Blockchain y Tecnología de Contabilidad Distribuida (DLT)

<https://documents1.worldbank.org/curated/en/177911513714062215/pdf/122140-WP-PUBLIC-Distributed-Ledger-Technology-and-Blockchain-Fintech-Notes.pdf>



**Blockchain** es un tipo de **libro mayor distribuido**. Los libros de contabilidad distribuidos utilizan computadoras independientes (denominadas nodos) para registrar, compartir y sincronizar transacciones en sus respectivos libros de contabilidad electrónicos (en lugar de mantener los datos centralizados como en un libro mayor tradicional). Blockchain organiza los datos en bloques, que se encadenan en un modo de solo apéndice.

* Blockchain / DLT son el bloque de construcción de "internet del valor" y permiten el registro de interacciones y la transferencia de "valor" de igual a igual, sin necesidad de una entidad de coordinación central. "Valor" se refiere a cualquier registro de propiedad de activos, por ejemplo, dinero, valores, títulos de propiedad, y también la propiedad de información específica como identidad, información de salud y otros datos personales.

**La tecnología de contabilidad distribuida** (DLT) podría cambiar fundamentalmente el sector financiero, haciéndolo más eficiente, resistente y confiable.

* Esto podría abordar los desafíos persistentes en el sector financiero y cambiar el papel de las partes interesadas del sector financiero. DLT también tiene el potencial de transformar varios otros sectores, como la fabricación, los sistemas de gestión financiera del gobierno y la energía limpia.
* **Dado que esta tecnología aún es incipiente, el Grupo del Banco Mundial no tiene recomendaciones generales sobre su uso para el desarrollo internacional.** Estamos en diálogo con organismos de normalización, gobiernos, bancos centrales y otras partes interesadas para monitorear, investigar y probar aplicaciones basadas en blockchain y DLT.
* Sin embargo, esperar soluciones DLT "perfectas" podría significar perder la oportunidad de ayudar a darle forma. Para comprender cómo DLT puede abordar los desafíos en el sector financiero se requiere tanto investigación como aplicaciones y pilotos de la vida real.
* También requiere resolver problemas de protección del consumidor, preocupaciones de integridad financiera, velocidad de transacciones, huella ambiental, problemas legales, regulatorios y tecnológicos que surgen con el advenimiento de nuevas tecnologías.
* Las aplicaciones DLT probablemente serán incrementales y probablemente reemplazarán primero los procesos y actividades que aún son manuales e ineficientes. (Como el mantenimiento de datos de referencia en los sistemas de pago y liquidación, la financiación del comercio, los préstamos sindicados y el seguimiento de la procedencia de los productos agrícolas y los productos básicos, su posterior venta o uso como garantía de financiación).
* Eventualmente, DLT podría aumentar la eficiencia y reducir los costos de remesas, y potencialmente mejorar el acceso a la financiación para las poblaciones no bancarizadas, que actualmente están fuera del sistema financiero tradicional.
* Mensajes basados en la nota fintech del GBM sobre [tecnología de contabilidad distribuida y Blockchain,](https://documents.worldbank.org/en/publication/documents-reports/documentdetail/177911513714062215/distributed-ledger-technology-dlt-and-blockchain) publicada en diciembre de 2017.

Última actualización: Abr 12, 2018

Tecnología de contabilidad distribuida (DLT) y Blockchain



Glosario

La terminología en este campo todavía está evolucionando y las definiciones universales aún no se han formalizado. A los efectos de esta nota, se utilizan las siguientes definiciones.

**Un token** es una representación de un activo digital. Por lo general, no tiene valor intrínseco, pero está vinculado a un activo subyacente, que podría ser cualquier cosa de valor.

**La tecnología de contabilidad distribuida** se refiere a un enfoque novedoso y de rápida evolución para registrar y compartir datos entre múltiples almacenes de datos (o libros de contabilidad). Esta tecnología permite que las transacciones y los datos se registren, compartan y sincronicen a través de una red distribuida de diferentes participantes de la red.

**Una 'blockchain'** es un tipo particular de estructura de datos utilizada en algunos libros de contabilidad distribuidos que almacena y transmite datos en paquetes llamados "bloques" que están conectados entre sí en una 'cadena' digital. Las cadenas de bloques emplean métodos criptográficos y algorítmicos para registrar y sincronizar datos a través de una red de manera inmutable.

**Los libros de contabilidad distribuidos (DL)** son una implementación específica de la categoría más amplia de "libros de contabilidad compartidos", que simplemente se definen como un registro compartido de datos entre diferentes partes.

**Un libro mayor compartido** puede ser un solo libro mayor con permisos en capas o un libro mayor distribuido, que consiste en múltiples libros de contabilidad mantenidos por una red distribuida de nodos, como se definió anteriormente.

**Las DL se clasifican como autorizadas o sin permiso,** dependiendo de si los participantes de la red (nodos) necesitan permiso de cualquier entidad para realizar cambios en el libro mayor.

**Los libros de contabilidad distribuidos se clasifican como públicos o privados** dependiendo de si cualquier persona puede acceder a los libros de contabilidad o solo a los nodos participantes en la red.

**Las monedas digitales** son representaciones digitales de valor que están denominadas en su propia unidad de cuenta, distinta del dinero electrónico, que es simplemente un mecanismo de pago digital, que representa y denomina en dinero fiduciario.

**Las criptomonedas** son un subconjunto de monedas digitales que se basan en técnicas criptográficas para lograr el consenso, por ejemplo, Bitcoin y Ether.

**Los nodos** son participantes de la red en una red de contabilidad distribuida.

**La criptografía de clave pública** es un esquema de cifrado asimétrico que utiliza dos conjuntos de claves: una clave pública que se difunde ampliamente y una clave privada que solo es conocida por el propietario. La criptografía de clave pública se puede utilizar para crear firmas digitales y se utiliza en una amplia gama de aplicaciones, como el protocolo de Internet HTTPS, para la autenticación en aplicaciones críticas y también en tarjetas de pago basadas en chips.

**Abreviaturas y acrónimos**

AML/CFT Lucha contra el blanqueo de capitales/financiación del terrorismo

CDD Customer Due Dilegence

DLT Tecnología de contabilidad distribuida

DL Libro mayor distribuido

KYC Conozca a su cliente

FSP Proveedor de servicios financieros

SWIFT Sociedad para las Telecomunicaciones Financieras Interbancarias Mundiales

SME Pequeña y Mediana Empresa

B2B De empresa a empresa

B2P De empresa a igual

P2P Peer-to-Peer

WBG Grupo del Banco Mundial

Visión general

El sector financiero está experimentando actualmente una importante transformación, provocada por el rápido desarrollo y difusión de las nuevas tecnologías. La confluencia de "finanzas" y "tecnología" a menudo se conoce como "Fintech", que generalmente describe empresas o innovaciones que emplean nuevas tecnologías para mejorar o innovar los servicios financieros. Los desarrollos de 'Fintech' se observan en todas las áreas del sector financiero, incluidos los pagos y las infraestructuras financieras, los préstamos al consumidor y las pymes, los seguros, la gestión de inversiones y la financiación de riesgo. Esta nota sobre la tecnología de contabilidad distribuida (DLT) y las cadenas de bloques es parte de una serie de notas cortas que exploran las nuevas tendencias y desarrollos en Fintech y analizan su relevancia potencial para las actividades del GBM. Las próximas notas de esta serie cubrirán los préstamos en el mercado, 'InsureTech' y otros temas.

Esta nota describe los mecanismos, orígenes y características clave de la TRD; la diferencia entre TRD «pública» y «privada»; las principales ventajas, desafíos y riesgos de la tecnología; ejemplos pertinentes de aplicaciones de TRD (con especial atención a las aplicaciones del sector financiero); y una breve reseña de las actividades de los gobiernos, las organizaciones multilaterales y otras partes interesadas en este espacio. Por último, en esta nota se proponen los próximos pasos para que el Banco Mundial estudie y evalúe las esferas en las que la TRD podría integrarse en las operaciones del sector financiero del Banco Mundial.

**¿Qué es DLT? ¿Qué es una cadena de bloques?**

DLT se refiere a un enfoque novedoso y de rápida evolución para registrar y compartir datos entre múltiples almacenes de datos (o libros de contabilidad). Esta tecnología permite que las transacciones y los datos se registren, compartan y sincronicen a través de una red distribuida de diferentes participantes de la red.

Una 'blockchain' es un tipo particular de estructura de datos utilizada en algunos libros de contabilidad distribuidos que almacena y transmite datos en paquetes llamados 'bloques' que están conectados entre sí en una 'cadena' digital. Las cadenas de bloques emplean métodos criptográficos y algorítmicos para registrar y sincronizar datos a través de una red de manera inmutable.

Por ejemplo, una nueva transacción de moneda digital se registraría y transmitiría a una red en un bloque de datos, que primero es validado por los miembros de la red y luego vinculado a una cadena existente de bloques de manera solo anexa, produciendo así una cadena de bloques. A medida que la cadena lineal crece cuando se agregan nuevos bloques, los bloques anteriores no pueden ser alterados retrospectivamente por ningún miembro de la red (consulte la figura 4 para obtener una representación gráfica de la estructura de una cadena de bloques).

Tenga en cuenta que no todos los libros de contabilidad distribuidos emplean necesariamente la tecnología blockchain y, a la inversa, la tecnología blockchain podría emplearse en diferentes contextos.

Resumen ejecutivo

DLT basado en blockchain, que se aplicó por primera vez como la tecnología subyacente de la criptomoneda Bitcoin, tiene una variedad de aplicaciones potenciales más allá del estrecho ámbito de las monedas digitales y las criptomonedas. Por ejemplo, DLT podría tener aplicaciones en pagos transfronterizos, infraestructura de mercados financieros en los mercados de valores y en registros de garantías.

Pero las aplicaciones potenciales de DLT no se limitan al sector financiero. DLT se está explorando actualmente para facilitar los productos de identidad digital (como la identificación nacional, los registros de nacimiento, matrimonio y defunción) o construir registros descentralizados a prueba de manipulaciones del flujo de productos básicos y materiales a través de una cadena de suministro mediante el uso de partes interesadas de confianza para validar los flujos y movimientos.

Los defensores de DLT generalmente destacan una serie de ventajas potenciales sobre los libros de contabilidad centralizados tradicionales y otros tipos de libros de contabilidad compartidos, incluida la descentralización y la desintermediación, una mayor transparencia y una auditabilidad más fácil, ganancias en velocidad y eficiencia, reducciones de costos y automatización y programabilidad.

Dicho esto, la tecnología aún está evolucionando y puede plantear nuevos riesgos y desafíos, muchos de los cuales aún no se han resuelto. Los desafíos tecnológicos, legales y regulatorios más comúnmente citados relacionados con DLT se refieren a la escalabilidad, interoperabilidad, seguridad operativa y ciberseguridad, verificación de identidad, privacidad de datos, disputas de transacciones y marcos de recursos, y desafíos en el desarrollo de un marco legal y regulatorio para las implementaciones de DLT, que puede traer cambios fundamentales en los roles y responsabilidades de las partes interesadas en el sector financiero.

Otro desafío, particularmente relevante para el área de las infraestructuras de los mercados financieros, son los costos sustanciales relacionados con la migración de los sistemas de TI existentes de larga data, los arreglos operativos y los marcos institucionales a la infraestructura basada en LA DLT. Muchos observadores de la industria señalan que, debido a estos desafíos, las aplicaciones DLT probablemente comenzarán en áreas sin muchas inversiones heredadas en automatización, como la financiación del comercio y los préstamos sindicados en el sector financiero.

Los sistemas de contabilidad distribuida pueden ser abiertos/sin permiso o con permiso, y existen diferencias fundamentales entre estos dos tipos, que conducen a perfiles de riesgo muy diferentes. En los sistemas sin permiso, no hay un propietario central que controle el acceso a la red. Todo lo que se necesita para unirse a la red y agregar transacciones al libro mayor es un servidor informático con el software relevante. En los sistemas con permisos, los miembros de la red son preseleccionados por un propietario o un administrador del libro mayor que controla el acceso a la red y hace cumplir las reglas del libro mayor.

Hay ventajas y desventajas para ambos tipos, que varían significativamente con diferentes casos de uso. Por ejemplo, los sistemas autorizados son mejores para resolver problemas relacionados con la verificación de identidad y la privacidad de los datos, pero requieren una entidad central que regule el acceso, lo que crea un objetivo potencial para los ciberataques. Los sistemas autorizados también pueden encajar más fácilmente en los marcos legales y reglamentarios y los arreglos institucionales existentes. Sin embargo, hasta cierto punto, los DL autorizados eliminan los beneficios clave de la innovación más crítica de DLT. Esto se debe a que la seguridad y la integridad del sistema de los DL abiertos y sin permiso se logran a través de soluciones criptográficas y algorítmicas que aseguran que los participantes anónimos de la red estén incentivados para hacer cumplir la precisión del libro mayor, sin la necesidad de barreras de entrada o confianza entre los participantes.

La mayor parte de los recursos de I+ D para DLT se dedican actualmente a mejorar la infraestructura y los procesos financieros, y existe un potencial significativo para que esta inversión sea aprovechada por las organizaciones de desarrollo en beneficio de los países en desarrollo.

Dicho esto, la tecnología aún se encuentra en una etapa temprana de desarrollo y todavía hay un largo camino por recorrer antes de que se pueda realizar todo su potencial, especialmente con respecto a cuestiones relacionadas con la privacidad, la seguridad, la escalabilidad, la interoperabilidad y las cuestiones legales y reglamentarias. Por lo tanto, el Grupo del Banco Mundial aún no está en condiciones de emitir ninguna recomendación general sobre la usabilidad, independientemente de los contextos específicos.

Sin embargo, esperar soluciones DLT "perfectas" no es necesariamente un enfoque ideal para las organizaciones de desarrollo. Dado el potencial de la TRD para estructurar soluciones a los desafíos del desarrollo en el sector financiero y más allá, el GBM puede seguir de cerca y dar forma a los desarrollos y, cuando sea apropiado, fomentar su adopción segura, manteniendo al mismo tiempo la neutralidad institucional hacia los actores del sector privado. Comprender el verdadero potencial de DLT para los objetivos de desarrollo requiere no solo investigación, sino también aplicaciones y ensayos de la vida real.

Además de desarrollar la tecnología en sí, el empleo de DLT para ayudar a alcanzar los objetivos de desarrollo en el sector financiero requiere el desarrollo y la promoción activa de elementos críticos que la acompañan. Entre ellas cabe destacar: el diseño de la interfaz de aplicación fácil de usar, la educación y la capacidad financieras, un marco sólido de protección del consumidor financiero, la interoperabilidad con los servicios e infraestructura financieros y de pago tradicionales; y una supervisión eficaz.

1 ¿Qué es la tecnología de contabilidad distribuida (DLT) y cómo funciona?

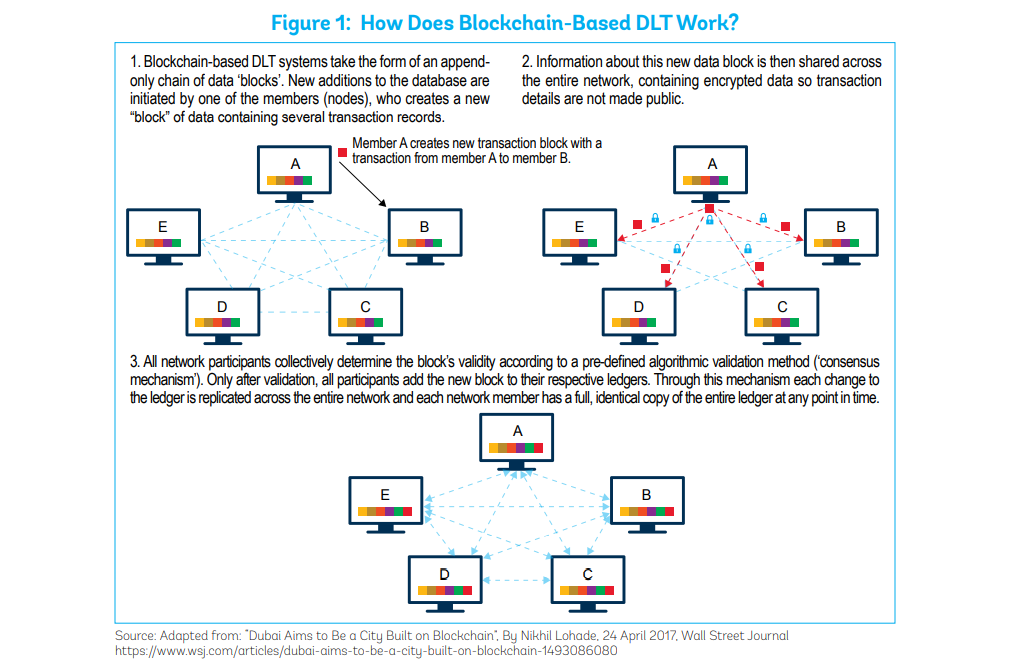
DLT viene de la mano de varias tecnologías peer-to-peer (P2P) habilitadas por Internet, como el correo electrónico, el intercambio de música u otros archivos multimedia, y la telefonía por Internet. Sin embargo, las transferencias de propiedad de activos basadas en Internet han sido durante mucho tiempo esquivas, ya que esto requiere garantizar que un activo solo sea transferido por su verdadero propietario y garantizar que el activo no se pueda transferir más de una vez, es decir, sin doble gasto. El activo en cuestión podría ser cualquier cosa de valor.

En 2008, un documento histórico escrito por una persona aún no identificada utilizando el seudónimo Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System", propuso un enfoque novedoso de transferir "fondos" en forma de "Bitcoin" de manera P2P. La tecnología subyacente para Bitcoin descrita en el documento de Nakamoto se denominó Blockchain, que se refiere a una forma particular de organizar y almacenar información y transacciones. Posteriormente, se idearon otras formas de organizar la información y las transacciones para las transferencias de activos de una manera P2P, lo que llevó al término "Tecnología de contabilidad distribuida" (DLT) para referirse a la categoría más amplia de tecnologías.

DLT se refiere a un enfoque novedoso y de rápida evolución para registrar y compartir datos a través de múltiples almacenes de datos (libros de contabilidad), cada uno de los cuales tiene exactamente los mismos registros de datos y son mantenidos y controlados colectivamente por una red distribuida de servidores informáticos, que se denominan nodos. Una forma de pensar acerca de DLT es que es simplemente una base de datos distribuida con ciertas propiedades específicas (ver sección 3). Blockchain, un tipo particular de DLT, utiliza métodos criptográficos y algorítmicos para crear y verificar una estructura de datos en continuo crecimiento, solo de apéndice, que toma la forma de una cadena de los llamados "bloques de transacciones", la cadena de bloques, que cumple la función de un libro mayor.

Las nuevas adiciones a la base de datos son iniciadas por uno de los miembros (nodos), que crea un nuevo "bloque" de datos, por ejemplo, que contiene varios registros de transacciones. La información sobre este nuevo bloque de datos se comparte en toda la red, conteniendo datos cifrados para que los detalles de la transacción no se hagan públicos, y todos los participantes de la red determinen colectivamente la validez del bloque de acuerdo con un método de validación algorítmica predefinido («mecanismo de consenso»). Solo después de la validación, todos los participantes agregan el nuevo bloque a sus respectivos libros de contabilidad. A través de este mecanismo, cada cambio en el libro mayor se replica en toda la red y cada miembro de la red tiene una copia completa e idéntica de todo el libro mayor en cualquier momento. Este enfoque se puede utilizar para registrar transacciones en cualquier activo que pueda representarse en forma digital. La transacción podría ser un cambio en el atributo del activo o una transferencia de propiedad. Véase la figura 1.

Dos atributos principales de una infraestructura basada en DLT son: (i) la capacidad de almacenar, registrar e intercambiar "información" en forma digital entre diferentes contrapartes interesadas sin la necesidad de un guardián de registros central (es decir, peer-to-peer) y sin la necesidad de confianza entre las contrapartes; y, (ii) garantizar que no haya un "doble gasto" (es decir, el mismo activo o token no se puede enviar a múltiples partes).



**Terminología**

La terminología en este campo todavía está evolucionando y las definiciones universales aún no se han formalizado. Blockchain es un mecanismo particular o estructura de datos que emplea criptografía y algoritmos para registrar datos de manera inmutable. No todos los libros de contabilidad distribuidos emplean blockchains y, por el contrario, la tecnología blockchain podría usarse en otros contextos. Sin embargo, los términos "tecnología blockchain" y "tecnología de contabilidad distribuida" se usan comúnmente indistintamente.

Los "libros de contabilidad distribuidos" (DL) son una implementación específica de la categoría más amplia de "libros de contabilidad compartidos", que simplemente se definen como un registro compartido de datos entre diferentes partes. Un libro mayor compartido puede ser un solo libro mayor con permisos en capas o un libro mayor distribuido que consiste en múltiples libros de contabilidad mantenidos por una red distribuida de nodos, como se definió anteriormente. En este documento, estamos usando comúnmente el término libros de contabilidad distribuidos (DL), y específicamente usamos el término blockchain solo cuando nos referimos a LOS DL que usan una estructura de datos de blockchain.

Las DL se clasifican como autorizadas o sin permiso, dependiendo de si los participantes de la red (nodos) necesitan permiso de cualquier entidad para realizar cambios en el libro mayor. Los libros de contabilidad distribuidos se clasifican como públicos o privados dependiendo de si cualquier persona puede acceder a los libros de contabilidad o solo a los nodos participantes en la red.

2. ¿Cómo se relacionan DLT y Blockchain con las monedas digitales?

DLT ha estado estrechamente vinculado a las monedas digitales desde su inicio porque, como se señaló anteriormente, se inventó como la tecnología subyacente de la criptomoneda Bitcoin. El inventor de Bitcoin, escribiendo bajo el seudónimo de Satoshi Nakamoto, describió la tecnología en un libro blanco de 2008 como un "sistema de pago electrónico basado en pruebas criptográficas en lugar de confianza, que permite a dos partes dispuestas a realizar transacciones directamente entre sí sin la necesidad de un tercero de confianza".1 Nakamoto no ha sido identificado hasta el día de hoy, después de haber borrado toda su presencia en línea en 2011.

**Terminología**

Las definiciones en este campo todavía están evolucionando y las definiciones universales aún no han surgido. A los efectos de esta nota, las monedas digitales son representaciones digitales de valor que están denominadas en su propia unidad de cuenta, distintas del dinero electrónico, que es simplemente un mecanismo de pago digital, que representa y denomina en dinero fiduciario. Un informe de CPMI de 2015, "Monedas digitales", señaló tres características específicas de las monedas digitales no fiduciarias: 1) No están respaldadas por ningún activo subyacente, tienen un valor intrínseco cero y no representan un pasivo en ninguna institución. 2) Se intercambian a través de libros de contabilidad distribuidos sin confianza entre los socios y sin mantenimiento de registros centrales. 3) Como resultado de las dos características anteriores, no se basan en acuerdos institucionales específicos o intermediarios para los intercambios entre pares. Las criptomonedas son un subconjunto de monedas digitales que se basan en técnicas criptográficas para lograr el consenso, por ejemplo, Bitcoin y Ether. Tenga en cuenta que las monedas fiduciarias digitales, emitidas por los bancos centrales, también pueden usar libros de contabilidad centralizados.

La tecnología Blockchain para Bitcoin fue diseñada para resolver el problema del "doble gasto", que inhibió una evolución completa del dinero en el mundo digital, similar a las transformaciones digitales de la música, los correos electrónicos y los documentos. Antes de Bitcoin, para evitar el doble gasto, se necesitaba una parte central de confianza para validar las transacciones para garantizar la propiedad de la cuenta y el saldo. La innovación crítica de DLT en el contexto de las monedas digitales es que proporciona una solución criptográfica para proporcionar seguridad y proteger la integridad del sistema en un libro mayor descentralizado que es mantenido por una red de participantes anónimos sin necesidad de confianza en una o más instituciones.

La cadena de bloques de Bitcoin fue diseñada con la intención específica de crear una moneda digital que esté libre del control del gobierno y anonimice las identidades de los participantes de su red. "A diferencia de HTML o HTTP, Bitcoin fue un proyecto ideológico desde el principio",2 profundamente arraigado en la ideología anti censura de la comunidad en línea de la que surgió, conocidos como "cypherpunks", que defienden una corriente radical de tecno-libertarismo. Si bien Bitcoin fue la aplicación original de DLT, y la primera en alcanzar la escala, la tecnología tiene una gran cantidad de aplicaciones potenciales mucho más allá de las monedas digitales (ver sección 7).

El anonimato ofrecido para realizar transacciones rápidamente en línea atrajo la atención de los delincuentes y Bitcoin se ha utilizado para financiar actividades ilícitas. Sin embargo, a pesar de que las identidades de los socios que realizan transacciones pueden ser anónimas, todas las transacciones de Bitcoin se registran en un libro mayor distribuido que es visible para el público y es posible asociar las transacciones de Bitcoin con entidades anónimas específicas. (Esta es la razón por la cual el término "seudónimo" se usa a menudo en el contexto de Bitcoin). El anonimato proporcionado por Bitcoin se puede comparar con el anonimato proporcionado por una dirección de correo electrónico. Todas las transacciones de Bitcoin contienen una dirección de billetera del remitente y el receptor, que puede considerarse como seudónimos, similares a las direcciones de correo electrónico.

Si bien se conocen las direcciones vinculadas a la transacción, los propietarios detrás de las direcciones pueden permanecer anónimos, de manera similar a enviar un mensaje a una dirección de correo electrónico. Los funcionarios encargados de hacer cumplir la ley tuvieron éxito en vincular identidades del mundo real con la entidad anónima en la red Bitcoin en el caso de los arrestos relacionados con Silk Road3, un mercado negro en línea para actividades ilícitas, incluida la venta de drogas ilegales.

Varias características de la cadena de bloques de Bitcoin han dañado la reputación de la criptomoneda y causan preocupaciones para los gobiernos y los reguladores. Esto incluye la falta de regulación de muchos de los intercambios de bitcoin y el aumento del malware informático ransomware que exige un rescate pagado en bitcoin para proporcionar anonimato. Otro tema de preocupación es el problema de pérdida de datos de bitcoin: si pierde su clave privada de su billetera, pierde todo su dinero (consulte la sección 3 para obtener una explicación de la "clave privada"). La banca tradicional y centralizada es mucho más resistente a esto. Todas estas son características específicas de las aplicaciones e industrias que rodean a bitcoin, en lugar de las características de la infraestructura DLT. Hasta la fecha, no ha habido ningún problema de integridad grave que surja de la cadena de bloques central de bitcoin en sí.

A pesar de sus orígenes anti-autoridad, DLT también se puede utilizar para crear monedas fiduciarias digitales emitidas por los bancos centrales (consulte la sección 7 para obtener más detalles sobre las aplicaciones de DLT).

3. Características clave de DLT

Los libros de contabilidad individuales con permisos en capas que son compartidos, accedidos y editados por una red de participantes examinados han existido durante mucho tiempo, pero el concepto de un libro mayor descentralizado, distribuido e inmutable se realizó por primera vez a través de DLT. A continuación, se describen tres características de DLT que generalmente se consideran clave para la tecnología: la naturaleza distribuida del libro mayor, el mecanismo de consenso y los mecanismos criptográficos.

También debe enfatizarse que DLT no es una tecnología única y bien definida. En cambio, una pluralidad de blockchains y libros de contabilidad distribuidos están activos o están en desarrollo hoy en día y sus diseños y configuraciones precisas varían según los objetivos de los creadores y el propósito y la etapa de desarrollo del DL.

Naturaleza distribuida del libro mayor

El mantenimiento de registros siempre ha sido un proceso centralizado que requiere confianza en el encargado del registro. La innovación más importante de DLT es que el control sobre el libro mayor no recae en ninguna entidad, sino en varios o todos los participantes de la red, dependiendo del tipo de DL. Esto lo diferencia de otros desarrollos tecnológicos como la computación en la nube o la replicación de datos, que se utilizan comúnmente en los libros de contabilidad compartidos existentes. De hecho, esto significa que, en un DL, ninguna entidad en la red puede modificar las entradas de datos pasadas en los libros mayores y ninguna entidad puede aprobar nuevas adiciones al libro mayor. En su lugar, se utiliza un mecanismo de consenso descentralizado predefinido (ver más abajo) para validar nuevas entradas de datos que se agregan a la cadena de bloques y, por lo tanto, formar nuevas entradas en el libro mayor. Existe, en cualquier momento, solo una versión del libro mayor y cada participante de la red posee una copia completa y actualizada de todo el libro mayor. Cada adición local al libro mayor por parte de un participante de la red se propaga a todos los nodos. Una vez aceptada la validación, la nueva transacción se agrega a todos los libros de contabilidad respectivos para garantizar la coherencia de los datos en toda la red.

Esta característica distribuida de DLT permite a los participantes interesados en una red peer-to-peer registrar colectivamente datos verificados en sus respectivos libros de contabilidad, por ejemplo, registros de transacciones, sin depender de una parte central de confianza. La eliminación de la parte central puede aumentar la velocidad y potencialmente eliminar los costos e ineficiencias asociadas con el mantenimiento del libro mayor y las conciliaciones posteriores. Es importante destacar que también puede mejorar la seguridad porque ya no hay un solo punto de ataque en toda la red. Para corromper el libro mayor, un atacante tiene que obtener el control sobre la mayoría de los servidores de la red; corromper a uno o varios participantes no compromete la integridad del sistema.

Sin embargo, los riesgos de seguridad en las capas de aplicación de software construidas sobre el DL pueden convertirse en superficies de ataque adicionales. Las debilidades en esta capa pueden causar pérdidas a los usuarios de un sistema DL, incluso cuando la tecnología central permanece segura y protegida. Ejemplos notables que causaron daños financieros y de reputación fueron los hackeos de Mt. Gox en Japón y Bitfinex.4

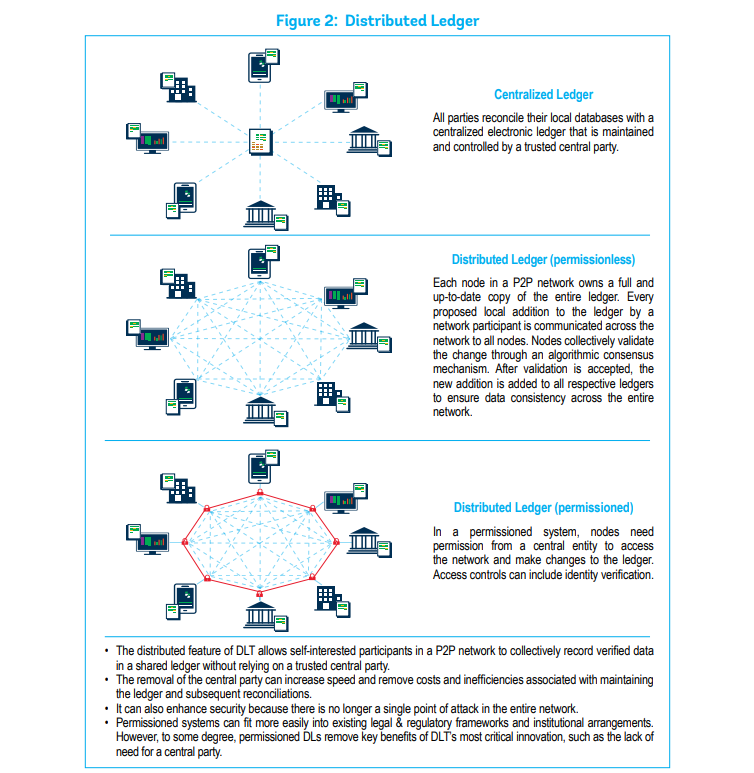
Mecanismo de consenso

La naturaleza distribuida del DL requiere que los participantes en la red («nodos») lleguen a un consenso sobre la validez de las nuevas entradas de datos siguiendo un conjunto de reglas. Esto se logra a través de un mecanismo de consenso que se especifica en el diseño algorítmico del DL y puede variar según su naturaleza, propósito y activo subyacente. En un DL, en general cualquiera de los nodos puede proponer una adición de una nueva transacción al libro mayor, sin embargo, hay implementaciones que proponen roles especializados para los nodos donde solo algunos nodos pueden proponer una adición. Es necesario un mecanismo de consenso para establecer si una transacción en particular es legítima o no, utilizando un método de validación criptográfica específico predefinido designado para este DL. El mecanismo de consenso también es importante para manejar conflictos entre múltiples entradas competidoras simultáneas, por ejemplo, diferentes transacciones en el mismo activo son propuestas por diferentes nodos. Este mecanismo garantiza la correcta secuenciación de las transacciones y evita la adquisición por parte de malos actores (en el caso de un DL sin permiso). El mecanismo de consenso y la secuencia protegen contra el problema del doble gasto antes mencionado.

La cadena de bloques de Bitcoin utiliza la "prueba de trabajo" para establecer un consenso en una red descentralizada global, un concepto que se desarrolló por primera vez como una medida contra el spam. Para agregar un nuevo bloque a la cadena, lo que significa agregar un nuevo conjunto de entradas de datos al libro mayor, se requiere un protocolo de "prueba de trabajo". Este es un desafío computacional que es difícil de resolver (en términos de potencia de cálculo y tiempo de procesamiento) pero fácil de verificar. La prueba de trabajo se genera ejecutando repetidamente algoritmos hash criptográficos unidireccionales hasta que se produce una cadena de números que satisface una condición predefinida pero arbitraria, específicamente en la cadena de bloques de Bitcoin este es un cierto número de ceros iniciales y el proceso de generación de prueba de trabajo se llama "minería". Resolver este rompecabezas de "prueba de trabajo" es un proceso computacionalmente difícil y no hay atajos, lo que significa que cualquier nodo individual en la red solo tiene una posibilidad diminutamente pequeña de generar la prueba de trabajo requerida sin gastar una gran cantidad de costosos recursos informáticos. El sistema Bitcoin está calibrado de tal manera que se produce una prueba de trabajo válida cada 10 minutos y, en caso de que se creen dos exactamente al mismo tiempo, el protocolo con la puntuación de dificultad más alta se acepta como válido ("la cadena más larga"). Cada "minero" que produce una prueba de trabajo válida en la red de Bitcoin recibe Bitcoins como recompensa (algo así como una tarifa de transacción), que sirve como un incentivo económico para mantener la integridad del sistema. Por lo tanto, el gran tamaño de un sistema abierto y sin permiso es clave para su seguridad. La seguridad de la red está directamente relacionada con tener un gran número de nodos en el sistema que están incentivados para validar nuevos cambios en el libro mayor con precisión y establecer un consenso en toda la red para garantizar la consistencia de los datos.

La "prueba de trabajo" inflige un costo computacional significativo a los participantes de la red para mantener el DL (es decir, crear nuevos bloques de datos y agregar estos bloques a la cadena de bloques), que solo se requiere en sistemas con participantes desconfiados. Las estimaciones sugieren que los mineros de Bitcoin actualmente consumen electricidad equivalente al consumo de electricidad de Irlanda5 y podrían alcanzar el nivel de Dinamarca para 20206 (suponiendo que el mecanismo de consenso de Bitcoin permanezca sin cambios). Según una estimación, si la red Bitcoin escalara a los niveles de uso de los sistemas de pago existentes como Visa y MasterCard, la electricidad requerida excedería el consumo mundial actual de electricidad. Sin embargo, este problema es más pronunciado para la cadena de bloques de Bitcoin. El sistema DLT utilizado por Ether, una moneda digital recientemente introducida por Ethereum, requiere significativamente menos recursos informáticos y el mecanismo de consenso es mucho más rápido.

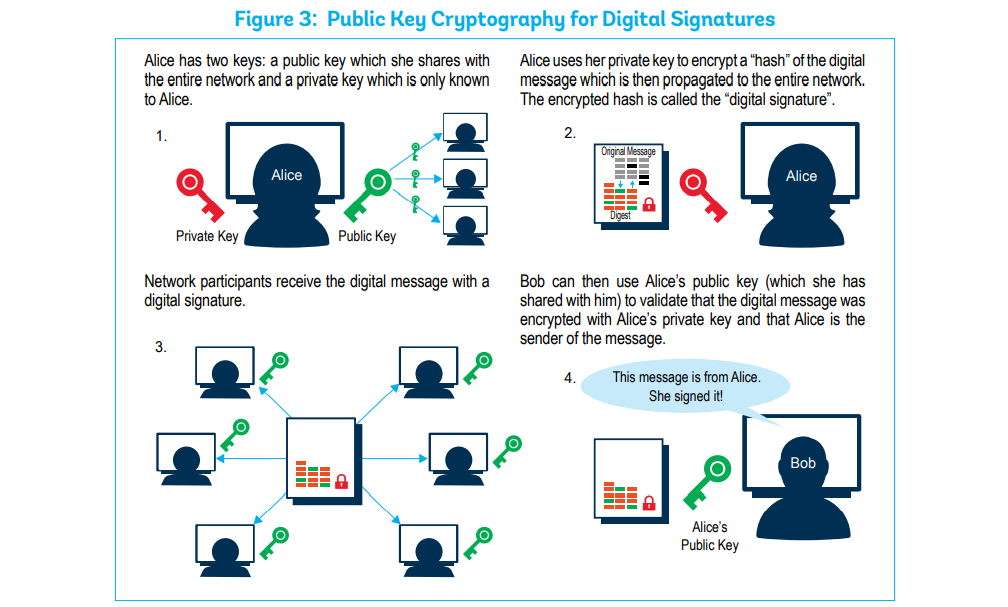
Las cadenas de bloques autorizadas no suelen requerir "pruebas de trabajo" difíciles como mecanismo de consenso para verificar las transacciones porque los participantes de la red son preseleccionados y confiables. También hay otros mecanismos de consenso, por ejemplo, la prueba de participación que recompensa la antigüedad sobre la potencia de cálculo y requiere una prueba de propiedad de un determinado activo.



Funciones hash criptográficas y firmas digitales

La criptografía es el núcleo de DLT, en particular para las implementaciones de blockchain. Cada nueva entrada de datos, es decir, un registro de transacción, es "hashed", lo que significa que se aplica una función hash criptográfica al mensaje original. Un hash toma datos de cualquier tamaño de entrada y calcula una huella digital similar a una huella digital humana que no se puede cambiar a menos que se cambien los datos en sí. La salida hash es un llamado "resumen" de una longitud definida que parece aleatoria y no está relacionada con la entrada original, pero de hecho es determinista. Esto significa que para una entrada original solo es posible un hash y es muy improbable que otra entrada tenga el mismo valor hash.7 El hashing también aplica una marca de tiempo al mensaje original. Estos hashes de transacción se recopilan en un "bloque de transacciones" que puede contener cualquier número de transacciones, pero que generalmente tiene un tamaño total limitado.8 El hash permite la detección de cualquier manipulación de los datos de transacción subyacentes, ya que cuando se vuelve a calcular un hash, producirá un hash diferente al hash generado originalmente.

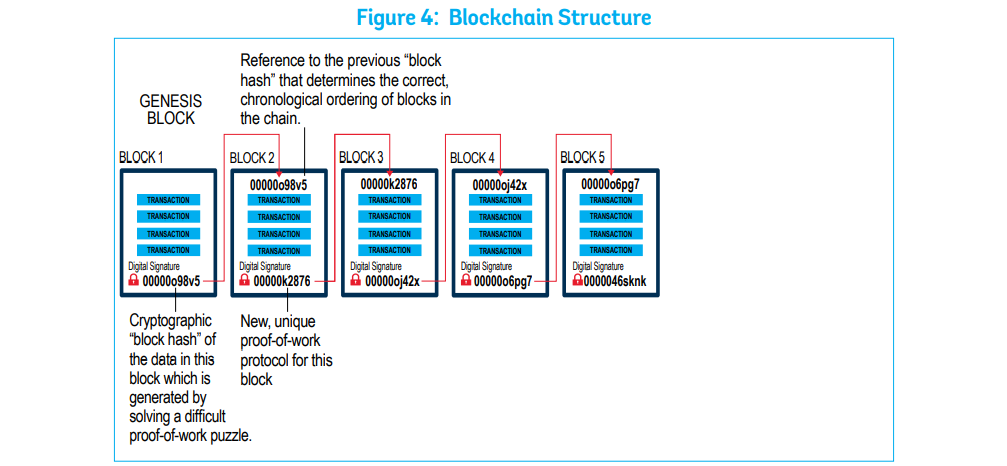
Los bloques se firman con una firma digital, que vincula al remitente al contenido del bloque, similar a una firma en un contrato. DLT utiliza la "criptografía de clave pública" para las firmas digitales, que es un método común que se utiliza en una amplia gama de otras aplicaciones, como el protocolo de Internet HTTPS, para la autenticación en aplicaciones críticas y también en tarjetas de pago basadas en chips. Las firmas digitales son ampliamente aceptadas como equivalentes a las firmas físicas por ley en muchos países. Cada participante de la red tiene una clave privada, que se utiliza para firmar mensajes digitales y solo es conocida por el usuario individual, y una clave pública que es de conocimiento público y se utiliza para validar la identidad del remitente de un mensaje digital. La clave pública también se utiliza para identificar al destinatario.



Estos tres conceptos ayudan a explicar los fundamentos de la TRD. El proceso por el cual los datos se registran en un libro mayor distribuido basado en blockchain es mediante la formación de una cadena de "bloques de transacciones" en orden cronológico que contiene resúmenes hash de las transacciones (mensajes digitales) que se agregarán al libro mayor, una prueba de trabajo (o una salida de mecanismo de consenso diferente) y una firma digital del hash por la clave privada del remitente. y claves públicas del remitente y del destinatario previsto de la transacción. Esta cadena comienza con la primera entrada en el libro mayor (el 'bloque génesis') y cada bloque anexado contiene información hash del bloque anterior, estableciendo el orden cronológico de la cadena.

La Figura 4 a continuación muestra un ejemplo de una estructura de blockchain: El último bloque (bloque 5) se agregó a una blockchain existente (bloques 1-4, el bloque 1 es el 'bloque génesis'). Cada bloque contiene un protocolo único de "prueba de trabajo", una referencia al bloque anterior que determina el orden cronológico correcto de los bloques, una serie de resúmenes hash de información de transacción que no se pueden cambiar y una firma digital. En esta figura, el bloque 5 representa la adición más reciente a esta cadena de bloques que actualiza el libro mayor.

Una vez que se agrega un nuevo bloque a la cadena a través de un mecanismo de consenso especificado, la cadena no se puede cambiar retroactivamente y los bloques no se pueden eliminar o modificar sin volver a hacer el protocolo de prueba de trabajo para cada bloque. Esto significa que a medida que la cadena crece en longitud, esto se vuelve progresivamente más difícil porque todos los nodos compiten constantemente por resolver rompecabezas de prueba de trabajo y agregar nuevos bloques a la cadena. Al hacer esto, solo consideran la cadena de bloques de transacciones que refleja la mayor cantidad de trabajo computacional. Cada adición exitosa a la cadena se transmite a toda la red y todos los nodos tienen una copia actualizada de toda la cadena de bloques.



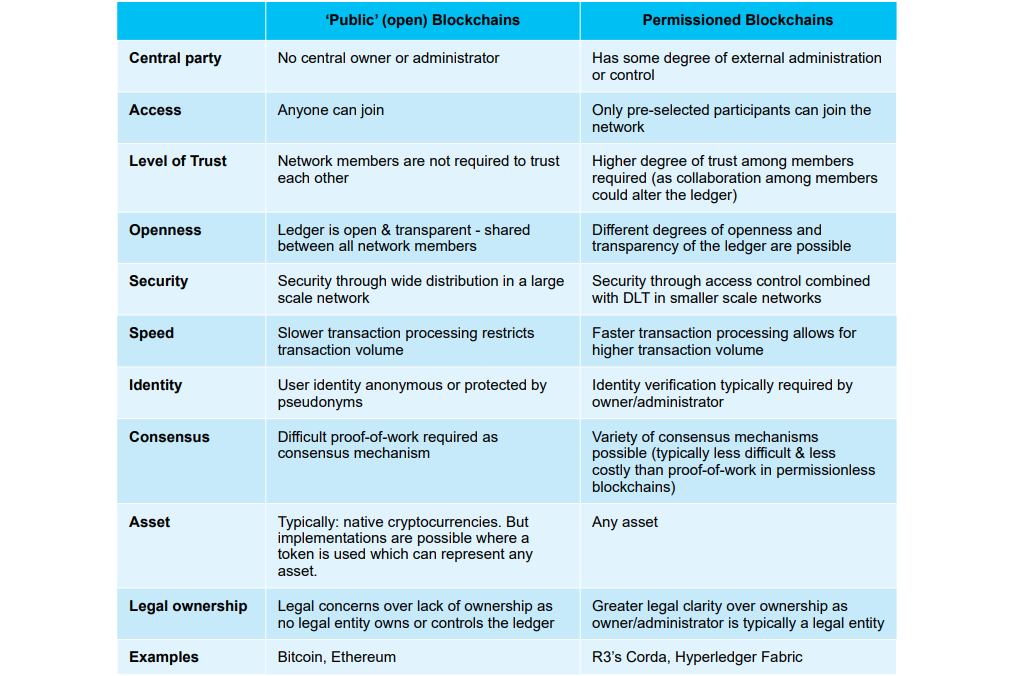
4. Libros de contabilidad distribuidos abiertos / sin permiso frente a libros de contabilidad distribuidos con permiso

Los sistemas de contabilidad distribuida pueden ser abiertos (sin permiso) o con permiso, y existen diferencias fundamentales entre los dos. Bitcoin y Ethereum son los ejemplos más destacados de cadenas de bloques completamente sin permiso, donde los participantes de la red pueden unirse o abandonar la red a voluntad, sin ser preaprobados o examinados por ninguna entidad. Todo lo que se necesita para unirse a la red y agregar transacciones al libro mayor es una computadora con el software relevante. No hay un propietario central y se distribuyen copias idénticas del libro mayor a todos los participantes de la red.

En los DL autorizados, los miembros son preseleccionados por alguien, un propietario o un administrador del libro mayor, que controla el acceso a la red y establece las reglas del libro mayor. Esto resuelve una serie de preocupaciones que los gobiernos y los reguladores tienen sobre los libros de contabilidad distribuidos sin permiso, como la verificación de identidad de los miembros de la red, a quién licenciar y regular, y la propiedad legal del libro mayor. Pero también reduce una ventaja principal de las cadenas de bloques sin permiso: la capacidad de funcionar sin la necesidad de que una sola entidad desempeñe un papel de coordinación, lo que necesariamente requiere que otros participantes confíen en esta entidad. Sin embargo, incluso en DL autorizados, en general no hay necesidad de un administrador para la ejecución de transacciones.

Los DL autorizados, que regulan el acceso a la red, generalmente no requieren una prueba de trabajo que requiera mucha potencia de cálculo para verificar las transacciones, sino que se basan en diferentes reglas algorítmicas para establecer un consenso entre los miembros. En los DL sin permiso, que no regulan el acceso a la red, no hay ningún requisito de confianza entre los participantes y, por lo tanto, se utiliza una prueba de trabajo complicada para generar consenso sobre las entradas del libro mayor. Por el contrario, en el caso de un DL autorizado, el administrador tiene la responsabilidad de garantizar que los participantes en el DL sean confiables. En los DL autorizados, cualquier nodo puede proponer una adición de una transacción, que luego se replica en otros nodos, potencialmente incluso sin ningún mecanismo de consenso.

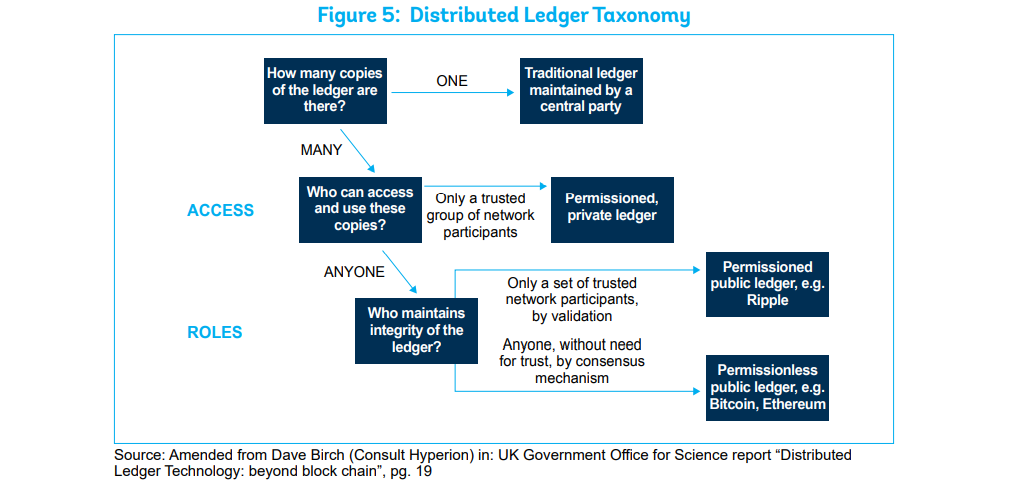
En realidad, esta no es una categorización binaria, pero el grado de apertura y descentralización de los sistemas de contabilidad distribuida cae en un espectro con cadenas de bloques totalmente abiertas y sin permiso, como Bitcoin en un extremo del espectro y cadenas de bloques autorizadas alojadas por entidades privadas en el otro, y las características precisas varían de una plataforma a otra. Los arreglos DLT se pueden definir en términos de diferentes dimensiones: acceso a la red (abierto /cerrado) vs. roles dentro de la red (restringido / sin restricciones) – ver taxonomía en la Figura 5. Muchas empresas emplean un enfoque híbrido en el que proporcionan la tecnología para que las redes autorizadas se construyan en la infraestructura pública de blockchain y, por lo tanto, restringen los roles en un sistema DLT con acceso abierto.9



Algunos actores de la industria hacen una distinción entre libros de contabilidad distribuidos públicos / privados (en términos de acceso) y autorizados / sin permiso (en términos de roles). Ripple, por ejemplo, tiene un libro mayor autorizado, pero los datos son validados por todos los participantes, por lo tanto, su sistema puede considerarse un libro mayor público y autorizado. Un DLT autorizado donde los datos son validados solo por un conjunto de participantes se consideraría un libro mayor privado y autorizado.

Con toda probabilidad, tanto las DL abiertas como las DL autorizadas tendrán aplicaciones útiles. La tecnología aún se encuentra en una etapa temprana de desarrollo y hay diferentes escenarios futuros: algunos creen que la industria eventualmente convergerá a una cadena de bloques pública mundial (similar a una Internet mundial) y muchas cadenas de bloques privadas diferentes (similares a muchas intranets privadas diferentes), mientras que otros creen que varias cadenas de bloques públicas continuarán existiendo lado a lado. Originalmente, Internet era un Internet de la información, que tenía el efecto de democratizar el acceso a la información. Un posible escenario futuro de la cadena de bloques podría ser un internet de valor, democratizando el acceso y el almacenamiento de activos digitales.

Desde el inicio de Bitcoin en 2009, han surgido más de 600 redes de contabilidad distribuida públicas y privadas diferentes, aunque solo unas pocas han logrado escala y una etapa de desarrollo más avanzada. La mayoría de las aplicaciones de blockchain (ver más abajo) se basan en blockchains públicas, predominantemente Bitcoin y Ethereum.



El Comité de Infraestructuras de Pago y mercado (CPMI) del Banco de Pagos Internacionales (BPI), en su reciente publicación sobre TRD, propuso un marco analítico para estudiar las aplicaciones de TRD en pagos y liquidaciones10. El marco propone los siguientes roles no exclusivos diferentes para un nodo:

• Administrador del sistema: Este rol implica decidir quién puede acceder a la red, mantener y administrar las reglas de resolución de disputas y realizar funciones notariales. Este rol no es necesario en un DLT sin permiso.

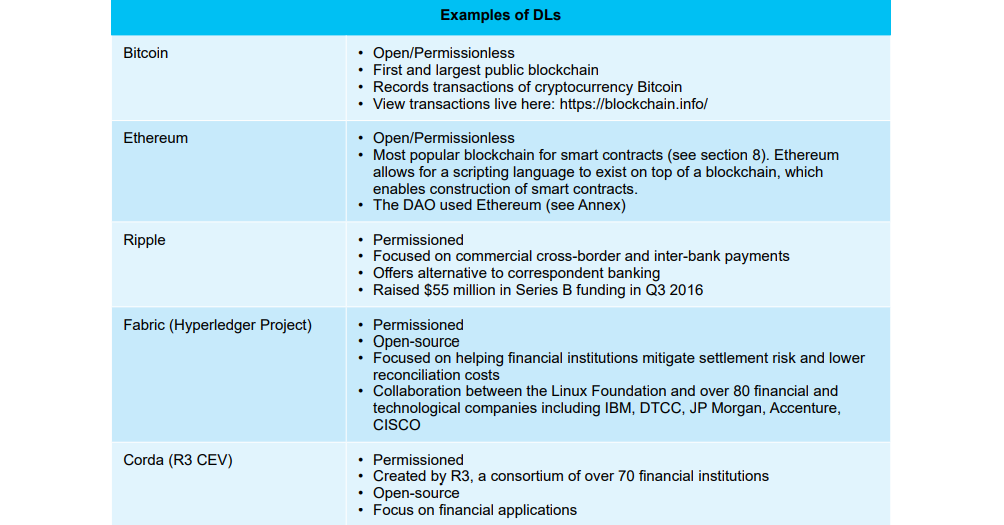
• Emisor de activos: Los nodos que desempeñan este papel son responsables de emitir nuevos "tokens" utilizados en la red. En la cadena de bloques de Bitcoin, no hay ninguna entidad que desempeñe este papel, el propio sistema crea nuevos bitcoins basados en reglas específicas. Un token es una representación de un activo digital. Por lo general, no tiene valor intrínseco, pero está vinculado al activo subyacente, que podría ser cualquier cosa de valor.

• Proponente: Este rol implica proponer nuevas transacciones para su inclusión en el libro mayor.

• Validador: Este rol implica validar solicitudes de adición de transacciones en el libro mayor. En un DL sin permiso, este rol es realizado por un mecanismo de consenso descentralizado.

• Auditor: Se permite ver el libro mayor pero no se le permite realizar cambios. Esto podría ser utilizado para realizar auditorías y también ser utilizado por reguladores y supervisores.

Las instituciones financieras, que son grandes usuarios de bases de datos, hasta ahora no muestran mucho interés en las cadenas de bloques abiertas y sin permiso debido a la dificultad de cumplir con los marcos regulatorios y de cumplimiento existentes. Otras preocupaciones del sector financiero se relacionan con el acceso abierto y la dificultad de la verificación de identidad en sistemas sin permiso, que a menudo están en desacuerdo con las prácticas comerciales existentes que requieren mantener la privacidad de las transacciones. Las instituciones financieras están realizando importantes inversiones en la investigación de DL autorizados como una solución tecnológica para reducir los costos y eliminar las fricciones en los pagos transfronterizos, la banca corresponsal, los procesos de compensación y liquidación, los préstamos sindicados y la financiación del comercio.



5. Ventajas clave de DLT

En el contexto adecuado, los libros de contabilidad distribuidos pueden tener potencialmente una serie de ventajas sobre los libros de contabilidad centralizados tradicionales y otros tipos de libros de contabilidad compartidos. Las ventajas potenciales más importantes de DLT se enumeran a continuación, aunque las generalizaciones son difíciles debido a la gran variedad de diseños y especificaciones que pueden tener las cadenas de bloques con permiso y sin permiso.

• Descentralización y desintermediación. DLT permite transferencias directas de valor digital o tokens entre dos contrapartes y mantenimiento de registros descentralizado, eliminando la necesidad de un intermediario o autoridad central que controle el libro mayor. Esto puede traducirse en menores costos, mejor escalabilidad y un tiempo de comercialización más rápido.

• Mayor transparencia y más facilidad de auditabilidad. Todos los miembros de la red tienen una copia completa del libro mayor distribuido (que se puede cifrar). Los cambios solo se pueden realizar cuando se establece un consenso y se propagan a través de toda la red en tiempo real. Esta característica, combinada con la falta de una autoridad central o la participación limitada de una autoridad central, tiene el potencial de reducir el fraude y eliminar los costos de reconciliación.

• Automatización y programabilidad. DLT permite programar condiciones preacordadas que se ejecutan automáticamente una vez que se mantienen ciertas condiciones. Esto se conoce como "contratos inteligentes" (consulte la sección 8), por ejemplo, facturas que se pagan solas cuando llega un envío o certificados de acciones que envían automáticamente dividendos a los propietarios o programas de efectivo por trabajo que pagan a los beneficiarios una vez que se completa el trabajo contratado. Los contratos inteligentes también se pueden realizar en los sistemas de contabilidad centralizados tradicionales, pero el diseño de los sistemas de contabilidad centralizados requiere que tales acciones se implementen solo después de que las partes interesadas hayan acordado la transacción subyacente registrada en el sistema central, lo que en algunos contextos puede llevar más de un día. Por el contrario, en un DL, las contrapartes por definición acuerdan el momento en que se completa la transacción, ya que ambas tienen el mismo registro de la transacción. Además, el resultado de la ejecución del "contrato inteligente" en sí mismo tomará tiempo adicional para propagarse y reconciliarse en un sistema de contabilidad tradicional.

• Inmutabilidad y verificabilidad. DLT puede proporcionar una pista de auditoría inmutable y verificable de las transacciones de cualquier activo digital o físico. Si bien en la mayoría de los casos, la inmutabilidad es deseable, puede crear problemas relacionados con los mecanismos de recurso si el sistema falla. Sin embargo, la inmutabilidad del libro mayor no significa que no se pueda crear una transacción compensatoria para anular una transacción impugnada. Esto está en línea con el funcionamiento de la resolución de disputas, por ejemplo, en los sistemas de tarjetas de pago. Sin embargo, el registro original aún permanecería en este caso. Dos investigadores del MIT han presentado recientemente una patente para una solución criptográfica que permitiría a un administrador "desbloquear" unidades en una cadena de bloques y editarlas, aunque esto es muy controvertido ya que la inmutabilidad se considera una de las ventajas centrales de las primeras cadenas de bloques.

• Ganancias en velocidad y eficiencia. DLT ofrece el potencial de aumentar la velocidad y reducir las ineficiencias al eliminar o reducir las fricciones en las transacciones o en los procesos de compensación y liquidación al eliminar intermediarios y automatizar los procesos.

• Reducción de costos. DLT ofrece el potencial de reducciones significativas de costos debido a la eliminación de la necesidad de reconciliación, ya que los sistemas basados en DLT por definición contienen la "verdad compartida" y, por lo tanto, no hay necesidad de reconciliar una versión de "verdad" con la de las contrapartes. Las fuentes adicionales de reducción de costos podrían ser menores costos de infraestructura para mantener un DL, así como reducciones en fricciones y fraudes. Según algunas estimaciones, la tecnología de contabilidad distribuida podría ahorrarle a la industria financiera por sí sola alrededor de $ 15-20 mil millones por año.11

• Mayor resiliencia de ciberseguridad. DLT tiene el potencial de proporcionar un sistema más resistente que las bases de datos centralizadas tradicionales y ofrecer una mejor protección contra diferentes tipos de ataques cibernéticos debido a su naturaleza distribuida, que elimina el único punto de ataque.

Fundamentalmente, DLT es un enfoque de diseño alternativo que permite un modelo comercial y operativo descentralizado en comparación con los enfoques de diseño centralizados existentes que se pueden utilizar para fines similares. Esto hace posible una mayor automatización, un procesamiento más rápido y un mayor potencial de escalabilidad. En contextos específicos, un enfoque de diseño basado en DLT puede proporcionar muchos de los beneficios discutidos anteriormente. El siguiente ejemplo de un registro de garantías ayuda a ilustrar la diferencia entre los enfoques basados en DLT y los enfoques de diseño alternativos.

El establecimiento de un registro de garantías utilizando enfoques centralizados existentes requiere que una entidad central configure una plataforma dedicada, establezca criterios de membresía y establezca reglas y procedimientos. Todas las transacciones relacionadas con la garantía se procesan en esta plataforma y todas las acciones comerciales son activadas por la plataforma centralizada. Esta plataforma se crea utilizando aplicaciones de software estandarizadas desarrolladas para la necesidad específica del negocio o desarrolladas a medida.

Un enfoque basado en DLT, por el contrario, presenta transacciones que involucran garantías que se intercambian de igual a igual, con condiciones integradas y predeterminadas, como la fecha de liberación y las reglas relacionadas con la falta de pago de un préstamo subyacente. No es necesario configurar ningún sistema centralizado y las reglas comerciales relacionadas con una garantía en particular se pueden adaptar en función del acuerdo específico entre contrapartes.

En un DL autorizado, puede haber un administrador que establezca criterios de participación e incorpore nuevos participantes. Pero a diferencia de la entidad centralizada en una implementación tradicional, el papel del administrador en un sistema basado en DLT sería muy mínimo. Las acciones empresariales pueden estar impulsadas por eventos y pueden activarse sin necesidad de intervenciones externas adicionales. La creación de un nuevo registro de garantías mediante un enfoque basado en DLT puede ser potencialmente más rápida y escalable, ya que los recursos necesarios a nivel de administrador son muy mínimos, la carga de procesamiento se distribuye entre todos los participantes y la lógica empresarial para las transacciones de garantía se puede adaptar y personalizar en función de las necesidades específicas de las contrapartes.

6. Desafíos y riesgos relacionados con la TRD

La tecnología aún está evolucionando y muchos problemas regulatorios y legales aún no se han resuelto. Por el momento, todavía no está claro qué aplicaciones DLT realmente ofrecerán ventajas sobre las soluciones tecnológicas existentes y es probable que las ganancias generales sean incrementales en lugar de radicales a mediano plazo. Además, existen varios desafíos relacionados con la migración de la infraestructura financiera y de pagos existente a DLT, como las contrapartes centrales y los sistemas de liquidación de valores, debido a la importante coordinación y colaboración requerida dentro del ecosistema. Los desafíos tecnológicos, legales y regulatorios más comúnmente citados relacionados con DLT se enumeran a continuación:

Retos tecnológicos

• Borde sangrante/Falta de madurez. DLT se encuentra en una etapa temprana de desarrollo y todavía existen serias preocupaciones sobre la robustez y la resistencia de DLT, especialmente para transacciones de gran volumen, la disponibilidad de aplicaciones estandarizadas de hardware y software, y también una amplia oferta de profesionales calificados. Sin embargo, los grandes actores de TI tradicionales como IBM y Microsoft, así como los actores del sector financiero como Visa y MasterCard han comenzado a desarrollar productos y servicios DLT, que eventualmente podrían proporcionar el mismo nivel de confianza que ofrecen los sistemas de TI tradicionales en la actualidad.

• Escalabilidad y velocidad de transacción. Las iteraciones actuales de libros de contabilidad distribuidos sin permiso enfrentan problemas relacionados con la escalabilidad de las cadenas de bloques, tanto en términos de volumen de transacciones como de velocidad de verificaciones. Las cadenas de bloques sin permiso existentes tienen una velocidad de transacción limitada. Bitcoin, por ejemplo, solo puede procesar entre 4-7 transacciones por segundo debido a la limitación del tamaño del bloque a un megabyte, un tema de controversia en la comunidad bitcoin. (El tamaño del bloque podría aumentarse, pero los bloques más grandes tardarían más en propagarse a través de la red, lo que empeoraría los riesgos de bifurcación). Este problema, sin embargo, podría resolverse con el tiempo y es más pronunciado en el sistema Bitcoin. Otros sistemas DLT sin permiso como Ethereum informan un mayor rendimiento de transacciones. Además, las cadenas de bloques autorizadas tienen una mayor capacidad y pueden procesar mayores volúmenes de transacciones, pero estas carecen de escala global y se producen a expensas de una plataforma más centralizada y menos transparente, lo que elimina muchos de los beneficios de la naturaleza distribuida y abierta de los sistemas DLT públicos.

• Interoperabilidad e Integración. Los diferentes sistemas DLT deberán ser interoperables con otros libros de contabilidad e integrados con los sistemas existentes si se quieren introducir a escala en el sistema financiero. Además, el costo de integrar DLT en infraestructuras financieras como los sistemas de pago y liquidación requerirá coordinación y colaboración en toda la industria y requerirá gastos significativos. Se están realizando esfuerzos para desarrollar marcos de DL específicamente para el sector financiero, en particular el marco CORDA de R3 CEV y el proyecto Fabric by Hyperledger. Estos dos marcos son un esfuerzo para abordar los requisitos específicos planteados por los profesionales de la industria en áreas tales como:

* permitir transacciones entre contrapartes de igual a igual; necesidad de validar la identidad de las contrapartes;
* limitar la visibilidad de las transacciones sobre la base de la necesidad de conocer; la necesidad de que los reguladores tengan acceso a las transacciones;
* garantizar la equivalencia entre los contratos inteligentes y la prosa jurídica real;
* utilizar las herramientas de software estándar de la industria existentes;
* interfaces entre múltiples libros de contabilidad distribuidos; y
* apoyar una variedad de modelos de consenso, incluido un enfoque de solo hacer que las contrapartes que realizan transacciones participen en el consenso.

Estos marcos, en esencia, exploran el uso de enfoques de DL dentro de las prácticas comerciales y regulatorias prevalecientes. CORDA se centra específicamente en el sector financiero, mientras que Hyperledger busca proporcionar un marco más amplio con aplicaciones iniciales propuestas para el sector financiero y para la gestión de la cadena de suministro.

• Ciberseguridad. Ningún software es inmune a las vulnerabilidades técnicas. Las estadísticas muestran que hay alrededor de 15-50 errores por cada 1000 líneas de código.12 Fallas como el ataque DAO en la cadena de bloques Ethereum han demostrado que cualquier debilidad en los contratos inteligentes puede ser explotada para crear efectos no deseados. La seguridad de la red se basa en la naturaleza distribuida del libro mayor y la presunción de que los atacantes no tendrán éxito en cambiar los algoritmos que determinan las reglas básicas del sistema DLT. Un posible ataque a un libro mayor distribuido sin permiso con mecanismo de consenso es el "ataque del 51%" donde un mal actor se hace cargo del 51% de la potencia informática de una red y puede mentir efectivamente a la red manipulando el consenso. La suposición de que ninguna entidad, ahora o en el futuro, podría controlar más de la mitad de la potencia de cálculo de todos los servidores en una cadena de bloques en particular depende críticamente de la solidez de la red subyacente. Las aplicaciones que se escriben para interactuar con estos DL deben revisarse y monitorearse cuidadosamente. ¿Qué sucede si un atacante obtiene acceso a un sistema sin permisos, obtiene credenciales de identidad y, a continuación, logra multiplicarse hasta que la mayoría de los participantes de la red estén bajo el control del atacante? Además, ¿qué pasa si los desarrollos futuros en computación como la computación cuántica hacen que los métodos criptográficos de hoy sean triviales de romper? Los incidentes recientes de ataques estándar de denegación de servicio distribuido (DDoS) en múltiples nodos de Ethereum muestran que las técnicas tradicionales de ciberataque también se pueden aplicar con éxito a los sistemas DLT (véase el anexo). A pesar de estas preocupaciones, vale la pena señalar que, si bien se han producido hackeos exitosos en las interfaces de acceso a DLT, la tecnología en el núcleo de la cadena de bloques de Bitcoin y otros sistemas DLT, hasta el momento de la publicación, nunca se ha visto comprometida.

• Gobernanza. La ausencia de una infraestructura centralizada y una entidad central genera preocupaciones sobre la garantía de una gobernanza efectiva de la infraestructura general. Los casos de bifurcaciones de Ethereum (ver anexo) y las propuestas de cambios en el protocolo de Bitcoin muestran lo difícil y polémico que es tomar decisiones sobre cambios críticos en la infraestructura DLT. Históricamente, los reguladores del sector financiero se han basado en el establecimiento de acuerdos de gobernanza eficaces en las infraestructuras centrales y otras entidades reguladas. En el contexto de la TRD sin permiso, a menudo no está claro a quién se aplican los acuerdos de gobernanza. En el caso de la TRD autorizada, el administrador puede estar sujeto a acuerdos de gobernanza específicos, pero dependiendo de la naturaleza del sistema de TRD en particular, es posible que el administrador no disponga en todos los casos de los medios adecuados para hacer cumplir estos acuerdos entre los participantes de la red.

**Los fundamentos de las bifurcaciones**

Las bifurcaciones surgen cuando la cadena de bloques en un libro mayor distribuido se divide en dos caminos competitivos hacia adelante que luego deben resolverse. En muchos casos, las bifurcaciones pueden resolverse por sí solas. Por ejemplo, en el caso de Bitcoin, las bifurcaciones ocurren con bastante regularidad como un subproducto del mecanismo de consenso distribuido y se resuelven rápidamente cuando se agregan bloques adicionales a un bloque mientras que el otro bloque es abandonado por toda la red. En otros casos, las bifurcaciones que permanecen sin resolver pueden crear dos historias de blockchain en competencia.13 Existen tres tipos generales de bifurcaciones:

• Una bifurcación accidental puede ocurrir si las actualizaciones de la plataforma son accidentalmente incompatibles con el código anterior, lo que significa que los nodos comienzan a usar dos versiones diferentes del software hasta que se corrigen las incompatibilidades.14

• Una bifurcación suave es compatible con versiones anteriores, lo que significa que los bloques extraídos por los nodos que utilizan software actualizado se consideran válidos por los nodos que no han actualizado su software, pero lo contrario no es cierto: los bloques extraídos por los nodos no actualizados no son válidos para los nodos actualizados.15 (Esto alienta a todos los nodos a actualizar su software).

• Una bifurcación dura no es compatible con versiones anteriores, lo que significa que la actualización de software ha introducido una nueva regla que no se considera válida hasta que se actualiza un nodo. En este caso, si los miembros de la comunidad de nodos no están de acuerdo con las nuevas reglas, pueden optar por no actualizar al nuevo consenso y, en su lugar, continuar operando en la cadena de bloques original (previa a la bifurcación) utilizando el software antiguo, creando una divergencia de la criptomoneda (como en el caso de Ethereum Classic y Ethereum One o Core, consulte la sección 8 y el anexo). Bit Cash fue una bifurcación dura de Bitcoin en el verano de 2017, donde se aumentó el tamaño de bloque para permitir que se procesaran más transacciones.

Desafíos legales y regulatorios

• Investigación regulatoria y estándares de la industria: La investigación regulatoria y el desarrollo de estándares de la industria son necesarios, pero aún se encuentran en fases de desarrollo muy tempranas. Algunos reguladores de todo el mundo están estudiando activamente la tecnología, pero aún no han surgido marcos regulatorios específicos para DLT (ver sección 9 para más detalles sobre las actividades de los reguladores y organismos de normalización.

• Claridad legal sobre la propiedad y la jurisdicción: En los sistemas de pago y liquidación, existen preocupaciones específicas relacionadas con la forma en que se definiría el "punto de finalidad" de una transacción en un entorno de DL. Además, existen preocupaciones sobre los sistemas de DL transfronterizos en términos de la jurisdicción de los datos y transacciones subyacentes. Regular los sistemas de contabilidad distribuida abiertos y sin permiso es particularmente complicada ya que ninguna entidad legal tiene el control del libro mayor distribuido. La regulación de los libros de contabilidad privados y autorizados es comparativamente más directa, ya que generalmente hay un administrador o propietario del sistema que puede estar sujeto a regulación o se podrían utilizar los marcos regulatorios existentes para los acuerdos de subcontratación.

• KYC y CDD: Para su adopción en el sistema financiero, los sistemas DLT deberán cumplir con los requisitos de Conozca a su cliente (KYC) y Diligencia debida del cliente (CDD) en las regulaciones contra el lavado de dinero / lucha contra el financiamiento del terrorismo (ALD / CFT). La mayoría de los sistemas DLT sin permiso disfrazan la identidad de los miembros de la red mediante el uso de cifrado de clave pública, lo que dificultará el cumplimiento de las regulaciones AML / CFT existentes y permitiría transacciones con partes no examinadas. Muchos intercambios, por ejemplo, Coinbase, ofrecen tiempos de verificación y transacción más rápidos si los usuarios verifican más información para cumplir con los requisitos de KYC. Los sistemas DLT autorizados resuelven este problema porque el acceso a la red está controlado y la verificación de identidad del participante generalmente se requiere para el proceso de investigación, lo que podría requerir el cumplimiento de AML / CFT de todos los participantes de la red.

• Mecanismos de recurso: Como una característica definitoria de los libros de contabilidad distribuidos es la inmutabilidad, existen preocupaciones sobre cómo se resolverán las disputas de transacciones, en particular cómo se anularán las transacciones erróneas. Estas preocupaciones podrían abordarse mediante la integración de un marco de transacción de reversión, que tendrá el efecto de que se inicie una transacción separada para devolver los derechos sobre el activo digital subyacente al remitente original. (Como se señaló anteriormente, así es como funciona actualmente el proceso de resolución de disputas en los sistemas de tarjetas de pago y también en los sistemas de transferencia electrónica de fondos). Sin embargo, esto requeriría la existencia de algún marco normativo general que pueda invocarse para iniciar reversiones en circunstancias específicas. Sin un marco de este tipo, las transacciones incompletas o erróneas podrían dar lugar a problemas con el acceso a los fondos. Tradicionalmente, la administración de un marco normativo es gestionada por una entidad central, a menudo denominada «propietario de un sistema», por ejemplo, Visa, MasterCard, Union Pay y otras marcas de tarjetas de pago; o entidades como NACHA (Electronic Payments Association) para transferencias electrónicas de fondos en los Estados Unidos. En las DL autorizadas, el administrador del DL puede desempeñar este papel. En los DL sin permiso, se espera que este rol se automatice a través de contratos inteligentes. Otra preocupación se refiere a la cuestión de la responsabilidad por pérdidas derivadas de deficiencias en la TRD subyacente. Esta preocupación es más fácil de abordar en sistemas de DL con permiso que en sistemas sin permiso.

Otros desafíos

• Privacidad: En los libros de contabilidad sin permiso, como Bitcoin y Ethereum, todas las transacciones son abiertas y visibles para todos los miembros de la red, aunque se pueden cifrar y la identidad del usuario está oculta. En ciertos contextos, la identidad del participante se puede inferir en función de patrones de transacción u otros marcadores. Las DL autorizadas encuentran el mismo problema. Esta es una de las principales preocupaciones de la aplicación de DLT a las infraestructuras de los mercados financieros y es una de las cuestiones que CORDA y Fabric proponen abordar en su diseño.

• Costos ambientales. El uso de la prueba de trabajo como mecanismo de consenso crea una gran huella eléctrica a medida que se utilizan grandes cantidades de potencia de procesamiento informático para la "minería". (Esta preocupación se aplica principalmente a las cadenas de bloques sin permiso que utilizan protocolos de prueba de trabajo).

7. Aplicaciones de DLT

DLT tiene una amplia gama de aplicaciones potenciales más allá de las criptomonedas en el sector financiero y en una amplia variedad de otras industrias. Las aplicaciones que están escritas en una cadena de bloques pública utilizan la infraestructura de cadena de bloques, pero pueden ser distintas de la criptomoneda subyacente (por ejemplo, Bitcoin) o tener un valor nocional de criptomoneda etiquetado como una representación digital del activo subyacente.

Las dos tendencias más grandes en el desarrollo de aplicaciones blockchain son: 1) las nuevas empresas comerciales de Fintech están desarrollando aplicaciones digitales para una variedad de propósitos que utilizan la infraestructura pública de blockchain, principalmente Bitcoin y Ethereum; y 2) se están formando consorcios de la industria para investigar y desarrollar blockchain privados y autorizados para resolver soluciones empresariales específicas de la industria.

Existe un interés particularmente fuerte en DLT en el sector financiero: en el momento de la publicación, al menos la mitad de los 30 principales bancos estaban participando en pruebas de concepto de blockchain. R3 CEV, uno de los consorcios de I + D de blockchain más grandes para instituciones financieras, tenía más de 100 miembros, incluidos bancos, reguladores y asociaciones comerciales, mientras que el consorcio de código abierto Hyperledger incluía más de 170 organizaciones diversas.16 Las bolsas de valores de todo el mundo también están investigando y probando DLT para mejorar las plataformas de negociación de valores, incluidas NASDAQ, NYSE y LSE.17 DLT podría interrumpir la forma en que se emiten y negocian las acciones, y, a largo plazo, potencialmente reemplazar las plataformas de negociación existentes administradas por las bolsas de valores.

• En diciembre de 2015, la Comisión de Bolsa de Valores de los Estados Unidos aprobó un plan de Overstock.com para emitir acciones de la compañía a través de la cadena de bloques de Bitcoin.18

• El banco central y la bolsa de valores de Alemania "Deutsche Börse" construyeron un nuevo prototipo de blockchain para el comercio de activos digitales.19

• La Bolsa de Tokio e IBM están probando blockchain para registrar operaciones en mercados de bajas transacciones.

• La Bolsa de Valores de Australia y Digital Asset Holdings, una start-up, están explorando el uso de DLT para mejorar los procesos de compensación y liquidación.

• La bolsa de valores de Corea del Sur (Korea Exchange KRX) ha lanzado un mercado basado en blockchain para acciones de capital en startups, llamado Korea Startup Market (KSM) en asociación con Blocko, una start-up coreana de blockchain. El CEO de Blocko describió esto como el "primer ejemplo" de cómo blockchain podría usarse en el mercado de valores nacional de venta libre, lo que podría alentar desarrollos similares para otros activos.20

• La Depository Trust and Clearing Corporation (DTCC), el principal tenedor de libros que proporciona servicios de compensación y liquidación para transacciones de valores, se ha asociado con IBM y dos nuevas empresas de blockchain, Axoni y R3, para desarrollar un software basado en blockchain para el procesamiento posterior a la negociación de swaps de incumplimiento crediticio.21

DLT e inclusión financiera

Como se señaló anteriormente, la TRD tiene un potencial aparente para mejorar la eficiencia, la resiliencia y la fiabilidad de una variedad de actores e infraestructuras del sector financiero. Esto podría ayudar a abordar, o aliviar, algunos de los desafíos de larga data para mejorar el acceso a los servicios financieros.

A pesar de los fuertes avances en la expansión de la inclusión financiera, persisten las barreras para atraer a las poblaciones no bancarizadas y excluidas al sistema financiero. A corto y mediano plazo, es probable que muchos de los beneficios y las ganancias de eficiencia de la TRD sean cosechados por nuevas empresas e instituciones financieras en el mundo desarrollado. Pero a mediano y largo plazo, la TRD tiene potencial para expandir la inclusión financiera al abordar las siguientes barreras para el acceso a la financiación, en contextos específicos de países:

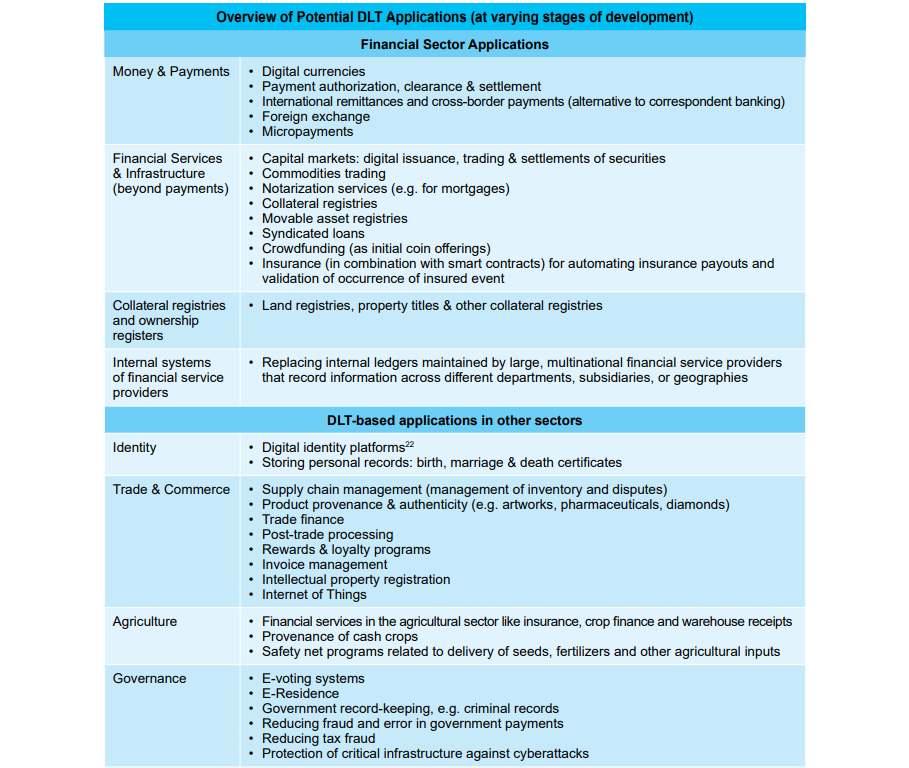
• Asequibilidad de los productos y servicios financieros

• Falta de sistemas de identificación robustos y verificables para KYC y otros requisitos de elegibilidad y diligencia debida

• Infraestructuras de pago y crédito deficientes

• Marcos incompletos de operaciones garantizadas y registros de garantías reales

• Impacto de la reducción del riesgo en las remesas internacionales



Ejemplos seleccionados de aplicaciones de DLT que podrían conducir a un mayor acceso financiero e inclusión para las poblaciones desatendidas son:

• Pagos y remesas transfronterizas

• Sistemas de Identidad Digital

• Registros de Activos

• Monedas digitales

Pagos y remesas transfronterizas

Las personas y las PYME de las economías en desarrollo se enfrentan a la incertidumbre, los altos costos y las largas demoras en la realización de pagos transfronterizos interbancarios, que actualmente se realizan normalmente a través de una red de bancos corresponsales o proveedores de transferencias de dinero, sin un sistema central de compensación. Los pagos transfronterizos a través de canales bancarios corresponsales están restringidos al horario comercial de los bancos y están sujetos a tarifas de transacción en tres puntos diferentes del proceso: tarifas cobradas por la institución de envío, tarifas cobradas por la institución receptora y tarifas cobradas por la transferencia interbancaria transfronteriza (esto podría ser a través de varios intermediarios, cada uno cobrando su propia tarifa).

Los actores no bancarios, como los operadores de transferencia de dinero (MTO) como Western Union y otros, han desarrollado marcos patentados que implican la prefinanciación en las instituciones agentes de las instituciones receptoras para permitir un desembolso más rápido y liquidar los montos agregados periódicamente. Los vínculos entre las instituciones financieras, los proveedores de servicios de pago no bancarios y los MTO han traído consigo una mayor eficiencia en las etapas de envío y recepción. Sin embargo, el tramo de fondos transfronterizos no ha experimentado mucha innovación y, en particular, las comisiones de cambio siguen siendo una gran parte de las comisiones de remesas, alrededor del 20 % del coste total.23

Al crear una red distribuida para la liquidación de fondos entre divisas que reemplaza a la red de corresponsalía bancaria, DLT puede eliminar las ineficiencias en el sistema actual y ofrece potencial para reducciones significativas de costos, especialmente en el tramo transfronterizo e interbancario de la transacción. Al reducir los costos de liquidación y aumentar la eficiencia de las transferencias interbancarias y transfronterizas, la TRD podría ayudar a reducir aún más el precio de las remesas. DLT también puede permitir nuevos enfoques para la banca corresponsal, que potencialmente puede ser parte de un marco de solución para abordar la reducción de riesgos.

Ejemplos

Ripple. Se centra en los pagos comerciales transfronterizos e interbancarios combinados con la liquidación de fondos en divisas. Ripple permite alejarse del establecimiento de relaciones de corresponsalía bancaria por adelantado hacia un enfoque más dinámico. Este enfoque implica identificar un "camino" para el flujo de fondos de un remitente en una moneda particular a un receptor en una moneda en particular, a través de una serie de instituciones participantes que ofrecen servicios para esa moneda. Esto puede conducir a un mejor descubrimiento de los precios de las transacciones de divisas y a la ampliación del acceso a dichos servicios para las empresas de remesas más pequeñas.

Ripple tiene su propia criptomoneda, XRP, que se negocia activamente en varios intercambios de criptomonedas. Ripple también opera su propio intercambio, estructurado como una red descrita anteriormente, en el que las principales monedas intercambiadas activamente son CNY, USD, JPY y EUR. Además, otras criptomonedas como BTC (Bitcoin) y ETH (Ether) también se intercambian activamente. El banco Shanghái Huarui anunció recientemente que está trabajando en un producto de remesas utilizando Ripple para el corredor ENTRE Estados Unidos y China.24

Abra. Ofrece transferencias de dinero P2P instantáneas sin tarifas de transacción a través de la red de Abra, combinando criptomonedas con cajeros bancarios físicos. Debido a la existencia de cajeros, no se requiere ninguna cuenta bancaria para realizar un pago transfronterizo; solo el número de teléfono del destinatario. A partir de 2017, Abra está disponible a nivel mundial y admite más de 50 monedas, además de Bitcoin.

Bitpesa.25 Ofrece pagos transfronterizos para empresas y particulares entre varios países africanos (Kenia, Nigeria, Tanzania, Uganda) y China. Utiliza Bitcoin para la etapa transfronteriza y ha ganado tracción entre algunos importadores africanos por pagar a proveedores chinos.

Bita. Empresa de blockchain con sede en Barbados que comenzó como la primera compañía de intercambio de bitcoin del Caribe y lanzó una moneda fiduciaria digital del dólar de Barbados en la cadena de bloques de Bitcoin en febrero de 2016. Planes para crear una red unificada de liquidación financiera para la región de CARICOM a fin de reducir los tiempos de liquidación, reducir el costo de las remesas y erradicar las fricciones causadas por los sistemas monetarios fragmentados del Caribe.

Sistemas de Identidad Digital

A nivel mundial, el 18% de las personas no bancarizadas citan la falta de documentación relacionada con la identificación como una de las razones para no estar bancarizadas en 2014.26 DLT se puede usar para registrar y almacenar documentos relacionados con la identificación, como certificados de nacimiento y certificados de matrimonio, pero también historiales de transacciones, títulos de propiedad o registros de salud de una manera segura y verificable. Una ventaja de DLT es que permite un sistema en el que los datos personales podrían ser propiedad de individuos, en lugar de las respectivas agencias gubernamentales. Bajo algunas implementaciones, las personas podrían decidir qué partes seleccionadas de sus datos personales digitales eligieron divulgar a terceros. Esto podría, en algunas circunstancias, ser particularmente valioso en contextos de conflicto frágil y violencia afectados (FCV) donde existe una capacidad institucional débil y / o regímenes gubernamentales volátiles. Sin embargo, las instituciones estatales (u otros organismos oficiales) seguirían siendo, en la mayoría de los casos, necesarias como organismos de autenticación de los datos de identidad.

Si bien los sistemas de identidad digital que utilizan DLT pueden resolver potencialmente los problemas relacionados con la propiedad de los datos y el almacenamiento de datos de identidad, lograr una aceptación generalizada de los productos de identidad digital entre las agencias gubernamentales y los proveedores de servicios sigue siendo un desafío. Además, es necesario desarrollar o revisar marcos legales y regulatorios para garantizar los estándares de privacidad de datos para las aplicaciones de identificación que utilizan DLT, especialmente las cadenas de bloques sin permiso.

Ejemplos

ShoCard. ShoCard, con sede en Palo-Alto, es una tarjeta de identidad digital, optimizada para dispositivos móviles, que almacena información de identificación en la cadena de bloques de Bitcoin. La compañía está en el proceso de desarrollar soluciones para casos de uso como la verificación de identidad, incluso en aeropuertos y centros de llamadas; credencialización de servicios financieros; registros automatizados para compras en línea, comprobante de edad y dirección, por ejemplo, en las paradas policiales.

BanQu. La compañía blockchain BanQu proporciona una "identidad económica" a las personas al almacenar la identidad y otra información crítica, incluida la biometría, en la cadena de bloques Ethereum. Se centran en el espacio humanitario y los países en desarrollo, y están probando la identidad digital BanQu en una serie de proyectos, incluido el de proporcionar una identidad digital a los refugiados sirios en Ammán, solucionar las fugas de la cadena de suministro en la entrega de medicamentos y vacunas, e implementar seguros de microcultivos a través de contratos inteligentes.

IBM anunció un proyecto de blockchain con el startup fintech de Singapur KYCK! para permitir a los proveedores de servicios financieros abordar los desafíos de KYC y incorporar más rápidamente a los clientes en un entorno seguro. Su proyecto se probará y construirá en la cadena de bloques Hyperledger 'Fabric'. ¡Una vez confirmada la verificación de identidad, KYCK! ingresará la información del cliente en cheques bancarios actuales o en un KYCK de terceros. sistema antes de la incorporación de la cuenta.27

Registros de Activos

Los marcos incompletos de las operaciones garantizadas y la ausencia de registros fiables de activos (incluidos los registros de bienes muebles) significan que la falta de pruebas de garantías puede ser un obstáculo importante para el derecho al crédito en muchos países. Solo dos mil millones de personas en todo el mundo tienen un título que es legal, efectivo y público con respecto a su control sobre un activo y el economista peruano Hernando de Soto estima que el valor de este "capital muerto" asciende a $ 9.3 billones a nivel mundial.

Tradicionalmente, los registros de activos se gestionan de forma centralizada. Con servicios adicionales habilitados además para validar la propiedad, verificar la existencia de gravámenes, etc., DLT podría hacer posible una forma más descentralizada y, por lo tanto, potencialmente más rápida de crear registros de activos mediante el uso de la sociedad civil y otras partes interesadas de confianza para validar la propiedad y registrarlos en un DL. Una vez que se registran en una cadena de bloques pública, son inmutables y verificables, lo que reduce el riesgo de manipulación inadecuada debido a la corrupción y el favoritismo político. Los activos subyacentes también podrían ser activos móviles como inventarios y activos en un almacén (con mecanismos de etiquetado apropiados), que pueden utilizarse para mejorar la solvencia crediticia y, por lo tanto, abrir más vías para acceder al crédito.

Existen aplicaciones potenciales de DLT para crear registros confiables de la procedencia de las materias primas, especialmente los insumos agrícolas y los productos básicos, en combinación con otras tecnologías como el geoetiquetado y el registro de métricas específicas como la calidad del suelo, las condiciones climáticas y el uso de fertilizantes. Como ejemplo, un comprador internacional a granel de cacao podría determinar de manera confiable que un lote particular de granos de cacao provenía de una granja en particular con prácticas agrícolas específicas y pasaba a través de un conjunto específico de intermediarios. Esto podría aumentar el poder de fijación de precios del agricultor y los intermediarios, aumentando así la rentabilidad. El número de partes que necesitan ver un conjunto coherente de información podría ser dinámico en estos contextos, lo que dificulta su administración en un sistema centralizado tradicional.

Ejemplos

• Proyecto de titulación de tierras de la República de Georgia. La Agencia Nacional de Registro Público de la República de Georgia anunció una asociación con Bitfury (una compañía minera de Bitcoin) y el economista peruano Hernando de Soto en abril de 2016 para diseñar y probar un proyecto de titulación de tierras blockchain. El plan es crear una cadena de bloques privada adaptada para el registro de derechos de propiedad que esté anclada a la cadena de bloques pública de Bitcoin.28

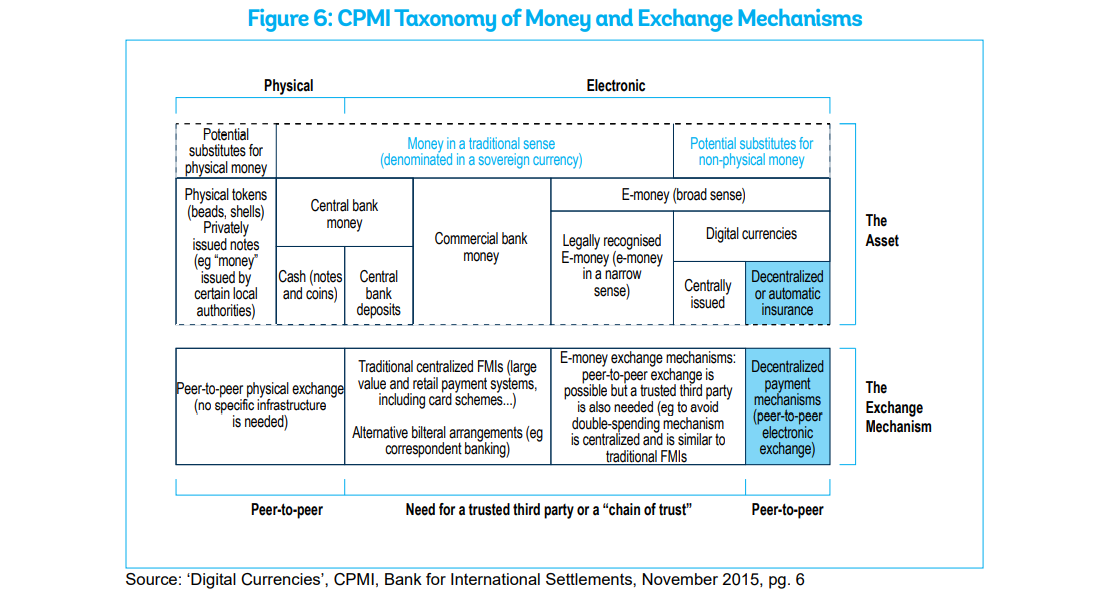
• Ubitidad. La start-up de blockchain con sede en los Estados Unidos, Ubitquity, lanzó una plataforma de bienes raíces en la cadena de bloques de Bitcoin para el seguimiento de la propiedad de títulos de bienes raíces en los Estados Unidos. Ubitquity y el Banco Mundial fueron coautores de un libro blanco sobre aplicaciones de blockchain para la administración de tierras para una conferencia del Banco Mundial sobre tierra y pobreza en marzo de 2016.29

• Everledger. La start-up de blockchain con sede en Londres Everledger lanzó un sistema global de certificación y seguimiento de diamantes en blockchain. Actualmente hay 980,000 diamantes registrados en la cadena de bloques Everledger que permiten registros confiables para aseguradoras, financieros y otras partes interesadas.30

Monedas digitales

La definición del término monedas digitales todavía está evolucionando. Un informe de 2015 del CPMI identificó tres características clave de las monedas digitales (no fiduciarias): (i) el activo subyacente no tiene valor intrínseco; en cambio, el valor está determinado por la demanda y la oferta; ii) utilizan la TRD como mecanismo subyacente para las transferencias de igual a igual; y (iii) no se basan en arreglos institucionales específicos o intermediarios para los intercambios entre pares.31 La Figura 6 describe la taxonomía del CPMI para los mecanismos monetarios y cambiarios, que explica dónde se podría colocar el dinero electrónico y las monedas digitales en relación con otros tipos de dinero, e ilustra las diferencias clave entre las monedas digitales y el dinero electrónico.

En los últimos años, ha habido mucha discusión sobre las monedas digitales emitidas por el banco central que utilizan la moneda fiduciaria como el "activo" subyacente en el marco anterior. Esta sección analiza las monedas digitales no fiduciarias, mientras que las monedas fiduciarias digitales emitidas por el banco central se mencionan en la sección 9.



El potencial de las monedas digitales para reducir las barreras de entrada en el sistema financiero para las poblaciones no bancarizadas y excluidas justifica una mayor investigación y exploración. Las aplicaciones que combinan marcos de dinero electrónico y dinero móvil con monedas digitales basadas en DLT para transferencias interbancarias podrían ser especialmente relevantes para las poblaciones financieramente excluidas y desatendidas: los marcos de dinero electrónico y dinero móvil amplían el alcance geográfico y reducen la dependencia de la infraestructura bancaria física, como sucursales bancarias o agentes, y DLT tiene el potencial de mejorar la eficiencia. Las ganancias de eficiencia se derivan principalmente del uso de la moneda digital como medio de transferencia entre el pagador y el beneficiario sin intermediarios, a menudo a costo cero. Esto se combina con el uso de teléfonos móviles como mecanismo de acceso y el uso de agentes o intercambios para convertir la moneda digital a moneda fiduciaria, como dinero electrónico, efectivo o crédito en una cuenta bancaria. Es probable que se incurra en costos en el momento de convertir la moneda digital en moneda fiduciaria.

Pero a pesar de estas ventajas, existen preocupaciones regulatorias y otros desafíos relacionados con las monedas digitales que requieren más atención antes de que la adopción a gran escala se convierta en una opción realista. Existen preocupaciones particulares relacionadas con la protección del consumidor y la lucha contra el blanqueo de capitales y la financiación del terrorismo. Al igual que en efectivo, las transacciones en monedas digitales basadas en DLT generalmente no son reversibles, lo que plantea preguntas sobre los mecanismos de recurso y la resolución de disputas. Los saldos mantenidos en monedas digitales no fiduciarias tampoco están cubiertos actualmente por las agencias de seguros de depósitos, por ejemplo, la FDIC en los Estados Unidos, y las agencias de aplicación de la ley no hacen un seguimiento sistemático de los casos de fraude que involucran monedas digitales. El valor de las monedas digitales está determinado por la demanda y la oferta y, por lo tanto, puede exhibir amplias fluctuaciones, lo que puede hacer que no sea adecuado como reserva de valor, a diferencia de las monedas fiduciarias. Además, muchas discusiones sobre monedas digitales asumen la existencia de un ecosistema completo donde esta moneda digital ya es ampliamente aceptada y, por lo tanto, no hay necesidad de convertir la moneda digital en moneda fiduciaria. Esto, sin embargo, aún no refleja la realidad de grandes segmentos de la población en la mayoría de los países hoy en día.

Actualmente, es poco probable que DLT reemplace completamente cualquier infraestructura financiera, instituciones y protocolos existentes y algunas de las aplicaciones basadas en DLT más prometedoras utilizan y se basan en las estructuras existentes. Las billeteras digitales que contienen monedas digitales que permiten transacciones transfronterizas electrónicas directas actualmente todavía dependen de la infraestructura de pagos nacionales para ser financiadas, lo que generalmente se hace a través de un banco convencional o una cuenta móvil o una tarjeta de pago, pero en teoría también podría hacerse a través de un agente o cajero (ver ejemplo de Abra arriba). Sin embargo, esto podría, al menos en teoría, cambiar en el futuro si la aceptación de las monedas digitales entre los comerciantes fuera de línea y en línea se generalizara, por ejemplo, una vez que los bancos centrales emitan monedas fiduciarias digitales.

También vale la pena señalar que el empleo de DLT para ayudar a alcanzar los objetivos de inclusión financiera requiere el desarrollo y la promoción activa de importantes elementos de acompañamiento. Entre ellas cabe destacar: (i) el diseño de una interfaz de aplicación fácil de usar, (ii) la educación y la capacidad financieras, (iii) un marco sólido de protección del consumidor financiero que se aplique a los servicios financieros habilitados por DLT, (iv) la interoperabilidad con los servicios e infraestructura financieros y de pago tradicionales; y v) una supervisión eficaz. Los enfoques alternativos para abordar las limitaciones de la infraestructura financiera existente deben considerarse paralelos y potencialmente en complemento con la TRD, como la computación en la nube, el dinero electrónico y el dinero móvil, y los sistemas de identificación biométrica.

8. Contratos inteligentes

Los 'contratos inteligentes', en el contexto de DLT, son programas que se escriben en el libro mayor distribuido subyacente y son ejecutados automáticamente por los nodos de la red. Cualquier instrucción que pudiera ser ejecutada por una computadora podría teóricamente ser ejecutada por un contrato inteligente. Las transacciones o datos registrados en el libro mayor distribuido activan el contrato inteligente y las acciones tomadas se registran a su vez en el libro mayor. Otra forma de expresar esto es que los contratos inteligentes "permiten que la lógica se programe sobre la transacción de blockchain".32 Lo mismo se aplica a otros DL, ya que los contratos inteligentes también pueden ser ejecutados por DL que no son blockchains. Los contratos inteligentes deben ser verificables por cada nodo de la red, lo que significa que todos los nodos de la red deben ver los mismos datos.

El término fue acuñado por primera vez por el criptógrafo Nick Szabo en un artículo de 1997 donde utilizó una máquina expendedora para ilustrar la idea de un contrato inteligente.33 La máquina expendedora, un dispositivo mecánico, controla la propiedad de un activo, la barra de caramelo, y ejecuta la transferencia de propiedad cuando se activa por una entrada definida, el evento de ingresar una moneda en la máquina. Por lo tanto, la máquina expendedora hace cumplir los términos del "contrato" pre-acordado que define los activos subyacentes, los insumos y las acciones consecuentes. Una analogía moderna omnipresente serían las reglas de negociación automáticas, ejecutadas por un programa informático, que inician ventas o compras de valores a un precio de ejercicio predefinido. Las aplicaciones potenciales de los contratos inteligentes podrían utilizarse en los mercados de derivados, fusiones y adquisiciones, y en transacciones de valores, entre muchos otros.

Los sistemas DLT proporcionan una plataforma que permite que los contratos inteligentes, escritos en código informático, controlen realmente los activos del mundo real, como bienes raíces, acciones, títulos de propiedad o depósitos en garantía, sin la necesidad de un tercero que controle la liberación de los activos, como un corredor, un administrador de títulos de propiedad o un agente de custodia, por ejemplo. Esto se debe al hecho de que los nodos en la red distribuida tienen la capacidad de hacer cumplir un contrato mediante la ejecución de código. Por ejemplo, la figura 7 ilustra cómo se podría utilizar un contrato inteligente en el contexto de la financiación del comercio. Un enfoque similar basado en DLT también podría aplicarse a una variedad de otros contextos, como los procesos hipotecarios o los registros de garantías.

Los contratos inteligentes han cautivado a los idealistas porque hacen posibles empresas automatizadas que no dependen de ningún aporte humano, ni gerentes ni directores de juntas, excepto patrocinadores financieros. Ethereum es la segunda cadena de bloques pública más grande, después de Bitcoin, y está optimizada para aplicaciones de contratos inteligentes. Se han lanzado una serie de DAO (Organizaciones Autónomas Descentralizadas) en la plataforma Ethereum, que son, en efecto, fondos de capital de riesgo para negocios automatizados. CoinDesk define el objetivo de un DAO como "codificar las reglas y el aparato de toma de decisiones de una organización, eliminando la necesidad de documentos y personas en el gobierno, creando una estructura con control descentralizado. Así es como funciona:

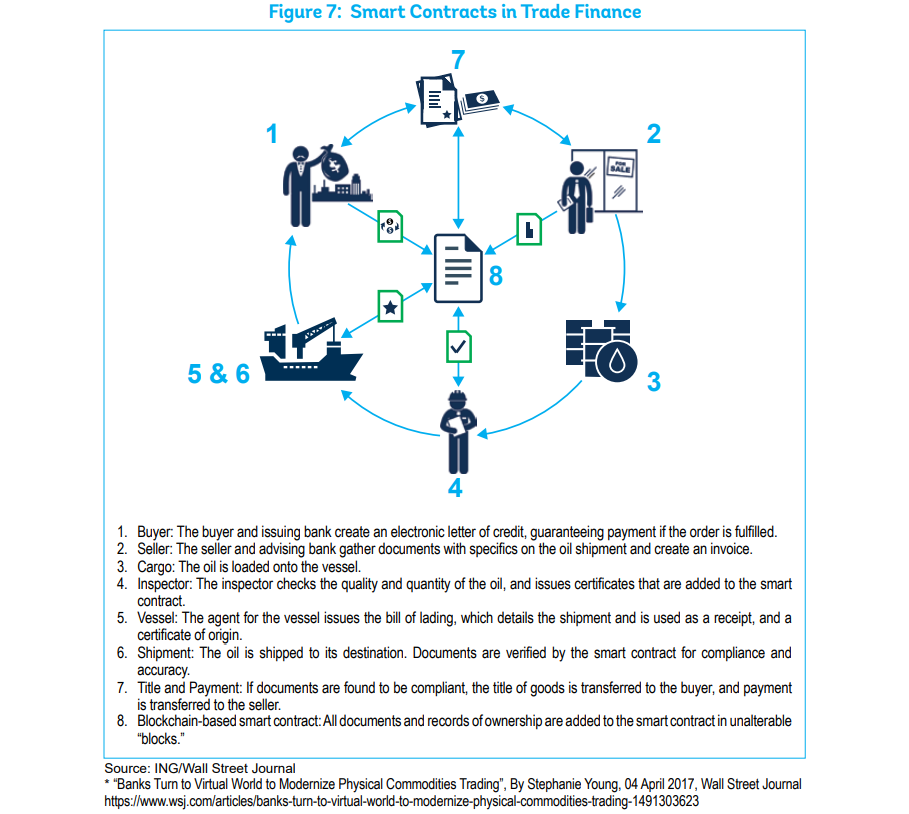
• Un grupo de personas escribe los contratos inteligentes (programas) que ejecutarán la organización.

• Hay un período de financiación inicial, en el que las personas agregan fondos al DAO comprando tokens que representan la propiedad, esto se llama crowdsale u oferta inicial de monedas (ICO), para darle los recursos que necesita.

• Cuando finaliza el período de financiación, la DAO comienza a operar.

• Las personas pueden hacer propuestas a la DAO sobre cómo gastar el dinero, y los miembros que han comprado pueden votar para aprobar estas propuestas".34

Sin embargo, la confianza en Ethereum se puso a prueba después de un ataque exitoso contra dicha entidad, conocida como "The DAO", en junio de 2016 en el que un atacante desvió 3,5 millones de unidades de la criptomoneda "Ether" de Ethereum, por un valor de alrededor de US $ 50 millones en el momento del hackeo. El DAO, que estaba dirigido por un startup alemán llamada Slock.it, había roto récords de crowdsourcing al recaudar el equivalente a US $ 120 millones de Ether en un mes, lo que constituyó el 14% de todo el Ether jamás emitido. Un hacker explotó una falla en el software DAO, una aplicación ejecutada en Ethereum, pero la cadena de bloques central de Ethereum en sí no fue pirateada. Este hack es un ejemplo de un exploit de una vulnerabilidad de seguridad que existía en la capa de aplicación en la parte superior de la cadena de bloques, que son una preocupación de seguridad importante.



En respuesta al ataque, la comunidad Ethereum tomó una decisión controvertida de completar una llamada "bifurcación dura" en la cadena de bloques ethereum para recuperar los fondos robados. Como resultado, la cadena de bloques de Ethereum se dividió en dos criptomonedas activas separadas: Ether (que contiene la bifurcación dura que restauró los fondos robados, también conocida como Ethereum One o Ethereum Core) y Ethereum Classic (registro de transacción original con fondos robados aún bajo control del hacker). Una encuesta entre más de 240 líderes técnicos en la comunidad blockchain realizada por CoinDesk reveló que el 63% no informó ningún cambio en su uso de Ethereum después de la bifurcación, a pesar de que un tercio se había opuesto originalmente a la bifurcación dura.35 (Consulte el anexo para obtener más información sobre el hack DAO y las bifurcaciones de Ethereum).

Además de las vulnerabilidades técnicas, el uso de contratos inteligentes automatizados combinados con DLT también plantea una serie de cuestiones legales y reglamentarias, por ejemplo, relacionadas con la responsabilidad, la jurisdicción, las modificaciones y la anulabilidad de los contratos.

9. ¿Qué están haciendo los gobiernos, las organizaciones de desarrollo y los donantes en este espacio?

La Oficina de Ciencia del Gobierno del Reino Unido publicó un importante informe sobre blockchain y DLT, publicado en enero de 2016, que evalúa las oportunidades de DLT para ser utilizado dentro del gobierno y por el sector privado y recomienda una amplia iniciativa gubernamental para facilitar el uso beneficioso de DLT. En este informe, el asesor científico jefe del Reino Unido, Mark Walport, escribe: "Las tecnologías de contabilidad distribuida tienen el potencial de ayudar a los gobiernos a recaudar impuestos, entregar beneficios, emitir pasaportes, registrar registros de tierras, asegurar la cadena de suministro de bienes y, en general, garantizar la integridad de los registros y servicios gubernamentales. [...] Para el consumidor de todos estos servicios, la tecnología ofrece el potencial, según las circunstancias, para que los consumidores individuales controlen el acceso a los registros personales y sepan quién ha accedido a ellos. [...] La tecnología de contabilidad distribuida proporciona el marco para que el gobierno reduzca el fraude, la corrupción, el error y el costo de los procesos intensivos en papel. Tiene el potencial de redefinir la relación entre el gobierno y el ciudadano en términos de intercambio de datos, transparencia y confianza. Tiene posibilidades similares para el sector privado".36 El informe establece ocho acciones recomendadas para que el gobierno maximice las oportunidades y reduzca los riesgos de DLT, entre ellas:

• Proporcionar la visión, el liderazgo y la plataforma para DLT dentro del gobierno

• Invertir en investigación

• Crear un marco regulatorio para DLT

• Establecer estándares de seguridad, privacidad e integridad

• Generar confianza e interoperabilidad

• Asegurar la implementación de protocolos efectivos de identificación y autenticación

• Establecer ensayos de DLT para evaluar la usabilidad dentro del sector público

• Desarrollar capacidades y habilidades dentro del gobierno.

Plataforma de residencia electrónica de Estonia. El gobierno estonio ha estado experimentando con DLT durante años, utilizándolo para verificar registros en bases de datos gubernamentales, por ejemplo, certificados de nacimiento y matrimonio. Estonia también ha sido pionera en el concepto de residencia electrónica como una forma de identidad digital transnacional. La residencia electrónica estonia está disponible para cualquier persona en el mundo interesada en utilizar los servicios en línea estonios, abrir una cuenta bancaria o iniciar una empresa. Los residentes electrónicos pueden solicitar una cuenta bancaria, realizar operaciones bancarias en línea, declarar impuestos, firmar documentos de forma remota y obtener acceso a proveedores de pagos internacionales. NASDAQ se está asociando con la plataforma de residencia electrónica de Estonia para permitir el voto electrónico seguro en las reuniones de accionistas.

Los bancos centrales de todo el mundo están explorando las monedas digitales basadas en DLT. En el Reino Unido, Canadá, Rusia, Australia, Suecia, China, los bancos centrales están evaluando los riesgos y beneficios de emitir moneda digital respaldada por moneda fiduciaria en la cadena de bloques, e investigando sus posibles efectos en la economía y en la estabilidad financiera. Cualquier moneda digital emitida por el banco central probablemente se vería sustancialmente diferente del modelo abierto, descentralizado y peer-to-peer de Bitcoin y podría no necesitar un enfoque DLT. A diferencia del efectivo, las monedas digitales crean un registro permanente y rastreable de cada transacción y se eliminarían los costos de manejo de efectivo. Otra ventaja potencial de las monedas digitales basadas en DLT es la perspectiva de "dinero inteligente". Una moneda basada en DLT con un libro mayor digital abre la posibilidad de programar ciertos términos y condiciones sobre el dinero digital, por ejemplo, cómo, dónde, cuándo y por quién se puede gastar. Se están discutiendo muchos escenarios diferentes, una opción radical evitaría a los bancos comerciales como intermediarios al permitir que los clientes individuales tengan cuentas directamente con el banco central, utilizando DLT.37 En Senegal, el Banque Régionale de Marchés (BRM) lanzó una solución de dinero electrónico en 2016, con la diferencia de que los fondos del grupo de clientes se mantienen con el banco central regional BCEAO. Esta solución ha sido proporcionada por eCurrency Mint Limited (eCurrency). El banco central de China, el Banco Popular de China, probó una moneda digital basada en blockchain en enero de 2017.

Un documento reciente publicado por el Banco de Inglaterra analiza las oportunidades de ahorros significativos de las monedas digitales emitidas por el banco central a través de una reducción en las tasas de interés reales, así como menores costos de transacción.38 Según este análisis, un régimen de moneda digital emitida por el banco central resultaría en un "aumento permanente" en los flujos de ingresos fiscales para el gobierno (debido a las reducciones en los gastos netos por intereses), lo que permitiría un aumento del gasto público o una reducción de las tasas impositivas por parte de la autoridad fiscal, con metas de déficit y deuda sin cambios. Además, el documento argumenta que las monedas fiduciarias digitales podrían mejorar la estabilidad financiera al proporcionar al banco central una herramienta de política adicional para reducir las tasas de interés por debajo del límite inferior cero y también poder financiar directamente las compras de activos por parte de no bancos sin necesidad de intermediación bancaria.

Los reguladores de todo el mundo, tanto en los países de la OCDE como en los países en desarrollo, por ejemplo, Uganda,39 están estudiando la regulación de las monedas digitales. Los esfuerzos de autorregulación también están en marcha: la Asociación Australiana de Moneda y Comercio Digital, por ejemplo, ha lanzado el Código de Conducta de la Industria de la Moneda Digital, que se centra en la protección y el alcance del consumidor.40

El FMI publicó un informe sobre los beneficios y riesgos de las monedas digitales en enero de 2016.41 El informe examina las implicaciones preliminares de las monedas digitales (denominadas «monedas virtuales» en el informe) para la regulación y la política, incluidas las cuestiones relacionadas con la lucha contra el blanqueo de capitales y la financiación del terrorismo, la protección de los consumidores, la fiscalidad, los controles de cambio y la gestión de los flujos de capital, la estabilidad financiera y la política monetaria.

El CPMI publicó un informe sobre monedas digitales en noviembre de 2015, que considera las implicaciones de las monedas digitales y sus mecanismos de pago descentralizados subyacentes para los bancos centrales, las cuestiones regulatorias y los factores del lado de la demanda y la oferta que influyen en el desarrollo de las monedas digitales.42 El Banco Mundial participó en el grupo de trabajo que produjo el informe. El CPMI también publicó un informe sobre el uso de DLT para el pago, la compensación y la liquidación en febrero de 2017, que proporciona un marco analítico para que los bancos centrales y otras autoridades revisen y analicen los casos de uso de DLT (centrándose en los libros de contabilidad autorizados) e identifiquen riesgos y oportunidades.43

El Banco Mundial también participa en varios grupos de trabajo sobre este tema en el FSB, CPMI-IOSCO y el GAFI.

El Departamento de Trabajo y Pensiones del Reino Unido puso a prueba DLT para transferencias gubernamentales. DLT ofrece la oportunidad para que los gobiernos monitoreen la observancia o las reglas del programa relacionadas con las transferencias gubernamentales condicionales a través de contratos inteligentes. Por ejemplo, los pagos relacionados con los programas de dinero por trabajo se pueden ejecutar automáticamente una vez que se completa el trabajo o los pagos por proyectos de obras públicas que están condicionados a la finalización del proyecto de obras se pueden ejecutar automáticamente. El Departamento de Trabajo y Pensiones del Reino Unido comenzó una prueba en junio de 2016 para usar DLT para los pagos de beneficios sociales, trabajando con GovCoin Systems y otros socios (Barclays, RWE Npower, University College London). Los reclamantes están utilizando una aplicación en sus teléfonos a través de la cual están recibiendo y gastando sus pagos de beneficios, que está diseñada para ayudarlos a administrar el dinero de sus beneficios. Con su consentimiento, las transacciones se registran en un libro mayor distribuido con el objetivo de crear una infraestructura de bienestar más eficiente y segura que evite el fraude.

Sandboxes regulatorios y "Test and Learn"

Enfoques regulatorios. Los reguladores están explorando diferentes enfoques regulatorios para las innovaciones basadas en DLT. Un sandbox regulatorio, tal como lo define la Autoridad de Conducta Financiera del Reino Unido, "tiene como objetivo crear un 'espacio seguro' en el que las empresas puedan probar productos, servicios, modelos de negocio y mecanismos de entrega innovadores en un entorno en vivo sin incurrir inmediatamente en todas las consecuencias regulatorias normales de participar en la actividad en cuestión".44 Varios reguladores en los países de la OCDE y también en países de ingresos medios como Malasia han implementado un marco de este tipo que permite a las nuevas empresas e instituciones reguladas experimentar, probar y lanzar servicios a pequeña escala utilizando DLT y otros enfoques Fintech. Aprovechando este marco, la Autoridad Monetaria de Singapur anunció recientemente sus planes de llevar a cabo un piloto utilizando DLT para pagos y liquidaciones interbancarias. Malasia y la Comisión de Bolsa de Valores de Hong Kong recientemente dieron permiso para una plataforma de financiación colectiva basada en DLT.

La firma internacional de consultoría de desarrollo Chemonics, un importante contratista de USAID, estableció un 'Blockchain for Development Solutions Lab' en asociación con la compañía de tecnología blockchain BanQu, anunciada en octubre de 2016. El objetivo del laboratorio es "construir, probar y escalar soluciones de blockchain para reducir la pobreza y aumentar la efectividad de la ayuda".45

BitLicense – Departamento de Servicios Financieros del Estado de Nueva York (NYDFS). En junio de 2015, el estado de Nueva York lanzó BitLicense, un marco regulatorio para empresas dedicadas a la "actividad comercial de moneda virtual" que actúan como intercambios de criptomonedas y / o funcionan como custodios de bitcoin y otras criptomonedas. Como parte del proceso de solicitud, el regulador del estado de Nueva York revisa las políticas de las compañías contra el lavado de dinero, la protección del consumidor y la ciberseguridad.46 A partir de octubre de 2017, NYDFS ha otorgado BitLicenses a tres compañías, que son todos los principales actores de la industria: Circle, Ripple y Coinbase. Además de BitLicense, el regulador también ha otorgado cartas bancarias a los intercambios de bitcoin Gemini e itBit. La BitLicense ha generado algunas críticas por parte de la comunidad de start-ups por los altos costos asociados con la aplicación, lo que ha llevado a algunas empresas a cesar sus operaciones en Nueva York.

Las "Enmiendas Blockchain" de Delaware de 2017.

En julio de 2017, la Asamblea General de Delaware aprobó una serie de enmiendas que reconocen blockchain como una forma aceptable de mantenimiento de registros corporativos, a partir del 1 de agosto de 2017. Bajo esta ley, las corporaciones de Delaware tienen la capacidad de emitir acciones y administrar registros de propiedad utilizando la tecnología blockchain.47

10. ¿Cómo se puede aprovechar la TRD para los programas y proyectos del Banco Mundial en el sector financiero?

DLT aún se encuentra en una etapa temprana de desarrollo y muchos desafíos deben resolverse antes de que se pueda realizar todo el potencial de la tecnología, como los problemas relacionados con la privacidad, la seguridad, la escalabilidad, la interoperabilidad y los problemas legales y regulatorios. La mayor parte de los recursos de I+D para DLT se dedican actualmente a mejorar la infraestructura y los procesos financieros, y esta inversión podría ser aprovechada por las organizaciones de desarrollo en beneficio de los países en desarrollo. Sin embargo, como la tecnología aún se está desarrollando y probando, y aún no es lo suficientemente robusta y escalable, el Grupo del Banco Mundial no puede, en esta etapa, emitir recomendaciones generales sobre la usabilidad independientemente de los contextos específicos.

El Banco de Inglaterra (BoE) lanzó una revisión del sistema de liquidación bruta en tiempo real (RTGS) que opera, seguida de una consulta de la industria en la que consideró las aplicaciones de DLT. El BoE concluyó recientemente esta consulta con la evaluación de que DLT es inmaduro en este momento, sin embargo, explorará cómo integrar e incorporar DLT a medida que la tecnología madure.48 El Banco de Canadá también llegó a una conclusión similar.

Existe una visión emergente de que las aplicaciones DLT en finanzas que probablemente ganarán tracción primero no serán los sistemas de pago y liquidación, sino áreas en las que hay poca automatización y un uso intensivo de procesos manuales con altas ineficiencias. Las áreas sugeridas que se ajustan a estas características son: (i) mantenimiento de datos de referencia en los sistemas de pago y liquidación; ii) financiación del comercio; iii) préstamos sindicados; y iv) el seguimiento de la procedencia de los productos agropecuarios, los productos básicos y similares y su posterior venta o utilización como garantía sobre la base de la cual se proporciona financiación. También hay discusiones sobre las aplicaciones de DLT como parte del marco de la solución para reducir el riesgo a través de: (i) el mantenimiento confiable y auditable de la identidad, incluidos los datos de Conozca a su cliente y la debida diligencia del cliente; ii) desarrollar una alternativa al modelo de corresponsalía bancaria (como se señaló en el debate sobre Ripple); y (iii) el uso de una criptomoneda para el tramo transfronterizo (como se señaló en la discusión de Abra).

También se debe considerar el argumento presentado en el informe de 2016 de la Oficina de Ciencia del Gobierno del Reino Unido de que "si el gobierno espera soluciones 'perfectas', perderá la oportunidad de dar forma y adquirir implementaciones de la tecnología que proporcionarán el máximo beneficio al sector público, y el Reino Unido también puede perder oportunidades de beneficio económico". Se requiere más investigación y exploración para alcanzar un mayor nivel de sofisticación técnica y robustez de DLT, especialmente cuando se usa en combinación con contratos inteligentes. Pero comprender el verdadero potencial de DLT para los objetivos de desarrollo requiere no solo investigación, sino también aplicaciones y ensayos de la vida real.

Dado el potencial del DLT para estructurar soluciones a los desafíos del desarrollo en el sector financiero y más allá, el GBM debería seguir de cerca y dar forma a este desarrollo y, cuando proceda, fomentar su adopción.

Los diversos bancos centrales están estudiando activamente las aplicaciones de la TRD en los sistemas de pago y liquidación, y el GBM debería seguir de cerca la evolución mediante la participación en los diversos grupos de trabajo de los órganos normativos y mediante compromisos bilaterales. Sin embargo, otras áreas, en particular las relacionadas con el desarrollo del sector financiero y la inclusión financiera, no están recibiendo mucha atención de muchos actores y reguladores del sector privado. Esta es una esfera en la que el GBM podría desempeñar un papel más activo. Esto podría incluir, en particular, las solicitudes de financiación de la agricultura, la financiación de facturas y créditos por cobrar y los registros de garantías.

Entre las posibles medidas que podría adoptar el GBM figuran las siguientes:

Supervisar la evolución

• Seguir de cerca los acontecimientos en el ámbito de la TRD, especialmente las medidas adoptadas por los gobiernos y las organizaciones de desarrollo.

• Aplicar los instrumentos existentes, como la base de datos mundial sobre los precios de las remesas del Banco Mundial, para reunir sistemáticamente información sobre los costos de los posibles servicios de remesas basados en la TRD; y la Encuesta de Sistemas De Pagos Globales para recopilar información cualitativa y cuantitativa sobre el uso de la moneda digital y los enfoques de DLT y su marco regulatorio, y explorar oportunidades para recopilar información sobre los usos de los enfoques de DLT en los pagos minoristas en las encuestas de Costos de Pago Minorista.

• Aprovechar las participadas de IFC y los foros del sector privado como el Foro de Pymes para el intercambio de conocimientos y para identificar cuellos de botella regulatorios que obstaculizan el desarrollo de DLT.

• Aprovechar los foros existentes como ID4D, el Comité Internacional de Informes de Crédito (ICCR), el Foro de Pymes, el Grupo de Trabajo Global de Remesas y la próxima Iniciativa Global de Inclusión Financiera (FIGI) para monitorear y analizar de cerca los desarrollos en DLT y, cuando sea factible, diseñar e implementar pilotos.

Fomentar la colaboración y la coordinación con los organismos internacionales de normalización

• Únase a consorcios de la industria como el laboratorio de I+D de R3 y / o Hyperledger, proponga proyectos de investigación específicos con un enfoque de desarrollo, por ejemplo, proyectos relacionados con la identidad digital, abordando los desafíos de AML y KYC, registros de activos, aplicaciones relacionadas con la financiación agrícola o pagos y remesas transfronterizos.

• Fomentar la cooperación y la colaboración internacionales, aprovechando la participación continua en los grupos de trabajo de los organismos internacionales de normalización.

• Alentar a las empresas y otras entidades que trabajan en DLT a explorar la aplicabilidad de la tecnología para un contexto de desarrollo y proporcionar asistencia con la realización de pilotos y pruebas de concepto. Esto podría incluir un análisis exhaustivo de los verdaderos costos y beneficios del uso de enfoques DLT.

Mejorar el conocimiento de la TRD dentro del GBM y explorar las aplicaciones

• Mejorar el nivel de conciencia sobre DLT dentro de la Práctica Global de Finanzas y Mercados y más allá y alentar los Servicios de Asesoría y Análisis (ASA) y los programas de inversión en curso y en desarrollo para explorar oportunidades para aprovechar DLT.

• Aprovechar el nuevo WBG Blockchain Lab, que se asocia con un grupo de empresas de DLT y otras empresas de tecnología, para estudiar y desarrollar aún más soluciones basadas en DLT para pagos transfronterizos, particularmente en el contexto de reducir el riesgo y mantener los flujos de pago a las regiones afectadas por la fragilidad, el conflicto y la violencia (FCV). Cuando sea factible, esto podría hacerse en asociación con los países clientes. El laboratorio de blockchain del GBM49 también podría utilizarse para apoyar a los clientes en las pruebas piloto específicas de cada país.

• En las operaciones financiadas por el Banco Mundial, alentar a las contrapartes nacionales a invitar a las empresas que ofrecen soluciones de TRD a participar en el proceso de adquisición, cuando proceda, potencialmente como parte de un proceso de adquisición de 2 etapas.50 Como mínimo, se podría pedir a los licitadores que compartan enfoques de implementación alternativos y también compartan información sobre cómo funcionaría la infraestructura en cuestión en un marco de TRD.

• Explorar la financiación de proyectos piloto a pequeña escala como parte de los programas de asa e inversión del GBM, en particular en las áreas de financiamiento agrícola, financiamiento de facturas/ cuentas por cobrar y registros de garantías (que se identificaron anteriormente).

Participar activamente con los países clientes del BM que trabajan en estos temas:

• Apoyar a los países clientes del BM en el establecimiento de sandboxes regulatorios o participar como observadores en los sandboxes de otros países (por ejemplo, como colaboración Sur-Sur con países como México, Sudáfrica, Jordania y Malasia).

• Apoyar a los países clientes del Banco Mundial en la exploración de posibles aplicaciones de DLT en sus contextos específicos a través de toda la gama de compromisos del GBM: asistencia técnica, convocatoria e inversión, especialmente en las áreas de pagos transfronterizos y remesas, identidad y registros.

• Participar en revisiones de implementaciones piloto para evaluar los costos y beneficios de DLT

Anexo: El hack DAO y las bifurcaciones de Ethereum

Las bifurcaciones surgen cuando la cadena de bloques en un libro mayor distribuido se divide en dos caminos competitivos hacia adelante, y pueden interrumpir el valor y la estabilidad de las criptomonedas subyacentes. Una de las bifurcaciones más controvertidas tuvo lugar en julio de 2016, cuando la comunidad Ethereum completó una "bifurcación dura", lo que resultó en que la cadena de bloques de Ethereum divergiera en dos criptomonedas separadas (Ethereum One o Core y Ethereum Classic). Desde entonces, Ethereum se ha bifurcado tres veces más, y está planeando una quinta bifurcación dura, "Metrópolis", que se lanzará a finales de este año.51

La historia de las bifurcaciones de Ethereum

En abril de 2016, los miembros de la comunidad Ethereum, el equipo detrás de la start-up alemana "Slock.it", anunciaron el inicio de la Organización Autónoma Descentralizada (DAO), una organización con control descentralizado, gobernada por contratos inteligentes. Fue diseñado para operar como un fondo de capital de riesgo para la criptomoneda y el espacio descentralizado.52 El DAO construyó contratos inteligentes en la cadena de bloques Ethereum, lo que permitió a las personas hacer propuestas de financiamiento, y si suficientes inversores de DAO votaron a favor de la propuesta, el financiamiento se liberó después de 28 días. La iniciativa financió con éxito aproximadamente 150 millones de dólares de más de 11,000 inversionistas, uno de los mayores éxitos de crowdfunding en la historia.53 El DAO también tuvo una "función dividida" que permitió a los inversores abandonar la organización en caso de que vieran que se aceptaban propuestas perjudiciales. Sin embargo, a mediados de junio, los creadores de DAO anunciaron que habían encontrado un "error" en el software, y los programadores estaban comenzando a arreglar el código mientras más de 50 propuestas de proyectos aún estaban pendientes para la votación de DAO. En este momento, un hacker comenzó a explotar la vulnerabilidad del contrato inteligente y drenar el DAO de Ether (la criptomoneda de Ethereum). Para el 18 de junio, el hacker había acumulado más de $ 50 millones de dólares en Ether, pero, debido a la ventana de financiamiento, los fondos no estaban disponibles para su retiro durante 28 días, como se estipula en los contratos inteligentes de la DAO.54

La comunidad Ethereum debatió cómo reclamar los fondos. Debido a la naturaleza distribuida del libro mayor, no había una autoridad central para tomar una decisión rápida, y las bifurcaciones propuestas requerían un voto de consenso por parte de los miembros de la comunidad Ethereum. Se formularon dos propuestas:

• La propuesta de soft-fork, que no obtuvo suficientes votos, tenía la intención de mantener la compatibilidad con versiones anteriores, de modo que no fuera necesario reescribir bloques y los mineros pudieran continuar "permitiendo transacciones como de costumbre, esperar el código de soft-fork y estar listos para descargarlo y ejecutarlo si están de acuerdo con (el camino propuesto) hacia adelante para el ecosistema Ethereum".55 Esto habría intentado efectivamente poner en la lista negra al hacker. En respuesta a esta propuesta, el hacker (o un individuo que se hace pasar por un hacker, ya que los mensajes no fueron verificados) amenazó con acciones legales justificando que las reglas de los contratos inteligentes deben mantenerse. El hacker intentó proteger el éter "robado" ofreciendo a los mineros que no se actualizan al soft-fork una "recompensa". Debido a una vulnerabilidad que se descubrió en la propuesta de bifurcación suave, esta solución no se pudo implementar de manera efectiva.

• La propuesta de hard-fork alcanzó un consenso suficiente después de unas semanas de discusión (siguiendo las respuestas del "supuesto" hacker) y propuso una remodelación de la plataforma para arreglar el código subyacente vulnerable de los contratos inteligentes y permitir reparaciones para los inversores de DAO. Una minoría escindida dentro de la comunidad se negó a aceptar las nuevas reglas, continuó comerciando con Ether en la antigua plataforma y, por lo tanto, creó una cadena de bloques divergente que ahora continúa existiendo como la criptomoneda alternativa "Ethereum Classic", junto con la criptomoneda "Ethereum One" (o Ethereum Core), que aceptó la bifurcación dura.

Bifurcaciones posteriores

Después de la bifurcación dura histórica de Ethereum, la plataforma continuó implementando múltiples bifurcaciones a lo largo del tiempo en respuesta a los ataques distribuidos de denegación de servicio (DDoS), es decir, ataques que infectan y comprometen múltiples sistemas para inundar el host de Ethereum. Los ataques contribuyeron a lo que se llama un "estado hinchado", por el cual los mineros y los nodos pasan mucho tiempo procesando bloques, lo que dificulta el procesamiento y la verificación de las transacciones.56 Aunque se lanzó una bifurcación suave,57 según el blog de Ethereum, los piratas informáticos continuaron explotando varias debilidades a través de ataques DDoS, lo que planteó problemas inmediatos de salud de la red.58 Ethereum propuso una solución de bifurcación dura de dos etapas: la primera bifurcación dura, cuyo nombre en código es "tangerinewhistle", abordó las vulnerabilidades inmediatas; y la segunda bifurcación dura, "Spurious Dragon" (lanzada el 22 de noviembre de 2016), permitió la "desinflación del estado blockchain".59 Spurious Dragon marcó la cuarta bifurcación emprendida por Ethereum en general.

El futuro puede seguir bifurcándose

Las bifurcaciones se están convirtiendo en una ocurrencia frecuente en la comunidad blockchain. Sin embargo, las implicaciones de la bifurcación continua son desconocidas y muchos escépticos desconfían de las divergencias y la falta de cohesión comunitaria que acompañan a las bifurcaciones. Por ejemplo, la primera bifurcación dura de Ethereum creó cierta desconfianza en la comunidad,60 ya que los miembros se quejaron de que las ventanas de votación eran demasiado cortas y no estaban bien publicitadas, y como resultado, solo un pequeño porcentaje de miembros de la comunidad votó sobre las propuestas de bifurcación. Las implicaciones adicionales incluyen la fractura de las comunidades de criptomonedas, como en el caso de Ethereum Classic vs. Ethereum One (o Ethereum Core). Al dividirse en variantes, plataformas similares aumenta los riesgos de múltiples ataques, ya que existen las mismas vulnerabilidades en múltiples cadenas de bloques. A pesar de estos riesgos, las bifurcaciones se están volviendo rápidamente más ampliamente aceptadas dentro de la comunidad, y Ethereum está planeando dos bifurcaciones duras adicionales para mejorar la plataforma. El lanzamiento de 'Metrópolis' está previsto para finales de este año en 2017 y proporcionará una mayor flexibilidad en los contratos inteligentes para los desarrolladores. Además, hay anticipación para el lanzamiento de 'Serenity', que incluirá la transición de la prueba de trabajo al consenso de prueba de participación a través de un nuevo algoritmo llamado "Casper".61 La comunidad blockchain en línea estará esperando el lanzamiento de estas bifurcaciones para comprender sus implicaciones más amplias en el futuro de las criptomonedas públicas y la capacidad de una comunidad para actualizar, actualizar y manejar de manera cohesiva las evoluciones de la plataforma a lo largo del tiempo.

Notas

1. Satoshi Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System”. <https://bitcoin.org/bitcoin.pdf>

2. Adrian Chen, “We need to know who Satoshi Nakamoto is”, The New Yorker, 09 May 2016 <http://www.newyorker.com/business/currency/we-need-toknow-who-satoshi-nakamoto-is>

3. <http://www.fatf-gafi.org/publications/fatfgeneral/documents/guidance-rbavirtual-currencies.html>

4. En estos casos, los intercambios fueron pirateados y las monedas que se mantuvieron en los intercambios fueron robadas, al igual que una billetera en línea que contiene dinero electrónico o dinero fiduciario podría ser pirateada. El libro mayor de Bitcoin en sí nunca se corrompió como resultado de estos hackeos.

5. “Bitcoin Mining and its Energy Footprint”, Karl Dwyer and David Malone - <https://karlodwyer.github.io/publications/pdf/bitcoin_KJOD_2014.pdf>

6. <http://motherboard.vice.com/read/bitcoin-could-consume-as-much-electricityas-denmark-by-2020>

7. Esto significa que la aplicación de la misma función hash a la misma entrada siempre produce la misma salida. A diferencia del cifrado, que es un proceso bidireccional, el hashing es un proceso unidireccional. Un mensaje se puede cifrar y luego descifrar, pero es imposible revertir una salida hash a su mensaje original utilizando la función hash o cualquier otro método criptográfico.

8. El límite de tamaño de bloque de la cadena de bloques de Bitcoin es objeto de un intenso debate en la comunidad de Bitcoin. Satoshi Nakamoto decidió limitar el tamaño de un bloque a un megabyte, o alrededor de 1.400 transacciones. Los bloques podrían hacerse más grandes, pero los bloques más grandes tardarían más en propagarse a través de la red, empeorando los riesgos de bifurcación.

9. See CoinDesks’s Q3 State of Blockchain for more information on this: http://[www.coindesk.com/research/state-of-blockchain-q3-2016/#](http://www.coindesk.com/research/state-of-blockchain-q3-2016/)

10. <http://www.bis.org/cpmi/publ/d157.pdf>

11. Esta estimación proviene de un informe de 2015 del banco español Santander; la consultora de gestión Oliver Wyman y el inversor de capital riesgo Anthemis Group.

<http://santanderinnoventures.com/wp-content/uploads/2015/06/The-Fintech2-0-Paper.pdf>

12. Steve McConnell, “Code Complete: A Practical Handbook of Software Construction”, Microsoft Press; 2nd edition 2004. Cited in: <https://blog.slock.it/the-history-of-the-dao-and-lessonslearned-d06740f8cfa5>

13. <http://www.coindesk.com/short-guide-bitcoinforks-explained/>

14. <http://www.tech-recipes.com/rx/48517/cryptocurrency-what-is-a-fork/>

15. Existe la posibilidad de que los nodos no actualizados continúen minando y abandonen la cadena de bloques extraída de los nodos actualizados o se bifurquen en su propia criptomoneda.

16. CoinDesk, Estado de la cadena de bloques, Q3 2016

17. <http://www.coindesk.com/10-stock-exchangesblockchain/>

18. <http://www.wired.com/2015/12/sec-approvesplan-to-issue-company-stock-via-the-bitcoinblockchain/>

19. <http://www.coindesk.com/german-central-bankblockchain-trading/>

20. <http://www.coindesk.com/korea-exchangelaunches-blockchain-powered-private-marketservice/>

21. <http://www.forbes.com/sites/laurashin/2017/01/09/dtcc-selects-partnersfor-blockchain-solution-for-credit-defaultswaps/#1ebe0994ad88>

22. La identidad se convierte en un token, que se puede afirmar según sea necesario y el registro de validación de identidad se almacena también en el DL.

23. Sobre la base del análisis de los precios de las remesas registrados en la base de datos de precios de las remesas del Banco Mundial (remittanceprices.worldbank.org), en una serie de corredores.

24. <https://ripple.com/insights/several-global-banksjoin-ripples-growing-network/>

25. <https://www.bitpesa.co/blog/connectingpayments-with-africa-and-china/>

26. Global Findex 2014, World Bank

27. <http://www-03.ibm.com/press/us/en/pressrelease/51054.wss>

28. Esto significa en la práctica que los activos se gestionarán en un sistema de cadena de bloques cerrado, por lo que ninguna transacción individual será identificable, pero los datos en el sistema cerrado se estamparán en una cadena de bloques pública, es decir, Bitcoin, haciendo que cualquier cambio fraudulento sea visible públicamente.

29. <https://www.ubitquity.io/home/resources/worldbank_land_paper_ubitquity_march_2016.Pdf>

30. <http://media.everledger.io/wp-content/uploads/2016/09/Everledger_OnePager_2016-1.pdf>

31. <http://www.bis.org/cpmi/publ/d137.htm>

32. Autonomous Research LLP, “Block Chain: Backoffice Block Buster”. <https://www.autonomous.com/fintech/d9335db1-bf1a-4ab2-8d1d-a36cb747a6ae>

33. Nick Szabo, “The Idea of Smart Contracts” (1997) <http://szabo.best.vwh.net/smart_contracts_idea.html>

34. CoinDesk, “Understanding The DAO Attack”, by David Siegel, 25 June 2016. <https://www.coindesk.com/understanding-dao-hackjournalists/>

35. CoinDesk, "CoinDesk Research: Ethereum Hard Fork Had Little Impact on Sentiment". A cargo de Bradley Miles. 17 de noviembre de 2016.

<https://www.coindesk.com/coindesk-research-spotlight-studyq3-ethereum-hard-fork/>

36. Oficina del Gobierno del Reino Unido para la Ciencia. "Tecnología de contabilidad distribuida: más allá de blockchain". Un informe del Asesor Científico Jefe del Gobierno del Reino Unido. 19 de enero de 2016.

<https://www.gov.uk/government/publications/distributed-ledgertechnology-blackett-review>

37. Financial Times, "Los bancos centrales explorarán blockchain para crear monedas digitales". A cargo de Jane Wild. 02 de noviembre de 2016.

<https://www.ft.com/content/f15d3ab6-750d-11e6-bf48-b372cdb1043a>

38. Documento de trabajo n.º 605 de los servicios del Personal del Banco de Inglaterra, «Macroeconomía de las monedas digitales emitidas por el banco central», julio de 2016. <http://www.bankofengland.co.uk/research/Documents/workingpapers/2016/swp605.pdf>

39. <http://www.coindesk.com/uganda-africa-firststeps-bitcoin-blockchain-regulation/>

40. <http://www.coindesk.com/australia-digitalcurrency-self-regulation/>

41. <http://www.imf.org/external/pubs/cat/longres.aspx?sk=43618>

42. <http://www.bis.org/cpmi/publ/d137.htm>

43. <http://www.bis.org/cpmi/publ/d157.htm>

44. <https://ripple.com/insights/several-global-banksjoin-ripples-growing-network/>

45. <https://www.chemonics.com/news/blockchaintransforming-development/>

46. <http://www.dfs.ny.gov/legal/regulations/bitlicense_reg_framework.htm>

47. <http://legis.delaware.gov/BillDetail?LegislationId=25730>

48. <http://www.bankofengland.co.uk/markets/Pages/paymentsystem/strategy.aspx>

49. El WBG Blockchain Lab se lanzó en junio de 2017 como una incubadora para el aprendizaje, la experimentación y el intercambio de conocimientos sobre tecnologías de contabilidad distribuida (DLT). El Laboratorio se está asociando con compañías líderes en tecnología, nuevas empresas, empresarios, innovadores y organizaciones de desarrollo para experimentar, desarrollar y desplegar soluciones habilitadas para blockchain para el negocio y sus diversos desafíos de desarrollo. El laboratorio tiene un mandato transversal y ha identificado cuatro vías prioritarias de trabajo: Tecnología, Seguridad, Regulación y Política, y Aprendizaje e Intercambio de Conocimientos. La Práctica Global de Finanzas y Mercados está trabajando actualmente en una serie de casos de uso con el Laboratorio, incluidas las remesas transfronterizas.

50. En un proceso de contratación pública de 2 etapas, en la primera etapa se invitan propuestas sin restricciones específicas sobre los enfoques de solución, y en la segunda etapa se elige un enfoque de solución específico y se invita a presentar ofertas para este enfoque específico.

51. <https://themerkle.com/what-is-ethereumsmetropolis-hard-fork/>

52. CoinDesk, "Understanding The DAO Attack", por David Siegel, 25 de junio de 2016. <https://www.coindesk.com/understanding-dao-hackjournalists/>

53. <https://qz.com/730004/everything-you-need-toknow-about-the-ethereum-hard-fork/>

54. Una línea de tiempo útil de eventos relacionados con Ethereum y la bifurcación en respuesta al hackeo de DAO está disponible en el sitio web de Ethereum Classic: <https://ethereumclassic.github.io/>

55. <https://blog.ethereum.org/2016/06/17/criticalupdate-re-dao-vulnerability/>

56. <https://blog.ethereum.org/2016/09/22/ethereumnetwork-currently-undergoing-dos-attack/>

57. <https://news.bitcoin.com/ethereum-plans-hardfork-twice/>

58. <https://blog.ethereum.org/2016/11/18/hard-forkno-4-spurious-dragon/>

59. <https://blog.ethereum.org/2016/11/18/hard-forkno-4-spurious-dragon/>

60. <https://bitcoinmagazine.com/articles/op-edwhy-ethereums-hard-fork-will-cause-problemscoming-year/>

61. <https://www.ethnews.com/ethereums-road-mapfor-2017>

