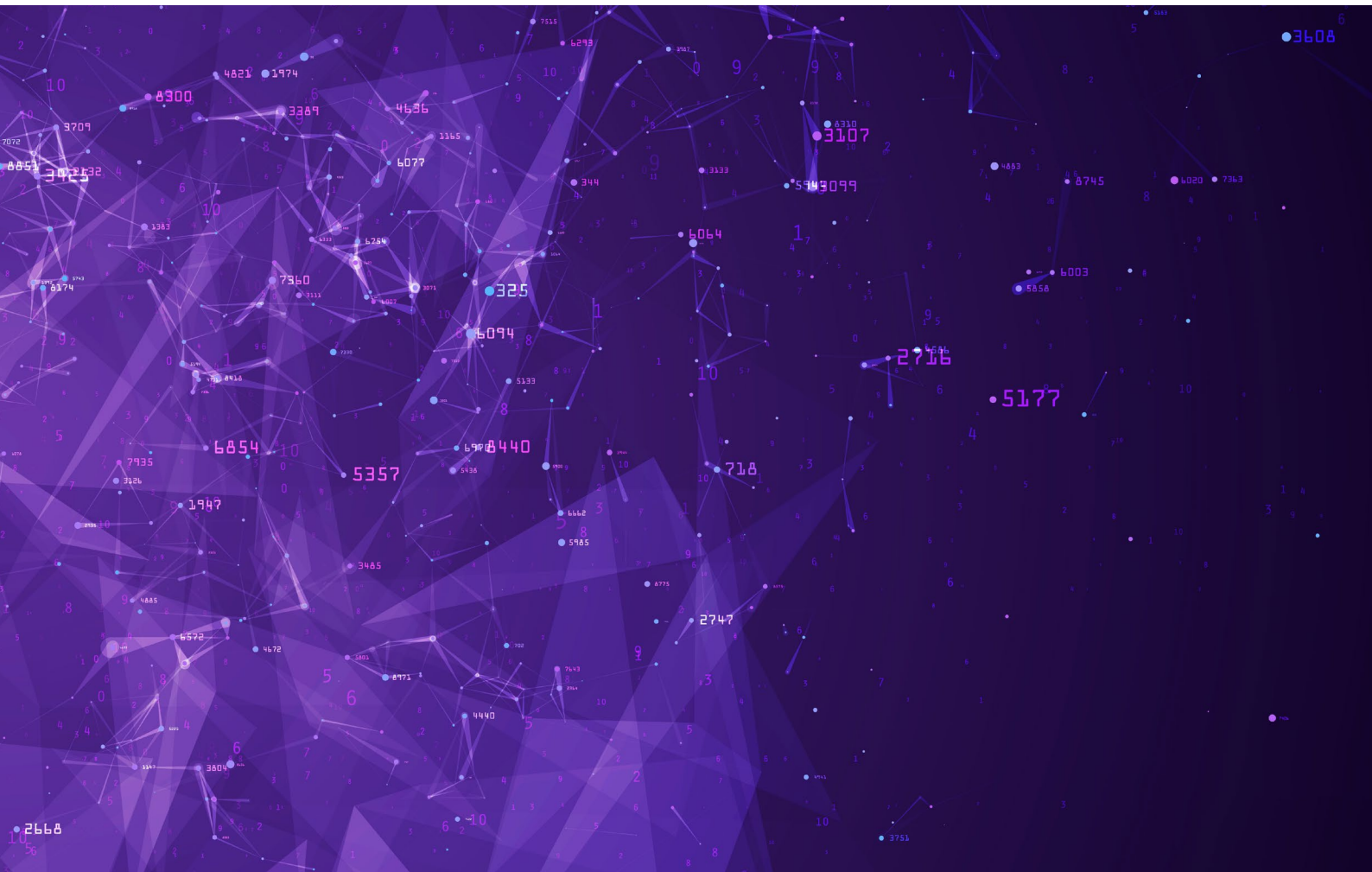
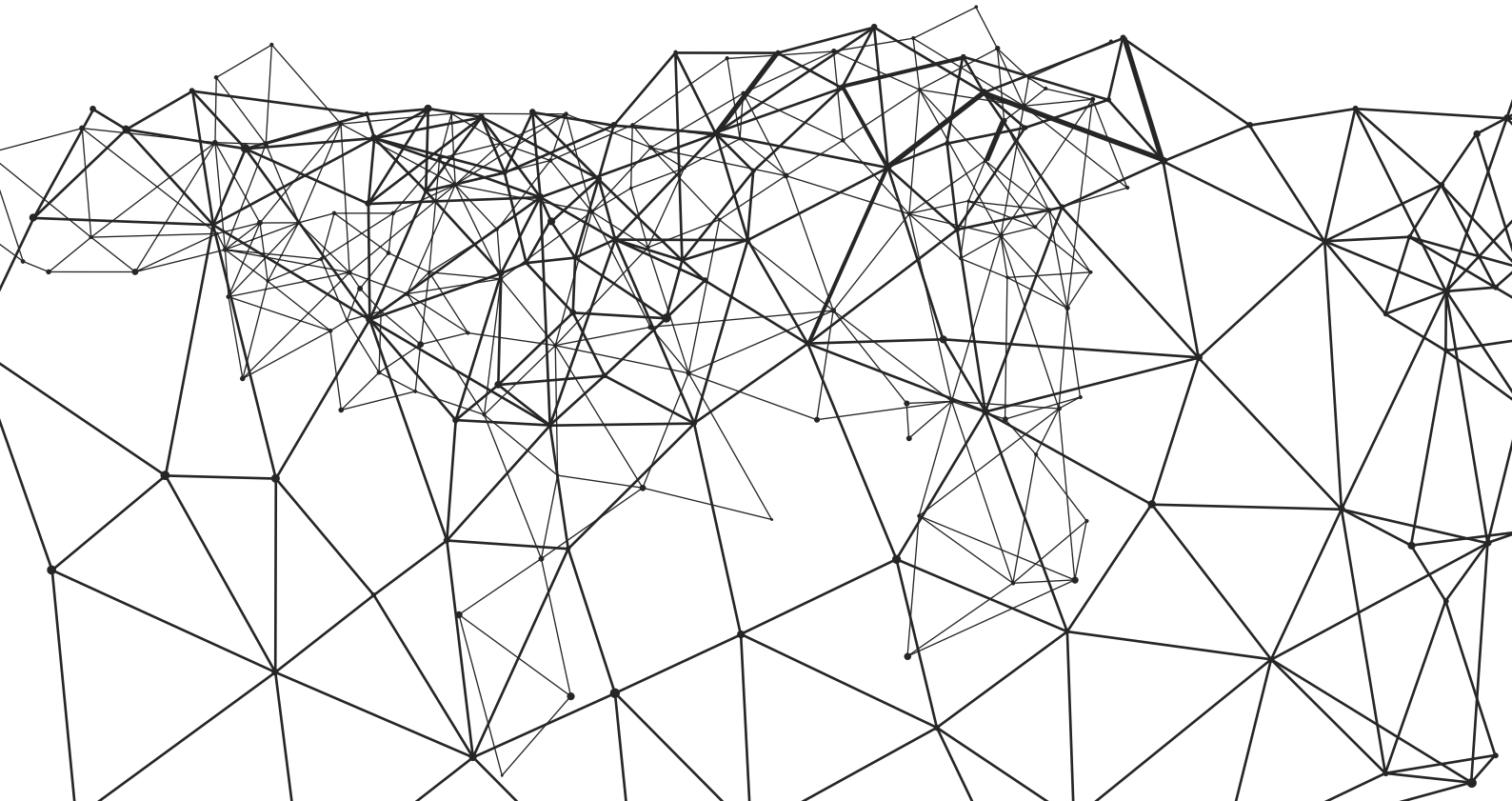
Iniciativa aporta

Descubriendo las claves de Blockchain



Contenido elaborado por Alejandro Alija, experto en Transformación Digital e Innovación.

Este estudio ha sido desarrollado en el marco de la Iniciativa Aporta desarrollada por el Ministerio de Energía, Turismo y Agenda Digital, a través de la Entidad Pública Empresarial Red.es, y en colaboración con el Ministerio de Hacienda y Función Pública. Los contenidos y los puntos de vista reflejados en esta publicación son responsabilidad exclusiva de su autor. El equipo Aporta no garantiza la exactitud de los datos incluidos en el estudio.



Existe mucha confusión sobre la diferencia entre Bitcoin y blockchain.

Blockchain fue la solución tecnológica adoptada para hacer funcionar los pagos mediante bitcoin (válida para casi cualquier moneda digital). Sería como distinguir entre Internet y los millones de sitios web en la world wide web.

Internet es la tecnología que soporta nuestra navegación por las páginas web y nos da acceso a inimaginables posibilidades como el correo electrónico, los pagos bancarios, el acceso a la televisión a la carta, entre otras muchas opciones.

¿Por qué es tan importante entonces Blockchain?

Blockchain modifica la forma en la que las personas, empresas u organizaciones de cualquier tipo realizamos transacciones. Transaccionar, negociar o hacer tratos son algunas de las acciones más cotidianas y antiguas de la humanidad. Abrir la puerta a hacer esto de forma radicalmente diferente a como se ha venido haciendo en los últimos miles de años merece un tipo de atención especial.

Desde un punto de vista conceptual, Blockchain es una tecnología que puede -para ciertas aplicaciones o sectores- eliminar intermediarios, también llamados terceros de confianza.
Por ejemplo, bancos, gobiernos, agencias de regulación, notarios, registradores, etc. Para explicarlo de forma práctica vamos a llevarlo al caso de los pagos digitales. Cuando Juan le quiere enviar dinero a su hermano Pedro, Juan realiza una transferencia bancaria a través de la página web de su banco. Esa t ransferencia es validada en su origen por el banco de Juan y posteriormente validada de nuevo por el banco de Pedro. Tras este proceso, el dinero de Juan pasa a la cuenta de Pedro y se descuenta de la cuenta de Juan. Blockchain abre la puerta a realizar esa transacción entre Juan y Pedro sin necesidad de la validación del banco (ni tan siquiera la figura del Banco). La transacción se realiza únicamente entre Juan y Pedro (a través de internet) y la red de participantes en la blockchain se encarga de validar la transacción. A día de hoy, esta transacción solo se puede realizar gracias a las criptomonedas como bitcoin y otras.

¿Cúal es ese problema tan importante que Blockchain resuelve?

En realidad, blockchain no es una nueva tecnología sino, la inteligente conjunción de un grupo de tecnologías bien establecidas que hasta este momento no se habían combinado en una única solución tecnológica. El conjunto de estas bien establecidas tecnologías es lo que define buena parte de las características que hacen única a blockchain. Blockchain vino a solucionar un problema clásico en la transacción de activos (cosas) digitales. Este problema es comúnmente conocido como el problema del doble gasto ("double spending" en inglés)

A través del siguiente ejemplo, vamos a tratar de explicar este problema:

Supongamos que estamos sentados en un banco del parque. Yo poseo una manzana y te la doy. Ahora tú tienes una manzana y yo no tengo ninguna.

Analicemos lo sucedido:

Yo te di la manzana en mano mientras tú podías observar cómo lo ejecutaba ya que ambos estábamos físicamente en el lugar en el que se producía la acción. No había necesidad de una tercera persona de confianza presente en aquel lugar y momento para ayudarnos a hacer la transacción o ejercer de tercero de confianza (juez, notario, etc.) y ratificar que yo te había traspasado mi manzana. Yo no puedo hacer nada más con esa manzana ya que ya no está en mi poder. Ahora la manzana te pertenece y tú puedes dársela a quien consideres o comerla. Así es como funciona el intercambio de cosas físicas entre personas. Incluso en este caso, cuando las personas intercambiamos bienes, existe la figura de un notario (una tercera persona, una autoridad de confianza) que da fe de que se ha realizado la transacción de acuerdo a las partes. Sin embargo, vamos a suponer ahora que nuestra manzana es una manzana digital (ceros y unos que representan una manzana). Tengo mi fichero de manzana digital y te lo envío. Aquí la cosa se empieza a poner interesante. ¿Cómo puedes tú tener la certeza de que la manzana digital que te he enviado es realmente mi manzana digital? ¿Cómo puedes saber que no se la he enviado a alguien más además de a ti? ¿Cómo puedes estar seguro de que no he hecho un millón de copias de mi manzana digital antes de enviártela y sigo en posesión de la misma?

El intercambio de información digital implica más desafíos que las transacciones físicas. En el mundo real, las transacciones se registran en un libro de transacciones o libro de contabilidad. Ese libro de contabilidad está habitualmente supervisado por una única persona o autoridad. Cuando ese libro es digital y está en manos de una única persona u organización existen problemas evidentes de manipulaciones, falsificaciones o creación de réplicas no autorizadas de ese libro.

¿Pero cómo soluciona realmente blockchain este problema?

¿Qué es esto de la cadena de bloques?

¿Es realmente una cadena?

La solución que propone BlockChain a estos desafíos es sencilla (la siguiente explicación es una simplificación con el objetivo de evitar excesivos tecnicismos).

Se llama cadena de bloques porque el sistema funciona de tal manera que las transacciones entre participantes (pares) de la red se van agrupando (y ordenando) en bloques. La información que contienen esos bloques se valida (proceso de minado en bitcoin) y finalmente, éstos se unen a la cadena. Cada bloque contiene su propia huella digital y la huella digital de su bloque predecesor. Estas huellas digitales son como un conjunto de llave y cerradura digital únicas. Cada llave es única en el mundo y solamente abre una única cerradura digital. De esta forma se compone la cadena. Los eslabones de la cadena son los bloques y sus uniones las huellas digitales de estos. Cada uno de los participantes en la red tiene su propia copia de esta cadena. Todas las copias están sincronizadas entre sí, de tal forma que cualquier cambio en una copia individual tiene que propagarse al resto. Realizar una modificación en la cadena de bloques es como intentar resolver el cubo de Rubick.

Supongamos que cada copia de la cadena es una cara del cubo. Si el cubo está resuelto, cada participante tiene un mismo color en su cara. Si un participante intenta modificar alguna línea de su cara (intenta modificar las transacciones en su copia de la cadena) automáticamente sería detectado por el resto, ya que las caras de los demás participantes se verían también afectadas.

¿Te he enganchado?
¿Te atreves con un nivel más en la cadena de bloques?

Pero, para entender realmente cómo es y cómo se construye la cadena de bloques necesitamos previamente entender algunos conceptos anteriores. A través de este ejemplo vamos a ver:

1. **Hashing o huella digital de la transacción**
2. **Cómo se forma un bloque**
3. **Cómo se une un bloque a la cadena**

1. **El Hash** es la huella digital única de nuestra transacción. Por transacción podemos entender cualquier cosa digital que queramos unir a la cadena de bloques. Puede ser un envío de dinero, una fotografía o el capítulo de un libro que hemos escrito. La magia del Hash está en que, con independencia del tipo de información que queramos enviar (o transaccionar), da igual la longitud y el tipo de esa información, el hash es una marca única y siempre con la misma estructura que se puede buscar, comparar y contrastar en cualquier momento.

Si quiero obtener el hash correspondiente a mi nombre - Alejandro- el algoritmo encargado de generar el hash (habitualmente SHA256 aunque existen otros) se encarga de generar la huella única de mi nombre:

30CC1CB006F560BE31DE08160F80E-FE06635BD3EFB8CB8745CF74D6CA-8F6D921

De la misma forma si quiero generar el hash de toda mi tesis doctoral (200 páginas) para identificarla de forma única, el algoritmo se encargará de generar un hash único exactamente de la misma longitud que el anterior que tan solo codifica mi nombre de 9 letras.

Los algoritmos de hash son muy interesantes por varias razones:

// Con tan solo modificar una sola letra de mi nombre, por ejemplo, en vez de Alejandro, escribo Alejandra, el hash cambia de forma radical reaccionando como si hubiera modificado por completo mi nombre. Vemos la diferencia:

Alejandro
30CC1CB006F560BE31DE08160F80E-FE06635BD3EFB8CB8745CF74D6CA-8F6D921
Alejandra
B 6 B D D E 0 3 5 6 D B E - 1F4104A8530A54E4C3F35BDFD9C-0FCC2D09167E033FE95D7774

// Además, la principal característica del hash es lo que se conoce como la "resistencia a la colisión". Esto es la capacidad del hash para que nadie pueda encontrar dos entradas distintas que generen un hash idéntico. Por esta razón el hash es una herramienta para comprobar la autenticidad de las cosas.

2. **Formación del bloque.** Un bloque es el conjunto mínimo de información que forma parte de la cadena. Es decir, un bloque puede contener un conjunto de transacciones. Esos bloques se van sumando a la cadena que, en definitiva, constituye ese libro distribuido del que ya hemos hablado.

Formación de un bloque en Bitcoin

Ahora bien, tenemos que buscar una forma competitiva de validar una transacción y dar por correcto un bloque. Aquí entra en juego el famoso proceso de minado. En realidad el proceso de minado es un cálculo matemático (efectuado por un ordenador) mediante el cual con los datos del bloque (identificador del bloque anterior y datos de las transacciones) se busca un número aleatorio (nonce) que unido a los datos anteriores, genera un hash que sea menor que un valor dado. Este valor define la dificultad del sistema. A mayor dificultad (y misma capacidad de cómputo), más tiempo se tarda en encontrar ese número nonce que dé con la solución del problema. Para garantizar e incentivar el funcionamiento de la red, el primero que encuentra ese número aleatorio se ve recompensado con una cantidad de bitcoins.

3. **Cadena de bloques.** Una vez validado el bloque tras este proceso, éste se envía al resto de participantes para su propia validación. Una vez hecho esto, el bloque se suma a la cadena, proporcionando el hash válido para este bloque (su identificador) que será usado en el siguiente minado para validar el siguiente bloque y así sucesivamente. Aquí es donde entra la cuasi-inviolabilidad (inmutabilidad) de la cadena. Dado que los bloques están enlazados mediante los hash. Cualquier mínimo cambio en el contenido de un bloque cambia el hash de ese bloque y subsecuentemente el hash del bloque siguiente. En el caso de que un atacante quiera modificar las transacciones en un bloque cualquiera de la cadena, tendría que volver a buscar ese número aleatorio de antes (nonce) para todos los bloques posteriores al actual bloque de la cadena. Además, cada participante de la red tiene su propia copia idéntica de la cadena. Así que, en caso de que una cadena individual mutara debido a una manipulación, esa manipulación quedaría invalidada, pues todas las demás copias de la cadena serían diferentes a la cadena mutada. Como en las caras del cubo de Rubik. Debido a que el proceso de minado (solo bitcoin) consume muchos recursos de cómputo de un ordenador, en la práctica es inviable re-minar una cantidad grande de bloques en una cadena.

¿Vemos un ejemplo práctico de cómo utilizar blockchain en una aplicación cotidiana?

El siguiente caso de aplicación se enmarca dentro de un grupo de aplicaciones en las que la tecnología Blockchain se aplica con el objetivo de hacer un proceso (existente) más rápido, más eficiente, con menor coste y sobre todo, garantizando la confianza en el proceso. ¡Vamos a ello!

Este ejemplo es completamente ficticio con el único fin de ilustrar una potencial aplicación de Blockchain en la vida cotidiana.

Supongamos que hemos comprado un billete de tren de alta velocidad para asistir a una reunión desde Madrid a Barcelona a primera hora. La empresa de trenes (el proveedor del servicio) asegura que en caso de retrasos superiores a 20 minutos se te reintegrará el 75% del coste del billete. En un proceso de este tipo en la actualidad, hemos de confiar en que el proveedor de servicio haga constar fehacientemente la hora de llegada del tren en la estación de destino y compruebe si el retraso es superior a esos 20 minutos. Hemos de confiar en que el reloj de la persona/sistema que marca la llegada del tren está perfectamente sincronizado y en hora. Nosotros, como pasajeros, nunca tendremos acceso a esa marca de tiempo en los sistemas de la empresa de trenes, así que hemos de asumir, que la empresa es confiable y aunque se haya producido un retraso de tan solo unos segundos, nos devolverán el dinero del billete. Nunca podremos comprobar ese dato y en caso de tener sospechas, podremos iniciar un tedioso proceso de reclamación que, probablemente, abandonaremos tarde o temprano dado que nos consumirá más energía y tiempo del que estimamos oportuno para reclamar el 75% de un billete de tren.

Estoy seguro de que esta situación nos sonará habitual a la mayoría de nosotros. Bien, este mismo proceso, modelado en caso de utilizar la tecnología blockchain se describiría de la siguiente manera:

En caso de haber comprado nuestro billete a través de una app de la empresa de trenes, obtendremos un billete digital con todas las características necesarias: fecha de compra, precio, salida, destino, nombre del comprador, identificador único del billete, condiciones de compra (turista, business, etc.). Esta información de compra del billete sería una transacción colocada en un bloque junto con el resto de compras de billetes del resto de participantes en la red. En

el momento del embarque en el tren, ese billete sería validado y esa transacción también sería ingresada en el blockchain en su correspondiente bloque. En el momento de la salida del tren, un sistema se encargaría de registrar el momento exacto de la salida, que a su vez sería una nueva transacción ingresada en la blockchain. Recordamos que, como participantes de una red abierta, todos podemos tener acceso a esa transacción única que representa la salida del tren. Todos tenemos nuestra propia copia de esta transacción - viajeros y empresa de trenes- En caso de que alguien intentara modificar la hora de salida, sería inmediatamente detectado pues el hash de la transacción hora de salida sería diferente e inválido comparado con el del resto de copias de la cadena.

Una vez llegado a destino, el mismo sistema que en origen se encargaría de registrar la hora exacta de llegada y comunicarlo como una nueva transacción en la red. Ahora llega la parte interesante, en caso de producirse un retraso que supere el umbral de los 20 minutos, un programa informático (smart contract o contrato inteligente), que a su vez forma parte de la blockchain, estaría programado para comparar hora de llegada frente a hora de salida y determinar en tiempo de retraso si lo hubiera. En caso de retraso superior a 20 minutos, el programa informático registraría una transacción en la red pública accesible por todas la partes. Nosotros, como viajeros consultaremos esa transacción de retraso en nuestra app.

Además, directamente a través de la app, podríamos ejecutar nuestro derecho a devolución del 75% del billete. Dado que la app está vinculada con la blockchain, nuestra solicitud de reembolso sería, de nuevo, una transacción registrada en la blockchain, que otro programa informático se encargaría de comprobar para efectuar el pago de nuestro reembolso.

Si has seguido sin dificultad este ejemplo, habrás visto que este proceso de reclamación modelado en tecnología blockchain, es:

// **Más transparente** para todos (viajeros, empresa de transporte, aseguradoras, etc.) puesto que la totalidad de las transacciones está siempre disponible.

// **Más eficiente** puesto que no hay intervención humana, formularios de reclamación, correos electrónicos, etc. La devolución se produce de forma automática.

// **Más seguro**, pues la probabilidad de fraude por todas las partes es muy baja.

// **Aporta más confianza** a los clientes de la empresa de trenes.

// **Más rápido**, puesto que todos los sistemas implicados (app de usuario, sistemas de compra de billetes, sistema de registro de salida y llegada de trenes) están sincronizados en la blockchain.

A pesar de estos beneficios, blockchain todavía es una tecnología incipiente en el mercado y son pocas las empresas u organismos que han implementado iniciativas reales de este tipo. Actualmente las empresas se encuentran en una fase de "realización de pilotos", muchas veces fáciles de escalar e implementar en diversas áreas.

Uno de los motivos de esta situación es que todavía quedan una serie de retos por resolver, algunos de los cuales se resumen a continuación:

Falta de talento cualificado, lo cual hace necesario invertir en la formación y el desarrollo de nuevas capacidades.

Necesidad de mejorar las prácticas de seguridad electrónica de los ciudadanos, promoviendo la gestión adecuada de claves.

Necesidad de adaptar las estructuras

Mejora de la capacidad de adaptación a los cambios regulatorios y normativos, tanto actuales como futuros, necesarios para dar soporte a esta tecnología.

Resistencia al cambio de los distintos perfiles implicados, por lo que es recomendable implementar políticas de transparencia y comunicación abierta.

A pesar de estos retos, los expertos creen que las múltiples ventajas ya mencionadas de transparencia, eficiencia y seguridad pesarán más que estos desafíos, e impulsarán la inversión. Por ello, se prevé que el mercado global de blockchain aumente de los 0.297 mil millones de dólares en 2017 a 4,401 mil millones en 2022, lo que supone una tasa de crecimiento anualizado (CAGR 2017-2022) de 71,46%.

Descubriendo las claves de Blockchain

Iniciativa aporta