuatro años se pusieron en circulación 10.5

millones de monedas; en los cuatro siguientes, 5.25 millones, y así sucesivamente. Aunque el correo no lo señalaba explícitamente, los cálculos muestran que este mecanismo se prolongará hasta el año 2140. Una vez concluida la emisión, el sistema continuará operando solo con las comisiones que los usuarios paguen por las transacciones. Cabe señalar que Bitcoin v.0.1 obtuvo en 2009 una licencia del MIT para *software* libre permisivo, que autoriza el uso, copia y modificación sin costo alguno para cualquier persona, —incluso con fines comerciales—, siempre que se incluya la copia de la licencia y el aviso del derecho de autor original (*copyright*).

Nakamoto se mantuvo activo durante 2009 y 2010: creó el bloque génesis (o bloque cero), realizó algunas transferencias a sus amigos y detalló el funcionamiento de los programas de computación. Sin embargo, a inicios de 2011 cesó toda comunicación pública y dejó el desarrollo del protocolo en manos de una comunidad de voluntarios, entre ellos, Gavin Andresen, quien asumió el liderazgo técnico. Posteriormente se creó la Fundación Bitcoin con el propósito de preservar el desarrollo del proyecto y lograr la estandarización mundial. Esta organización sin fines de lucro es una entidad legal vinculada a Bitcoin que tiene una moneda y sus registros, pero no es una empresa constituida. Probablemente se trata de un proyecto financiado por Nakamoto con la ayuda de familiares y amigos. Nunca realizó una oferta pública inicial, como sí ocurrió con la mayoría de las criptomonedas surgidas después de bitcoin.

Más allá de la pregunta abierta sobre la identidad de Satoshi Nakamoto, otra cuestión relevante es la cantidad de bitcoins que pudo haber acumulado. En la primera etapa del proyecto era el principal minero y cada bloque ofrecía una recompensa de 50 bitcoins. Las estimaciones varían: algunas estiman que fueron 600,000 bitcoins; otras, una cantidad por encima de 1.1 millones. En cualquier escenario, si permanecieran intactas, lo situarían entre las personas más ricas del mundo. Los actuales críticos del proyecto descentralizado sostienen que, aunque se trate del protocolo con mayor valor de capitalización de su moneda (véase la tabla 4) y existan más de 21,000 mineros con nodos completos (véase la tabla 5), el mayor poder de concentración y de gobernanza para toma de decisiones está en las manos de su creador. Vaya paradoja.

De acuerdo con bitbo.io, a media mañana del 27 de noviembre de 2025 se habían procesado más de 925,450 bloques y se habían emitido 19.95 millones de bitcoins. En 2008 cada nuevo bloque emitía 50 bitcoin para los mineros (nodos) que procesan las operaciones. Cada cuatro años, dicha

emisión (subsidios para los mineros) se reduce a la mitad: en 2012, el premio o la recompensa era de 25 bitcoins por bloque; en 2016, a 12.5; en 2020, a 6.25; y desde abril de 2024 es de 3.125 bitcoins por bloque. Se estima que el último minado de un satoshi (0.00000001 de un bitcoin) se minará alrededor del año 2140. A partir de entonces, los mineros dejarán de recibir el premio y solo obtendrán las comisiones que se cobran por cada transacción.

Cada bloque se genera en un promedio de diez minutos, lo que implica aproximadamente 144 bloques que, al multiplicarlos por la recompensa actual (3.125), resulta en la generación diaria de 450 bitcoins. En cuanto a la capacidad de procesamiento, el tamaño máximo por bloque es de aproximadamente cuatro megabytes, que equivale a un máximo de 3,000 transacciones por bloque.

Tras este panorama general sobre la emisión de bitcoin, procede explicar el proceso para realizar transacciones y el funcionamiento del libro público de contabilidad (base de datos) donde se registran y agrupan en bloques, es decir, la denominada cadena de bloques.

En la tercera página del libro blanco, Satoshi Nakamoto (2008) describe seis pasos para el funcionamiento de la red:

> 1) Las nuevas transacciones son transmitidas a todos los nodos.
> 2) Cada nodo recaba las nuevas transacciones en un bloque.
> 3) Cada nodo trabaja para encontrar el bloque que sea la prueba de su trabajo.
> 4) Cuando el nodo encuentra la prueba de su trabajo, lo difunde a los demás nodos.
> 5) Los otros nodos aceptan el bloque si todas las transacciones que contiene son válidas y no han sido gastadas.
> 6) Los nodos expresan su aceptación del bloque y continúan trabajando en la creación de un nuevo bloque en la cadena, aceptando la función resumen (*hash*) como la cadena previa.

Existen diversos tipos de transacciones de bitcoin, aunque la más común se refiere a pagos de una dirección a otra. En la vida cotidiana, las operaciones en efectivo se liquidan con billetes y monedas y, cuando no se entrega la cantidad exacta, se recibe cambio. Lo mismo sucede con las operaciones simples de bitcoin: la persona que paga desde su dirección recibe cambio en el caso de transferencias que son menores a sus monedas no gastadas. Bitcoin usa una base de datos de entradas y salidas, por

lo que en este caso hay un insumo y dos salidas que corresponden a la transferencia y al cambio.

Se denomina nodo a cualquier computadora conectada a la red descentralizada. Los nodos descritos en el libro blanco son nodos completos, explicados en el primer capítulo. Con el tiempo, estos nodos han evolucionado y hoy se trata de grupos de computadoras (granjas) que usan circuitos integrados de aplicación específica (semiconductores cada vez más poderosos). Estos equipos descargan y mantienen una copia completa y actualizada de la cadena de bloques y consumen cantidades significativas de energía eléctrica. A este subconjunto de nodos completos se les denomina mineros. Existen también otros nodos (usuarios) de peso ligero (véase el glosario) que solo mantienen una parte de la cadena de bloques y no pueden verificar las transacciones de manera directa.

Los usuarios envían sus transacciones primero a un nodo que normalmente tiene ocho vecinos, que a su vez tienen más vecinos y se encargan de hacer la transmisión por etapas al resto del sistema. Las direcciones de bitcoin inician con el número 1 o 3 y son seguidas de 34 letras (mayúsculas y minúsculas) y números. Es importante mencionar que, si en una transferencia de bitcoin, un usuario se equivoca en cualquiera de los caracteres, el importe no llegará al destinatario original. Dado que las operaciones son irreversibles, el usuario no podrá recuperar su dinero y el beneficiario no recibirá nada, por lo que el monto será recibido en otra dirección desconocida y anónima. Por ello, es indispensable verificar cuidadosamente los envíos.

Cada nodo tiene un inventario de transacciones pendientes y escoge algunas de ellas para ponerlas en un bloque candidato. Los nodos completos especializados —los mineros— compiten entre sí para resolver un problema matemático, ya sea de manera aleatoria o consecutiva, que consiste en un campo numérico de bits para validar las transacciones. El campo numérico de bits es conocido en inglés como *nonce*, que se compone de la primera letra de *number* (número) y la palabra *once* (una vez). El acertijo es un número aleatorio que solo se utiliza una vez para generar un nuevo bloque. La competencia entre mineros es justa en el sentido de que cualquiera de ellos puede ganar, siempre y cuando tengan inversiones similares de equipo computacional.

Se reitera que cada minero debe seleccionar las transacciones que tiene en su inventario para formar un bloque candidato. La cabecera de su bloque candidato debe estar ligada al bloque anterior y tiene que resolver antes que los demás el acertijo que es utilizado como la prueba de su tra-

bajo. El protocolo de Bitcoin establece un objetivo de dificultad del algoritmo necesario para demostrar la prueba de trabajo de cada bloque. Cada minero tiene que encontrar, con la ayuda de sus computadoras, un *hash* de 256 bits de longitud que sea numéricamente igual o menor que el objetivo arbitrariamente establecido. Dicho objetivo se ajusta automáticamente cada 14 días (2,016 bloques) para mantener el tiempo promedio de generación de bloques en diez minutos. Si la generación de bloques de los últimos 14 días es menor a diez minutos, el objetivo o la dificultad se tiene que aumentar, y viceversa.

Si el bloque candidato gana la competencia, el minero recibe la recompensa de 3.125 bitcoins más las comisiones generadas en ese nuevo bloque que está ligado a uno anterior. El nuevo bloque se difunde para su validación, tanto de las transacciones como de los bitcoins y las comisiones ganadas por el nodo. No obstante, las transacciones del bloque ganador no se consideran confirmadas sino hasta que otros seis bloques las acepten.

Todo este proceso no solo protege la seguridad de las operaciones, sino que también obtiene el voto mayoritario de los participantes mediante el mecanismo de la prueba de trabajo de cada uno de ellos. En particular, consigue un acuerdo público en el orden de los bloques y, por lo tanto, de las transacciones contenidas en cada uno de ellos.

Para describir cómo los usuarios de bitcoins interactúan con la cadena de bloques, el libro público de contabilidad o la base de datos, es necesario hablar de los monederos (*wallets*). En el caso de las monedas y billetes en circulación emitidos por los bancos centrales, suelen ser retirados de los cajeros automáticos (ATM) de los bancos múltiples, y guardados en monederos o billeteras para usarlos en operaciones de bajo valor. El caso de las criptomonedas es diferente, ya que las monedas «residen» en las cadenas de bloques y no pueden extraerse de estos libros para guardarlas físicamente en monederos. Por ello, estos *wallets* no sirven para guardar o almacenar criptomonedas.

Los monederos o billeteras sirven para conectar a los usuarios de Bitcoin con las cadenas de bloques, a través de un programa de cómputo o de un dispositivo físico (*hardware*). Esta interacción les permite enviar y recibir bitcoin, así como determinar su saldo (diferencia entre entradas y salidas). En resumen, se puede decir que los monederos no contienen monedas, sino claves privadas (equivalente al número de identificación personal, NIP) que sirven para generar firmas digitales y obtener claves públicas, que a su vez generan direcciones (similares al número de una cuenta bancaria). Por esta razón, algunos autores señalan que sería

más preciso hablar de llaveros que de monederos. En 2013, Andreas Antonopoulos popularizó la expresión: «Si no tienes las llaves, no tienes tus monedas» (*not your keys, not your coins*).

Hoy existen numerosas empresas que facilitan la creación de monederos. El usuario puede escoger el monedero que mejor satisfaga sus necesidades e incluso utilizar varios. Algunos son gratuitos y otros tienen costo. Los que se obtienen a través de la computadora de escritorio o de su teléfono inteligente suelen ofrecer menor seguridad que los dispositivos físicos especializados. La mayoría genera un número hexadecimal aleatorio de 256 bits que es traducido al inglés —u otra lengua, como el español— con el equivalente del uso de un diccionario de 2,048 palabras, en una frase mnemotécnica, denominada semilla, que contiene 24 palabras predefinidas.

La semilla sirve para generar una cadena determinada de números y letras (caracteres) que constituyen la llave privada; no es la clave en sí, pero concede acceso a ella. Por ello, debe mantenerse en secreto y resguardarse adecuadamente. A partir de la clave privada se genera un árbol de llaves públicas que tienen también una cantidad determinada de números y letras (caracteres) que, a su vez, produce múltiples direcciones para bitcoin o cualquier otra criptomoneda. Así, un monedero único puede administrar numerosas claves y direcciones. En cursos impartidos en 2023 en la Universidad de Nicosia (UNIC), Andrea Antonopoulos reiteró una advertencia complementaria: «Si no tienes tu semilla, no tienes tus monedas».

Las direcciones y transacciones de cada usuario quedan registradas en la cadena de bloques y pueden rastrearse; sin embargo, no están vinculadas directamente a la identidad de las personas (nombres y apellidos), sino a una cadena de números y letras. Finalmente, para completar la operación, la llave privada crea la firma digital para autorizarla y autenticarla. Por ello, se suele afirmar que Bitcoin no opera de manera anónima, como lo dijo Nakamoto en su primer correo electrónico, sino cuasianónima o seudónima.

Conviene distinguir, finalmente, entre huella digital y firma digital. La primera es resultado de una función resumen (*hash*) aplicada a una transacción. La segunda se genera mediante la llave privada del dueño de bitcoins no gastados que, a su vez, produce otra función resumen en la que adjunta y autoriza la huella digital.

En su mayoría, los usuarios de Bitcoin utilizan el *software* principal, Bitcoin Core, que cualquier persona puede descargar para participar en la red. Estos programas de cómputo operan tanto en el protocolo del internet superficial o visible (IP) como en protocolos del internet profundo, del

oculto y del oscuro, como Tor, I2P o Hotspot shield. Según datos estimados por bitbo.io al 29 de noviembre de 2025, la red pública entre pares de Bitcoin contaba con 23,933 nodos distribuidos alrededor del mundo. Este número es superior al reportado en la tabla 5, elaborada en junio de 2025. La plataforma reporta que 15,378 nodos del total operaban en la red Tor antes mencionada. Es decir, el 64 % de los nodos localizables de Bitcoin funciona a través del internet oscuro.

El *software* continúa en etapa experimental y actualmente se encuentra en la versión 30.0. Bitcoin Core sincroniza la red (nodos) y las bases de datos (cadena de bloques) para validar y confirmar transacciones. No está diseñado para la creación directa de monederos o billeteras; por ello, las empresas dedicadas a la producción de *wallets* emplean otro *software* para conectarse con Bitcoin Core y acceder a la cadena de bloques.

En resumen, Bitcoin es parte de una moneda digital descentralizada que puede operar sin intermediario. Sin embargo, su gobernanza podría considerarse concentrada si se toma en cuenta la tenencia de su creador —el monedero de Satoshi— y la participación de la empresa Strategy, que cotiza sus acciones en el Nasdaq y mantiene en su tesorería 650,000 bitcoins adquiridos mediante capital propio, acciones preferentes y deuda. Bitcoin es una red abierta: cualquiera puede entrar o salir sin permiso alguno. Es pública, ya que los registros de las transacciones pueden verificarse y están disponibles para todos los nodos completos. De igual manera, es global —no tiene fronteras— y opera en internet entre pares, las 24 horas del día, todos los días del año.

Se trata del primer proyecto que logró consolidar una moneda global descentralizada y una plataforma ampliamente distribuida. Puede afirmarse que se autorregula mediante protocolos y algoritmos matemáticos. Permite realizar pagos entre pares, ya que nunca ha sido hackeada y mantiene registros inmutables desde 2009.

Conviene precisar que Bitcoin, como red de nodos y cadena de bloques, no usa criptografía alguna; está fundamentada en matemáticas que incluyen las funciones resumen, los árboles de Merkle, los sellos de tiempo, además de múltiples códigos numéricos y computacionales. La criptografía se emplea en el diseño de los llaveros (*wallets*), donde se crea una clave privada y, a partir de ella, se usa la encriptación para crear la clave pública. Este proceso fortalece la seguridad y la privacidad de todo el proceso.

Dado que su implementación completa ha impactado intereses económicos relevantes, Bitcoin recibe críticas por su consumo energético, ya que

la prueba de trabajo de los mineros supera el consumo de energía eléctrica de países pequeños. Aunque una proporción creciente de mineros emplea fuentes renovables, el debate ambiental persiste. Como se verá más adelante, hay otras monedas digitales que usan mecanismos de consenso con consumos de energía reducidos. A pesar de lo anterior, la paradoja actual consiste en que, mientras la reducción de gases de efecto invernadero constituye uno de los mayores desafíos que enfrenta la humanidad, Bitcoin representa el 57.3 % del valor total de capitalización de las criptomonedas (tabla 4). Surge así la disyuntiva relevante: ¿debe priorizarse la innovación financiera descentralizada o la mitigación del cambio climático? La respuesta depende del enfoque que se adopte.

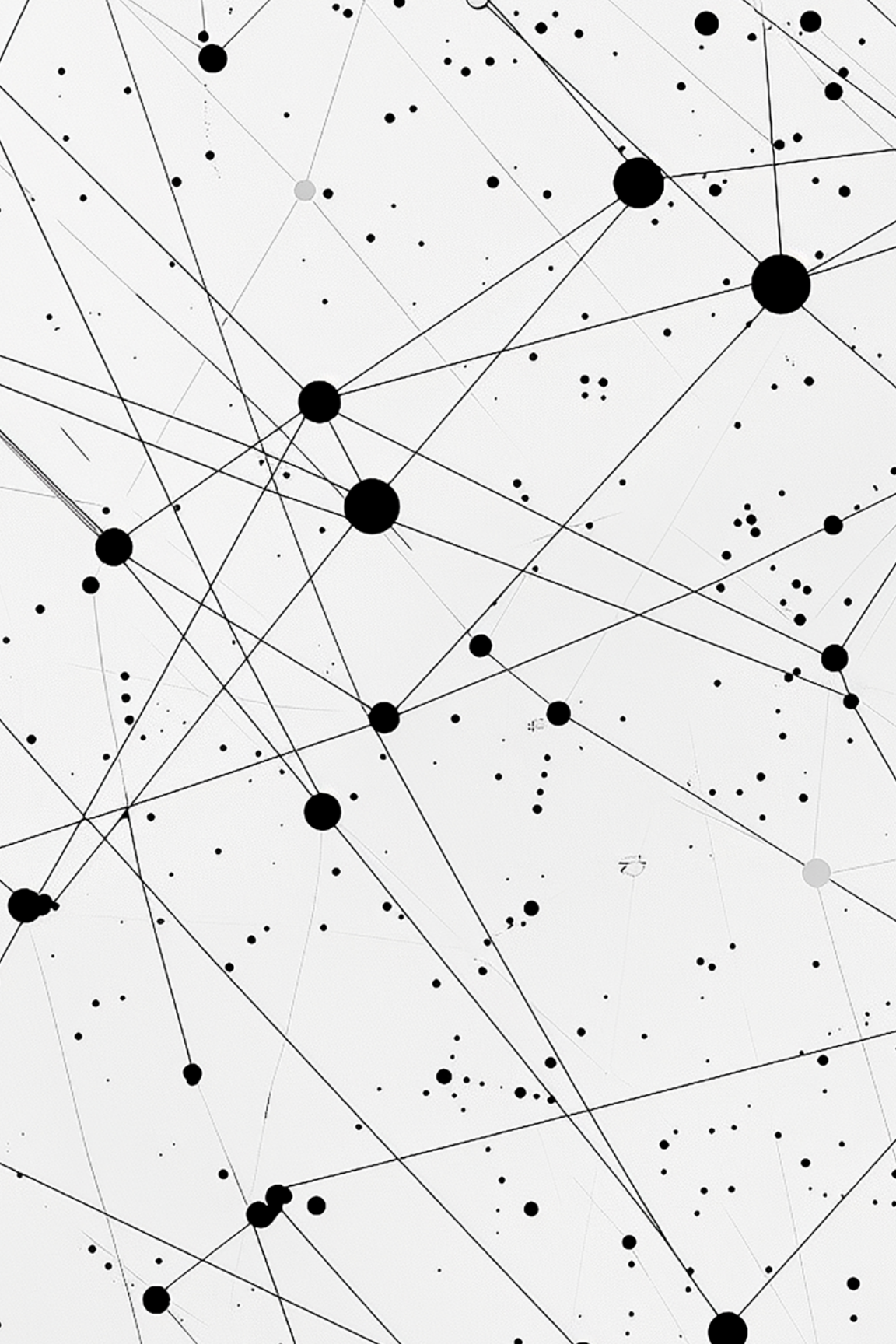
Tampoco se cuestiona su carácter cuasianónimo, que dificulta la labor de los países miembros del Grupo de Acción Financiera Internacional (GAFI), especialmente en la prevención del lavado de dinero. Las autoridades fiscales enfrentan retos para supervisar y gravar las operaciones cuando los usuarios convierten bitcoin en dinero fíat. A ello se suma la desaparición de su creador y la ausencia de una entidad corporativa formal, lo que complica cualquier intento de regulación directa, principalmente porque la moneda y su base de datos fue desarrollada con su propio dinero.

Otro grupo señala su alta volatilidad. En sus 17 años de existencia, su precio ha pasado de valer apenas unos centavos a alcanzar 126,277 dólares el 5 de octubre de 2025. Las variaciones pueden producirse en cuestión de minutos, en cualquier dirección de dos dígitos. Para atender esta preocupación surgieron las denominadas monedas estables (*stablecoins*), mencionadas en el primer capítulo.

La volatilidad se intensifica parcialmente porque los participantes pueden operar en plataformas descentralizadas (DEX), como Hyperliquid, que permiten apalancamientos de hasta 40 a 1 en futuros de bitcoin a perpetuidad, que son implementados con la moneda estable USDC. Esto contrasta con los futuros tradicionales que tienen un plazo fijo de vencimiento y un apalancamiento de dos a uno. Por ejemplo, el viernes 10 de octubre de 2025, tras un anuncio del presidente Trump sobre posibles aranceles adicionales a China, se produjo una venta masiva de bitcoins en cuestión de minutos. La caída del precio activó liquidaciones automáticas en posiciones sin margen suficiente, lo que ocasionó mayores bajas y generó pérdidas estimadas en cerca de 20 billones de dólares en unas horas. Algunas personas han denominado este episodio como la gran caída del bitcoin. Ese viernes, su cotización se situaba cerca de los 114,000 dólares;

al día siguiente ya se encontraba por debajo de los 109,000 y, al 31 de diciembre de 2025, había descendido a 87,800 dólares.

Para terminar esta sección, se aclara que actualmente se distingue entre la criptomoneda y su tecnología. En el primer caso, la moneda digital se escribe con minúscula (bitcoin) y para el segundo, la cadena de bloques se escribe con mayúscula inicial (Bitcoin). En el ámbito tecnológico, dado que Bitcoin agrupa las transacciones en bloques que los une de manera lineal en el tiempo, los usuarios y desarrolladores acuñaron el término cadena de bloques (*blockchain*) en una primera instancia, para después usar el término genérico de tecnología de registros distribuidos.



Anexo 2

Ethereum y ether

Este apartado inicia con la aclaración de que la moneda digital ether y su tecnología, Ethereum, tienen nombres distintos, lo que facilita su explicación. A pesar de ello, hay usuarios que emplean ambos términos como sinónimo, lo que técnicamente se considera incorrecto.

Ethereum es una de las pocas tecnologías que cuenta con un libro blanco (usado por los desarrolladores para los inversionistas iniciales), un libro amarillo (dirigido para las personas con conocimientos más avanzados) y un libro beige (enfocado para el resto de los usuarios). El primero fue escrito por Vitálik Buterin, el segundo por Gavin Wood y el tercero, por Micah Dameron. El estudio de estos documentos representa un punto de partida adecuado para analizar este tema, reconociendo que han tenido muchas evoluciones y su estado actual probablemente continuará cambiando.

En 2013, Vitálik Buterin escribió el libro blanco de Ethereum titulado *Una próxima generación de contratos inteligentes y una plataforma de aplicación descentralizada*, donde expresa desde la primera página que:

> *Lo que Ethereum pretende es proporcionar una cadena de bloques con un lenguaje integrado Turing completo y plenamente desarrollado que se puede usar para crear contratos que, a su vez, se pueden utilizar para codificar funciones arbitrarias de transición de estados, permitiendo a los usuarios crear cualquier aplicación.*

Ethereum creó una nueva cadena de bloques con un lenguaje original de programación de alto nivel denominado Solidity. El antecedente de los sistemas completos de Turing se remonta al inglés Alan Turing, considerado uno de los padres de la ciencia de la computación. Diseñó un aparato —hoy conocido como máquina de Turing— capaz de resolver cualquier problema matemático representable mediante un algoritmo. Durante la Segunda Guerra Mundial colaboró en el desciframiento de códigos nazis, particularmente los de la máquina Enigma.

Un mecanismo de Turing completo puede ejecutar cualquier programa de lógica matemática. Esto implica que admite bucles o ciclos (instrucciones repetitivas), estructuras condicionales (*if-then*) y, al menos en teoría, pueden trabajar de manera infinita. Ethereum es considerado como Turing

completo, a diferencia de Bitcoin, cuyo lenguaje de programación es más limitado y especializado.

Los contratos inteligentes son programas de computadora almacenados en una cadena de bloques que permiten convertir acuerdos entre personas (contratos tradicionales) en sus paralelos digitales. Una vez que son implantados en la cadena de bloques, no pueden ser modificados; de ahí que se les califique como inmutables. Técnicamente, un contrato inteligente es un conjunto de código e información alojado en una cuenta o dirección de la cadena de bloques. En términos generales, se trata de un programa informático que se ejecuta automáticamente, sin la mediación de terceros. Dado que utiliza programas computacionales, su lenguaje difiere del utilizado en los contratos legales a los que estamos acostumbrados en la vida real. De manera figurada, suele afirmarse que el código es el equivalente a la ley en los contratos tradicionales. Lawrence Lessing, quien fue mencionado en la introducción de este libro, acuñó la frase «el código es la ley» (*code is law*), originalmente como advertencia ante la falta de regulación.

En resumen, los contratos inteligentes son programas de computadoras inmutables en el sentido de que, una vez que son implementados, su código no puede alterarse; es decir, la única forma de modificarlo es implementar uno nuevo. Además, son deterministas: ejecutados en la máquina virtual de Ethereum (EVM, por sus siglas en inglés), su resultado es el mismo para cualquier usuario. La EVM es otro *software* (Geth) que opera en la cadena de bloques de Ethereum y se encarga de ejecutar los contratos inteligentes.

El concepto de contrato inteligente fue acuñado en la década de 1990 por Nick Szabo, quien lo definió como un protocolo de transacciones computarizadas que ejecutan los términos de un acuerdo. Su objetivo era posibilitar transacciones sin intermediarios. Como se verá, estos contratos inteligentes son la base para las aplicaciones descentralizadas.

Tras el lanzamiento de Ethereum en 2015, Vitálik Buterin escribió en Twitter (hoy X): «Para ser claro, en este momento me arrepiento de haber adoptado el término de contratos inteligentes. Debí de haberlos llamado con algo que fuera más aburrido y técnico, probablemente algo como comandos básicos y persistentes».

En 2025 el debate continúa. Algunos sostienen que no son contratos ni son inteligentes. Argumentan que no son contratos en el sentido tradicional, ya que, aunque exista un convenio informal entre las partes, su cumplimiento no puede ser compelido (obligado por alguna autoridad). También

cuestionan su carácter «inteligente», ya que no incorporan inteligencia artificial generativa, sino que simplemente ejecutan los códigos programados. Otros, en cambio, defienden que sí pueden considerarse contratos en un sentido funcional y que su automatización justifica el calificativo. La postura del lector puede situarse en cualquier punto intermedio entre estas posiciones.

Una aplicación descentralizada (*dapp* o DA) fue descrita por Vitálik Buterin en una publicación realizada el 6 de mayo de 2014 en el blog de Ethereum, titulada «Organizaciones autónomas descentralizadas, Compañías autónomas descentralizadas, Aplicaciones descentralizadas y más: Una guía terminológica incompleta» (*DAOs, DACs, DAs, and more: An incomplete terminology guide*) en los siguientes términos:

> *Una aplicación descentralizada es similar a un contrato inteligente, pero se diferencia en dos aspectos clave. En primer lugar, una aplicación descentralizada tiene un número ilimitado de participantes en todos los ámbitos del mercado. En segundo lugar, una aplicación descentralizada no tiene por qué ser necesariamente financiera.*

Las aplicaciones descentralizadas requieren, como mínimo, un contrato inteligente y una interfaz de usuario. En términos generales, una aplicación descentralizada es una aplicación web construida sobre una red abierta y descentralizada de pares. Como se mencionó en el párrafo anterior, las aplicaciones pueden ser financieras (relacionadas con el dinero) o no financieras (como votaciones en línea y gobernanza descentralizada).

Esta tecnología se acompaña de una criptomoneda denominada ether, usada primordialmente para pagar el uso de la plataforma. Una de sus subdivisiones para el pago del denominado gas es el gwei, donde 1 ether equivale a 1 gwei seguido de nueve ceros. No debe confundirse el gwei con el wei —mencionado en la tabla 5—, que es la unidad más pequeña: 1 ether equivale a 1 wei seguido de dieciocho ceros.

En general, hay dos tipos de cuentas: las cuentas de propiedad externa (EOA, por sus siglas en inglés), controladas por claves privadas, y las cuentas de contrato, controladas por su propio código. Una cuenta de propiedad externa no tiene código y puede, a través de su monedero (llavero), enviar

mensajes mediante la creación y firma de transacciones. Cada vez que una cuenta de contrato recibe un mensaje, su código se activa, lo que le permite leer y escribir en el almacenamiento interno y enviar otros mensajes o crear contratos uno por uno. Los contratos, al igual que las EOA, tienen direcciones y pueden enviar y recibir ether. Sin embargo, solo las EOA pueden iniciar transacciones.

Como se mencionó en el primer capítulo, el libro amarillo, escrito por Gavin Wood y titulado *Ethereum: un libro generalizado y seguro de contabilidad descentralizado para las transacciones*, es un documento de carácter técnico. En él se señala que la máquina virtual de Ethereum (EVM) es una máquina de Turing cuasicompleta. El prefijo cuasi se añade porque la ejecución de los contratos inteligentes está intrínsicamente limitada por el parámetro denominado gas (véase el glosario), que acota la cantidad total de cómputo a realizar. Las comisiones se expresan en gas, unidad de costos fundamental en la red. Esta se paga exclusivamente en ether y se convierte en gas conforme es requerida. El gas no existe fuera de la EVM. Su precio total es determinado por el tiempo de uso de la cadena de bloques y la complejidad de las operaciones que realizan. Dado que el ether se emplea para ejecutar contratos inteligentes —los cuales se procesan en la EVM— y que los nodos de la red están distribuidos globalmente, Gavin Wood y los seguidores de la red de Ethereum consideran la EVM como la «computadora mundial».

La máquina virtual de Ethereum es parte fundamental del modelo de ejecución asociado a cada cuenta. Puede compararse con una unidad central de procesamiento (CPU) que normalmente existe en las computadoras comunes. Todos los nodos de la red Ethereum operan la EVM y ejecutan las transacciones de las cuentas. Para facilitar el desarrollo de contratos inteligentes, los desarrolladores de Ethereum crearon un programa denominado Solidity, de alto nivel. Este lenguaje se compila posteriormente en un código de bytes o código intermedio (*bytecode*), que puede ejecutar la EVM (código Geth). Entre estos dos puntos se establecen una serie de códigos opcionales (*opcodes*), es decir, instrucciones predefinidas. Del mismo modo que la EVM ejecuta directamente el código de bytes, una CPU física ejecuta directamente el código binario de máquina.

Una analogía útil para comprender el código intermedio es la traducción entre lenguas poco comunes. Por ejemplo, si se desea traducir del español al luxemburgués y no se dispone de un traductor directo, puede emplearse una lengua intermedia, como el inglés, para realizar primero la traducción al inglés y, posteriormente, del inglés al español.

La EVM procesa las transacciones de manera secuencial hasta terminar un bloque. Cada vez que la EVM procesa una transacción, el estado de las cuentas y su saldo correspondiente es actualizado. Cada transacción cambia el estado de la cadena de bloques. De esta forma, cada usuario puede ver sus saldos a lo largo del tiempo.

Este modelo resulta más sencillo que el utilizado por Bitcoin, basado en las transacciones de salida no gastadas (UTXO, por sus siglas en inglés). El modelo contable de Bitcoin se asemeja al uso de efectivo en la vida cotidiana: al realizar una compra, se entregan billetes o monedas y se recibe cambio por la diferencia. Ese cambio puede equipararse a una transacción de salida no gastada o, en su defecto, se puede decir que el Bitcoin se registra con sus monedas no gastadas. El Bitcoin se basa en los cambios de los estados de las monedas no gastadas. En el modelo UTXO, los usuarios no pueden obtener su saldo de la cadena de bloques y tienen que recurrir a sus monederos para que sean calculados y se les dé a conocer. En este sistema, las monedas de Bitcoin no son completamente fungibles, ya que su protocolo considera que no todas las monedas son iguales y que cuando una moneda es usada (consumida), otra es creada, de forma tal que las entradas de cada transacción (*inputs*) deberían ser iguales a las salidas (*outputs*) que representan las monedas no gastadas. Las entradas y las salidas no son iguales, ya que en estas últimas se contabilizan las recompensas que reciben los mineros (3.125 BTC) y las comisiones cobradas por los mismos. Estas dos partidas quedan registradas en la transacción base de cada bloque (*coinbase transaction*). Bitcoin adopta este diseño para evitar el doble gasto y reforzar la privacidad con el uso de múltiples direcciones. Bitcoin usa UTXO para evitar que una misma transacción pueda reutilizarse fraudulentamente.

El libro beige fue publicado por Micah Dameron y expone «una especificación técnica de Ethereum». Curiosamente, es el libro menos técnico de todos, y es ahí donde se establece que el protocolo de Ethereum es determinístico, aunque, en la práctica, pueda operar de manera infinita o sin límites. El protocolo tiene dos funciones básicas. La primera consiste en proporcionar acceso global a un estado inicial único. La segunda es actuar como una máquina virtual que aplica cambios al estado inicial.

En la actualidad hay una gran variedad de proyectos que se basan en Ethereum, entre los que destacan Uniswap, MakerDAO, Aave, Curve Finance y 1inch. Derivado de esto, hay varias implementaciones del protocolo que están descritas en diferentes lenguajes de programación; sin embargo, la considerada implementación oficial es el Go-Ethereum (Geth).

Para ejecutar ciertos contratos inteligentes es necesario recurrir a datos externos que se encuentran fuera de la cadena de bloques. Por ejemplo, en los mercados de derivados de acciones se necesita obtener los precios de las acciones cotizadas en el NYSE o en el Nasdaq. Esto exige algún tipo de puente para conectar la vida real con la cadena de bloques. Este problema de Ethereum y de otras cadenas de bloque se denomina «problema de los oráculos». El término alude a la mitología griega, donde los oráculos servían, al menos en teoría, como intermediarios entre el mundo real y los dioses. En Ethereum, se refiere al mecanismo mediante el cual determinados nodos pueden acceder a información externa verificable.

En septiembre de 2022, Ethereum cambió su mecanismo de consenso, pasando de prueba de trabajo (POW) a prueba de participación (POS), lo que redujo el consumo de energía eléctrica en un 99 %. A partir de este cambio, los validadores ya no cobran comisiones por procesar las transacciones, sino por el cobro del consumo o renta de la cadena de bloques.

El 29 de septiembre de 2025, Ethereum recibió un reconocimiento importante por parte de la red SWIFT (Sociedad de las Telecomunicaciones Financieras Interbancarias), mencionada en el primer capítulo de este libro. Esta empresa trabaja con cerca de 11,500 instituciones corresponsales. Sin embargo, debido a que las transferencias transfronterizas pueden tomar varios días en liquidarse, ha perdido mercado frente al uso de las monedas estables, que permite completar estas operaciones en minutos u horas. En respuesta, SWIFT anunció el desarrollo de una cadena de bloques privada en la segunda capa de Ethereum, en colaboración con 34 instituciones financieras importantes (entre ellas J. P. Morgan, HSBC, Santander, Wells Fargo y Deutsche), y la empresa privada Consensys, liderada por Joseph Lubin, cofundador de Ethereum, y responsable del diseño del prototipo. Esta iniciativa busca complementar su sistema de mensajería con una infraestructura interoperable de pagos. El sistema operará en tiempo real, las 24 horas del día, los siete días de la semana, y liquidará las transferencias internacionales mediante depósitos tokenizados y contratos inteligentes. Se trata de un ejemplo representativo de cómo el sistema financiero formal ha incorporado tecnologías de registros distribuidos para ofrecer servicios de manera más rápida y con menores costos. Aunque aún no se ha dado una fecha para su implementación, el proyecto posee un alcance significativo, pues pretende integrar las finanzas tradicionales con las de las finanzas descentralizadas.

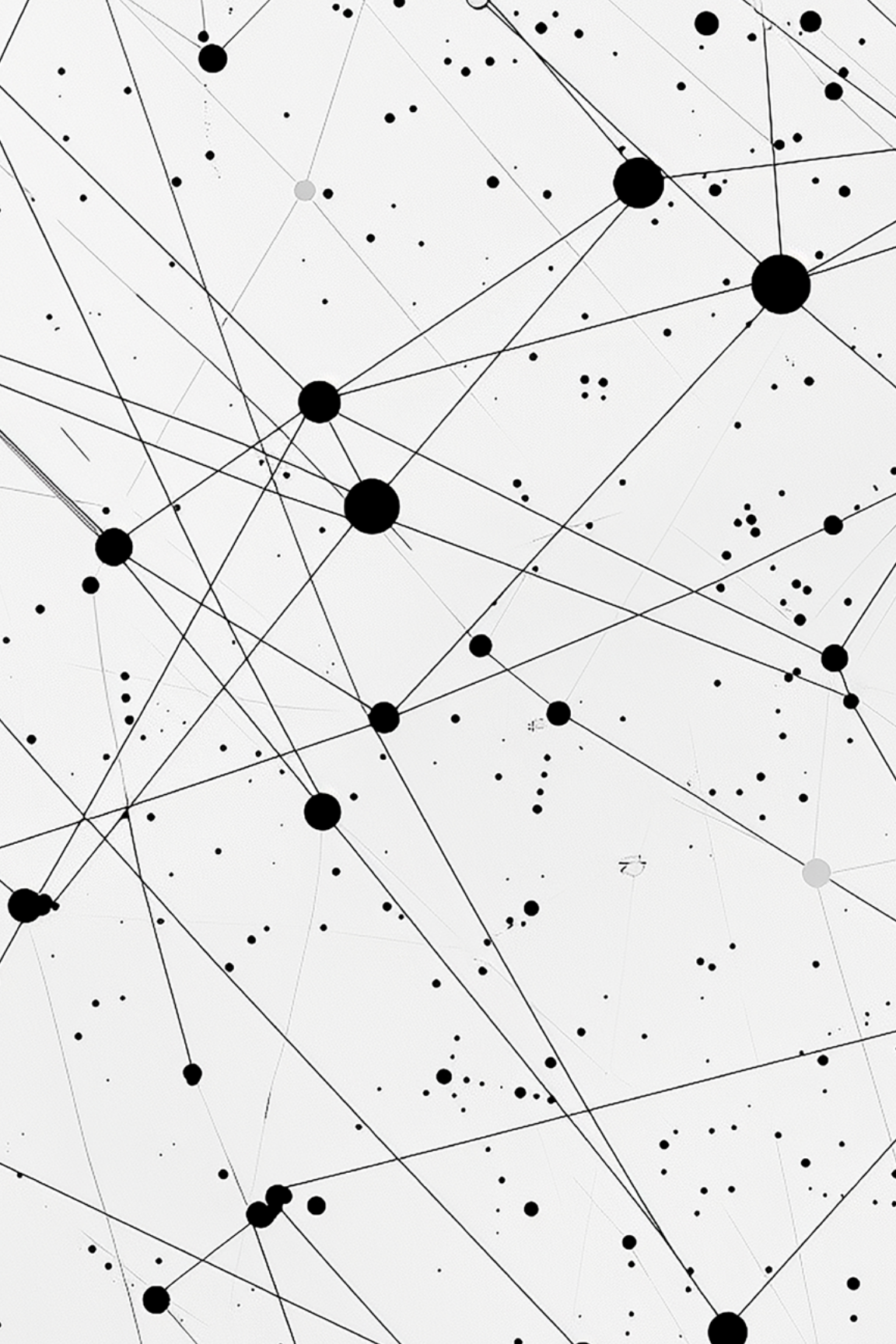
Lo anterior refuerza el liderazgo de Ethereum en el corto plazo para la implementación de aplicaciones descentralizadas. No obstante, tiene gran-

des competidores como Solana, Cardano y Polkadot. Cabe destacar que esta última plataforma fue desarrollada por Gavin Wood, autor también del libro amarillo de Ethereum.

Aunque en la tabla 5 del primer capítulo se presenta una comparación general entre Bitcoin y Ethereum, se reitera que sus monedas nativas tienen políticas y visiones distintas. En el caso de ether, su política monetaria no está limitada y su visión principal es ser implementada para el consumo de su cadena de bloques. No fue concebido prioritariamente como sustituto de las monedas fíat para pagos generalizados. Asimismo, mientras que la cadena de bloques de Bitcoin solo sirve para procesar las transacciones y almacenarlas de manera segura, Ethereum amplió ese alcance al permitir que su cadena de bloques guarde programas de cómputo y los ejecute, así como el registro de sus resultados. Bitcoin ha introducido cambios relativamente limitados en sus protocolos, mientras que Ethereum los cambia constantemente para mejorar.

Nate Silver, en su libro *Al límite*, tiene una sección titulada «Bitcoin es de Marte, Ethereum es de Venus». En ella relata una entrevista con Vitálik Buterin, quien explicó que el lanzamiento de Ethereum recibió fuertes opiniones y obstáculos de los libertarios de Bitcoin, cuyos defensores consideraban que esta debía ser la única criptomoneda relevante. Ante ello, Buterin señaló: «Bitcoin no es realmente un proyecto tecnológico: es una especie de proyecto político, cultural y religioso donde la tecnología es un mal necesario». Persiste cierta rivalidad entre los dos proyectos con mayor valor de capitalización del espacio.

Silver sugiere que la posición número uno de Bitcoin puede explicarse, en parte, mediante la teoría de juegos y, específicamente, el dilema del prisionero: los participantes coordinan sus acciones en foros y comunidades de confianza para sostener el sistema. Mientras exista confianza, pueden formarse burbujas prolongadas. A ello se suma el hecho de que Bitcoin fue la primera en el tiempo y que mantiene una política monetaria con un límite máximo de emisión de 21 millones de unidades. La competencia continuará, dada la magnitud de los intereses económicos en juego.



Anexo 3

Solana y SOL

El cofundador principal de Solana, Anatoly Yakovenko, escribió la versión original del libro blanco entre 2017 y 2018, documento que ha sido actualizado en diversas ocasiones. La versión más reciente puede descargarse en el sitio oficial, bajo el título *Una nueva arquitectura para una cadena de bloques de alto rendimiento (V0.8.13)*.

Una de las innovaciones que ha permitido a Solana alcanzar una cadena de bloques de alta velocidad, con tiempos mínimos de confirmación y bajas comisiones en las transacciones, es que complementa su mecanismo de consenso —prueba de participación— con una prueba del historial (PoH, por sus siglas en inglés). Esta última equivale, en términos conceptuales, a incorporar un reloj dentro de la cadena de bloques, lo que permite demostrar que una transacción ocurrió antes o después de otra. Solana utiliza el algoritmo SHA-256 junto con una función de retraso verificable para crear un registro histórico y ordenado de las transacciones dentro de la cadena de bloques. Para ello, utiliza el *hash* de la operación anterior para generar uno nuevo de forma continua. El *hash* se utiliza para asignar sellos o marcas de tiempo únicas e imposibles de falsificar.

La red cuenta con un líder, designado por los 1,502 nodos validadores, encargado de generar la secuencia de la prueba del historial. El líder cumple su función durante un periodo determinado, que dura entre dos y tres días; para después dejar su posición a otro validador designado. En términos técnicos se afirma que el líder opera durante una época (*epoch*), la cual comprende 432,000 franjas horarias (*slots*), cada una con una duración mínima de 400 milisegundos por bloque. El tiempo para procesar un bloque es variable. Al momento de redactar este texto, habían transcurrido 755 épocas desde el inicio de operaciones de Solana en 2020.

El diseño de la arquitectura de la red funciona de la siguiente manera: el líder recibe todas las transacciones para generar la prueba del historial y ordenarlas cronológicamente. Posteriormente, el líder ejecuta estas transacciones, arma los bloques, los firma digitalmente y los propaga para facilitar el trabajo de los validadores. Estos últimos ejecutan los mismos bloques con transacciones en sus nodos, los ratifican con sus firmas y devuelven al líder. Estas confirmaciones constituyen votos para el algoritmo de consenso. Los validadores confirman los bloques en un tiempo menor al que requirió el líder para generarlos.

Para entender el funcionamiento técnico de Solana es vital conocer su terminología. En esta red, las cuentas de Solana no se limitan a direcciones únicas de 256 bits con saldo en la moneda nativa; también pueden representar archivos que sirven para almacenamiento. Los contratos inteligen-

tes en Solana son denominados programas; están escritos en el lenguaje Rust y pueden considerarse un tipo especial de cuenta. Tanto los programas como las transacciones no tienen estado propio (*stateless*), es decir, no almacenan directamente, aunque sí pueden leer y escribir datos a otras cuentas, lo que permite ejecuciones en paralelo. Aunque técnicamente Solana no emplea bloques de transacciones, el término se utiliza con fines comparativos respecto de las primeras plataformas del mercado. Las transacciones son agrupadas en lotes que contienen los registros o asientos contables (*entries*), los cuales pueden ser votados o confirmados por los validadores. Estos registros o asientos pueden considerarse funcionalmente equivalentes a un bloque de datos.

El libro blanco describe estos registros de Solana, pero no desarrolla con detalle la moneda SOL. Para profundizar en este aspecto es necesario recurrir a la documentación oficial. La moneda nativa de Solana se usa para cubrir el uso de la red (renta de almacenamiento), pagar comisiones derivadas de las transacciones y otorgar recompensas a validadores y delegantes. No existe un límite para la acuñación o emisión de esta moneda, aunque sí reglas relacionadas con sus incrementos anuales, así como otras relacionadas con su quema.

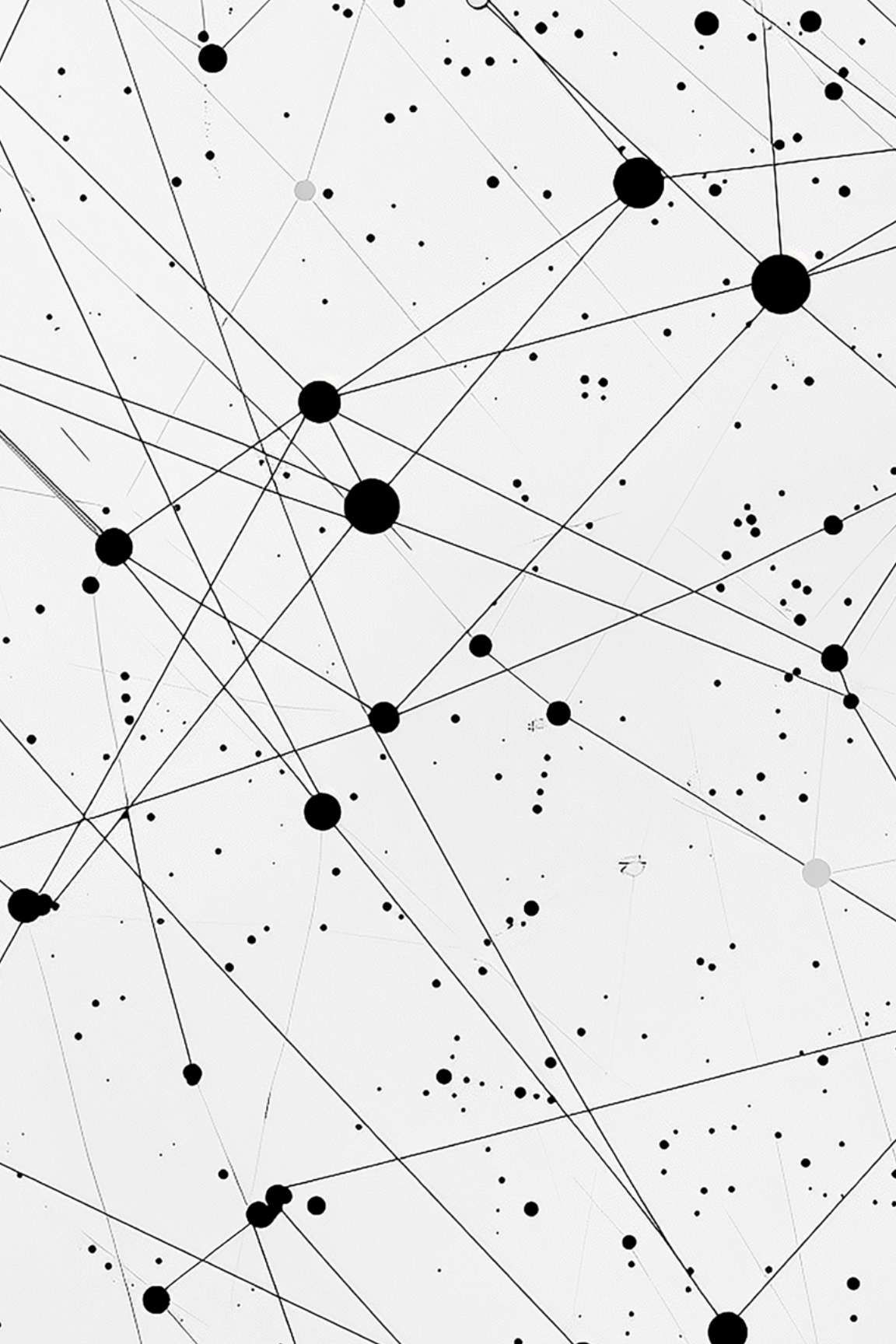
La oferta total de monedas (fichas o tókenes) en 2020 fue de 500 millones de SOL, distribuidos entre inversionistas privados —grandes y pequeños— y la comunidad. Una parte significativa se asignó a Solana Labs Inc. (EE. UU.), la Fundación Solana (Suiza), y los desarrolladores. Posteriormente, el 28 de abril de 2020, Anatoly Yakovenko anunció la quema de 11.36 millones de SOL, con lo que la oferta total se redujo a 488.6 millones de fichas. Entre los grandes inversionistas se encontraba Sam Bankman-Fried a través de Alameda Research y FTX, que metieron en aprietos temporales a Solana. Sam Bankman-Fried fue declarado culpable de fraude, conspiración y lavado de dinero en noviembre de 2023 y sentenciado a 25 años de cárcel en abril de 2024. Durante el proceso de quiebra y liquidación de Alameda Research y FTX, se informó que aproximadamente 36,000 clientes podrían recuperar una parte sustancial del capital invertido.

Con el fin de financiar las recompensas para validadores y delegantes, Solana y su comunidad decidieron emitir nuevas monedas , lo cual comenzó con un incremento anual del 8 %, seguido de reducciones progresivas durante los diez años posteriores, hasta estabilizarse en una inflación del 1.5 % anual. Al momento de redactar este texto, la recompensa que reciben los validadores que apuestan, empeñan o pignoran (*stake*) se sitúa en torno al 5 % anual.

Por otro lado, la mitad de las comisiones por transacción que pagan los usuarios son destruidas (quemadas), mientras que el 50 % restante le corresponde al líder actual que procesa la transacción. Los incrementos en las recompensas representan una cantidad mayor que las comisiones quemadas, por lo que se puede afirmar que en la actualidad SOL es una moneda inflacionaria. Esta afirmación se corrobora al comparar la oferta total actual de SOL (609.4 millones) con los 488.6 millones registrados en 2020. Conviene precisar que, a la fecha, la oferta en circulación asciende a 542.3 millones; sin embargo, no se dispone de información suficiente para identificar a las personas o instituciones propietarias de estas fichas. El aumento sostenido en la emisión de SOL contrasta con ether que, tras el cambio del mecanismo de consenso a la prueba de participación en septiembre de 2022 y hasta marzo de 2024, y en combinación con otros factores, logró una ligera disminución de la oferta total. Por ello, puede considerarse que ether fue deflacionaria en ese periodo. A pesar de ello, la situación de ether cambió en el segundo trimestre de 2024, cuando volvió a presentar inflación tras la emisión de más de 200,000 unidades. En este contexto, los inversionistas disponen de distintas alternativas: bitcoin tiene un límite; ether presenta una oferta total que fluctúa; y SOL conserva, hasta ahora, una dinámica inflacionaria predominante.

Otra circunstancia relevante para Solana fue la mención de la Comisión de Valores y Bolsa de los Estados Unidos respecto de la posible consideración de SOL como valor. Esta referencia aparece en la demanda interpuesta por la SEC contra Binance el 5 de junio de 2023. En la página 85 del documento se señala que las plataformas de Binance negociaban activos considerados como valores, entre ellos SOL (Solana), ada (Cardano) y otros más. Posteriormente, en julio de 2024, la SEC retiró su solicitud de estatus de valor para SOL, ada (Cardano) y matic (Polygon). Ello no implica necesariamente que haya declarado explícitamente que SOL no sea un valor. La situación fue muy confusa. Por un lado, algunos la entendieron como una estrategia de litigio, más que como un cambio de política; otros consideraron que respaldaba la postura sostenida por la Fundación Solana, que ha defendido que SOL no debe clasificarse como valor. El panorama regulatorio experimentó nuevos ajustes en 2025, tras los cambios de orientación normativa impulsados por el presidente Trump. En ese contexto, Solana ha manifestado su intención de solicitar autorización para operar un ETF al contado en Estados Unidos.

Actualmente, Solana (séptima en la tabla 4) compite de forma directa con Ethereum (segunda), y ambas constituyen las principales plataformas sobre las que se desarrollan las aplicaciones de las finanzas descentralizadas (DeFi). Asimismo, otras redes como Tron (octava en la clasificación de CoinGecko) y Cardano (ubicada en el lugar 12) compiten en el segmento de cadenas de bloque generales. Esta descripción corresponde al momento de redacción, aunque en el ámbito de los criptoactivos, la constante es la transformación del entorno tecnológico y regulatorio.



Anexo 4

Tecnología de registros distribuidos (TRD) y cadenas de bloques

Se inicia este anexo con las definiciones que el Reglamento de la Unión Europea 2023/1114 ofrece sobre la TRD y los registros distribuidos. Ambas se encuentran en el artículo 3 de esta disposición relativa a los mercados de criptoactivos (MiCA). En dicho artículo se establece que la

> *TRD es una tecnología que permite el uso y el funcionamiento de registros distribuidos", y estos últimos lo define como "un repositorio de información que mantiene registros de operaciones y se comparte a través de un conjunto de nodos de red TRD y está sincronizado entre dichos nodos, utilizando un mecanismo de consenso. (p. 63)*

El reglamento no define el concepto de tecnología. En términos generales, puede entenderse como el aprovechamiento práctico del conocimiento científico. De ahí la expresión «ciencia y tecnología». Sin embargo, en un sentido amplio, el término también abarca técnicas desarrolladas con anterioridad a la formalización de las ciencias, como es el caso de la escritura, la imprenta o la lectura.

También es importante aclarar el tipo de registros al que hace referencia. Desde antes de la era común existen registros textuales o numéricos de una sola partida. En 1494 se generaron los registros por partida doble con la creación de la contabilidad financiera de Luca Paccioli. Hoy, tenemos la contabilidad de partida triple (Ian Grigg, 2005), en la que la contabilidad de partida doble se puede complementar con la firma digital que usa criptografía asimétrica para fortalecer la integridad del sistema. No todos los registros son equivalentes: la tecnología aquí analizada se refiere específicamente a registros distribuidos vinculados a redes descentralizadas.

El concepto de repositorio de información puede equipararse al de base de datos. Antes de 2009 predominaban bases de datos centralizadas; aunque desde la implementación de Bitcoin surgió una de las principales aplicaciones de la tecnología de registros distribuidos: la cadena de bloques.

A partir de lo anterior, puede afirmarse que la TRD es una base de datos digital con múltiples copias distribuidas entre varios participantes, que se actualizan de manera sincronizada a través de internet. De acuerdo con José Luis Romero (2018, p. 3), esta tecnología de registros distribuidos

resulta de la combinación de tres elementos: (a) una red entre pares, abreviada como P2P, (b) criptografía y (c) algoritmos de consenso.

Dado que en el primer capítulo y en los anexos 1, 2, y 3 se analizaron los algoritmos de consenso y la criptografía asimétrica, en esta sección hablaremos de las redes entre pares (P2P). No obstante, conviene señalar brevemente que existen distintas formas de aplicar la TRD. La principal es la cadena de bloques, cuya implementación inició con Bitcoin en 2009. Según su modalidad de acceso, las cadenas de bloques descentralizadas o distribuidas pueden ser públicas, privadas o híbridas. Las públicas —también llamadas de permiso abierto (no restringido)— permiten la participación de cualquier persona para entrar y salir de la red correspondiente. Bitcoin es el ejemplo típico de esta cadena de bloques. Las privadas (de acceso restringido, cerradas o administradas) requieren autorización para operar en la red, en donde se requiere de autorización para todos aquellos que quieran entrar a operar. Una vez adentro, la salida de la red es mucho más fácil de realizar. La Fundación Linux ha patrocinado la creación de una plataforma común y universal para las cadenas de bloques llamada Fabric (Hyperledger Project). En particular, el sector financiero y bancario, junto con R3, diseñó una cadena de bloques privada (cerrada) conocida como Corda (R3 CEV LLC con sede en Nueva York). En esta red, únicamente las partes contratantes (nodos) realizan las anotaciones, las cuales no son de acceso público. Entre sus aplicaciones destaca la emisión de monedas digitales de bancos centrales (CBDG). Las redes híbridas, por su parte, tienen características de las dos anteriores. Un ejemplo de un proyecto híbrido es XRP, ya mencionado en este libro. Conviene reiterar que tiene una red pública (abierta) para el desarrollo de nuevas aplicaciones, y al mismo tiempo, de un esquema operativo restringido a un número reducido de nodos, representados por bancos, CEX y universidades.

Aunque no es el objetivo de este documento, existen otras formas de implementar la TRD, como (a) los diagramas (grafos) acíclicos dirigidos (DAG, por sus siglas en inglés), que son utilizados para procesar micropagos y nanopagos de manera masiva en el internet de las cosas; y (b) Holochain, que propone una arquitectura centrada en los agentes en lugar de una centrada en los datos.

Retomando el tema de las redes entre pares, conviene señalar que no todas las redes representan la misma estructura. En la primera parte de este documento, al abordar el sistema financiero mexicano, se reportó que entre los intermediarios financieros que concentraban los registros de los usuarios estaban los bancos múltiples y las compañías de seguros. Tam-

bién se afirmó que las autoridades financieras comprendían al Banco de México y a la Secretaría de Hacienda y Crédito Público, esta última con control directo sobre los organismos desconcentrados e indirecto sobre los organismos descentralizados. Es decir, se describieron intermediarios centralizados, organismos desconcentrados y organizaciones descentralizadas. Del mismo modo, los registros consignados en el acta de nacimiento, la credencial de elector, el título universitario y el estado de cuenta bancario son emitidos por un ente central, es decir, proviene de una red centralizada, ya sea el registro civil, la autoridad electoral, la universidad o el banco correspondiente. Sin embargo, desde la aparición de internet con fines comerciales a partir de 1993, han aparecido registros y redes descentralizadas, entre las que destacan Bitcoin y Ethereum.

Surge entonces la pregunta: ¿cuál es la diferencia entre una red distribuida y una descentralizada? Para contestar esta interrogante, es pertinente aludir a los trabajos de Paul Baran (1926-2011), ingeniero informático estadounidense de origen polaco, quien explicó las diferencias entre las redes centralizadas y descentralizadas y agregó una tercera categoría: la red distribuida.

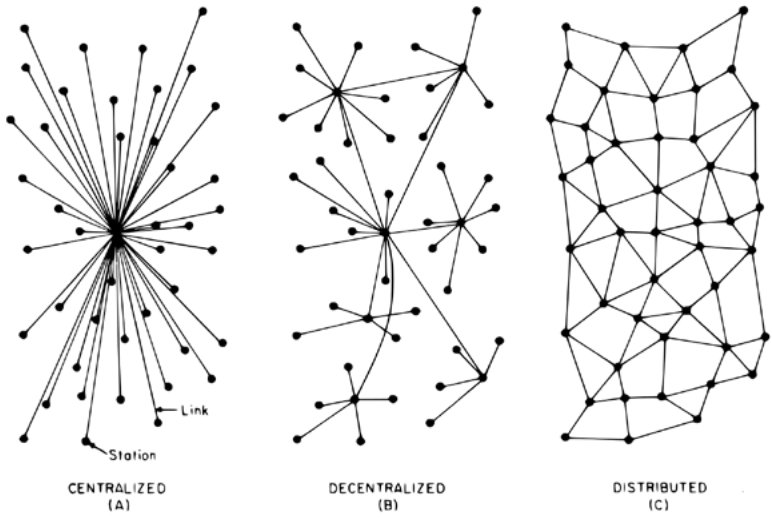


Figura 2. Las redes de Paul Baran
Fuente: *On distributed communications networks* (1964).

En esa época se tenía clara la diferencia entre redes centralizadas (todos los nodos eran conectados directamente a un punto focal o a un interruptor) y las descentralizadas, conformadas por diferentes núcleos interconectados. En este último caso, cada nodo individual dependía del adecuado funcionamiento de su núcleo y de la ruta que lo enlazaba con él. Durante la crisis de los misiles en Cuba (1962), Baran propuso una tercera alternativa: la red distribuida, diseñada para aumentar la resiliencia de los sistemas de comunicación. En este modelo, múltiples estaciones principales podrían comunicarse entre sí incluso después de un ataque, ya que cada nodo dispondría de diversas rutas para transmitir datos. Si una ruta o un nodo vecino resultaban destruidos, existirían trayectorias alternativas.

Este planteamiento dio lugar a un debate que se mantiene hasta hoy. Algunos investigadores mantienen la triple clasificación, mientras que otros prefieren considerar las redes centralizadas (aquellas con una sola unidad de control) y descentralizadas (las que carecen de ella).

En los párrafos anteriores se ha señalado que los registros se califican como distribuidos y que las cadenas de bloques de Bitcoin y Ethereum son consideradas como descentralizadas. Dado que no existe consenso absoluto para diferenciar ambos conceptos, en este documento se emplearán como sinónimos.

Con este antecedente, es importante especificar que, cuando se habla de redes y registros descentralizados o distribuidos en el ámbito de las criptomonedas, normalmente se refiere a su funcionamiento y operación. En este sentido, la ejecución podrá realizarse por nodos cuyo número podrá ser de dos o cinco dígitos, y todas las redes serán descentralizadas en mayor o menor medida. La descentralización es un término relativo.

La siguiente pregunta que se tiene que hacer en el ámbito de las criptomonedas es: ¿es preferible usar una red gestionada por casas de intercambio centralizadas (CEX) o una red descentralizada (DEX), en la que el usuario conserva la custodia de las monedas?

Cada una de las redes tiene ventajas y desventajas. No obstante, se evaluarán los desafíos actuales de las redes descentralizadas en general, particularmente de Bitcoin y Ethereum. Para hacer más fácil la comparación, en este apartado no se incluye a Solana, cuya cantidad de nodos activos es significativamente menor que la de Bitcoin y Ethereum.

Como se mencionó en el capítulo 1, una de las respuestas puede describirse mediante el trilema de las cadenas de bloques públicas y descentralizadas, término acuñado en 2018 por el cofundador de Ethereum, Vitá-

lik Buterin. Este plantea que las tres principales características de una red pública deberían ser la descentralización, la seguridad (la protección de los datos y la información), y la escalabilidad (ampliable). Afirma que para el diseño de la red solo se pueden lograr dos de las tres propiedades, por lo que se debe elegir. Existen tres opciones: (a) una red segura y descentralizada, pero no escalable; (b) una red escalable y descentralizada, pero no segura; y (c) una red escalable y segura, pero no descentralizada. Son decisiones mutuamente excluyentes. En el caso de Ethereum, se optó por priorizar la descentralización y la seguridad, con la desventaja de una escalabilidad limitada en términos de velocidad (29 operaciones por segundo), aunque mayor que la que tiene Bitcoin (siete operaciones por segundo).

Las operaciones realizadas a través del sistema financiero se pueden considerar, en lo general, seguras y escalables, pero no son descentralizadas. Buterin ha subrayado que su trilema es una hipótesis válida con la tecnología actual; sin embargo, se trata de una cuestión abierta que podría modificarse con el avance tecnológico. Existen proyectos que indican que en 2026 el trilema quedará superado.

Si en lugar de aplicar el concepto de la descentralización a la operación de los registros, la aplicamos al ámbito de la gobernabilidad del proyecto, de la empresa o de la fundación, la situación cambia radicalmente. Nadler y Schär (2020), en su artículo «¿Finanzas descentralizadas, propiedad centralizada?», proponen un modelo iterativo para medir adecuadamente la distribución de tókenes de gobernanza y concluyen que existe una estructura de propiedad concentrada en todo el espacio. Su respuesta es afirmativa: sí, existe una concentración en la propiedad de los protocolos de las finanzas descentralizadas.

La revista trimestral del Banco de Pagos Internacionales, en su edición de diciembre de 2021, publicó el artículo «Los riesgos de las finanzas descentralizadas» y la ilusión de la descentralización. Sus tres autores Aramonte, Huang y Schrimpt sostienen que:

> *Todas las plataformas de las finanzas descentralizadas tienen un elemento de centralización, que típicamente se desarrolla alrededor de los que poseen los tokens de gobernanza (frecuentemente los desarrolladores de las plataformas) que votan las propuestas, de una manera no muy diferente a como lo hacen los accionistas de una empresa. Este elemento de centralización puede servir como la base para reconocer estas plataformas como entes legales similares a una*

> *corporación. Mientras los sistemas legales están en una primera etapa de adaptación, a las organizaciones autónomas descentralizadas (DAO), que gobiernan muchas de las aplicaciones de las finanzas descentralizadas, se les ha permitido registrarse como compañías de responsabilidad limitada en el estado de Wyoming en los Estados Unidos desde mediados de 2021. (p. 28)*

Asimismo, las DAO son consideradas estructuras legales en Tennessee, Vermont, Suiza, Liechtenstein y las Islas Caimán, donde quedan sujetas a la regulación de cada jurisdicción. Sin embargo, dado que pueden operar alrededor del mundo a través de internet, su estatus legal no es del todo claro. En 2023 existían más de 4,000 DAO en el mundo y, hasta donde llega nuestro conocimiento, no existe ninguna registrada en México.

Uno de los problemas derivados de la concentración en los órganos de gobierno de las plataformas de las finanzas descentralizadas es que puede facilitar la colusión y limitar la vida de las cadenas de bloques.

El Banco Central Europeo, en su Boletín Macroprudencial de julio de 2022, incluyó el artículo «Finanzas descentralizadas-un nuevo sistema no bancario no regulado», escrito por Born, Gschossmann, Hodbod, Lambert y Pellicani. Los autores concluyen que los protocolos o las plataformas de las finanzas descentralizadas afirman contar con una estructura de gobernanza descentralizada, aunque en la práctica su gobernabilidad está frecuentemente concentrada. Reiteran que la gobernabilidad está fundamentada en los derechos de voto que otorgan los tókenes, así como en su participación en las organizaciones autónomas descentralizas (DAO). Afirman:

> *Los poseedores de los tokens de gobernabilidad pueden influenciar las principales características del protocolo, así como los depósitos requeridos para las votaciones y la elegibilidad de los activos. Aunque en principio los derechos o tokens de gobernabilidad pueden ser detentados por diversos grupos, en esta etapa los tokens están frecuentemente en manos de los desarrolladores, de los inversionistas iniciales o aquellos que tienen grandes saldos, lo que sugiere una propiedad institucional. Por ejemplo, el 80 % de los tokens de gobernanza de la oferta total en circulación de Uniswap*

(UNI) están en manos de su equipo, inversionistas iniciales y aquellos que mantienen saldos por arriba de un millón de UNI. Además, el 1 % del total de tokens que poseen una dirección son propietarios del 97 % del total de la oferta de token de gobernanza.

Una vez más, la conclusión es que la estructura de gobierno de las plataformas o protocolos tiene un alto nivel de concentración. La gran mayoría de las criptomonedas y de las finanzas descentralizadas (DeFi) se crearon para evitar los intermediarios tradicionales como los bancos y las casas de bolsa. A pesar de ello, en la práctica el usuario debe operar mediante nuevos intermediarios digitales.

¿Prefiere depositar su dinero fíat en el banco BBVA o convertirlo en una criptomoneda para operar con Uniswap (DEX)? ¿Prefiere invertir su dinero fíat en la casa de bolsa Inbursa o transformarlo en una moneda estable para operar en PancakeSwap (DEX)?, o ¿prefiere tener como intermediario a un ente altamente regulado o uno con escasa supervisión?

Para terminar, retomamos el título de este libro: *Finanzas descentralizadas en México: ¿advertencia u oportunidad?* Existen, sin duda, oportunidades en los servicios financieros descentralizados por su eficiencia, rapidez y menores costos derivados del uso de tecnologías de registro distribuido (TRD), pero también es un hecho que las autoridades monetarias y financieras han advertido constantemente de los riesgos involucrados en este ecosistema. En consecuencia, la decisión es personal; no obstante, cualquiera que sea la alternativa elegida, resulta indispensable contar con educación financiera suficiente para comprender sus implicaciones. Se espera que estas notas sirvan como un primer acercamiento al tema.

Israel Cedillo Lazcano

Doctor en Derecho por la Universidad de Edimburgo. Maestro en Gobernanza y Globalización, así como en Estudios Antropológicos de México. Es profesor-investigador de tiempo completo en el Departamento de Derecho de la Universidad de las Américas Puebla (UDLAP), así como director general de Investigación en la misma institución. Se ha desempeñado profesionalmente como asesor en materia de propiedad intelectual y protección de datos personales en diversas instituciones, y ha contribuido con reguladores e instituciones internacionales. Sus actividades de investigación se centran en la naturaleza jurídica del dinero, los riesgos operacionales en las infraestructuras comerciales y financieras, la historia económica, la propiedad intelectual y los desafíos que presenta el desarrollo y despliegue de la IA. Ha presentado su trabajo en diversos congresos y publicaciones en México y el extranjero. Recibió premios como el primer lugar de la quinta edición de la Competencia de Monografías Jurídicas para Jóvenes Abogados, organizada por la Federación Latinoamericana de Bancos (FELABAN), y el Premio Edward Elgar Publishing por su presentación en la IVR UK Branch Annual Conference 2017.

Miguel Hakim Simón

Doctor en Finanzas por la Universidad de Claremont en los Estados Unidos de América. Ha sido catedrático en la Universidad Veracruzana y en la Universidad de las Américas Puebla (UDLAP). Fue ejecutivo de casas de bolsa y bancos en el sistema financiero mexicano, y consultor externo del Banco Mundial y del Banco Interamericano de Desarrollo (BID). Se desempeñó como subsecretario de Relaciones Exteriores de México en dos ocasiones, una en temas económicos y de cooperación, otra en asuntos políticos de la región de América Latina y el Caribe. También fue secretario para la Cooperación de la Secretaría General Iberoamericana (SEGIB) con sede en España. Ha publicado cuatro libros universitarios y hoy se desempeña como asesor y consultor de empresas y gobiernos.

Universidad de las Américas Puebla

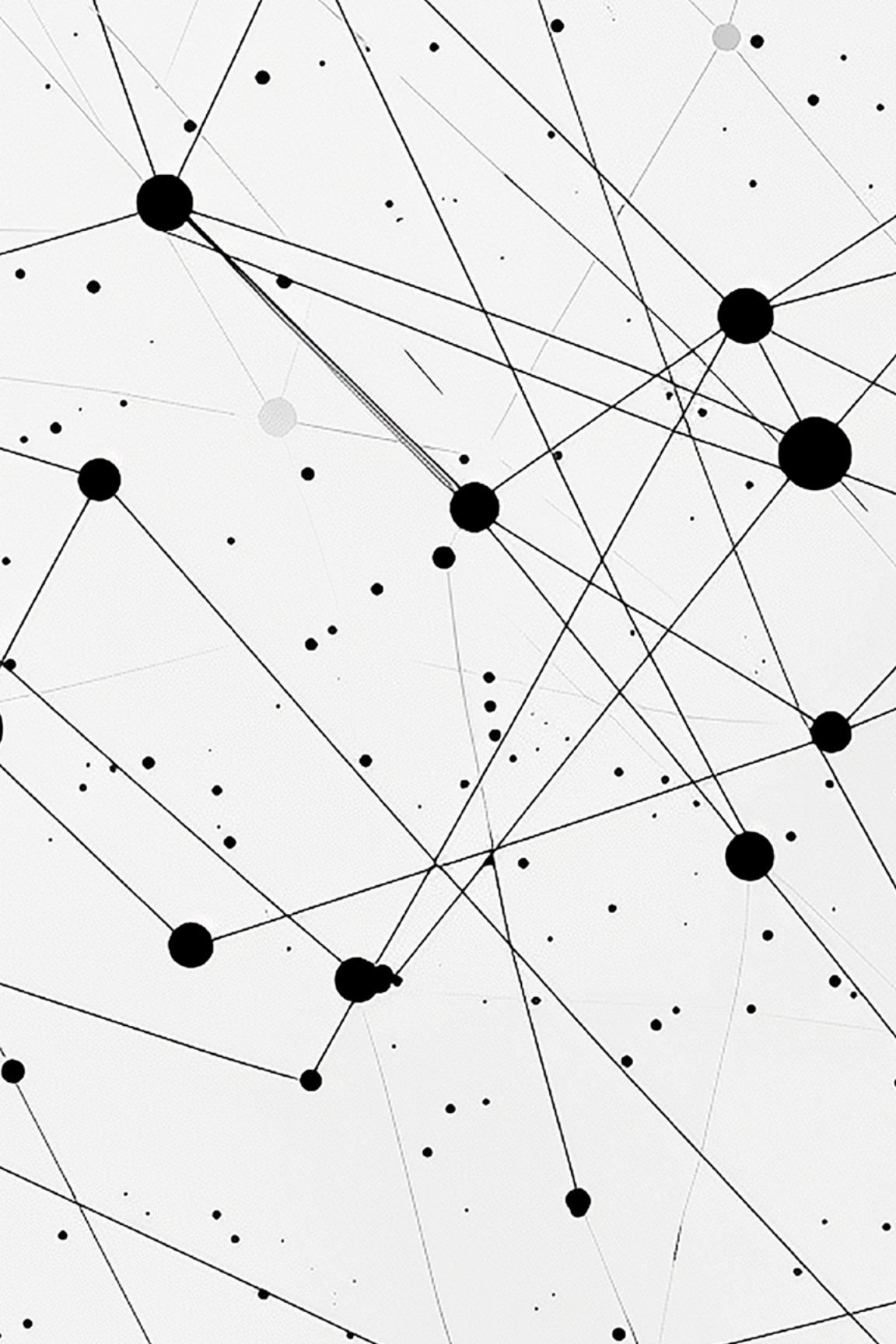
Luis Ernesto Derbez Bautista
Rector

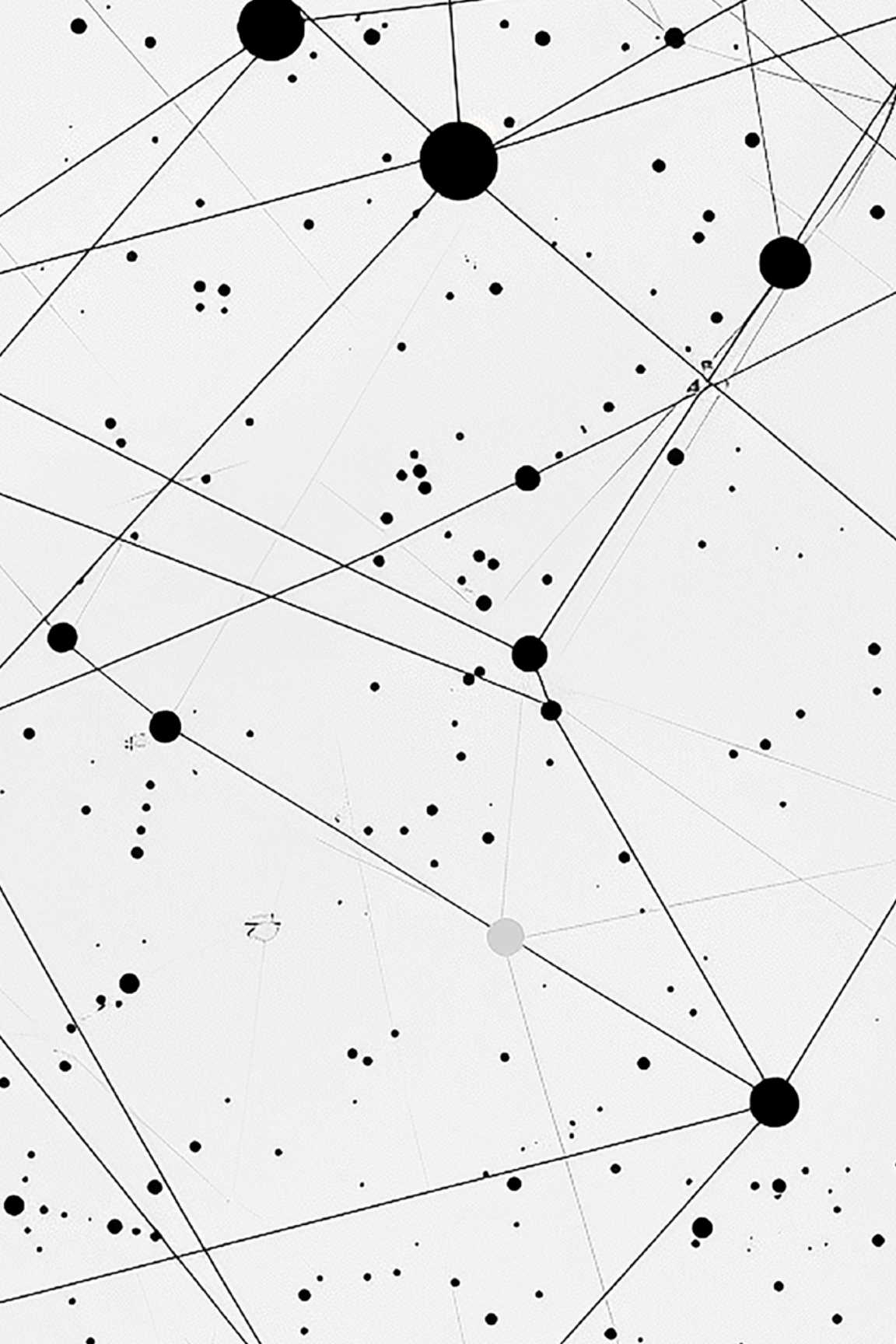
José Daniel Lozada Ramírez
Vicerrector académico

René Alejandro Lara Díaz
Vicerrector de Investigación, Posgrado y Extensión

Juan Antonio Le Clercq Ortega
Decano de la Escuela de Ciencias Sociales

Israel Cedillo Lazcano
Director general de Investigación





Finanzas descentralizadas en México

¿Advertencia u oportunidad?

fue preparado como libro electrónico en PDF por el Departamento de Publicaciones de la Universidad de las Américas Puebla, Ex hacienda Santa Catarina Mártir s. n., San Andrés Cholula, Puebla, el 15 de mayo de 2026.

Este es el primer libro universitario **integral** que explica los aspectos monetarios, legales y técnicos ligados a los servicios financieros descentralizados que son utilizados por millones de mexicanos en la economía de la denominada Cuarta Revolución Industrial.

La obra que tiene en sus manos expone los argumentos de los usuarios y de las autoridades de México en relación con las **criptomonedas** (activos virtuales o criptoactivos) y las **monedas estables** (*stablecoins*), que son parte importante de las aplicaciones informáticas descentralizadas que emulan, con innovaciones digitales, a los sistemas monetarios y financieros.

Por un lado, explica las **oportunidades** de usar las finanzas descentralizadas, comúnmente abreviadas como **DeFi**, cuyos protocolos con programas computacionales de código abierto operan por internet (24/7) de manera cuasi anónima, y favorecen la inclusión financiera, así como la realización de transferencias internacionales más rápidas con menores costos.

Por otro, detalla las **advertencias** oficiales y la falta de respaldo, tanto del Banco de México como de la Secretaría de Hacienda y Crédito Público, relacionadas con su alta volatilidad, riesgos tecnológicos, cibernéticos, legales, manipulaciones, fraudes, estafas o lavado de dinero, así como la imposibilidad de revertir operaciones con activos virtuales una vez que son ejecutadas.

Los autores consideran que algunas oportunidades son reales y las advertencias son serias, por lo que la decisión que usted tome debe estar basada en el conocimiento, el análisis minucioso y el uso de la razón. Por eso, destacan la necesidad de contar con una **mayor y mejor educación financiera**, tanto de las finanzas descentralizadas como de las tradicionales.

UDLAP®