Definiciones y Divulgación de riesgos de activos digitales

1. Definiciones

Los términos y abreviaturas establecidos a continuación tendrán el siguiente significado, si no se indica de otro modo en el contrato.

Bitcoin	Es una criptomoneda, una moneda digital descentralizada sin un banco central o administrador único, que se puede enviar de un usuario a otro en la red Bitcoin sin necesidad de intermediarios. Los nodos de la red verifican mediante criptografía las transacciones, que se registran en un libro de cuentas público distribuido llamado blockchain.
Blockchain	Es una tecnología de contabilidad distribuida (DLT). Es un libro de cuentas o base de datos digital a la que se pueden agregar datos continuamente y que no se puede modificar. Una red de ordenadores (denominados "nodos") ejecuta el protocolo de software.La red agrupa transacciones u otros datos en bloques de forma independiente y continua, los valida y los agrega a una cadena existente de bloques validados. Las cadenas de bloques o blockchains se utilizan, por ejemplo, para transacciones en Bitcoin, Ethereum y otras criptomonedas. La tecnología blockchain utiliza una firma criptográfica conocida como "hash" para encadenar bloques. El hash emplea un procedimiento de cifrado asimétrico en el que cada usuario tiene una clave pública y una privada. Estas se guardan en un monedero que puede almacenarse online en un ordenador, un Smartphone o un monedero hardware e incluso un monedero de papel. Una blockchain pública se distribuye, es accesible para cualquier persona y es gestionada por un gran número de participantes anónimos sin intermediarios (por ejemplo, Bitcoin y Ethereum). Por otro lado, una blockchain privada es gestionada por uno o más administradores de red y solo es accesible para participantes identificados y autorizados. También existen formas híbridas y blockchains de consorcio en las que el protocolo puede ser público, pero solo ciertos participantes pueden validar las transacciones.
Criptomoneda	Es una moneda digital de valor no emitida ni garantizada por un banco central o una autoridad pública, que no posee un estatus legal de moneda o dinero.
Activos digitales	Se refiere a las criptomonedas basadas en tecnología blockchain u otra DLT, que están destinadas o se utilizan con fines de pago y no reúnen los requisitos ni representan valores u otros instrumentos financieros.
Libro de cuentas distribuido (DLT)	Es un medio compartido y seguro de gestión de datos en una red informática distribuida. En términos simples, un libro de cuentas distribuido es una base de datos que se distribuye en una gran cantidad de ordenadores en red y que sincroniza y valida de manera independiente y continua los datos o transacciones introducidos por los participantes. Los participantes tienen acceso en todo momento a un historial verificable de toda la información almacenada, que no se puede manipular, . DLT tiene una definición más amplia que "blockchain" y cubre más posibilidades.

Ether	Es la criptomoneda generada por la plataforma Ethereum como recompensa a los nodos de minería por los cálculos realizados y es la única moneda aceptada en el pago de tarifas de transacción en la plataforma Ethereum.
Ethereum	Es una plataforma informática distribuida de código abierto, pública y basada en blockchain que ofrece la funcionalidad de contrato inteligente (scripting).
Moneda fiduciaria o "Fiat"	Moneda de curso legal que cuenta con el respaldo del gobierno central que la emite. Algunos ejemplos son el franco suizo, el euro y el dólar estadounidense.
Hot Wallet	Es un monedero online. Al estar conectado a Internet, un Hot Wallet es más accesible, pero tiene la desventaja de ser más vulnerable a la piratería o robo que un monedero frío o Cold Wallet.
Clave privada	Es un código criptográfico que funciona como una contraseña secreta que permite al usuario firmar una transacción de activos digitales y transferir los activos digitales a otra dirección. El uso de la clave privada demuestra la propiedad de los activos digitales.
Dirección pública	Es una cadena de letras y números desde los que se pueden enviar activos digitales. Una dirección de Bitcoin comienza con 1,3 o bc1 y tiene una longitud de 27 a 34 caracteres alfanuméricos. La dirección suele ser una versión hash de la clave pública.
Clave pública	Es una cadena de letras y números derivada de una clave privada. Una clave pública permite recibir criptoactivos generando una dirección pública.
Contrato inteligente	Es un protocolo informático autoejecutable basado en una "blockchain" que replica condiciones contractuales predefinidas en forma de código de programa. Una transacción realizada mediante un contrato inteligente se ejecuta automáticamente si todas las partes involucradas cumplen las condiciones predefinidas. Los contratos inteligentes pueden replicar, verificar o ayudar técnicamente a procesar el contenido de los contratos legales. El protocolo informático supervisa automáticamente las condiciones predefinidas y lleva a cabo de manera independiente las acciones acordadas por las partes cuando ocurre un evento desencadenante específico. En función de su diseño, los contratos inteligentes también pueden constituir contratos legales por derecho propio.
Transferir	Se refiere a la ejecución de transferencias entrantes y salientes en moneda Fiat o en activos digitales con terceros aprobados siguiendo los criterios de la regla de viaje (o "Travel Rule") con un proceso sólido de KYC/AML.
Monedero	Es una herramienta (aplicación de software, hardware u otro mecanismo o medio) que permite mantener, almacenar y transferir activos digitales.
Warm Wallet	Es un monedero con características de seguridad mejoradas gracias a un procedimiento de firma múltiple.

2. Observaciones generales

2.1. Descripción de criptomonedas

Las criptomonedas son una representación digital de valor no emitida ni garantizada por un banco central o una autoridad pública, que no posee un estatus legal de moneda o dinero.

Las criptomonedas son aceptadas por personas físicas o jurídicas como medio de intercambio y pueden ser transferidas, almacenadas y comercializadas electrónicamente. Su valor depende en gran medida de la oferta y demanda del mercado.

2.2. Libro de cuentas distribuido

La tecnología de contabilidad distribuida (DLT) es un medio compartido y seguro de gestionar datos en una red informática distribuida. En términos simples, un libro de cuentas distribuido es una base de datos que se distribuye en una gran cantidad de ordenadores en red y, en principio, sincroniza y valida de manera independiente y continua los datos o transacciones introducidos por los participantes. Los participantes tienen acceso en todo momento a un historial verificable, que no se puede manipular, de toda la información almacenada en un conjunto de datos específico. DLT tiene una definición más amplia que "blockchain" y cubre más posibilidades.

2.3. Blockchain

La tecnología "blockchain" o de cadena de bloques es una forma posible de tecnología de contabilidad distribuida (DLT). Es un libro de cuentas o base de datos digital a la que se pueden agregar datos continuamente y que no se puede modificar. Una red de ordenadores (denominados "nodos") ejecuta el protocolo de software. En principio, la red agrupa transacciones u otros datos en bloques de forma independiente y continua, los valida y los agrega a una cadena existente de bloques validados. Las cadenas de bloques o blockchains se utilizan, por ejemplo, para transacciones en Bitcoin, Ether y otras criptomonedas. La tecnología blockchain utiliza una firma criptográfica conocida como "hash" para encadenar bloques. El hash emplea un procedimiento de cifrado asimétrico en el que cada usuario tiene una clave pública y una privada. Estas se guardan en un monedero que puede almacenarse online en un ordenador, un Smartphone o un monedero hardware e incluso un monedero de papel. Una blockchain pública se distribuye, es accesible para cualquier persona y es gestionada por un gran número de participantes anónimos sin intermediarios (por ejemplo, Bitcoin y Ethereum). Por otro lado, una blockchain privada es gestionada por uno o más administradores de red y solo es accesible para participantes identificados y autorizados. También existen formas híbridas y "blockchains" de consorcio en las que el protocolo puede ser público, pero solo ciertos participantes pueden validar las transacciones.

2.4. Bitcoin y Ether

Bitcoin es una criptomoneda. Es una moneda digital descentralizada sin un banco central o administrador único que se puede enviar de un usuario a otro en la red Bitcoin sin necesidad de intermediarios. Los nodos de la red verifican mediante criptografía las transacciones, que se registran en un libro de cuentas público distribuido llamado blockchain.

Ether es la criptomoneda generada por la plataforma Ethereum como recompensa a los nodos de minería por los cálculos realizados y es la única moneda aceptada en el pago de tarifas de transacción en la plataforma. Ethereum es una plataforma informática distribuida de código abierto, pública y basada en blockchain que ofrece la funcionalidad de contrato inteligente (scripting).

Actualmente, el Banco no admite la custodia, administración o ejecución de contratos inteligentes basados en Ethereum o en cualquier otra plataforma de computación distribuida basada en blockchain.

El Banco puede, a su discreción, determinar de vez en cuando ofrecer servicios de custodia, administración, ejecución o cualquier otro tipo de servicios para y con respecto a cualquier tipo de contratos inteligentes.

2.5. Moneda fiduciaria o "Fiat"

La moneda fiduciaria es una moneda de curso legal cuyo valor está respaldado por el gobierno que la emitió. Algunos ejemplos son el franco suizo, el euro y el dólar estadounidense.

3. Acuerdo de activos digitales

3.1. Términos y definiciones en mayúscula

Los términos en mayúscula en este documento de Divulgación de riesgos de activos digitales tienen el mismo significado que se define en el Acuerdo de activos digitales con BBVA.

Al igual que en el Acuerdo de activos digitales, las criptomonedas, en particular Bitcoin y Ether, se definen como Activos digitales en esta Divulgación de riesgos de activos digitales.

4. Riesgos de los activos digitales

4.1. Notas preliminares

La presente Divulgación de riesgos de activos digitales describe ciertos riesgos asociados con estos activos. Es probable que existan riesgos adicionales relacionados, ya que no se pueden anticipar todos los riesgos de los Activos digitales. Debido a la nueva tecnología en la que se basan los Activos digitales, pueden surgir nuevos riesgos.

El Banco recomienda al Cliente que obtenga asesoramiento profesional antes de invertir en Activos digitales.

4.2. Volatilidad

El valor de la criptomoneda depende principalmente de la voluntad de los participantes del mercado de cambiar moneda fiduciaria por Activos digitales o criptomonedas por criptomonedas o de aceptar criptomonedas como pago.

Esta gran dependencia de la oferta y la demanda de criptomonedas y la falta de garantía de que una persona que acepta una moneda digital como pago hoy continúe haciéndolo en el futuro conduce a una mayor volatilidad en comparación con las monedas tradicionales.

Los Activos digitales no son moneda de curso legal y, por lo tanto, ningún banco central u otra institución pueden intervenir para estabilizar el valor de los mismos ni prevenir o mitigar la evolución ilógica de los precios.

Otras circunstancias como cambios y avances en tecnología, fraude, robo y ciberataques, entre otros, pueden incrementar aún más la volatilidad y así aumentar la posibilidad de ganancias y pérdidas de inversión.

Esta volatilidad y, como consecuencia, la imprevisibilidad del precio de las criptomonedas puede resultar en pérdidas significativas en un corto período de tiempo e incluso en un mismo día.

4.3. Riesgos de liquidez

Dependiendo de las condiciones del mercado, puede ser difícil si no imposible liquidar rápidamente las posiciones de Activos digitales por un precio razonable, en particular si el Banco no puede negociar los Activos digitales en un momento determinado o de forma permanente. Tales condiciones pueden ocurrir, por ejemplo, si ningún Proveedor externo está dispuesto a negociar los Activos digitales o si la negociación se detiene en circunstancias específicas, o en el caso de una actividad de comercialización inusual. La ejecución de una transacción será particularmente difícil cuando la volatilidad de un Activo digital en particular sea alta.

Esto significa que en determinadas circunstancias, en particular en casos de iliquidez, es posible que el Banco no pueda (i) comprar o vender Activos digitales y/o (ii) ejecutar Órdenes o Transacciones. La capacidad del Cliente para comprar o vender Activos digitales o para realizar liquidaciones puede ser limitada. En tales circunstancias, al Cliente puede resultarle difícil e incluso imposible poder comprar o vender Activos digitales.

4.4. Riesgos legislativos y regulatorios

Los cambios o acciones legislativas y reglamentarias de cualquier estado o a nivel internacional pueden afectar negativamente el uso, la transferencia, el intercambio y el valor de los Activos digitales y pueden aumentar la volatilidad de estos.

4.5. Riesgos de transacción

Las transacciones en moneda digital pueden ser irreversibles. Como resultado, las pérdidas debidas a transacciones fraudulentas o accidentales pueden no ser recuperables.

4.6. Riesgos informáticos

El Cliente puede experimentar pérdidas debido a uno o más de los siguientes riesgos informáticos (la lista no es exhaustiva): fallos del sistema, fallos de hardware, fallos de software, interrupciones de la conectividad de la red y corrupción de datos.

El funcionamiento de los Activos digitales se basa en la tecnología de Contabilidad distribuida, que aún se encuentra en una etapa inicial. Por tanto, es probable que experimente cambios importantes en el futuro. Los avances tecnológicos como la criptografía, el descifrado de códigos y las técnicas informáticas específicas pueden suponer un riesgo para la seguridad de los Activos digitales. Además, las tecnologías alternativas pueden afectar negativamente el precio y la liquidez de los Activos digitales.

El funcionamiento de los Activos digitales y de las criptomonedas está basado en software de código abierto. Los desarrolladores de dicho software de código abierto no son empleados ni están controlados por el Banco y pueden instalar errores de programación en el software de código abierto manteniendo las debilidades de los Activos digitales, como errores de programación y amenazas de fraude, robo o ciberataques.

Las redes de Contabilidad distribuida han experimentado un aumento en el número de transacciones en los últimos años. Un número cada vez mayor de transacciones junto con la incapacidad de implementar cambios en la tecnología de Contabilidad distribuida puede resultar en un tiempo de procesamiento de las Transacciones más lento.

4.7. Riesgos cibernéticos

La naturaleza de los Activos digitales puede conducir a un mayor riesgo de fraude o ciberataques, como ataques que utilizan la potencia informática suficiente para sobrecargar el funcionamiento normal de la cadena de bloques de los Activos digitales u otra tecnología subyacente. Dichos ataques podrían resultar en una pérdida sustancial, inmediata e irreversible de monedas virtuales. Incluso un evento menor de ciberseguridad con respecto a los Activos digitales puede resultar en un precio a la baja del Activo digital respectivo.

4.8. Conocimientos necesarios sobre comercialización de Activos digitales

La comercialización de Activos digitales requiere conocimiento de los mercados de Activos digitales. Al intentar obtener ganancias a través de la comercialización de Activos digitales, el Cliente compite con comerciantes de todo el mundo. El Cliente debe tener el conocimiento y la experiencia adecuados antes de participar en la comercialización sustancial de Activos digitales.

4.9. Las inversiones y la comercialización de Activos digitales son especulativas

Las inversiones y la comercialización de Activos digitales son especulativas y, por lo tanto, pueden conllevar un riesgo extremo. La comercialización de Activos digitales puede generar pérdidas financieras importantes e inmediatas. La volatilidad e imprevisibilidad del precio de los Activos digitales en relación con la moneda fiduciaria pueden tener como resultado una pérdida total o significativa en un corto período de tiempo.

Existe el riesgo de una pérdida sustancial o total al invertir o comerciar con Activos digitales. El Cliente reconoce y acepta que accederá y utilizará este servicio bajo su propio riesgo.

4.10. Bifurcaciones (Hard Forks) y otros ataques

Cualquier desacuerdo entre las partes interesadas de un libro de cuentas distribuido en particular puede originar la división de un Activo digital relevante en dos o más versiones incompatibles (como un evento llamado "Hard Fork" o bifurcación). El tratamiento de las bifurcaciones y eventos similares (como los "airdrops" y otros eventos de asignación de Activos digitales) es incierto desde una perspectiva legal y práctica. Las bifurcaciones pueden hacer que los Activos digitales se dupliquen, es decir, una versión de los Activos digitales permanecerá en una versión específica del libro de cuentas distribuido, mientras que la otra versión de los Activos digitales se comercializará en otra versión del mismo libro de cuentas distribuido.

El Cliente reconoce que es posible que el Banco no pueda disfrutar de bifurcaciones o eventos similares (como "airdrops" y otros eventos de asignación de Activos digitales). Es posible que el Banco tampoco pueda admitir ambas versiones de un libro de cuentas distribuido (y no tiene obligación de hacerlo). Dependiendo de la decisión del Banco, es posible que el Cliente no pueda reclamar la versión de los Activos digitales admitida por el Banco. Esto podría conducir a la pérdida total de valor de los Activos digitales.

Un ataque del 51 % se refiere a un ataque a un blockchain por un grupo de mineros que controlan más del 50 % de la tasa de hash de minería o la potencia de cálculo de la red.

Los atacantes podrían evitar que las nuevas transacciones obtengan confirmaciones, lo que les permitiría detener los pagos entre algunos o todos los usuarios. También podrían revertir las transacciones que se completaron mientras tenían el control de la red, lo que significa que podrían gastar el doble de los Activos digitales.

Naturaleza pública de los libros de cuentas distribuidos

Los clientes deben saber que cualquier compra y venta de Activos digitales puede almacenarse en un libro de cuentas distribuido público y, por lo tanto, puede tener visibilidad pública.