BITCOIN PRIMERO:

Por qué los inversores deben considerar el Bitcoin por separado de otros activos digitales

CHRIS KUIPER, CFA, DIRECTOR DE INVESTIGACIÓN
JACK NEUREUTER, ANALISTA DE INVESTIGACIÓN

ENERO 2022

Fidelity DIGITAL ASSETS℠

RESUMEN EJECUTIVO

Una vez que los inversores han decidido invertir en activos digitales, la siguiente pregunta es: "¿Cuál?". Por supuesto, el bitcoin es el activo digital más reconocido y el primero, pero hay cientos e incluso miles de otros activos digitales en el ecosistema.

Una de las primeras preocupaciones de los inversores respecto al bitcoin es que, como primer activo digital, puede ser vulnerable a la destrucción innovadora de los competidores (como la historia de MySpace y Facebook). Otra consideración común que rodea al bitcoin es si ofrece la misma recompensa potencial o la misma ventaja que algunos de los activos digitales más nuevos y más pequeños que han surgido.

En este documento proponemos:

- El Bitcoin se entiende mejor como un bien monetario, y una de las principales tesis de inversión para el bitcoin es como activo de almacenamiento de valor en un mundo cada vez más digital.
- Bitcoin es fundamentalmente diferente de cualquier otro activo digital. No es probable que ningún otro activo digital mejore a bitcoin como bien monetario porque bitcoin es el dinero digital más seguro, descentralizado y sólido (en relación con otros activos digitales) y cualquier "mejora" tendrá necesariamente que hacer frente a compensaciones.
- No existe necesariamente una exclusividad mutua entre el éxito de la red Bitcoin y todas las demás redes de activos digitales. Más bien, el resto del ecosistema de activos digitales puede satisfacer diferentes necesidades o resolver otros problemas que Bitcoin simplemente no resuelve.
- Otros proyectos que no son de Bitcoin deberían ser evaluados desde una perspectiva diferente a la de Bitcoin.
- El bitcoin debe considerarse un punto de entrada para los asignadores tradicionales que buscan ganar exposición a los activos digitales.

- Los inversores deben tener dos marcos distintos para considerar la inversión en este ecosistema de activos digitales. El primer marco examina la inclusión del bitcoin como bien monetario emergente, y el segundo considera la adición de otros activos digitales que presentan propiedades similares a las del capital riesgo.

¿QUÉ ES EL BITCOIN?

Está fuera del alcance de este documento ofrecer una explicación detallada del bitcoin. Sin embargo, creemos que es importante destacar algunos de los aspectos básicos necesarios para entender cómo bitcoin ha mantenido una ventaja competitiva en la búsqueda de representar el bien monetario no soberano de facto del ecosistema de activos digitales.

Bitcoin la red vs. bitcoin el activo

Uno de los conceptos más confusos para aquellos que son nuevos en el mundo del bitcoin es entender que la palabra "bitcoin" puede referirse a dos cosas relacionadas, pero claramente diferentes. Está el Bitcoin, la red o sistema de pago, y luego está el bitcoin, el token o activo. Para evitar confusiones, adoptaremos la norma de escribir Bitcoin en mayúsculas cuando nos refiramos a la red y usaremos una minúscula para el bitcoin, el token o el activo.

Bitcoin fue primero sólo una idea que se propuso resolver el problema de crear un verdadero sistema de dinero electrónico entre pares. Aunque en el mundo físico podemos realizar transacciones sin intermediario utilizando dinero en efectivo, hasta que se inventó Bitcoin esto no era posible en el ámbito digital. Esta idea se puso en práctica escribiendo código. Por lo tanto, Bitcoin es sólo código y la red Bitcoin está formada por millones de ordenadores que ejecutan este mismo software Bitcoin. Este código actúa como un protocolo y proporciona las reglas que rigen la red Bitcoin. Esta red opera un sistema de pagos, donde los usuarios pueden enviar y recibir un token digital, también llamado bitcoin

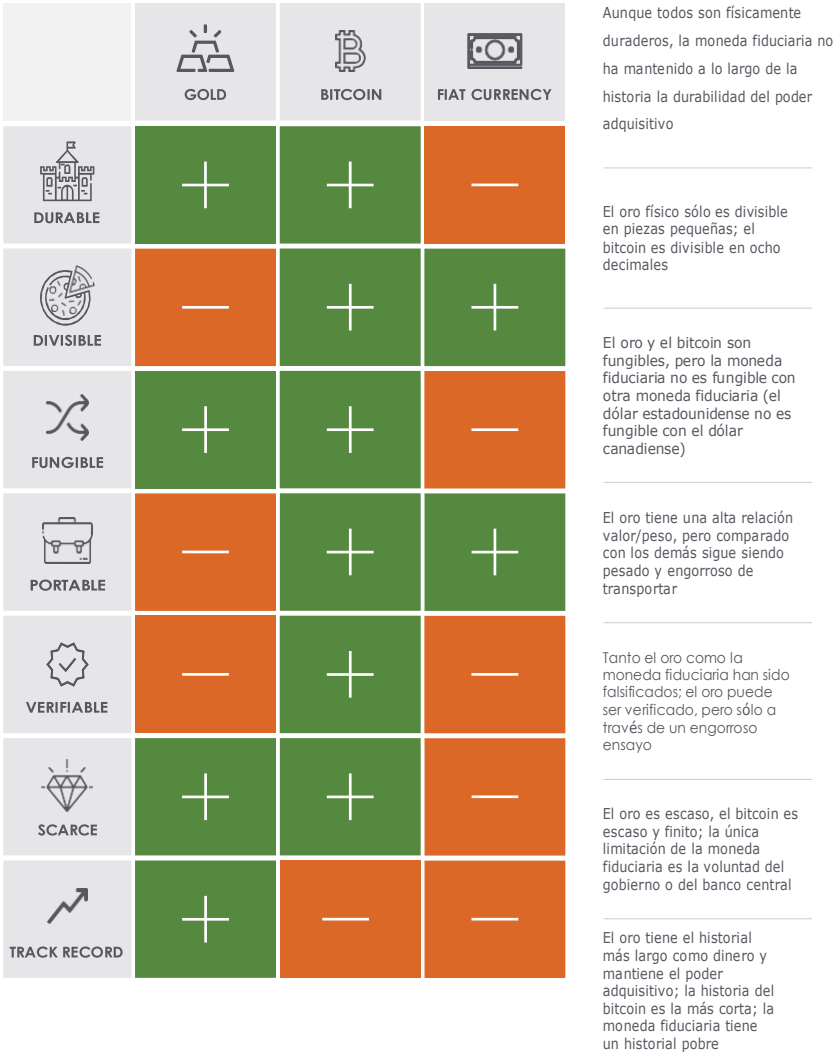
La red Bitcoin no es compatible con otras redes

Cualquiera puede unirse a la red Bitcoin o abandonarla, siempre que siga las reglas básicas. Cualquiera que intente cambiar las reglas sin el consenso de un número suficiente de participantes será excluido de la red. Por tanto, aunque el código de Bitcoin es de código abierto y puede copiarse y modificarse, estas copias o derivaciones de Bitcoin son redes completamente separadas y no son "retrocompatibles" con la red original de Bitcoin. Además, los tokens de Bitcoin son nativos de la red Bitcoin y no pueden ser retirados o transportados a otra red blockchain. La importancia de esto se

revelará más adelante en este documento cuando discutamos el poder de los efectos de red y por qué vemos que una red domina el mercado.

POR QUÉ CREEMOS QUE EL BITCOIN SE ENTIENDE MEJOR COMO UN BIEN MONETARIO

¿Qué es el dinero? Creemos que el dinero es una herramienta que permite el intercambio más que el trueque. A lo largo de la mayor parte de la historia hemos visto a los humanos iterar en busca de la "mejor" representación del dinero. Un bien monetario es un bien que se valora por su capacidad de intercambio por otros bienes, no por su consumo o uso. A lo largo de la historia se han utilizado, diversos bienes como dinero, como conchas, cuentas piedras, pieles y wampum. Lo que nos lleva a preguntarnos ¿por qué algunas cosas se convierten en un bien monetario y otras no? Los economistas e historiadores sugieren que la respuesta se encuentra en una serie de características que hacen que un bien sea "buen dinero"[1]. Cuantas más características posea un bien, mejor podrá servir como dinero o más probable será que surja o sea aceptado como dinero.



[1] Véase "On the Origins of Money," Carl Menger, Economic Journal 2 (1892)

[2] Por ejemplo, después de Bretton Woods ha habido 201 crisis monetarias entre 1975 y 2007, es decir, una media de más de cinco por año. Véase Glick, Reuven, and Michael Hutchison. "Currency Crisis." Serie de documentos de trabajo del Banco de la Reserva Federal de San Francisco, Sept. 2011, https://www.frbsf.org/economic-research/files/wp11-22bk.pdf

Está claro que Bitcoin posee muchas de las cualidades del dinero, combinando la escasez y la durabilidad del oro con la facilidad de uso, almacenamiento y transporte del fiat (incluso mejorándolo).

También cabe destacar que, al igual que otros bienes monetarios, el bitcoin no es una empresa, o paga dividendos ni tiene flujos de caja. Por lo tanto, su valor debe derivarse de su capacidad para cumplir mejor las características de un bien monetario en comparación con las alternativas tradicionales.

El valor de Bitcoin se debe a su escasez exigible

Una de las mayores características de las propiedades de bitcoin es su escasez. No sólo es escaso (la tasa de inflación actual de bitcoin, del 1,8%, es aproximadamente igual a la tasa de inflación del oro en este momento) 3, sino que, a diferencia del oro, también es probadamente finito. Sólo habrá 21 millones de bitcoins. Ningún otro activo digital posee una política monetaria inmutable al nivel de bitcoin. En otras palabras, la política monetaria de bitcoin puede considerarse la más creíble.

Pero, ¿cómo se impone la escasez de bitcoin (su tope de oferta de 21 millones)? Hay dos características clave que sustentan esta credibilidad y que son necesarias para entender el límite de suministro de bitcoin y por qué se diferencia de cualquier otro activo digital.

La primera es la descentralización de bitcoin. Ninguna persona, corporación o gobierno posee o controla la red Bitcoin o las reglas que gobiernan la red. Al ser una red completamente descentralizada que ejecuta un código abierto, los participantes en la red deben adherirse a las reglas del código que gobiernan la red. El límite de suministro de 21 millones se incluyó en el código fuente original de bitcoin, que sigue funcionando en la actualidad.

Pero si la red se rige por un mero código, ¿no se puede cambiar este código? Sí, pero sólo mediante el consenso de los participantes en la red (los operadores de los nodos). Un cambio en el programa de suministro de bitcoin es algo que podría ocurrir en teoría, pero que casi nunca ocurrirá en la práctica. En primer lugar, conseguir el consenso es enormemente difícil porque la red de Bitcoin y los participantes en el mercado están muy dispersos. No hay un gran "consorcio" que tenga influencia o poder de voto. Y lo que es más importante, la red fue diseñada con incentivos para no cambiar este tope de oferta. A los participantes actuales de la red no les interesaría económicamente aumentar o ajustar el límite de suministro, ya que hacerlo solo sirve para inflar la oferta de bitcoin y diluir el valor de sus participaciones, o en el caso de los mineros, sus recompensas de minería. Aquí vemos los poderosos efectos de la teoría de juegos en funcionamiento, ya que a todos los participantes

[3] World Gold Council, 2019, annual reports and https://www.gold.org/about-gold/gold-supply/gold-mining/how-much-gold

les conviene coordinarse, cooperar y no cambiar el límite de la oferta.

En segundo lugar, la red Bitcoin es resistente a la censura. Dado que ninguna persona, corporación o gobierno posee o controla la red Bitcoin, es muy resistente a la censura. Además, la red Bitcoin no tiene límites geográficos, lo que hace difícil que un estado nación asuma el control o la regulación de la red y del propio código central de Bitcoin.

Para repasar la lógica paso a paso de por qué creemos que el bitcoin es un bien monetario que tiene valor:

1. Un bien monetario es algo que tiene un valor atribuido por encima de su valor de utilidad o de consumo. Aunque la red de pagos de Bitcoin tiene ciertamente un valor de utilidad, la gente también atribuye un valor monetario superior a los tokens de bitcoin.
2. Una de las principales razones por las que los inversores atribuyen valor al bitcoin es su escasez. Su oferta fija es la razón por la que tiene la capacidad de ser un depósito de valor.
3. La escasez de Bitcoin se sustenta en sus características de descentralización y resistencia a la censura.
4. Estas características están codificadas en bitcoin y es casi seguro que nunca se cambiarán porque las mismas personas que atribuyen valor a bitcoin y lo poseen no tienen ningún incentivo para hacerlo. De hecho, los participantes de la red están incentivados a defender estas mismas características de un activo escaso y un libro de contabilidad inmutable.

Por qué creemos que el bitcoin tiene el potencial de ser el principal bien monetario

Los inversores pueden estar de acuerdo en que el bitcoin posee muchas de las cualidades que hacen que sea un buen dinero, pero ¿quién puede decir que sólo puede existir o existirá un bien monetario?

No nos atreveremos a predecir que sólo habrá un dinero, pero sí creemos que un bien monetario llegará a dominar el ecosistema de los activos digitales debido a los poderosos efectos de las redes.

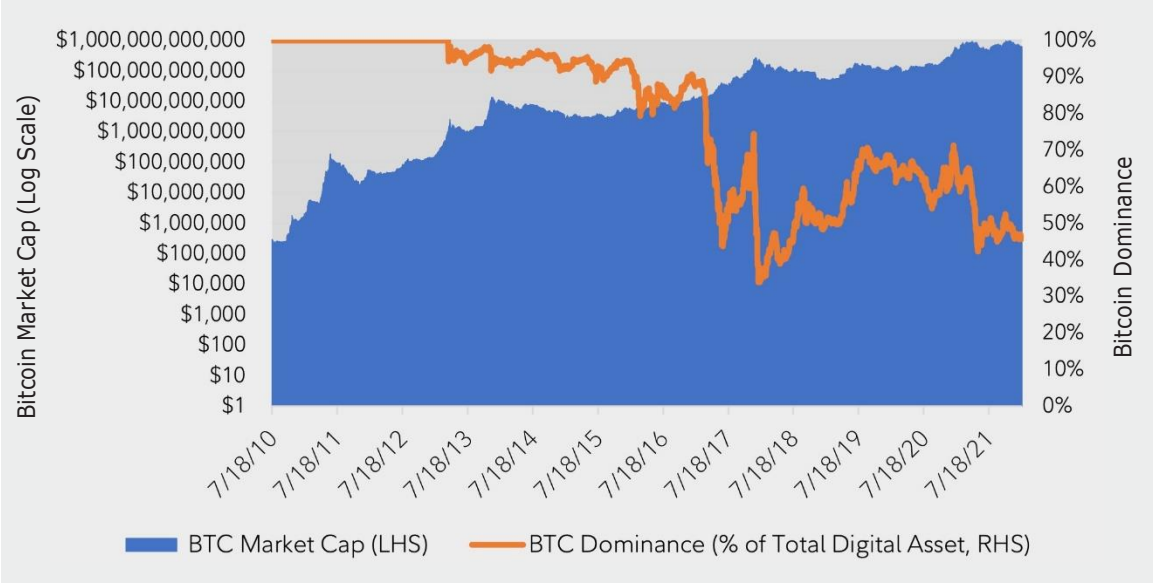
Los efectos de las redes monetarias son extremadamente poderosos

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

Si los inversores buscan un activo digital como bien monetario, uno con la capacidad de actuar como depósito de valor, entonces elegirán naturalmente el que tenga la red más grande, más segura, más descentralizada y líquida. El bitcoin, como primer activo digital realmente escaso que se inventó, recibió una ventaja por ser el primero en actuar y la ha mantenido a lo largo del tiempo. Obsérvese que, aunque el dominio de Bitcoin, o su capitalización de mercado como porcentaje de todo el ecosistema de activos digitales, ha disminuido del 100% al 50% aproximadamente, esto no se debe a que haya disminuido su tamaño, sino a que el resto del ecosistema ha crecido.

DOMINIO DEL BITCOIN



Fuente de los datos: Coin Metrics, Fecha: 1/18/2022

Las redes monetarias también tienen una propiedad reflexiva. Las personas observan a otros que se unen a una red monetaria, lo que les incentiva a unirse también, ya que también quieren estar en la red donde residen sus compañeros o socios comerciales. Esto puede observarse a menor escala con las redes de pago actuales, ya que plataformas como PayPal y Venmo han crecido a un ritmo acelerado.

En el caso de bitcoin, la propiedad reflexiva es aún más pronunciada porque no sólo 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 tiene propiedades monetarias superiores y optan por almacenar su riqueza en él, la demanda aumenta. Esto, a su vez, conduce a un aumento de los precios (sobre todo porque la oferta es inelástica o no responde al precio). Los

mineros se ven entonces incentivados a aumentar su gasto de capital y su potencia de cálculo, ya que unos precios más altos conllevan mayores márgenes de beneficio. Una mayor potencia de cálculo dedicada a la minería de bitcoins conduce a una mayor seguridad de la red, lo que a su vez hace que el activo sea más atractivo, lo que conduce de nuevo a más usuarios e inversores.

Es probable que esta competencia en la red dé lugar a un escenario en el que el ganador se lleve todo a medida que la red crezca y adquiera más valor, ya que la elección de cualquier otra red monetaria que no se convierta en la dominante supondrá una pérdida de la inversión. Todo inversor que desee almacenar valor en un bien monetario está eligiendo la red monetaria a la que opta, lo reconozca o no.

Cualquier bien monetario posterior sería "reinventar la rueda"

La frase "no reinventar la rueda" es tan común que se ha convertido en un cliché. Sin embargo, creemos que es aplicable al bitcoin como bien monetario digital. La invención de la rueda representó una tecnología totalmente nueva que, una vez inventada, nunca pudo ser reinventada. Del mismo modo, nunca antes en la historia de la humanidad el problema de la escasez digital y de un verdadero dinero electrónico entre pares había sido resuelto hasta que se inventó Bitcoin. Resolver este problema no fue simplemente una mejora incremental, sino un salto adelante o un desbloqueo del rompecabezas de cómo podía existir la escasez digital.

Dado que Bitcoin es actualmente la red monetaria más descentralizada y segura (en relación con todos los demás activos digitales), una red blockchain y un activo digital más nuevos que intenten mejorar a bitcoin como bien monetario tendrán necesariamente que diferenciarse sacrificando una o ambas propiedades, una idea que exploramos con más detalle a continuación (el "Trilema Blockchain"). Un competidor que intente simplemente copiar todo el código de Bitcoin también fracasará, ya que no habrá ninguna razón para pasar de la mayor red monetaria a una completamente idéntica, pero con una fracción de su tamaño.

El efecto Lindy y las cualidades antifrágiles de Bitcoin

El efecto Lindy, también conocido como Ley de Lindy, es una teoría según la cual cuanto más tiempo sobreviva una cosa no perecedera, más probable será que sobreviva en el futuro. Por ejemplo, una obra de teatro de Broadway que ha estado en cartelera durante diez años tiene más probabilidades de seguir en cartelera otros diez años que una que sólo ha estado en cartelera un año. Creemos que lo mismo puede aplicarse a Bitcoin. Cada minuto, hora, día y año que Bitcoin sobrevive, aumenta sus posibilidades de continuar en el futuro, ya que gana más confianza y sobrevive a más choques. También vale la pena señalar que esto va de la mano con la propiedad de antifragilidad, donde algo se vuelve más robusto o más fuerte con cada ataque o tiempo que el sistema está bajo alguna forma de estrés.

De hecho, si a un inversor se le presentara la idea de Bitcoin y se le pidiera que elaborara una lista de factores de estrés, ataques, choques o fallos que probablemente supondrían la desaparición de esta tecnología naciente, probablemente subestimaría todos los acontecimientos negativos que Bitcoin ya ha soportado y que no han resultado ser la sentencia de muerte de la red.

Una lista no exhaustiva de algunos de los acontecimientos negativos que ha soportado bitcoin:

Creado por una persona(s) anónima(s) cuyo verdadero motivo o cualquier afiliación se desconoce	Algunos tokens de bitcoin han sido confiscados por el FBI	Múltiples hacks de intercambio	Ha sido declarado "muerto" cientos de veces por los por los principales medios de comunicación y famosos inversores, directores generales, etc.
Utilizado en la web oscura para compras ilícitas	Ha soportado una "guerra civil" en relación con el código del núcleo (véase la sección sobre la guerra del tamaño de los bloques)	El precio ha sufrido múltiples caídas de más del 50%, muchas superiores al 80%.	Prohibido en muchos países
Ha sido tachado de fraude, esquema ponzi, apuesta especulativa	Sigue siendo la principal forma de pago de los ataques de ransomware	Ha soportado múltiples bifurcaciones en su código	Copiado por los competidores miles de veces

Por qué es improbable que otro activo digital desbanque al bitcoin como bien monetario

Quizás los inversores estén de acuerdo en que el bitcoin es actualmente el mejor bien monetario del mercado de activos digitales y que es probable que un bien monetario digital domine el mercado debido a los efectos de red.

Sin embargo, ¿no podría crearse una versión superior o mejorada de bitcoin y convertirse en el bien

monetaria dominante? ¿No es el código de bitcoin de código abierto para que cualquiera pueda copiarlo y mejorarlo?

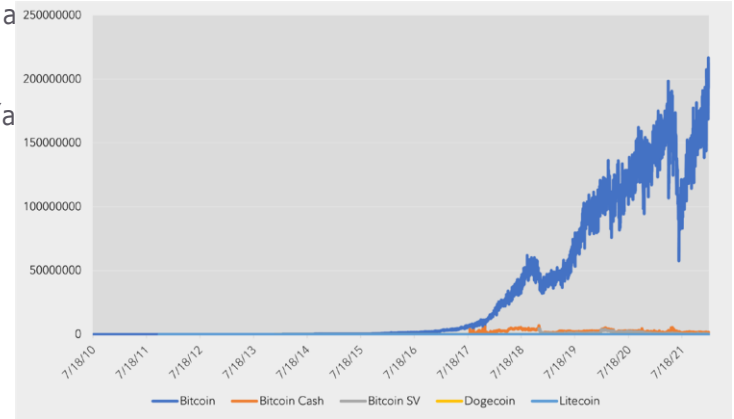
Aunque ciertamente es posible en un mercado libre de activos digitales emergentes, creemos que es muy poco probable que el bitcoin sea sustituido por un activo digital "mejorado" por varias razones. Una de las principales razones es que cualquier mejora en una característica de bitcoin, como la mejora de su velocidad o escalabilidad, conduce a una reducción de otra característica, como el nivel de descentralización o seguridad de bitcoin. Esta disyuntiva se conoce como el trilema de la cadena de bloques.

El trilema de la cadena de bloques

Ya a principios de la década de 1980, los informáticos identificaron un tipo de trilema en las bases de datos descentralizadas4. Más recientemente, el creador de Ethereum, Vitalik Buterin, ha esbozado una variación de este trilema, conocida como el "trilema de la cadena de bloques", en la que afirma que una base de datos descentralizada (de la que Bitcoin es un tipo) sólo puede ofrecer dos de tres garantías a la vez: descentralización, seguridad o escalabilidad.[5]

La **seguridad** se refiere a la probabilidad de que la red pueda ser atacada o comprometida. En el caso de una red descentralizada como Bitcoin, la principal preocupación es un ataque del 51%, por el que una sola persona o entidad controla más de la mitad de la potencia de cálculo de la red Bitcoin (conocida como tasa de hash). Si esto se consigue, el atacante podría controlar la red o, más concretamente, realizar cambios en el libro mayor abierto, como realizar un doble gasto o anular transacciones. La confianza en la red se perdería y podría colapsar toda la red. A medida que la red Bitcoin se hace más grande, con más nodos y mineros distribuidos entre más personas, entidades y áreas geográficas, se hace más difícil y costoso de atacar

TASA MEDIA DE HASH



Fuente de los datos: Coin Metrics, Fecha: 1/18/2022

[4] Véase "The CAP Theorem", también conocido como Teorema de Brewer, para una de las primeras compensaciones identificadas entre tres propiedades en una base de datos descentralizada.

[5] Conocido específicamente como el "Trilema de la Escalabilidad" por Vitalik Buterin, https://eth.wiki/sharding/Sharding-FAQs

Lamentablemente, debido a las diferencias en los algoritmos de hash, la tasa de hash de bitcoin no puede compararse directamente con la tasa de hash de otros activos digitales, sobre todo el éter, el segundo mayor activo digital por capitalización de mercado. Sin embargo, podemos comparar el uso total de energía anual como indicador de seguridad, con un mayor uso de energía como medida de más recursos mineros dedicados a la seguridad de la red. Según esta medida, se estima que el bitcoin consume aproximadamente 137 teravatios-hora (TWh) 6 anuales, frente a los 25 TWh de Ethereum.7

La descentralización se refiere al grado de control que una persona, entidad o grupo puede tener sobre un sistema o red. En una red descentralizada, el consenso se consigue mediante una especie de mecanismo de votación. En este sistema ninguna entidad puede controlar o restringir los datos. En una red descentralizada abierta, cualquiera es también libre de unirse y ninguna entidad puede excluirlo siempre que siga las reglas o el protocolo de la red. Esto permite que la red funcione sin intermediarios. El coste de una mayor descentralización es un menor rendimiento de la red, o la velocidad a la que puede pasar la información debido a la necesidad de un mayor consenso. Lo contrario de una red descentralizada sería una red completamente centralizada en la que un intermediario controla todos los aspectos de la red. La ventaja de esto es la increíble velocidad y rendimiento, ya que no es necesario un consenso, pero la desventaja es la necesidad de confiar en este único intermediario.

El Bitcoin es el activo digital más descentralizado en base a muchos factores. Por ejemplo, como señalaba un reciente informe de Coin Metric8, el bitcoin sigue mostrando una creciente descentralización a medida que el número de poseedores se ha distribuido, las direcciones activas siguen aumentando y los pools de minería de Bitcoin siguen siendo más fragmentados y competitivos. Además, la potencia de cálculo de Bitcoin, conocida como hash rate, ha experimentado recientemente una gran distribución. Hace sólo unos años se estimaba que aproximadamente el 75% de la tasa de hash de la red Bitcoin procedía de operadores ubicados en China y sólo el 4% de Estados Unidos. Recientemente, debido a la prohibición de China sobre estas actividades, prácticamente ninguno está ubicado en China y ahora Estados Unidos ocupa el primer lugar con aproximadamente un 35%.9

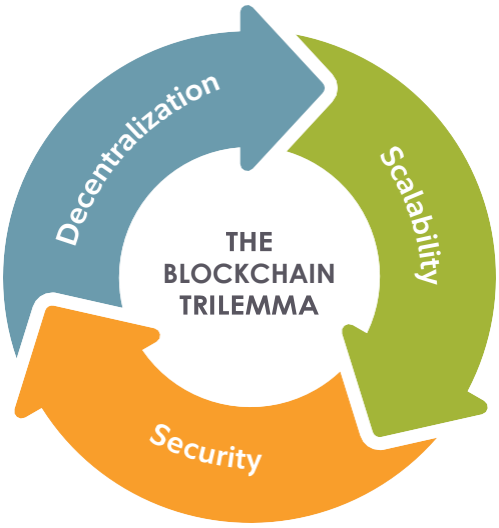
[6] Cambridge Bitcoin Electricity Consumption Index (CBECI) (ccaf.io), consultado 1/21/2022
[7] Ethereum Emissions (kylemcdonald.github.io), consultado 1/21/2022
[8] https://coinmetrics.io/measuring-bitcoins-decentralization
[9] https://ccaf.io/cbeci/mining_map

La **escalabilidad** se refiere a lo bien que la red puede manejar el crecimiento, como el crecimiento del número de usuarios y el número de transacciones que la red puede manejar en un tiempo limitado. La escalabilidad ha sido el talón de Aquiles de la red Bitcoin, ya que maximiza la descentralización y la seguridad, pero como resultado es la red con uno de los rendimientos de transacción más lentos. La red Bitcoin añade un nuevo bloque y valida las transacciones cada 10 minutos de media, y como el tamaño de los bloques de Bitcoin es limitado, sólo un número determinado de transacciones puede caber en cada bloque. Para poner esto en perspectiva, la red Bitcoin es capaz de procesar aproximadamente de tres a siete transacciones por segundo, frente a una red de pagos altamente centralizada, como Visa, que procesa aproximadamente 1.700 transacciones por segundo con la capacidad de escalar y procesar múltiples veces si es necesario.

Ninguna de las características anteriores es, por sí sola, mejor que otra. Depende del caso de uso. Algunos usuarios pueden preferir la escalabilidad a la descentralización o viceversa. Lo único que queremos decir aquí es que hay una compensación inherente.

En resumen, creemos que bitcoin es actualmente la red monetaria más segura y descentralizada. Por lo tanto, esto excluye a otras redes que compiten en diferentes casos de uso además del dinero.

También creemos que la red bitcoin seguirá siendo la más segura y descentralizada en el futuro debido al trilema de la cadena de bloques, tal y como se ha descrito anteriormente y también como se ejemplifica en un ejemplo del mundo real (la guerra del tamaño de los bloques). También creemos que, dado que las redes monetarias tienen efectos de red masivos, la seguridad y la descentralización de bitcoin se fortalecerán con el tiempo. ¿Podría aparecer otra red en el futuro que mejore de alguna manera a bitcoin como red monetaria? Admitimos que hay una posibilidad no nula, pero creemos que es increíblemente pequeña debido a nuestros argumentos aquí expuestos.



Un ejemplo del mundo real de intentar "mejorar el bitcoin": La guerra del tamaño de los bloques

Como hemos señalado anteriormente, el rendimiento de las transacciones de Bitcoin está limitado

tanto por el tiempo que transcurre entre la adición de cada bloque y la validación de las transacciones (aproximadamente cada 10 minutos) como por el tamaño del bloque (poco más de un megabyte), que limita el número de transacciones que pueden caber en cada bloque.

Por ello, algunos usuarios y desarrolladores propusieron una forma aparentemente sencilla y directa de solucionar este problema: aumentar el tamaño del bloque a más de un megabyte. Aunque esto puede parecer un cambio sencillo y no controvertido, en realidad dio lugar a una feroz guerra dentro de la comunidad de desarrolladores que duró años.[10]

El debate puede resumirse dividiendo las opiniones opuestas en dos bandos: los "pequeños bloqueadores" frente a los "grandes bloqueadores". Mientras que el tamaño de los bloques era la pieza de código específica en el centro del debate, la cuestión en juego era en realidad más amplia en cuanto a los principios de lo que es Bitcoin y cómo debería o no evolucionar. Aquellos que querían el tamaño de bloque original, o bloques más pequeños, generalmente estaban a favor de reglas de protocolo robustas que deberían ser muy difíciles de cambiar con un enfoque a largo plazo en la estabilidad de Bitcoin. Este ethos continúa hoy en día con muchos cambios de código propuestos, incluso actualizaciones que se consideran mejoras, que no se implementan. En opinión de los pequeños bloqueadores, cualquier cambio en el código podría abrir la red Bitcoin a un vector de ataque nuevo o imprevisto. Los pequeños bloqueadores también creían que la posibilidad de que los individuos o los usuarios medios pudieran gestionar un nodo personal era importante para preservar la seguridad y la descentralización de Bitcoin. Los bloques más grandes significarían más historia que archivar en la cadena de bloques, y por lo tanto harían que el funcionamiento de un nodo (el libro de contabilidad de Bitcoin) fuera más difícil y costoso.

Por otro lado, los grandes bloqueadores querían reglas de protocolo que pudieran cambiarse más fácil y rápidamente para centrarse en desmantelar los obstáculos a corto plazo o abordar las oportunidades que surgieran con una mentalidad más de "start-up". Los bloques más grandes permitirían una mayor escalabilidad y transacciones más rápidas.

Sin embargo, el aumento del tamaño de los bloques no está exento de contrapartidas. En primer lugar, los bloques más grandes conducen a cadenas de bloques más grandes. Actualmente, toda la cadena de bloques (todas las transacciones registradas en el libro de contabilidad de código abierto de Bitcoin) tiene un tamaño de aproximadamente 400 gigabytes.11 Esto hace que casi cualquiera pueda descargar toda la cadena de bloques y ejecutar un nodo completo desde su ordenador personal o incluso desde un ordenador sencillo especialmente construido que cuesta aproximadamente 100 dólares. Si la cadena de bloques fuera más grande, sería más caro y difícil para los individuos

gestionar un nodo y podría llevar a una menor descentralización, ya que sólo las corporaciones o aquellos con el equipo más caro podrían construir y gestionar nodos.

Los bloques más grandes también significan que podría haber bloques no completos, lo que llevaría a unas tasas de transacción bajas. Si bien es cierto que esto ayuda a la escalabilidad, a la inversa podría reducir los incentivos para los mineros debido a las menores tasas de transacción, sobre todo porque la subvención por bloque (la otra parte de las recompensas que reciben los mineros) sigue reduciéndose a la mitad cada cuatro años. Si los mineros dejan de operar, esto disminuye la seguridad de la red de Bitcoin.

En resumen, la guerra del tamaño de los bloques demuestra el trilema de la cadena de bloques inherente a la red de Bitcoin. Los bloques más grandes podrían aumentar la escala o el rendimiento, pero con la pérdida potencial de descentralización y seguridad.

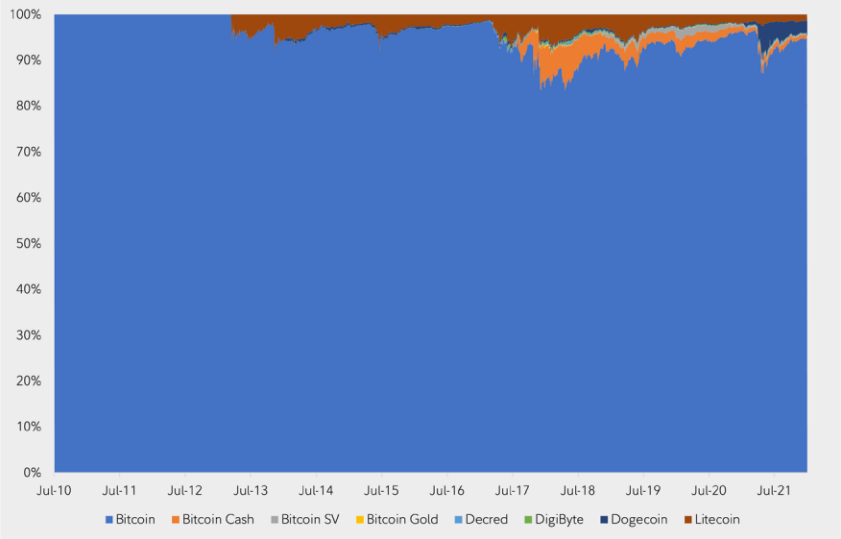
[10] Para más detalles y un relato de primera mano sobre esto, véase "The Blocksize War: The battle over who controls Bitcoin's protocol rules" de Jonathan Bier (2021)

[11] https://www.blockchain.com/charts/blocks-size

El otro punto importante de esta historia es que los cambios propuestos resultarían (y resultaron) en una bifurcación dura, lo que significa que el cambio en el código no sería compatible hacia atrás y todos los nodos tendrían que actualizarse para evitar una división en la red. Los diferentes hard forks que han surgido a causa o en relación con la guerra del tamaño de los bloques ha fracasado por completo (como Bitcoin XT y Bitcoin Classic) o han luchado por conseguir algún tipo de dominio del mercado (como Bitcoin Cash (BCH) y Bitcoin SV (BSV) o "Satoshi's Vision").

Bitcoin sigue dominando la capitalización de mercado de todos los tokens monetarios de la competencia, como puede verse en el gráfico:

DOMINIO DEL BITCOIN VS LA COMPETENCIA



Fuente de los datos: Coin Metrics, Fecha: 1/18/2022

Estudio de caso de Bitcoin Cash

Una de las bifurcaciones duras más notables que surgió de la guerra del tamaño de los bloques fue Bitcoin Cash (BCH). Los defensores de este hard fork creen que bitcoin debería ser ante todo un "sistema de efectivo electrónico entre pares" o un sistema que pueda manejar una gran cantidad de transacciones. En otras palabras, los defensores de Bitcoin Cash creen que bitcoin debería centrarse primero en convertirse en un medio de intercambio fiable más que en un depósito de valor.

Insistimos en que no hay nada intrínsecamente "malo" en este enfoque, pero demuestra una vez más las compensaciones que se hacen para obtener más escalabilidad. Tampoco hay nada que impida a los desarrolladores y al mercado elegir Bitcoin Cash para realizar pagos más rápidos o baratos a costa de la seguridad y la descentralización. Sin embargo, podemos ver que, en términos de valor global, con la capitalización de mercado de bitcoin 100 veces superior a la de Bitcoin Cash (BCH), los inversores han seguido eligiendo bitcoin (BTC) como la red monetaria preferida y, por tanto, parecen valorar un depósito de valor seguro y sólido por encima de los pagos más rápidos o baratos.

Bitcoin como bien monetario superior es más valioso que una red de pagos mejor

Esto nos lleva a otro punto de por qué creemos que el bitcoin debe ser considerado principalmente como un bien monetario en lugar de una red de pago. El hecho de que el mercado haya mostrado una preferencia hacia el bitcoin, que es más lento como sistema de pago en comparación con otros activos digitales y blockchains, indica que el mercado valora actualmente un almacén de valor altamente seguro y descentralizado en lugar de otra red de pago. Como señalamos anteriormente, la revolucionaria invención de Bitcoin fue resolver el problema de la escasez digital y crear un depósito digital de valor, no hacer una mejora incremental de un sistema de pago.

Estudio de caso de Ethereum

Está fuera del alcance de este documento examinar la red Ethereum y el token ether en su totalidad. Sin embargo, es instructivo observar algunas de las similitudes y diferencias entre el bitcoin y el ether, que es el segundo mayor activo digital por capitalización de mercado.[12]

Desde sus inicios y como idea publicada en forma de libro blanco, Bitcoin se propuso resolver el problema de una "versión puramente peer-to-peer de dinero electrónico".13 Su red se diseñó para ser descentralizada y segura, de modo que se pudiera enviar valor sin tener que confiar en un

intermediario. Esto se combinó con un calendario monetario preprogramado y un tope de oferta creíble de 21 millones, lo que dio a bitcoin la capacidad de convertirse en un bien monetario y un depósito de valor.

Ethereum también comenzó como un libro blanco, publicado originalmente en 2013 por Vitalik Buterin.14 En resumen, Ethereum se propuso tomar la tecnología blockchain iniciada por Bitcoin y ampliarla para incluir más capacidades, sobre todo la capacidad de realizar transacciones más complejas. Del libro blanco de Ethereum: "Lo que Ethereum pretende ofrecer es un blockchain con un lenguaje Turing de programación completo incorporado que puede utilizarse para crear "contratos" que pueden utilizarse para codificar funciones de transición de estado arbitrarias..."

Esto permite que la red de blockchain de Ethereum albergue y ejecute "contratos inteligentes" que pueden utilizarse para programar todo tipo de aplicaciones. Es por esta razón que a algunos les gusta referirse a la red Ethereum como un "ordenador mundial distribuido". La red también permite que se emitan diferentes tokens en el blockchain de Ethereum. Esta red actúa como una especie de plataforma que otros pueden utilizar para construir múltiples aplicaciones sobre ella, incluyendo aplicaciones financieras descentralizadas, juegos, herramientas de medios sociales, etc.

Aunque Ethereum puede ser considerada por algunos como una red superior o más avanzada en comparación con Bitcoin, las capacidades adicionales y la flexibilidad tienen un coste, sobre todo una red más compleja que aumenta la posibilidad de que se produzcan errores de software, así como una menor descentralización y una posible disminución de la seguridad.

[12] https://coinmetrics.io/crypto-prices
[13] Nakamoto, S. (2008) Bitcoin: A Peer-to-Peer Electronic Cash System. https://bitcoin.org/bitcoin.pdf
[14] https://ethereum.org/en/whitepaper

A continuación, se resumen algunas de las diferencias y compensaciones entre las redes Bitcoin y Ethereum:

	RED BITCOIN	RED ETHEREUM
Objetivo Principal	Red monetaria descentralizada, segura	Ordenador mundial distribuido
Velocidad de implementación de las mejoras	Muy lenta y deliberada	Rápida y con capacidad de respuesta a la demanda de los usuarios
¿Contratos programables o inteligentes?	No	Sí
¿Capacidad de albergar múltiples tokens?	No, solo bitcoin	Sí
Política monetaria	Fija, pre-programada y nunca ha cambiado	Ha cambiado y se espera que vuelva a cambiar[15]
Auditoría (¿Cuántos tokens existen?)	Sí, muy fácil de auditar en cualquier momento	Se puede auditar, pero podría ser más difícil[16]
Nivel de Centralización	Muy descentralizada	Más centralizada[17]
Coste del nodo	Barato (~$100)	Caro
Mecanismo de consenso	Proof-of-Work	Actualmente proof-of-work; hay planes para pasar a proof-of-stake[18]

[15] https://decrypt.co/84520/ethereum-supply-pace-shrink-eth-2-upgrade
[16] https://www.coindesk.com/tech/2020/08/11/how-much-ether-is-out-there-ethereum-developers-create-new-scripts-for-self-verification/
[17] Un análisis de 2019 sugería que más del 60% de todos los nodos de Ethereum estaban alojados en un puñado de servicios de los principales proveedores de la nube: https://chainstack.com/the-ethereum-cloud-vs-on-premises-nodes-conundrum/
[18] Véase la sección "Sustainability" en https://ethereum.org/en/eth2/vision/

Cómo puede posicionarse el bitcoin frente al resto del ecosistema de activos digitales

Como hemos señalado anteriormente, la naturaleza de código abierto de Bitcoin crea la posibilidad de que los individuos copien, alteren y construyan fácilmente el código base original de Bitcoin para sus propios tokens y proyectos. Esto ha permitido la creación de una cantidad masiva (literalmente miles) de monedas alternativas (o "alt-coins"), lo que lleva a la confusión a los recién llegados a este espacio, y a veces hace que algunos afirmen erróneamente que el bitcoin no es escaso porque hay cientos de monedas.

Sin embargo, de nuestra discusión hasta ahora hemos propuesto:

- La red Bitcoin no es compatible con otras redes blockchain y los tokens bitcoin no son fungibles con otros tokens. Por lo tanto, los tokens de bitcoin son escasos, mientras que los tokens digitales, en general, no lo son.
- El principal motor de valor de los tokens de bitcoin es la escasez y el límite de oferta creíble
- Bitcoin se entiende mejor como un bien monetario.
- Es probable que Bitcoin sea el principal bien monetario y no es probable que otro activo digital sustituya a bitcoin en este papel.

Además, hemos visto que Bitcoin es actualmente la red más segura y descentralizada, pero en la base o capa de red nativa, no es la más escalable. La red de Bitcoin tampoco permite funcionalidades adicionales o programabilidad como hemos visto en nuestra comparación con Ethereum.

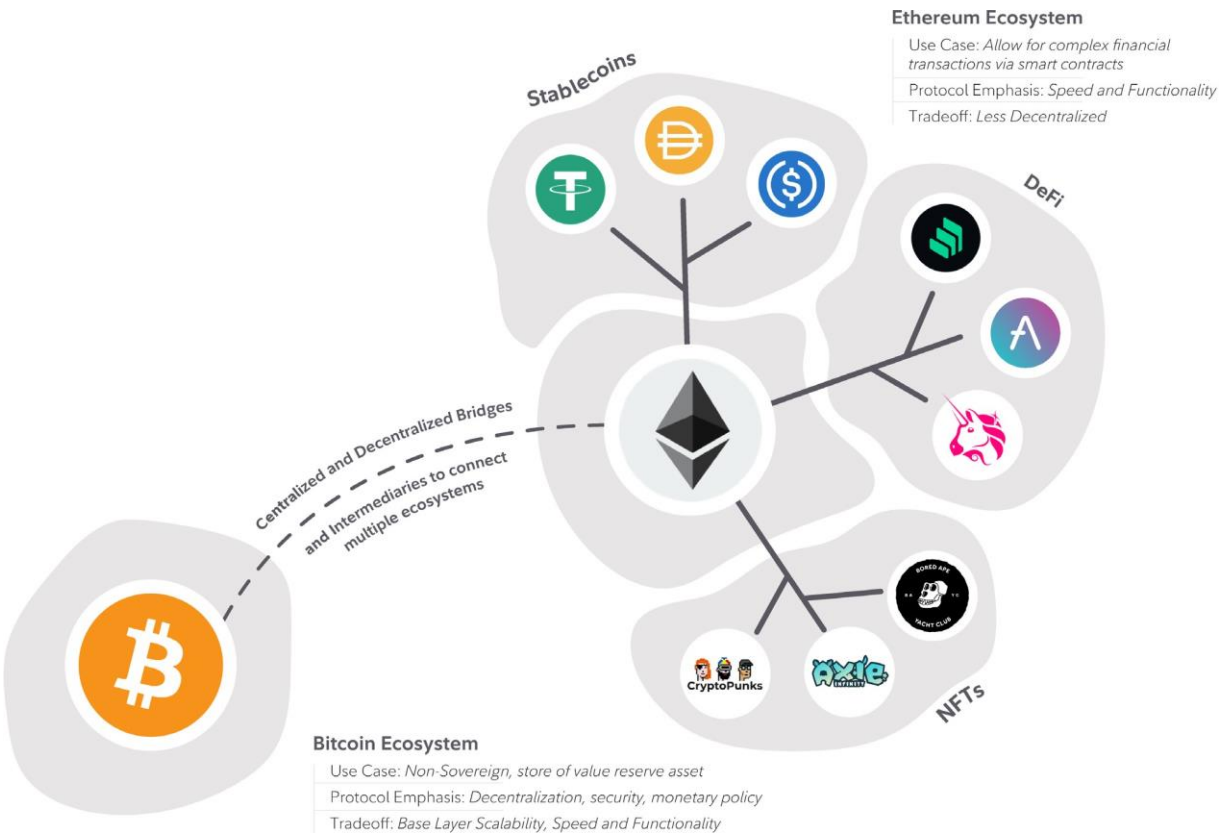
Debido a estas compensaciones inherentes, hemos asistido a un auge del ecosistema de activos digitales con cientos, si no miles, de proyectos diferentes que buscan alcanzar algún nivel diferente de usabilidad para satisfacer una necesidad del mercado.

Por supuesto, los inversores se preguntan cuál será el estado final de esta innovación. Aunque nadie sabe exactamente en qué puede convertirse, creemos que es instructivo examinar dos narrativas dominantes que se han hecho populares para imaginar el futuro ecosistema de activos digitales. En particular, nos interesa saber cómo puede imponerse Bitcoin en cada uno de estos escenarios.

1. Un mundo multicadena

La construcción actual de varios tokens ha dado lugar a un universo de activos digitales relativamente aislado en el que los desarrolladores optan por trabajar dentro de un ecosistema concreto. Por ejemplo, la construcción de Bitcoin es fundamentalmente diferente a la de Ethereum. El resultado es que Ethereum y todo su ecosistema de tokens y NFTs son incompatibles con el Bitcoin nativo, e incapaces de interactuar de manera fácil y sin confianza. Hasta la fecha, los terceros de confianza han sido un requisito fundamental para intercambiar activos que viven en diferentes silos.

Se están construyendo puentes para conectar varios ecosistemas de blockchain entre sí, un tema importante que hemos observado y esperamos que continúe en los próximos meses y años. La interoperabilidad será un desarrollo clave para el éxito del ecosistema de activos digitales si queremos asumir que varias cadenas ganarán debido a las diversas compensaciones de la capa base, los casos de uso y las propuestas de valor.



En un mundo de múltiples cadenas ganadoras, sigue pareciendo que Bitcoin es probablemente el mejor equipado para cumplir el papel de bien monetario no soberano del ecosistema con relativamente menos competencia que otros activos digitales que intentan cumplir con casos de uso alternativos. El énfasis explícito en la seguridad y la máxima descentralización refuerza su conjunto de reglas y hace valer los derechos de todos los usuarios por igual. Además, como resultado de su escasez y del límite de suministro impuesto, Bitcoin es lo más cercano que un protocolo digital podría estar de aplicar la escasez absoluta. En otras palabras, cualquier proyecto u otra red de blockchain que requiera que sus usuarios crean que están realizando transacciones con un token que tiene un valor monetario real, probablemente necesita estar directa o indirectamente conectado a bitcoin como el bien monetario por excelencia. Por ejemplo, la gente utiliza tokens en una sala de juegos por su facilidad de uso y utilidad y les atribuye valor porque sabe que representan una determinada cantidad de dólares o que pueden ser intercambiados por otros bienes y premios. Sin embargo, fuera del entorno nativo de las máquinas recreativas, las fichas tienen poco o ningún valor.

Este mundo deja a los tokens que no son de Bitcoin luchando por demostrar otros casos de uso viables para su tecnología. Tratan de encontrar la compensación adecuada para un nivel concreto de escalado de la capa base y se encountering con una gran competencia para el desarrollo y la mejora de la funcionalidad. Esto no es una acusación a quienes construyen o invierten en cadenas que no son de Bitcoin, sino simplemente una observación de que la clara ventaja de bitcoin como activo de almacenamiento de valor reduce su riesgo incluso en un mundo que contiene un ecosistema de muchos activos digitales vibrantes.
Asumiendo este resultado, el bitcoin sigue siendo un claro beneficiario de los flujos hacia el espacio de activos digitales en general, dado que se considera el activo digital monetario por excelencia, lo que lo convierte en la inversión más ajustada al riesgo y más fácil de entender y asignar en todo el panorama de activos digitales.

2. Un mundo en el que el ganador se lo lleva todo o la mayoría

Las cadenas de bloques son, sin duda, una importante creación tecnológica. La capacidad de tomar una base de datos de información que de otro modo estaría centralizada y eliminar a un tercero de confianza fue una innovación radical, no incremental. Sin embargo, una cadena de bloques centralizada es relativamente indistinguible de una base de datos y reduce las importantes cualidades que ofrece una cadena de bloques descentralizada, como la inmutabilidad, la resistencia

al embargo, la resistencia a la censura y el diseño sin confianza.

Por lo tanto, podemos prever un espectro de descentralización que ha tenido lugar con los tokens. Esto varía desde lo más descentralizado posible (Bitcoin) hasta tokens cuyos protocolos son descentralizados sólo de nombre y dan un poder exorbitante a los desarrolladores o a ciertos miembros de la comunidad. Por lo tanto, existe un posible escenario en el que los usuarios e inversores preferirán diferentes tokens en función de la compensación de menos descentralización por más características. Esto es similar al mundo multicadena descrito anteriormente.

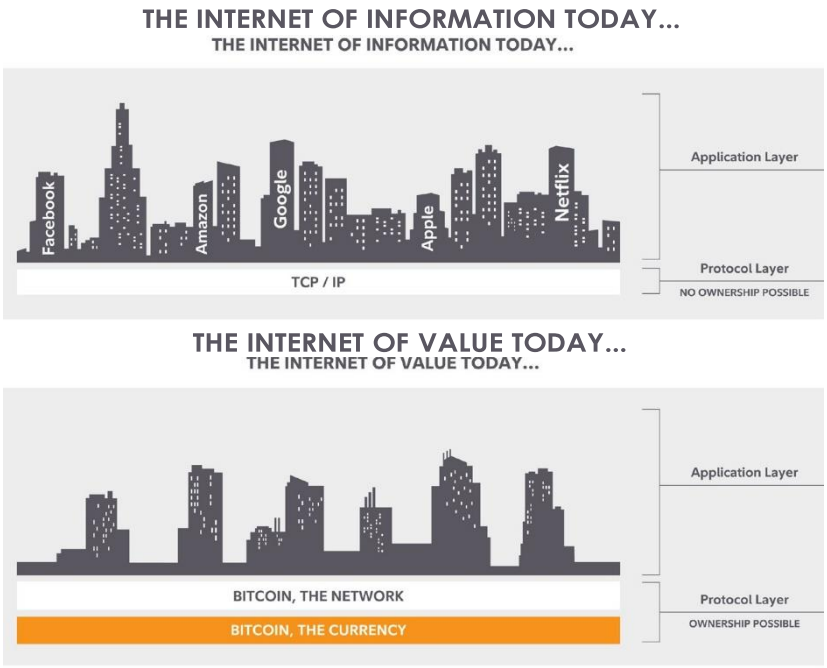
Sin embargo, hay otro escenario que podría surgir debido a la posibilidad de que las aplicaciones y las soluciones de escalado se construyan sobre la "capa base" o la "capa uno" de las cadenas de bloques. Si las aplicaciones pueden construirse sobre una red de blockchain existente en lugar de verse obligadas a iniciar una nueva red, los usuarios querrán construir sobre las redes más fuertes y seguras. Por lo tanto, podríamos ver un mundo en el que una o muy pocas de estas cadenas acumulen la mayor parte del valor en el ecosistema de activos digitales y sean elegidas como la principal red de blockchain. Dado que Bitcoin es posiblemente la cadena de bloques más descentralizada e inmutable que existe, parece ser la principal candidata a ser una de las ganadoras, o incluso la única, si se diera esta situación.

LA RED BITCOIN LIGHTNING

Una interesante aplicación de "capa dos" que ya estamos viendo cómo se construye sobre la red central de Bitcoin es la red lightning. Se trata de una red descentralizada que se construye utilizando la funcionalidad de los contratos inteligentes y que permite realizar transacciones fuera de la cadena entre personas, pero con la capacidad de realizar una transacción de liquidación final en la capa base de la red Bitcoin. Una analogía simple de esto sería que los participantes abrieran una cuenta privada entre ellos, realizando transacciones de ida y vuelta con mayor velocidad y con tarifas de transacción muy bajas. Esto aumenta la escalabilidad de Bitcoin, pero con la opción de liquidar en cualquier momento en la capa base sigue beneficiándose de la seguridad de Bitcoin.

Internet y su capa base, TCP/IP, son el ejemplo perfecto de ello. El conjunto de protocolos de Internet conocido como TCP/IP es una capa base de código abierto por la que fluye la comunicación y,

posteriormente, se construyen aplicaciones y contenidos sobre ella. El protocolo TCP/IP no es propiedad de nadie y, como es de código abierto, esta Internet de la información no permite la propiedad de la capa base. La propiedad sólo es posible para las aplicaciones y la tecnología construidas sobre ella. En cambio, la propiedad de la capa base es posible en el mundo de los activos digitales. Al igual que TCP/IP, las aplicaciones también pueden construirse utilizando la capa base y luego estas actualizaciones tecnológicas mejoran el valor capturado de la capa base. Las innovaciones de Amazon, Facebook, Google, Netflix y otros hicieron que la capa base de Internet fuera mucho más valiosa e importante. Del mismo modo, la innovación que tiene lugar en y alrededor de determinados protocolos de activos digitales hace que aumente la amplitud de la propiedad de su respectiva capa base y mejora sus casos de uso y utilidad.



Fuente: @Croesus_BTC en Twitter[19]

Lo interesante de esta arquitectura es que un inversor puede poseer parte de la capa base de esta nueva tecnología y puede ser relativamente agnóstico en cuanto a las aplicaciones específicas que se construyen sobre ella. Sería similar a ser capaz de poseer la capa base de Internet y estar expuesto a toda la innovación en la parte superior (por ejemplo, Google, Google, Amazon etc.) sin tener que tratar de elegir a los ganadores y perdedores específicos.

Bitcoin pretende satisfacer una clara necesidad del mercado

Por supuesto, no sabemos cómo será el nuevo sistema de activos digitales a medida que siga madurando, o si veremos un mundo multicadena de diferentes tokens con diferentes grados de centralización o si veremos un enfoque de "el ganador se lo lleva todo" en el que se construyen más aplicaciones en la cadena más segura y descentralizada. Sin embargo, parece que Bitcoin ha encontrado un papel en el ecosistema de los activos digitales como un activo escaso y de valor, como mínimo. En nuestra opinión, aún se está por ver la capacidad de los demás activos digitales para

cumplir con algún otro caso de uso necesario. No se puede decir lo mismo de Bitcoin. Esto crea perfiles de inversión de riesgo-rendimiento muy diferentes entre Bitcoin y todos los demás activos digitales y, en última instancia, debería influir en la forma en que los asignadores consideran la incorporación de cada uno de ellos en su cartera de inversiones.

El lugar de los activos digitales en una cartera

Es probable que los inversores que trabajen en su comprensión del ecosistema de activos digitales y creen un marco para considerar la inversión en el espacio se beneficien de la segmentación del bitcoin y de todas las demás inversiones en activos digitales como decisiones separadas. Esto simplifica el proceso de construcción de la cartera y permite que los asignadores tomen dos decisiones simultáneas pero separadas: la importancia de mantener la exposición al activo monetario más escaso de esta categoría de activos digitales emergentes (bitcoin), al tiempo que se considera el potencial de exposición a la innovación y la experimentación en curso dentro del ecosistema fuera de bitcoin.

Para entender el lugar adecuado de los tokens de bitcoin y no bitcoin en una cartera de inversión tradicional, los inversores deben derivar primero los factores clave de riesgo y rendimiento de sus respectivas tesis de inversión. Esto permite delimitar ambos y sacar una conclusión sobre el papel potencial que cada uno podría desempeñar dentro de una cartera tradicional.

Riesgos de Bitcoin, fuentes potenciales de rentabilidad y papel en un portfolio

La ventaja de ser el primero en llegar al mercado ha hecho que no haya una verdadera competencia en el uso principal del bitcoin como activo monetario y depósito de valor, y crea un perfil de rentabilidad drásticamente diferente para los inversores en bitcoin. Muchos de los riesgos que podrían haberse utilizado para justificar el fin del bitcoin han desaparecido y cada día la red se fortalece con más usuarios, mineros e infraestructura. Casi todos los riesgos que el bitcoin sigue teniendo hoy en día pueden verse también en cualquier otro activo digital, siendo los ataques de estados-nación y los fallos de protocolo dos de los riesgos más notables de la red.

[19] https://twitter.com/Croesus_BTC/status/1367165017280237569

Errores de protocolo: El potencial de una vulnerabilidad en cualquier código es siempre una amenaza presente. Este problema se puede mitigar si se mantiene la sencillez del software en cuestión y se lleva a cabo una revisión y un escrutinio exhaustivos del código. En el caso de Bitcoin, podría decirse que es el protocolo con menos probabilidades de encontrar un fallo importante en esta etapa de su vida, dado que ha existido durante más tiempo que cualquier otro proyecto, tiene un código intencionadamente simplista y tiene una recompensa de 1 billón de dólares para cualquiera que sea capaz de explotarlo.

Ataques de Estados-nación: Otro riesgo válido para la tesis del bitcoin es la posibilidad de que grandes países se opongan al crecimiento del ecosistema de activos digitales. El panorama geopolítico hasta la fecha ha hecho que una regulación adecuada parezca mucho más probable que la ilegalización de estos activos. En cualquier caso, Bitcoin está mejor posicionado para defenderse de ataques coordinados debido a su priorización de la descentralización.

Los riesgos a los que se enfrenta bitcoin hoy en día parecen menores en comparación con el resto de activos digitales, dada la falta de complejidad del código y el énfasis en la descentralización. La escasa o nula competencia en su caso de uso principal y los 13 años de funcionamiento como almacén de valor contribuyen a reforzar la idea del bitcoin como la base del ecosistema de activos digitales.
En otras palabras, no es que pensemos que una asignación a bitcoin no está exenta de riesgos, sino que creemos que algunos inversores están sobreestimando los riesgos a la baja de bitcoin en comparación con otros activos digitales.
También pensamos que algunos inversores pueden estar haciendo lo mismo con el lado de la rentabilidad de la ecuación, pero en la dirección opuesta, ya que pueden estar subestimando los rendimientos potenciales de bitcoin en comparación con otros activos digitales. Esta idea tiene cierto mérito, ya que el bitcoin, con una capitalización de mercado de alrededor de 1 billón de dólares, puede tener más dificultades para revalorizarse por un factor de 100 en comparación con su historia temprana, cuando sí se multiplicó por 100 (más de una vez), pero partiendo de una base de capitalización de mercado mucho menor. Sin embargo, estas recompensas iban acompañadas de mucho más riesgo en ese momento. Como se ha descrito anteriormente, el nivel de riesgo de bitcoin se ha reducido drásticamente desde sus primeros días. Además, creemos que el potencial de rentabilidad del bitcoin sigue siendo muy considerable.

El perfil de rentabilidad de Bitcoin está impulsado por dos fuertes vientos de cola: el crecimiento del

ecosistema de activos digitales y la potencial inestabilidad de las condiciones macroeconómicas tradicionales. Es probable que estos vientos de cola de rentabilidad se capten de forma más fácil y con menos riesgo que a través de la mayoría de los demás activos digitales.

Crecimiento del ecosistema de activos digitales: A medida que el dinero fluye por toda la clase de activos, el estándar de reserva de valor gana más legitimidad e importancia. Cada proyecto, token o pieza de infraestructura que se construye y financia está ampliando el caso de uso y el valor asociado a tener un activo digital de reserva neutral y escaso. Mientras que otros tokens se benefician del dinero que fluye indirectamente hacia el espacio, bitcoin es la forma más fácil de beneficiarse de este crecimiento. Como se ha comentado anteriormente, la falta de competencia de bitcoin para ser reconocido como el activo de reserva de valor preeminente significa que hay poca amenaza para su actual fortaleza de ser el "dinero" del ecosistema. Gran parte del crecimiento asociado al desarrollo de todos los activos digitales es bueno para el bitcoin.

Posible inestabilidad de las condiciones macroeconómicas tradicionales: El creciente uso de la política monetaria y fiscal como forma de proporcionar apoyo al crecimiento económico en curso puede dar lugar a preocupaciones sobre la estabilidad general del sistema financiero y la capacidad de la economía para mantenerse por sí misma. La acumulación de estas políticas ha llevado a niveles de deuda soberana mundial nunca vistos.20 El apalancamiento ha conducido históricamente a los sistemas financieros hacia la fragilidad. Uno de estos resultados potenciales como consecuencia de la La situación actual es una senda de represión financiera (tipos de interés reales negativos).21 Este tipo de entornos macroeconómicos han tendido históricamente a beneficiar a los activos escasos cuya oferta no puede alterarse. Por ejemplo, el rendimiento superior del oro en el episodio más reciente de alta inflación y, por tanto, de tipos de interés reales negativos, a finales de la década de 1970. En el mundo de los activos digitales, el conjunto de reglas de Bitcoin, los precedentes históricos y la descentralización han creado el mayor nivel de escasez de cualquier protocolo de activos digitales. Esto hace que sea un caso convincente como la mayor cobertura disponible para algunos de los posibles vientos en contra que enfrenta el sistema financiero heredado.

Dada la capacidad de cubrir los posibles resultados asociados a los activos tradicionales y de captar el crecimiento general del ecosistema, el bitcoin se convierte en una forma sencilla y eficiente de obtener exposición al ecosistema de activos digitales.

[20] https://blogs.imf.org/2021/12/15/global-debt-reaches-a-record-226-trillion

Riesgos y factores de rentabilidad no relacionados con el bitcoin

Muchos inversores suelen citar el potencial de rendimientos extremadamente ventajosos como razón para sobreponderar los activos digitales alternativos o no relacionados con el bitcoin y, en algunos casos, omitir el bitcoin por completo de su cartera. Aunque este perfil de rentabilidad potencial puede existir para determinados activos digitales, es importante tener en cuenta que estos proyectos también suelen conllevar mayores riesgos generales y una posibilidad significativa de que el token pierda su valor si no cumple las expectativas.

Los riesgos de los tokens que no son bitcoins varían ciertamente en función de cada caso y tienden a ser más extremos en los tokens más especulativos y de cola larga. Sin embargo, muchos de estos riesgos siguen siendo compartidos por la mayoría de estos proyectos. A continuación, se señalan algunos riesgos clave:

Mostrar una descentralización adecuada: El algoritmo de prueba de trabajo de Bitcoin, la estructura de gobierno y el lanzamiento justo crearon las bases para un proyecto descentralizado con una confianza lanzamientos de tokens alternativos, que suelen reducir su nivel de descentralización. Dado que es una de las propuestas de valor clave que prometen la mayoría de estos protocolos, los inversores deberían considerar el grado de descentralización de su proyecto en particular Una falta de descentralización adecuada hace que un protocolo concreto sea más susceptible de ser supervisado por las autoridades y perjudica los derechos de los usuarios.

La amenaza de la competencia: La diferenciación se hace difícil con el código abierto cuando una plataforma es capaz de copiar y aprovechar los defectos de otra. Históricamente, hemos sido testigos de muchos proyectos fallidos y la rotación entre las 10 o 20 monedas más valiosas ha sido extrema. Los protocolos deben construir un efecto de red lo suficientemente grande en torno a su caso de uso determinado con la esperanza de poder defenderse de los competidores, ya que casi todas las redes que no son de bitcoins intentan añadir algún nivel de escalabilidad o funcionalidad a su capa base para demostrar su valía.

[21] Véase por ejemplo "The Liquidation of Government Debt" por C. M. Reinhart y M. B. Sbrancia, IMF Working Paper (2015) https://www.imf.org/external/pubs/ft/wp/2015/wp1507.pdf

Los impulsores de la rentabilidad de todos los activos digitales que no son bitcoins también son muy diferentes, dado que los protocolos se ven obligados a hacer ciertas concesiones para mejorar la velocidad, la funcionalidad y otras características para justificar un caso de uso. Dentro de todos los activos digitales que no son bitcoins se encuentra el impulsor más importante de los rendimientos:

Atraer a los desarrolladores y crear efectos de red: Los proyectos que han demostrado su capacidad para tener éxito y crear algo prometedor lo han hecho atrayendo al talento adecuado y reteniendo a su base de usuarios. Ethereum y Solana proporcionan un gran ejemplo de lo que es posible para un protocolo que puede atraer a una gran cantidad de desarrolladores, construir una plataforma utilizable y ganar una red de usuarios leales. Si se hace bien, está claro que se puede crear mucho valor para los inversores.

10 PRINCIPALES ACTIVOS DIGITALES POR CAPITALIZACIÓN DE MERCADO

	2017	2022
1	*Bitcoin*	*Bitcoin*
2	*Ethereum*	*Ethereum*
3	*XRP*	Tether (Stablecoin)
4	Litecoin	BNB
5	Monero	Cardano
6	Ethereum Classic	USD Coin (Stablecoin)
7	Dash	Solana
8	Augur	*XRP*
9	MaidSafeCoin	Terra
10	Steem	Polkadot

Fuente: CoinMarketCap, Fecha: 1/18/2022

Dado el aumento de la competencia y las posibles vías de fracaso de muchos de estos proyectos, la asignación a los tokens que no son bitcoins se realiza a menudo con una mentalidad similar a la del capital riesgo. En lugar de elegir un proyecto concreto, los inversores suelen tomar pequeñas posiciones en muchos nombres individuales. Esto suele dar lugar a la búsqueda de una solución de gestión activa para hacer frente al aumento de la complejidad general. Una vez más, esto muestra un marcado contraste con un simple enfoque de bitcoin en este espacio de activos digitales.

CONCLUSIÓN

Los inversores tradicionales suelen aplicar un marco de inversión en tecnología al bitcoin, lo que lleva a la conclusión de que el bitcoin, como tecnología pionera, será fácilmente suplantado por otra superior o tendrá una rentabilidad menor.

Sin embargo, como hemos argumentado aquí, el primer avance tecnológico de bitcoin no fue como tecnología de pago superior, sino como forma de dinero superior. Como bien monetario, el bitcoin es único. Por lo tanto, no sólo creemos que los inversores deben considerar el bitcoin en primer lugar para entender los activos digitales, sino que el bitcoin debe ser considerado en primer lugar y por separado de todos los demás activos digitales que han venido después.

1012662.1.0