

**Tether: monedas fiduciarias en la cadena de bloques de Bitcoin**

**Abstracto**. Un token digital respaldado por moneda fiduciaria proporciona a las personas y organizaciones un método robusto y descentralizado para intercambiar valor mientras se usa una unidad de contabilidad familiar. La innovación de las cadenas de bloques es un libro mayor global auditable y criptográficamente asegurado. Los emisores de tokens respaldados por activos y otros participantes del mercado pueden aprovechar la tecnología blockchain, junto con los sistemas de consenso integrados, para realizar transacciones en monedas y activos familiares y menos volátiles. Para mantener la responsabilidad y garantizar la estabilidad en el precio de cambio, proponemos un método para mantener una relación de reserva de uno a uno entre un token de criptomoneda, llamado amarre, y su activo asociado en el mundo real, la moneda fiduciaria. Este método utiliza la cadena de bloques de Bitcoin, Prueba de reservas,

# Tabla de contenido

Tabla de contenido Introducción

Pila de tecnología y procesos Tether Technology Stack Flujo de fondos Proceso Prueba de reservas Implementación del proceso Debilidades

Aplicaciones principales Para intercambios de particulares por comerciantes

Innovaciones futuras

Contratos inteligentes y multifirma Prueba de innovaciones de solvencia

Conclusión Apéndice

Defectos de auditoría: intercambios y carteras Limitaciones de los sistemas Fiatpegging existentes Ejemplos de riesgo de mercado

Legal y Cumplimiento Glosario de términos Referencias

# Introducción

Existe una amplia gama de activos en el mundo que la gente elige libremente como depósito de valor, medio transaccional o inversión. Creemos que la cadena de bloques de Bitcoin es una mejor tecnología para realizar transacciones, almacenar y contabilizar estos activos. La mayoría de las estimaciones miden la riqueza mundial en alrededor de 250 billones de dólares [1] y gran parte de esa riqueza está en manos de bancos o instituciones financieras similares. La migración de estos activos a la cadena de bloques de Bitcoin representa una oportunidad proporcionalmente grande.

Bitcoin fue creado como “un sistema de pago electrónico basado en pruebas criptográficas en lugar de confianza, lo que permite a dos partes interesadas realizar transacciones directamente entre sí sin la necesidad de un tercero de confianza”. [2]. Bitcoin creó una nueva clase de moneda digital, una moneda digital descentralizada o criptomoneda1.

Algunas de las principales ventajas de las criptomonedas son: bajos costos de transacción, transferibilidad y convertibilidad internacional sin fronteras, propiedad e intercambio sin confianza, pseudoanonimato, transparencia en tiempo real e inmunidad a los problemas del sistema bancario heredado [3]. Las explicaciones comunes para el uso general limitado actual de las criptomonedas incluyen: fluctuaciones volátiles de precios, comprensión inadecuada de la tecnología del mercado masivo y facilidad de uso insuficiente para usuarios no técnicos.

La idea de las criptomonedas vinculadas a activos se popularizó inicialmente2 en la comunidad de Bitcoin por el documento técnico de Mastercoin escrito por JR Willett en enero de 2012 [4]. Hoy, estamos comenzando a ver estas ideas construidas con BitAssets, Ripple, Omni, Nxt, NuShares / Bits y otros. Se debe tener en cuenta que todos los intercambios y billeteras de Bitcoin (como Coinbase, Bitfinex y Coinapult) que le permiten mantener el valor como moneda fiduciaria ya brindan un servicio similar en el sentido de que los usuarios pueden evitar la volatilidad (u otros rasgos) de una criptomoneda en particular al vendiéndolos por moneda fiduciaria, oro u otro activo. Además, casi todos los tipos de instituciones financieras existentes, proveedores de pagos, etc., que le permiten mantener el valor fiduciario (u otros activos) posteriormente brindan un servicio similar.

Si bien el objetivo de cualquier criptomoneda exitosa es eliminar por completo el requisito de confianza, cada una de las implementaciones mencionadas anteriormente depende de un tercero confiable o tiene otros inconvenientes y limitaciones técnicos, basados ​​en el mercado o basados ​​en procesos3.

1 Para obtener definiciones en todo, consulte Glosario de términos

2 Pero se ha discutido desde el BitGold propuesto por el Dr. Szabo [5]

3 Resumido en el Apéndice, aquí: Limitaciones de los sistemas Fiatpegging existentes

En nuestra solución, las criptomonedas fiatpeg se denominan "ataduras". Todas las ataduras se emitirán inicialmente4 en la cadena de bloques de Bitcoin a través del protocolo Omni Layer y, por lo tanto, existen como un token de criptomoneda. Cada unidad de Tether emitida en circulación está respaldada en una proporción de uno a uno (es decir, un Tether USDT es un dólar estadounidense) por la correspondiente unidad de moneda fiduciaria mantenida en depósito por Tether Limited con sede en Hong Kong. Los Tethers pueden canjearse / canjearse por la moneda fiduciaria subyacente de conformidad con los términos de servicio de Tether Limited o, si el titular lo prefiere, el valor al contado equivalente en Bitcoin. Una vez que se ha emitido un tether, se puede transferir, almacenar, gastar, etc., como bitcoins o cualquier otra criptomoneda. La moneda fiduciaria en reserva ha ganado las propiedades de una criptomoneda y su precio está permanentemente ligado al precio de la moneda fiduciaria.

Nuestra implementación tiene las siguientes ventajas sobre otras criptomonedas fiatpegged:

* Las ataduras existen en la cadena de bloques de Bitcoin en lugar de una cadena de bloques "altcoin" menos desarrollada / probada ni dentro de un software de código cerrado que se ejecuta en bases de datos privadas centralizadas.
* Los Tethers se pueden utilizar como bitcoins, es decir, en un entorno p2p, pseudoanónimo, descentralizado y criptográficamente seguro.
* Los Tethers se pueden integrar con comerciantes, intercambios y billeteras con la misma facilidad que Bitcoin o cualquier otra criptomoneda.
* Tethers hereda las propiedades del protocolo Omni Layer que incluyen: un intercambio descentralizado; cifrado de billetera, código abierto y basado en navegador; transparencia basada en Bitcoin, responsabilidad, seguridad multipartita y funciones de informes.
* Tether Limited emplea un enfoque simple pero efectivo para realizar la Prueba de Reservas que reduce significativamente nuestro riesgo de contraparte como custodio de los activos de reserva.
* La emisión o rescate de Tether no enfrentará restricciones de precios o liquidez. Los usuarios pueden comprar o vender tantas ataduras como quieran, rápidamente y con tarifas muy bajas.
* Tethers no enfrentará ningún riesgo de mercado5, como eventos del cisne negro, crisis de liquidez, etc., ya que las reservas se mantienen en una proporción uno a uno en lugar de depender de las fuerzas del mercado.
* La implementación de respaldo uno a uno de Tether es más fácil de entender para los usuarios no técnicos en comparación con las técnicas de garantía o las estrategias derivadas.

En cualquier momento dado, el saldo de la moneda fiduciaria mantenida en nuestras reservas será igual (o mayor que) el número de ataduras en circulación. Esta configuración simple soporta más fácilmente un proceso confiable de Prueba de Reservas; un proceso que es fundamental para mantener la paridad de precios entre las ataduras en circulación y la moneda fiduciaria subyacente mantenida en reservas. En este artículo proporcionamos evidencia6 que muestra el intercambio y

Pronto llegarán 4 más protocolos de Bitcoin 2.0, como Ripple, Nxt, etc.

5 Ver Apéndice, sección: Ejemplos de riesgo de mercado

6 Ver sección: Prueba de proceso de solvencia

Las auditorías de billetera (en su estado actual) son muy poco confiables (es decir, fallas en los métodos de prueba de solvencia [6]) y en su lugar proponen que los intercambios y las billeteras nos subcontraten la custodia de los fondos de los usuarios a través de ataduras.

Los usuarios pueden comprar amarres en Tether.to (nuestra billetera web) o en intercambios compatibles como Bitfinex, que admiten amarres como método de depósito y retiro. Los usuarios también pueden realizar transacciones y almacenar ataduras con cualquier billetera habilitada para Omni Layer como Ambisafe, Holy Transaction u Omni Wallet. Se alienta a otros intercambios, billeteras y comerciantes a que se comuniquen con nosotros sobre la integración de tether como sustituto de los métodos tradicionales de pago fiduciario.

Reconocemos que nuestra implementación no está perfectamente descentralizada7 ya que Tether Limited debe actuar como un custodio centralizado de los activos de reserva (aunque las ataduras en circulación existen como una moneda digital descentralizada). Sin embargo, creemos que esta implementación sienta las bases para la creación de innovaciones futuras que eliminarán estas debilidades, crearán una plataforma sólida para nuevos productos y servicios y respaldarán el crecimiento y la utilidad de la cadena de bloques de Bitcoin a largo plazo. Algunas de estas innovaciones incluyen:

* Facilitación de pagos móviles entre usuarios y otras partes, incluidos otros usuarios y comerciantes
* Transferencia de valor fiduciario instantánea o casi instantánea entre partes descentralizadas (como múltiples intercambios)
* Introducción al uso de contratos inteligentes y capacidades de firma múltiple para mejorar aún más el proceso de seguridad general, Prueba de reservas y habilitar nuevas funciones.

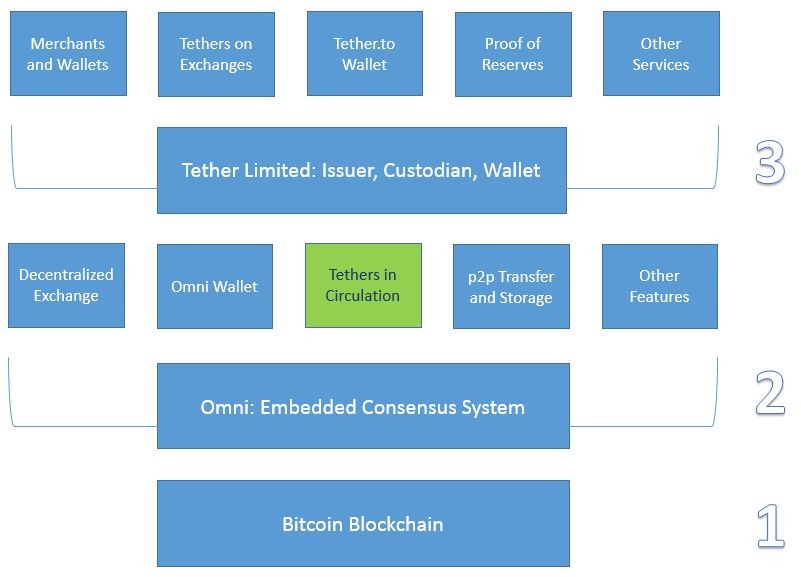
# Pila de tecnología y procesos

Cada tether emitido en circulación estará respaldado en una proporción de uno a uno con la cantidad equivalente de la moneda fiduciaria correspondiente mantenida en reservas por Tether Limited con sede en Hong Kong. Como custodio del activo de respaldo, actuamos como un tercero de confianza responsable de ese activo. Este riesgo se mitiga con una implementación simple que reduce colectivamente la complejidad de realizar auditorías tanto fiduciarias como criptográficas, al tiempo que aumenta la seguridad, demostrabilidad y transparencia de estas auditorías.

## Pila de tecnología Tether

La pila tiene 3 capas y numerosas características, que se entienden mejor a través de un diagrama.

7 Ver sección: Debilidades de implementación

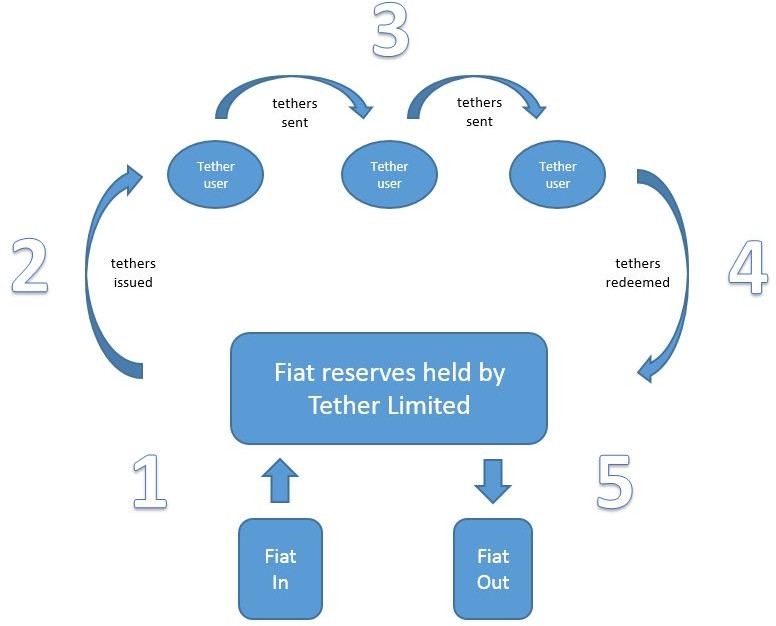


Aquí hay una revisión de cada capa.

1. La primera capa es la cadena de bloques de Bitcoin. El libro mayor transaccional de Tether está integrado en la cadena de bloques de Bitcoin como metadatos a través del sistema de consenso integrado, Omni.
2. La segunda capa es el protocolo Omni Layer. Omni es una tecnología fundamental que puede:
   1. Otorgue (cree) y revoque (destruya) tokens digitales representados como metadatos incrustados en la cadena de bloques de Bitcoin; en este caso, tokens digitales fijados, amarres.
   2. Rastree e informe la circulación de amarres a través de Omnichest.info (el ID de activo de Omni # 31, por ejemplo, representa TetherUSD) y la API de Omnicore.
   3. Permita que los usuarios realicen transacciones y almacenen ataduras y otros activos / tokens en un:
      1. p2p, pseudoanónimo, entorno criptográficamente seguro.
      2. Webwallet cifrado, basado en navegador y de código abierto: Omni Wallet.
      3. sistema de soporte de almacenamiento en frío de múltiples firmas y fuera de línea
3. La tercera capa es Tether Limited, nuestra entidad comercial principalmente responsable de:
   1. Aceptar depósitos fiduciarios y emitir los amarres correspondientes
   2. Envío de retiros fiduciarios y revocación de los amarres correspondientes
   3. Custodia de las reservas fiduciarias que respaldan todas las ataduras en circulación
   4. Informar públicamente la prueba de reservas y otros resultados de auditoría
   5. Iniciar y administrar integraciones con billeteras, intercambios y comerciantes de Bitcoin / blockchain existentes
   6. Operación de Tether.to, una billetera web que permite a los usuarios enviar, recibir, almacenar y convertir amarres de manera conveniente.

## Proceso de flujo de fondos

Hay cinco pasos en el ciclo de vida de una correa, que se comprenden mejor a través de un diagrama.



**Paso 1** El usuario deposita moneda fiduciaria en la cuenta bancaria de Tether Limited.

**Paso 2** Tether Limited genera y acredita la cuenta de Tether del usuario. Las correas entran en circulación. Cantidad de moneda fiduciaria depositada por el usuario = cantidad de ataduras emitidas al usuario (es decir, 10k USD depositados = 10k tetherUSD emitidos).

**Paso 3** Los usuarios realizan transacciones con ataduras 8. El usuario puede transferir, intercambiar y almacenar ataduras a través de una plataforma p2p de código abierto, pseudoanónimo, basada en Bitcoin.

**Paso 4** El usuario deposita amarres con Tether Limited para canjearlos en moneda fiduciaria.

**Paso 5** Tether Limited destruye las ataduras y envía moneda fiduciaria a la cuenta bancaria del usuario.

Los usuarios pueden obtener ataduras fuera del proceso mencionado anteriormente a través de un intercambio u otra persona. Una vez que una correa entra en circulación, se puede comerciar libremente entre cualquier empresa o individuo. Por ejemplo, los usuarios pueden comprar amarres de Bitfinex, y pronto habrá más intercambios.

El concepto principal que debe transmitir el diagrama de flujo de fondos es que Tether Limited es la única parte que puede poner en circulación amarres (crearlos) o sacarlos de circulación (destruirlos). Este es el proceso principal mediante el cual se mantiene la solvencia del sistema.

## Proceso de prueba de reservas

Prueba de solvencia, Prueba de reservas, Transparencia en tiempo real y otras frases similares han ido creciendo y resonando en la industria de las criptomonedas.

Las auditorías de cambio y billeteras, en su forma actual, son muy poco confiables. La insolvencia se ha producido en numerosas ocasiones en el ecosistema de Bitcoin, ya sea a través de piratería, mala gestión o fraude total. Los usuarios deben ser diligentes con su selección de intercambios y vigilantes en su uso de los intercambios. Incluso entonces, un usuario inteligente no podrá eliminar por completo los riesgos. Además, hay usuarios de intercambios como comerciantes y empresas que deben mantener saldos fiduciarios no triviales en los intercambios en todo momento. En lenguaje financiero, esto se conoce como el "riesgo de contraparte" de almacenar valor con un tercero.

Creemos que es seguro concluir que las auditorías de intercambio y billetera en su forma actual no son muy confiables. Estos procesos no garantizan a los usuarios que un custodio o intercambio sea solvente. Aunque ha habido grandes contribuciones para mejorar los procesos de auditoría de intercambio, como el enfoque del árbol de Merkle [6], fallas importantes

Aún quedan 9.

La configuración de prueba de reservas de Tether es novedosa porque simplifica el proceso de demostrar que el número total de ataduras en circulación (pasivos) siempre está totalmente respaldado por una cantidad igual de moneda fiduciaria mantenida.

8 Vea los beneficios de usar ataduras en la sección: Aplicaciones principales

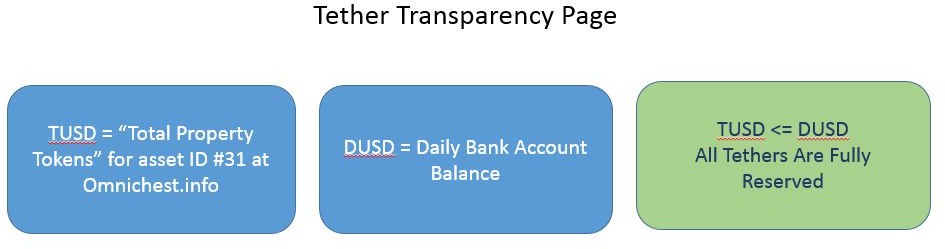
9 Ver sección: Defectos de auditoría: intercambios y carteras

en reserva (activos). En nuestra configuración, cada tetherUSD en circulación representa un dólar estadounidense mantenido en nuestras reservas (es decir, una proporción de uno a uno), lo que significa que el sistema está completamente reservado cuando la suma de todas las ataduras existentes (en cualquier momento) es exactamente igual al saldo. de USD mantenidos en nuestra reserva. Dado que las ataduras viven en la cadena de bloques de Bitcoin, la demostrabilidad y la contabilidad de las ataduras en cualquier momento dado es trivial.

Por el contrario, el monto total correspondiente de USD mantenidos en nuestras reservas se prueba mediante la publicación del saldo bancario y la realización de auditorías periódicas por parte de profesionales. Encuentre esta implementación más detallada a continuación:

* Tether Limited emite todas las ataduras a través del protocolo Omni Layer. Omni opera sobre la cadena de bloques de Bitcoin y, por lo tanto, todas las ataduras emitidas, canjeadas y existentes, incluido el historial de transacciones, son auditables públicamente a través de las herramientas proporcionadas en Omnichest.info.
  + El ID de activo de Omnichest.info para tetherUSD es # 31.
    - Aquí hay un enlace: <http://omnichest.info/lookupsp.aspx?sp=31>
  + Deje que el número total de ataduras emitidas con este ID de activo se indique como TUSDissue
  + Deje que el número total de ataduras canjeadas con este ID de activo se indique como TUSDredeem
  + Deje que el número total de amarres en circulación en cualquier momento se denote como TUSD
    - TUSD = TUSDissue TUSDredeem
    - TUSD = "Total de tokens de propiedad" @ <http://omnichest.info/lookupsp.aspx?sp=31>
* Tether Limited tiene una cuenta bancaria que recibirá y enviará moneda fiduciaria a los usuarios que compren / canjeen amarres directamente con nosotros.
  + Deje que la cantidad total depositada en esta cuenta se denote como DUSDdepo
  + Deje que el monto total retirado de esta cuenta se denote como DUSDwithd
  + Deje que el saldo en dólares de esta cuenta bancaria se denote como DUSD
    - DUSD = DUSDdepo DUSDwithd
* Cada tether emitido estará respaldado por la cantidad equivalente de unidad monetaria (un tetherUSD equivale a un dólar). Al combinar los procesos contables criptográficos y fiduciarios anteriores, concluimos la "Ecuación de solvencia" para el sistema Tether.
  + La ecuación de solvencia es simplemente TUSD = DUSD.
  + Cada tether emitido o canjeado, según lo registrado públicamente por la cadena de bloques de Bitcoin, corresponderá a un depósito o retiro de fondos de la cuenta bancaria.
  + La probabilidad de TUSD se basa en la cadena de bloques de Bitcoin como se discutió anteriormente.
  + La demostrabilidad de DUSD se basará en varios procesos:
    - Publicamos el saldo de la cuenta bancaria en la página de Transparencia de nuestro sitio web.
    - Los auditores profesionales verificarán, firmarán y publicarán regularmente nuestro saldo bancario subyacente y el estado de transferencia financiera.

Los usuarios podrán ver esta información desde nuestra página de transparencia, que se verá así:



Para mayor claridad, nos gustaría reconocer que el Tether System10 es diferente al Tether.to webwallet en términos de Prueba de Reservas. En este artículo, nos enfocamos principalmente en la Prueba de Reservas para el Sistema de Tether, es decir, todos los amarres en circulación en cualquier momento. La billetera Tether.to es una billetera web orientada al consumidor que opera en un código fuente cerrado y servidores centralizados. La realización de una prueba de reservas para esta billetera es fundamentalmente diferente a lo que hemos descrito para el sistema Tether.

Estamos planeando la implementación de una solución de transparencia basada en PoR para la billetera Tether.to. Creemos que será el sistema PoR más avanzado que existe en la actualidad. Supera casi todos los desafíos descritos en el apéndice11 sobre este tema. Eso sí, los usuarios siempre pueden proteger las ataduras mediante la administración de las claves privadas ellos mismos o mediante Omni Wallet.

## Debilidades de implementación

Entendemos que nuestra implementación no crea de inmediato un sistema de criptomonedas totalmente confiable. Principalmente porque los usuarios deben confiar en Tether Limited y nuestra institución bancaria heredada correspondiente para ser el custodio de los activos de reserva. Sin embargo, casi todos los intercambios y carteras (suponiendo que tengan USD / fiats) están sujetos a las mismas debilidades. Los usuarios de estos servicios ya están sujetos a estos riesgos. A continuación, se muestra un resumen de las debilidades de nuestro enfoque:

* Podríamos ir a la quiebra
* Nuestro banco podría declararse insolvente
* Nuestro banco podría congelar o confiscar los fondos.
* Podríamos fugarnos con los fondos de reserva

10 Ver Glosario de términos

11 Ver Defectos de auditoría: intercambios y carteras

* Recentralizado del riesgo a un solo punto de falla

Observe que casi todas las carteras y los intercambios de divisas digitales (suponiendo que tengan USD / fiat) ya enfrentan muchos de estos desafíos. Por tanto, los usuarios de estos servicios ya están sujetos a estos riesgos. A continuación, describimos cómo se abordan cada una de estas inquietudes.

*Podríamos ir a la quiebra* En este caso, la entidad comercial Tether Limited iría a la quiebra, pero los fondos del cliente estarían seguros y, posteriormente, todas las ataduras seguirían siendo canjeables. La mayoría de las violaciones de seguridad en las empresas de Bitcoin se han dirigido a las criptomonedas en lugar de a las cuentas bancarias. Dado que todas las ataduras existen en la cadena de bloques de Bitcoin, las personas pueden almacenarlas directamente mediante la seguridad de sus propias claves privadas.

*Nuestro banco podría declararse insolvente* Este es un riesgo que enfrentan todos los usuarios del sistema financiero heredado y todos los operadores de cambio. Tether Limited actualmente tiene cuentas en Cathay United Bank y Hwatai Bank en Taiwán, quienes conocen y confían en que el modelo comercial de Tether es aceptable. Se están estableciendo socios bancarios adicionales en otras jurisdicciones para mitigar aún más esta preocupación.

*Nuestro banco podría congelar o confiscar los fondos.* Nuestros bancos son conscientes de la naturaleza de Bitcoin y aceptan negocios de Bitcoin. También brindan servicios bancarios a algunos de los intercambios de Bitcoin más grandes del mundo. Los procesos KYC / AML que seguimos también son utilizados por los otros intercambios de moneda digital que actualmente realizan. Nos han asegurado que cumplimos plenamente12.

*Podríamos fugarnos con los activos de reserva* El estatuto corporativo es público13, así como los nombres, ubicaciones y reputación de los propietarios de negocios. La propiedad de la cuenta está legalmente vinculada a los estatutos corporativos. Cualquier transferencia dentro o fuera de la cuenta bancaria tendrá los rastros asociados y estará sujeta a políticas internas rígidas.

*Recentralización del riesgo a un solo punto de falla* Tenemos algunas ideas sobre cómo superar esto y las compartiremos en las próximas actualizaciones de blogs y productos. Hay muchas formas de abordar este problema. Por ahora, esta implementación inicial nos lleva por el camino correcto para realizar estas innovaciones en las siguientes versiones.

Al aprovechar las plataformas que hemos elegido, hemos reducido el riesgo de centralización a una responsabilidad singular: la creación y redención de tokens. Todos los demás aspectos del sistema están descentralizados.

12 Ver sección sobre Legal y Cumplimiento para más información

13 Igual que la nota al pie # 10

# Aplicaciones principales

En esta sección resumiremos y discutiremos las principales aplicaciones de las ataduras en el ecosistema Bitcoin / blockchain y para otros consumidores a nivel mundial. Dividimos a los beneficiarios en tres grupos de usuarios: intercambios, particulares y comerciantes.

Los principales beneficios, aplicables a todos los grupos:

* Propiedades de Bitcoin otorgadas a otras clases de activos
* Unidad de cuenta menos volátil y familiar
* Los activos del mundo migran a la cadena de bloques de Bitcoin

## Para intercambios

Los operadores de intercambio entienden que aceptar depósitos y retiros fiduciarios utilizando sistemas financieros heredados puede ser complicado, arriesgado, lento y costoso. Algunos de estos problemas incluyen:

* Identificar los proveedores de pago adecuados para su intercambio
  + transacciones irreversibles, protección contra fraudes, tarifas más bajas, etc.
* Integrando la plataforma con bancos que no tienen API
* Servir de enlace con estos bancos para coordinar el cumplimiento, la seguridad y generar confianza
* Costos prohibitivos para transferencias de pequeño valor
* 37 días para que se liquiden las transferencias bancarias internacionales
* Tarifas de conversión de moneda bajas y desfavorables

Al ofrecer ataduras, un intercambio puede aliviar las complicaciones anteriores y obtener beneficios adicionales, como:

* Acepte criptofiats como método de depósito / retiro / almacenamiento en lugar de utilizar un banco o proveedor de pago heredado
  + Permite a los usuarios mover fiat dentro y fuera del intercambio de manera más libre, rápida y económica.
* Subcontrate el riesgo de custodia fiduciaria a Tether Limited solo administre criptomonedas
* Agregue fácilmente otras monedas fiduciarias atadas como pares comerciales a la plataforma
* Asegure los activos del cliente únicamente a través de criptoprocesos aceptados
  + Seguridad multifirma, billeteras frías y calientes, billeteras HD, etc.
  + Realice auditorías de forma más fácil y segura en un entorno puramente criptográfico
* Cualquier cosa que uno pueda hacer con Bitcoin como intercambio se puede hacer con ataduras

Los usuarios de Exchange saben lo arriesgado que puede ser mantener monedas fiduciarias en un intercambio. Con el creciente número de casos de insolvencia, puede resultar bastante peligroso. Como se mencionó anteriormente, creemos que el uso de ataduras expone a los usuarios del intercambio a un menor riesgo de contraparte que mantener continuamente fiat en los intercambios. Además, hay otros beneficios de sujetar las correas, que se explican en la siguiente sección.

## Para individuos

En la actualidad, existen muchos tipos de usuarios individuales de Bitcoin en el mundo. Desde comerciantes que buscan obtener ganancias a diario; hasta inversores a largo plazo que buscan almacenar sus Bitcoins de forma segura; hasta compradores expertos en tecnología que buscan evitar las tarifas de las tarjetas de crédito o mantener su privacidad; hasta usuarios filosóficos que buscan cambiar el mundo; hasta aquellos que buscan remitir pagos a nivel mundial más efectivamente; para aquellos en países del tercer mundo que buscan acceso a servicios financieros por primera vez; para desarrolladores que buscan crear nuevas tecnologías; para todos aquellos que han encontrado muchos usos para Bitcoin. Para cada una de estas personas, creemos que las ataduras son útiles de formas similares, como:

* Realice transacciones en USD / valor fiduciario, de forma pseudoanónima, sin intermediarios / intermediarios
* Valor de USD / fiat de la cámara frigorífica asegurando las propias claves privadas
* Evite el riesgo de almacenar dinero fiduciario en intercambios, mueva el criptofiat dentro y fuera de los intercambios fácilmente
* Evite tener que abrir una cuenta bancaria fiduciaria para almacenar el valor fiduciario
* Mejore fácilmente las aplicaciones que funcionan con bitcoin para que también admitan tether
* Cualquier cosa que uno pueda hacer con Bitcoin como individuo también se puede hacer con tether

## Para comerciantes

Los comerciantes quieren centrarse en su negocio, no en los pagos. La falta de soluciones de pago globales, económicas y ubicuas continúa afectando a los comerciantes de todo el mundo, tanto grandes como pequeños. Los comerciantes merecen más. Estas son algunas de las formas en que Tether puede ayudarlos:

* Precio de los productos en USD / valor fiduciario en lugar de Bitcoin (sin tasas de conversión móviles / ventanas de compra)
* Evite la conversión de Bitcoin a USD / fiat y las tarifas y procesos asociados
* Evite las devoluciones de cargo, reduzca las tarifas y obtenga una mayor privacidad
* Proporcione servicios novedosos debido a las características de fiatcrypto
  + Microtip, tarjetas de regalo, más
* Cualquier cosa que uno pueda hacer con Bitcoin como comerciante también se puede hacer con tether

Innovaciones futuras Innovaciones de prueba de solvencia de contratos inteligentes y multifirma

# Conclusión

Tether constituye las primeras criptomonedas vinculadas a fiat basadas en Bitcoin que existen en la actualidad. Tether se basa en la cadena de bloques de Bitcoin, la cadena de bloques y el libro mayor público más seguro y probado que existe. Los Tethers están completamente reservados en una proporción uno a uno, completamente independiente de las fuerzas del mercado, los precios o las restricciones de liquidez. Tether tiene una implementación de Prueba de Reservas simple y confiable y se somete a auditorías profesionales regulares. Nuestras relaciones bancarias subyacentes, el cumplimiento y la estructura legal brindan una base segura para que seamos los custodios de los activos de reserva y emisores de ataduras. Nuestro equipo está compuesto por empresarios experimentados y respetados del ecosistema Bitcoin y más allá.

Estamos enfocados en organizar integraciones con negocios existentes en el espacio de las criptomonedas. Negocios como intercambios, billeteras, comerciantes y otros. Ya estamos integrados con Bitfinex, HolyTransaction, Omni Wallet, Poloniex, CCEX y más por venir. Comuníquese con nosotros para obtener más información.

# Apéndice

Defectos de auditoría: intercambios y carteras

A continuación, se muestra un resumen de las fallas actuales encontradas en las auditorías de billeteras y de intercambio basadas en tecnología14.

En el enfoque del árbol Merkle [6], los usuarios deben informar manualmente que sus saldos (hoja del usuario) se han incorporado correctamente en la declaración de responsabilidad del intercambio (el hash Merkle de la base de datos de los saldos del usuario del intercambio). Esta solución propuesta funciona si suficientes usuarios verifican que su cuenta se incluyó en el árbol y, en el caso de que su cuenta no esté incluida, se informará de esta instancia. Un riesgo potencial es que el propietario de una base de datos de intercambio pueda producir un hash que no sea la verdadera representación de

14 A diferencia de contratar a un auditor profesional

la base de datos en absoluto; tiene una base de datos incompleta que reduciría sus responsabilidades aparentes con los clientes, haciéndolos parecer solventes para una parte verificadora. Estos son algunos escenarios en los que un intercambio fraudulento excluiría cuentas y:

* + Cuentas “Bitdust”: las cuentas inactivas o con poca actividad reducirían la posibilidad de que un usuario desinteresado verificara o informara inconsistencias. En algunos casos, estas cuentas de largo plazo podrían representar un porcentaje significativo de los pasivos de la bolsa.
  + Ataque de "ballenas coludidas": Existe evidencia de que los grandes comerciantes de Bitcoin están operando en varios intercambios y moviendo los mercados significativamente. Dichos comerciantes deben tener reservas de capital en las bolsas más grandes para ejecutar órdenes rápidamente. A menudo, los comerciantes eligen intercambios en los que "confían". De esta manera, pueden estar seguros de que en caso de que surja un problema de piratería o de liquidez, tienen prioridad para sacar su dinero. En este caso, el intercambio y el comerciante podrían coludirse para eliminar el saldo de la cuenta de las ballenas de la base de datos antes de que se procese.
  + Ataque de alquiler de claves: para aprobar la auditoría, un intercambio malicioso podría alquilar las claves privadas a bitcoins que no son de su propiedad. Esto los haría parecer solventes al aumentar sus activos sin ningún reconocimiento de que esos fondos les fueron prestados. Asimismo, podrían "pedir prestada" moneda fiduciaria para hacer lo mismo.
  + Hay más ataques que no se comentan aquí.

Alcanzar la importancia estadística (integridad de los informes): incluso fuera de estos tres vectores de ataque, es posible que una base de datos que haya sido manipulada nunca se detecte si un número suficiente de usuarios no está validando los saldos. La probabilidad de que el 100% de los usuarios verifique los saldos es probablemente cero, incluso con una estructura de incentivos adecuada para que los usuarios verifiquen sus saldos. Por lo tanto, los auditores necesitarían herramientas estadísticas para hacer declaraciones sobre la validez de la base de datos de un intercambio en función de la frecuencia de muestreo, el tamaño y otras propiedades.

Actualmente, los usuarios no tienen forma de recibir una compensación por medios legales en caso de que algo salga mal con el intercambio. Por ejemplo, cuando Mt.Gox cerró las operaciones, es posible que muchos usuarios no hayan registrado de forma independiente los saldos de sus cuentas (pantallas impresas, mensajes firmados para sí mismos, etc.) de una manera que pudiera demostrar de manera concluyente a las autoridades que los pagarés de este intercambio realmente existían. Dichos usuarios están a merced del intercambio para publicar de alguna manera un registro de ese árbol hash o base de datos original.

La estructura propuesta en la que se realizarían estas auditorías todavía contiene algunos defectos sutiles pero importantes. En particular, el informe de datos (árbol hash) en el sitio web de la institución no ofrece ninguna garantía de

usuarios, ya que un intercambio malicioso podría publicar diferentes estados / saldos para diferentes grupos de usuarios, o cambiar retroactivamente el estado. Por lo tanto, es fundamental publicar estos datos a través de un canal de transmisión seguro, por ejemplo, la cadena de bloques de Bitcoin.

La privacidad es una barrera de entrada para la adopción de un sistema de auditoría automatizado / abierto. Si bien se han logrado algunos avances hacia una mejor privacidad, todavía no existe una solución perfecta. Además, para construir un espacio de responsabilidad preciso verificado por el usuario, estos usuarios deberán informar los saldos de las cuentas con las direcciones de intercambio y Bitcoin. Es probable que algunos usuarios no reporten esta información independientemente del incentivo, por lo tanto, brindar privacidad criptográficamente segura mientras se obtiene el objetivo de reporte es primordial.

Serie temporal: el hash del árbol Merkle es una instantánea única de la base de datos en un solo momento. No tener una serie de tiempo algo continua de la base de datos abre importantes vectores de ataque. Además, también se necesitaría una serie temporal de información reportada por el usuario para reconstruir el historial de cualquier incidente de fraude reportado.

Terceros de confianza: todas las auditorías de intercambio actuales se han basado en algún tercero de confianza "de buena reputación" para realizar algún tipo de verificación. En la auditoría de Coinbase [7], ese era Andreas Antonopoulos, en la auditoría de Kraken [8], ese era Stefan Thomas. Si absolutamente debemos confiar en un tercero confiable, entonces algunos estándares y procedimientos de auditoría deberían garantizar que esta debilidad se fortalezca.

## Limitaciones de los sistemas Fiatpegging existentes

Aquí hay una lista de algunos de los inconvenientes y limitaciones comunes de los sistemas de fiatpegging existentes.

* Los sistemas se basan en software de código cerrado, que se ejecuta en bases de datos privadas y centralizadas, fundamentalmente no diferentes de Paypal o cualquier otro sistema de almacenamiento, transferencia o comercio de activos institucionales o minoristas de mercado masivo existente.
* Sistemas descentralizados que se basan en cadenas de bloques de altcoins que no han sido sometidas a pruebas de estrés, desarrolladas o revisadas tan de cerca como otras cadenas de bloques, como Bitcoin.
* Procesos de vinculación que se basan en la cobertura de metaactivos derivados, la teoría del mercado eficiente o la garantía del activo subyacente, en los que pueden existir liquidez, transferibilidad, seguridad y otros problemas.
* Falta de transparencia y auditorías para el custodio, ya sea criptográfico, fiduciario o en relación con sus propios libros de contabilidad internos (lo mismo que las bases de datos centralizadas y de código cerrado).
* Dependencia de sistemas bancarios heredados y terceros confiables (propietarios de cuentas bancarias) como mecanismo de transferencia y liquidación de activos de reserva.

## Ejemplos de riesgo de mercado

En el método de colateralización, el riesgo de mercado existe porque el precio del activo que se utiliza como garantía puede moverse en una dirección adversa al precio del activo que está respaldando / vinculando. Esto haría que el valor total de la garantía fuera menor que el valor total del activo emitido y haría que el sistema fuera insolvente. Este riesgo se mitiga cuando el custodio cierra la posición antes de que esto suceda; es decir, cuando el precio de la garantía es igual al precio del activo fijo, la garantía se liquida (se vende en el mercado abierto) y la posición se cierra. Un gran enfoque, con mérito, y utilizado en muchos mercados líquidos en los mercados bancarios y financieros tradicionales. Sin embargo, como vimos en la crisis financiera mundial, Pueden surgir situaciones en las que la aceleración de tales eventos provoque una “crisis de liquidez” y, por lo tanto, la garantía no pueda liquidarse con la suficiente rapidez para cumplir con las obligaciones comerciales, lo que posteriormente generará pérdidas. Dado que los mercados de criptomonedas son tan pequeños y volátiles, este tipo de evento es mucho más probable. Además, el enfoque general adolece de otras limitaciones de liquidez y precios, ya que debe haber una cantidad suficiente de usuarios que presenten garantías para que exista la creación de activos fijos en primer lugar.

En el enfoque de derivados, el precio del activo se fija mediante el ingreso de una de varias estrategias de derivados, tales como: estrategias de swap, estrategias de opciones cubiertas y desnudas, diversas estrategias de futuros y forwards. Cada estrategia tiene sus propias fortalezas y debilidades, cuya discusión no abordaremos aquí. En resumen, cada uno de estos procesos de vinculación tienen características de "riesgo de mercado" similares al método de garantía mencionado anteriormente. Cabe señalar que los dos métodos no son mutuamente excluyentes y, a menudo, se combinan en una función específica de negociación, cobertura o gestión de riesgos en las instituciones financieras del sistema heredado.

Finalmente, comprenda que creemos que alguna combinación de los enfoques anteriores puede convertirse en un proceso seguro, confiable y generalmente libre de riesgos para respaldar / vincular activos; sin embargo, en este momento, esta no es una dirección que creemos que sea factible de tomar para garantizar liquidez y estabilidad de precios. Además, creemos que siempre existirá un enfoque basado en reservas y que complementará estos otros enfoques a medida que la industria entera crezca. A medida que continúen los avances en la tecnología, evaluaremos e incorporaremos cualquier beneficio disponible mientras mantenemos la garantía de 100% de canje.

## Legal y Cumplimiento

Tether Limited ("Tether") es una sociedad limitada constituida de conformidad con la Ordenanza de empresas de Hong Kong. Es propiedad total de Tether Holdings Limited, una empresa comercial de las Islas Vírgenes Británicas constituida de conformidad con la Ley de Compañías Comerciales de las Islas Vírgenes Británicas de 2004.

Tether está registrada como una empresa de servicios monetarios en la Red de ejecución de delitos financieros del

Departamento del Tesoro de EE. UU. (Número de registro MSB 31000058542968). Tether está estableciendo una relación con una institución financiera de EE. UU. Con el fin de brindar un mejor servicio a los usuarios de Tether en los Estados Unidos.

Tether está celebrando un acuerdo de agencia principal con RenRenBee Limited ("RenRenBee"). RenRenBee tiene licencia como Operador de Servicios Monetarios por el Departamento de Aduanas e Impuestos Especiales de Hong Kong (Licencia No.

130901265). De conformidad con el acuerdo, RenRenBee proporcionará trabajo de cumplimiento antilavado de dinero y procedimientos de diligencia debida del cliente como agente de Tether como principal.

A través de estas y otras medidas, Tether está llevando a cabo procedimientos de diligencia debida, mantenimiento de registros y presentación de informes de acuerdo con la ley de los EE. UU. Y con la Ordenanza contra el lavado de dinero y el financiamiento del terrorismo (instituciones financieras) de Hong Kong.

Tether Limited actualmente tiene cuentas con Cathay Bank y Hwatai Bank en Taiwán, quienes conocen y confían en que el modelo comercial de Tether es aceptable.

Estos bancos están satisfechos con nuestros procesos y también satisfechos de que nuestro negocio opere de acuerdo con las regulaciones bancarias extraterritoriales de Taiwán, ya que se les había solicitado a todos los bancos que verificaran esto con su propia oficina central, legal y de cumplimiento antes de abrir cuentas (también a pedido nuestro ). Nuestro objetivo desde el principio fue tener una operación compatible y brindar el máximo nivel de comodidad a nuestros socios bancarios aquí. Además, estos bancos tienen y están trabajando con otras empresas basadas en Bitcoin.

# Glosario de términos

**Moneda digital:** Según lo definido por <http://en.wikipedia.org/wiki/Digital_currency>

**Criptomoneda o moneda digital descentralizada:** cualquier tipo de criptomoneda que sea de código abierto, criptográficamente seguro y utilice un libro mayor distribuido. Ver:<http://en.wikipedia.org/wiki/Cryptocurrency>

**Moneda del mundo real, moneda fiduciaria o moneda nacional / soberana:** todos los tipos de moneda que no sean criptomonedas como se definen anteriormente.

**Sistema de criptomonedas:** Una colección de software y procesos creados principalmente para permitir la existencia de una criptomoneda.

**Sistema financiero heredado:** cualquier sistema financiero que no sea un sistema de criptomonedas.

**Tokens digitales respaldados por servicios públicos, también conocidos como Dapps:** Un token digital descentralizado cuyo valor se deriva de la utilidad de su aplicación en lugar de ser un simple sistema de transferencia de valor.

**Criptomoneda respaldada por activos / vinculada:** Cualquier criptomoneda cuyo precio esté vinculado a un activo del mundo real,

es decir, no es una criptomoneda "respaldada por servicios públicos".

**Tether (s):** una sola unidad (o varias unidades) de criptomoneda fijada por moneda emitida por Tether Limited

**TetherUSD o tUSD:** una sola unidad de cryptoUSD emitida por Tether Limited

**TUSD:** cantidad colectiva de tUSD en circulación en cualquier momento.

**Sistema de anclaje:** colectivamente se refiere a todos los procesos y tecnologías que permiten que existan ataduras

**Prueba de reservas:** El proceso mediante el cual el emisor de cualquier token digital descentralizado respaldado por activos, demuestra criptográficamente / matemáticamente que todos los tokens que se han emitido están completamente reservados y respaldados por el activo subyacente.

# Referencias

1. [https://www.thefinancialist.com/wp](http://www.thefinancialist.com/wp)content / uploads / 2012/10 / 2012GlobalWealthReport.pdf
2. https://bitcoin.org/bitcoin.pdf [[3] http://www.deloitte.com/assets/Dcom](http://www.deloitte.com/assets/Dcom)Estados Unidos / Activos% 20 locales / Documentos / FSI / us\_fsi\_BitcointheNe wGoldRush\_031814.pdf
3. https://github.com/mastercoinMSC/spec
4. <http://unenumerated.blogspot.com/2005/12/bit>gold.html
5. https://iwilcox.me.uk/2014/provingbitcoinreserves
6. <http://antonopoulos.com/2014/02/25/coinbase>revisión/
7. <http://www.coindesk.com/krakens>auditprovesholds100bitcoinsreserve /