

Blockchain la tecnología que está en boca de todos

Joan Berenguer. Director Infraestructuras tecnológicas

¿Que es Blockchain?

Es una tecnología en crecimiento, basada en un conjunto de protocolos en Internet, que está cambiando la forma en que las entidades y particulares interactuamos a través de la red. Permite realizar transacciones seguras en línea tales como darnos de alta en organizaciones, liquidación de fondos, pagos en moneda o cualquier otra clase de activos sin necesidad de que intervengan intermediarios de confianza que den validez a dichas operaciones.

Profundizando un poco más desde un punto de vista técnico, una blockchain (cadena de bloques) está formada por una lista de archivos los cuales están enlazados entre si de forma segura mediante criptografía avanzada. Cada bloque básicamente contiene un enlace a un bloque anterior, una fecha de registro y los datos de la transacción. Por diseño, los bloques son intrínsecamente resistentes a la modificación de los datos guardados.

Una blockchain se puede considerar como una base de datos descentralizada y distribuida que se utiliza para registrar transacciones entre muchas computadoras, de modo que los registros no pueden modificarse retroactivamente sin el consenso de toda la red implicada. Esto permite a los participantes verificar y auditar las transacciones y reconciliar obligaciones de manera eficiente y económica. Este último punto es el que, a mi entender, está potenciando el crecimiento de esta tecnología llamando la atención de muchas entidades que hasta la fecha utilizaban mecanismos tradicionales mas costosos y complejos.

¿Cuáles son las principales características?

1. Descentralización: No existe un operador central. Los datos están replicados en todos los bloques por lo se elimina la dependencia de un nodo central.
2. Mecanismo consensuado: Todos los participantes en el sistema llegan a un acuerdo que contiene el conjunto de reglas para ejecutar las transacciones, las cuales quedan registradas en el tiempo dentro de ese proceso.
3. Irreversible: Las operaciones que han sido ejecutadas no pueden ser posteriormente modificadas dando al sistema la rigurosidad necesaria. Las reglas para resolución de conflictos y remediación deben ser establecidas previamente.
4. Interoperabilidad: es una plataforma abierta lo que permite que esta red pueda ser integrada con todo tipo de registros y entidades que quieran participar, incluyendo las tradicionales instituciones financieras y bancos centrales.
5. Basado en Identidades: La firma digital habilita a los participantes a autorizar y verificar transacciones e identificar a las contrapartes que realizan estas.

6. Seguridad: cuentas, saldos y otras transacciones quedan protegidos por las técnicas criptográficas más avanzadas.

¿Cuáles son sus orígenes?

Aunque los primeros trabajos sobre cadenas con cifrado seguro entre bloques se remontan a principios de la década de los noventa, podemos considerar que la puesta en escena del primer blockchain fue con la llegada de Bitcoin sobre el año 2009. Bitcoin, como criptomoneda resolvía el problema en el mundo digital del multiple gasto (utilizar el mismo pago más de una vez de forma fraudulenta) sin necesidad de tener que acudir a una institución financiera. En un mundo físico sería el equivalente a falsificar moneda. Otra cosa es el reconocimiento actual de esta criptomoneda por las entidades financieras y bancos centrales.

Bitcoin fué la inspiración para que posteriormente otras iniciativas tales como Ripple (2012) y Ethereum (2015) aparecieran como parte de plataformas abiertas para el intercambio de transacciones. Aunque estas últimas aportan ventajas como mayor seguridad y velocidad, no está claro cual será la adoptada por la mayoría y actualmente hay múltiples iniciativas enfocadas a blockchains abiertos o privados.

Grandes fabricantes y consultoras tecnológicas están invirtiendo en plataformas y aplicaciones para facilitar y potenciar el uso de esta tecnología. Como siempre, las vinculadas a entornos financieros y tecnológicos (las llamadas Fintech) son las que lideran este barco, pero también hay otras como por ejemplo la reciente alianza ID2020 entre diversas entidades públicas y privadas con el objetivo de solucionar problemas de exclusión de identidad a nivel mundial.

ID2020 se ha desarrollado sobre la creencia de que la identidad personal es un requisito previo para la inclusión social y económica en el mundo moderno y promueve el derecho a que todo el mundo tenga acceso a conceptos tan básicos como la educación, la salud, o la justicia; como millones de refugiados pueden probar que existen y por lo tanto poder reclamar así sus derechos?

¿Cuáles pueden ser los casos de uso?

El principal uso de los blockchains suele asociarse a entornos financieros y criptomonedas, pero se están desarrollando iniciativas orientadas en sectores y aplicaciones de todo tipo: transporte, administración pública, salud, notariado, seguros, IoT (Internet de las cosas) en compañías de agua, gas y electricidad, suministros al pormenor,...

Caso 1: Pagos Internacionales entre entidades financieras donde, en lugar utilizar los costosos y lentos métodos tradicionales, adoptando plataformas basadas en Ripple pueden agilizar y abarcar las transacciones.

Caso 2: Contratos Inteligentes y otro tipo de documentos que pueden ser registrados y validados en fecha y firma criptográfica sin intervención humana vinculando así a las partes implicadas.

Caso 3: Gestión de Identidades, que combinadas con biometría (huellas, voz, reconocimiento facial, etc) agilizan los procesos de inscripción de clientes en entidades de todo tipo sin requerir la presencia física de estos. Esto habilita un marco legal/contractual para que se puedan realizar operaciones como firma digital de

documentos, compra y venta de activos, intercambio de información confidencial o sensible, etc. Otro ejemplo de uso es la iniciativa ID2020 citada anteriormente.

Conclusiones

Es indiscutible que blockchain está cambiando, entre otras cosas, el mundo de los negocios en internet y que directa e indirectamente esto nos tiene que aportar beneficios a los ciudadanos de a pie. Todavía hay muchas cuestiones de todo tipo a solventar (estándares, legales, regulatorias, financieras, etc.) y existe una resistencia al cambio de sectores más tradicionales que se podrían sentir amenazados. Sin embargo, yo creo que el avance es imparable y prevalecerá aquello de que "si no puedes con tu enemigo, únete a él"