Qué es blockchain: la explicación definitiva para la tecnología

17 Noviembre 2017 Actualizado 23 Septiembre 2018, 11:59

Javier Pastor

8901 publicaciones de Javier Pastor

¿Qué es el blockchain? Entre otras cosas, es una de las palabras de moda en los últimos tiempos. La cadena de bloques es también un concepto que plantea una enorme revolución no solo en nuestra economía, sino en todo tipo de ámbitos.

Entender lo que es esa cadena de bloques no es tan difícil, y dado que cada vez se utiliza más este concepto hemos querido hacer una especie de curso rápido de introducción al blockchain, para explicar qué es, cómo funciona y cuál es esa revolución que plantea la cadena de bloques.

Adiós, señor (banquero) intermediario

Pongámonos en situación. Lo normal es que si una persona llamada por ejemplo Mariano quisiera enviarle 1.000 euros a otra persona llamada por ejemplo Luis, lo normal es que la operación se realizase a través de un banco. Ese banco actúa como intermediario de esa y otras muchas transacciones, centralizando de forma efectiva el movimiento de capital de un lado a otro.

Mariano le pediría a su banco que retirara 1.000 euros de su cuenta y los transfiriese a la cuenta de Luis: en apenas unas horas (dependiendo del banco, claro) ese banco habrá anotado en su cuenta la transacción, restando 1.000 euros en su cuenta y comunicando al otro banco que debe añadir 1.000 euros en la cuenta de Luis. Alguien en el banco de Luis (a estas alturas, ya sabemos que ese

alguien es un programa informático) anotará que en la cuenta de Luis hay 1.000 euros más procedentes de la cuenta bancaria de Mariano.

Esa gestión no ha necesitado de un trasiego de billetes de un lado a otro, sino que simplemente ha habido uno o dos bancos que se han encargado de hacer que el dinero pase de uno a otro con un simple cambio en los balances de sus cuentas. Todo estupendo y fantástico, salvo por un problema:

Que ni Mariano ni Luis tienen control alguno sobre el proceso, del que solo esos bancos tienen toda la información. Ambos dependen de esos bancos y de su forma de hacer las cosas para completar esa transacción. Están sujetos a sus condiciones (y a sus comisiones, por supuesto).

En Xataka
Bitcoin, blockchain y criptomonedas, explicado de forma sencilla (y en vídeo)

Hola, cadena de bloques

Es ahí donde entra la cadena de bloques, que básicamente elimina a los intermediarios, descentralizando toda la gestión. El control del proceso es de los usuarios, no de los bancos —seguimos hablando del dinero, pero el ejemplo es extrapolable a otros tipos de transacción—, y son ellos los que se convierten básicamente parte de un enorme banco con miles, millones de nodos, cada uno de los cuales se convierte en partícipe y gestor de los libros de cuenta del banco.

¿Qué es entonces la cadena de bloques? Pues un gigantesco libro de cuentas en los que los registros (los bloques) están enlazados y cifrados para proteger la seguridad y privacidad de las transacciones. Es, en otras palabras, una base de datos distribuida y segura (gracias al cifrado) que se puede aplicar a todo tipo de transacciones que no tienen por qué ser necesariamente económicas.

Esa cadena de bloques tiene un requisito importante: debe haber varios usuarios (nodos) que se encarguen de verificar esas transacciones para validarlas y que así el bloque correspondiente a esa transacción (en cada bloque hay un gran número de transacciones que eso sí, es variable) se registre en ese gigantesco libro de cuentas.

Así funciona una transacción en la cadena de bloques

El proceso es relativamente sencillo, pero como decimos implica a más personas. Ahora Mariano y Luis no están solos, y formarán parte de un gran grupo de usuarios que se encargan de comprobar que todo el proceso se produce como debe producirse.

Cómo f

1 A quiere enviar dinero a B

2

4 Los que están en la red aprueban que la transacción es válida

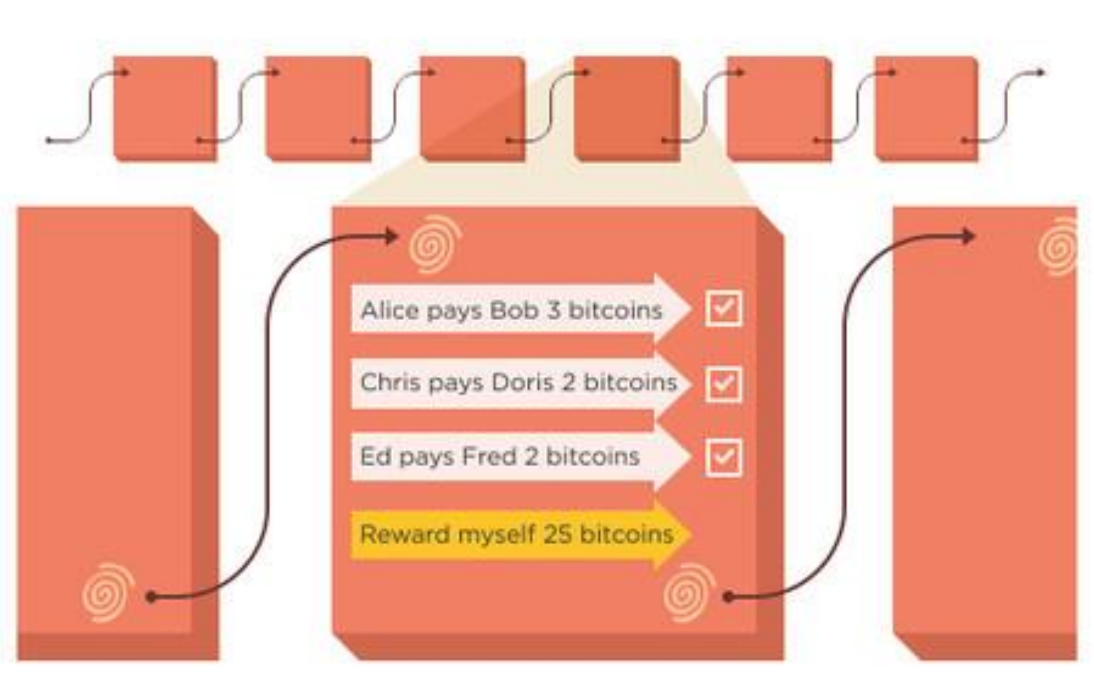
Si Mariano quiere retirar un bitcoin de su cuenta para dárselo a Luis, primero avisa a todo el mundo con una peculiaridad: nadie sabe que Mariano es Mariano y que Luis es Luis. Solo saben que desde una cartera digital (lo que sería una cuenta bancaria) se quiere transferir esa cantidad (que sí se conoce) a otra.

Mariano, por lo tanto, avisa de sus intenciones, pero sin revelar su identidad: "¡Eh, chicos, quiero mandarle un bitcoin desde mi cartera a esta otra, por favor, actualizad vuestros libros de cuentas!". Al enviar ese mensaje, todos los usuarios de esa red primero comprueban que ~~Mariano~~ la cartera de origen tiene suficiente dinero para enviárselo a la cartera de destino. Si es así, todos anotan esa transacción, que pasa a completarse y a formar parte del bloque de transacciones. Eso sí: todavía no están registrados en esa base de datos de forma definitiva.

A medida que pasa el tiempo, más y más transacciones van completándose y pasando a ese bloque, que tiene una capacidad limitada que depende de la estructura de la cadena de bloques y del tamaño de cada transacción. Cuando un bloque ya no admite más transacciones, llega un momento importante: el de "validarlo" o "sellarlo", que es lo que los usuarios hacen cuando hacen minería de bitcoin.

Soy minerooo ♫♪

Ese minado de bloques consiste en la realización de una serie de complejos cálculos que requieren tiempo y (cada vez más) electricidad, pero cuando el proceso esos bloques quedan registrados de forma permanente en esa cadena de bloques, y no pueden ser modificados sin que se alteren todos los bloques que están enlazados con él, una operación que además necesitaría que la mayoría de los nodos la validasen.



En esa red P2P los mineros reciben avisos de nuevas transacciones y las reúnen en un nuevo bloque, pero lo hacen además compitiendo con otros mineros, porque el primero que logra crear un bloque válido y lo sella recibe bitcoins (si está minando bitcoins, claro) por ese servicio. Gracias al uso de una cadena de bloques común que se sincroniza entre los nodos se logra la irreversibilidad de las transacciones, lo que permite que nadie "truque" el sistema o haga fraudes para beneficiarse, modificando el libro de cuentas para desviar dinero (bitcoins) de un lado a otro sin que otros se enteren.

De hecho añadir nuevos bloques es un proceso cada vez más costoso, lo que hace normalmente que los mineros trabajen agrupados (los famosos "pools" que funcionan de forma similar a una cooperativa) en lugar de trabajar por sí mismos ("solo mining", con unas probabilidades de éxito/recompensa muy bajas). Cuando uno de los mineros resuelve el problema criptográfico que representan los cálculos para "sellar" un bloque, avisa a los demás, que comprueban que efectivamente es así y añaden ese bloque a la cadena de bloques completa que tienen en sus ordenadores.

Ese libro de cuentas no solo está distribuido y es seguro: los bloques enlazados (de ahí lo de cadena de bloques) cuentan con un puntero hash (codificado) que enlaza al bloque anterior, además de una marca de tiempo y los datos de la transacción, y esa información es pública. ¿Qué significa eso? Que la cadena de bloques, aunque protege la privacidad de sus usuarios, sí que permite controlar la trazabilidad de esas transacciones.

O lo que es lo mismo: permite saber todo el camino que ha seguido el bitcoin de la cartera que pertenece a alguien (en este caso a Mariano, aunque su identidad no se conoce por el resto de usuarios) antes de llegar a la cartera de otro alguien (de Luis, aunque su identidad no sea conocida por el resto de usuarios).

El propio diseño de la cadena de bloques tiene ventajas claras, y por ejemplo confirma que cada unidad de valor (por ejemplo, cada bitcoin) solo se ha transferido una única vez, lo que evita el tradicional problema con el doble gasto de monedas digitales o con el dinero falso, que reduce la confianza de los usuarios en esa moneda y también en la propia circulación de la misma.

De ICOs y cadenas de bloques

Uno de los conceptos que más están apareciendo al hablar de las criptodivisas y las cadenas de bloques es el de las ICO, las *Initial Coin Offerings*.

Una ICO es como explicamos en profundidad una forma de financiación de un proyecto empresarial que en lugar de ofrecer acciones ofrece tokens virtuales, o lo que es lo mismo, nuevas critpodivisas.

Estas nuevas criptodivisas tienen cierto valor hipotético debido a su escasez y demanda, y están directamente asociadas al proyecto empresarial que las crea, como ocurre con ejemplos muy conocidos como el del navegador Brave: si ese proyecto triunfa, las criptomonedas en las que se basó su financiación ganan valor y eso acaba ofreciendo un interesante retorno de la inversión para los inversores.

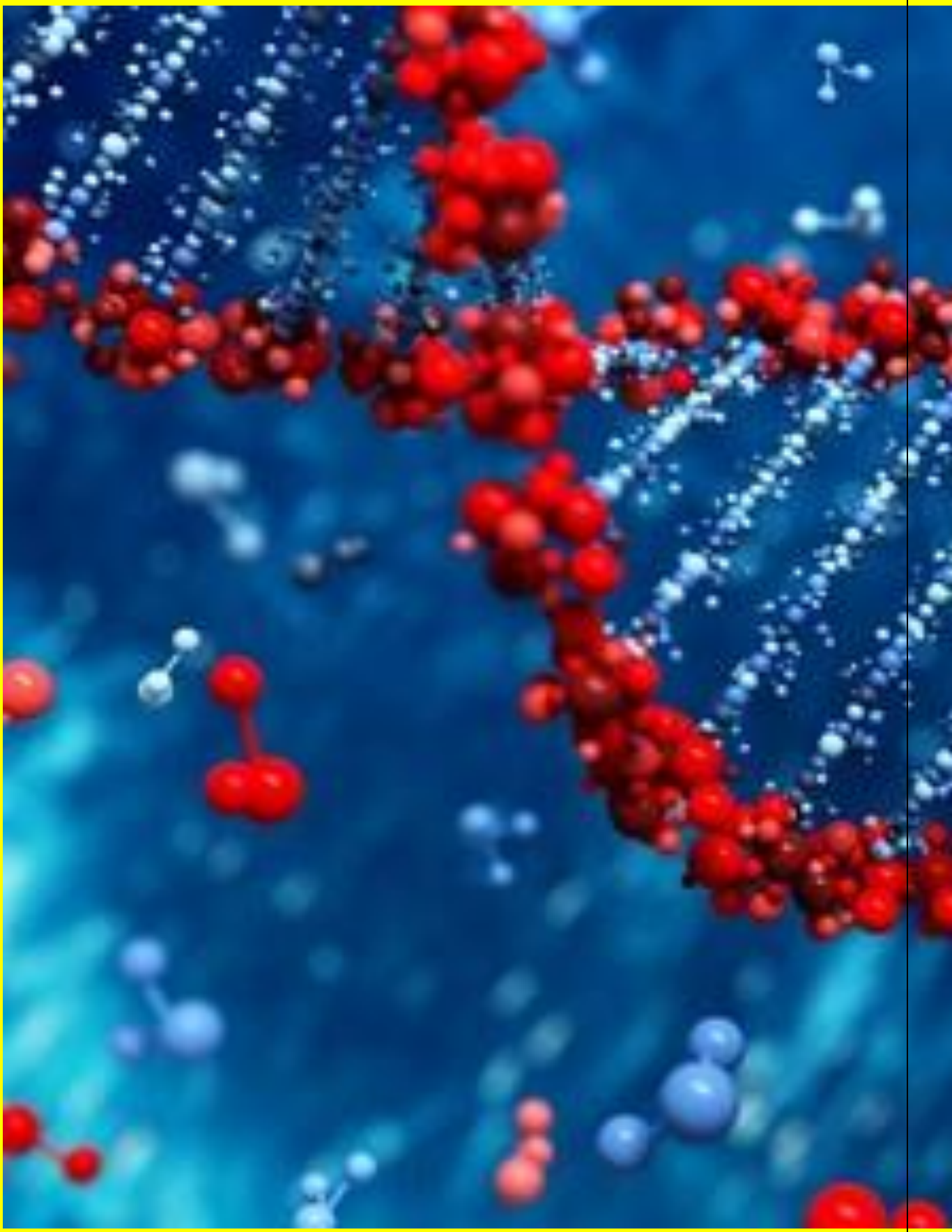
El funcionamiento es por tanto similar al de las ofertas públicas de venta, pero en lugar de comprar acciones de una empresa —una que además tiene un producto en el mercado y que ha pasado por rigurosos controles financieros antes de poder hacer su OPV— compramos criptodivisas en una operación con un formato mucho más incierto, sin regulación alguna y en el que básicamente estamos "apostando" por el futuro de ese proyecto empresarial con muchas menos pruebas o garantías de que ese futuro éxito se produzca.

El componente especulativo, como en todo lo que rodea actualmente a las criptodivisas, es muy alto, y de hecho hay quien califican a las ICO como la mayor estafa nunca vista, pero también hay claros defensores de un modelo de financiación cada vez más atractivo.

Todas estas nuevas criptodivisas se apoyan en una cadena de bloques que soporta la estructura de ese nuevo token virtual. La más utilizada es la de Ethereum por su versatilidad y por la facilidad que plantea esa plataforma. Un desarrollador explicaba recientemente cómo crear una de estas cadenas de bloques fácilmente a partir de Geth, una de las implementaciones más conocidas (en este caso, en lenguaje Go, de ahí el nombre, "Go Ethereum") del protocolo ethereum.

La cadena de bloques más allá de la economía

Aunque la cadena de bloques está íntimamente relacionada con las nuevas criptodivisas o criptomonedas, es lógico preguntarse si este sistema sería válido para otro tipo de transacciones, y la respuesta es un rotundo sí.



De hecho eso es lo que está intentando lograr desde sus inicios la plataforma Ethereum, que tiene su propia cadena de bloques (podéis echarle un vistazo en

sitios como Etherscan.io) y su propia moneda, llamada Ether. A diferencia de bitcoin, las transacciones aquí son los contratos inteligentes —los programadores aman este concepto—, que pueden ser más o menos complejos y que permiten definir todo tipo de transacciones.

Al igual que ocurre con bitcoin, lo bueno de esas transacciones es que se mantendrán en la cadena de bloques, inalterables y accesibles durante toda la vida de esa cadena de bloques. Si nos vamos al extremo, Ethereum podría sustituir básicamente a cualquier intermediario, sustituyendo productos y servicios que dependen de terceros para estar totalmente descentralizados.

Por supuesto esta es solo una de las alternativas que se han originado con la cadena de bloques como protagonista, y de hecho hay muchas ideas que tratan de explotar las bondades de una tecnología que tiene un alcance virtualmente ilimitado. Veamos algunos ejemplos:

- **Consorcio R3: las propias entidades financieras que muchos tratan de reemplazar con bitcoin o Ethereum han creado el consorcio R3 para averiguar cómo aprovechar la cadena de bloques en los sistemas financieros tradicionales. Uno de los primeros problemas de la aplicación de este esquema es el anonimato que proporciona el diseño de la cadena de bloques, algo que han resuelto con el llamado "libro de contabilidad autorizado" ('permissioned ledger'), una variante muy peculiar de la cadena de bloques de bitcoin, por ejemplo, que sí que identifica a los usuarios que añaden bloques y que hace que las transacciones del sistema solo puedan consultarse por ciertas partes.**
- **Registro de propiedades: el gobierno japonés ha iniciado un proyecto para unificar todo el registro de propiedades urbanas y rústicas con tecnología de cadena de bloques, lo que permitiría contar con una base de datos abierta en la que se pudieran consultar los datos de las 230 millones de fincas y 50 millones de edificios que se estima existen en el país asiático. En Dubai están planeando algo muy parecido.**
- **Pagos en el mundo real: una startup llamada TenX ha creado una tarjeta prepago que se puede recargar con distintas criptodivisas para luego pagar con ella en cualquier sitio como si esa tarjeta tuviera dinero convencional, sin importar si ese establecimiento acepta o no este tipo de monedas virtuales.**
- **Carsharing: la empresa EY, subsidiaria de Ernst & Young Global Ltd está desarrollando un sistema basado en la cadena de bloques que permite a empresas o grupos de personas acceder a un servicio para compartir coches de forma sencilla. El llamado Tesseract permitiría registrar quién es el propietario del vehículo, el usuario de ese vehículo y generar los costes basados en el seguro y otras transacciones en este tipo de servicios.**
- **Almacenamiento en la nube: normalmente los servicios de almacenamiento están centralizados en un proveedor específico, pero la empresa Storj quiere descentralizar este servicio para mejorar la seguridad y reducir la dependencia de ese proveedor de almacenamiento.**
- **Identidad digital: los últimos y gigantescos fallos de seguridad y robos de datos han hecho que la gestión de nuestras identidades se convierta en un problema muy real. La cadena de bloques podría proporcionar un sistema**

único para lograr validar identidades de forma irrefutable, segura e inmutable. Hay muchas empresas desarrollando servicios en este ámbito, y todas ellas creen que aplicar la tecnología de la cadena de bloques para este propósito es una solución óptima.

- **Música: aunque hay críticas que afirman que esta opción no tiene validez, hay quien afirma que la distribución musical podría sufrir toda una revolución si se lograra implantar un sistema basado en la cadena de bloques para gestionar su reproducción, distribución y disfrute. La mismísima Spotify está apostando fuerte por su propia cadena de bloques.**
- **Servicios públicos/gubernamentales: otro de los ámbitos más interesantes de la aplicación de la cadena de bloques es en los servicios públicos que podrían presumir así de una transparencia absoluta. Las áreas de actividad son múltiples: desde la gestión de licencias, transacciones, eventos, movimiento de recursos y pagos, gestión de propiedades hasta la gestión de identidades. De hecho el robo masivo de datos en Equifax han hecho que algunos propongan la sustitución de los números de la seguridad social en Estados Unidos con un sistema basado en la cadena de bloques. Hay iniciativas incluso para "descentralizar el gobierno", y Bitnation es una de esos proyectos que tratan de llamarnos convertirnos en "ciudadanos del mundo".**
- **Seguridad social y sanidad: aunque se podría englobar dentro de los servicios públicos mencionados, la sanidad pública podría sufrir una verdadera revolución con un sistema de cadena de bloques que sirviera para registrar todo tipo de historiales médicos y resolver uno de los problemas clásicos de la gestión de la sanidad.**
- **Gestión de autorías: aunque relacionado con lo mencionado para el mundo de la música, Ascribe es una plataforma que trata de ayudar a creadores y artistas a atribuirse la autoría de sus trabajos a través de la cadena de bloques. Hay otras muchas plataformas en este ámbito (Bitproof, Blockai, Stampery, por ejemplo) que entre otras cosas permiten generar tiendas en las que se puedan comprar trabajos originales de una forma segura y sencilla.**

Son tan solo algunos ejemplos de la aplicación de la cadena de bloques a todo tipo de ámbitos, pero hay muchísimos más: la versatilidad de esta tecnología es tan enorme que es difícil pensar en un área que no pueda ser transformada por esta idea.

En Xataka
El revolucionario blockchain sigue sin demostrar lo revolucionario que es

De momento, eso sí, todas estas ideas son solo proyectos en pleno desarrollo, por lo que la revolución, aunque posible, parece lejana, sobre todo cuando los intermediarios (en todos los ámbitos) se han convertido en parte integral de la economía y la sociedad. Descentralizar todas estas industrias es mucho más complejo de lo que parece, sobre todo porque esos mismos intermediarios tratarán de rechazar esos cambios o adaptarlos a sus propias necesidades.

Qué es blockchain e introducción a criptomonedas, en vídeo

Con Carlos Domingo

https://youtu.be/01eMdxe9tds