



vector ITC
a Softtek Company

Blockchain:

disrupción, valor y seguridad.

Índice

01 **3 - 13**

Introducción.

02 **14 - 23**

Impacto del Blockchain.

03 **24 - 37**

Aplicaciones Sectoriales.

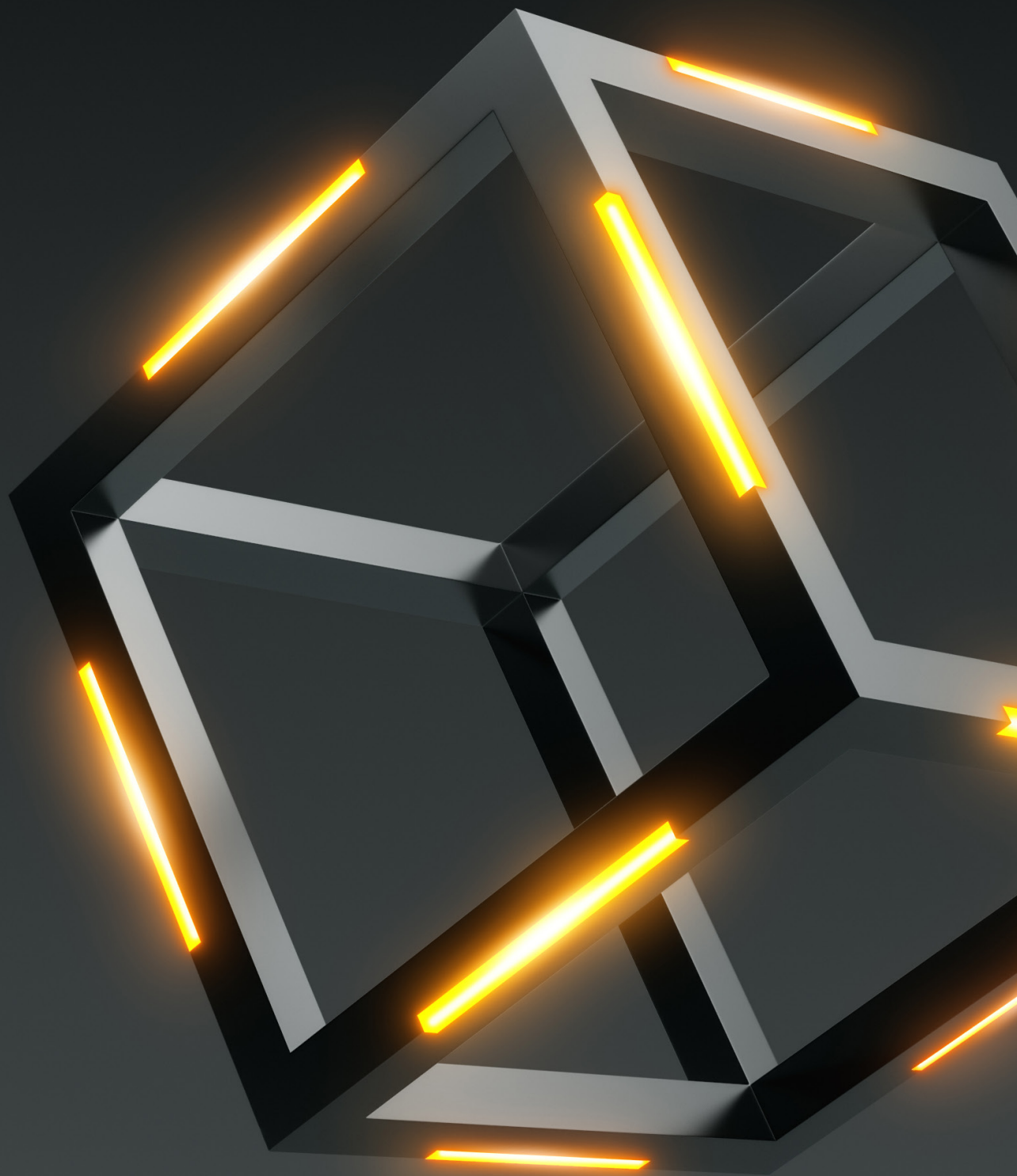
04 **38 - 43**

Tecnologías Blockchain.

05 **44 - 47**

Nuestras Conclusiones.





Introducción: ¿Qué es el Blockchain?

01

El Blockchain en su definición más básica es un libro de transacciones digitales. No obstante, esta definición varía y aumenta según se van añadiendo usos. Por lo que se podría definir como:

“Libro de contabilidad digital incorruptible de transacciones económicas que se puede programar para registrar no solo transacciones financieras sino prácticamente todo lo que tenga valor”.

Como toda tecnología novedosa, **tiene a su alrededor una serie de elementos y procesos** que ayudan a comprender mejor su funcionamiento y finalidad.



CONCEPTOS RELACIONADOS:

BITCOIN

La tecnología Blockchain se describió por primera vez en 1991 cuando Haber y Stornetta quisieron implementar un sistema donde las marcas de tiempo de los documentos no pudieran ser manipuladas.

Sin embargo, Blockchain surgió de las sombras durante la agitación financiera de 2008, en forma de un libro blanco titulado Bitcoin: un sistema de efectivo electrónico de igual a igual, que describía **cómo una cadena de bloques de datos digitalizados podía unirse para crear una nueva moneda digital**. El documento fue escrito por una fuente anónima que permanece sin identificar, bajo el seudónimo de Satoshi Nakamoto.

Bitcoin es una forma de moneda digital, a menudo llamada criptomoneda, que se crea al resolver una serie de complejos acertijos matemáticos (minería), que conducen a la recompensa de **una "moneda" que tiene un valor monetario fuera del sistema financiero tradicional**.

Una vez que se crea, el Bitcoin resultante puede transferirse con o sin una autoridad central, transferirse a través de un intercambio o entre pares. **Cualquier transacción con Bitcoin es rastreada por la red de usuarios a lo largo de una cadena de bloques.**

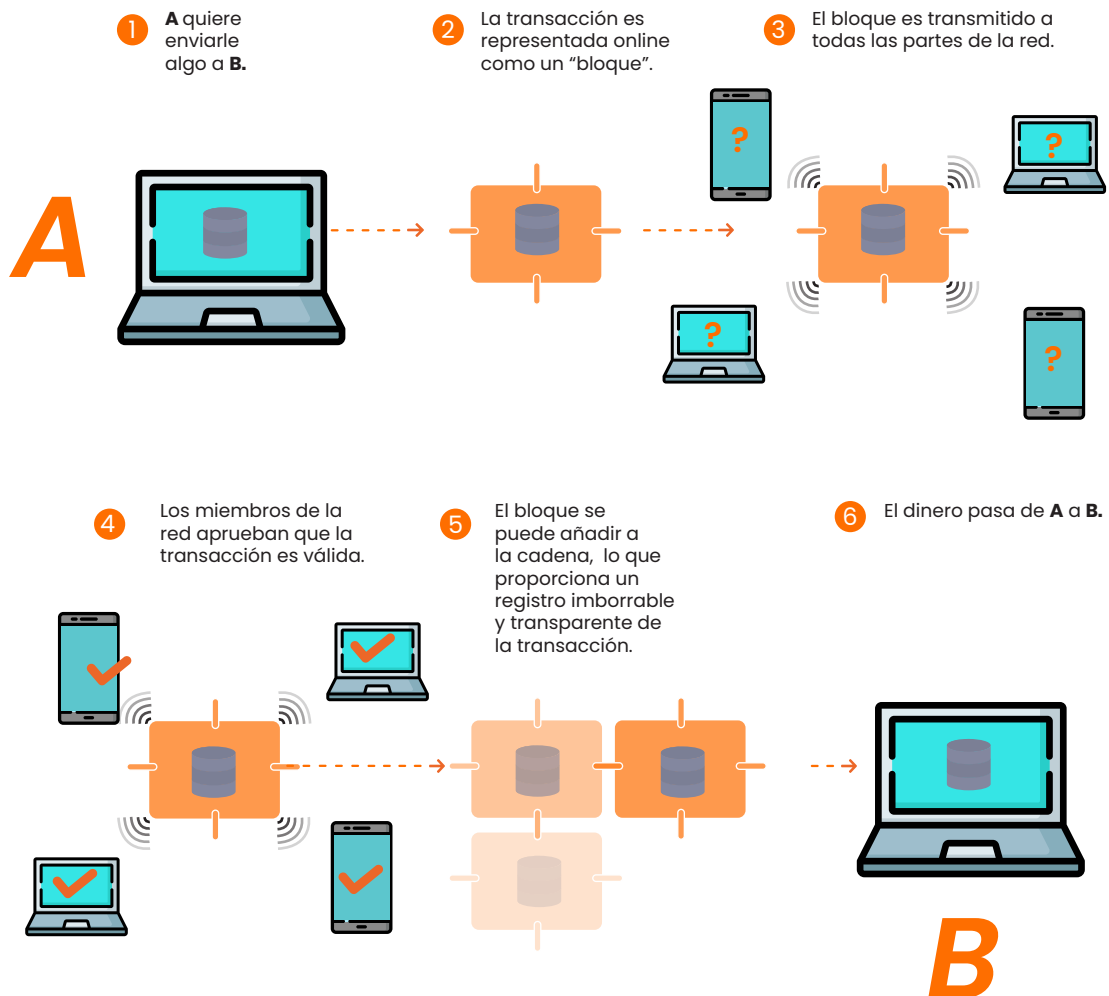


BLOQUE

Como se ha mencionado anteriormente, Blockchain es un registro electrónico de transacciones. Esos registros o transacciones, cada uno de los cuales tiene una marca de tiempo y están vinculados a un usuario, se llaman "bloques". **Cada bloque se crea cronológicamente y está vinculado al bloque anterior.**

Cada bloque es una transacción registrada, que se comparte en una red de igual a igual que consta de nodos. Un nodo es un dispositivo, como una computadora, que contiene un historial de todas las transacciones para una cadena de bloques en particular, es decir, todos los bloques de esa cadena.

Para poder agregar un nuevo bloque a la cadena, todos los nodos de la red deben verificarlo. Una vez que se agrega a la cadena, la información no se puede modificar ni eliminar, creando un registro confiable y transparente de información transaccional.



CRIPTOGRAFÍA

La criptografía abarca todos los métodos de cifrado matemático (o códigos) que se utilizan para **proteger o “encriptar” las transacciones de terceros a medida que las transacciones se almacenan o** comparten.

Estos métodos permiten al Blockchain **verificar a los remitentes en una red a través de firmas**, así como garantizar que las transacciones y los “bloques”, no se puedan cambiar. A su vez, Blockchain también utiliza algoritmos de hash para asignar un hash único a cada bloque, lo que le permite distinguir entre bloques.

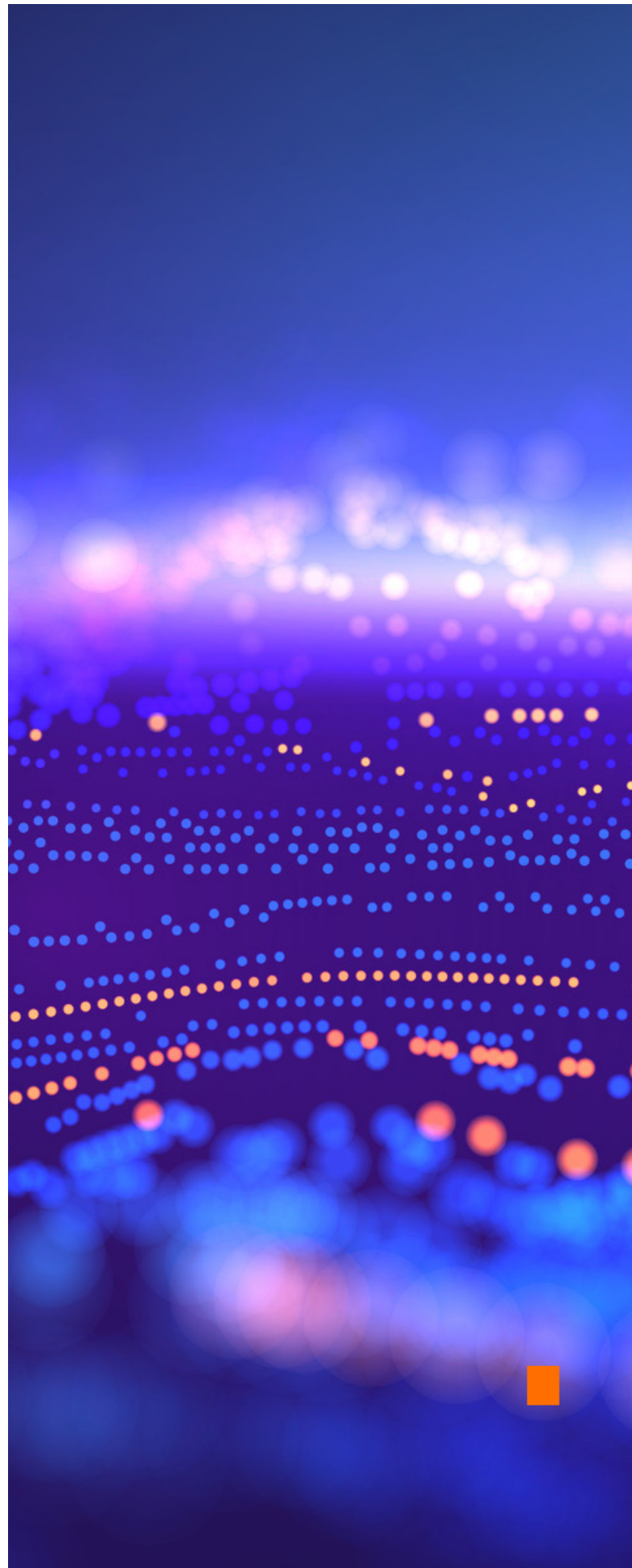
PROOF OF WORK

Dentro de todo el proceso, la Prueba de Trabajo (Proof of Work) es el primer algoritmo de consenso introducido en la red Blockchain. Se utiliza por varias tecnologías para **validar las transacciones y agregar bloques relevantes a la cadena de una red**. Contiene toda la información relacionada con los bloques, por lo que es esencial cuidar todos los bloques transaccionales.

Los mineros deben de administrar los bloques de transacciones que se pueden crear con el proceso de minería. **El concepto detrás de esta técnica es resolver problemas matemáticos complicados y proporcionar una solución**. Dado que requiere una gran cantidad de poder computacional para resolverlos, la Prueba de Trabajo tiene ciertas limitaciones. Cuanto más crece una red, más potencia se requiere.

Los mineros tienen que resolver los acertijos para crear nuevos bloques y confirmar las transacciones.

La complejidad de un rompecabezas depende del número máximo de usuarios, la carga general y la potencia actual mínima de la red.



DLT Y BLOCKCHAIN

Es habitual confundir Blockchain y Tecnología de Contabilidad Distribuida (DLT):

Generalmente ambos se refieren a un registro de información que se distribuye a través de una red, a la vez que fomentan un mayor grado de transparencia y apertura que el que habían permitido las bases de datos centralizadas anteriores o los registros digitales. Sin embargo, aquí terminan las analogías, ya que cada tecnología tiene sus propias características distintivas importantes.

¿Qué es la Contabilidad Distribuida?:

Es una base de datos descentralizada, distribuida en varios ordenadores o nodos. Cada nodo mantendrá el libro y si ocurre algún cambio en los datos, el libro se actualizará de forma independiente en cada nodo.

¿Qué es Blockchain?:

Es una de las tecnologías de libro distribuido donde cada nodo obtiene su propia copia del libro. Cada vez que alguien añade una nueva transacción, se actualizan todas las copias del libro. Se puede considerar que el DLT es la tecnología madre de Blockchain.

DLT vs. Blockchain:

El Blockchain es una clase de DLT. Sin embargo, no se puede llamar Blockchain a cada DLT.



ESTRUCTURA EN BLOQUES: Blockchain representa los datos como una cadena de bloques. Esta estructura no es la de datos real de los ledgers distribuidos. Un ledger distribuido es una base de datos repartida en diferentes nodos. Sin embargo, estos datos pueden representarse de diferentes maneras.



SECUENCIA: En la tecnología Blockchain, se pueden encontrar todos los bloques en una secuencia determinada. Los ledgers distribuidos no necesitan seguir la secuencia de datos de la cadena de bloques. Otros DLTs tienen un tipo diferente de secuencia de datos; depende de la tecnología.



CONSENSO SOBRE EL ANSIA DE PODER: En la mayoría de los casos hay un amplio uso del mecanismo de Prueba de Trabajo en el Blockchain. Sin embargo, también hay otros mecanismos, pero al final, también asumen el poder. Pero el ledger distribuido no necesita este tipo de consenso, así que en resumen, son comparativamente más escalables.



PUESTA EN MARCHA: Muchas empresas e instituciones gubernamentales están realmente utilizando la tecnología Blockchain, pero los proyectos o el uso de DLT todavía están en desarrollo. Por lo tanto, no tiene implementaciones en la vida real.



TOKENS: En una tecnología de ledger distribuido no es necesario tener tokens o cualquier tipo de moneda en la red. Pero muchas plataformas de Blockchain tienen algún tipo de economía simbólica. Sin embargo, la tecnología moderna de la cadena de bloques está tratando de salir de la sombra de la criptomoneda.

El Blockchain es solamente un tipo de libro mayor distribuido. Lo que significa que se puede considerar al DLT como la tecnología principal de Blockchain. Por otro lado, también se pueden encontrar diferencias en el funcionamiento de un libro mayor distribuido. Por ejemplo, **en el caso del DLT, un consenso es esencial.** En cambio, en el Blockchain, los desarrolladores pueden utilizar múltiples métodos para lograr un consenso entre los que se incluyen la Prueba de Participación (PoS) y la Prueba de Trabajo (PoW), como se ha visto anteriormente.

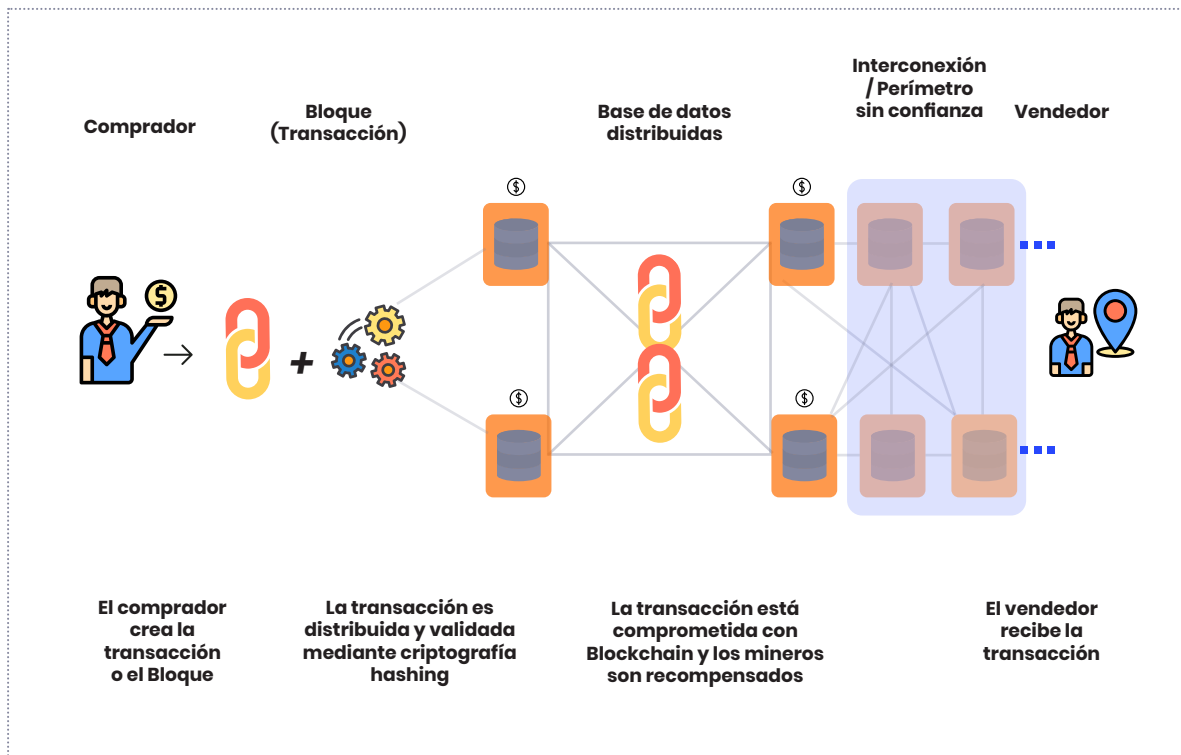
TIPOS DE BLOCKCHAIN

Hasta ahora se ha hablado de Blockchain como si fuera una tecnología con un único registro, sin embargo, nada más lejos de la realidad, pues **actualmente existen principalmente tres tipos de Blockchain.**

BLOCKCHAIN PÚBLICO:

Las redes de Blockchain públicas son de código abierto y se diferencian porque permiten que cualquier persona participe como usuario, minero, desarrollador o miembro de la comunidad.

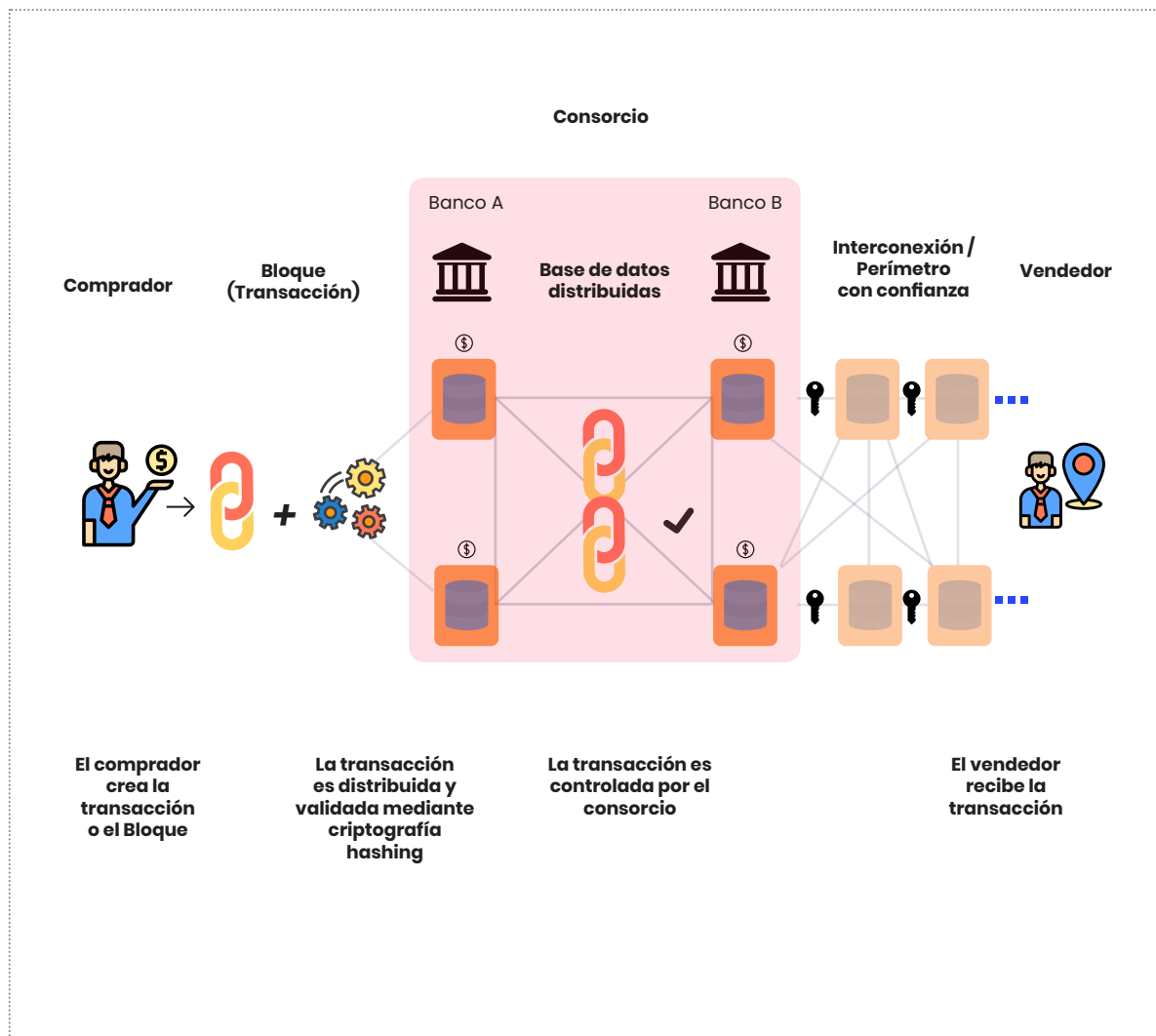
- Todas las transacciones que tienen lugar son totalmente transparentes, lo que significa que cualquiera puede examinar los detalles de la transacción.
- Está diseñada para estar completamente descentralizada, sin que ningún individuo o entidad controle qué transacciones se registran o el orden en que se procesan.
- Puede ser altamente resistente a la censura, ya que cualquiera está abierto a unirse a la red, independientemente de su ubicación, nacionalidad, etc. Esto hace que sea extremadamente difícil para las autoridades cerrarla.
- Toda red pública tiene un token asociado con ellas que generalmente está diseñado para incentivar y recompensar a los participantes en la red.



BLOCKCHAIN PRIVADO:

Otro tipo de cadenas son las cadenas de bloques privadas, también conocidas como cadenas de bloques autorizadas, que poseen una serie de diferencias notables con respecto a las cadenas de bloques públicas.

- Los participantes necesitan consentimiento para unirse a las redes.
- Las transacciones son privadas y solo están disponibles para los participantes del ecosistema que tienen permiso para unirse a la red.
- Pueden tener o no una ficha relacionada con la cadena.
- Están más centralizadas que las redes de Blockchain públicas.
- Las cadenas de bloques privadas son valiosas para las empresas que desean colaborar y compartir datos, pero no quieren que sus datos comerciales confidenciales sean visibles en una cadena de bloques pública.



BLOCKCHAIN HÍBRIDO:

La red Blockchain híbrida, es una combinación de los extremos de Blockchains públicos y privados y aprovecha las características de ambos. Al utilizar una solución híbrida de Blockchain, los miembros de la red o las entidades dominantes pueden decidir qué transacciones pueden seguir siendo públicas y cuáles estarán abiertas a un grupo más pequeño de miembros.

La cadena de bloques híbrida que consta del estado público y privado de la red garantiza que las transacciones sean privadas pero verificables utilizando un historial inmutable en la cadena de bloques pública. Cada transacción deberá ser verificada por una red masiva y, por lo general, es confiable y segura.

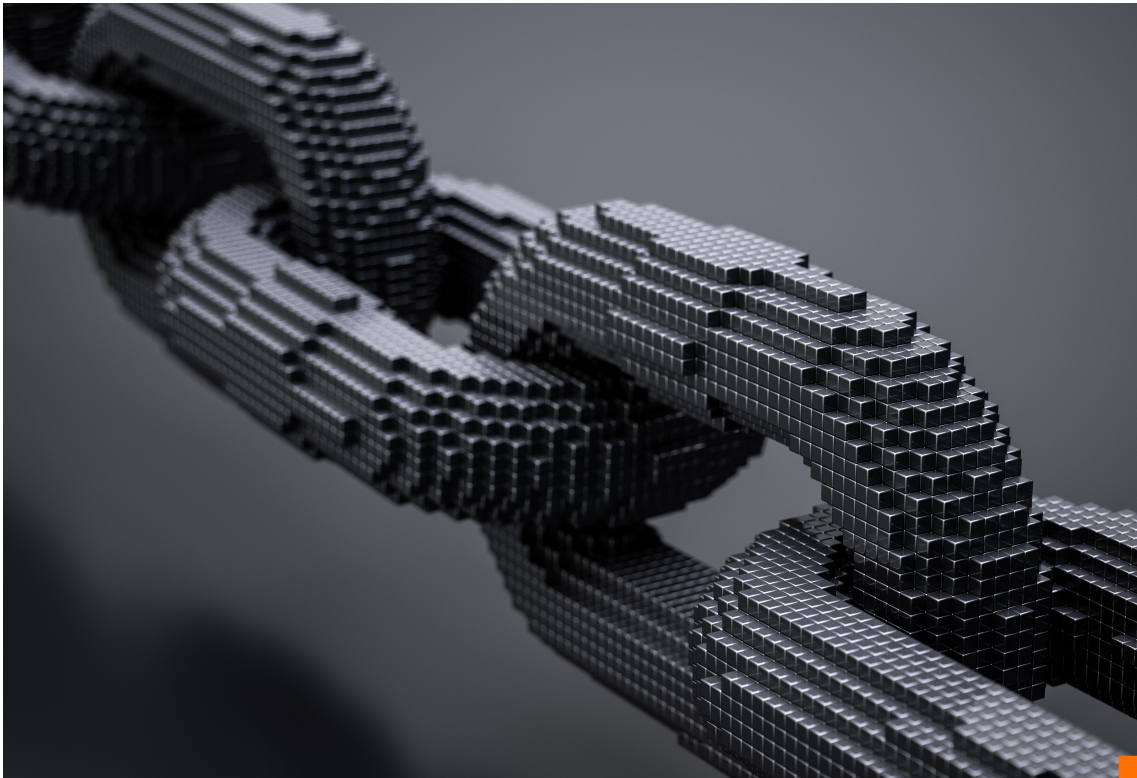
Por lo tanto, no requiere una entidad central de gobierno o una compleja cadena de intermediarios para controlar las cosas. Cualquier alteración de una transacción deberá realizarse bajo un proceso de verificación innato, lo que hace extremadamente difícil que una sola entidad manipule la transacción o las entradas.

Los participantes tienen los mismos derechos para ver, editar y agregar su permiso a una transacción, sin embargo, la identidad de las partes involucradas en la transacción nunca se revela a otras partes de la red.

La visibilidad ilimitada del estado público de la red descubre todos los datos en una red masiva, un rasgo que no cumple con las obligaciones de confidencialidad de los datos.

Este tipo de Blockchain puede ayudar a construir herramientas a nivel empresarial de la tecnología de código abierto. Además, la sólida seguridad permite su uso en pagos transfronterizos confiables para financiación y comercio.

Las aplicaciones industriales son otro aspecto en el que la cadena de bloques híbrida puede desempeñar un papel crucial, como viajes, energía, aviación, etc.



BLOCKCHAIN AS A SERVICE

Dada la popularidad que ha generado el Blockchain en todos los sectores empresariales, ha surgido un nuevo tipo de mercado, el Blockchain as a Service (BaaS). **Se trata de una parte importante de la economía Blockchain** y está contribuyendo al desarrollo de la tecnología.

Los modelos de BaaS **han logrado que el desarrollo de Blockchain sea más simple y seguro para las organizaciones** cuyas competencias centrales se encuentran alejadas del sector IT. El uso de este nuevo modelo puede ayudar a las compañías a enfocarse más en sus áreas centrales mientras se preocupan menos por el espacio de desarrollo.



¿Qué es BaaS?

Un producto único donde los consumidores pueden usar una solución de base Cloud para desarrollar, usar y alojar sus soluciones, funciones y Smart Contracts Blockchain. Ofrecen plataformas de Blockchain totalmente funcionales de acuerdo a sus necesidades.



¿Cómo funciona BaaS?

Los proveedores de BaaS configurarán la implementación de Blockchain, pero se les deberá de pagar una cuota. Por lo tanto, para pagar el BaaS, estarás pagando al proveedor de BaaS para desplegar y mantener tus nodos de Blockchain en lugar de los mismos.

Se trata de un modelo único que permite a los consumidores utilizar los servicios basados en la nube para desarrollar, usar y alojar sus aplicaciones, funciones y contratos inteligentes.

¿Cómo elegir una plataforma de BaaS?



Rápido aprovisionamiento

El rápido aprovisionamiento es en realidad la capacidad de desarrollar cualquier red de Blockchain con bastante rapidez y sin problemas.



Servicios Backend

Toda empresa necesita servicios backend y los proveedores de BaaS necesitan integrar el sistema con los servicios.



Plataformas IAM

El BaaS debería ofrecer medidas de seguridad con la integración de la gestión de identidades dentro de la plataforma.



Smart Contract

Los Smart Contracts son una parte esencial de cualquier solución de BaaS. Debes asegurarte de que tu proveedor de BaaS ofrece integración con Smart Contracts.



Clientes

Un proveedor de BaaS con una buena base de clientes es una señal de una buena calidad de servicio.



Diferentes frameworks y tiempos de ejecución

Elige un BaaS que ofrezca soporte para un conjunto diverso de frameworks y tiempos de ejecución.



Mecanismos de consenso basados en la identidad

Buscar soluciones de consenso para las bases de identidad, ya que toda empresa operará con identidades conocidas.



Blockchains autorizados

Los Blockchains autorizados son un imprescindible para un proveedor de BaaS, básicamente debido a la necesidad de privacidad.



Monitorización de bloques y herramientas de exploración

Necesitarás herramientas de monitorización y exploración para controlar el estado general de tu solución de BaaS.



Servicios Blockchain-First

Hay algunos servicios de Blockchain-First disponibles en el mercado, ofrecidos por proveedores de BaaS.



Transacciones privadas y canales estatales/locales

Tu compañía BaaS debería poder ofrecerte transacciones privadas e incluso canales locales/estatales.



Comunidad ejecutora

Una fuerte comunidad de implementadores dentro de un BaaS estructurará su desarrollo mucho más rápido.



Comunidad de desarrolladores

Si tu compañía de BaaS ofrece una buena comunidad de desarrolladores, es buena señal para contratarlos.



Innovación en Blockchain

La innovación propia puede ser un buen ejemplo de cualquier desarrollo de Blockchain.

Entre todas las virtudes que presenta BaaS se encuentran:

FLEXIBILIDAD Y EFICIENCIA

Ofrece una amplia gama de mecanismos de consenso. Dichos algoritmos de consenso pueden proporcionar la flexibilidad requerida en un ecosistema empresarial, la principal razón por la cual varias soluciones BaaS pueden procesar hasta 5.000 transacciones por segundo. Además, los proveedores de BaaS ofrecen otras herramientas como la unión dinámica, la administración de recursos físicos y los protocolos de conmutación para hacer que las soluciones sean eficientes.

PROTECCIÓN DE LA PRIVACIDAD Y SEGURIDAD

Permite **administrar niveles de permisos, nodos y claves** desde un solo panel de control. Todos los proveedores de BaaS ofrecen el panel de control para facilitar el acceso.

MAYOR RENTABILIDAD

Su coste es más bajo que construir una aplicación Blockchain desde cero. Usando las plataformas BaaS, **los usuarios pueden utilizar solo las funciones que específicamente necesitan**. Por lo tanto, solo será necesario invertir en las funciones que se están utilizando, y no en el marco completo.



02 Impacto del Blockchain

El Blockchain es una tecnología disruptiva que tiene la capacidad de aumentar la eficiencia del flujo de trabajo de cualquier industria, entre otros beneficios como:

DESCENTRALIZACIÓN Y CONFIANZA

Construido en un entorno de confianza, en el que las transacciones son realizadas de forma codificada y cifrada. Además, con la descentralización, si la información fuese interceptada y cayera en manos no deseadas, solo una pequeña cantidad de datos se vería comprometida.

TRANSPARENCIA

Los historiales de transacciones se están volviendo más transparentes. Debido a que Blockchain es un tipo de libro mayor distribuido, todos los participantes de la red comparten la misma documentación que las copias individuales. Esa versión compartida solo se puede actualizar a través del consenso, lo que significa que todos deben estar de acuerdo. Cambiar un solo registro de transacción requeriría la alteración de todos los registros posteriores y la colisión de toda la red. Por lo tanto, los datos en una cadena de bloques son más precisos, consistentes y transparentes, mejorando de esta manera la confianza de todos los usuarios. También está disponible para todos los participantes que tienen acceso autorizado.

DURABILIDAD, FIABILIDAD Y LONGEVIDAD

Es muy poco probable que se reviertan los bloques confirmados, lo que significa que una vez que los datos se han registrado en la cadena de bloques, es extremadamente difícil eliminarlos o cambiarlos. Esto hace que Blockchain sea una gran tecnología para almacenar registros financieros o cualquier otro dato donde se requiera un seguimiento de auditoría porque cada cambio se rastrea y se registra permanentemente en un libro mayor distribuido y público.

REDUCCIÓN DE COSTES DE TRANSACCIÓN

Con Blockchain, una empresa no necesita tantos intermediarios para garantizar las transacciones porque no importa si puede confiar en su socio comercial, ya que este ha sido previamente verificado. En cambio, solo tiene que confiar en los datos de la cadena de bloques. Tampoco tendrá que revisar tanta documentación para completar una operación porque todos tendrán acceso autorizado a una única versión inmutable. Se estima que aproximadamente el 70% del valor que aporta el Blockchain a una compañía es en reducción de costes, seguido de una mayor generación de ingresos.

ALTA DISPONIBILIDAD

Los datos de Blockchain son precisos, oportunos, completos, consistentes y de fácil acceso. Simplifica no solo el comercio, sino también acelera los procesos, aumenta la trazabilidad de su procedencia y facilita la disponibilidad de los registros, entre otras cosas.



TRANSACCIONES MÁS RÁPIDAS

Cuando se realizan procesos tradicionales, el comercio de cualquier bien es un proceso que conlleva mucho tiempo y que es propenso a errores humanos y que a menudo requiere la mediación de terceros. Al racionalizar y automatizar estos procesos con Blockchain, las transacciones se pueden completar de manera más rápida y eficiente.

Al tener todos acceso a la misma información, se hace más fácil confiar entre sí sin la necesidad de numerosos intermediarios: la compensación y la liquidación serán mucho más rápidas.

DATOS VERIFICADOS Y "ASEGURADOS"

En la mayoría de los sistemas de pago tradicionales, las transacciones no solo dependen de las dos partes involucradas, sino también de un intermediario, como un banco, una compañía de tarjetas de crédito o un proveedor de pagos. Cuando se usa la tecnología Blockchain, esto ya no es necesario porque la red distribuida de nodos verifica las transacciones a través de un proceso conocido como minería. Por lo tanto, un sistema Blockchain elimina el riesgo de confiar en una sola organización.

SIMPLIFICACIÓN DE LOS ECOSISTEMAS

Blockchain tiene el potencial de transformar la economía y las transacciones eliminando la duplicación de esfuerzos y procesos innecesarios, garantizando una mayor integridad de datos, simplificación de ecosistemas, empoderamiento de usuarios, y en general entregando un sistema más eficiente y seguro.

PRINCIPALES APLICACIONES

SMART CONTRACTS

El término 'contrato inteligente' se acuñó por primera vez en 1993, pero recientemente se ha convertido en un término de moda gracias al lanzamiento en 2013 del Proyecto Ethereum y se espera que para el 2020, el 70% de las instituciones financieras hayan adoptado este tipo de contratos.

El Proyecto Ethereum es una plataforma descentralizada que ejecuta contratos inteligentes: aplicaciones que se ejecutan exactamente como están programadas, sin posibilidad de tiempo de inactividad, censura, fraude o interferencia de terceros.

Los Smart Contracts son programas informáticos automáticos que pueden cumplir los términos de cualquier contrato, están basados en eventos futuros y códigos criptográficos, que se cumplirán siempre que se den las condiciones preestablecidas.

Por otro lado, también es importante destacar que este tipo de contratos pueden funcionar de forma independiente, pueden operar en una instancia única, pero también pueden ejecutarse junto con otros contratos inteligentes y la finalización exitosa de uno activará el comienzo de otro, y así sucesivamente.

Hasta el momento, los contratos inteligentes se han considerado potencialmente revolucionarios en una gran variedad de industrias, donde algunos profesionales afirman que reemplazarán a los contratos tradicionales.

Esta afirmación viene dada por la creencia de que todo acuerdo legal se expresa en su código. En general, los Smart Contracts se perciben como un código (no ley) utilizado para automatizar la ejecución de un acuerdo legal subyacente.

Como código programable, los contratos inteligentes son altamente personalizables y pueden diseñarse de muchas maneras diferentes, ofreciendo muchos tipos de servicios y soluciones. Como programas descentralizados y autoejecutables, pueden proporcionar una mayor transparencia y menores costes operativos. Dependiendo de la implementación, también pueden aumentar la eficiencia y reducir los gastos burocráticos.

Pueden diseñarse para una amplia variedad de casos de uso incluyendo la creación de activos tokenizados, sistemas de votación, billeteras criptográficas, intercambios descentralizados, juegos y aplicaciones móviles, etc. También se pueden implementar junto con otras soluciones de Blockchain que abordan los campos de la salud, la cadena de suministro, la gobernanza y las finanzas descentralizadas (DeFi).



GESTIÓN DE IDENTIDAD DIGITAL

Cuando se habla de aprovechar la tecnología Blockchain para la gestión de identidad, es importante tener en cuenta que hay **tres actores diferentes en juego: propietarios de identidad, emisores de identidad y verificadores de identidad.**

El emisor de identidad puede emitir credenciales personales para un usuario. Al emitir una credencial, el emisor de identidad da fe de la validez de los datos personales en esa credencial (por ejemplo, apellido y fecha de nacimiento). El propietario de la identidad puede almacenar esas credenciales en su billetera de identidad personal y usarlas más tarde para probar declaraciones sobre su identidad a un tercero (el verificador).

Las credenciales son emitidas por terceros que dan fe de la validez de los datos dentro de la credencial. La utilidad y confiabilidad de una credencial depende completamente de la reputación / confiabilidad del emisor.

Así, a través de la infraestructura de una cadena de bloques, las partes verificadoras no necesitan constatar la validez de los datos reales en la prueba provista, sino que pueden usar la cadena de bloques para verificar la validez de la certificación.

Por ejemplo, cuando el propietario de una identidad presenta una prueba de su fecha de nacimiento, en lugar de verificar la verdad de la fecha de nacimiento, la parte que verifica validará la firma del usuario que emitió y certificó esta credencial para luego decidir si él confía en la evaluación del emisor sobre la precisión de los datos. Por lo tanto, la validación de una prueba se basa en el juicio del verificador sobre la confiabilidad del certificador.

De este modo, es posible aprovechar Blockchain para garantizar la autenticidad de los datos y las declaraciones, sin almacenar realmente ningún dato personal en la cadena de bloques. Esto es crucial, ya que un libro mayor distribuido es inmutable, por lo que es recomendable no añadir datos personales o altamente confidenciales que no se puedan eliminar en un futuro.

Ante esta situación, la privacidad puede garantizarse mediante principios de no correlación. En lugar de almacenar información privada real, se almacena otro tipo de información como los identificadores descentralizados públicos (DID públicos) y los objetos descriptores DID asociados (DDO).

Los DID son un nuevo tipo de identificadores únicos para verificar identidades digitales, y están totalmente controlados por el propietario de la identidad. Los DID son independientes de registros centralizados, autoridades o proveedores de identidad.

Este tipo de identificadores no deben ser reasignables sino permanentes. Y a su vez deben poder resolverse, con un documento DID que establece las claves públicas, protocolos de autenticación y puntos finales de servicio necesarios para iniciar interacciones confiables con la entidad identificada.

Por otro lado, deben de ser criptográficamente verificables y estar descentralizados. Gracias a todas estas características, los identificadores descentralizados mejoran la seguridad, ya que le dan al propietario de la identidad la oportunidad de revelar selectivamente información específica sobre sí mismo. En última instancia, convertirán las identidades digitales en identidades soberanas, ya que permiten a cada individuo poseer y controlar su identidad sin depender de otras partes.





SEGUIMIENTO DE LA CADENA DE SUMINISTRO / TRAZABILIDAD

La naturaleza descentralizada de la tecnología Blockchain permite que diferentes sectores estén interesados en utilizarla para registrar, informar y rastrear interacciones verificadas de manera eficiente.

La tecnología Blockchain funciona con la gestión de la cadena de suministro (SCM) para proporcionar un libro de contabilidad inmutable que permita mantener y transferir registros. **Esto facilita el seguimiento y la gestión del abastecimiento, fabricación, almacenamiento, transferencia y distribución de materias primas, materiales y productos.**

Cuando se combina con otras tecnologías como la Inteligencia Artificial o el Internet de las cosas, la cadena de bloques proporciona beneficios significativos para la SCM. Estos incluyen la transparencia y el acceso a los datos de la cadena de suministro, la resolución rápida de problemas de ineficiencias y desperdicio, el seguimiento y la autenticación en tiempo real, y el movimiento más rápido de los productos a través de la cadena de suministro.

No obstante, también se enfrenta a una serie de obstáculos. El principal desafío con el uso de Blockchain en la cadena de suministro es garantizar que las partes interesadas y las organizaciones registren datos de manera consistente y precisa. Es vital que el SCM requiera que todas las partes usen la misma plataforma integrada de Blockchain.

Además, la complejidad de Blockchain puede ser un desafío para muchas compañías. Idealmente, la integración de Blockchain debería ser transparente y desplegarse a través de plataformas fáciles de utilizar para una correcta adopción.

TRANSACCIONES ENTRE USUARIOS SIN INTERMEDIACIÓN

Antes de la aparición de la tecnología Blockchain, las transacciones digitales entre dos usuarios requerían que un tercero de confianza actuara como intermediario. Dado que Blockchain es un libro de contabilidad digital público, anónimo e inmutable, ayudará a introducir un nuevo modo de realizar transacciones que no dependen en absoluto de intermediarios.

Cuando se habla de eliminar intermediarios, no significa que las instituciones oficiales como bancos y organizaciones estatales desaparecerán, por el contrario, con esta tecnología se fortalecerán al facilitar el acceso a los datos que requieren. Blockchain va un poco más allá, ya que además de compartir información online, también permite intercambiar el valor sin la necesidad de la intermediación de una entidad que valide la transacción.

Otro ejemplo: en las compras online no se requiere intermediario, ya que el dinero se cobra directamente. También se puede aplicar para títulos de propiedad, certificados, archivos y cualquier activo digital. Los activos digitales se entienden como un recurso que está disponible en Internet, son de su propiedad y se utilizan. Se tratan como propiedades, ya que se pueden negociar para la venta, compra o licencia.

Sin embargo, algunos informes sugieren que no es probable que esto sea posible en todos los casos. En el ámbito del Bitcoin, la eliminación de intermediarios al 100% es real, pero fuera de él no siempre es viable, ya que lo que Blockchain no hace es permitir la integración con el mundo externo. Cuando una red Blockchain necesita interactuar con otras bases de datos, con otros aspectos del mundo externo, generalmente requiere un intermediario de algún tipo.

Blockchain puede ayudar a que el proceso de intermediación sea más eficiente. Incluso puede ayudar a minimizar la confianza requerida de los participantes del ecosistema. Sin embargo, es poco probable que los intermediarios desaparezcan por completo.

No obstante, lo que la tecnología Blockchain ayuda a facilitar es la automatización. **Esta tecnología permite la reconciliación de datos entre partes independientes que, en muchos casos, ni siquiera necesitan confiar entre sí.**

De esta manera, y debido a que Blockchain puede sincronizar datos en un número ilimitado de servidores en tiempo real, muchos de los procesos, desde la auditoría hasta la administración de la base de datos, pueden hacerse mucho más eficientes.

En definitiva, los ecosistemas de Blockchain sin permisos, como bitcoin, excluyen a los intermediarios dentro de esos sistemas. Sin embargo, hay muchas áreas (registros nacionales, sistemas de votación, plataformas comerciales, etc.) que probablemente continuarán requiriendo terceros.

Blockchain puede ayudar a reducir el papel de estos intermediarios y a alterar las relaciones de confianza previamente requeridas, pero es poco probable que las elimine por completo.



CONSECUENCIAS

Como se ha podido ver hasta ahora, la tecnología Blockchain cuenta con una larga lista de beneficios, sin embargo, también se enfrenta a grandes desafíos, como la dificultad para encajar en los ordenamientos jurídicos actuales.

Ante la rápida evolución y adopción de esta tecnología, se han dado una serie de situaciones a las que tanto las organizaciones gubernamentales como las empresas interesadas en la adopción han tenido que hacer frente.

ADAPTACIÓN DEL ENTORNO REGULATORIO.

La falta de estándares comunes y regulaciones claras es una limitación importante en la escalabilidad de las aplicaciones Blockchain. Por norma general, los estándares se pueden establecer con relativa facilidad si hay un solo actor dominante o una agencia gubernamental que pueda exigir la posición legal. Sin embargo, cuando es necesaria la cooperación entre múltiples actores, establecer tales estándares se vuelve más complejo.

A nivel mundial, las instituciones encargadas de promulgar la legislación han tomado diferentes posiciones ante el Blockchain, pero la mayoría están comprometidas a permitir su expansión. Hasta ahora, muchos gobiernos están adoptando un enfoque regulatorio tecnológicamente neutral, sin promover ni prohibir usos específicos.

La desconfianza y la incertidumbre regulatoria son problemas que también afectan. Esta extrañeza se debe a que la primera cadena de bloques ampliamente adoptada, Bitcoin, fue creada expresamente para permitir transacciones financieras "sin depender de la confianza" o de los gobiernos que supervisan la moneda. No obstante, los usuarios siguen teniendo la sensación de vulnerabilidad.

Actualmente las redes Blockchain en sí mismas suelen ser muy seguras y eliminan la vulnerabilidad que entraña el hecho de que una sola empresa, controle las transacciones. Sin embargo, las cadenas de bloques identifican al propietario de una cuenta en función de su clave privada criptográfica, una cadena de números y letras de apariencia aleatoria, por lo que, si los delincuentes consiguen descifrar esa clave, todas las transacciones quedan al descubierto.

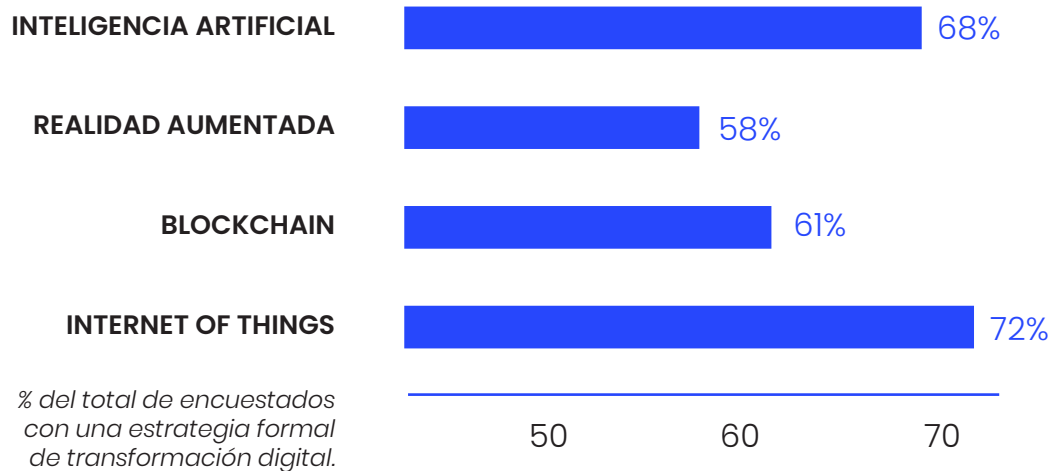
Ante esta situación, los reguladores están trabajando para equilibrar la flexibilidad para realizar transacciones de nuevas formas a través de criptomonedas con las garantías adecuadas. Aunque no todos toman la misma ruta, por ejemplo, en EEUU cada estado ha seguido un camino diferente: Nueva York adoptó requisitos de registro rígidos llamados BitLicense, mientras Wyoming inició una serie de proyectos de ley que aclaran el estado legal de las criptomonedas al tiempo que imponen protecciones mínimas.

Como cualquier sistema tecnológico, las cadenas de bloques combinan código de software y actividad humana. No es suficiente confiar totalmente en los ordenadores, que, después de todo, son dispositivos construidos y programados por personas. Para que la tecnología se utilice ampliamente y con prudencia, también debe haber mecanismos para responsabilizar a los humanos.

TRANSFORMACIONES EMPRESARIALES MÁS AMPLIAS.

Paralelamente a la creación de una legislación precisa sobre el uso del Blockchain, las empresas mejorarán su situación y obtendrán más facilidades para disfrutar de los beneficios que ofrece la tecnología, redefiniendo completamente sus estructuras de costes y ganando proximidad con sus clientes. Según los últimos informes el 61% de las empresas con estrategias formales de transformación digital, tienen en mente adoptar la tecnología Blockchain.

¿Su empresa invierte en esta tecnología como parte de su estrategia de transformación digital?



AUMENTO DE INTEGRACIÓN

Para las empresas cuyos casos de uso se vuelcan en la cadena de bloques, los beneficios potenciales de la integración serán más claros: más asociaciones dentro de un ecosistema que pueden generar más valor y aumentar el ROI.

Las organizaciones pueden aprovechar Blockchain para transformar los procesos comerciales existentes. Hasta ahora se han visto muchas mejoras tecnológicas, las cuales se centran en la integración del sistema en lugar de los aspectos de integración de aplicaciones.

Esta infraestructura de integración de primera generación permite las integraciones B2B mediante el intercambio de datos con formato EDI, por ejemplo, pero sin ningún conocimiento de los datos, ni del proceso comercial, de los que forman parte.

MEJORA DE PROCESOS

Si bien el intercambio de datos a través de protocolos y estándares comunes ayuda, los contratos de servicio no proporcionan información sobre los procesos comerciales ocultos detrás de los contratos y que se ejecutan en sistemas remotos. Esto hace que la tecnología Blockchain sea muy atractiva para implementar procesos comerciales distribuidos entre múltiples partes.

Con Blockchain, todas las entidades participantes comparten el mismo proceso comercial en forma de contratos inteligentes. Pero para validar las solicitudes, procesar y llegar a la misma conclusión, los procesos comerciales también necesitan el mismo estado, y eso se logra a través del libro mayor distribuido. Compartir todos los estados pasados de un contrato inteligente no es un objetivo en sí mismo, sino un requisito previo del tiempo de ejecución del proceso comercial compartido.

Visto desde este ángulo, Blockchain se puede ver como el siguiente paso en la evolución de la integración. **Las redes Blockchain actúan como un tipo de maquinaria distribuida de ESB y BPM que no están contenidas dentro de una sola entidad comercial, sino que abarcan múltiples organizaciones.** Con Blockchain, los modelos de datos comunes y ahora los procesos comerciales se están trasladando de las organizaciones a las redes comerciales compartidas. Algo para tener en cuenta es que este movimiento no es universalmente aplicable y no es probable que se convierta en un mecanismo de integración convencional.

Tal movimiento solo es posible cuando todos los participantes en la red tienen la misma comprensión de los modelos de datos y los procesos comerciales; por lo tanto, es aplicable solo en ciertas industrias donde los procesos pueden estandarizarse, como las finanzas, la cadena de suministro, la atención médica, etc.

AUMENTO DE DESCENTRALIZACIÓN

La inmutabilidad, la incapacidad de ser editado, es a la vez la mayor fortaleza de Blockchain y su mayor barrera para una adopción significativa. Las presiones del código inalterable pueden desalentar tanto a los desarrolladores como a los usuarios. Sin embargo, estas limitaciones se ven compensadas por otra característica de la tecnología Blockchain: la descentralización, que ofrece enormes beneficios.

Así, la imparcialidad de las reglas permanentes y universales y la transparencia del código y el comportamiento, combinados, crean seguridad. Sin embargo, en ocasiones Blockchain hace que el desarrollo ágil sea imposible y ralentiza a los equipos. Para compensar esta situación se plantea una descentralización progresiva en etapas.

Para ello se construirían mecanismos en contratos inteligentes que confieren poderes especiales a intermediarios, que posteriormente irían desapareciendo de manera gradual y transparente. La condición principal es que los mecanismos de bloqueo deben ser públicos e inmutables desde el principio. El intermediario no puede decidir modificar los términos más tarde y extender indefinidamente su poder.

La descentralización progresiva es realmente un paraguas que abarca muchas estrategias, mecanismos y herramientas para hacer que la construcción de Blockchain sea más viable. La mejor manera de aplicar la descentralización progresiva siempre dependerá del proyecto. Así las cosas, los contratos inteligentes son perfectos para estas tareas por su sencillez. Cómo, cuánto y cuándo incorporarlo es una decisión que debe tomarse tras evaluarse caso por caso.



Aplicación Sectorial

03

La importancia del Blockchain para las empresas está fuera de toda duda. Esta tecnología va a revolucionar muchos de los sectores productivos de la economía actual y, a medio plazo, **servirá de base para el impulso de nuevos modelos de negocio** en los que cambiará tanto en el funcionamiento interno, como las relaciones con los clientes.

El Blockchain es una tecnología que **puede ayudar a todos los sectores a afrontar el reto de la transformación digital** o, dicho de otro modo, a sobrevivir y tener un modelo de negocio digitalizado, sostenible y que genere beneficios en el mercado actual.



BANCA

La denominada como cuarta revolución industrial va a suponer, según los expertos, un antes y un después para las entidades financieras que, desde hace años, exploran las posibilidades del Blockchain e incluso están desarrollando sus propios consorcios para el impulso de esta tecnología. Actualmente ya hay bancos considerando el uso de la tecnología Blockchain, incluso realizando pruebas para implementarla. Además, los grandes bancos también están invirtiendo en Startups que están desarrollando interesantes soluciones basadas en esta tecnología.

Puede implicar una importante reducción del tiempo, los costes y la burocracia que actualmente parece necesaria para la realización de transacciones entre instituciones. Cuando se trata de bancos y organizaciones financieras el Blockchain tiene el potencial de resolver muchos problemas.

PAGOS Y REMESAS

Uno de los principales beneficios de la tecnología Blockchain en el sector bancario es tener un sistema de pagos más eficiente. Con Blockchain un pago puede ser efectuado en segundos, reduciendo así tanto el tiempo como los costes. Esta tecnología hace posible realizar transacciones financieras entre dos participantes de manera segura, confiable e irreversible, sin necesidad de utilizar un intermediario para establecer una relación de confianza entre las partes; y esta eliminación de intermediarios es la que posibilita un evidente ahorro de costes. Dichos pagos se pueden respaldar aún más con contratos inteligentes (Smart Contracts), agregando más certeza para el remitente y el receptor. Y esto sumado a las criptomonedas da como resultado un cambio radical en la forma en que se realizan los pagos.

Permite registrar cualquier tipo de transacción financiera, no solo monetaria, ya que también se pueden registrar bonos, acciones, transferencias de propiedades y cualquier tipo de derecho u obligación.

Algo parecido ocurre con el envío de remesas. En la actualidad, las remesas representan el principal flujo de fondos hacia los países en vías de desarrollo, superando a la inversión extranjera directa y las ayudas al desarrollo oficiales.

El problema de todo esto reside en las elevadas comisiones, además, la mayoría de las soluciones del sector de las remesas dependen de servicios ofrecidos por terceros e instituciones financieras. La necesaria intervención de múltiples intermediarios hace que el sistema actual sea muy ineficiente. No sólo porque los servicios son caros, sino también porque las transferencias pueden llegar a tardar días o incluso semanas.

En este contexto, la tecnología Blockchain puede proporcionar alternativas viables y más eficientes para la industria de las remesas, simplificando todo el proceso, eliminando intermediarios innecesarios.

La idea es ofrecer soluciones de pago sin fricción y prácticamente instantáneas, ya que un sistema Blockchain puede ejecutar transacciones financieras internacionales partiendo de una red distribuida de computadoras.

Esto significa que múltiples ordenadores participan en el proceso de verificación y validación de las transacciones. Proceso que puede ser realizado de una forma descentralizada y segura.

TRANSFERENCIAS INTERNACIONALES

Lo mismo ocurre con las transferencias internacionales. Los bancos han empezado a utilizar la tecnología Blockchain porque permite realizar transferencias internacionales en el mismo día. El proceso de una transferencia internacional normal puede alargarse hasta los 7 días hábiles, en los que el dinero va saltando entre diferentes intermediarios y por cada intermediario se añade un coste asociado. A su vez, hay que añadir los tipos de cambio, no siempre favorables, a los que el importador y el exportador están expuestos.

El escenario de Blockchain permite por un lado reducir los tiempos en los cuales se cursa la transferencia, haciendo posible que sea en el mismo día o incluso en minutos, permite tener certeza de todos los costes de antemano, y poder elegir la moneda en la cual se quiere hacer el pago sin tener que incurrir en cambios de moneda innecesarios. En resumen, transferencias rápidas, sencillas y seguras.



MONEDAS ESTABLES O STABLECOINS

En el contexto actual, las criptomonedas de referencia como Bitcoin o Ether siguen caracterizadas por una fuerte volatilidad, por lo tanto, su uso y la inversión en ellas siguen estando relegados a un ámbito de elevado riesgo, marcado por la escasez de garantías.

En este contexto, los instrumentos financieros asociados a Blockchain evolucionan constantemente para encontrar soluciones a los retos a los que aún se enfrenta la tecnología. Un ejemplo de los últimos esfuerzos para reducir la volatilidad de las monedas virtuales es la creación de las stablecoins.

Son 'tokens' que están asociados al valor de una moneda FIAT (Tether y TrueCoin), a bienes materiales como el oro o los inmuebles (G-Coin), o a otra criptomoneda (DAI). También hay stablecoins que no están asociadas a ninguna otra moneda, sino que están controladas mediante algoritmos para mantener un precio estable, por ejemplo, USDX o Basecoin. La principal motivación para crear una stablecoin es tratar de dar refugio a los inversores en momentos de volatilidad.

Inicialmente las stablecoins pretenden hacer de puente entre el sistema financiero tradicional y las criptomonedas, al permitir el intercambio con moneda legal.

Por lo tanto, facilitan la entrada y salida del sistema de criptomonedas y la consolidación de las ganancias en un activo más estable.

SECURITY TOKENS

Un token es una unidad de valor similar a las monedas, pero carecen de valor en curso legal. Son emitidos por organizaciones para un uso determinado y así gestionar su modelo de negocio. Estos tienen el valor que le otorgue la comunidad. Existen varios tipos de Tokens, uno de ellos son los Security Tokens.

Los Security Token son tokens criptográficos similares a cualquier otro, pero vinculados a los security tradicionales. **Un Security es un tipo de activo financiero intercambiable: Bonos, swaps, futuros, etc. Existen muchos tipos de Security, y uno de ellos muy recurrente son las acciones tradicionales de empresas.**

La tecnología Blockchain permite digitalizar los Security dotándolos de muchas ventajas que permiten reducir costes, tiempo y burocracia. Con ello nacen los Security Token, cuyo objetivo es ofrecer derechos bastante similares a las acciones tradicionales, permitiendo llegar a un público más amplio, eliminar burocracia y lentitud, y a un coste más reducido que tener que cotizar acciones. Al igual que el resto de los tokens, estos pueden ofrecerse a través de una ICO, lo cual permite a las empresas obtener capital mediante la venta de acciones (en forma de token criptográfico) a un coste teóricamente más bajo de lo que valdrá en un futuro.

Los security tokens están respaldados por algo tangible, tales como activos o beneficios de una compañía, siendo, por consiguiente, consideradas como inversiones a efectos legales. Los emisores de Security Tokens tienen que cumplir con requisitos legales aplicables a títulos-valor (Securities) allí donde los tokens estén siendo emitidos y activamente comercializados.

Muchos expertos consideran que los Security Tokens serán la siguiente gran revolución después del fenómeno de las ICOs. Este tipo de tokens son más transparentes y atractivos para inversores, dados los derechos que se obtienen al comprar este tipo de activos.

CROWDFUNDING O MICROMECEAZGO

El Crowdfunding es un mecanismo colaborativo para conseguir financiación a través de campañas de recaudación anunciadas en plataformas específicas tiene como objetivo ser una alternativa a las formas más tradicionales y poder financiar todo tipo de ideas. Su principal ventaja es que permite tener liquidez de forma relativamente rápida y sin procesos complicados de solicitud. Casi cualquier idea puede entrar en una campaña.

Según la inversión, el micromecenazgo puede ser:

Donativos: los mecenas financian una causa sin recibir nada a cambio.

Inversión: los inversores recibirán una participación en los beneficios.

Recompensas: el organizador de la campaña ofrece una recompensa física a los donantes a cambio de sus inversiones (un producto físico o servicio).

El Blockchain es lo que hace que este proceso de financiación sea seguro, accesible desde cualquier parte del mundo y completamente transparente; de modo que las plataformas de microfinanciación que usan Blockchain pueden ayudar a maximizar el éxito de un proyecto.

Actualmente, hay un par de formas diferentes en que el crowdfunding de Blockchain o Bitcoin se está utilizando para ayudar a financiar negocios; como las llamadas ofertas iniciales de monedas o ICO, o un proyecto llamado OpenLedger, entre muchos otros, que está utilizando la tecnología Blockchain dentro del campo del crowdfunding.

SEGUROS

La tecnología Blockchain se está haciendo fuerte en el ámbito de los seguros. Esta tecnología moverá casi 1.394 millones de dólares en el mercado asegurador en 2023. La tecnología presenta una serie de características inherentes: transparencia, inmutabilidad, trazabilidad, integridad, seguridad, simplicidad y acceso rápido a la información. Así las cosas, la cadena de bloques se irá implantando de forma exponencial en segmentos del sector asegurador como la gestión de reclamaciones, defunciones e identidades; la detección de fraudes; los pagos; y los contratos inteligentes.

Muchas empresas en la industria han comenzado a utilizar y experimentar con Blockchain, y múltiples proveedores de seguros implementan contratos inteligentes basados en esta tecnología para reducir el coste de la verificación, la ejecución y la prevención del fraude. Aunque, en este momento, hay muchos proyectos de prueba donde las ideas son más un concepto que una realidad.

Sin embargo, habría primeros adoptadores que tendrán la ventaja del primer movimiento. Los principales casos de uso y aplicaciones incluyen:

SEGURO DE AUTOMÓVIL Y EL IOT DESCENTRALIZADO

Los vehículos conectados se convertirán en dispositivos que transmitirán información a la nube. Esta información será compartida con la infraestructura que se genere, permitiendo optimizar la movilidad y reducir las situaciones de riesgo que se generan. La tecnología Blockchain aportará una mayor seguridad al intercambio de información entre vehículos, constituyéndose además en el registro que permitirá establecer responsabilidades en el caso de que algún sistema falle y, de este modo, poder implementar las medidas que sean necesarias para evitar que situaciones conflictivas se repitan.

SEGUROS DE PROPIEDAD Y ACCIDENTES

El procesamiento de las reclamaciones de P&C está plagado de problemas como la evaluación y el ingreso manual de datos, la coordinación entre las partes, etc. La entrada manual de datos conduce a errores que luego resultan en pérdidas para cualquiera de las partes dependiendo del tipo de error. La falta de un marco adecuado para el procesamiento de reclamaciones perjudica al usuario final.

La tecnología Blockchain, basada en contratos inteligentes (Smart Contracts), facilita la recopilación y el análisis automatizado de datos en tiempo real, y por eso puede acelerar algunos procesos en las reclamaciones de P&C. En resumen, las reclamaciones pueden procesarse automáticamente mediante contratos inteligentes. Además, todos los cambios se pueden rastrear para la autenticidad, lo que los hace auditables.

Estos contratos serán hasta 3 veces más rápidos y 5 veces más baratos que en la actualidad. Podrían ahorrar a las aseguradoras de P&C más de 200.000 millones de dólares al año en costes operativos y reducir su ratio operativo entre 5 y 13 puntos porcentuales.



SEGUROS DE SALUD

En este caso, Blockchain posibilita la encriptación de los datos del historial del paciente y su transferencia a la vez que se protege la privacidad. La necesidad de mantener la confidencialidad del paciente significa que los proveedores a menudo no tienen acceso a la historia clínica completa, y esta falta de datos puede dar lugar a denegaciones en las reclamaciones.

Es una red criptográficamente segura que proporciona a la atención médica la infraestructura necesaria para funcionar correctamente. Puede utilizarse para crear privacidad en la red y, a cambio, ayudar a la industria de la salud a ahorrar miles de millones de dólares. El objetivo principal de Blockchain es crear una red que garantice que los pacientes siempre tengan el control de sus datos médicos. Al hacerlo, pueden dejar que los pacientes decidan cuándo y cómo se comparten sus datos a los profesionales o institutos médicos.

REASEGUROS

El actual proceso de reaseguro es extremadamente complejo y notoriamente ineficiente. Se procesa manualmente y se determina mediante contratos puntuales. En este ámbito, la tecnología de cadena de bloques simplifica el flujo de información y los pagos entre aseguradores y reaseguradores.

Además, con los datos compartidos en un libro de cuentas inmutable, los reaseguradores pueden estar mejor equipados para asignar capital para siniestros casi en tiempo real, lo que les permite procesarlos y liquidarlos rápidamente, sin tener que depender de los aseguradores primarios para los datos relativos a cada uno.

LEGAL

La posibilidad de agilizar y automatizar relaciones entre partes desconocidas de forma verificable y sin necesidad de intermediarios es una de las principales virtudes que hace del Blockchain una tecnología potencialmente aplicable a multitud de sectores económicos. Y el sector legal quizá sea uno de los sectores que más está percibiendo el impacto.

La agilización en la forma de inscribir documentos en los registros es una de las muchas mejoras que Blockchain podría suponer para el sector legal. Países como Suecia ya han desarrollado pruebas piloto en este sentido, aprovechando las ventajas de inmutabilidad, transparencia y trazabilidad que aporta esta tecnología. En este caso, el proyecto se basa en una plataforma Blockchain que permite identificar cada bien objeto de inscripción con una huella digital única, de modo que solo tenga que ser registrada en papel una sola vez.

PROPIEDAD INTELECTUAL

Es posible proveer registros indiscutibles, accesibles a escala global. Dado que Blockchain es irreversible, segura y da fe de la fecha de cada evento, ofrece el mejor mecanismo para proveer evidencias de primer uso y sus aplicaciones prácticas para cualquier tipo de patentes, copyrights y marcas registradas.

REGISTROS DE PROPIEDAD

Otro de los usos de Blockchain será en los registros de propiedad de bienes raíces y en la gestión de los respectivos títulos y escrituras, pues habrá un registro fácilmente verificable. Y desde el Estado hasta los propietarios podrán acceder a la misma información, para conocer de quién es el dominio y cuándo ha habido una transferencia a un nuevo propietario.

CONTRATOS RICARDIANOS

Recientemente, algunas tecnologías basadas en Blockchain han comenzado a respaldar los contratos ricardianos, una forma de documentos digitales que actúan como un acuerdo entre dos partes sobre los términos y condiciones para una interacción entre las partes acordadas. Lo que hace únicos este tipo de contratos es que está firmado y verificado criptográficamente. Es un acuerdo o documento legal único que es legible al mismo tiempo para los programas informáticos y para los humanos.

Es decir, tiene dos propósitos, por un lado, es un contrato fácil de leer entre dos o más partes, y por otro, es un contrato legible para máquinas, que con las plataformas de Blockchain estos contratos ahora se pueden hashear, firmar y guardar fácilmente.

La diferencia fundamental entre los Contratos Ricardianos y los Smart Contracts es el tipo de acuerdo. Uno (Contratos Ricardianos) registra el acuerdo entre varias partes, mientras que el otro (contratos inteligentes) ejecuta todo lo que se define en el acuerdo como acciones. El contrato ricardiano es un contrato legalmente válido, mientras que los contratos inteligentes no lo son. Convierte un contrato legal legible por humanos en un código legible por máquinas que puede ser ejecutado por el software.

¿Qué es un Contrato Ricardiano?

Es un acuerdo legal legible para personas que, una vez acordado y firmado por ambas partes, se convierte en un contrato legible para máquinas para definir las intenciones de ambas partes



PROPÓSITO

Registra los términos de un acuerdo como un documento legal.



FLUJO

Puede automatizar operaciones en las aplicaciones basadas en Blockchain.



VALIDEZ

Es un documento o acuerdo legalmente vinculante.



VERSATILIDAD

Cualquier Contrato Ricardiano también puede ser un contrato Inteligente.



LEGIBILIDAD

Los Contratos Ricardianos son legibles tanto por máquinas como por humanos.

BENEFICIOS DE LOS CONTRATOS RICARDIANOS



COSTES

Los Contratos Ricardianos pueden ahorrarte esfuerzos, costos y tiempo cuando tengas que invertir cuando surja una disputa.



ACUERDO LEGAL VINCULANTE

A diferencia de los contratos inteligentes, los Contratos Ricardianos unen ambas partes en un acuerdo legal. Si algo sale mal, una parte puede poner un caso contra la otra en el tribunal de justicia.



ACTUA COMO UN CONTRATO LEGAL INTELIGENTE

No solo definen las intenciones de ambas partes en términos legales, sino que también pueden ejecutar instrucciones.

EDUCACIÓN

La tecnología Blockchain se va introduciendo poco a poco también en el sector educativo. Cada vez más centros educativos aplican esta tecnología con intenciones pedagógicas. Por su complejidad, su utilización sigue siendo privilegio de una minoría de expertos en informática, pero su implementación es cada vez más habitual.

Su uso es aún poco común y se da en casos muy concretos como, por ejemplo, la autenticación de currículums para el profesorado y el cuerpo estudiantil, o la certificación de validez de algunos cursos. Esta tecnología permite tener una gestión automatizada de calificaciones y exámenes, además de evitar cualquier tipo de fraude, como, por ejemplo, los cambios de notas y plagios.

CÓMO SE APLICA EL BLOCKCHAIN EN EDUCACIÓN

Blockchain facilita que los estudiantes puedan gestionar sus datos y decidan qué contenidos quieren compartir y con quién. Además, si un alumno tiene que gestionar una transacción económica, por ejemplo en el caso de querer matricularse en otro colegio, éste necesitará abonar las tasas correspondientes, pudiéndose realizar el proceso de manera segura.

Por otro lado, otra de las aplicaciones que utilizan la tecnología Blockchain, permite que haya un nuevo sistema de emisión y certificación de documentos oficiales y titulaciones. Gracias a esto se puede asegurar la veracidad de las evaluaciones y títulos que consigue un estudiante. En este caso, la tecnología que aplica el sistema certifica el registro de manera segura y asegura la autenticidad de todo el histórico de cada alumno. Por ello, es una herramienta que todos los profesores deberán de conocer y, además, explicar a sus alumnos, ya que tendrán que entregar todos los trabajos escritos y exámenes a través de esa plataforma.

BENEFICIOS DE LA TECNOLOGÍA BLOCKCHAIN EN EDUCACIÓN

Actualmente, el uso de esta nueva tecnología que consiste en cadenas de bloques es poco común y aún se usa en casos muy concretos. Algunos de sus principales beneficios son los siguientes:

- **Certificación online universal:** La inmutabilidad y garantía de veracidad que otorga el Blockchain podría dar lugar a la creación de un nuevo sistema de emisión y certificación, tanto de documentos oficiales como de titulaciones académicas.
- **Respeto medioambiental:** Gracias a la tecnología Blockchain aplicada a la educación, se consigue disminuir en gran medida el uso del papel. Se evita imprimir grandes números de documentos, que serán accesibles de manera segura y digital.
- **Expediente académico:** Gracias a la inmutabilidad de la aplicación, es un entorno perfecto para salvaguardar todos los informes y trabajos de los alumnos dentro de la plataforma. Blockchain ofrece un modelo seguro para la recopilación de calificaciones, cartas de recomendación, certificados, entre otros. Esta tecnología será fundamental para evitar el fraude.
- **Adiós a los plagios:** Aplicando la trazabilidad de Blockchain se puede registrar quien fue la primera persona en publicar un contenido, por lo que permite demostrar la autoría cuando se da un plagio.
- **Evitar usurpación de identidad:** Todos los alumnos serán sus propios gestores. Deberán controlar sus datos y serán los que decidan qué contenido publicar y con quién compartirlo. Blockchain tiene capacidad para administrar, compartir y proteger contenido digital.

RETAIL

La industria del Retail ha cambiado más en los últimos 10 años que en los anteriores 40, y la principal causa es la digitalización. En la actualidad, hay diferentes tecnologías que están comenzando a desempeñar un papel más decisivo en todas las áreas de la empresa, y una de esas tecnologías es el Blockchain. Esta tecnología no sólo ayudará a estimular procesos internos eficientes, innovación, crecimiento de marca y rentabilidad, sino que también mejorarán la experiencia del consumidor. Se puede utilizar de múltiples maneras dentro del sector, especialmente en temas de seguimiento y monitorización de productos, flujo de información, integración con proveedores, servicios e incluso capital.



TRANSPARENCIA EN LA CADENA DE SUMINISTRO

- **Trazabilidad y visibilidad:** La cadena de suministro conectada permitirá a los fabricantes, ordenar, vender, rastrear y pagar bienes. Esta tecnología permite a las empresas rastrear productos a través de cada eslabón de la cadena de suministro, desde las materias primas hasta la producción y el producto final.
- **Autenticidad de producto y origen:** Cada transacción a lo largo de la cadena de suministro, ya sea de un proveedor o fabricante, se puede agregar como un registro válido y verificable para corroborar la autenticidad.
- **Registro automatizado:** El almacenamiento y análisis de los datos relevantes de productos, así como cadenas de suministro pueden ayudar a las empresas a lograr una mejor gestión de su inventario.
- **Retirar un producto:** Las compañías podrán identificar aquellos productos que son inseguros o tienen partes defectuosas, por lo mismo, podrán hacer retiros específicos y efectivos de productos en mal estado.
- **Transacciones fraudulentas:** Rastrea todo el proceso del pedido hasta que llega a destino, controlando si existe desviación de la ruta.
- **Cadena de suministro de comercio y finanzas:** Los pagos B2B serán más sencillos y confiables al simplificar las transacciones financieras, acelerar los procesos, reducir los costes y riesgos intermedios.



FOMENTAR LA LEALTAD DEL CLIENTE

- Creación de programas de lealtad inteligentes, en los que se registran una mayor cantidad de datos de clientes a través de Smart Contracts con el objetivo de realizar campañas más personalizadas. Blockchain ofrece integridad de datos precisa e instantánea, lo cual es aplicable a los esquemas de fidelización de clientes que dependen de los datos. La naturaleza de la tecnología garantiza que los datos se capturen en cada etapa de la interacción con el cliente, lo que significa que se mejorará el análisis cualitativo junto con las capacidades de modelado del cliente. La gran cantidad de información podría vincularse a la IA a través del análisis Big Data, para crear comunicaciones personalizadas, ofreciendo la recompensa adecuada en el momento adecuado.
- Participación del consumidor, permitiendo guardar de forma más segura datos y encuestas.
- Localización de los productos robados, mediante un seguimiento de la trazabilidad del producto. Los consumidores tendrán acceso a la información detallada en cualquier momento.
- Servicios conectados que pueden proporcionar un mejor servicio postventa y mayores garantías.
- Economía compartida: mediante una plataforma P2P los usuarios se pueden conectar ofreciendo habilidades, servicios, etc.
- Pagos de consumidores seguros y rápidos.
- Acceso a servicios de asistencia. Acceso a contratos y acuerdos predefinidos para servicios y garantías de cuidados posteriores.
- Protección de la privacidad del consumidor. Los registros digitales de datos del consumidor y compras en plataformas habilitadas con Blockchain serán seguros, es decir, menos propensos a las infracciones que aquellos respaldados en plataformas locales.

PAGOS Y CONTRATOS

- Pagos al consumidor más rápidos y seguros, incluyendo el uso de criptomonedas.
- Pagos B2B, facilitando los pagos entre empresas, simplificando la transacción, eliminando intermediarios y permitiendo pagos transfronterizos.
- Protección al consumidor, creando registros digitales de las compras del cliente.

TURISMO

La industria turística está sujeta a numerosos procesos en los que verificar la identidad e información de los usuarios es un paso indispensable del que depende el modelo de negocio. Por este motivo, la existencia de un “gran libro de registro compartido” a través del que distintas entidades y personas pueden intercambiar información y valor es de gran utilidad.

El Blockchain y el turismo tienen el potencial de convertirse en una combinación muy ventajosa, y es que esta tecnología puede aportar seguridad y transparencia en ciertos puntos clave. Por ejemplo, cuando una agencia de viajes reserva vuelos y hoteles para un cliente envía sus datos a las diferentes compañías. El Blockchain puede hacer que la transferencia y almacenamiento de esta información sea más fácil y segura, ya que la responsabilidad se comparte por toda una red. Lo mismo ocurre con los pagos en el extranjero, lo que aumenta el nivel de confianza entre todas las partes.

PAGOS FÁCILES, SEGUROS Y TRAZABLES

Los pagos con criptomonedas serían mucho más seguros y trazables, ya que todas las transacciones que se realizan a través de la red de Blockchain quedan registradas en la cadena de bloques y no se pueden modificar. Además, al ser un sistema descentralizado, no habría intermediarios que pudieran intervenir o retrasar el pago en cuestión. Del mismo modo, ya no sería necesario hacer cambios de divisas cuando se viaja a otro país y quedar sujetos a la fiabilidad o volatilidad de estas.

LOS SISTEMAS DE RESERVA

Blockchain puede ofrecer la oportunidad de lograr que los hoteles, al igual que los diferentes prestadores de servicios turísticos, puedan mantener un registro más preciso y directo de los clientes, haciendo de esta forma los procesos de pago más eficientes, la verificación de los clientes más rápida y aumentar también los programas de fidelización.

OVERBOOKING

La capacidad para evitar el doble gasto podría, en teoría, eliminar el problema de duplicar las reservas en la industria. Como Blockchain tiene la capacidad de crear sistemas de seguimiento sin fisuras, esta tecnología se puede utilizar para garantizar la capacidad máxima sin overbooking.

GESTIÓN DE EQUIPAJES EN AEROPUERTOS

El Blockchain puede resultar de gran utilidad para rastrear el movimiento del equipaje una vez se deja en el mostrador de facturación. Este va cambiando de manos y realiza, al igual que los turistas, un largo viaje siendo posible un seguimiento entre empresas conociendo en todo momento dónde se encuentra la maleta.

PRIVACIDAD DE LOS CLIENTES E ID DIGITAL ÚNICA

Este nuevo paradigma afectará a la gestión de la identidad digital y hará posible que los usuarios revelen sólo la información necesaria para el servicio que van a consumir y, además, de forma automática y sin necesidad de intermediarios.

Una de las grandes ventajas que aportará Blockchain al mundo del turismo es la identidad única. En un sistema en que todas las partes comparten de forma segura la información, el viajero tendrá una identificación única desde que reserva su viaje hasta que vuelve a casa. Es decir, no tendrá que aportar más datos personales que los estrictamente necesarios para demostrar quién es y a qué tiene derecho en cada momento.

SECTOR PÚBLICO

El sector público es uno de los más lentos en la transformación digital, pero poco a poco los gobiernos van dando pasos hacia una mayor digitalización. En este proceso, la tecnología Blockchain puede ser de gran ayuda gracias a sus características. Si se aplica una capa de inteligencia y se vinculan tecnologías Blockchain con Big Data, se abren grandes oportunidades en el contexto de las ciudades conectadas, con casos de gestión de mobiliario, de parques, aguas, electricidad, etc., para, finalmente, superponer una última categoría relacionada con la identidad digital que permitiría encontrar modelos disruptivos en sanidad, justicia o educación.

CONTRATACIÓN, GESTIÓN FINANCIERA Y PRESUPUESTARIA, CUMPLIMIENTO NORMATIVO

A pesar de los esfuerzos de modernización, procesos rutinarios como la contratación, la gestión financiera y el cumplimiento normativo siguen estando basados en gran medida en papel. Se trata de procesos costosos y complejos, con un alto riesgo derivado de errores o del fraude. Blockchain puede aportar beneficios significativos en estas áreas.

Blockchain reduce los tiempos, costes y riesgos derivados de aplicar las normas administrativas, establece una pista de auditoría inmutable que asegura los tiempos de los procesos y frena los costes. Con el acceso a datos más completos y confiables, las organizaciones gubernamentales pueden tomar mejores decisiones sobre dónde centrar su atención.

GESTIÓN DE IDENTIDADES Y ACCESOS, SERVICIOS CIUDADANOS, E-VOTACIÓN

Blockchain hace referencia cruzada y verifica múltiples fuentes de datos, eventos y transacciones de forma segura, y puede establecer y validar la identidad de un individuo cuando faltan pruebas tradicionales.

Desde la votación hasta la recaudación de impuestos o el registro de tierras, dependerán en gran medida de la gestión de la identidad y es improbable que varíen considerablemente sin ella. Asimismo, el alcance de nuevos servicios, seguros y sin fisuras, se amplía drásticamente cuando se introduce la gestión de activos a través de la tecnología Blockchain.

Debido a que los participantes en una transacción en Blockchain tienen acceso a los mismos registros, no hay necesidad de que un intermediario valide las transacciones o verifique identidades o propiedad. Las licencias comerciales, los títulos de propiedad, las matriculaciones de vehículos y otros registros podrían trasladarse a Blockchain, liberando a los ciudadanos de la necesidad de abogados, notarios y desplazamientos a las oficinas gubernamentales para certificar que las transacciones son legales. Ya hay organizaciones gubernamentales explorando cómo Blockchain podría facilitar servicios sin fronteras como el registro de una empresa extranjera o la recaudación de impuestos.

IDENTIDADES DIGITALES Y CONECTIVIDAD ENTRE ADMINISTRACIONES

La tecnología que da soporte a Blockchain aporta la transparencia necesaria, pero empatizando con el ciudadano, construye propuestas que respondan a una necesidad real y no a una funcionalidad. Cambia el concepto de identidad digital, entendiéndolo por ésta no sólo nombre y DNI, sino el historial completo de una persona como contribuyente, pagador de hipotecas, con una vida bancaria, historial médico, historial profesional en LinkedIn, de alquileres en Airbnb, etc.

Un ejemplo de esto es el Plan de e-Government de Estonia. El país está desplegando un sistema de Blockchain para agilizar la compartición de diversos tipos de datos entre la Administración Pública (de carácter legal, jurídico, etc., así como su protección, seguridad y transparencia).



Tecnologías Blockchain 04

Las compañías están cada vez más interesadas en la tecnología Blockchain debido a su promesa de mejorar la eficiencia y reducir los costes. Sin embargo, no pueden usar las cadenas de bloques públicas sin permiso debido a la falta de privacidad, baja escalabilidad y menor rendimiento de las transacciones.

CARACTERÍSTICAS	ETHEREUM	HYPERLEDGER FABRIC	R3 CORDA
Descripción de la plataforma	Plataforma Blockchain genérica	Plataforma Blockchain modular	Plataforma de contabilidad distribuida especializada para la industria financiera
Gestión	Desarrolladores de Ethereum	Linux foundation	R3
Modo de operación	Sin permiso público o privado	Autorizado, privado	Autorizado, privado
Consenso	- Minería basada en la Prueba de Trabajo (PoW). - Nivel ledger	- Amplia comprensión del consenso que permite múltiples enfoques. - Nivel de transacción	- Comprensión especializada del consenso (p.e. nodos notariales) - Nivel de transacción
Smart Contracts	- Smart Contract Code (e.g., Solidity)	Smart Contract Code (e.g., Go, Java)	- Smart Contract cCode (Kotlin, Java) - Smart Legal Contract (doctrina legal)
Moneda	- Ether - Tokens a través de Smart Contract	- Ninguna - Moneda y tokens mediante código de cadena	- Ninguna

HYPERLEDGER FABRIC

Hyperledger Fabric fue lanzado en 2016 por un consorcio de empresas entre las que se encuentran IBM, Intel, CISCO, SAP, Daimler y American Express. Se trata de un marco de Blockchain modular que se ha convertido en el estándar de facto para las plataformas de Blockchain empresariales. Ofrece un enfoque único que permite el rendimiento a escala y al mismo tiempo que preserve la privacidad de datos que exigen las empresas. A través del código y la gobernanza abiertos, presenta nuevas capacidades innovadoras reforzadas para el uso por parte de las empresas, marcando el comienzo de una nueva era de confianza, transparencia y responsabilidad.

- **Capacidad Plug-n-play** para integrar componentes como algoritmos de consenso y servicios de membresía.
- **Contratos inteligentes llamados 'chaincodes'**, que se alojan utilizando contenedores.
- **Tecnología de canales** para transacciones confidenciales.
- **Servicio de pedidos que entrega la transacción a 'pares'**, un grupo de nodos responsables de confirmar las transacciones en el libro mayor.
- **Política de respaldo** para la validación de transacciones.
- **Servicios de bases de datos** como CouchDB.

Hyperledger Fabric admite soluciones de contabilidad distribuidas en redes autorizadas para una amplia gama de industrias. Su arquitectura modular maximiza la confidencialidad, resistencia y flexibilidad de las soluciones Blockchain entre otras ventajas:

Membresía autorizada.

Marco para redes autorizadas, donde todos los participantes tienen identidades conocidas. Al considerar una red autorizada, se debe pensar si el caso de uso de Blockchain debe cumplir con las regulaciones de protección de datos. Muchos casos de uso, en particular en el sector financiero y en la industria de la salud, están sujetos a leyes de protección de datos que requieren saber quiénes son los miembros de la red y quién accede a datos específicos.

Rendimiento, escalabilidad y niveles de confianza.

Hyperledger Fabric se basa en una arquitectura modular que separa el procesamiento de transacciones en tres fases: procesamiento y acuerdo de lógica distribuida ("chaincode"), pedidos de transacciones y validación, y compromiso de transacciones. Esta separación confiere varias ventajas: se requieren menos niveles de confianza y verificación en todos los tipos de nodos, y la escalabilidad y el rendimiento de la red están optimizados.

Datos que se basan en la vertiente "need-to-know".

Las empresas, debido a la competitividad, las leyes de protección y la regulación sobre la confidencialidad de los datos personales tienen la necesidad de mantener la privacidad de ciertos tipos de datos, lo que se puede lograr mediante la partición de datos en la cadena de bloques. Los canales, compatibles con Hyperledger Fabric, permiten que los datos vayan solo a las partes que necesitan conocerlos.

Arquitectura modular.

La modularidad de la arquitectura Hyperledger Fabric permite a los diseñadores de red conectar sus implementaciones preferidas para componentes, lo cual es una ventaja. Una de las áreas más solicitadas para la modularidad es "bring your own identity". Algunas redes de compañías múltiples ya tienen administración de identidad y desean reutilizar en lugar de reconstruir. Otros componentes de la arquitectura que se pueden conectar fácilmente incluyen consenso o cifrado. De hecho, algunos países ya tienen sus propios estándares de cifrado.

Protección de claves digitales y datos sensibles.

El soporte de HSM (Hardware Security Module) es vital para salvaguardar y administrar claves digitales para una autenticación sólida. Hyperledger Fabric proporciona PKCS11 modificado y no modificado para la generación de claves, que admite casos como la gestión de identidad, que necesitan más protección. Para escenarios relacionados con la gestión de identidades, HSM aumenta la protección de claves y datos confidenciales.

RIPPLE

Por otro lado, se puede encontrar Ripple, que fue creada como una nueva solución ante la situación complicada que viven los pagos online. Sus creadores lanzaron Ripple con la idea de utilizar la tecnología Blockchain y los activos digitales para permitir que las instituciones financieras envíen dinero a través de las fronteras, de forma instantánea, confiable y con un coste mínimo.

Esta unificación de la infraestructura subyacente que une a las instituciones y los proveedores no solo ayuda a los clientes de Ripple a hacer crecer sus negocios, sino que también permite que el mundo mueva dinero como lo hace la información hoy en día, un concepto que los creadores de la compañía definen como "Internet de valor".

Ripple es una cadena de bloques de código abierto y semi-autorizada dirigida por los laboratorios Ripple. En la superficie, hay muchas cosas que ofrece Ripple que no son muy diferentes de otras aplicaciones de Blockchain: tiene un libro mayor distribuido, una variedad de aplicaciones de billetera y un activo nativo, XRP. Sin embargo, a pesar de sus similitudes con otros Blockchains como Bitcoin, Ripple decidió diferenciarse en el uso de pasarelas, emisión y líneas de confianza.

En lugar de usar el concepto de minería Blockchain, Ripple utiliza un mecanismo de consenso distribuido único a través de una red de servidores para validar las transacciones, lo que significa que, aunque este dentro del mismo área que Blockchain, se puede considerar una DLT.

No obstante, sigue siendo una tecnología cercana al Blockchain, la cual, al realizar una encuesta, los servidores o nodos de la red deciden por consenso sobre la validez y autenticidad de la transacción. Esto permite confirmaciones casi instantáneas sin ninguna autoridad central, lo que ayuda a mantener a Ripple descentralizado y más rápido y confiable.

Estas características son especiales, porque fueron las que dieron a Ripple el impulso necesario para ingresar en el mundo financiero, al permitir a los bancos crear su propia red de socios y permitirles realizar transacciones de activos en la cadena de bloques, introduciendo una nueva forma de reducir los costes de transacción.

ETHEREUM

Ethereum es otra de las redes Blockchain que en los últimos años ha ganado más relevancia. La estructura fundamental de cómo funciona la criptomoneda se aplica tanto a Ethereum como a Bitcoin. Sin embargo, cada tecnología tiene un objetivo diferente. Bitcoin es estrictamente una moneda digital, y en su mayoría funciona como una forma de pago.

En cambio, Ethereum funciona como una plataforma a través de la cual las personas pueden usar tokens para crear y ejecutar aplicaciones y crear Smart Contracts.

Todo este proceso se lleva a cabo en la cadena de bloques y todos pueden ver lo que se ha hecho. Entre los beneficios de esta tecnología se incluyen:

- **La seguridad.** En el corazón de todas las tecnologías Blockchain están la seguridad y la protección. Este sistema evita que un tercero altere o cambie los datos.
- **Censura y prevención de la corrupción.** Ethereum se basa en una red entre pares que se forma en torno a principios específicos que hacen que la censura sea prácticamente imposible.
- **Tiempo de inactividad y seguridad.** Las aplicaciones no se desactivarán, sino que los datos siempre estarán disponibles porque se ejecutan en software de código abierto.

En definitiva, el principal beneficio de Ethereum es que permite utilizar una forma alternativa de moneda digital, pero también proporciona características adicionales que ofrecen seguridad y protección, como la construcción de Smart Contracts.

No obstante, a pesar de traer una serie de beneficios, las aplicaciones descentralizadas no son impecables. Debido a que el código de Smart Contract está escrito por humanos, son tan buenos como las personas que los escriben. Los errores o descuidos del código pueden conducir a acciones adversas no intencionadas. Si explota un error en el código, no hay forma eficiente de detener un ataque o explotación que no sea obtener un consenso de la red y reescribir el código subyacente. Esto va en contra de la esencia de la cadena de bloques, que debe ser inmutable. Además, cualquier acción tomada por una parte central plantea dudas sobre la naturaleza descentralizada.

Independientemente de las desventajas que pueda presentar, al proporcionar una plataforma fácil de utilizar que permite a las personas aprovechar el poder de la tecnología Blockchain, Ethereum está acelerando la descentralización de la economía mundial, dando pie a la creación de nuevas plataformas que se basan en su funcionamiento, entre las que se encuentran:



QUORUM

Basado en Ethereum y desarrollada por JP Morgan, Quorum es una plataforma Blockchain de código abierto que combina la innovación de la comunidad pública de Ethereum con mejoras para satisfacer las necesidades de la empresa.

Su principal misión es hacer que la adopción de Blockchain sea un proceso continuo, ya que no es solo una plataforma, sino que brinda un soporte de servicio completo. Sus cuatro características diferenciadoras del Ethereum más puro son: la administración de permisos de red y de pares, una mayor privacidad de transacciones y contratos, mecanismos de consenso basados en votación y un mejor rendimiento.

CORDA

La plataforma Corda de código abierto está diseñada principalmente para negocios y fue creada para abordar las deficiencias más destacadas de Blockchain, como son la falta de privacidad y de finalidad, permitiendo transacciones privadas con una finalidad inmediata.

Una de las características definitorias de Corda es Corda Network, una red subyacente que proporciona una capa común de identidad y consenso en las redes empresariales.

El principal beneficio de Corda Network para los participantes es **poder mover efectivo, activos digitales y datos de identidad de una aplicación o línea de negocio a otra**. Los operadores de redes empresariales también se benefician al poder acceder a servicios de toda la red y reutilizar los servicios de red y raíz de confianza, en lugar de construir y administrar los suyos.

ALASTRIA

A nivel nacional, las principales empresas españolas de banca, energía y telecomunicaciones, entre otros sectores, han establecido Alastria, la primera red nacional regulada del mundo basada en Blockchain. Este consorcio se convertirá en el nuevo ecosistema de intercambio de datos y permitirá acelerar la transformación digital de diferentes sectores industriales y comerciales en los próximos años gracias a su agilidad, veracidad, seguridad y eficiencia.

La red actual de Alastria se basa en Quorum. El trabajo de construcción se ha iniciado a su vez en dos redes nuevas, una basada en Parity y otra en HyperLedger Fabric (The Linux Foundation), sin descartar la construcción de otros tipos de redes en el futuro, con el que experimentar interoperabilidad entre ellos.

La red proporcionará una plataforma compartida en la que los diversos participantes, y en particular las grandes empresas, podrán crear representaciones digitales de los activos con los que trabajan en su actividad económica habitual, también conocidos como tokens.

Con estos es posible desarrollar nuevos productos y servicios innovadores, además de poder desarrollar los procesos actuales de manera más rápida, segura y eficiente. De esta manera, la red acelera la transformación digital de los procesos actuales y permite un nuevo paradigma de innovación colaborativa y multisectorial de manera eficiente.



Nuestras Conclusiones

Blockchain es una innovación tecnológica que se está emancipando progresivamente de su origen, la criptomoneda Bitcoin, y que está imponiéndose progresivamente como nuevo paradigma para la transmisión, registro y verificación de datos. Su valor de mercado ha alcanzado ya los 2.200 millones de dólares, pero **el crecimiento previsto es radicalmente exponencial: alcanzará los 7.000 millones en 2021**, y los 23.300 millones en el año 2023.

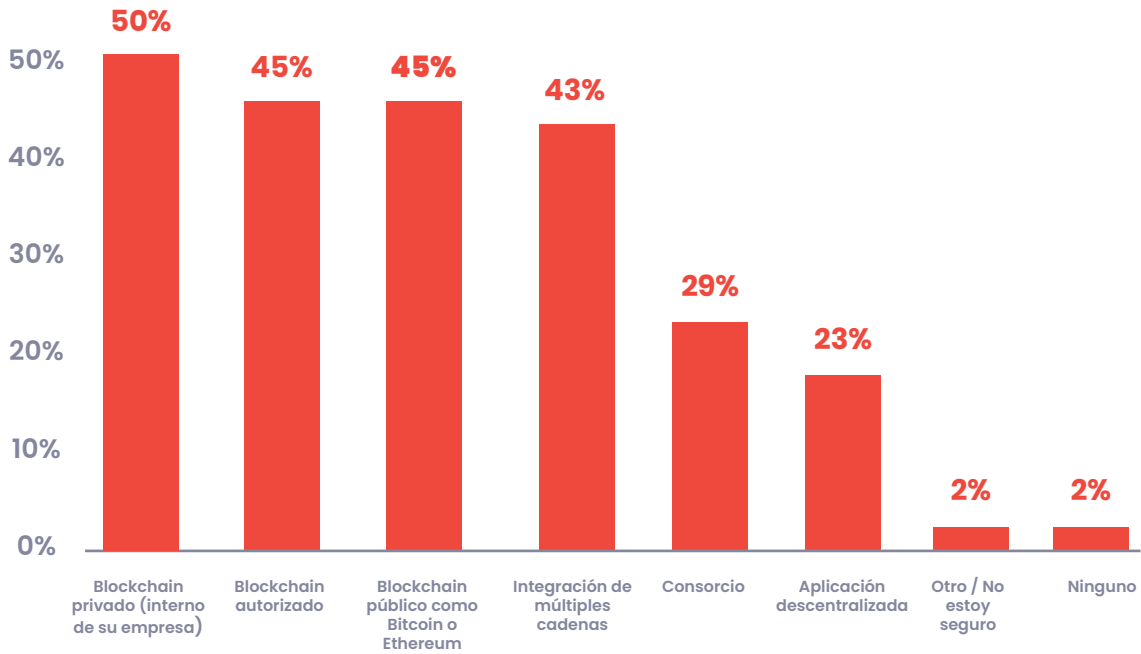
La apuesta de las empresas a nivel global es cada vez más decidida, teniendo en cuenta el carácter multisectorial de la tecnología, el surgimiento de nuevos marcos de Blockchain como Hyperledger, y la diversificación de usos más allá de las transacciones de criptomonedas: Smart Contracts, la gestión de la ID digital, el seguimiento de la cadena de suministro, etc. De hecho, este año **las empresas han invertido 2.700 millones de dólares en la adopción de la tecnología en cuestión, pero se prevé que la inversión alcance los 15.900 millones en 2023.**



Esta inversión, no obstante, no se reparte de manera homogénea. El 50% de las compañías que apuestan por la tecnología en cuestión, están adoptando Blockchains privados internos para la transformación del flujo operacional de su propia empresa. Paralelamente, el 45% se centran en Blockchains públicos como Bitcoin o Ethereum, pese a las problemáticas asociadas a las redes de este tipo, como la falta de privacidad o la limitada escalabilidad. En este contexto, **un 43% de las organizaciones invierten en la integración de múltiples Blockchain: públicos, privados e híbridos.**

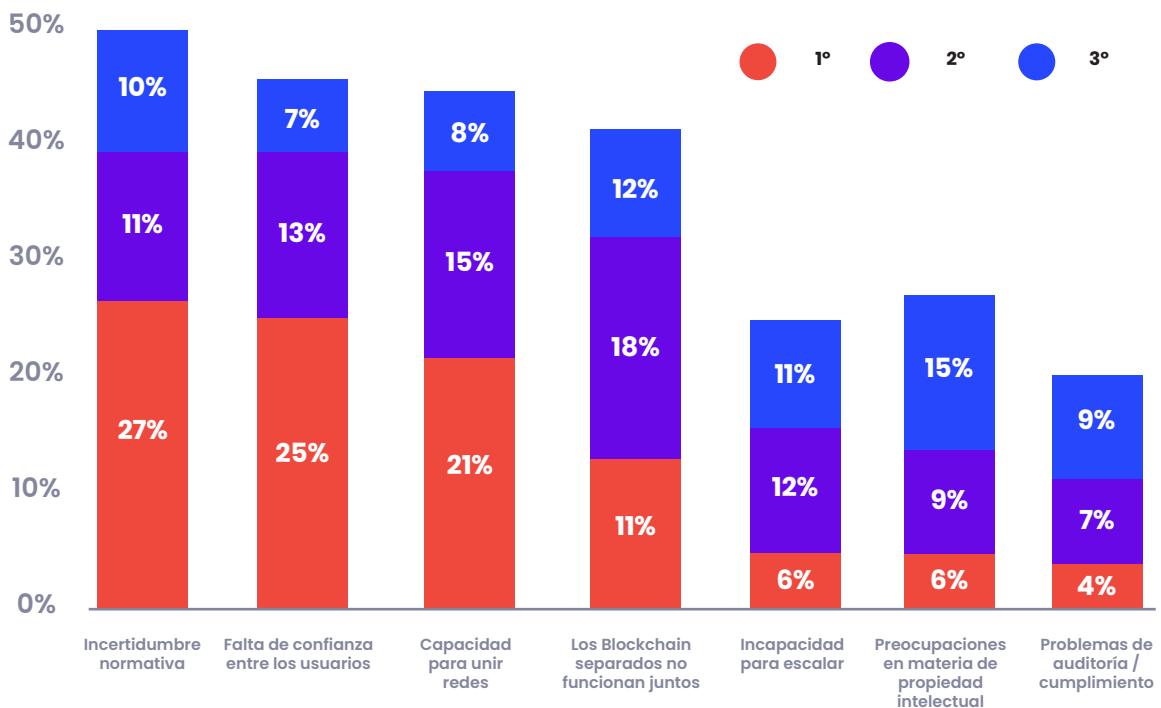
% Encuestados

Modelos de Blockchain desplegados en organizaciones de todo el mundo a partir de 2019.



% Encuestados

Las mayores barreras para la adopción de la tecnología Blockchain en todo el mundo a partir de 2018.





En cuanto a las principales barreras para la adopción de Blockchain, **para un 27% de las empresas a nivel global el obstáculo principal es la incertidumbre regulatoria**, y para un 25% lo es la falta de confianza por parte de los usuarios. Problemáticas también desarrolladas en el presente informe, como la dificultad para integrar múltiples Blockchain, son identificadas como principal barrera por el 11% de las compañías.

En definitiva, Blockchain tiene potencial para revolucionar todo tipo de industrias, mejorando la eficiencia del flujo de trabajo, gracias **a principios como la descentralización, la transparencia, la durabilidad, la reducción de costes, la alta disponibilidad o la rapidez de las transacciones**. Y aunque su adopción no está exenta de retos, supone una ventaja competitiva clave para las empresas que logren hacerlo.

**Somos expertos en servicios,
productos y soluciones digitales,
en innovación tecnológica y en
procesos ágiles de transformación.**

Con un equipo humano de **más de 2.500 profesionales**, tenemos presencia a nivel nacional e internacional, con sedes en EE. UU., Perú, Brasil, Chile, México, Colombia, Paraguay, Reino Unido y Alemania.

¿Nuestra misión? Generar el mayor valor a nuestros clientes, a los sectores económicos y al conjunto de la sociedad, mediante el diseño y desarrollo de iniciativas **basadas en tecnología de vanguardia**, con el objetivo de accionar el cambio digital de una manera disruptiva.

www.vectoritcgroup.com

