EL BITCOIN VERSUS LOS SISTEMAS DE PAGO TRADICIONALES: ¿ES UNO MÁS EFICIENTE QUE EL OTRO?

Florian Ginez, CFA, Senior Quantitative Associate
August 2019

Cuando Bitcoin se presentó por primera vez al mundo en un white paper publicado en 2008, bajo el seudónimo de Satoshi Nakamoto, contó con el apoyo de solamente un puñado de entusiastas. Sin embargo, en los últimos años, las cosas han cambiado drásticamente y la criptodivisa se ha convertido en uno de los desarrollos tecnológicos más seguidos del mundo.

Al presentar el concepto de "blockchain" para pagos, Bitcoin prometió brindar un mayor nivel de confianza y seguridad a las transacciones financieras. Y si bien se han lanzado otros sistemas de blockchain –cadena de pagos- desde la llegada del Bitcoin, muchos consideran que Bitcoin es el sistema más desarrollado y confiable; evidenciado en parte por el hecho de que la infraestructura construida a su entorno, todavía supera a la de sus alternativas.

Hoy en día, Bitcoin gestiona un gran número de transacciones, en las cuales muchas de ellas, son de gran valor. Esto ha llamado la atención del mundo sobre su potencial como sistema de pago. Sin embargo: ¿cómo se compara con los sistemas de pago tradicionales? ¿Es más efectivo?

En este informe, analizaremos las diferencias fundamentales entre Bitcoin y los sistemas de pago tradicionales y examinaremos las fortalezas y debilidades de cada uno.

¿Qué es el Bitcoin?

Diseñado como un sistema de pago, Bitcoin permite la transferencia de valor de la misma manera que lo hacen las transferencias bancarias o los pagos con tarjeta. Sin embargo a veces, el término "Bitcoin" puede ser confuso, ya que no siempre parece referirse a lo mismo. De hecho, el término se utiliza para referirse a una divisa, a un protocolo y a una red. A un nivel de detalle muy fino, por más de que estos subcomponentes son similares a los que comprenden los sistemas de pago electrónico tradicionales, existen diferencias clave en la forma en que operan ambos sistemas. Antes de comparar el sistema de Bitcoin con los sistemas de pago tradicionales, exploremos los subcomponentes de Bitcoin con más detalle.

UNA MONEDA

Una moneda es una forma de dinero generalmente aceptada que se utiliza como un medio de cambio, una reserva de valor o una unidad de cuenta. Las divisas tradicionales, como el dólar estadounidense, el euro o la libra esterlina, a menudo denominadas divisas de reserva, están respaldadas por sus respectivos gobiernos y obtienen su valor de este respaldo. Hoy en día, además, las divisas no están respaldadas directamente por el oro o cualquier otro producto o activo.

El Bitcoin es similar a sus contrapartes tradicionales, en el sentido de que se utiliza como medio de intercambio, depósito de valor y unidad de cuenta. Y al igual que las divisas de reserva, la criptodivisa no está respaldada por ningún otro producto u activo. Sin embargo, una diferencia clave entre el Bitcoin y las monedas de reserva tradicionales es que, si bien las divisas de reserva son de curso legal respaldadas por un gobierno y controladas por un banco central, el Bitcoin es una moneda global "distribuida" que no está controlada por ninguna entidad centralizada y su suministro aumenta automáticamente a una velocidad predeterminada.

Gráfico 1: la transacción de una divisa de reserva versus una transacción de Bitcoin

mBTC = millibitcoin.

UN PROTOCOLO

Un protocolo puede describirse como un conjunto de reglas que rigen la acción o la comunicación bajo ciertas condiciones.

El término Bitcoin también se refiere las transacciones subyacentes de protocolo o al conjunto de reglas y mecanismos que permiten que el sistema funcione de manera segura, distribuyéndose en lugar de centralizarse.

El protocolo Bitcoin utiliza la tecnología de libro de contabilidad distribuida (DLT, por sus siglas en inglés), una base de datos distribuida y consensuada, así como la criptografía (que protege la información) para la verificación y el registro de las transacciones. El DLT además resuelve el problema del "doble gasto", el cual es el riesgo de que el efectivo digital se copie y se gaste varias veces. El protocolo Bitcoin es el primer sistema que gestiona este problema sin la necesidad de una autoridad centralizada.

Gráfico 2: la transacción bancaria versus la transacción de Bitcoins

El sistema bancario tradicional también se basa en estándares de comunicación y varios conjuntos de reglas y mecanismos para autorizar, borrar y liquidar transferencias. La diferencia crítica, una vez más, es el hecho de que el sistema tradicional depende de contrapartes centralizadas, mientras que el protocolo Bitcoin, elimina la necesidad de estos intermediarios.

UNA RED

El sistema de pago tradicional, se basa en la red bancaria para procesar transacciones. Los bancos de todo el mundo están conectados directa o indirectamente entre sí y cuando se inicia un pago desde el banco de quien lo realiza, pasa secuencialmente a través de varios procesos de verificación a través de una red de intermediarios.

Por el contrario, la red Bitcoin es una red peer-to-peer o un ecosistema de computadoras interconectadas que verifican y aprueban transacciones mientras mantienen un registro de todas las transacciones pasadas (Blockchain). Este libro de contabilidad es público, y cualquiera puede instalar el software de Bitcoin y ver el historial completo de todas las transacciones de Bitcoin procesadas. Estas computadoras se llaman "nodos".

Gráfico 3: la red de un banco versus la transacción de Bitcoin

¿Cómo difiere el sistema de pago de Bitcoin de los sistemas de pagos internacionales?

En el núcleo de cada sistema de transacción, se encuentra un elemento esencial: la confianza. Cuando Ud. acepta vender un producto a cambio de dinero, debe saber que realmente recibirá el dinero. ¿El cliente tiene el dinero? ¿Puede él o ella detener el pago después de que se haya iniciado? Veamos cómo las transacciones en efectivo y con tarjeta, se comparan con las transacciones de Bitcoin.

LAS TRANSACCIONES EN EFECTIVO

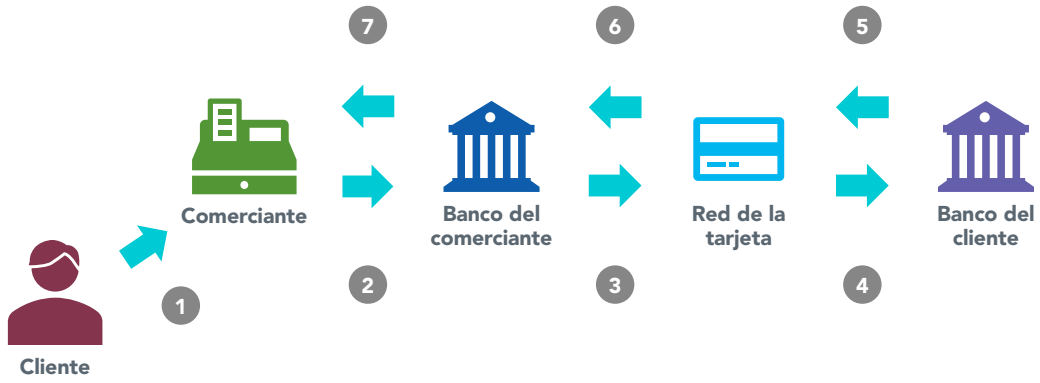
Una transacción en efectivo trata el problema de confianza de manera bastante efectiva. Si un cliente le da un billete, usted tiene el dinero de la venta. No hay intermediario. Sin embargo, todavía existen fallas. Por ejemplo, el cliente podría darle un billete falsificado.

Gráfico 4: una transacción en efectivo

TRANSACCIONES DE TARJETA

El pago con tarjeta, debe ser procesado por una red de tarjetas como VISA o Mastercard, así como por una red bancaria para su autorización, compensación y liquidación. La confianza se genera al depender de instituciones financieras bien establecidas, las cuales ejecutan una serie de controles mientras la transacción está en curso. En los gráficos 5 a 7 que se presentan a continuación, mostramos el flujo del proceso para los pagos con tarjeta.

Gráfico 5: el proceso de autorización de pagos con tarjeta

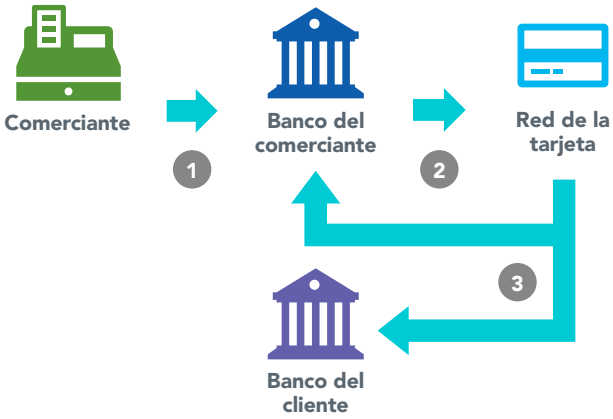


La fase de autorización tiene como objetivo verificar la identidad de un cliente como propietario de los fondos que está tratando de utilizar, así como la disponibilidad de los fondos.

Cuando Ud. inserta su tarjeta en una terminal y escribe su código PIN (1) durante una transacción, los detalles del pago y la información de su tarjeta, se envían al banco del comerciante (2), para que después envíe esos detalles a la red de la tarjeta (3). A su vez, la red solicitará autorización a su banco (4) y si los detalles son correctos y Ud. tiene los fondos disponibles, su banco enviará una autorización al comerciante a través de los mismos intermediarios, uno tras otro (5, 6 7).

Por más de que este proceso ocurra en unos pocos segundos y Ud. pueda salir de la tienda con sus productos, el proceso continúa de fondo. Si bien se le ha otorgado la autorización, los fondos aún están en su cuenta.

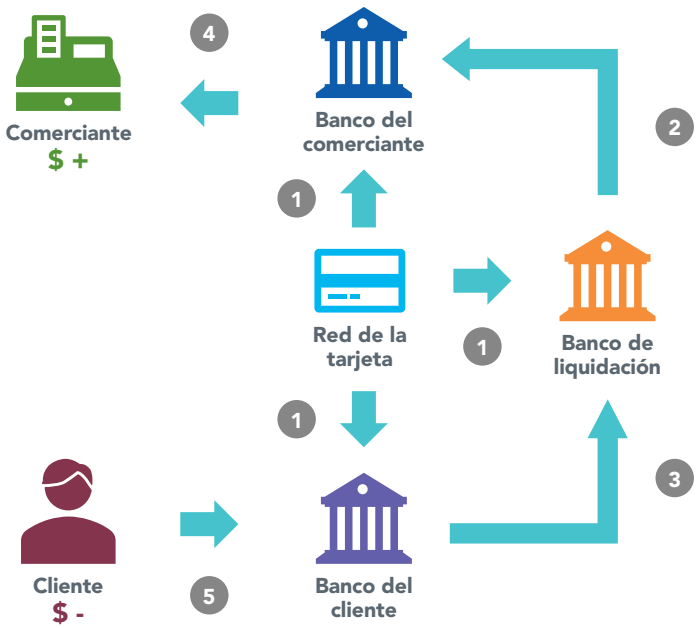
Gráfico 6: el proceso de compensación de las tarjetas



El proceso de compensación implica el intercambio de información relacionada a la transacción, utilizado para la verificación del dinero a debitarse del banco del cliente y a acreditarse en el banco del vendedor.

Al final de cada día, todas las transacciones aprobadas durante la jornada, se envían del comerciante al banco del comerciante (1), el cual a continuación transmite los detalles a la red de la tarjeta (2). La red de tarjetas valida la información, envía la información de compra a los bancos de los clientes y finalmente, envía la información de conciliación a los bancos de los comerciantes y de los clientes (3).

Gráfico 7: la estructura del proceso de los pagos por tarjeta



Finalmente, el pago puede someterse a una liquidación, como se muestra en el gráfico 7. La liquidación ocurre diariamente en una base agregada neta e implica la transferencia real de los fondos. La red de tarjetas calcula la posición de liquidación neta que el banco del cliente debe pagar al banco del comerciante y envía esa información a ambos bancos, más un nuevo actor: el banco de liquidación (1). El banco de liquidación paga al banco del comerciante (2) y el banco del cliente paga al banco de liquidación (3). Finalmente, al comerciante se le acredita el monto (4) y al cliente se lo debita (5).

Todo este proceso (autorización de liquidación) generalmente demora entre 24 y 48 horas. Como se muestra en los diagramas precedentes, es un proceso bastante pesado e informativo e involucra a varias contrapartes que necesitan crear y transmitir información secuencialmente.

Sin embargo, este sistema está bien establecido y es lo suficientemente fiable como para generar un alto nivel de confianza entre los usuarios. De hecho, se ha vuelto tan ampliamente aceptado, que países como Suecia apuntan a convertirse en sociedades sin efectivo.

En este modelo, la red de tarjetas juega un papel esencial. Como hay muchos actores involucrados, todos con sus propios sistemas de información, puede ser bastante difícil comunicarse entre sí. La red "es responsable de recopilar todas las transacciones y proporcionar una puerta de enlace. Intercambia información entre el banco de los clientes y el banco de los comerciantes, establece reglas y procesos para la participación en la red, crea estándares de formato para la información que atraviesa la red y facilita la liquidación monetaria entre los bancos de los clientes" .

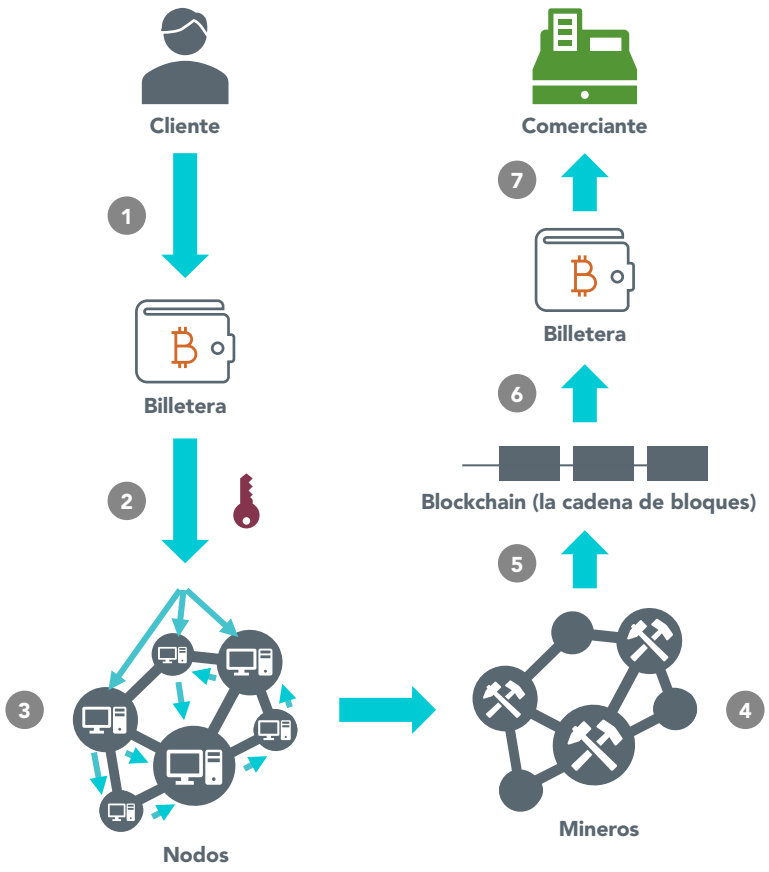
En otras palabras, proporciona los estándares y la infraestructura para el intercambio de información entre las partes involucradas.

[1] Herbst-Murphy, Susan (2013). "Clearing and Settlement of Interbank Card Transactions: A MasterCard Tutorial for Federal Reserve Payments Analysts".

LAS TRANSACCIONES POR VÍA BITCOIN

Cuando se realiza el envío de bitcoins a través de la red Bitcoin, el proceso sigue un camino muy diferente.

Gráfico 8: el proceso de transacción de bitcoins



Primero, como remitente, Ud. ingresa la dirección de Bitcoin del destinatario (esto es similar a un número de cuenta bancaria en una transferencia bancaria) y la cantidad de bitcoins para enviar, usando su interfaz de billetera digital (1). Ud. puede considerar este paso como equivalente a la terminal de pago del comerciante que prepara la información de pago en una transacción con tarjeta. Para los pagos en la tienda con bitcoins, los comerciantes a menudo escanean sus artículos y posteriormente crean un código QR que puede escanearse con su billetera digital en su teléfono, completando automáticamente el monto a pagar y la dirección del comerciante.

A continuación, la billetera envía esta información a la red, utilizando su "clave privada" para firmar digitalmente la transacción (2). La firma digital es de alguna manera similar a que un cliente ingrese su código PIN o firme el recibo en una transacción con tarjeta; su propósito es probar la propiedad del remitente de los fondos.

Algunos nodos recibirán la transacción, antes de transferir los detalles a otros nodos y posteriormente en unos segundos, su transacción queda propagada en toda la red (3). Todos los nodos pueden verificar de forma independiente la transacción y verificar que realmente tenga los bitcoins que Ud. busca enviar verdaderamente y que no los haya enviado previamente. Los pasos 1, 2 y 3 son similares al paso de autorización en pagos con tarjeta.

Los "mineros" reunirán a las transacciones en un lote y comenzarán a tratar de resolver un problema computacionalmente intensivo. El primero en resolver el problema, notifica a la red que se ha completado (4). Todos los demás nodos pueden verificar fácilmente si este minero está diciendo la verdad, en cuyo caso este nuevo lote -un bloque-, se agrega a la cadena de bloques –Blockchain- (5). El paso 5 es similar a la fase de liquidación en el ejemplo de transacción de la tarjeta, ya que es donde el dinero realmente cambia de propietario.

El propósito del paso 4 es garantizar que la cadena de bloques no se pueda modificar. La modificación de la cadena requeriría una gran cantidad de potencia de cálculo y por lo tanto, operativamente es muy difícil hacerlo. A medida que se agregan más bloques después del bloque que contiene su transacción, se vuelve exponencialmente más difícil modificar ese bloque.

Una vez que el bloque que contiene la transacción, se agrega a la cadena de bloques y se registra en el libro de contabilidad distribuida. La billetera del comerciante verá el pago confirmado (6) y el comerciante será el nuevo propietario de esos bitcoins (7).

El tiempo para todo este proceso puede variar dependiendo de una serie de factores. No obstante, el tiempo medio para extraer un bloque, es de 10 minutos. Por lo tanto, incluso si desea esperar cinco bloques más (seis confirmaciones, el nivel estándar de la comunidad) para realmente considerar la transacción efectiva, Ud. puede esperar razonablemente que ocurra en aproximadamente una hora.

¿Cuáles son las ventajas del Bitcoin sobre los sistemas de pagos tradicionales?

Si bien algunas ventajas potenciales del sistema Bitcoin, como su anonimato, la transparencia y la independencia de los gobiernos y de los bancos centrales, parecen ser una cuestión de ideología, Bitcoin ciertamente ofrece beneficios cuando se trata de eficiencia operativa y confianza.

MENOS INTERMEDIARIOS

Al enviar bitcoins a otra parte, básicamente sólo se necesitan dos intermediarios necesarios para que las monedas se transfieran de manera efectiva: su billetera y la red Bitcoin. Los nodos y los mineros son solo partes secundarias de la red y el agregar o eliminar algunos de ellos, no afecta a su funcionamiento. Por el contrario, el sistema de pago con tarjeta requiere un mínimo de cuatro intermediarios y a menudo, más en realidad.

EFICIENCIA MEJORADA

Como un sistema distribuido, el protocolo Bitcoin permite que todos los componentes del sistema accedan y verifiquen todas las transacciones pendientes y transacciones pasadas, todo el tiempo y simultáneamente, lo que crea eficiencia en el tiempo. Y los errores no pueden ocurrir en el camino; siempre que ingrese la dirección correcta al iniciar la transacción, los fondos llegarán a su destino previsto.

El sistema de pago tradicional no sólo tiene más intermediarios, sino que también multiplica los intercambios de comunicación de un lado a otro, lo que debe suceder secuencialmente. Esto lleva tiempo y pueden ocurrir errores en el camino.

LA CONFIANZA DISTRIBUIDA Y LOS PUNTOS ÚNICOS DE FALLA

Sin embargo, la ventaja clave de Bitcoin realmente reside en la forma en que gestiona la confianza en las transacciones y elimina los puntos únicos de falla.

Con el sistema tradicional, Ud. debe confiar en que las reglas y los mecanismos, no conducirán a errores y que cada **contraparte** involucrada opere correctamente. Si una contraparte a lo largo de la cadena se ve comprometida de algún modo, entonces toda la cadena se verá comprometida.

Con Bitcoin, el conjunto de reglas y mecanismos que sustentan el sistema, hace imposible el fraude, la manipulación y los errores. Dado que el software de Bitcoin es de código abierto, cualquier persona en el mundo puede acceder a él y revisarlo. En el historial de 10 años de Bitcoin, nunca se ha descubierto ninguna falla de seguridad. Nadie ha encontrado una manera de cambiar una transacción firmada o modificar la cadena de bloques.

Además, la belleza de un sistema distribuido, es que no necesita confiar en ninguno de sus componentes, ya que no existe un único punto de falla. El comprometer a uno o algunos nodos, no comprometería la red. Para modificar de manera fraudulenta las transacciones pendientes o la cadena de bloques de transacciones pasadas, sería necesario tomar el control de la mayoría de la potencia de cálculo de la red.

En última instancia, el riesgo radica en su billetera digital, ya que almacena sus claves privadas. Cualquiera que acceda a sus claves privadas puede gastar los fondos de la billetera. Esta es la razón por la cual las billeteras sin conexión, denominadas "almacenamiento en frío", se usan con frecuencia para evitar piratería. Pero desde el momento en que se firma su transacción, es segura. No hay puntos únicos de falla, y no necesita depositar su confianza en ninguna de las partes.

¿Existe un mejor sistema de confianza que uno en el que Ud. no necesite confiar en nadie?

INFORMACIÓN IMPORTANTE

Comunicaciones emitidas en el Espacio Económico Europeo («EEE»): Este documento ha sido emitido y aprobado por WisdomTree Ireland Limited, sociedad autorizada y regulada por el Banco Central de Irlanda.

Comunicaciones emitidas en jurisdicciones fuera del EEE: Este documento ha sido emitido y aprobado por WisdomTree UK Limited, sociedad autorizada y regulada por la Autoridad de Conducta Financiera del Reino Unido.

WisdomTree Ireland Limited y WisdomTree UK Limited se denominan cada una de ellas «WisdomTree» (según corresponda). Nuestra Política e Inventario de conflictos de interés están disponibles previa solicitud.

Exclusivamente para clientes profesionales. La información contenida en este documento se ofrece únicamente para su información general y no constituye una oferta de venta ni una solicitud de oferta de compra de valores o acciones. No se deberá utilizar este documento como base a la hora de adoptar una decisión de inversión. El valor de su inversión puede tanto disminuir como aumentar y es posible pueda perder una parte o la totalidad del importe invertido. Las rentabilidades pasadas no son indicativas de los resultados futuros. Cualquier decisión de inversión debe basarse en la información contenida en el folleto correspondiente, tras haber solicitado asesoramiento independiente en materia de inversión, fiscal y jurídico.

El presente documento no constituye, y bajo ninguna circunstancia debe interpretarse como una oferta o cualquier otra acción destinada a fomentar una oferta pública de acciones o valores en Estados Unidos o en cualquier provincia o territorio de dicho país. Ni este documento ni ninguna copia del mismo deberá ser aceptado, enviado o distribuido (directa o indirectamente) en Estados Unidos.

Este documento puede incluir comentarios de mercado independientes elaborados por WisdomTree sobre la base de información disponible al público. Aunque WisdomTree se esfuerza por verificar la exactitud del contenido del presente documento, no ofrece garantía alguna sobre su exactitud o integridad. Ningún tercer proveedor de datos externo a quien se haya recurrido para obtener la información contenida en este documento ofrece ninguna garantía ni realiza manifestación alguna en relación con dichos datos. Las opiniones expresadas por WisdomTree en relación con el producto o la actividad del mercado, pueden variar. Ni WisdomTree, ni ninguna filial, ni ninguno de sus respectivos directivos, consejeros, socios o empleados aceptan responsabilidad alguna por cualquier pérdida directa o indirecta que se derive del uso de este documento o de su contenido.

El presente documento podrá incluir declaraciones a futuro, incluyendo aseveraciones basadas en nuestras opiniones, expectativas y previsiones actuales con respecto al rendimiento de ciertas clases de activos y/o sectores. Las declaraciones a futuro están sujetas a determinados riesgos, incertidumbres e hipótesis. No es posible garantizar que dichas declaraciones sean exactas y los resultados reales podrían diferir sustancialmente de los anticipados en dichas declaraciones. WisdomTree le recomienda encarecidamente que no confíe excesivamente en estas declaraciones a futuro.

Cualquier rentabilidad pasada incluida en este documento se puede basar en pruebas retrospectivas. Las pruebas retrospectivas consisten en el proceso de evaluar una estrategia de inversión aplicándola a los datos históricos para simular la posible rentabilidad de dicha estrategia. Sin embargo, la rentabilidad basada en estas pruebas es puramente hipotética y se proporciona en este documento únicamente con fines informativos. Los datos derivados de pruebas retrospectivas no representan la rentabilidad real y no deben interpretarse como una indicación de la rentabilidad real o futura.