ASOCIACIÓN ESPAÑOLA DE BANCA

DLT (BLOCKCHAIN)

La *Distributed Ledger Technology* (DLT) o tecnología de registro distribuido es una base de datos digitales replicados, compartidos y sincronizados, distribuidos geográficamente a través de múltiples sitios, países y /o instituciones.

La DLT es, esencialmente, un registro de propiedad de activos virtual mantenido en forma descentralizada, en el que las transacciones y los cambios de propiedad se realizan y verifican por medio de criptografía, permitiendo la realización de transacciones entre dos partes de manera segura, sin que sea necesario que intervenga una autoridad central o terceras partes que las verifiquen, ya que el propio sistema es el encargado de ello, a través de sus nodos[1].

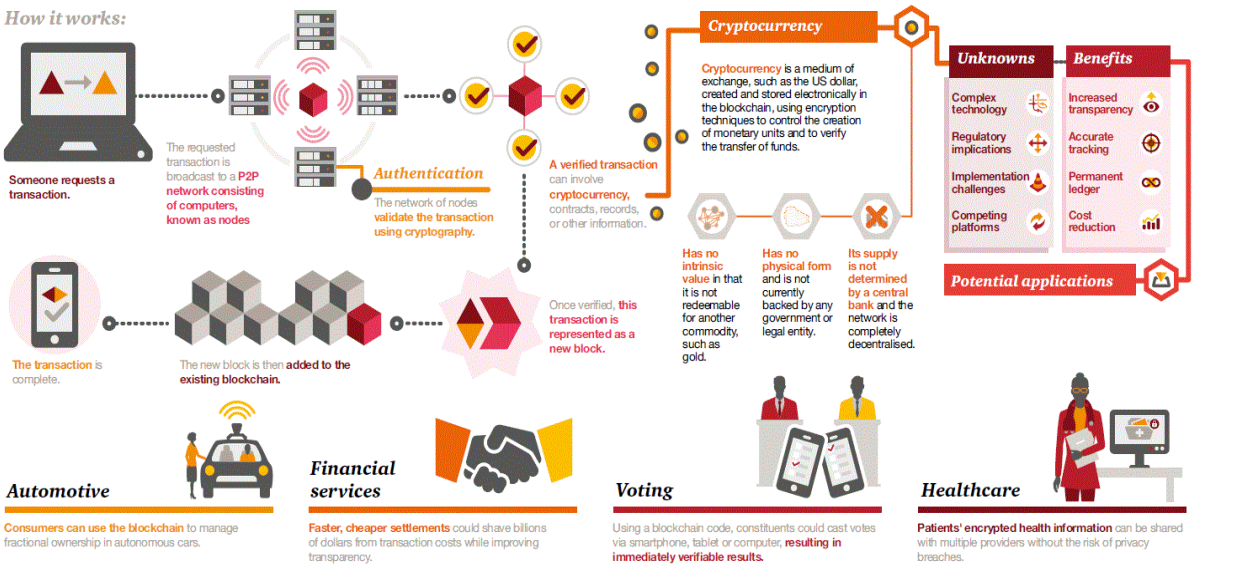
Todos los participantes pueden tener su propia copia idéntica de la base de datos. Cualquier cambio en ella se refleja en todas las copias en minutos, o en algunos casos en segundos. Los activos registrados pueden ser financieros, legales, físicos o electrónicos. Toda la información en el registro se almacena de forma segura y precisa mediante criptografía y se puede acceder mediante claves y firmas criptográficas. Una vez que la información se almacena, se convierte en una base de datos inmutable y se rige por las reglas de la red. Mientras que los registros centralizados son propensos a ataques cibernéticos, los distribuidos son intrínsecamente más difíciles de *hackear* porque todas las copias distribuidas deben ser atacadas simultáneamente para que un ataque tenga éxito. Además, estos registros son resistentes a los cambios perniciosos por una sola parte.

Aunque esta tecnología puede resultar en una pérdida de valor para las entidades financieras tradicionales y su labor de intermediación fiduciaria, su potencial de utilización en muchas áreas financieras -pagos internacionales (no SEPA), préstamos sindicados, actividades post-trade (compensación y pagos) y custodia, o para obligaciones de reporting y cumpliento - está incentivando la investigación de su uso por las mismas.

Aún es prematuro conocer con precisión cuáles serán las futuras aplicaciones prácticas de este tipo de tecnología en el sistema financiero. No obstante, en general se estima que la DLT, que funcionaría como un notario público, podría permitir reducir costes y ganar eficiencia a la hora de tramitar operaciones y registrarlas.

Subyacente a esta tecnología está la tecnología *blockchain* o de "cadena de bloque", que fue inventada para crear la moneda digital Bitcoin en 2008. Los algoritmos de cadena de bloque permiten que las transacciones de Bitcoin se agreguen en bloques y éstas se añadan a un 'cadena' de bloques existentes almacenados de forma lineal y utilizando una firma criptográfica. Es decir, el blockchain es un tipo de DLT, compuesto de datos digitales inalterables grabados en paquetes llamados "bloques".

[1] Los nodos son cada uno de los participantes en un libro distribuido. Los diferentes nodos pueden tener diferentes derechos para leer, escribir y / o eliminar datos.



Tipos de DLT:

- **Permissionless ledgers** (registros o libros sin permiso): Es una DLT sin propietario único, como la utilizada en Bitcoin. Estos ledgers descentralizados públicos son accesibles para todos los usuarios de Internet. Esto permite que cualquier persona aporte datos y que todos tengan exactamente la misma copia del registro, de tal manera que nadie puede impedir que se agreguen transacciones.
  El objetivo del diseño público, aparentemente, es evitar la censura (por una autoridad central), eliminar la exposición de contraparte y permitir una participación abierta y global.

- **Permissioned ledgers**: Existen dos tipos de ledgers con permiso: públicos y privados. Son registros o libros con uno o muchos propietarios, donde un número limitado de participantes tienen el poder de aprobar los datos nuevos que se van añadiendo.

  - En el caso de los ***permissioned private ledgers*** (ledgers privados autorizados), sólo las entidades autorizadas pueden leer el contenido del ledger y escribir en el ledger; por ejemplo, Corda de R3. Los ledgers privados autorizados pueden tener uno o muchos propietarios. Cuando se agrega un nuevo registro, se comprueba la integridad del libro mayor mediante un proceso de consenso limitado. Esto es llevado a cabo por agentes de confianza como departamentos gubernamentales o bancos. Este proceso hace que la entrada y verificación de datos sea más rápida y eficiente cuando se compara con el proceso de consenso de libros libres de permisos. Además, el uso de firmas digitales por nodos en la cadena también crea conjuntos de datos altamente verificables.
  - En los ***permissioned public ledgers*** (ledgers públicos autorizados), sólo las entidades autorizadas pueden escribir en el ledger, pero cualquiera puede ver el contenido del libro mayor, por ejemplo, Ripple. Un ledger autorizado puede tener algunos aspectos 'sin permiso' en circunstancias donde las entidades 'no autorizadas' pueden tener acceso restringido para ver conjuntos de datos parciales. Sin embargo, invariablemente no tendrán derechos de edición en ese blockchain.

Smart contracts*: Los contratos basados en la tecnología *Blockachain

Las bases de datos distribuidas (DLT), de las que *blockchain* es una tipología concreta, garantizan que todo el mundo tenga acceso y pueda ver la misma información, sin necesidad de que exista un intermediario de confianza. Estas plataformas se han posicionado como las más adecuadas para los *smart contracts* (contratos inteligentes) debido a que no se puede falsificar nada de lo que hay en *blockchain*.

Los contratos inteligentes son contratos cuyos términos se registran en un lenguaje de ordenador en lugar de en un documento impreso con lenguaje jurídico. Pueden ser diseñados para promulgar contratos legales o regulaciones. Los contratos inteligentes pueden ser automáticamente ejecutados por un sistema informático en tiempo real. Sin embargo, estos contratos hay que considerarlos como una evolución del sistema legal y no una sustitución del mismo. El papel de los abogados no desparece con la aparición de estos contratos, sino que cambia y pasa de adjudicar contratos individuales a producir plantillas de *smart contracts* en un mercado competitivo.

Un *smart contract* puede ser creado por personas físicas y/o jurídicas, pero también por máquinas u otros programas que funcionan de manera autónoma. Un *smart contract* tiene validez, sin depender de autoridades, debido a su naturaleza: es un código visible por todos y que no se puede cambiar al existir sobre la tecnología *blockchain*, la cual le da ese carácter descentralizado, inmutable y transparente. Es importante destacar que, al estar distribuido por miles de ordenadores, se evita así que una gran compañía los custodie, lo que elimina burocracia, censuras y elevados costes/tiempos implícitos.

Poco a poco van apareciendo nuevas implementaciones de los *smart contracts* en Bitcoin pero, actualmente, ya se aplica en algunas funcionalidades como los monederos multifirma, en los que dos partes o más deben aprobar la realización de una transacción antes de que los fondos sean liberados.

Cloud computing es un modelo de prestación de servicios de negocio y tecnología. La computación en la nube permite ofrecer servicios de procesamiento y almacenamiento de datos de forma masiva en un conjunto de servidores que alojan la información del usuario, a los que se puede acceder a través de internet en cualquier momento.

Atendiendo al documento elaborado por BBVA Research (link en documentos de interés), hay tres modalidades de servicio de *cloud computing*, en función de la capa de tecnología que se provea, y por tanto, del control que tenga el usuario final sobre la infraestructura tecnológica:

- *Infrastructure as a Service* (IaaS): modelo en el que se provisiona de sistemas hardware como el acceso a servidores, capacidad de cómputo, sistemas de almacenamiento o dispositivos de comunicaciones. El usuario tiene control total sobre los sistemas operativos, los aplicativos y las bases de datos que se ejecutan en el hardware suministrado. Por ejemplo, los servicios de *Amazon* o *Microsoft Azure*.

- *Platform as a Service* (PaaS): modelo en el que se suministra un entorno de desarrollo donde los programadores pueden generar, probar y/o ejecutar sus aplicaciones informáticas. En este modelo el proveedor ofrece el uso de su plataforma, que a su vez se encuentra alojada en sus infraestructuras. El usuario final tiene control sobre sus aplicaciones y en muchos casos sobre la configuración del entorno. Por ejemplo, el servicio de *Google App Engine* permite crear y alojar páginas web sobre la infraestructura de Google.

- *Software as a Service* (SaaS): modelo en el que se ofrecen aplicaciones finales que se alojan y ejecutan en una infraestructura física y de aplicación controlada por el proveedor (en la infraestructura *cloud*). La tecnología utilizada para proporcionar el servicio es totalmente transparente para el usuario, que sólo tiene acceso a un interfaz de aplicación para el procesamiento de la información. Por ejemplo, *Gmail, Dropbox, iCloud de Apple*, que son los servicios más conocidos por el consumidor final, pero también suites completas de gestión de ventas y marketing a clientes como *Salesforce*.

Dependiendo de cómo se presten los servicios de *cloud* hay distintos modelos de implantación:

- *Cloud pública*: los servicios están disponibles para cualquier usuario con acceso a internet. Normalmente, estos servicios los ofrecen empresas tecnológicas desde sus propios locales y los usuarios comparten la infraestructura del proveedor.
- *Cloud privada*: la infraestructura de *cloud* es para el uso exclusivo de un único usuario (u organización) que comprende múltiples consumidores. La infraestructura puede ser propiedad de la organización y estar gestionada por la misma, por terceros, o por una combinación de ambos. La instalación de la infraestructura puede estar dentro o fuera de las instalaciones del usuario.
- *Cloud híbrida*: combina los modelos de *cloud* pública y privada, de esta forma parte del servicio se ofrece de forma privada como podría ser la infraestructura y otra parte se ofrece de forma compartida, como las herramientas de desarrollo.

En los últimos años, se ha observado un creciente interés del sector bancario por la computación en la nube como medio para apoyar la digitalización sostenible del negocio. El almacenamiento en la nube permite eliminar los costes de adquisición y mantenimiento de invertir en la propia infraestructura de almacenamiento, aumentando así la eficiencia, incrementando la agilidad, y proporcionando a la organización una escala global.

Documentos de interés	
ESMA	Report: The Distributed Ledger Technology Applied to Securities Markets
Blockchain Technologies	Blockchain Technology Glossary
BBVA Research	Blockchain in financial services: Regulatory landscape and future challenges for its commercial application
CAPCO	Journal 44: Financial Technology
FMI	Virtual Currencies and Beyond: Initial Considerations
Blockchain revolution	http://blockchain-revolution.com/
BBVA Innnovation center	Blockchain Technology
PwC FinTEch	Q&A: What is blockchain?
Blog bit2me	Smart contracts, ¿Qué son, cómo funcionan y qué aportan?
BCE	Distributed Ledger Technology