

2025

Informe sobre criptomonedas: Bitcoin (BTC)

Una visión general de Bitcoin y sus
posibles casos de uso.

Información importante

Este material está destinado únicamente a inversores institucionales y profesionales de la inversión, y NO debe distribuirse al público en general ni ser utilizado por inversores privados.

Los activos digitales son especulativos y altamente volátiles, pueden volverse ilíquidos en cualquier momento y están dirigidos a inversores con alta tolerancia al riesgo. Quienes invierten en activos digitales podrían perder la totalidad de su inversión.

La información aquí contenida es proporcionada por Fidelity Digital Asset Services, LLC («FDAS LLC») y Fidelity Digital Assets, Ltd («FDA LTD»). Fidelity Digital Assets® fue designada por FIL para brindar liderazgo intelectual y recursos educativos, y se reproduce con su autorización. Fidelity Digital Assets es una marca de servicio registrada de FMR LLC. Fidelity Digital Assets® es una filial de Fidelity Investments, una empresa independiente y distinta de FIL.

Parte de esta información es prospectiva y está sujeta a cambios. El rendimiento pasado no garantiza resultados futuros. Los resultados de la inversión no se pueden predecir ni proyectar.

Taiwán: Esta información no debe reproducirse ni distribuirse sin autorización previa. Exclusivamente para clientes de instituciones financieras que se ajusten a la definición de «clientes de instituciones financieras» según lo dispuesto en el artículo 3, párrafos 3 y 4 del Reglamento sobre productos estructurados offshore.

Singapur: Inversores institucionales según la definición establecida en la Ley de Valores y Futuros de Singapur.



Conclusiones clave

Hechos

Bitcoin fue el primer sistema de dinero electrónico totalmente descentralizado y de igual a igual, lo que supuso un gran avance en varios campos, como la criptografía, la informática y la economía.

La palabra "Bitcoin" puede referirse a dos cosas distintas pero relacionadas: Bitcoin como red (un conjunto de reglas o protocolos que operan una red de pagos) y Bitcoin como token (un activo que reside en la red).

Bitcoin mantiene un calendario de emisión programático, lo que contribuye a su escasa oferta.

Existe un suministro máximo de 21 millones de bitcoins que no puede modificarse sin el consenso de la mayoría de la red.

La escasez de Bitcoin se sustenta en su descentralización y resistencia a la censura, características que se hacen posibles gracias a un mecanismo de consenso llamado prueba de trabajo.

Fortalezas

El bitcoin se entiende mejor como un bien monetario, y una de las principales tesis de inversión para el bitcoin es como un activo de reserva de valor en un mundo cada vez más digital.

Bitcoin suele considerarse un punto de entrada para los inversores tradicionales que buscan exponerse a los activos digitales, dadas sus características distintivas como ser la cadena de bloques más descentralizada y segura, y su trayectoria comparativamente más larga.

Bitcoin es fundamentalmente diferente de cualquier otro activo digital. Es improbable que otro activo digital supere a Bitcoin como medio monetario en el futuro, ya que es seguro, descentralizado y constituye una moneda digital sólida. Cualquier posible "mejora" conllevará inevitablemente desventajas.

El perfil de rentabilidad de Bitcoin está impulsado por fuertes factores favorables: una creciente adopción, dadas sus características como reserva de valor, en un contexto de estímulos fiscales y monetarios sin precedentes.

Debilidades

Bitcoin sacrifica complejidad y velocidad a cambio de un mayor nivel de seguridad, descentralización, integridad de la red y una estructura de incentivos que se autocorrije.

En vista de lo anterior, resulta más difícil desarrollar aplicaciones sobre Bitcoin. Realizar transacciones directamente en la capa base (Capa 1) es más lento y costoso que en las cadenas de bloques de Capa 1 más recientes.

Bitcoin no genera flujo de efectivo, y su utilidad reside en su valor percibido como activo monetario y en su tasa de adopción.

El Bitcoin es más volátil que otras clases de activos, lo que significa que su precio puede fluctuar significativamente en cortos períodos de tiempo.

Algunos gobiernos aún están trabajando en marcos regulatorios y en la protección de los inversores para este sector, lo que podría tener un impacto en la trayectoria de los precios.

¿Qué es Bitcoin y cuál es su propuesta de valor?

Bitcoin la red vs. Bitcoin la activo

Es importante aclarar que el término «bitcoin» puede referirse a dos conceptos relacionados pero distintos: Bitcoin, la red y el sistema de pago, y bitcoin, el token o activo. Este informe utiliza la capitalización de Bitcoin al referirse a la red y la minúscula para el token.

Bitcoin se presentó originalmente como una solución hipotética para abordar los desafíos asociados con la creación de un sistema de efectivo electrónico verdaderamente entre pares. Si bien las personas pueden realizar transacciones en el mundo físico sin un intermediario utilizando efectivo, no era posible hacerlo en el ámbito digital hasta la invención de Bitcoin.

Bitcoin no está gobernado por una sola persona u organización. En cambio, está compuesto por miles de computadoras que ejecutan el software Bitcoin. Esta red funciona como un protocolo simple que proporciona reglas globales que la rigen. Mediante este proceso, la red puede utilizarse como un sistema de pago donde los usuarios pueden enviar y recibir una moneda digital llamada bitcoin.

Historia y evolución del proyecto Bitcoin fue creado en 2009 por Satoshi Nakamoto, un individuo o grupo que utiliza un seudónimo, y se considera ampliamente el primer lanzamiento exitoso de un sistema de efectivo digital entre pares. Bitcoin se diferencia de los intentos anteriores de efectivo digital al introducir un mecanismo de consenso de prueba de trabajo basado en hash, combinado con firmas digitales y un marco descentralizado para evitar el doble gasto. La prueba de trabajo se analiza con mayor detalle en este informe; sin embargo, la conclusión principal es que este mecanismo permite a Bitcoin mantener su naturaleza descentralizada y sus altas garantías de liquidación.

Potencial como reserva de valor y

Bitcoin, como medio de intercambio, mantiene un calendario de emisión programático, lo que contribuye a su escasez. Existe un suministro máximo de 21 millones de bitcoins que no puede modificarse sin el consenso de la mayoría de la red.

La oferta máxima fija de Bitcoin lo distingue de muchos otros activos digitales. A diferencia de Bitcoin, numerosos tokens carecen de un límite predefinido en la oferta total o emplean mecanismos dinámicos de ajuste de la oferta. Estos enfoques pueden involucrar diversos factores económicos que dificultan la predicción de la oferta futura. En comparación, los inversores pueden estimar con mayor precisión la oferta futura de Bitcoin debido a su calendario de emisión. Bitcoin puede considerarse un método alternativo para almacenar valor a largo plazo. Su calendario de emisión y su oferta máxima ofrecen un activo digital único con costos de mantenimiento mínimos o nulos, a diferencia de los depósitos de valor tradicionales.

Además, su naturaleza digital y su poder adquisitivo permiten a los usuarios realizar transacciones globales sin intermediarios. Esta propuesta de valor se ve reforzada por el hecho de que Bitcoin es global, neutral y resistente a la censura. Esto se aplica tanto al uso a gran como a pequeña escala de Bitcoin: particulares, bancos e incluso países pueden utilizarlo como medio de intercambio y reserva de valor.













Un bien monetario en ciernes. Dadas

sus dos propuestas de valor como reserva de valor y medio de cambio, el bitcoin puede entenderse como un bien monetario. Un bien monetario se define como aquel que se valora por su comerciabilidad, más que por su consumo o uso.

¿Por qué algunos bienes se consideran monetarios y otros no? Economistas e historiadores sugieren que la respuesta reside en varias características que definen un bien monetario. Cuantas más de estas características posea un bien, mayor será la probabilidad de que se convierta en una forma de moneda o dinero aceptada.

Bitcoin posee varias cualidades positivas del dinero, combinando la escasez y durabilidad de un bien tangible con la facilidad de uso, almacenamiento y transporte del dinero fiduciario. Cabe destacar también que, al igual que otros bienes monetarios, Bitcoin no es una empresa: no paga dividendos ni genera flujos de efectivo.

Por lo tanto, su valor se deriva de su capacidad para cumplir con las características de un bien monetario en comparación con las alternativas tradicionales.

 Fiat currency	—	+	—	+	—	—	—
 Bitcoin	+	+	+	+	+	+	—
 Gold	+	—	+	—	—	+	+
							
Durable	Divisible	Fungible	Portable	Verifiable	Scarce	Track record	

Fuente: Fidelity Digital Assets Research, 2025

Solo existe una red Bitcoin.

Bitcoin es, por naturaleza, una red de participación voluntaria, lo que significa que cualquiera puede unirse o abandonarla a su antojo. Sin embargo, cualquier persona que intente cambiar las reglas sin el consenso de la mayoría de los participantes será ignorada por la red. Por lo tanto, si bien el código de Bitcoin es de código abierto y puede copiarse y modificarse, estas copias

Las versiones derivadas de Bitcoin son redes completamente separadas y no son compatibles con versiones anteriores de la red Bitcoin original.

Además, los tokens de Bitcoin son propios de Bitcoin y no se pueden eliminar ni transportar a otra red blockchain, lo que contribuye a los efectos de red de Bitcoin.

El valor de Bitcoin está impulsado por su escasez obligatoria.

Una de las propiedades más fuertes del bitcoin es su escasez. El bitcoin no solo es escaso (a junio de 2025, su tasa de inflación era del 0,8%), sino que además es finito. Solo existirán 21 millones de bitcoins.

Ningún otro activo digital posee una política monetaria inmutable al nivel del bitcoin. El límite de suministro impuesto al bitcoin se sustenta en dos características clave, las cuales lo distinguen de cualquier otro activo digital.

La primera característica es la descentralización de Bitcoin.

Ninguna entidad posee ni controla Bitcoin ni sus reglas. Al ser una red completamente descentralizada que utiliza código abierto, los participantes deben acatar las reglas del código. El límite de suministro de 21 millones de bitcoins se estableció en el código fuente original de Bitcoin, que sigue vigente en la actualidad.

Este código fuente solo puede modificarse mediante el consenso de los participantes de la red (los operadores de nodos). Un cambio en el calendario de suministro de bitcoin es algo que podría ocurrir en teoría, pero que probablemente nunca se materialice en la práctica.

En primer lugar, lograr un consenso es muy difícil debido a la gran dispersión de la red y los participantes del mercado de Bitcoin. Más importante aún, la red se diseñó con incentivos para no modificar el límite de suministro. No sería económicamente viable para los participantes actuales de la red aumentar o ajustar dicho límite, ya que esto inflaría la oferta de Bitcoin y diluiría el valor de sus tenencias o, en el caso de los mineros, sus recompensas. Aquí, los inversores pueden observar los poderosos efectos de la teoría de juegos, pues a todos los participantes les conviene coordinarse, cooperar y no modificar el límite de suministro.

La segunda característica es que Bitcoin es resistente a la censura porque ninguna entidad lo posee ni lo controla. Dado que la red no tiene fronteras geográficas, sería difícil para un Estado nación asumir el control o la regulación de la red y del propio código fuente de Bitcoin.



Tecnología

Comprender la prueba de trabajo

Bitcoin logra la descentralización y la resistencia a la censura mediante el mecanismo de consenso de prueba de trabajo.

La cadena de bloques está compuesta por miles de ordenadores que ejecutan el mismo código de software. Estos ordenadores, que cualquiera puede manejar, guardan una copia de un registro que muestra todas las transacciones realizadas en la red. Las transacciones son mensajes que se envían a estos ordenadores indicándoles que actualicen el registro (por ejemplo, «mover X bitcoins de esta dirección a esta otra»). Por lo tanto, la red puede funcionar como una red de pagos.

Debido a que Bitcoin es descentralizado y ninguna entidad lo controla, necesita un mecanismo de consenso para llegar a un acuerdo sobre el estado real del libro mayor. La prueba de trabajo actúa como ese mecanismo de consenso.

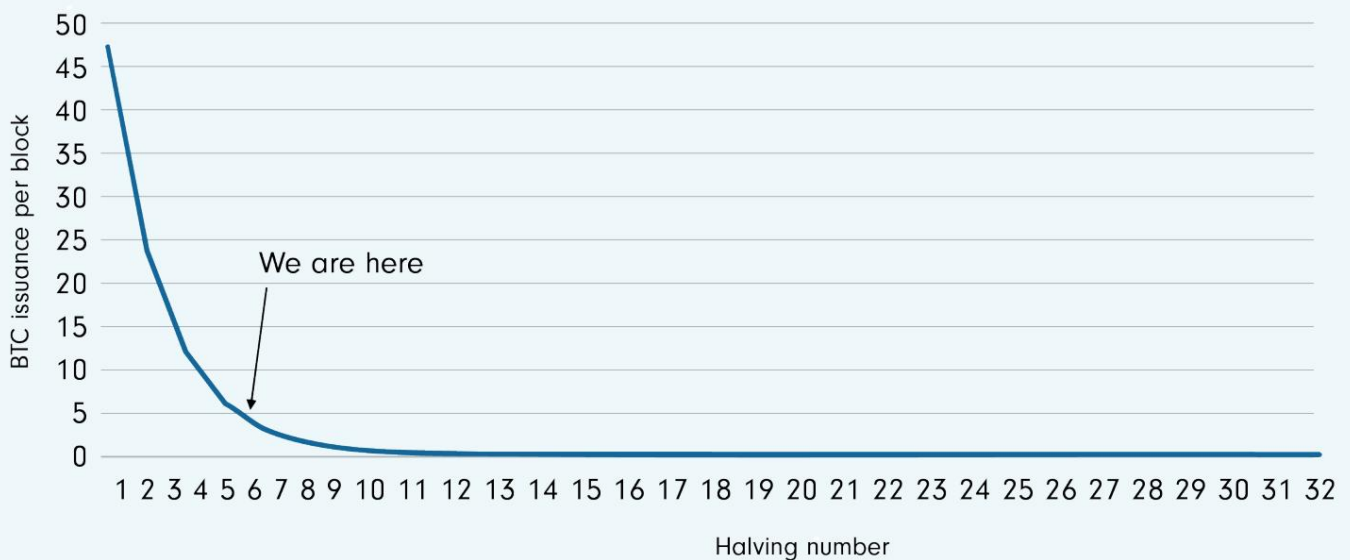
Además, este avance tecnológico también abordó el problema del doble gasto, asegurando que un token virtual no pueda gastarse dos veces ni copiarse. Cómo Bitcoin lo logra

Este mecanismo de prevención del fraude es especialmente importante porque se logra sin depender de un tercero o intermediario, algo que nunca se había hecho antes.

La reducción a la mitad: el calendario monetario de Bitcoin

Cada 210 000 bloques, o aproximadamente cada cuatro años, el código de Bitcoin reduce a la mitad la compensación total que reciben los mineros por minar con éxito un bloque válido. Se prevé que la tasa de emisión de Bitcoin se reduzca a la mitad aproximadamente cada cuatro años hasta alcanzar los 21 millones de unidades, lo que se estima que ocurrirá en 2140.

Tasa de emisión de Bitcoin a lo largo del tiempo



Fuente: Fidelity Digital Assets Research, 2025

Análisis competitivo

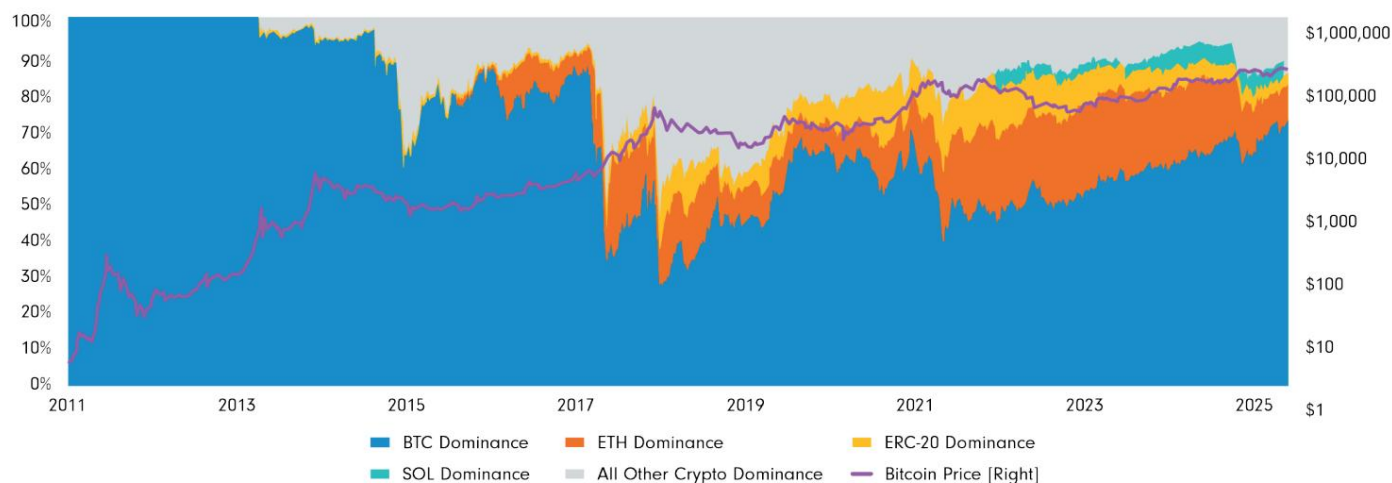
El potencial de Bitcoin para ser el principal bien monetario

Los inversores pueden coincidir en que el bitcoin posee muchas de las cualidades que lo convierten en una buena moneda, pero ¿quién puede asegurar que solo existirá una? Si bien es muy improbable que exista una sola moneda, este informe sostiene que, debido a los efectos de red, una de ellas acabará dominando el ecosistema de activos digitales.

El poder de los efectos de red monetarios

Muchos inversores están familiarizados con el poder de los efectos de red, donde el valor de una red determinada aumenta exponencialmente a medida que crece el número de sus usuarios. Las redes monetarias no son diferentes. Sin embargo, son aún más poderosas.

Dominancia (ex-stablecoins) frente al precio



Fuente: Fidelity Digital Assets Research a través de Coin Metrics, 22/06/25.

que otras redes porque el incentivo para elegir el dinero correcto es mucho más fuerte que cualquier otra elección de una red, como una red social.

Si los inversores buscan un activo digital como bien monetario con capacidad para funcionar como reserva de valor, probablemente elegirán aquel con la red más grande, segura, descentralizada y líquida. Como primer activo digital verdaderamente escaso, Bitcoin obtuvo una ventaja competitiva y la ha mantenido a lo largo del tiempo.

Aunque el dominio del bitcoin, es decir su capitalización de mercado como porcentaje del ecosistema total de activos digitales, había disminuido del 100 % a aproximadamente el 55 %, ha vuelto a superar el 64 %. Cabe destacar que, si se excluyen las stablecoins, el dominio del bitcoin se sitúa por encima del 72 %.

Esto no se debe a que su tamaño se esté reduciendo, sino más bien al crecimiento del resto del ecosistema.

Las redes monetarias también poseen una propiedad reflexiva. Las personas observan cómo otros se unen a una red monetaria, lo que las incentiva a unirse, ya que también desean formar parte de la red donde se encuentran sus pares o socios comerciales. Esto se puede observar a menor escala en las redes de pago existentes, ya que plataformas como PayPal y Venmo han crecido a un ritmo acelerado.

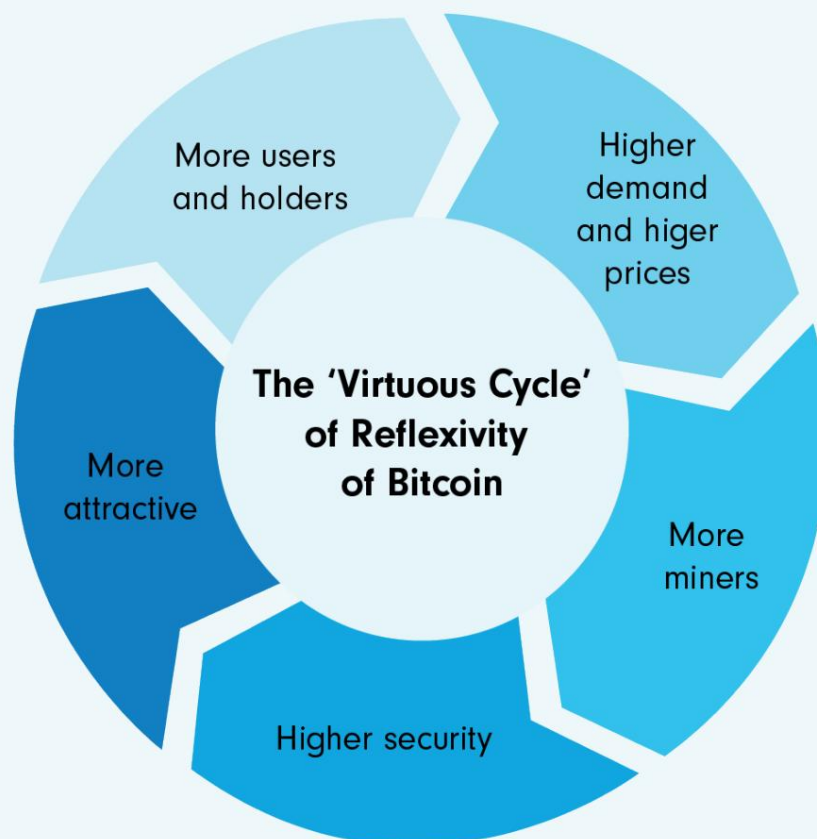
En el caso del bitcoin, la propiedad reflexiva es más pronunciada porque no solo incluye a los poseedores pasivos del activo, sino también a los mineros que aumentan activamente la seguridad de la red.

A medida que más personas creen que el bitcoin posee propiedades monetarias superiores y optan por almacenar su patrimonio en él, la demanda aumenta, lo que potencialmente conduce a precios más altos (especialmente porque la oferta es inelástica o no responde a los precios). Los mineros se ven incentivados a aumentar su inversión de capital y su capacidad de procesamiento, ya que los precios más altos se traducen en mayores márgenes de beneficio. Una mayor capacidad de procesamiento dedicada a la minería de bitcoin aumenta la seguridad de la red, lo que a su vez hace que el activo sea más atractivo, atrayendo aún más usuarios e inversores.

Bitcoin es actualmente la red monetaria más descentralizada y segura (en comparación con otros activos digitales). Cualquier red blockchain o activo digital nuevo que intente superar a Bitcoin como medio de pago tendrá que diferenciarse sacrificando una o ambas propiedades, una idea que se explora más adelante en el «Trilema de la Blockchain».

Es probable que un competidor que intente copiar todo el código de Bitcoin también fracase, ya que no habrá motivo para cambiar de la red monetaria más grande a una que sea completamente idéntica pero de una fracción de su tamaño.

Además, el efecto Lindy, también conocido como la ley de Lindy, es una teoría que postula que cuanto más tiempo perdure algo no perecedero, como una tecnología o una idea, mayor será la probabilidad de que se mantenga vigente en el futuro. Lo mismo podría aplicarse a Bitcoin.



Por qué creemos que es improbable que otro activo digital reemplace a Bitcoin como bien monetario.

Si bien teóricamente es posible en un mercado libre, es improbable que el bitcoin sea reemplazado por un activo digital "mejorado" por varias razones.

Una de las razones más importantes es que cualquier mejora en una característica de Bitcoin, como la velocidad o la escalabilidad, conlleva una reducción en otra, como su nivel de descentralización o seguridad. Esta disyuntiva se conoce como el trilema de la cadena de bloques.

El trilema de la cadena de bloques

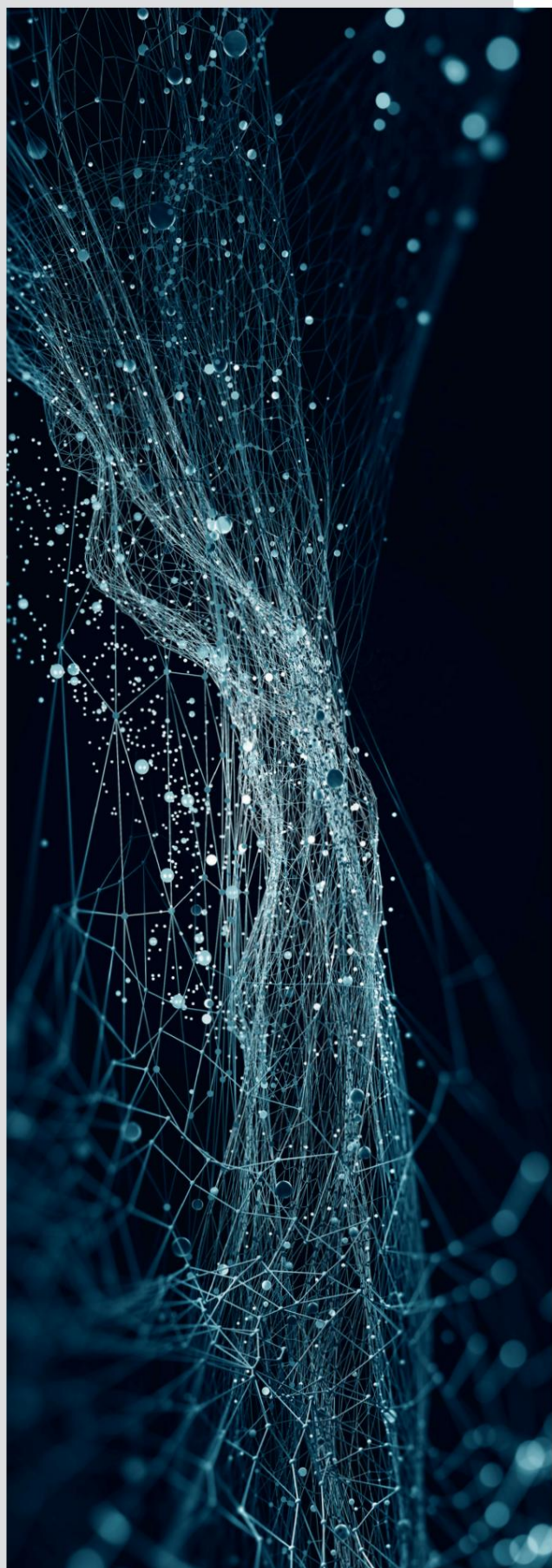
A principios de la década de 1980, los informáticos identificaron un trilema inherente a las bases de datos descentralizadas.

Más recientemente, Vitalik Buterin, creador de Ethereum, esbozó una variante de este trilema: el trilema de la cadena de bloques. Buterin propone que una base de datos descentralizada (de la cual Bitcoin es un ejemplo) solo puede cumplir plenamente con dos de las tres garantías: descentralización, seguridad o escalabilidad.

La seguridad se refiere a la probabilidad de que la red sea atacada o comprometida. En el caso de una red descentralizada como Bitcoin, la principal preocupación es un ataque del 51%, en el que una sola persona o entidad controla más de la mitad de la potencia de cálculo de la red (conocida como tasa de hash).

Si esto se logra, el atacante podría controlar la red o modificar el registro abierto, por ejemplo, realizando un doble gasto o revirtiendo transacciones. Se perdería la confianza en la red, lo que podría provocar su colapso. Sin embargo, a medida que Bitcoin crece y cuenta con un número cada vez mayor de nodos y mineros, atacarlo se vuelve más difícil y costoso.

Bitcoin es el activo digital más seguro si se mide por la tasa de hash o la potencia de cálculo que protege la red, en comparación con otros activos digitales que utilizan el mismo algoritmo de hash. El consumo energético anual total puede utilizarse como indicador de seguridad: un mayor consumo energético indica una mayor cantidad de recursos de minería dedicados a proteger la red. Se estima que Bitcoin consume aproximadamente 173,77 teravatios-hora al año, lo que representa aproximadamente el 0,68 % del consumo eléctrico mundial en 2025. La potencia de cálculo o tasa de hash utilizada para proteger la red ha aumentado con el tiempo.



La descentralización se refiere a cuánto control cualquier persona, entidad o grupo puede tener acceso a un sistema o red. En una red descentralizada, el consenso se logra mediante un mecanismo de votación, de modo que ninguna entidad puede controlar ni restringir los datos. En una red abierta y descentralizada, cualquiera puede unirse libremente, y ninguna entidad puede excluirlo si sigue las reglas o el protocolo de la red. Esto permite que la red funcione sin intermediarios.

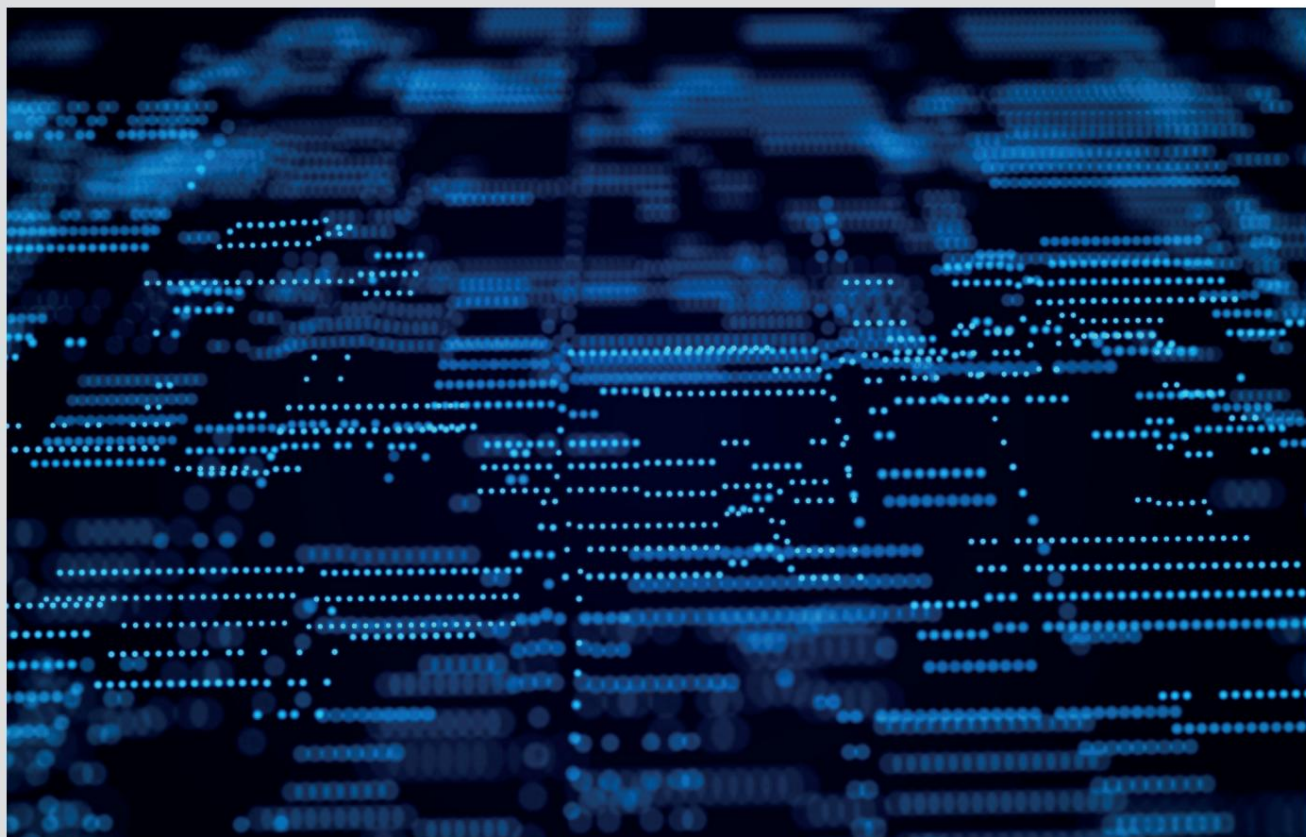
El coste de una mayor descentralización reside en un menor rendimiento de la red, es decir, en la menor velocidad de transmisión de información debido a la necesidad de un mayor consenso. Lo opuesto a una red descentralizada sería una red completamente centralizada, en la que un único intermediario controla todos los aspectos. La ventaja reside en la velocidad y el rendimiento, ya que no se requiere consenso, pero la desventaja radica en la necesidad de confiar en este único intermediario.

La escalabilidad se refiere a la capacidad de la red para gestionar el crecimiento, como el aumento en el número de usuarios y la cantidad de transacciones que puede procesar en un tiempo limitado. La escalabilidad ha sido, sin duda, el mayor obstáculo para Bitcoin, ya que maximiza la descentralización y la seguridad. Bitcoin es la red con una de las más lentas como resultado, el rendimiento de las transacciones.

La red agrega un nuevo bloque y lo valida.

Las transacciones se realizan solo cada 10 minutos en promedio, y debido a que el tamaño del bloque de Bitcoin es limitado, solo una cantidad determinada de transacciones puede caber en cada bloque. Para poner esto en perspectiva, Bitcoin puede procesar aproximadamente entre tres y siete transacciones por segundo. En comparación, una red de pagos altamente centralizada como Visa procesa casi 9000 transacciones por segundo.

Ninguna de estas características es intrínsecamente mejor que otra, pero esto puede depender del uso. caso.



Competidores

Ethereum

La red Ethereum y su token, ether, no se analizan en este informe. Sin embargo, Ethereum es el segundo activo digital más grande por capitalización de mercado. Por lo tanto, es relevante destacar algunas de las principales similitudes y diferencias entre Bitcoin y Ethereum.

Desde sus inicios, Bitcoin se propuso cumplir con los criterios de una "versión puramente entre pares de dinero electrónico". Fue diseñado para ser descentralizado y seguro, de modo que el valor pudiera enviarse sin necesidad de confiar en un intermediario. Esto se combinó con un calendario monetario preprogramado y un límite de suministro impuesto, lo que le otorgó a Bitcoin la capacidad de convertirse en un bien monetario y una reserva de valor.

Ethereum también comenzó como un documento técnico, publicado originalmente en 2013 por Vitalik Buterin. Los creadores de Ethereum se propusieron tomar la tecnología blockchain, pionera de Bitcoin, y extenderla para incluir más capacidades, sobre todo la capacidad de realizar transacciones que requieren mayor capacidad de procesamiento. La red blockchain de Ethereum puede alojar y ejecutar contratos inteligentes que se pueden usar para programar diversas aplicaciones. Por esta razón, algunos se refieren a Ethereum como una "computadora mundial distribuida". La red también permite la emisión de diferentes tokens en la blockchain de Ethereum, actuando como una plataforma que otros pueden usar para crear aplicaciones, incluyendo aplicaciones de finanzas descentralizadas, juegos y herramientas de redes sociales.

Si bien algunos miembros de la comunidad de activos digitales consideran que Ethereum es una red superior o más avanzada que Bitcoin, sus capacidades adicionales y su flexibilidad conllevan ciertas desventajas. En particular, una red más compleja aumenta la probabilidad de errores de software, así como los riesgos de centralización y una posible disminución de la seguridad.

Una comparación de alto nivel de Bitcoin, Ethereum y Litecoin.

	Industrial Distribution	Supply	Market cap (USD)	Annual inflation / issuance rate	30 day avg tx free (USD)	Daily value transacted in USD (1-year SMA)	Daily number of transactions settles (1-year SMA)
Bitcoin	0	19.88m	\$2.03t	0.84%	\$1.43	\$10.76b	483,195
Litecoin	150	75.99m	\$6.22b	1.77%	\$0.005	\$0.11b	203,363
Ethereum	72,000,000	120.71m	\$275.95b	0.49%	\$0.95	\$5.99b	1,218,319

Fuente: Fidelity Digital Assets Research a través de Coin Metrics, 22/06/25.

Litecoin

Otro tipo de competidor de Bitcoin es Litecoin. Litecoin se lanzó en 2011 y utilizó gran parte del código original de Bitcoin, con algunas modificaciones menores para construir su red blockchain. El objetivo de Litecoin es ser una versión "ligera" de Bitcoin, más eficiente y económica para realizar transacciones. Si bien es relativamente fácil reutilizar código de una blockchain a otra, el valor de Bitcoin reside en sus efectos de red, que son mucho más difíciles de transferir. En 2025, la capitalización de mercado de Litecoin era de 6200 millones de dólares, menos del 1 % de la de Bitcoin. Litecoin es un ejemplo de las muchas redes relacionadas con Bitcoin que han tenido dificultades para competir con la original.

Análisis fundamental y tesis de inversión

Bitcoin como cobertura macroeconómica

El perfil de rentabilidad de Bitcoin está impulsado por dos factores favorables: su escasez y las condiciones macroeconómicas.

Los niveles sin precedentes de estímulo monetario y fiscal han llevado a que más inversores y usuarios vean el bitcoin

como una "póliza de seguro" que puede brindar protección contra las consecuencias desconocidas.

Históricamente, el apalancamiento ha impulsado la fragilidad de los sistemas financieros.

Históricamente, este tipo de entornos macroeconómicos han tendido a beneficiar a los activos escasos cuya oferta no puede modificarse. En el mundo de los activos digitales, las reglas de Bitcoin, sus precedentes históricos y su descentralización han generado el mayor grado de escasez de cualquier protocolo de activos digitales.

Esto constituye un argumento convincente como la mejor cobertura disponible para algunos de los posibles obstáculos que enfrenta el sistema financiero tradicional.

competidor de materias primas duras

En el estudio de Fidelity Digital Assets de 2023 sobre activos digitales para inversores institucionales, el 51 % de los encuestados declaró tener una inversión actual en activos digitales. La razón por la que los inversores institucionales deciden invertir ahora es que el mercado crecerá considerablemente si se generaliza su uso como reserva de valor en el futuro.

Con una capitalización de mercado estimada en más de 22,85 billones de dólares a junio de 2025, el oro sigue siendo la principal reserva de valor. Sin embargo, la capitalización de mercado del bitcoin está creciendo. En 2020, representaba el 1,6 % de la del oro; a junio de 2025, esa cifra ascendería al 8,9 %.

A medida que invertir en bitcoin se vuelve más accesible a través de diversas vías tradicionales, esta brecha podría seguir reduciéndose.

Valuación

Una vez que los inversores comprenden la propuesta de valor del bitcoin, surge la cuestión de cómo valorarlo.

Existen muchos métodos de valoración diferentes.

En una amplia gama de clases de activos, ya sean generadores de flujo de efectivo o materias primas físicas, los inversores pueden aplicar su propio marco de análisis al ámbito de los activos digitales. Este informe se centra en el papel del bitcoin como reserva de valor, constituyendo así la principal tesis de inversión. Dado su potencial como bien monetario y la ausencia de flujo de efectivo o aplicaciones industriales, este informe sostiene que el análisis del bitcoin se realiza mejor desde la perspectiva de la oferta y la demanda.

La oferta de Bitcoin está predeterminada y es inelástica a la demanda. Su escasez puede ser uno de los factores que impulsan su valor y puede aumentar a medida que la oferta disminuye o la demanda aumenta. Sin embargo, la escasez por sí sola no puede generar valor sin un caso de uso válido y una demanda de mercado para dicho uso. En la página siguiente se analizan los modelos de valoración basados tanto en la oferta como en la demanda.



La oferta: creciente escasez

Históricamente, los eventos de reducción a la mitad de Bitcoin han ido seguidos de fuertes subidas de precio en los meses posteriores al evento preprogramado. Estas reducciones a la mitad son el resultado del calendario de emisión predeterminado de Bitcoin, que reduce automáticamente su tasa de emisión aproximadamente cada cuatro años.

En años anteriores, las reducciones a la mitad parecían provocar un mayor desequilibrio entre la oferta emitida y la demanda total de bitcoin. Cada reducción posterior ha ido seguida de una disminución en la oferta emitida, lo que probablemente tenga un menor impacto en el desequilibrio entre la oferta y la demanda, y, históricamente, ha ido seguida de aumentos de precio menos drásticos.

Halving event (date)	Annual inflation	Daily BTC issuance	Two-year forward returns
1st Halving (2012)	8%	3,600	2,964%
2nd Halving (2016)	4%	1,800	922%
3rd Halving (2020)	1.8%	900	348%
4th Halving (2024)	0.8%	450	?

Fuente: Fidelity Digital Assets Research a través de Coin Metrics, 23/08/24.

El lado de la demanda: efectos de red

Los efectos de red son un componente clave en los modelos operativos de muchas empresas. Representan la idea de que el nivel de utilidad o valor percibido de un bien o servicio en particular es resultado directo del número de usuarios de dicho bien o servicio.

La ley de Metcalfe, un método utilizado para explicar los efectos de red, establece que el valor de una red de telecomunicaciones es directamente proporcional al cuadrado del número de usuarios de dicho sistema. Cada usuario único está conectado con todos los demás usuarios, lo que genera un crecimiento exponencial en el número de conexiones posibles en esa red y una mayor adopción entre la población general.

Los efectos de red suelen generar una curva de adopción similar en diversas tecnologías exitosas. Esta curva, conocida como «curva en S», se explica mediante la lógica de las tendencias de adopción. Los primeros usuarios de una tecnología suelen percibir un valor presente y potencial en el futuro en esa red, aunque aún no esté ampliamente extendida.

Si una tecnología muestra una ventaja suficientemente grande en relación con sus predecesoras a lo largo del tiempo, y los costos de cambio son lo suficientemente bajos, entonces la adopción comenzará a acumularse. Es entonces cuando una tecnología comienza a alcanzar una masa crítica.

Una vez que el producto o servicio se acepta como una tecnología superior y ampliamente utilizada, su tasa de adopción disminuye gradualmente, formando una asíntota cercana a la plena madurez.

La Ley de Metcalfe puede servir de base para una posible valoración de Bitcoin a partir del crecimiento proyectado de direcciones y su relación con el precio. Las curvas de adopción históricas pueden utilizarse para proyectar el crecimiento potencial futuro de direcciones, dado que la curva de adopción de Bitcoin hasta ahora ha evolucionado de forma similar a otras curvas de adopción tecnológica. Sin embargo, esta metodología puede generar una amplia gama de resultados, dependiendo de la curva de adopción tecnológica específica a la que finalmente se asemeje Bitcoin, por lo que dista mucho de ser precisa. Podemos suponer que Bitcoin aún se encuentra en una fase temprana de adopción masiva, con estimaciones de 53,63 millones de direcciones únicas de Bitcoin con saldo distinto de cero, teniendo en cuenta que una persona o entidad puede poseer más de una billetera y que algunas pueden estar inactivas.

Análisis de escenarios



Caso alcista:

Bitcoin experimenta un punto de inflexión donde el valor bloqueado en la red y el número de usuarios se vuelven tan atractivos para los desarrolladores que estos se inclinan por la cadena de bloques como la opción predeterminada para crear casos de uso adicionales, como aplicaciones financieras. La red podría experimentar mejoras tecnológicas que hagan a Bitcoin más escalable sin sacrificar la descentralización ni la seguridad. En este caso, el mercado potencial total para Bitcoin se extiende más allá de ser un activo digital, llegando a convertirse potencialmente en la columna vertebral del sistema financiero, con Bitcoin ampliamente aceptado como una valiosa forma de garantía. Otros factores relevantes podrían ser un cambio en el tratamiento fiscal de Bitcoin y una disminución continua de su volatilidad de precios, lo que podría permitir un uso más amplio como método de pago.



Caso base:

Bitcoin continúa su adopción institucional y minorista, consolidándose como una protección contra la inflación y una reserva de valor. Esto ocurriría a lo largo de varios años, dado que el mercado aún se encuentra en una etapa temprana del proceso. Además, el progreso regulatorio podría evolucionar de forma no lineal, como ha sucedido en el pasado, lo que significa que el acceso a productos estandarizados y regulados podría ser irregular. Finalmente, un mundo más incierto, donde los gobiernos sigan registrando déficits fiscales históricamente altos y provocando una continua devaluación de la moneda, podría acelerar la curva de adopción incluso sin un mejor acceso o regulación.



Caso del oso:

Una posible regulación que obstaculice el acceso y la adopción generalizada de Bitcoin, y reduzca la demanda, podría generar un panorama desalentador para la inversión en esta criptomoneda. Si bien actualmente Bitcoin es reconocido por más jurisdicciones en todo el mundo, algunas se muestran reacias o inconsistentes en su enfoque, dado que perciben esta clase de activos como más riesgosa. Además, podría surgir una tecnología superior, así como otras alternativas, y los inversores podrían volverse indiferentes ante las características clave de Bitcoin, como su límite máximo de suministro o su naturaleza descentralizada.

Gobernanza y hoja de ruta

¿Quién “gobierna” el código de Bitcoin?

El documento técnico de Bitcoin se envió a una lista de correo de ciberactivistas a finales de 2008 bajo el seudónimo de Satoshi Nakamoto. No está claro si ese nombre pertenecía a un grupo de personas o a un individuo. Sin embargo, hubo usuarios y colaboradores iniciales cuyos nombres no se ocultaron, incluidos activistas criptográficos que contactaron con Satoshi tras la publicación del documento.

Satoshi participó activamente en el desarrollo de Bitcoin desde su lanzamiento hasta finales de 2010, cuando realizó su última contribución al proyecto. Posteriormente, en abril de 2011, anunció que se dedicaría a otros proyectos. Antes de marcharse, cedió el control del repositorio a Gavin Andresen, desarrollador y figura clave en la comunidad Bitcoin, y transfirió dominios relacionados con Bitcoin a varios miembros destacados de la comunidad.

Satoshi no ha movido ni transferido los tokens iniciales que estaban bajo su control desde que aparentemente desapareció en 2011.

El software Bitcoin Core se ha integrado plenamente en la comunidad. Los cambios en el código se implementan mediante el consenso de la comunidad de desarrolladores y se adoptan a través del conjunto descentralizado de operadores de nodos.

Sin embargo, el proyecto mantiene un control más estricto del acceso para realizar confirmaciones y de las capacidades de fusión para garantizar la integridad del proyecto principal.

Es importante destacar que estas personas selectas no tienen el control unilateral del repositorio y que cualquiera puede contribuir a la red hoy en día. El desarrollo de Bitcoin ha sido financiado en gran medida mediante subvenciones y patrocinios de numerosos contribuyentes individuales y organizaciones.

Lanzamiento inicial del token

Bitcoin se anunció por primera vez con su libro blanco en 2008, lo que permitió un lanzamiento abierto y transparente de las reglas de la red. El protocolo se lanzó oficialmente en enero de 2009. El primer bloque minado, el bloque génesis, produjo los primeros 50 bitcoins que se presumía que habían sido

Se le otorgó a Satoshi. Pasarían otros tres días antes de que se encontrara el siguiente bloque.

En aquel entonces, cualquiera podía unirse a la red y competir por estas recompensas en bitcoin. Sin embargo, es importante destacar que bitcoin no se lanzó con un tipo de cambio.

Los primeros usuarios, en efecto, invertían su tiempo y energía en una "idea" de dinero que, por aquel momento, carecía de valor.

Bitcoin no se lanzó con preventa ni preminado, lo que se consideró un lanzamiento justo para la red. El mecanismo de recompensa de prueba de trabajo sigue distribuyendo nuevos bitcoins a los mineros que consumen electricidad.

Hoja de ruta

El conjunto de reglas descentralizadas de Bitcoin impide que la red experimente cambios importantes en el consenso. Estos cambios, conocidos como bifurcaciones duras (hard forks), han dado lugar históricamente a cadenas de bloques completamente nuevas y diferentes. Algunos ejemplos son Bitcoin Cash, Bitcoin SV, Bitcoin Classic y Bitcoin Unlimited.

Sin embargo, podría decirse que Bitcoin nunca ha realizado una bifurcación dura de sus propias reglas. En otras palabras, en toda la historia de Bitcoin, la política monetaria y otros atributos identificables importantes no se han modificado ni flexibilizado de forma que provocaran una bifurcación dura. Esto también significa que es menos probable que los nodos de Bitcoin sean expulsados arbitrariamente de la red por negligencia, en comparación con los protocolos que suelen realizar bifurcaciones duras para mejorar o modificar las reglas fundamentales de la red.

Actualmente, la comunidad está investigando y debatiendo numerosas mejoras y actualizaciones. Estas mejoras se conocen como Propuestas de Mejora de Bitcoin (BIP, por sus siglas en inglés).

Cabe destacar que la comunidad de Bitcoin ha priorizado la descentralización y la seguridad por encima de todo. Por lo tanto, la mayoría —si no todas— las propuestas de cambio a la red se realizan mediante una bifurcación suave (soft fork). Los cambios en Bitcoin son inherentemente lentos, y pueden transcurrir años entre la introducción de una propuesta de mejora de Bitcoin (BIP) y su implementación final. El estado actual de las BIP se puede consultar [aquí](#).

Riesgos e incertidumbres

Casi todos los riesgos asociados al bitcoin se observan hoy en día en cualquier otro activo digital, siendo los ataques de estados nación y los fallos de protocolo dos de las amenazas más notables para la red. Asimismo, la evolución de la regulación puede influir en la evolución futura del precio, al igual que la percepción de su valor, dado que el bitcoin no genera flujo de caja. También es importante destacar la volatilidad, aunque aún elevada, que puede traducirse en grandes fluctuaciones de precio en comparación con otras inversiones.

Riesgo técnico

La posibilidad de una vulnerabilidad en su código siempre representa una amenaza latente, ya que Bitcoin es un software que se ejecuta en hardware informático. De hecho, Bitcoin sufrió dos fallos de software distintos en sus inicios, lo que requirió la implementación de parches. Este problema puede mitigarse manteniendo el software sencillo y realizando revisiones y análisis exhaustivos del código.

En el caso de Bitcoin, es menos probable que su protocolo presente un fallo importante en esta etapa de su desarrollo. Existe desde hace más tiempo que cualquier otro proyecto, cuenta con un código intencionadamente sencillo y ofrece una recompensa de más de un billón de dólares a quien logre explotarlo.

Cualquier vulnerabilidad podría generar una pérdida de confianza en el activo, anulando su valor como método seguro para desarrollar aplicaciones financieras. Dado que, por el momento, el bitcoin no genera flujo de efectivo ni tiene otros casos de uso, su valor podría llegar a cero.

Riesgo regulatorio

El panorama regulatorio del bitcoin ha mejorado notablemente, ya que cada vez más países buscan brindar claridad legal sobre el activo e integrar a los participantes del mercado que operan con bitcoin en sus sistemas financieros mediante marcos regulatorios. Esto representa un cambio significativo con respecto al pasado, cuando una minoría de países intentó prohibirlo y la incertidumbre regulatoria preocupaba a los inversores institucionales. Hoy en día, si bien existen diferencias en los enfoques regulatorios, se está eliminando un obstáculo importante para las instituciones, lo que convierte un riesgo en un potencial impulsor de su adopción.

Cabe destacar la normativa europea sobre Mercados de Criptoactivos (MiCA), que entró en vigor en enero de 2025 y que garantiza que el bitcoin no sea un valor. No obstante, establece normas para los participantes del mercado, centrándose en la protección del consumidor y la estabilidad del mercado dentro de un marco armonizado.

Julio de 2025 marcó un hito histórico para Estados Unidos con la promulgación de su primera ley sobre activos digitales. El éxito bipartidista de la Ley GENIUS, centrada en un marco federal para la emisión de stablecoins, impulsa ahora el proyecto de ley más integral sobre la estructura del mercado: la Ley CLARITY. Esta ley establece que, como activo asociado a un "sistema blockchain maduro", el bitcoin es una mercancía digital bajo la jurisdicción de la CFTC. Si bien la Ley CLARITY fue aprobada por la Cámara de Representantes, aún debe ser aprobada por el Senado al momento de redactar este texto. Junto con la Ley GENIUS, la Ley CLARITY crearía un marco coherente para una gama más amplia de activos digitales. Si la Ley CLARITY se convierte en ley, codificará la clasificación del bitcoin bajo la legislación federal y creará una hoja de ruta de cumplimiento más clara para los participantes del mercado. Esto eliminaría las zonas grises existentes anteriormente con respecto a la supervisión regulatoria de la SEC y la CFTC, ofreciendo mayor certeza tanto a los inversores como a las instituciones financieras que exploran los activos digitales.

Riesgo competitivo

Este informe ha presentado numerosos argumentos sobre por qué el riesgo competitivo para el bitcoin parece ser bajo. Sin embargo, siempre existe el riesgo de que otro activo (digital o de otro tipo) pueda ganar (o mantener) su ventaja como bien monetario, cumpliendo así la función de reserva de valor o medio de intercambio.

Riesgo de apatía del inversor

Finalmente, otro posible riesgo para el bitcoin como inversión es la apatía de los inversores. Si bien muchos ven el bitcoin como una tecnología revolucionaria con numerosas ventajas, su valor es, en última instancia, subjetivo. Como ocurre con muchas inversiones, si los inversores pierden interés, no reconocen su valor y, en consecuencia, su adopción disminuye, el valor del bitcoin podría depreciarse significativamente.

Información importante

Este material está dirigido exclusivamente a inversores institucionales y profesionales de la inversión, y no debe distribuirse al público en general ni ser utilizado por inversores privados. Este material está destinado únicamente a la persona o entidad a la que se envía. Se proporciona únicamente con fines informativos y no constituye una recomendación, asesoramiento de inversión de ningún tipo ni una oferta para comprar o vender ningún activo. No debe reproducirse ni distribuirse a terceros sin la autorización previa de Fidelity. Este material no constituye una distribución, oferta ni solicitud para contratar los servicios de gestión de inversiones de Fidelity, ni una oferta para comprar o vender, ni una solicitud de oferta para comprar o vender valores en ninguna jurisdicción o país donde dicha distribución u oferta no esté autorizada o sea contraria a las leyes o regulaciones locales.

Fidelity no garantiza que el contenido sea apropiado para su uso en todas las ubicaciones ni que las transacciones o servicios aquí descritos estén disponibles o sean apropiados para su venta o uso en todas las jurisdicciones o países, ni para todos los inversores o contrapartes.

La información aquí contenida, así como los informes de Fidelity Digital Assets® a los que se hace referencia, son proporcionados por Fidelity Digital Asset Services, LLC («FDAS LLC») y Fidelity Digital Assets, Ltd («FDA LTD»). Fidelity Digital Assets® fue designada por FIL para ofrecer liderazgo intelectual y recursos educativos, y se reproduce con su autorización. Fidelity Digital Assets es una marca de servicio registrada de FMR LLC.

Esta comunicación no está dirigida a personas dentro de los Estados Unidos, quienes no deben actuar en consecuencia. Todas las personas y entidades que accedan a la información lo hacen por iniciativa propia y son responsables del cumplimiento de las leyes y regulaciones locales aplicables, y deben consultar con sus asesores profesionales.

Los activos digitales son especulativos y altamente volátiles, pueden volverse ilíquidos en cualquier momento y están dirigidos a inversores con alta tolerancia al riesgo. Quienes invierten en activos digitales podrían perder la totalidad de su inversión.

Las opiniones expresadas corresponden a la fecha indicada, se basan en la información disponible en ese momento y pueden variar según las condiciones del mercado u otras circunstancias. Salvo que se indique lo contrario, las opiniones expresadas son las del orador o autor y no necesariamente las de Fidelity Digital Assets ni sus filiales. Fidelity Digital Assets no asume ninguna obligación de actualizar la información.

Fidelity, Fidelity International, el logotipo de Fidelity International y el símbolo F son marcas registradas de FIL Limited. FIL Limited y sus subsidiarias se conocen comúnmente como Fidelity International. Fidelity Investments se refiere colectivamente a FMR LLC, una compañía estadounidense, y a ciertas subsidiarias, incluyendo, entre otras, Fidelity Management & Research Company LLC, FDAS LLC y FDA LTD. Fidelity International y Fidelity Investments no pertenecen al mismo grupo de compañías.

Fidelity solo ofrece información sobre productos y servicios y no brinda asesoramiento de inversión basado en circunstancias individuales. Le recomendamos que obtenga información detallada antes de tomar cualquier decisión de inversión. Las inversiones deben realizarse con base en el prospecto/documentación de oferta vigente. Ciertas declaraciones contenidas en este documento se basan en expectativas, estimaciones, proyecciones, opiniones y/o creencias actuales y constituyen "declaraciones prospectivas", que pueden identificarse mediante el uso de terminología prospectiva como "puede", "espera", "anticipa", "proyecta", "estima", "tiene la intención", "objetivo" o "cree", o terminología comparable o sus negaciones.

No se ofrece ninguna declaración ni garantía con respecto a dichas afirmaciones, y los acontecimientos futuros pueden diferir sustancialmente de los reflejados o contemplados en ellas.

Ninguna declaración o representación contenida en este documento es legalmente vinculante para Fidelity International ni para el destinatario. Las marcas comerciales, los derechos de autor y demás derechos de propiedad intelectual de terceros son y seguirán siendo propiedad de sus respectivos dueños.

Europa: Emitido por FIL (Luxemburgo) SA (autorizada y supervisada por la CSSF, Commission de Surveillance du Secteur Financier), FIL Gestion (autorizada y supervisada por la AMF (Autorité des Marchés Financiers) N°GP03-004, 21 Avenue Kléber, 75016 Paris) y FIL Investment Switzerland AG.

En Hong Kong, este documento se distribuye únicamente a inversores institucionales que se ajustan a la definición de «inversor profesional institucional» contemplada en el Código de Conducta para Personas Autorizadas o Registradas ante la Comisión de Valores y Futuros, así como en los apartados (a) a (i) de la definición de «inversor profesional» establecida en la Ordenanza de Valores y Futuros. Este material es emitido por FIL Investment Management (Hong Kong) Limited y no ha sido revisado por la Comisión de Valores y Futuros.

Singapur: FIL Investment Management (Singapore) Limited (N.º de registro mercantil: 199006300E) es el representante legal de Fidelity International en Singapur. Este documento/anuncio no ha sido revisado por la Autoridad Monetaria de Singapur. Esta información no debe reproducirse ni distribuirse sin autorización previa. Dirigido exclusivamente a inversores institucionales, según lo definido en la Ley de Valores y Futuros de 2001.

En Taiwán, operado independientemente por Fidelity Securities Investment Trust Co. (Taiwan) Limited. 11F, No. 68, Sección 5, Zhongxiao East Road, Distrito Xinyi, Taipei 110, Taiwán, ROC. Número de atención al cliente: 0800-00-9911. N.º 004 de 2023 Jin-Guan-Tou-Xin-Sin. Sitio web: www.fidelity.com.tw. FIL SITE opera independientemente en Taiwán. Este documento se distribuye en Taiwán únicamente a clientes de instituciones financieras que se ajustan a la definición de «clientes de instituciones financieras» según lo dispuesto en el artículo 3, párrafos 3 y 4 del Reglamento que rige los productos estructurados offshore.

GCT260240GLO