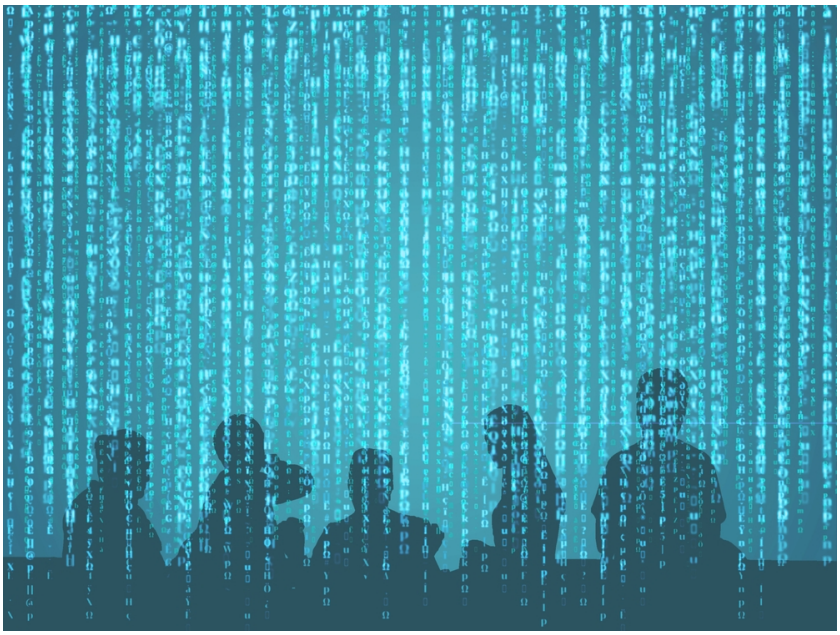
Parlamento europeo

Cómo puede cambiar nuestra vida la tecnología de la cadena de bloques



ANÁLISIS EN PROFUNDIDAD

EPRS | Servicio de Estudios del Parlamento Europeo
Autor: Philip Boucher
Unidad de Previsión Científica (STOA)
PE 581.948

ES

.

Cómo puede cambiar nuestra vida la tecnología de la cadena de bloques

Análisis en profundidad

Febrero de 2017

PE 581.948

AUTORES

Philip Boucher, Unidad de Prospectiva Científica (STOA), DG EPRS, Parlamento Europeo

Susana Nascimento, Unidad de Estudios Prospectivos, Aportaciones de las Ciencias del Comportamiento y Diseño de Políticas, DG CCI, Comisión Europea (capítulos 6 a 8)

Mihalis Kritikos, Unidad de Prospectiva Científica (STOA), DG EPRS, Parlamento Europeo (secciones de formulación de políticas de anticipación)

VERSIONES LINGÜÍSTICAS

Original: EN
DE, ES, FR, IT, PL, PT

SOBRE EL EDITOR

Para ponerse en contacto con STOA o suscribirse a su boletín mensual, escriba a: STOA@ep.europa.eu
Este documento está disponible en la siguiente dirección de Internet: http://www.ep.europa.eu/stoa/

Manuscrito terminado en febrero de 2017

EXENCIÓN DE RESPONSABILIDAD

PE 581.948
ISBN 978-92-846-1046-4
doi: 10.2861/087736
QA-02-17-043-ES-N

Índice

Cómo puede cambiar nuestra vida la tecnología de la cadena de bloques

Las cadenas de bloques son una forma notablemente transparente y descentralizada de registrar listas de transacciones. Su uso más conocido son las monedas digitales, como Bitcoin, que anunció al mundo la tecnología de la cadena de bloques con un aumento del valor del 1 000 % en el transcurso de un solo mes en 2013 que acaparó titulares. Esta burbuja explotó con rapidez, pero el crecimiento continuo desde 2015 significa que las bitcoins están más valoradas ahora que nunca.

Hay muchas formas diferentes de utilizar cadenas de bloques para crear nuevas monedas. Se han creado cientos de estas monedas con distintas características y objetivos. El modo en que las transacciones con monedas basadas en cadenas de bloques crean registros públicos rápidos, baratos y seguros implica que también pueden utilizarse para numerosas tareas no financieras, como votar en las elecciones o demostrar que un documento existió en un momento determinado. Las cadenas de bloques son especialmente idóneas para situaciones en las que es necesario conocer historiales de propiedad. Por ejemplo, podrían ayudar a gestionar mejor las cadenas de suministro, con el fin de ofrecer la certeza de que los diamantes se han extraído de manera ética, las prendas de ropa no se han confeccionado en talleres clandestinos y el champán viene de Champagne. Podrían ayudar a resolver por fin el problema de la piratería de música y vídeo, permitiendo al mismo tiempo comprar, vender, heredar o regalar legítimamente medios digitales como libros, discos de vinilo y cintas de vídeo. También ofrecen oportunidades en todos los tipos de servicios públicos como sanidad y prestaciones sociales y, en la frontera del desarrollo de la cadena de bloques, son contratos autoejecutables que allanan el camino para que las empresas se dirijan solas sin intervención humana.

Las cadenas de bloques transfieren el control de las interacciones cotidianas con la tecnología, alejándolo de las élites centrales y redistribuyéndolo entre los usuarios. Con ello, hacen que los sistemas sean más transparentes y, quizá, más democráticos. Dicho esto, probablemente no generen a una revolución. De hecho, los Gobiernos y los gigantes de la industria que invierten grandes sumas de dinero en investigación y desarrollo de la cadena de bloques no están tratando de quedarse obsoletos, sino de mejorar sus servicios. También hay otras cuestiones generales que considerar. Por ejemplo, la transparencia de la cadena de bloques está bien para asuntos de dominio público como los registros catastrales, pero ¿qué ocurre con los saldos bancarios y otros datos sensibles? Es posible (aunque solo a veces y con un esfuerzo sustancial) identificar a las personas asociadas a las transacciones, lo que podría comprometer su privacidad y anonimato. Aunque algunas cadenas de bloques sí ofrecen anonimato total, cierta información sensible simplemente no debería distribuirse de esta manera. No obstante, aunque las cadenas de bloques no sean la solución a todos los problemas y no revolucionen todos los aspectos de nuestra vida, podrían tener una repercusión sustancial en muchos ámbitos y es necesario estar preparados para las dificultades y oportunidades que presentan.

Este informe ofrece un punto de entrada accesible a las personas del Parlamento Europeo y fuera de él que estén interesadas en aprender más sobre el desarrollo de la cadena de bloques y sus posibles repercusiones. El objetivo es estimular la reflexión y el debate sobre esta complicada y controvertida tecnología en rápida evolución. El informe no es secuencial, por lo que se invita a los lectores a escoger las selecciones que les interesen y leerlas en cualquier orden. La sección inmediatamente posterior presenta una introducción sobre cómo funciona la tecnología de la cadena de bloques. Cada una de las ocho secciones siguientes presenta resúmenes de dos páginas sobre cómo puede utilizarse en distintos ámbitos de aplicación, sus posibles repercusiones y sus implicaciones para la política europea. Por último, la sección final recoge algunas observaciones generales y posibles respuestas al desarrollo de la cadena de bloques.

¿Cómo funciona la tecnología de la cadena de bloques?

Antes de intentar entender cómo funcionan los libros contables de la cadena de bloques, merece la pena echar un vistazo a los libros contables tradicionales. Durante siglos, los bancos han utilizado libros contables para mantener bases de datos de las transacciones de cuentas, y los gobiernos los han utilizado para llevar registros de la propiedad de tierras. Hay una autoridad central —el banco o el organismo público— que gestiona las modificaciones en el registro de las transacciones, por lo que puede identificar quién es propietario de qué en un momento dado. Esto les permite comprobar que las nuevas transacciones son legítimas, que no se han gastado dos veces los mismos 5 EUR y que no se venden casas que no pertenecen a los vendedores. Puesto que los usuarios confían en que el gestor del libro contable comprueba adecuadamente las transacciones, las personas pueden comprar y vender entre sí aunque no se hayan visto nunca ni se fíen una de la otra. El intermediario también controla el acceso a la información que figura en el libro contable. Podría decidir que cualquiera pueda averiguar quién es el propietario de un edificio, pero solo los titulares de cuentas pueden comprobar su saldo. Estos libros contables están **centralizados** (hay un intermediario, en el que confían todos los usuarios, que controla totalmente el sistema y media en cada transacción) y son **opacos** (el funcionamiento del libro contable y sus datos no son totalmente visibles para sus usuarios). La digitalización ha hecho que estos libros contables sean más rápidos y fáciles de utilizar, pero siguen estando centralizados y siendo opacos.

La cadena de bloques ofrece la misma funcionalidad de mantenimiento de registros pero sin una arquitectura centralizada. La cuestión es cómo se puede estar seguro de que una transacción es legítima cuando no hay una autoridad central que lo compruebe. Las cadenas de bloques resuelven este problema al descentralizar el libro contable, de forma que cada usuario tiene una copia de él. Cualquiera puede solicitar que se añada una transacción a la cadena de bloques, pero las transacciones solo se aceptan si todos los usuarios están de acuerdo en que es legítimo, es decir, que la solicitud proviene de la persona autorizada, que el vendedor de la casa no la ha vendido ya y que el comprador no ha gastado ya el dinero. Esta comprobación se realiza de manera fiable y automática en nombre de cada usuario, creando un sistema de libros contables muy rápido y seguro que es excepcionalmente inalterable.

Cada nueva transacción que va a registrarse se agrupa junto con otras nuevas transacciones en un «bloque», que se añade como último eslabón a una larga «cadena» de transacciones históricas. Esta cadena forma el libro contable de la cadena de bloques que tienen todos los usuarios. Este trabajo se llama «minería». Cualquiera puede ser minero y competir por ser el primero en resolver el complejo problema matemático de crear un bloque encriptado válido de transacciones que añadir a la cadena de bloques. Existen varios medios para incentivar a las personas a hacer este trabajo. Lo más frecuente es que el primer minero en crear un bloque válido y añadirlo a la cadena sea recompensado con la suma de las comisiones por sus transacciones. Las comisiones se sitúan actualmente en torno a los 0,10 EUR por transacción, pero los bloques se añaden periódicamente y contienen miles de transacciones. Los mineros también pueden recibir nuevas monedas que se crean y ponerlas en circulación como mecanismo de inflación.

La adición de un nuevo bloque a la cadena implica la actualización del libro contable que obra en poder de todos los usuarios. Los usuarios solo aceptan un nuevo bloque cuando se ha verificado que todas las transacciones son válidas. Si se encuentra una discrepancia, el bloque se rechaza. De lo contrario, el bloque se añade y se mantendrá ahí como dominio público permanente. Ningún usuario puede eliminarlo. Mientras que la destrucción o corrupción de un libro contable tradicional exige atacar al intermediario, en el caso de una cadena de bloques exige atacar a cada una de las copias del libro contable simultáneamente. No puede haber un «falso libro contable», porque todos los usuarios tienen su propia versión genuina con la que comparar. La confianza y el control en las transacciones basadas en cadenas de bloques no son centralizados y opacos, sino que son **descentralizados** y **transparentes**. Estas cadenas de bloques se califican como «sin permiso», porque no hay una autoridad especial que pueda denegar el permiso para participar en la comprobación y adición de transacciones. También puede decirse que encarnan valores sociales y políticos como la transparencia y la redistribución de poder.

También es posible crear cadenas de bloques «con permiso», donde un limitado grupo de actores conservan el poder de acceso, comprobación y adición de transacciones al libro contable. Esto permite a actores convencionales como bancos y Gobiernos mantener un control sustancial sobre sus cadenas de bloques. Las cadenas de bloques con permiso son menos transparentes y descentralizadas que sus homólogas sin permiso y, por lo tanto, encarnan valores sociales y políticos algo diferentes.

1. Monedas: la vanguardia de la tecnología de la cadena de bloques

Aunque las monedas constituyen solo uno de los diversos ámbitos de aplicación posibles de la tecnología de la cadena de bloques, son el más popular con diferencia. Asimismo, aunque Bitcoin es solo una de las muchas monedas implantadas a través de una cadena de bloques, es de lejos la más conocida. Muchas iniciativas recientes se han centrado en las posibilidades más amplias de la tecnología de la cadena de bloques, pero es raro encontrar un debate generalizado de la cadena de bloques sin referencia a Bitcoin o, como mínimo, a las monedas habilitadas por la cadena de bloques. Puesto que las aplicaciones monetarias dominan los debates sobre la cadena de bloques y representan las aplicaciones más maduras y conocidas, tienen una gran influencia en el desarrollo de las tecnologías de la cadena de bloques en general. A continuación se analiza brevemente cómo funcionan las aplicaciones de la cadena de bloques en el caso de las monedas y algunas de sus implicaciones. Sin embargo, puesto que ya existen varias guías y debates accesibles sobre este tema, la atención se centrará en cómo podría afectar el dominio de la cadena de bloques por parte de Bitcoin al desarrollo generalizado de la tecnología y otras aplicaciones de libros contables distribuidos.

¿Cómo funcionan?

Bitcoin fue lanzada por Satoshi Nakamoto, pseudónimo del misterioso y evasivo editor o editores de un artículo que describe cómo podría utilizarse la criptografía, combinada con un libro contable público distribuido, para implantar una moneda digital sin una autoridad central que autentique los pagos. Tradicionalmente, las personas pueden intercambiar dinero con otras que no conocen porque ambos actores confían en una tercera parte, normalmente la validez de un billete o un intermediario como un banco o el cambio de divisas. El sistema de Nakamoto no tiene una moneda palpable ni tampoco intermediarios, sino que crea un sistema fiable mediante el uso innovador de la criptografía y la creación de redes entre pares. Cuando un usuario envía bitcoins a otro, los detalles de la transacción (como la dirección del emisor y el destinatario y el importe de los fondos transferidos) se transmiten a la red Bitcoin, de modo que la transacción puede ser validada por todos los pares de la red. Una vez que ha sido validada por la red, la transacción se empaqueta en un «bloque» de transacciones y se añade, mediante el proceso de «minería», a la creciente lista de bloques que conforman el libro contable de la cadena de bloques. Esta lista es almacenada por los pares en la red. Bitcoin también presenta una característica que hace que se generen nuevas bitcoins y se añadan al sistema, provocando un efecto inflacionista. Estas se distribuyen a los mineros (además de la suma de las comisiones de transacción en el bloque) como recompensa por añadir con éxito transacciones a la cadena de bloques. Cualquier usuario con un ordenador puede practicar la minería, pero ha surgido una industria de mineros profesionales, que utilizan ordenadores específicos desarrollados especialmente para este fin. La estructura distribuida del sistema, junto con su funcionalidad criptográfica, hacen que Bitcoin sea increíblemente sólida. La confianza necesaria para posibilitar las transacciones se logra al saber que todas las transacciones —pasadas, presentes y futuras— son presenciadas (aunque automáticamente) por todos los usuarios.

Bitcoin es con diferencia la mayor moneda basada en cadenas de bloques, aunque existen varias otras con características técnicas ligeramente diferentes. Las diferencias residen a menudo en el proceso de minería, que puede exigir recursos informáticos sustanciales. Por ejemplo, algunas monedas utilizan algoritmos con menor intensidad de recursos que Bitcoin. El algoritmo de Peercoin está diseñado para utilizar menos

recursos a medida que se desarrolla. También varían respecto al ritmo y el mecanismo mediante el que se generan y distribuyen nuevas monedas (por ende, en sus políticas de inflación). Muchas tienen un número predefinido de monedas y, una vez que se alcanza el límite máximo, no se generan nuevas monedas y los mineros solo se beneficiarán de las comisiones de las transacciones. Algunas monedas utilizan algoritmos que están diseñados para evitar la aparición de «mineros profesionales» que utilizan equipos de minería especializados.

Puesto que las transacciones cuestan muy poco (actualmente entre 0 y 0,10 EUR), pero ofrecen un registro seguro y permanente, es posible utilizar la cadena de bloques de Bitcoin para otros fines no financieros. Podría aprovecharse para explotar y lanzar varias otras aplicaciones no relacionadas con monedas, desde la votación a la protección de patentes. Aunque este tipo de planteamiento impide al desarrollador aplicar características personalizadas que podría haber introducido en su propia cadena de bloques, ofrece una infraestructura de bajo coste, fácilmente accesible y estable, lo que lo convierte en un excelente punto de partida para explorar ideas. Se han creado otras monedas basadas en cadenas de bloques teniendo en mente explícitamente aplicaciones más amplias. Ethereum es una configuración de cadenas de bloques que sigue el libro blanco y la campaña de microfinanciación colectiva de Vitalik Buterin. Incluye una moneda (ether, que se califica como «combustible») y también un código que puede utilizarse para aplicar una amplia gama de funciones no financieras (véase contratos inteligentes, gestión de derechos digitales y organizaciones autónomas descentralizadas).

Evolución y posibles efectos

En 2014, un dictamen de la Autoridad Bancaria Europea puso de relieve varios riesgos que presentan las monedas basadas en cadenas de bloques. También descartó sus beneficios inmediatos —en particular transferencias rápidas, seguras y baratas— por ser irrelevantes en la Unión, donde las transferencias convencionales ya son relativamente rápidas, seguras y baratas. Para muchos usuarios, las ventajas reales de las monedas basadas en cadenas de bloques residen, más allá del menor tiempo y el ahorro de costes, en la funcionalidad y los valores que no se encuentran en las monedas tradicionales. Entre ellos se incluyen algunos de los «problemas» tan publicitados de Bitcoin, como sus enormes subidas de precios y su uso en mercados ilegales y en la web oscura, los cuales en realidad pueden haber atraído a muchos nuevos usuarios. Sencillamente, si no hubiese ventajas sustanciales en el uso de monedas basadas en cadenas de bloques en Europa, no se registraría un uso sustancial de las mismas en el continente. Sin embargo, la adopción de monedas basadas en cadenas de bloques sigue creciendo, a pesar del importante fallo de seguridad que puso a prueba los fundamentos ideológicos de Ethereum.

Estas monedas ya están a la vanguardia del desarrollo de la cadena de bloques, lo que podría provocar una importante convulsión tecnológica. Si materializan su potencial, podrían encabezar un proceso de descentralización mediante el que las instituciones que rigen tradicionalmente las finanzas —incluidos los gobiernos y los bancos— pierdan poder. Por otro lado, estos mismos Gobiernos y bancos están impulsando actualmente la investigación y el desarrollo de la cadena de bloques en direcciones que se adaptan a sus propios propósitos. Estas cadenas de bloques pueden resultar menos descentralizadas y transparentes que otras.

Sin embargo, quizá la mayor repercusión de las monedas basadas en cadenas de bloques se encuentre en otros ámbitos más allá del sistema financiero. Bitcoin *et al* ofrecen una amplia base de usuarios, espacios fértiles para la experimentación y «combustible» para impulsar nuevas ideas. Aunque Bitcoin no revolucione el sistema financiero, sí podría allanar el camino a otras aplicaciones que podrían ofrecer importantes ventajas a las cadenas de suministro y los servicios públicos, por ejemplo. Aunque ahora es habitual debatir una amplia gama de aplicaciones de la cadena de bloques, las monedas como Bitcoin han acaparado la mayoría de la atención mediática y política prestada a la cadena de bloques en los últimos años, lo que podría afectar a la forma en que se desarrolla la tecnología. En otras palabras, la referencia frecuente al valor fluctuante de Bitcoin y su uso en mercados negros puede distraer a los actores pertinentes

y a la ciudadanía del debate más productivo sobre la amplia gama de oportunidades y dificultades que presenta la tecnología actualmente.

Formulación de políticas de anticipación

Las monedas basadas en cadenas de bloques presentan numerosas dificultades jurídicas y reguladoras, como los mecanismos de protección del consumidor, los métodos de cumplimiento y las posibilidades de realización de actividades ilegales como evasión fiscal y venta de bienes ilícitos. También presentan varias posibles ventajas para los ciudadanos, entre ellas reducción de costes, mejora de la seguridad y un sistema financiero más accesible e innovador. Estas y otras cuestiones se reconocieron en una propuesta reciente aprobada por el Parlamento Europeo, que también destacaba el potencial general de la tecnología de la cadena de bloques «mucho más allá del sector financiero» y pedía un enfoque regulador proporcionado y un desarrollo de capacidad y conocimientos especializados suficientes a nivel de la Unión.

2. Contenidos digitales: cadena de bloques y gestión de derechos

La falsificación de obras de arte y el fraude son disciplinas arraigadas, pero en la era de internet puede ser tan fácil como presionar Ctrl+C. El contenido multimedia se ha copiado y compartido de manera generalizada —y a menudo ilegal— desde que los sistemas hi-fi facilitaron la copia de discos de vinilo y las emisiones de radio en cintas de casete. Internet facilitó aún más la piratería. Los primeros usuarios organizaron redes mundiales para compartir por correo CD copiados. A medida que aumentó el ancho de banda y aparecieron los formatos electrónicos, las redes de intercambio de archivos hicieron de la piratería lo normal. En la actualidad, la piratería multimedia se organiza habitualmente a través de «*torrents*» y, cada vez más, emisión en continuo. Aunque la distribución de contenidos multimedia de este modo suele ser ilegal, la práctica es tan generalizada y la vigilancia del cumplimiento tan difícil que este último a menudo se trata como si fuese voluntario. Recientemente, los servicios de suscripción legítimos han desplazado en cierto grado a la piratería proporcionando acceso a medios mediante el pago de cánones a los titulares de derechos utilizando los ingresos derivados de las cuotas de los miembros o la publicidad. Sin embargo, ningún modelo de distribución, hasta la cadena de bloques quizá, ha conseguido responder eficazmente a la realidad del comercio ilegal de contenidos digitales en la era de internet, equilibrando al mismo tiempo los intereses del autor original, el cliente y los diversos intermediarios.

Cuando los consumidores compran libros y discos, pasan a ser propietarios de objetos físicos que posteriormente pueden vender, regalar o legar como parte de su herencia. Existen limitaciones a sus derechos; por ejemplo, no deben distribuir copias y deben pagar cánones si emiten el contenido. Al comprar el equivalente digital de estos mismos medios, los consumidores saben que no obtendrán la propiedad de un objeto físico, pero muchos no se dan cuenta de que tampoco obtienen la propiedad del contenido. En cambio, celebran un acuerdo de licencia que es válido durante un período de tiempo o un número fijo de reproducciones. Estas licencias no pueden venderse, regalarse y ni siquiera legarse como parte de una herencia. La creación de una colección de música, literatura, juegos y películas digitales de legítima propiedad a menudo supone un coste similar al de una colección de varios discos y libros con el mismo contenido. Es una inversión sustancial de por vida, pero no puede transferirse y expira tras la muerte. Mientras que las generaciones más mayores podrían deleitarse en revivir los gustos y las experiencias de los seres queridos a través de las cajas de vinilos, libros y juegos que estos dejaron, los niños de hoy puede que no disfruten del mismo acceso al contenido digital de sus padres. ¿Podría ayudar la tecnología de la cadena de bloques a resolver estos y otros problemas con los medios digitales?

Cómo podrían gestionarse los derechos digitales en la cadena de bloques

La tecnología de la cadena de bloques podría utilizarse para gestionar los derechos de los consumidores asociados a los productos digitales. En la mayoría de los casos, atañerá a obras reproducidas en masa, el equivalente digital de los CD, DVD y libros, cuando el artista original vende muchas copias de la obra. Sin

embargo, también es relevante para el ámbito emergente de las obras de arte digitales únicas, que son el equivalente digital de, por ejemplo, una pintura. En este caso, el comprador no está comprando una versión extraída, como un MP3 de una canción, sino los derechos exclusivos de la propia obra original. La cadena de bloques podría proteger a consumidores y creadores de obras digitales de todo tipo registrando el historial de propiedad del bien digital y quizá incluso haciendo efectivos los derechos digitales.

La cadena de bloques podría utilizarse para registrar todas las ventas, préstamos, donaciones y otras transferencias de este tipo de objetos digitales individuales. Todas las transacciones son presenciadas y acordadas por todos los usuarios. Al igual que con las transacciones en una cuenta bancaria o un registro catastral, los objetos no pueden transferirse si su propiedad no es legítima. Los compradores pueden verificar que están comprando copias legítimas de archivos de MP3 y vídeo. De hecho, el historial de transacciones permite a cualquiera comprobar que las diversas transferencias de propiedad se remontan hasta el propietario original, es decir, el creador de la obra. El concepto podría combinarse con contratos inteligentes, de forma que el acceso al contenido pueda prestarse a otros durante períodos de tiempo determinados antes de devolverse automáticamente, o que las últimas voluntades puedan cumplirse automáticamente tras el registro de un certificado de defunción. Para que cualquiera de ello funcione, es crucial que, cuando se transfiera la propiedad del contenido de una parte a la siguiente, los anteriores propietarios pierdan su acceso, como sucedería si vendiesen un disco de vinilo en el mercado de segunda mano. De hecho, es igual de importante saber cuándo terminan los derechos de un usuario que saber cuándo empiezan los derechos de otro. A este respecto, la cadena de bloques permitiría comprobar quién era el propietario del contenido, así como el historial de propiedad, lo que a su vez permitiría a los clientes asegurarse de que están comprando bienes legítimos en lugar de copias ilegítimas, y a los titulares hacer valer sus derechos. Las comprobaciones de la propiedad legítima podrían incluso realizarse mediante tecnología, con dispositivos que comprueben la propiedad en el perfil del usuario antes de permitir la reproducción. Esto exigiría desarrollar nuevos códecs y estándares sectoriales y formatos de archivo que unan el contenido a permisos.

Aparte de comprar copias autorizadas de obras digitales como canciones en MP3, también es posible comprar y vender obras originales, es decir, la propia canción. Al igual que comprar una pintura confiere más derechos que comprar una copia de la pintura, el comprador de obras digitales originales también adquiere el derecho exclusivo a difundir el contenido, vender copias de él y emprender acciones judiciales contra quienes lo utilicen ilegalmente. Para los compradores es esencial saber si están comprando la propiedad de la obra, con el valor y los derechos asociados, o simplemente una reproducción autorizada para uso personal. En este caso, la cadena de bloques podría utilizarse para comprobar el propietario real del contenido, si es la versión original o una copia legítima de él, y el conjunto de derechos asociados a este contenido.

Al margen de los derechos de los compradores y vendedores, la cadena de bloques podría utilizarse para proteger los derechos de los creadores originales de obras, que quizá conserven algunos derechos tras la venta de su contenido. Estos creadores originales pueden comprender una compleja red de actores que reclaman la propiedad parcial y el derecho al pago de cánones cuando se utiliza el contenido con fines comerciales. En el caso de las pistas musicales, por ejemplo, podrían incluirse los autores, músicos y otros artistas, así como ingenieros de sonido, representantes y una serie de intermediarios especializados. Los derechos de cada uno de estos actores, así como las condiciones y los medios de retribución, pueden codificarse digitalmente, permitiendo un pago más fiable y eficiente. El pago de cánones podría incluso ejecutarse automáticamente a través de contratos inteligentes.

Evolución y posibles efectos

El uso de la tecnología de la cadena de bloques de este modo podría por primera vez permitir a los consumidores comprar y vender copias digitales de segunda mano, regalarlas o donarlas a tiendas benéficas, prestarlas a amigos temporalmente o legarlas como parte de una herencia —como solía hacerse con los discos de vinilo y los libros— asegurándose de que no están propagando múltiples copias no

autorizadas. Para que la cadena de bloques logre sostener un método de gestión de derechos digitales donde tantos otros han fallado, tendría que equilibrar los derechos de los compradores, los vendedores, la red de actores que conforman el propietario original del contenido y una enorme variedad de otros intermediarios, incluidos los que desarrollan y mantienen la propia cadena de bloques. Con unas redes de intereses tan complejas en juego, sería idealista esperar que surja una solución rápida y no controvertida, aunque algunos sugieren que en un plazo de entre diez y quince años cabe esperar que la tecnología de la cadena de bloques tenga una incidencia real en la industria musical, con oportunidades más inmediatas para los primeros impulsores.

Formulación de políticas de anticipación

La legislación seguirá teniendo un importante papel en la identificación de las obras protegidas por derechos de autor y la solución de controversias. La tecnología de la cadena de bloques en este ámbito podría dar lugar a políticas de licencia multiterritorial y mejorar la seguridad jurídica de los creadores y compradores, ofreciendo al mismo tiempo mecanismos de solución de controversias eficaces, especialmente en relación con las tarifas, condiciones de licencia, encomendación de los derechos en línea para su gestión y retirada de derechos en línea.

3. Patentes: proteger a los innovadores incentivando al mismo tiempo la innovación

Las patentes confieren a sus propietarios el derecho exclusivo de explotación de innovaciones durante un período específico. El sistema de patentes se diseñó para incentivar la innovación dando a los innovadores una ventaja inicial sobre sus competidores para sacar provecho a sus ideas. A fin de cuentas, ¿por qué invertirían los inventores el tiempo y el dinero necesarios para desarrollar una idea si otros pudiesen copiarla y beneficiarse inmediatamente sin contribuir a los costes de desarrollo? Sin embargo, proteger a los innovadores no es lo mismo que incentivar la innovación. El sistema de patentes debe equilibrar la protección de los innovadores con la protección de los competidores. Si no se protege a los innovadores, la exposición a la competencia oportunista desalentará la inversión en nuevas innovaciones. Por otro lado, la ausencia de protección de los competidores los disuadiría de invertir en mejoras y ahorros de costes e incluso podría bloquear su entrada al mercado y la ruptura del monopolio del innovador original. En esencia, el sistema de patentes puede considerarse un intercambio en el que el gobierno confiere a los innovadores un monopolio (limitado en tiempo y alcance) para explotar su innovación y, a cambio, los titulares de patentes publican detalles de cómo funciona su innovación, lo que ayuda a otros a desarrollar mejoras y alternativas.

Existen varios problemas conocidos con el sistema de patentes. Por ejemplo, los competidores a veces pueden explotar la patente antes que el innovador, bien porque la patente no era lo suficientemente sólida, bien porque los titulares fueron incapaces de defenderse de las infracciones. Esto, combinado con el gasto de obtención de protección de la patente en varias regiones, implica que algunas empresas prefieren asumir el riesgo de comercializar sus innovaciones sin ninguna protección de patentes. Otro de los problemas se detecta en la complejidad del sistema de patentes. Existen diferentes políticas y sistemas en distintos países. A pesar de los recientes avances, todavía no existe un sistema unificado de patentes en la Unión. Sin embargo, la Oficina Europea de Patentes ofrece una «ventanilla única» para registrar patentes en el sistema de cada uno de los Estados miembros, aunque el coste de las traducciones, las validaciones y las renovaciones en varios sistemas hacen que las patentes sean relativamente caras en Europa.

Otro problema del sistema de patentes es la aparición de «troles de patentes», que no innovan como tal, sino que adquieren patentes y solicitan indemnizaciones por daños y perjuicios por su infracción. Aunque sus pretensiones no siempre tienen una base jurídica sólida, las empresas a menudo no pueden o no quieren cubrir los gastos judiciales necesarios para defenderse y prefieren alcanzar acuerdos

extrajudiciales. Las autoridades europeas de competencia están investigando cada vez más este abuso de patentes, sobre todo en el sector de la alta tecnología.

Aunque muchos aspectos del sistema de patentes están ahora digitalizados, no ha habido grandes cambios en su estructura desde la revolución de la información. Se ha sugerido que el uso de la cadena de bloques en lugar de las patentes tradicionales podría permitir una innovación más fluida al reducir las controversias contractuales, y que la cadena de bloques podría brindar la oportunidad de corregir algunos aspectos del sistema de patentes. Aquí se intenta explicar cómo podría intervenir la cadena de bloques en el sistema de patentes y qué ventajas podría traer, antes de examinar algunas de las afirmaciones más radicales que indican que podría sustituir o incluso «poner fin» al sistema de patentes.

Cómo podría ayudar la cadena de bloques al sistema de patentes

Dos características de la tecnología de la cadena de bloques la hacen especialmente pertinente para el sistema de patentes: la «encriptación» (*hashing*) y la «prueba de existencia». La primera, la encriptación, es un proceso mediante el cual un documento se transforma en un código de longitud fija que se describe como huella digital o, más frecuentemente, como resumen criptográfico (*hash*). Todos los resúmenes criptográficos son únicos e incluso diferencias mínimas, como la omisión de un acento en una letra de un documento largo, darían lugar a un resumen criptográfico radicalmente diferente. Solo la repetición del proceso de encriptación en una copia idéntica del documento original producirá el mismo resumen criptográfico. Y lo más importante, es imposible volver a generar un documento a partir de su resumen criptográfico. La segunda característica, la prueba de existencia, supone el registro de estos resúmenes criptográficos en la cadena de bloques. Al hacerlo, se crea un registro que indica que este resumen criptográfico existió en un momento dado. El registro puede ser verificado por cualquiera, pero nadie puede interpretar el contenido del resumen criptográfico. Sin embargo, los titulares del documento original pueden demostrar que el documento existía en el momento en que se realizó la transacción repitiendo el proceso de encriptación en una copia idéntica de su documento original (al utilizar el mismo algoritmo de encriptación para producir el mismo resumen criptográfico se desprende que tienen el mismo documento original). Esto presenta la interesante posibilidad de registrar públicamente el hecho de que un documento existió sin revelar su contenido. Se ha propuesto que los innovadores utilicen este proceso para proteger su obra registrando un resumen criptográfico de la descripción de su patente (o, quizá, una obra literaria o el extracto de un código informático) en la cadena de bloques. De hecho, los servicios de «prueba de existencia» ya están disponibles en el contexto de la protección de patentes. En este caso, aprovechan las capacidades de cadenas de bloques existentes más grandes, en concreto Bitcoin, aunque también podría diseñarse y aplicarse un sistema a medida para el registro de resúmenes criptográficos específicamente para fines de «prueba de existencia».

Evolución y posibles efectos

La utilización de la tecnología de la cadena de bloques dentro del sistema de patentes podría reducir las ineficiencias en el registro y el acuerdo del momento del registro de manera eficiente, quizá en varios sistemas de patentes nacionales. Podrían ofrecerse servicios de prueba de existencia basados en cadenas de bloques como primer paso en el proceso de solicitud de patentes. A partir de aquí, el proceso podría racionalizarse y consolidarse, haciendo los pasos más transparentes para el solicitante y reduciendo simultáneamente la posibilidad de corrupción. Sin embargo, aunque las mejoras en la forma de registrar y fechar las innovaciones aportarían beneficios tangibles al sistema de patentes, los problemas más graves —como los troles de patentes y el coste asociado a la traducción— pueden requerir un tipo distinto de respuesta.

Se han escuchado algunas afirmaciones (erróneas) de que una patente no es más que «un concepto sellado y conservado en un lugar donde es infalsificable». De hecho, se ha sugerido que la cadena de bloques podría sustituir al sistema de patentes permitiendo a los innovadores mantener la privacidad de sus datos. Sin embargo, la publicación de las patentes constituye una parte fundamental de su función: el fomento de

la innovación. Al publicar las patentes, se alienta a los competidores a desarrollar alternativas y mejoras, lo que podría romper los monopolios tras la expiración de la patente, inspirando al mismo tiempo innovaciones en otros ámbitos no abarcados por ella. Documentar quién registró una idea y cuándo es solo una pequeñísima fracción del trabajo que realizan los intermediarios en las oficinas de patentes. Los funcionarios de estas oficinas también evalúan la novedad de las patentes propuestas, comprueban si son conformes con las normativas y las políticas de la región y publican archivos de búsqueda de patentes aceptadas, todo lo cual es una labor importante que no puede sustituirse mediante la tecnología de la cadena de bloques.

Formulación de políticas de anticipación

Los sistemas de patentes actuales podrían ser más eficientes con el uso de la tecnología de la cadena de bloques, y las oficinas de patentes podrían ofrecer servicios de «prueba de existencia» de bajo coste. Sin embargo, debe dejarse claro que la prueba de existencia mediante una cadena de bloques (o por otros medios) no puede interpretarse como equivalente de la protección de patentes. Para que se acepten las pruebas de existencia aportadas por terceros, por ejemplo los que utilizan la cadena de bloques existente de Bitcoin, como medio legítimo para mantener registros, tendrían que ser reconocidas como tal por los órganos de vigilancia del cumplimiento competentes.

4. Votación electrónica: ¿revolución del sistema electoral?

Pese a la digitalización de varios aspectos importantes de la vida moderna, las elecciones siguen celebrándose en gran medida fuera del mundo virtual, en papel. Desde el cambio de siglo, la votación electrónica se ha considerado un avance prometedor, y quizá inevitable, que podría agilizar, simplificar y reducir el coste de las elecciones. Se ha visto como un posible medio para aumentar el compromiso y la participación e incluso restablecer los vínculos entre los ciudadanos y las instituciones políticas, afirmaciones que deben tomarse con cierto escepticismo. La votación electrónica podría adoptar muchas formas: utilizar internet o una red aislada específica; obligar a los votantes a acudir a un centro electoral o permitir la votación sin supervisión; utilizar dispositivos existentes, como teléfonos móviles y ordenadores portátiles, o exigir equipos especializados. Hay otra decisión más que debe tomarse: seguir confiando en las autoridades centrales para la gestión de las elecciones o utilizar la tecnología de la cadena de bloques para distribuir un registro de votación abierto entre los ciudadanos. Muchos expertos están de acuerdo en que la votación electrónica en las elecciones nacionales exigiría avances revolucionarios en los sistemas de seguridad. Sin embargo, existen muchos otros tipos de elecciones regionales y organizativas que podrían digitalizarse de manera más sencilla mediante el uso de la cadena de bloques, simplificándolas para que participen más personas en la toma de decisiones importantes, la adopción de estrategias a largo plazo, la realización de inversiones y la selección de personas para una amplia variedad de puestos.

Cómo puede utilizarse la tecnología de la cadena de bloques para la votación electrónica

La cadena de bloques es un medio transparente y distribuido entre los usuarios para grabar y verificar registros. Normalmente, una autoridad central registra, gestiona, contabiliza y comprueba los votos. La votación electrónica habilitada mediante cadena de bloques facultaría a los votantes para realizar ellos mismos estas tareas al permitirles conservar una copia del registro de votación. El historial de registros no puede modificarse, porque otros votantes verían que el registro difiere del suyo. Tampoco puede añadirse un voto ilegítimo, porque otros votantes podrían ver que no es compatible con las normas (quizá porque ya se ha contabilizado o no está asociado al registro de un votante válido). La votación electrónica habilitada mediante cadena de bloques trasladaría el poder y la confianza alejándolos de los actores centrales, como las autoridades electorales, y fomentaría el desarrollo de un consenso comunitario habilitado por la tecnología.

Una forma de desarrollar sistemas de votación electrónica habilitada mediante cadena de bloques es crear un nuevo sistema a medida, diseñado para reflejar las características específicas de las elecciones y el electorado. Un segundo planteamiento que podría resultar más barato y fácil es aprovechar una cadena de bloques más establecida, como Bitcoin. Teniendo en cuenta que la seguridad del libro contable de una cadena de bloques reside en la amplitud de su base de usuarios, este planteamiento también podría ser más seguro para elecciones organizativas menores con un pequeño número de votantes y recursos limitados para desarrollar un sistema a medida.

El mayor potencial de la votación electrónica habilitada mediante cadena de bloques se encuentra en los contextos organizativos. De hecho, ya se ha utilizado para elecciones internas de partidos políticos en Dinamarca y votaciones de accionistas en Estonia. Llevando el concepto un paso más allá, la votación electrónica habilitada mediante cadena de bloques podría combinarse con contratos inteligentes para emprender automáticamente acciones en determinadas condiciones acordadas. En este caso, por ejemplo, los resultados electorales podrían activar el cumplimiento automático de promesas manifiestas, decisiones de inversión u otras decisiones organizativas.

Muchos analistas han considerado que la cadena de bloques apoya transformaciones más profundas, por ejemplos en debates de administraciones virtuales, «sistemas tecno-democráticos» y la posibilidad más lejana de aplicar la votación electrónica habilitada mediante cadena de bloques a las elecciones nacionales. Algunas sugerencias ambiciosas han planteado la posibilidad de utilizar la cadena de bloques para aplicar la democracia «líquida», combinando la democracia directa (en la que los ciudadanos votan periódicamente decisiones políticas específicas) con un sistema delegado (en el que los ciudadanos pueden votar estas cuestiones específicas por sí mismos o asignar su voto a otro ciudadano —ya sea un político, periodista, científico o amigo de confianza— y retirar o reasignar esta delegación en cualquier momento).

Evolución y posibles efectos

En el caso de las elecciones más pequeñas y la toma de decisiones organizativas, la votación electrónica habilitada mediante cadena de bloques podría ayudar a generar una estructura social más participativa y ascendente ofreciendo un sistema de votación electrónica relativamente barato y seguro. En el contexto de las sugerencias más ambiciosas relativas a las elecciones nacionales, las dificultades son mucho mayores y la situación es más delicada. Los críticos han cuestionado el nivel de anonimato y accesibilidad que ofrece la votación electrónica habilitada mediante cadena de bloques y plantearon el problema de la coacción. Sin embargo, aunque la votación electrónica habilitada mediante cadena de bloques puede ofrecer varias ventajas frente a los sistemas de votación en papel y otros sistemas de votación electrónica, muchas de estas preocupaciones se aplican también a los sistemas tradicionales en papel. La *coacción* constituye una amenaza en cualquier sistema de votación que ofrece participación a distancia (por ejemplo, votación por correo). En el caso tanto de la votación electrónica habilitada mediante cadena de bloques como de la votación en papel, el uso de cabinas de votación privadas es la única garantía contra ello. La *accesibilidad* a todos los votantes es otra preocupación clave en todas las elecciones. Dependiendo de la interfaz, la votación electrónica habilitada mediante cadena de bloques podría considerarse demasiado complicada para algunos votantes, sobre todo si el sistema está totalmente descentralizado sin opción de acceder a los datos y comprobar que se han seguido los procedimientos correctos. El *anonimato* suele considerarse un elemento crucial de participación democrática, aunque incluso algunas elecciones nacionales no son plenamente anónimas. El Reino Unido, por ejemplo, dispone de un sistema de votación en papel «pseudoanónimo» en el que un código vincula cada papeleta a una entrada personal en el registro electoral. Los votantes no tienen más opción que confiar en que las autoridades electorales protejan su anonimato. Aunque no sería fácil descubrir qué votaron las personas, sí sigue siendo una posibilidad. La votación electrónica habilitada mediante cadena de bloques también es pseudoanónima, por lo que a veces se podría descubrir lo que ha votado una persona. Se está trabajando en una respuesta técnica a este problema desarrollando sistemas de votación electrónica habilitada mediante cadena de bloques que ofrezcan anonimato total. Otro planteamiento podría consistir en confiar en una autoridad central que

distribuya pseudónimos para su uso en la votación electrónica habilitada mediante cadena de bloques y los mantenga en secreto, como se hace ahora en el sistema de votación en papel del Reino Unido. Con ello se introduciría un cierto grado de centralización en el sistema que podría considerarse aceptable en el contexto de las elecciones nacionales.

Otra cuestión esencial es cómo garantizar una confianza generalizada en la seguridad y la legitimidad del sistema. Al igual que con las elecciones en papel, no basta con que el resultado sea justo y válido. Todo el electorado, aunque esté decepcionado con el resultado, debe aceptar que el proceso fue legítimo y fiable. Por lo tanto, más allá de ofrecer seguridad real y precisión, la votación electrónica habilitada mediante cadena de bloques debe inspirar también confianza. La complicación considerable del protocolo de la cadena de bloques puede ser un obstáculo para generalizar la aceptabilidad pública de la votación electrónica habilitada mediante cadena de bloques.

Al evaluar la posible repercusión de la votación electrónica habilitada mediante cadena de bloques, deben tenerse en cuenta los valores y políticas que refleja. La votación electrónica habilitada mediante cadena de bloques no solo digitaliza el proceso de votación tradicional, sino que propone una alternativa con un conjunto distinto de valores y fundamentos políticos. Tradicionalmente, las autoridades gestionan las elecciones y el proceso es invisible, centralizado y descendente. La votación electrónica habilitada mediante cadena de bloques es lo contrario. El proceso es gestionado por las personas y es transparente, descentralizado y ascendente. Aunque la participación en las elecciones tradicionales refuerza la autoridad del Estado, la participación en la votación electrónica habilitada mediante cadena de bloques afirma la primacía de las personas. En este sentido, no sorprende que se establezcan vínculos entre la votación electrónica habilitada mediante cadena de bloques y la transición a una democracia más directa, descentralizada y ascendente y la democracia «líquida» antes mencionada. En cualquier caso, el grado en que la tecnología de la cadena de bloques florezca en el ámbito de la votación electrónica puede depender del grado en que pueda reflejar los valores y la estructura de la sociedad, la política y la democracia.

Formulación de políticas de anticipación

Si bien las organizaciones son muy libres de organizar elecciones internas con cadenas de bloques si así lo deciden, deben cumplir la legislación europea en materia de privacidad y protección de datos. Aunque la legislación europea no especifica protocolos para las elecciones políticas en los Estados miembros, se ha producido cierta convergencia y se han realizado esfuerzos para fomentar el uso de la votación electrónica respetando al mismo tiempo los principios constitucionales de la legislación electoral (sufragio universal, igualitario, libre, secreto y directo).

5. Contratos inteligentes: si el código fuera ley

Los libros contables de la cadena de bloques presentan varias características interesantes y novedosas frente a los libros contables centralizados. Sin embargo, además de registrar la fecha y los detalles de las transacciones, también pueden desempeñar un papel más activo y potencialmente autónomo en la gestión y la ejecución de las transacciones. Mediante la incrustación de un código en la cadena de bloques, pueden ejecutarse automáticamente transacciones en respuesta al cumplimiento de determinadas condiciones, ofreciendo una «garantía de ejecución». Los contratos inteligentes autoejecutables basados en esta funcionalidad se están desarrollando con rapidez. Sin embargo, surgen preguntas cuando el código y la ley se convierten en uno solo.

¿Cómo funcionan?

Aunque los contratos inteligentes podrían referirse a varios conceptos diferentes, su definición de 1994 como «protocolo de transacción informatizado que ejecuta las cláusulas de un contrato» sigue siendo muy útil en el contexto de las tecnologías de la cadena de bloques. En su forma más simple, las condiciones de un acuerdo entre dos o más partes se programan en un código (conjunto de instrucciones) que se

almacenan en una cadena de bloques casi de la misma manera que las transacciones se almacenan de forma rutinaria en otras cadenas de bloques. Cuando se cumplen determinadas condiciones que se describen en el código, se activan automáticamente acciones específicas, que también se definen en el código. De este modo, por ejemplo, la entrega de productos podría activar la instrucción de realización de un pago, lo que a su vez podría activar otras instrucciones en otros contratos inteligentes, quizá cambiar divisas o dar órdenes a agentes posteriores de la cadena de suministro. Muchos de los ejemplos propuestos de aplicaciones a corto plazo se hallan en el sector financiero, como préstamos y productos de seguro que requieren recursos manuales sustanciales que podrían automatizarse. Los contratos inteligentes podrían utilizarse para automatizar las herencias, con una activación automática de la distribución de bienes — incluidos contenidos multimedia — tras el registro de la defunción.

La cadena de bloques Ethereum presenta su propio lenguaje de programación y moneda, que se crearon específicamente para apoyar los contratos inteligentes. Otros planteamientos de contratos inteligentes utilizan otras aplicaciones de la cadena de bloques, incluida Bitcoin. En esta fase, los contratos inteligentes todavía exigen algunos esfuerzos y gastos iniciales para configurarse, por lo que son más aptos para acuerdos repetitivos que para contratos puntuales. Teniendo en cuenta su naturaleza predeterminada, no se adecuan a situaciones que son objeto de cambios sustanciales durante el período de vigencia del contrato. De hecho, el nivel de inseguridad jurídica haría prudente restringir los contratos inteligentes a relaciones y acuerdos relativamente consensuados que es poco probable que cuestione una de las partes. Por último, puesto que reaccionan a estímulos digitales y activan nuevos procesos digitales, son más eficaces cuando las diversas cláusulas y consecuencias son también de naturaleza digital y, por lo tanto, son adecuadas para la automatización digital.

Evolución y posibles efectos

Puesto que el libro contable de la cadena de bloques es inmutable, el código acordado (y, por ende, el contrato acordado) solo puede cancelarse o modificarse bajo condiciones ya permitidas en el propio código. Los contratos tradicionales ofrecen la opción de pagar lo debido con arreglo al contrato o romper el contrato y enfrentarse a las consecuencias, quizá con acciones judiciales de por medio. Sin embargo, si el pago está automatizado en un contrato inteligente, está opción deja de existir, puesto que la transacción se ejecuta automáticamente.

La interpretación radical de los contratos inteligentes reduciría el contrato al código, declarando efectivamente a este último como la propia ley: autónomo, autoejecutable y autoexigible. Esta podría ser la posición de una facción «extrema» del movimiento de base de la cadena de bloques, que se posiciona efectivamente fuera del control de las estructuras establecidas, como Estados naciones y jurisdicciones legales. Cuando el código se trata como ley, cualquier error o vulnerabilidad accidental se convierte en parte del contrato también. La explotación de estos errores para controlar activos no se consideraría robo, porque el error que permite la retirada forma parte del código y, por lo tanto, por definición, está dentro de la «ley». Los contratos inteligentes también podrían contener cláusulas ilegales, como códigos de distribución de herencias que no prevean los impuestos de sucesión que se aplican en esa jurisdicción.

Una interpretación más realista de los contratos inteligentes los posicionaría dentro del ordenamiento jurídico general. Al igual que los contratos en papel, pueden imponerse requisitos adicionales y pueden anularse o reinterpretarse cláusulas sobre la base de la intención de las partes y la legislación en general. El Derecho del país siempre prevalece por encima de la «ley» inscrita en el código, aunque los procedimientos judiciales y el cumplimiento puedan resultar difíciles. Por lo tanto, aunque la mayoría de debates sobre los contratos inteligentes reconocen que generarán mayor eficiencia en algunos ámbitos, no se espera que sustituyan al Derecho contractual tradicional o a los abogados especialistas en contratos tradicionales.

A diferencia de las cadenas de bloques más simples que registran transacciones, las que incluyen un código ejecutable presentan una dimensión adicional de complejidad y acción. Esto significa que pueden requerir

mayor potencia de tratamiento para la minería y el mantenimiento del sistema, lo que podría traducirse en mayores costes, incluido el uso de energía. Esta complejidad también puede exponer las cadenas de bloques a mayores vulnerabilidades de seguridad, que, combinadas con la ideología del «código como ley», podría crear graves problemas prácticos para los contratos inteligentes. Estos problemas pueden ser menos frecuentes a medida que se desarrollen normas y surja la primera generación de «abogados inteligentes» (es decir, abogados formados y con experiencia en la gestión de contratos inteligentes).

Formulación de políticas de anticipación

Existen varios ámbitos del Derecho que podrían ser vulnerables al abuso cuando el contrato no se considere parte de una jurisdicción legal tradicional. Entre los ejemplos están la fiscalidad (por ejemplo sobre la renta, las ventas, la sucesión y los rendimientos del capital), la explotación (por ejemplo de contratos de alquiler y empleo) y la delincuencia empresarial (por ejemplo, la fijación de precios y el tráfico de información privilegiada). Puede resultar necesario encontrar nuevas formas de afirmar la primacía del Derecho nacional en caso de que la automatización que entrañan los contratos inteligentes dificulte su aplicación. Podrían surgir nuevas responsabilidades gubernamentales en el proceso de aplicación de procesos judiciales tradicionales a los contratos inteligentes, como el arbitraje cuando se encuentren errores en el código de contrato. Cuando los programadores empiezan a traducir acuerdos en un código ejecutable, están tomando efectivamente decisiones sobre cómo se aplicarán en la práctica, lo que puede significar que tienen mayores responsabilidades legales.

Los contratos inteligentes pueden ser inflexibles e incapaces de adaptarse a circunstancias cambiantes o a las preferencias de las partes. No puede responderse a todas las preguntas posibles con antelación y siempre habrá circunstancias imprevistas que exijan una interpretación de la aplicación de las cláusulas contractuales. El código es sencillamente demasiado rígido para que todos los contratos se determinen de manera algorítmica. La resolución de litigios contractuales y el cumplimiento de cláusulas contractuales pueden presentar dificultades a medida que se desarrolle este ámbito.

Puede que tenga que modificarse el Derecho contractual tradicional, en concreto los requisitos de mantenimiento de registros y los requisitos probatorios, para tener en cuenta la naturaleza automatizada y determinista de los contratos inteligentes, así como cuestiones relacionadas con su validez y exigibilidad. Se espera que el Derecho se enfrente a cuestiones difíciles relativas a la necesidad de establecer un vínculo con el mundo físico, llevar a cabo los procedimientos de validación necesarios y garantizar la conformidad de las aplicaciones de las cadenas de bloques con la legislación aplicable. ¿Sería la forma de ley más significativa el código técnico abordado mediante la lente de Lessig? Claramente, se necesitan criterios para garantizar la validez legal y la exigibilidad de los contratos inteligentes con arreglo a la ley.

6. Cadenas de suministro: ¿transparencia y rendición de cuentas por fin?

El comercio mundial se basa en un sector de cadenas de suministro de 16 billones EUR. Los bienes se producen y distribuyen a través de una amplia red de productores, minoristas, distribuidores, transportistas y proveedores en un complejo mecanismo de procesos de gestión de contratos, pagos, etiquetado, sellado, logística y lucha contra la falsificación y el fraude.

La magnitud y la complejidad de los sistemas en cuestión dan lugar a elevados costes de transacción, discrepancias frecuentes y errores en el papeleo manual y pérdidas por degradación y robo en el camino. Otros problemas son las condiciones de trabajo abusivas o de riesgo; los daños medioambientales causados por las ineficacias y procesos de extracción y producción ilegales; la falsificación e imitación y los riesgos sanitarios por una mala gestión de la cadena de suministro. Estos problemas con frecuencia salen a la luz en incidentes de gran repercusión, por ejemplo en cadenas de suministro de alimentos, ropa y diamantes. Algunos indican que las normas y la certificación han mejorado la diferenciación de opciones y la

concienciación del consumidor, pero los procesos reales siguen siendo costosos y poco fiables, especialmente en regiones con elevados niveles de corrupción. Toda la «cadena de custodia», que demuestra el origen de cada producto o material, sigue estando fragmentada en las organizaciones y es vulnerable a fraude y error, incluso entre empresas certificadas. Existe una creciente demanda de cadenas de suministro de bienes y servicios más seguras, fiables y transparentes. La cuestión es si la tecnología de la cadena de bloques puede realmente mejorar las cadenas de suministro y el sector logístico actuales para responder a las ineficiencias operativas, el fraude y quizá incluso algunos grandes problemas como las prácticas laborales no éticas y la degradación medioambiental.

Cómo podrían gestionarse las cadenas de suministro en la cadena de bloques

Las aplicaciones basadas en la cadena de bloques pueden mejorar las cadenas de suministro ofreciendo una infraestructura para el registro, certificación y seguimiento a bajo coste de bienes que se están transfiriendo entre partes a menudo alejadas, que están conectadas a través de una cadena de suministro pero no confían necesariamente la una en la otra. Todos los bienes se identifican de forma unívoca a través de identificadores y pueden transferirse mediante la cadena de bloques, donde cada una de las transacciones se verifica y fecha en un proceso encriptado pero transparente. Esto da acceso a las partes pertinentes, ya sean proveedores, vendedores, transportistas o compradores. Los términos de cada transacción son irrevocables e inmutables, abiertos a inspección de todos o de auditores autorizados. También podrían utilizarse contratos inteligentes para ejecutar automáticamente pagos y otros procedimientos.

Evolución y posibles efectos

Varias empresas, innovadores y titulares ya están poniendo a prueba la cadena de bloques para el mantenimiento de registros en sus cadenas de suministro. Everledger permite a las empresas y los compradores hacer un seguimiento de la procedencia de los diamantes desde las minas hasta las joyerías y luchar contra el fraude en los seguros o la documentación. Para cada diamante, Everledger mide cuarenta atributos como el corte y la claridad, el número de grados en ángulos de pabellón y el lugar de origen. Se genera un número de serie para cada diamante, inscrito microscópicamente, y después se añade este ID digital a la cadena de bloques de Everledger (que numera actualmente 280 000 diamantes). Este proceso permite crear y mantener historiales completos de propiedad, que ayudan a luchar contra el fraude y apoyar a la policía y los investigadores de seguros que buscan joyas robadas. También permite a los consumidores tomar decisiones de compra más fundamentadas, por ejemplo limitar la búsqueda a diamantes con un historial «limpio» que esté exento de fraudes, robos, trabajo forzado e intervenciones de vendedores dudosos que están vinculados a la violencia o el tráfico de drogas o armas.

La empresa social Provenance, con sede en Londres, ha desarrollado una plataforma de datos en tiempo real que recopila y verifica el origen de un activo asignándole un identificador o «pasaporte digital» que puede rastrearse en toda la cadena de suministro hasta que llega a su destino. Podría resultar útil para luchar contra el fraude en la venta de bienes protegidos con denominaciones de origen, como las que se otorgan a especialidades regionales, por ejemplo vinos y quesos. SmartLog incorpora contratos inteligentes a los contenedores de embarque para rastrear su localización y alrededores para la planificación de recursos. La cadena de bloques también se está utilizando para minimizar el riesgo en pagos, y empresas como Skuchain y Fluent ofrecen apoyo basado en la cadena de bloques para la financiación y los pagos en la cadena de suministro. Otro proyecto está desarrollando un sistema para racionalizar el tratamiento manual de documentación, utilizando una cadena de bloques privada para compartir información entre exportadores, importadores y sus bancos. Wal-Mart, la cadena minorista más grande del mundo, está probando la cadena de bloques para la inocuidad alimentaria. Se espera que un registro preciso y actualizado basado en la cadena de bloques pueda ayudar a identificar el producto, cargamento y vendedor, por ejemplo cuando se produzca un brote, y obtener de este modo los datos de cómo y dónde se cultivó el alimento y quién lo inspeccionó. Un registro preciso también podría hacer más eficientes las

cadenas de suministro entregando más rápido los alimentos a las tiendas y reduciendo su deterioro y desperdicio.

Los sistemas basados en la cadena de bloques pueden mejorar la eficiencia de los procesos de adquisición, logística y pago, reducir el tratamiento manual de documentación de importación/exportación, garantizar la conformidad y la entrega de bienes y evitar pérdidas, reduciendo así en general los costes, mejorando la seguridad e inocuidad y minimizando el fraude. También pueden proporcionar los medios para verificar la autenticidad, el origen y los estándares éticos de los bienes y servicios. Los historiales de propiedad transparentes y rastreables revelarían fraudes, robos, utilización de trabajo forzoso, vínculos con la violencia o el tráfico de drogas o armas u otras prácticas dudosas, mejorando la capacidad para aplicar la ley y posibilitando un consumo más responsable. Sin embargo, existen razones para ser cautos. La confianza entre los participantes depende de la confianza en la tecnología de la cadena de bloques, pero esta no está completamente exenta de vulnerabilidades, incluidos errores accidentales y ataques maliciosos. La automatización no garantizará la eliminación de errores, conflictos de interés o corrupción en las cadenas de suministro mundiales complejas.

La cadena de bloques ofrece un pseudoanonimato; en otras palabras, todas las transacciones son transparentes, pero no están conectadas explícitamente con personas u organizaciones del mundo real, protegiendo la identidad de las partes en toda la cadena de suministro sin comprometer la identidad del registro. La comprobación de los atributos de los bienes y sus movimientos pueden desvincularse de la identidad completa de los usuarios, ocultando datos personales detallados sensibles que exceden de lo necesario para el registro. Sin embargo, el anonimato no es absoluto y, con esfuerzos suficientes, se pueden conectar las transacciones a determinadas partes. Aunque se considera en general una mejora del sistema actual, puede tener consecuencias para la privacidad. Una vez que los bienes llegan al consumidor, el seguimiento detallado debe cesar o, como mínimo, cumplir las normas de privacidad y protección de datos.

Formulación de políticas de anticipación

El desarrollo de la cadena de bloques en la gestión de la cadena de suministro presenta dificultades reguladoras considerables. Normativas como la Directiva europea sobre divulgación de información no financiera podrían influir en las aplicaciones de la cadena de bloques a las cadenas de suministro. Esta directiva obliga a las empresas a divulgar información fiable sobre asuntos medioambientales, aspectos sociales y laborales, el respecto de los derechos humanos y cuestiones de lucha contra la corrupción, impulsando así una mayor transparencia en sus operaciones. Sin embargo, la ausencia de un intermediario en la mayoría o la totalidad de los pasos de la cadena de suministro en el futuro podría crear incertidumbre para las partes involucradas, especialmente en lo que respecta a las formas automatizadas de ejecución y supervisión de las transacciones. En la mayoría de los casos, debe haber nociones y mecanismos de responsabilidad cuando se produzcan problemas imprevistos, que también deben poder revisarse.

7. Estados con cadenas de bloques: replanteamiento de los servicios públicos

En el contexto de la apertura de datos, servicios y decisiones en el sector público mediante las tecnologías digitales, se está desarrollando una nueva generación de servicios de administración electrónica abiertos, responsables, transparentes y colaborativos. El Asesor Científico Jefe del Gobierno británico publicó recientemente un informe que describe cómo podrían las tecnologías basadas en la cadena de bloques proporcionar nuevas herramientas para reducir el fraude, evitar errores, reducir gastos de explotación, impulsar la productividad, apoyar el cumplimiento y obligar a rendir cuentas en muchos servicios públicos. Entre las posibles aplicaciones están la recaudación de impuestos, la gestión de la identidad, la distribución de beneficios, las monedas digitales locales (o nacionales), los registros catastrales y de la propiedad y cualquier tipo de registro gubernamental. La misma tecnología abre puertas también a los

agentes no estatales para prestar servicios similares a los públicos, desde servicios de notaría a ciudadanía mundial e identidad. Queda por ver lo que implicará la cadena de bloques para el sector público.

Cómo podría apoyar la tecnología de la cadena de bloques los servicios públicos

Los datos utilizados por las instituciones públicas suelen estar fragmentados a nivel interno y ser opacos para otros actores, en concreto ciudadanos, empresas y vigilantes. La tecnología de la cadena de bloques podría permitir la creación y verificación de registros con un mayor nivel de velocidad, seguridad y transparencia. Las aplicaciones más inmediatas de la tecnología de la cadena de bloques en la administración pública se hallan en el mantenimiento de registros. Se espera que la combinación de fechado con las firmas digitales en un libro contable accesible genere ventajas para todos los usuarios, permitiéndoles realizar transacciones y crear registros (por ejemplo, registros catastrales, certificados de nacimiento y licencias empresariales) dependiendo menos de abogados, notarios, funcionarios públicos y otros terceros.

El Gobierno estonio ha experimentado con aplicaciones de la cadena de bloques que permiten a los ciudadanos utilizar sus carnés de identidad para solicitar recetas médicas, votar, realizar operaciones bancarias, solicitar prestaciones, registrar sus empresas, pagar impuestos y acceder a otros cerca de 3 000 servicios digitales. Este enfoque también permite a los funcionarios públicos encriptar documentos, revisar y aprobar permisos, contratos y solicitudes y presentar solicitudes de información a otros servicios. Este es un ejemplo de cadena de bloques con permiso, donde una parte del acceso está restringida para asegurar los datos y proteger la privacidad de los usuarios. Asimismo, el papel del Estado como autoridad que conserva el control del sistema contrasta con la estructura ascendente de muchas iniciativas promovidas por la comunidad de desarrollo de la cadena de bloques. Sin embargo, a medida que el sistema se extiende a las notarías públicas y los historiales médicos de pacientes, sigue siendo una de las iniciativas gubernamentales más avanzadas que utiliza la cadena de bloques.

Varios países, entre ellos Ghana, Kenia y Nigeria, han empezado a utilizar cadenas de bloques para gestionar registros catastrales. Su objetivo es crear un registro claro y fiable de la propiedad, en respuesta a los problemas de inscripción, corrupción y bajos niveles de acceso público a los registros. Suecia también está realizando pruebas para incorporar las transacciones inmobiliarias a la cadena de bloques, en este caso para que todas las partes (bancos, gobiernos, intermediarios, compradores y vendedores) puedan hacer un seguimiento del progreso del acuerdo de transacción en todas sus fases y garantizar la autenticidad y transparencia del proceso, ahorrando al mismo tiempo un tiempo y dinero considerables.

El Departamento de Trabajo y Pensiones del Reino Unido también ha probado el uso de la tecnología de la cadena de bloques con las prestaciones sociales. En este caso, los ciudadanos utilizan sus teléfonos para percibir y gastar las prestaciones y, con su consentimiento, sus transacciones se registran en un libro contable distribuido. El objetivo de la iniciativa es ayudar a las personas a gestionar sus finanzas y crear un sistema de bienestar más seguro y eficiente, evitando el fraude y aumentando la confianza entre los solicitantes y el Gobierno. El Gobierno británico también está estudiando cómo podría permitir la tecnología de la cadena de bloques hacer un seguimiento de la asignación y el gasto de fondos concedidos por el gobierno, donantes u organizaciones de ayuda a los beneficiarios reales, en forma de subvenciones, préstamos y becas.

Evolución y posibles efectos

La introducción de la tecnología de la cadena de bloques en las administraciones públicas podría dar lugar a la racionalización de los procesos internos, la reducción de los costes de transacción, interacciones e intercambios de datos más fiables con otras organizaciones o secciones gubernamentales y un aumento de la protección contra errores y falsificación. Algunos procesos podrían también automatizarse a través de contratos inteligentes. Sin embargo, también existen riesgos que deben tenerse en cuenta. En primer lugar, al pasar a un nuevo sistema de registros digitales, habrá costes de configuración y posibles dificultades

técnicas y procedimentales en la ejecución de sistemas de respaldo y paralelos durante las fases de transición. Además, es importante que las expectativas de custodia y control de los registros públicos en el momento en que se crean los registros sigan cumpliéndose mucho después de su creación. Por último, puesto que la tecnología almacena resúmenes criptográficos (descritos en la sección de patentes) u otras representaciones digitales incompletas de documentos, los particulares y las organizaciones tendrán que invertir más recursos para mantener sus documentos a largo plazo.

Aunque los libros contables de la cadena de bloques pueden registrar la fecha y los detalles de una transacción, no pueden verificar la precisión de lo que se describe en ella. Mientras la transacción cumpla los requisitos técnicos del protocolo, se convertirá en una parte inmutable del registro, con independencia de la veracidad de su contenido. De la misma forma que todas las solicitudes de información y documentos presentados a las oficinas públicas se examinan antes de aplicarse, sigue siendo necesario garantizar controles adecuados para aceptar e intercambiar información sobre sus equivalentes en la cadena de bloques. Aunque algún día sea posible automatizar, apoyar y proteger algunos de estos procesos, no se consideran un sustituto del papel vigilante de los funcionarios públicos.

El hecho de que los datos en la cadena de bloques sean inmutables —lo que significa que no pueden alterarse o eliminarse una vez que se han insertado— ofrece transparencia y rendición de cuentas. Sin embargo, también puede poner en riesgo la privacidad y la protección de datos, especialmente en lo que se refiere a datos personales o sensibles (que nunca deben almacenarse en una cadena de bloques). Las cadenas de bloques no garantizan el anonimato y, cuanto más personales son los datos, más fácil es identificar a la persona a la que pertenecen. Esta inmutabilidad puede poner en peligro el «derecho al olvido», conforme al cual los usuarios pueden, en determinadas circunstancias, exigir que se borren sus datos personales.

Es importante garantizar que todos los ciudadanos puedan acceder a sus servicios públicos. Existe el riesgo de que la cadena de bloques pueda exacerbar la brecha digital ya existente. Los ciudadanos que son incapaces de utilizar los servicios de internet por cualquier motivo pueden no ser capaces de aprovecharse de manera plena y directa de los avances en la cadena de bloques que les darían mayor control sobre sus datos y transacciones. A menudo, los servicios basados en la cadena de bloques estarían ocultos tras interfaces de servicio conocidas y fáciles de utilizar. La aplicación precisa del protocolo en términos tanto de estructura como de interfaz de usuario importa mucho para los valores políticos y sociales que promueve el sistema. Por último, cabe señalar que algunas iniciativas de cadenas de bloques fomentan la elusión de instituciones y autoridades centralizadas tradicionales, incluidos gobiernos y servicios públicos. Ya están apareciendo servicios similares a los públicos ofrecidos por agentes no estatales. Pueden atraer a comunidades cada vez más digitalizadas y globalizadas, pero también podrían presentar dificultades complejas para las autoridades públicas.

Formulación de políticas de anticipación

Es probable que las administraciones públicas mantengan un control central sustancial sobre sus aplicaciones de cadenas de bloques, y también puede que exijan «puertas traseras» a los sistemas privados de cadenas de bloques encriptadas con fines policiales y judiciales, aunque estas pueden generar nuevas vulnerabilidades en la seguridad. También puede que la próxima revisión de la Directiva de la Unión sobre privacidad electrónica tenga en cuenta la encriptación de extremo a extremo. Los gobiernos quizá estudien cómo podría ayudares la cadena de bloques a mejorar los servicios públicos, en particular ofreciendo transparencia y rendición de cuentas, y si deben reconocer los servicios independientes «similares a los públicos» dentro de sus jurisdicciones.

8. ¿Encadenar todo en bloques? Organizaciones autónomas descentralizadas

Los primeros pioneros de internet imaginaban un nuevo orden social de organizaciones más independientes, descentralizadas y ágiles facilitado por las tecnologías de la información y la comunicación. Algunos afirman que los modelos comunes y de igual a igual gestionarían mejor los recursos, y otros ya están desarrollando plataformas cooperativas de propiedad colectiva gobernadas democráticamente por sus usuarios o trabajadores. La cadena de bloques puede apoyar a estas organizaciones permitiendo el intercambio directo e instantáneo de datos o bienes, la ejecución de presupuestos, la ejecución automática de contratos o la toma de decisiones dentro de una organización, todo de manera transparente y encriptada. ¿Podría esto anunciar la aparición de nuevas organizaciones habilitadas mediante cadena de bloques, y qué significaría para la sociedad europea?

Libros contables descentralizados para organizaciones descentralizadas

Las organizaciones autónomas descentralizadas (OAD) pueden entenderse como agrupaciones de contratos inteligentes, que culminan en un conjunto de normas de gobernanza que se aplican y ejecutan automáticamente mediante cadenas de bloques. Una OAD podría adoptar un papel mediador entre distintas partes en una organización descentralizada pero controlada en última instancia por seres humanos, o podría constituir una organización plenamente autónoma controlada en su totalidad mediante algoritmos. Queda por ver el nivel de autonomía y autosuficiencia que alcanzarán las OAD. La OAD más madura —llamada «The DAO» — no es totalmente autónoma, pero no es descabellado imaginar un futuro en el que otras OAD sean casi completamente independientes de intervención humana, controlando sus propios recursos e interactuando con otros humanos y no humanos, incluidas otras OAD. Por ejemplo, una OAD podría poseer un coche de conducción autónoma que actúe como taxi las veinticuatro horas del día. Generaría ingresos que utilizaría para pagar su propio combustible, reparaciones y seguro y ahorraría dinero para sustituir el vehículo al final de su vida útil.

En las OAD, la cooperación entre personas dentro de las organizaciones y entre estas últimas puede basarse no en una autoridad centralizada o en fuerzas de mercado puras, sino más bien en un consenso criptográfico y transparencia como características técnicas básicas. Los contratos inteligentes en la cadena de bloques pueden no solo dejar un registro inalterable de todos los aspectos de la organización, sino también ejecutar de forma automática e incluso autónoma operaciones cotidianas, como apoyar el acceso a activos y edificios, asignar tareas, gestionar acciones y derechos de voto o facilitar la distribución de beneficios o la transmisión de micropagos.

Se ha sugerido que la tecnología de la cadena de bloques podría posibilitar una nueva generación de organizaciones para cambiar la dinámica económica y de poder de los órganos centralizados tradicionales. Por ejemplo, una plataforma de redes sociales que es propiedad de sus usuarios, que se califican entre sí y reciben automáticamente una recompensa por sus contribuciones; aplicaciones de transporte compartido donde los conductores también son copropietarios y gestionan las operaciones cotidianas; u otras comunidades como Steem-it donde los usuarios también son accionistas y donde el valor y las decisiones se distribuyen de manera transparente.

Evolución y posibles efectos

La cadena de bloques puede utilizarse para desarrollar estructuras descentralizadas dentro de las organizaciones. Sin embargo, al mismo tiempo, el uso de la cadena de bloques para cada transacción podría limitar flujos de información que hasta ahora eran predominantemente libres. La supervisión y el control del acceso a cada una de las transferencias de cualquier activo o contenido podrían dar lugar a reclamaciones de propiedad intelectual más intensas (por ejemplo en gestión de derechos digitales) y podrían ahogar la innovación y el auge de nuevos actores. Al suprimir la gestión centralizada, las OAD

podría eliminar los errores y la corrupción introducidos por los humanos. La confianza se trasladará de la reputación tradicional a redes tecno-sociales (como en los contratos y las monedas habilitados mediante cadena de bloques). Algunos afirman que esto podría generar nuevas formas de acción colectiva democrática, que transformen los enfoques de gobernanza descendentes que se critican por su inflexibilidad, opacidad, lentitud y déficit democrático.

The DAO recaudó más de 100 millones EUR en la mayor campaña de microfinanciación colectiva de la historia. Es una mezcla entre un sitio de microfinanciación colectiva y un fondo de capital riesgo basado en contratos inteligentes de Ethereum. Los financiadores votan para decidir todo, desde el nombramiento y despido de sus responsables hasta la financiación de proyectos. En junio de 2016, un ataque aprovechó las debilidades en el código de la OAD, desviando casi un tercio de sus activos y suscitando una controversia en la comunidad sobre lo que hacer después. Las opciones eran congelar los fondos en la cuenta (bifurcación suave, «*soft fork*»), hackear el sistema y restablecer el saldo original (bifurcación drástica, «*hard fork*») o no hacer nada. Por un lado, puesto que el o los atacantes aprovecharon una debilidad en el código, podría alegarse que no incumplieron el contrato y que la modificación de la cadena de bloques de The DAO minaría la confianza pública en su principio de inmutabilidad. Por otro lado, el ataque se produjo claramente contra el espíritu del contrato, puede haber contravenido el Derecho contractual y podría disuadir a participantes reales y potenciales en la comunidad. En cualquier caso, el incidente expuso las vulnerabilidades de seguridad existentes y puso a prueba los fundamentos ideológicos de la comunidad de desarrollo de la cadena de bloques.

La resistencia a utilizar estructuras jurídicas existentes (por ejemplo tratar a los desarrolladores principales y mineros como fiduciarios) dio lugar a demandas de mecanismos alternativos o más sofisticados, como sistemas de reputación/meritocráticos para incentivar la participación, o de normas y estándares éticos comunes. Sin embargo, el funcionamiento autónomo de estas organizaciones también plantea preocupaciones por la delegación en algoritmos y la regulación a cargo de ellos. Algunos afirman que esta gobernanza distribuida mediante código sigue entrañando obligaciones morales o responsabilidad por parte de la comunidad para intervenir en decisiones cruciales, mientras que otros están trabajando en la integración de los valores humanos y la voluntad general de los ciudadanos en contratos sociales algorítmicos.

Formulación de políticas de anticipación

Las OAD, como muchas iniciativas basadas en la cadena de bloques, existen en una zona gris reguladora que puede no ofrecer garantías de responsabilidad, protección o rendición de cuentas, especialmente cuando no se basan explícitamente en ordenamientos jurídicos existentes. También existe una preocupación jurídica por las ofertas de acciones de empresas criptográficas, que pueden colocar a las empresas en el mercado de valores existente, lo que exigiría su registro y cumplimiento de varias normas y obligaciones. Al operar fuera de un marco regulador, las organizaciones basadas en la cadena de bloques que no se han constituido como sociedad o no están legalmente reconocidas pueden correr riesgo de fraude de inversión o hackeos maliciosos, y sus miembros podrían estar expuestos a una responsabilidad como socios. Algunos han pedido una mayor supervisión y transparencia en la toma de decisiones algorítmicas y una modelización interactiva. La complejidad de los algoritmos avanzados hace que resulte difícil incluso para los desarrolladores entender totalmente sus normas de gobierno y comprobar su conformidad legal, por ejemplo con las leyes de lucha contra la discriminación y transparencia. Las organizaciones autogestionadas y autoexigibles también podrían cuestionar las nociones tradicionales de personalidad jurídica, acción individual y responsabilidad.

Las OAD podrían programarse para comerciar con bienes ilícitos o productos prohibidos. Aunque no esté garantizado el anonimato, la estructura eficiente, automática y distribuida de la cadena de bloques subyacente podría dificultarle a los órganos reguladores la aplicación de la ley y el cierre de operaciones. A las víctimas de delitos a manos de una OAD también podría costarles conseguir una indemnización u

obtener un mandato judicial contra la OAD maliciosa, puesto que la capacidad de adoptar dichas medidas no está específicamente codificada en su estructura.

Conclusiones

Aunque la aplicación de la cadena de bloques más conocida y utilizada y de mayor impacto es Bitcoin, la posible repercusión de la tecnología es mucho mayor y más amplia que las monedas virtuales. De hecho, puesto que otras aplicaciones pueden aprovechar la cadena de bloques de Bitcoin, los mayores efectos de Bitcoin pueden encontrarse fuera del ámbito de las monedas. Las transacciones de cualquier tipo son normalmente más rápidas y baratas para el usuario cuando se realizan a través de una cadena de bloques y también se benefician de la seguridad del protocolo. Aunque las transacciones en Europa suelen ser rápidas, baratas y suficientemente seguras para la mayoría de fines, los usuarios y los defensores de aplicaciones de la cadena de bloques a menudo ven ventajas adicionales en su transparencia e inmutabilidad. En efecto, se observa una creciente tendencia hacia una menor confianza en las instituciones financieras y de gobernanza y mayores expectativas sociales de rendición de cuentas y responsabilidad. La popularidad de la tecnología de la cadena de bloques también puede reflejar una tendencia social emergente a la priorización de la transparencia por encima del anonimato.

Por supuesto, por cada transacción que utiliza un libro contable distribuido en lugar de un sistema centralizado tradicional se desplaza a los intermediarios y mediadores, que pierden su fuente de poder e ingresos habitual. En el caso de las monedas, estos son los bancos, en el de las patentes, la oficina de patentes, en el de las elecciones, las comisiones electorales, en el de los contratos inteligentes, los ejecutores, y en el de los servicios públicos, las autoridades públicas. Un nivel considerable de crecimiento del uso de la tecnología de la cadena de bloques podría provocar un cambio sustancial en el fondo y, quizá, la cantidad de trabajo administrativo. Por ejemplo, una parte del trabajo de los intermediarios y los abogados especializados en contratos podría sustituirse por transacciones de igual a igual y contratos inteligentes. Muchos analistas están tranquilos ante esta perspectiva. Algunos afirman que la cadena de bloques solo desplazaría algunas de las tareas menos interesantes —como la aportación de pruebas de certificación—, dejando más tiempo para las tareas principales y más valiosas de prestación de servicios a medida. Aunque puede generar una cierta reducción de la cantidad total de trabajo, otros analistas citan similitudes con anteriores olas de automatización del trabajo manual —como las cadenas de producción robóticas— cuando las tareas repetitivas fueron desplazadas, dando lugar a la pérdida de puestos de trabajo, pero se crearon nuevos empleos de alta calidad en el diseño y el mantenimiento de los sistemas necesarios. En cualquier caso, aunque los datos siguen siendo escasos, la mayoría de analistas esperan un cambio en el perfil de las tareas realizadas por humanos sin una reducción general del número total de empleos y, quizá, un aumento de su calidad. Otro posible efecto indirecto del desarrollo de la cadena de bloques es el aumento del consumo de energía. En 2014, la cadena de bloques de Bitcoin fue responsable de un consumo eléctrico comparable al de Irlanda y no ha dejado de crecer desde entonces. Aunque podrían desarrollarse algoritmos y hardware más eficientes, la intensidad energética de las cadenas de bloques (y, de hecho, la de todos los procesos digitales) puede convertirse en un creciente problema en el futuro.

El efecto más profundo del desarrollo de la cadena de bloques podría encontrarse en efectos más sutiles en los valores sociales y estructurales generales. Estos efectos están asociados con los valores integrados en la tecnología. Todas las tecnologías tienen valores y políticas, que normalmente representan los intereses de sus creadores. En este contexto, las razonas por las que los sistemas de libros contables tradicionales posicionan a sus creadores como intermediarios centrales son claras: puesto que todas las transacciones pasan a través de ellos, los creadores mantienen su posición de poder y capacidad para beneficiarse de sus usuarios. Al utilizar tecnologías, las personas reafirman los valores y políticas que representan, por lo que cada vez que se utilizan estos libros contables para registrar una transacción, se reafirman la centralidad e indispensabilidad del actor que ocupa el centro. Por supuesto, un libro contable distribuido sin un intermediario central también está cargado de valor y política, al depositar la confianza en la tecnología de encriptación y creación de redes y redistribuir el poder de las autoridades centrales a

estructuras no jerárquicas entre iguales. En este contexto, utilizar este tipo de cadena de bloques *es* participar en un cambio general que reduciría la confianza en las instituciones tradicionales y su poder, por ejemplo bancos y gobiernos. Los casos estudiados en este informe revelan varios ejemplos de cómo encarnan las aplicaciones de la cadena de bloques estos valores. Desde luego, para que los cambios sean apreciables a un nivel social general, sería necesario un desarrollo realmente sustancial de la cadena de bloques, hasta el punto de que penetre en la vida cotidiana y la rutina mundana.

Cabe señalar que el interés en las aplicaciones basadas en la cadena de bloques a menudo parece ir de la mano del descontento con los sistemas, procesos y mediadores tradicionales. El desarrollo de la cadena de bloques suele presentar similitudes con la economía colaborativa en el sentido de que prometen conectar

Formulación de políticas de anticipación

A primera vista, el carácter descentralizado, encriptado y autoejecutable de las aplicaciones tecnológicas de la cadena de bloques parece asumir o basarse en un enfoque autorregulador que en principio funcionaría en paralelo a los instrumentos jurídicos tradicionales. Sin embargo, si se observan más detenidamente las aplicaciones más avanzadas de la cadena de bloques, se plantea una mezcla de interrogantes jurídicos y reguladores tradicionales y novedosos que deben considerarse de manera contextual, puesto que algunas de las aplicaciones mencionadas cuestionan los principios fundamentales del Derecho y dispersan el objeto de atención reguladora, como tal, de varias formas.

En primer lugar, el carácter descentralizado y transfronterizo de la cadena de bloques plantea problemas jurisdiccionales, puesto que parece dispersar la rendición de cuentas institucional y la responsabilidad legal de un modo sin precedentes, haciendo necesario un enfoque regulador armonizado a nivel transnacional más pertinente en comparación con uno local o regional. Si la tecnología de la cadena de bloques se desarrollase considerablemente, las estructuras jurídicas centralizadas podrían perder su capacidad para controlar el libro contable, con un traslado del control a sus usuarios o a otras partes del sistema, o para configurar las actividades de diferentes personas u organizaciones autónomas descentralizadas, puesto que nadie (incluido el creador original) puede controlar el libro contable después de su implantación. Habrá menos puntos de control para guiar y ayudar al flujo de datos. También hay varias cuestiones que deben tenerse en cuenta, como la exigibilidad legal de los contratos inteligentes y las cuestiones de responsabilidad y rendición de cuentas, puesto que los libros contables distribuidos carecen actualmente de la personalidad jurídica necesaria para que se les asignen responsabilidades y obligaciones. Este problema se agrava por el hecho de que operan a través de las fronteras y que los contratos inteligentes pueden no ser capaces todavía de realizar operaciones complejas.

Los sistemas descentralizados basados en la cadena de bloques pueden estar abiertos a la cooptación de poderes externos y, en ausencia de protección institucional suficiente, las plataformas podrían transformarse en oligarquías. Una organización autónoma descentralizada malintencionada podría ser una fuente de preocupaciones reguladoras en vista de las posibilidades de uso indebido de esta tecnología transformadora. Además, las cualidades encriptadas de la tecnología de la cadena de bloques pueden eliminar la posibilidad de utilizar formas legítimas de vigilancia con fines policiales y judiciales. La protección del consumidor también constituirá una preocupación fundamental para los reguladores, puesto que las cláusulas contractuales y las medidas de reparación pueden no quedar claras a los consumidores y, teniendo en cuenta su carácter automático, no ser fácilmente ajustables a un posible cambio de circunstancias. Además, existen preocupaciones en materia de seguridad de carácter regulador, puesto que se podría rastrear o deducir la identidad de una parte a partir de las transacciones. Por último, la cadena de bloques podría dar lugar a interrogantes sobre la elección del Derecho y la jurisdicción para la resolución de controversias en la materia.

a las personas entre sí, expulsando a los intermediarios y liberando a las personas de la intervención de los Estados, bancos y otras grandes instituciones, a menudo con una retórica de transición, alteración o incluso revolución. Sin embargo, como se ha visto, las iniciativas de mayor éxito de este movimiento se han convertido en los últimos intermediarios, muy alejadas desde el punto de vista estructural de la visión de descentralización que esperaban muchos ciudadanos. Lo mismo puede observarse con la cadena de bloques, donde la mayor repercusión se ha producido en aplicaciones que parecen distantes de la visión más idealista de descentralización y transparencia del desarrollo de la cadena de bloques. Por ejemplo, una autoridad electoral podría implantar un sistema de votación basado en la cadena de bloques con permiso, manteniendo el control de la distribución de pseudónimos para garantizar el anonimato y afirmando su papel como autoridad última y mediador central a través del cual deben pasar por los votos. Con ello no se niegan las posibles ventajas técnicas y políticas de este planteamiento. Más bien, es un recordatorio de que, en este tipo de cadena de bloques con permiso, el nivel de descentralización y transparencia se reduce, con consecuencias para la estructura técnica y la funcionalidad del libro contable, así como para los valores y la política que refleja. Es posible imaginar varios ejemplos paralelos para los catastros, bancos y oficinas de patentes, cada uno de los cuales podría adaptar aspectos técnicos del protocolo de la cadena de bloques, moderando al mismo tiempo los elementos idealistas de los valores que están integrados en él. Estos sistemas probablemente seguirían ofreciendo mejoras sustanciales en términos de mayor transparencia y rendición de cuentas y menor corrupción. De hecho, al cooptar a la cadena de bloques, las instituciones de gobernanza podrían utilizarla para crear «tecnologías reguladoras» que se empleen para cumplir los mismos objetivos reguladores —por ejemplo, transparencia o rendición de cuentas— que la legislación vigente.

Puesto que la cadena de bloques desplaza a los intermediarios, no puede confiarse en estos para regular su funcionamiento. Por lo tanto, deben desarrollarse otras palancas reguladoras alternativas para hacer cumplir la ley y mantener la capacidad de planificación y actuación eficaces. Pueden definirse cuatro amplias categorías de acción que podrían movilizar las instituciones de gobernanza en respuesta a la aparición de la tecnología de la cadena de bloques:

- Una opción es responder a los «problemas para los que la cadena de bloques representa una solución» sin utilizar en absoluto la cadena de bloques. Por ejemplo, si la demanda de la cadena de bloques se basa en un deseo de mayor transparencia en los procesos, podría ofrecerse a los ciudadanos un mayor acceso a los datos y procesos públicos sin utilizar sistemas de cadena de bloques.
- Una segunda opción es fomentar activamente el desarrollo y la innovación de la cadena de bloques por parte del sector privado dando legitimidad a sus productos. Por ejemplo, bajo determinadas condiciones, podría darse un reconocimiento jurídico explícito a las transacciones en las cadenas de bloques como registros de transacciones ejecutadas.
- La tercera opción es hacer lo contrario que en la segunda, es decir, desalentar el desarrollo negándose a aceptar la legitimidad de las transacciones basadas en la cadena de bloques, por ejemplo anulando y revocando las cláusulas de los contratos inteligentes.
- La cuarta opción es adoptar una cadena de bloques con permiso en los sistemas y estructuras existentes, manteniendo efectivamente el papel y el poder de los responsables como intermediarios ofreciendo parte de la funcionalidad básica de la cadena de bloques, pero sin ofrecer plena descentralización y transparencia. Este modelo ya se observa en el uso de la tecnología de la cadena de bloques en el sector público, por ejemplo en el Reino Unido y Estonia, así como en el sector privado.

Es probable que en la próxima década se apliquen variaciones y combinaciones de las cuatro estrategias en la tecnología de la cadena de valor en distintos ámbitos y jurisdicciones. Por el momento, hay poco interés en una intervención a nivel europeo. De hecho, un informe del Parlamento Europeo sobre monedas virtuales reciente reconoció los mayores riesgos, que exigirán aumentar la capacidad reguladora y los conocimientos técnicos especializados adecuados, al tiempo que pedía un enfoque regulador proporcionado en la Unión para no obstaculizar la innovación en esta fase incipiente.

Para concluir, el hecho de que el protocolo de la cadena de bloques proporcione plataformas para buenas acciones y malas acciones no significa que sea una tecnología neutra. En su forma más pura promueve la redistribución del poder de los actores centrales entre amplias comunidades de pares. Aunque probablemente la aspiración más idealista y revolucionaria del desarrollo de la cadena de bloques no pase de una aspiración, incluso su aplicación moderada puede promover un cierto grado de redistribución y transparencia. Como señala Glyptis, la cadena de bloques no hará mejores a las personas, pero podría hacer algunas de las precauciones necesarias en la vida cotidiana de las personas más rápidas, baratas, seguras y transparentes.

La tecnología de la cadena de bloques interesa cada vez más a ciudadanos, empresas y legisladores de toda la Unión. Este informe tiene como objetivo facilitar un punto de entrada a los curiosos de la tecnología de la cadena de bloques, con el fin de estimular el interés y suscitar un debate en torno a su posible repercusión. La introducción general viene seguida por un análisis más minucioso de ocho ámbitos en los que se ha descrito que la cadena de bloques tiene una posible repercusión sustancial. En cada uno de ellos se explica cómo se podría desarrollar la tecnología en ese ámbito particular, los posibles efectos que podría tener este desarrollo y cuáles son las posibles cuestiones que deben anticiparse en materia de políticas.

Publicación de la
Dirección de evaluación de impacto y valor añadido europeo
Dirección General de Servicios de Estudios Parlamentarios, Parlamento europeo

PE 581.948
ISBN 978-92-846-1046-4
doi: 10.2861/087736
QA-02-17-043-ES-N