

## Información sobre el riesgo de operaciones con criptomonedas

Existen riesgos muy específicos asociados al comercio de criptomonedas, que Trade Republic señala en primer lugar.

### ¿Qué son las criptomonedas y cómo funcionan?

"**Criptomonedas**" es un término colectivo para una serie de monedas digitales virtuales. En la actualidad se pueden negociar como activos especulativos en los mercados financieros globales. Algunos ejemplos de criptomonedas más importantes son Bitcoin, Ether y Litecoin. En la Ley Bancaria Alemana los denomina "criptoactivos" o "unidades de cuenta" y los clasifica como instrumentos financieros.

Una diferencia significativa entre las criptomonedas y el dinero tradicional, como el euro o el dólar, es que las criptomonedas funcionan independientemente de los bancos centrales o de los Estados. Esto es así porque no es una (o unas pocas partes) la que decide sobre el suministro de dinero y la aplicación de los derechos de propiedad, sino que suele ser una red descentralizada de muchos participantes la que coordina la organización de la criptomoneda. En este sentido, las criptomonedas no tienen ningún valor "propio", que, por ejemplo, en el caso de las monedas de oro, puede tener un valor material.

Mientras que con las monedas tradicionales suelen ser los bancos centrales los que deciden la creación de nuevo dinero y lo generan, la creación de nuevas "**monedas**" (unidades de valor de la criptomoneda) tiene lugar directamente en la base de datos encriptada y normalmente descentralizada de la criptomoneda. En esta base de datos, todas las transacciones y eventos se documentan y almacenan (sellados en bloques individuales) uno por uno. Dado que estos bloques suelen estar unidos en forma de cadena para garantizar que los bloques individuales no puedan modificarse posteriormente, la base de datos suele denominarse "**blockchain**" (cadena de bloques). Una moneda es nada más y nada menos que un registro de datos en este blockchain y, por tanto, una parte del código del programa del blockchain. Por tanto, se trata nada más y nada menos que de líneas de programación a las que el mercado otorga un determinado valor.

Blockchain, por tanto, puede considerarse como el diario de la criptomoneda, en el que se almacenan, públicamente visibles para todos, datos seudónimos sobre quién poseía cuántas monedas de criptomoneda, en qué momento y a dónde fueron transferidas.

"**Distributed Ledger Technology**" ("**DLT**") o simplemente "**Distributed Ledger**" es otro término usado para describir la tecnología ya mencionada. Hemos decidido usar el término "blockchain", ya que es más común. Sin embargo, se trata de un sinónimo y se refiere a los mismos procesos tecnológicos, que conllevan los mismos riesgos.

En la cadena de bloques, también se verifica la legitimidad de los eventos individuales antes de que en ella se almacenen irreversiblemente como nuevos eventos. Esta verificación se lleva a

cabo en el caso de las criptomonedas mediante diversos mecanismos de verificación. El más extendido es el llamado procedimiento de "**prueba de trabajo**", que se utiliza actualmente para Bitcoin, Bitcoin Cash, Litecoin y Ethereum, entre otros. En este procedimiento matemático, al final del cual la cadena de bloques se amplía con otro bloque, todos los participantes (los llamados "**mineros**") trabajan juntos para verificar y documentar la información que se va a almacenar resolviendo un rompecabezas criptográfico. Esto requiere una potencia informática importante por parte de los mineros. Los participantes que resuelvan el rompecabezas primero podrán añadir el nuevo bloque correspondiente a la cadena de bloques y serán recompensados por ello con nuevas unidades de la criptomoneda ("**recompensas de bloque**"). En el caso de la criptomoneda Bitcoin, la cantidad total de posibles Bitcoins existentes está limitada (aunque aún no se ha alcanzado), mientras que otras criptomonedas no tienen ese límite (al menos no todavía) como, por ejemplo, Ether. Los protocolos de consenso o mecanismos de verificación alternativos, por ejemplo, "**Proof of Stake**" o "**Delegated Proof of Stake**", requieren una potencia informática significativamente menor por parte de los participantes, ya que llegan a un consenso sobre qué participante puede añadir el siguiente bloque mediante una selección aleatoria ponderada, en la que la duración de la participación y la cuota de monedas poseídas, y no la potencia informática (como en el caso de Proof of Work), es decisiva.

El registro de las transacciones en las redes basadas en tecnologías de blockchain funciona a través de protocolos de consenso que pueden ser susceptibles a ataques que intenten modificar dicho registro y, en caso de tener éxito estos ataques, no existiría un registro alternativo que respalde dichas transacciones ni por tanto a los saldos correspondientes a las claves públicas, pudiéndose perder la totalidad de los criptoactivos.

Ya que la cadena de bloques no sólo es ampliada por todos los participantes/mineros, sino que también es almacenada de forma descentralizada por todos los participantes de la red, es particularmente difícil manipular el sistema, ya que una vez verificada la información puede ser confirmada por todos los participantes y la nueva información puede ser verificada por todos. Sólo cuando la mayoría de los participantes han verificado una transacción, ésta se documenta de forma irreversible en el siguiente bloque de la cadena. Este principio descentralizado de verificación de las transacciones, que se basa en la eliminación de las partes centralizadas (como los bancos o las autoridades), también se denomina principio "**peer-to-peer**".

Entre otras cosas, la cadena de bloques también almacena de forma anónima (o seudónima) qué usuario posee cuántas y también qué criptomonedas. Para ello, cada usuario dispone de una especie de dirección en la que se "almacenan" sus monedas y a la que otros participantes pueden enviar más monedas. Esta dirección es pública y también se llama "**clave pública**". Puedes comparar la clave pública con una especie de número de cuenta. Sin embargo, qué participante tiene qué clave pública -para iniciar transacciones, por ejemplo- debe intercambiarse fuera de la cadena de bloques. Además de la clave pública, cada participante dispone de la llamada "**clave privada**". Puedes pensar en esto como una contraseña: debe mantenerse en secreto por el usuario y permite a su propietario autorizar las transacciones en la cadena de bloques. Juntas,

estas dos claves forman el llamado "**wallet**", que es comparable a una cartera digital. Sin embargo, este monedero no almacena las criptomonedas, sino sólo las claves necesarias para acceder a ellas. El monedero, o sobre todo la clave privada, debe guardarse con extremo cuidado, ya que una pérdida es irreversible y no hay posibilidad de recuperación o restablecimiento (como ocurre con el olvido del PIN bancario, por ejemplo). Al comerciar con criptomonedas a través de Trade Republic, el cliente no gestiona su propio monedero: un criptocustodio garantiza la protección y la custodia de las claves.

Las criptomonedas no son un sustituto del dinero que pueda utilizarse de forma fungible en el mercado. La aceptación de criptoactivos como método de pago todavía es muy limitada y no existe obligación legal de aceptarlos. Además, las criptomonedas obtenidas a través de Trade Republic no pueden ser entregadas o puestas a disposición como medio de pago. Se trata, por tanto, de una especulación sobre la evolución del precio de las criptomonedas.

A diferencia de las monedas conocidas, que suelen estar respaldadas por el poder económico de un Estado, y a diferencia de las acciones, que están respaldadas por el poder económico de una empresa, éste no es el caso de las criptomonedas. No hay factores subyacentes que creen valor, un valor material o un valor establecido a través de décadas de aceptación en el mercado. El valor del precio viene determinado únicamente por la oferta y la demanda, la disponibilidad limitada y las expectativas de los inversores sobre la evolución futura de los precios. De este modo, pueden producirse ganancias o pérdidas considerables en los precios sin que se pueda reconocer por qué ocurre esto en un momento dado.

Las criptomonedas, por tanto, son instrumentos financieros altamente especulativos y cada cliente debe ser consciente de que asume un riesgo importante, hasta el riesgo de pérdida total. El valor de las inversiones y el rendimiento obtenido de las mismas puede experimentar significativas variaciones al alza y a la baja, pudiendo perderse la totalidad del importe invertido. Además de los riesgos habituales de las inversiones financieras, como el riesgo de precio, también existen riesgos específicos. Especialmente las inversiones en proyectos en etapas tempranas suponen un alto nivel de riesgo, por lo que resulta necesario entender adecuadamente su modelo de negocio.

Las tecnologías de registros distribuidos se encuentran todavía en un estadio temprano de maduración, habiendo sido muchas de estas redes creadas recientemente, por lo que pueden no estar suficientemente probadas y existir fallos significativos en su funcionamiento y seguridad.

## **Volatilidad y negociación 24 horas**

Como no siempre existe un vínculo comprensible entre los datos económicos y el valor del precio, y que el principal motor de la evolución del precio en el mercado es la oferta y la demanda, las criptomonedas suelen ser muy volátiles. En este contexto, cabe señalar que los precios de las criptomonedas se constituyen en ausencia de mecanismos que aseguren su correcta formación, como los presentes en los mercados regulados de valores. La aceptación de los participantes en el mercado con respecto a la respectiva criptomoneda también es decisiva para el desarrollo del precio. Esto significa que puede haber considerables oscilaciones de precios en un día de negociación e incluso en una sola hora de negociación, que pueden llegar a ser de dos dígitos. Por lo tanto, un cliente puede sufrir fácilmente una pérdida o un beneficio elevado en un solo día de negociación.

Además, incluso pequeñas cantidades de la criptomoneda pueden ser suficientes para desencadenar importantes movimientos de precios, ya que las criptomonedas no siempre son líquidas. Por lo tanto, no es imposible que los ataques a las criptomonedas sean llevados a cabo por terceros que actúen solos o en conjunto.

Las órdenes límite no son posibles.

Al especular, el cliente debe tener en cuenta que siempre pueden producirse ganancias y pérdidas considerables, **también por la noche o en domingos y días festivos**. Las criptomonedas suelen negociarse las 24 horas del día y sin interrupción. Esto puede llevar a que una criptomoneda experimente un cambio de valor significativo de la noche a la mañana mientras el cliente sigue durmiendo.

## **Liquidez**

Un instrumento financiero es líquido si su negociación es tan rápida que siempre se puede encontrar un comprador o un vendedor y, por lo tanto, se puede volver a desprender fácilmente de un instrumento financiero vendiéndolo. La liquidez de Bitcoin es actualmente alta, pero esto no se aplica a todas las criptomonedas. Muchas criptomonedas pueden verse carentes de la liquidez necesaria para poder deshacer una inversión sin sufrir pérdidas significativas, dado que su circulación entre inversores, tanto minoristas como profesionales, puede ser muy limitada. Por lo tanto, pueden surgir situaciones en las que no sea posible vender criptomonedas a tiempo o en las que haya que aceptar reducciones significativas del precio.

## **Clasificación legal**

La clasificación legal de las criptomonedas no está aclarada de momento. No está claro si pueden establecerse derechos sobre las criptomonedas y cómo estos derechos vuelven a caducar, si estos derechos están protegidos en caso de insolvencia y cómo, etc. Las criptomonedas no tienen propiedad y tampoco posesión. Esto conlleva al riesgo para el cliente de que los acuerdos celebrados no se mantengan en caso de insolvencia de una de las partes implicadas o de que terceros puedan acceder a las criptomonedas sin poder hacer nada al respecto. Tampoco está claro a qué sistema legal están sujetas las criptomonedas. En caso de conflicto, la situación jurídica puede ser desfavorable para el cliente.

### **No transferibles**

Las criptomonedas negociadas a través de Trade Republic no pueden ser entregadas ni transferidas a otro monedero. Sólo es posible comprarlas y venderlas.

### **Riesgo del operador del sistema**

La existencia y el funcionamiento de las criptomonedas depende de que ciertas entidades / operadores del sistema (los llamados "**nodos completos**") mantengan el sistema actualizando la cadena de bloques. Esto ocurre sin ningún tipo de control u obligación central. No se puede descartar que un individuo o todos estos llamados nodos completos terminen su actividad para una criptomoneda en particular y, por lo tanto, si no se encuentra un reemplazo, la criptomoneda ya no es negociable. Estos nodos completos también podrían aumentar significativamente los costes de transacción de las criptomonedas y, por tanto, hacer que las transacciones sean antieconómicas. Trade Republic tendría entonces que decidir si traslada los costes y cómo lo hace.

También es posible que algunos de estos operadores del sistema puedan fusionarse y, por tanto, tener menos instancias de control para una criptomoneda, lo que a su vez la haría más vulnerable a los ataques desde el exterior.

### **Riesgo del socio comercial / Riesgo de malversación**

Trade Republic ha conectado a socios comerciales líquidos y conecta a otros socios comerciales. No obstante, nunca se puede descartar que el socio comercial conectado suspenda las operaciones en caso de que aumente la volatilidad del mercado. Esto puede llevar a que los clientes no puedan vender sus criptomonedas mientras la negociación está suspendida y, por tanto, sufran pérdidas.

Trade Republic opera actualmente a través de sus socios comerciales Bankhaus Scheich Wertpapierspezialist AG ("**Bankhaus Scheich**") y B2C2 Limited ("**B2C2**").

Bankhaus Scheich es una empresa alemana con sede en Fráncfort del Meno. Se ha acordado la legislación alemana para el acuerdo sobre el centro de negociación con Trade Republic. B2C2 es una empresa inglesa con domicilio social en el Reino Unido (Londres). Allí se aplica la legislación local, lo que también se acuerda en el contrato de establecimiento comercial. Trade Republic, como comisionista, sólo transmite a los clientes lo que Trade Republic recibe por la ejecución de la comisión. Por lo tanto, las reclamaciones contractuales del cliente también se ven afectadas por estos contratos de centros de negociación. Los centros de negociación no están sujetos a la supervisión que se conoce en las bolsas de valores. No hay instancias de control con respecto a la calidad de los precios.

Además, los contratos contienen normas especiales de negociación, a cuyo contenido puede acceder el cliente a través de la app (perfil/ajustes/documentos en vigor/información sobre los mercados de negociación).

Es difícil seguir la pista a las operaciones con criptomonedas. Debido a la elevada volatilidad y a la inexistencia de centros de negociación centralizados y regulados, puede resultar complicado determinar un precio de referencia.

**Mistrades Bankhaus Scheich:**

Los clientes deben tener en cuenta que aunque Trade Republic puede tener una reclamación por daños y perjuicios contra el socio comercial aplicando el artículo 122 del Código Civil alemán (BGB) mutatis mutandis, no hay más reclamaciones por daños y perjuicios. Esto significa que Trade Republic sólo puede hacer valer la indemnización por daños y perjuicios dirigida al interés negativo de los clientes contra el socio comercial en caso de cancelación posterior de una transacción o su anulación en condiciones restringidas. Si el cliente sufre los daños correspondientes como resultado de una operación errónea, éstos no pueden ser compensados. Si el cliente comercia con criptomonedas a través de Trade Republic, está de acuerdo y acepta que Trade Republic ha acordado con el socio comercial las correspondientes regulaciones de comercio indebido, que también se aplican a él.

**Mistrades B2C2:**

Los clientes deben tener en cuenta que no se puede reclamar una indemnización por daños y perjuicios al socio comercial en virtud de la aplicación correspondiente del artículo 122 del BGB. Esto no ha sido aceptado por el socio comercial. Esto significa que Trade Republic no puede hacer valer los daños y perjuicios de los clientes contra el socio comercial en caso de cancelación posterior de una transacción o su anulación. Si el cliente sufre los daños correspondientes como resultado de una operación errónea, éstos no pueden ser compensados. Si a pesar de ello el cliente comercia con criptomonedas a través de Trade Republic, está de acuerdo y acepta que Trade Republic ha acordado con el socio comercial las correspondientes regulaciones de comercio indebido, que también se aplican a él.

## **Riesgo de pérdida de clave / Sin protección del depósito / Riesgo de seguridad**

La asignación de criptomonedas depende de la posesión de las claves necesarias (clave pública y privada). Si estas claves se pierden o se borran, las criptomonedas también se pierden para el cliente respectivo y ya no se pueden recuperar. La custodia de los criptoactivos supone una responsabilidad muy relevante ya que pueden perderse en su totalidad en el caso de robo o pérdida de las claves privadas.

Las facilidades de anonimato que pueden aportar los criptoactivos los convierten en un objetivo para los ciberdelincuentes, ya que en el caso de robar credenciales o claves privadas pueden transferir los criptoactivos a direcciones que dificulten o impidan su recuperación.

Trade Republic no gestiona ni almacena ninguna criptomoneda para sus clientes. Esto lo hace un criptocustodio que celebra un contrato con el propio cliente. El propio criptocustodio aplica altos estándares para garantizar un almacenamiento seguro. Sin embargo, no se puede descartar que se produzcan ataques físicos o de otro tipo contra estas empresas y que repercutan en las participaciones de los clientes. Es posible que se produzcan ataques de piratas informáticos en particular, pero también delitos por parte de los empleados.

Las criptomonedas mencionadas en este documento no están cubiertas por mecanismos de protección al cliente como el Fondo de Garantía de Depósitos o el Fondo de Garantía de Inversores. Sin embargo, el custodio ha contratado un seguro para los riesgos correspondientes, según su propio anuncio. Trade Republic no puede evaluar si las participaciones de los clientes están cubiertas y en qué medida.

Tampoco es imposible que el criptocustodio tenga dificultades económicas o incluso la insolvencia. Todavía no se ha aclarado de forma concluyente en términos legales qué efectos tendrá esto sobre las criptomonedas mantenidas en una "cartera de cliente" con el criptocustodio. En la actualidad, suponemos que las participaciones de los clientes están protegidas incluso en caso de insolvencia del criptocustodio o de Trade Republic.

Actualmente, los clientes de Trade Republic tienen que acceder a una relación comercial con

BitGo Deutschland GmbH,  
Neue Rothofstraße 13-19,  
60313 Fráncfort del Meno,  
Alemania,

una sociedad alemana de responsabilidad limitada que actúa como el custodio de criptoactivos. Este acuerdo de custodia entre BitGo Deutschland GmbH y el cliente estará sujeto a la legislación española.

Puesto que el inversor no dispone de los criptoactivos, ya que los mismos se encuentran en monederos digitales (wallets) del custodio, y tampoco dispone de acceso a las claves privadas de los wallets, el acuerdo de custodia que el inversor, cliente de TRADE REPUBLIC Bank GmbH, firma con el custodio BitGo Deutschland GmbH establece una descripción detallada de los derechos que tiene el inversor sobre sus criptoactivos. Por lo tanto, el inversor puede consultar sus derechos en dicho acuerdo, que habrá leído antes de suscribirlo.

En el citado acuerdo de inversión se reconocen los siguientes derechos de los inversores sobre sus criptoactivos:

Los inversores tienen derecho a que el custodio, BitGo Deutschland GmbH, mantenga un registro de los criptoactivos custodiados en el Wallet pertenecientes a cada inversor, y a acceder a la información de los criptoactivos que poseen a través de la plataforma de TRADE REPUBLIC.

El inversor tiene derecho a ser informado de las posibles restricciones o suspensiones temporales del servicio ofrecido por el custodio.

En el supuesto de que la plataforma de TRADE REPUBLIC dejara de estar disponible de forma permanente para la venta de criptoactivos el inversor tendrá derecho a solicitar la entrega de sus criptoactivos custodiados o la remisión de los mismos a otro wallet.

El inversor tiene derecho a que el custodio de los criptoactivos responda de los daños y perjuicios que se pudieran derivar para el inversor de conformidad con las disposiciones legales aplicables.

Además, el inversor dispone del derecho a desistir del contrato de custodia con el custodio de los criptoactivos sin indicación de los motivos y sin penalización alguna dentro del plazo de los 14 días siguientes a la fecha de su celebración.

Adicionalmente, las criptomonedas custodiadas no formarán parte de la masa concursal del eventual concurso de acreedores del custodio

La recepción y el envío de criptoactivos desde y hacia monederos de terceros no es posible. Tampoco es posible la entrega y el depósito de criptoactivos. Si el inversor desea disponer de los criptoactivos, esto sólo es posible mediante su venta.

## **Riesgo de los contratos a plazo / Riesgo de liquidación**

Las criptomonedas se asignan mediante entradas en la cadena de bloques. Esto se hace de forma descentralizada por varios organismos. La cadena de bloques es actualizada por diferentes organismos. Esto puede llevar a que la blockchain se actualice en paralelo en

8



diferentes hilos. Ejemplo: El nodo completo "A" actualiza simultáneamente el bloque XYZ de la cadena de bloques de Bitcoin con datos de transacciones, mientras que el nodo completo "B" actualiza otras transacciones en el mismo bloque. Posteriormente, la mayoría de las entidades que actualizan la blockchain se ponen de acuerdo sobre cuál de las cadenas es la cadena vinculante que se seguirá actualizando. La otra hebra se denomina entonces bifurcación y ya no se une. Si una transacción que afecta al cliente está en una bifurcación, éste no ha recibido la criptomoneda y no podrá seguir recibéndola. A continuación, debe haber una corrección de la transacción del cliente. Esto también puede significar una inversión. En este contexto, teóricamente también es posible que se "elimine" de este modo una transacción de hace mucho tiempo. Sin embargo, el mercado asume que si sólo se actualizan unos pocos bloques en la cadena de bloques, ya no existe un "riesgo de bifurcación" prácticamente relevante.

Las criptomonedas también tienen que ser liquidadas. Sin embargo, la liquidación de estas operaciones también puede tardar más que la de las transacciones de acciones normales. Por regla general, no es el caso, pero aquí tampoco se puede descartar que surjan dificultades en la entrega de criptomonedas y/o pagos. Esto puede llevar a que las transacciones correspondientes de un cliente tengan que ser anuladas.

## **Impuestos**

Las inversiones en los distintos tipos de activos pueden generar rentas o ganancias y pérdidas de capital. Por ejemplo, a través de la venta de una criptomoneda por un precio más alto al precio de compra original. Asimismo, las promociones de Trade Republic, pueden considerarse rendimientos de capital.

En cualquier caso, Trade Republic no deduce ningún impuesto a los clientes en las transacciones con criptomonedas ni realiza ninguna declaración de relevancia fiscal para el cliente. Cada cliente debe hacerlo de forma independiente con su asesor fiscal. Trade Republic no ofrece asesoramiento fiscal.

Trade Republic facilita con carácter anual un resumen de impuestos que incluye toda la información necesaria para cumplimentar la declaración de la renta en el que caso de que estés sujeto a esta obligación tributaria. Para acceder a este informe, visita tu perfil dentro de nuestra aplicación: Perfil -> Resumen de Impuestos

Puedes consultar más información al respecto en el sitio web oficial de la Agencia Tributaria.

## **Riesgo normativo**

Los Estados a veces miran con ojos críticos las criptomonedas porque son difíciles de controlar. No es imposible que una autoridad de supervisión o un Estado prohíba total o parcialmente las criptomonedas o regule el comercio de las mismas con más fuerza. Esto puede tener efectos adversos para los clientes, hasta el punto de que no puedan reducir sus participaciones o tengan que aceptar reducciones significativas de los precios. El aumento de la regulación también puede hacer que la criptomoneda sea menos atractiva para los inversores y que los precios caigan. Todo esto también puede ocurrir si una autoridad extranjera (o un estado) con el poder adecuado regula la criptomoneda e insta a todos los participantes del mercado en todo el mundo a cumplir con esta decisión.

### **Riesgos del software**

Las criptomonedas se basan en el software. Como cualquier otro software, nunca hay garantía de que el software subyacente a la criptomoneda esté libre de errores. Sin embargo, cualquier error puede afectar a las criptomonedas que tenga el cliente.

Una cadena de bloques también puede ser atacada por malware (por ejemplo, ataques de minería). También es posible que se espíen las claves privadas en el depósito y así se "roben" las criptomonedas.