Situación, impacto y retos actuales de la tecnología blockchain

Pablo Serrano Castillo
Ingeniero Full Stack y blockchain en Grant Thornton

Luis Pastor
Socio Responsable Consultoría Tecnológica e Innovación en Grant Thornton. Responsable del Centro de Competencia blockchain

Sara Esclapés Membrives
Abogada Especialista en blockchain

Rafael León Alemany
Abogado especialista en blockchain

Resumen

blockchain es la tecnología que, sin duda, está llamada a cambiar radicalmente la forma en que las personas y organizaciones intercambiamos valor (dinero, propiedad intelectual, derechos, contratos, activos, etc.), ofreciendo la posibilidad de minimizar e, incluso, prescindir de intermediarios y terceros de confianza.

blockchain salió a la luz en 2009, con la aparición de Bitcoin, una criptomoneda que hace uso de esta tecnología para evitar el doble gasto en las transacciones sin necesidad de ninguna autoridad central. Su propósito consistía en la creación de un sistema monetario paralelo a los bancos centrales y entidades financieras, gracias a una emisión de moneda propia y transparente, y con la posibilidad de realizar transferencias desde cualquier parte del mundo de manera confiable y segura.

Sin embargo, este solo fue el punto de partida. A partir de esta tecnología, tanto *startups* como grandes corporaciones están enriqueciendo y ampliando la manera de gestionar estas transacciones de valor, creando verdaderas aplicaciones descentralizadas mediante la ejecución de contratos inteligentes *(smart contracts),* gracias a las propiedades únicas ofrecidas por blockchain como la inmutabilidad, la transparencia o la trazabilidad.

Palabras clave

Blockchain, cadena de bloques, criptodivisa, transacción, smart contract, descentralización, inmutabilidad, transparencia, neutralidad, privacidad.

La realización de cualquier tipo de transacción requiere cierta confianza entre las partes que participan en ella. Por primera vez en la historia, una tecnología permite obviar esta necesidad en el mundo digital generando la confianza necesaria a través de una cadena de bloques: la tecnología blockchain.

Gracias a esta tecnología, surgida en 2009 como parte del protocolo de Bitcoin, las criptodivisas han conseguido resolver el desafío de intercambiar valor digitalmente sin tener que preocuparse de que alguien gaste el mismo activo dos veces («doble gasto»). Gracias a ello, blockchain cierra la etapa del Internet de la Información, para dar lugar al Internet del Valor.

Sin embargo, Bitcoin no fue el primer proyecto de moneda digital, ni es el último hito logrado al respecto. Proyectos basados en efectivo digital como eCash y Bit Gold sentaron las bases de lo que hoy son las criptodivisas. Igualmente, monedas como Dash, ZCash o Monero surgieron posteriormente con el objetivo de solventar el desafío de privacidad inherente a Bitcoin. Ethereum, por su parte, supone un salto enorme en el desarrollo de las criptodivisas creando el concepto de aplicaciones descentralizadas (DAPPs), en las que cada aplicación está compuesta por *smart contracts* que ejecutan lógica de negocio. Ello ha permitido utilizar la tecnología blockchain para otros fines distintos a la realización de transacciones con criptodivisas.

Precisamente, el crecimiento exponencial de diferentes tecnologías de blockchain y la proliferación del uso de las criptodivisas entre la población han llevado a multitud de pronunciamientos legales por parte de distintas autoridades, con el objetivo inicial de delimitar la naturaleza de las criptodivisas para, posteriormente, determinar cuál es la legislación aplicable.

Asimismo, el foco regulatorio también se ha centrado en definir las reglas aplicables a nuevas formas de financiación basadas en blockchain. Similar a la Initial Public Offering (IPO) tradicional de las empresas que cotizan en bolsa, la versión en moneda criptográfica se conoce como Initial Coin Offering (ICO): una forma de financiación basada en la emisión de tokens (representaciones digitales de cualquier tipo de valor).

Esta revolución económica, tecnológica y social que suponen blockchain y las criptodivisas requiere también analizar su impacto en términos de consumo energético, el cual es necesario para la sostenibilidad de la red. El mantenimiento de blockchains públicas que sustentan criptodivisas como Bitcoin o Ethereum requiere, hoy en día, de un alto consumo energético, teniendo implicaciones desde los prismas medioambiental y económico, por lo que se están desarrollando soluciones alternativas que permitan una emisión menos costosa.

Este, sin embargo, no es el único reto relacionado con la tecnología blockchain y las criptodivisas. La escalabilidad del sistema, la gobernanza de la red y la seguridad son desafíos que ya se están abordando en la actualidad y que, en muchos casos, cuentan con soluciones en desarrollo.

Asimismo, cabe reseñar que el impacto de blockchain y las criptodivisas a nivel geopolítico y social puede ser relevante. Entre otras razones, porque estas tecnologías ofrecen la oportunidad de realizar transacciones a aquellas personas que no pueden operar a través de un banco o que no pueden permitirse los costes de un tercero para intercambiar valor entre sí.

Igualmente, desde el punto de vista financiero e industrial, las oportunidades son prácticamente infinitas: desde la gestión de la cadena de suministro entre proveedores y clientes hasta sistemas de pago internacionales, pasando por la certificación de documentos.

Propiedades de blockchain

Las características y el valor añadido que aporta la tecnología blockchain se pueden resumir en:

- **Inmutabilidad:** ninguna operación ni información vertida en una blockchain puede alterarse o revertirse (transacción, balance o estado de una cuenta, etc.).
- **Trazabilidad:** todo registro queda almacenado históricamente con un sellado de tiempo, pudiendo trazarse.
- **Transparencia:** originalmente, todas las operaciones producidas en la blockchain son visibles para todos los participantes en la misma. No obstante, a causa de las necesidades empresariales, esta propiedad se ve alterada en ocasiones.
- **Descentralización:** tanto a nivel de poder (ausencia de intermediarios e igualdad entre los participantes), como a nivel de consumo de recursos (se reparte su utilización).

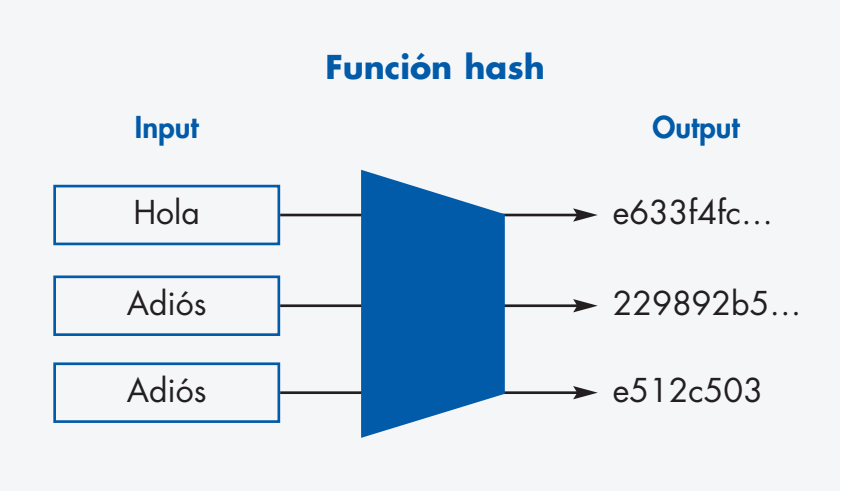
Estas propiedades generan una serie de beneficios de gran valor para los usuarios de plataformas blockchain:

- **Confianza:** una vez garantizadas la inmutabilidad, trazabilidad, transparencia y las condiciones para la descentralización del sistema, es posible afirmar que la confianza reside en la tecnología.
- **Creación e intercambio de valor:** posibilidad de emitir moneda propia o de tener una representación de activos que se intercambian entre distintos usuarios de un punto a otro, sin intermediarios y de manera prácticamente instantánea.
- **Ejecución de acuerdos en situación de igualdad:** posibilidad de garantizar la ejecución de cualquier acuerdo entre partes en situación de igualdad, sin posibilidad de que puedan modificar unilateralmente cualquier cláusula y sin necesidad de intervención de un tercero.

Cómo se garantizan las propiedades de blockchain

Estas propiedades o características que hacen única a la tecnología blockchain se garantizan mediante la aplicación de los siguientes mecanismos criptográficos:

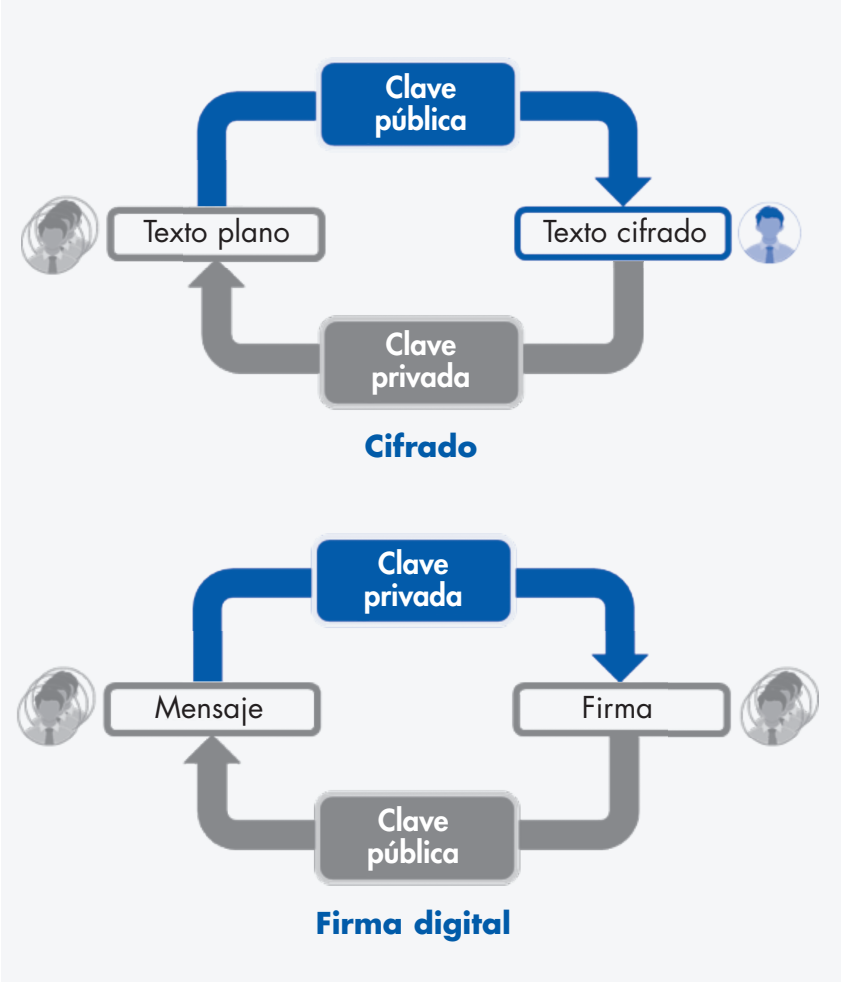
- **Función hash:** es una función computable mediante un algoritmo que permite obtener, a partir de cualquier información, un código alfanumérico único desde el cual se puede comprobar en cualquier momento futuro que dicha información no ha sido modificada, pero desde el que, por sí solo, no se puede obtener dicha información.



- **Criptografía asimétrica:** cada usuario de la red blockchain tiene un par de claves: pública y privada. La clave privada debe guardarse en un lugar seguro y la pública se difunde al resto de participantes en la red. Con ambas claves, la criptografía asimétrica tiene dos usos:

  –*Cifrado:* un mensaje cifrado mediante la clave pública solo podrá ser descifrado por el poseedor de la clave privada, garantizando la confidencialidad de la comunicación.

  –*Firma digital:* un mensaje cifrado mediante la clave privada podrá ser descifrado por cualquier persona usando la clave pública, verificando la autenticidad del mensaje y emisor.



- **Mecanismo de consenso:** es la manera mediante la cual los nodos validadores (participantes con el rol de garantizar la integridad de la cadena) llegan a un acuerdo sobre la veracidad de los datos incluidos en la misma para que, a continuación, pasen a conformarla de manera perpetua. Existen tres algoritmos principales:

  –Prueba de trabajo *(Proof of Work)*. La verificación de las transacciones depende de la potencia de cálculo de los nodos validadores de la red, llamados mineros. Cuanto más dinero invierta un minero en capacidad de procesamiento, más opciones tendrá de resolver un reto matemático que de lugar a la generación del último bloque de la cadena, por lo que es retribuido.

  –Prueba de autoridad *(Proof of Authority)*. La verificación de las transacciones depende de un conjunto de nodos autorizados previamente.

  –Prueba de Participación *(Proof of Stake)*. La verificación de las transacciones depende del total de criptomonedas o tokens de la blockchain que se posea. Cuantos más tokens o criptomonedas haya adquirido el staker, más probabilidades tendrá de ser el elegido para validar el bloque y de ser retribuido por ello.

- **Smart contracts.** Son programas informáticos compuestos de dos partes: un conjunto de datos (el estado del contrato) y un conjunto de métodos o funciones que hacen operaciones sobre esos datos. Por ejemplo un método sería *«enviar_dinero (origen, destino, cantidad)»*. El smart contract, para ello, deberá guardar el balance de ambos usuarios en el estado del contrato y, cuando el emisor active esta operación, el cliente o nodo blockchain

procederá a restar el dinero del balance del origen y lo añadirá al balance del destino. También permiten un mecanismo de eventos, mediante el cual un smart contract puede enviar notificaciones fuera de la blockchain.

Tecnologías como Ethereum aseguran que la ejecución de estos códigos o métodos (también llamados transacciones) se ejecuten de manera atómica. No obstante, en caso de error, debe instrumentarse la manera por la que hacerlo reversible por parte de los desarrolladores, mediante cláusulas que permitan deshacer la acción. Ejemplo de contrato en lenguaje Solidity (tecnología Ethereum).

```
contract ContratoDeEjemplo {
  uint numero;

  event miEvento(
    address indexed usuario,
    uint numero
  );

  function miFuncion(uint _numero) payable {
    numero = _numero;

    miEvento(msg.sender, msg.value);
  }

  function miFuncionConstante() constant returns(uint) {
      return numero;
  }
}
```

Aplicaciones de blockchain y casos de uso

Las características o propiedades que aporta blockchain pueden aplicarse a un gran abanico de sectores, a través de una infinidad de casos de uso. Sin embargo, antes de concebir un caso de uso debemos tener en cuenta el alcance de la propia blockchain, que puede ser de tres tipos o magnitudes:

- **Blockchain pública:** es la red mundial de nodos desplegada sobre la que se transfieren las criptomonedas creadas nativamente (Bitcoin, Ethereum, etc.). La gobernanza y los mecanismos de consenso sobre las que se rigen estas redes son críticos para su correcto funcionamiento, evitando que se produzcan ataques o abusos por parte de cualquier actor de la red, ya que cualquiera puede unirse a la misma.
- **Blockchain privadas:** son aquellas que requieren permisos de acceso y que puede tener uno o varios propietarios. Habitualmente, se construyen descargando el software libre para cada nodo y se transfieren las unidades de valor o tokens que la propia empresa u organismo emite (tokenizan sus propios activos). Los mecanismos de consenso por los que se rigen son más sencillos, lo que implica que su velocidad sea mucho mayor.

De forma genérica, las utilidades a partir de las cuales se construyen los casos de uso son las siguientes:

En muchos casos pueden aplicarse a la vez estas tres utilidades. Por ejemplo, podemos imaginar la gestión de un producto financiero como son las acciones de una compañía:

–Emisión de un token que represente una acción de una compañía.

–Creación de una lógica que gestione el token o activo de manera automatizada: un smart contract que almacene y gestione cuándo se compra esta acción, quién es su poseedor actual, su dividendo, el precio actual de la acción en mercados secundarios, cuándo se liquida el pago de ese dividendo al propietario, etc.

–Garantizar procesos de certificación o trazabilidad de ese token. Por ejemplo, se puede registrar quién y cuándo realizó la compra de esa acción, qué regulador o entidad validó la operación, etc.

Más allá de este ejemplo, a continuación veremos tres casos de uso concretos en el sector financiero (el más avanzado en su adopción) en los que se está trabajando y que permiten ilustrar las propiedades de la tecnología:

Identidad digital

En la actualidad, cada entidad financiera dispone de una información diferente de cada cliente. Ello es lógico, dado que cada estrategia comercial y operativa lleva a establecer unos requerimientos distintos. Quizá no lo sea tanto cuando nos referimos a entidades que pertenecen a un mismo grupo empresarial. Y, desde luego, no lo es si se trata de ofrecer una mejor experiencia al cliente, pues debe repetir procesos similares y aportar documentación idéntica a cada entidad con la que contrata.

Por si fuera poco, las exigencias legales relativas a este deber de conocimiento no dejan de aumentar, con el aumento de costes que ello lleva asociado. La ventaja competitiva buscada al diseñar unos requerimientos específicos no se basa en cumplir con la regulación –esa es una obligación común–, sino en disponer de una información más completa, precisa y veraz que permita mejorar la segmentación y, de esta manera, afinar las estrategias comerciales para maximizar tanto la captación de nuevos clientes como la venta de productos a clientes ya existentes.

Por tanto, mucha de la información de la que se dispone podría ser compartida sin que ello supusiera comprometer la ventaja competitiva. O, al menos, siendo los beneficios asociados a hacerlos superiores a los inconvenientes. Y es en este punto donde entra blockchain, la tecnología que garantiza un sistema de gobernanza neutral entre distintas entidades sin necesidad de incurrir en los costes asociados a un tercero.

Añadiendo los factores señalados previamente, como las diferencias en la información entre entidades de un mismo grupo empresarial o la potencial mejora de la experiencia de cliente, encontramos que blockchain ofrece una oportunidad única, lo que ha llevado a que este caso de uso sea uno de los más utilizados a nivel mundial.

Más si cabe en el contexto europeo, dada la entrada en vigor del nuevo Reglamento Europeo de Protección de Datos (más conocido como GDPR, por sus siglas en inglés) el próximo 25 de mayo. Los principios que establece, tales como la transparencia o la exactitud, y el derecho a la portabilidad del dato llevan a la necesidad del establecimiento de nuevos sistemas. Nuevos sistemas que encajan a la perfección con las propiedades de la tecnología blockchain.

Pagos y transferencias

En primer lugar, es necesario subrayar que la tecnología blockchain, tal y como la conocemos hoy en día, puede haber cambiado sustancialmente dentro de tres años. Hoy, Bitcoin soporta 7 transacciones por segundo. Visa, 56.000. Ello podría llevar a descartar la tecnología para cualquier medio de pago con un elevado volumen de transacciones. Sin embargo, se está trabajando en blockchains que multiplican el rendimiento de Visa y es pronto para saber si se terminarán imponiendo.

Ello no obsta para señalar que Bitcoin, por el momento, ha fracasado en su propósito de convertirse en un medio de pago masivo. Por el contrario, su éxito se debe a su consideración como valor refugio. ¿Significa eso que Bitcoin no tenga valor como medio de pago en la actualidad? Seguramente no. Hay millones de personas sin acceso a una cuenta bancaria, para quienes la criptodivisa facilita el acceso a los pagos digitales.

Cambiando el foco hacia las transferencias, la situación es distinta. El tiempo que tarda en completarse una transferencia en Bitcoin no varía en función del país a que se realice, si se trata de un día hábil o de la hora a la que se ha efectuado. Ello en sí mismo supone un enorme avance, pero ¿realmente es necesario blockchain para que una transferencia internacional no tarde varios días en completarse? ¿No sería posible con otras tecnologías ya existentes?

En este sentido, resulta fundamental diferenciar entre las transferencias que implican cambio de divisa y las que no. En la segunda, ya existen proyectos para convertirlas en casi instantáneas sin hacer uso de la tecnología blockchain. No así en el primer caso, dada la existencia de bancos corresponsales con intereses diferentes que ralentizan el proceso. Además, es necesario determinar parámetros como el tipo de cambio o el momento exacto en que se producirá, aspectos en los cuales blockchain podría aportar una ventaja única.

No obstante, dada la complejidad de la implantación por la diversidad de los intervinientes, una entidad con filiales en distintos países (o varios bancos integrantes de un consorcio) puede llevar un registro paralelo en blockchain, en el que los «criptoeuros» o «criptodólares» pasen de uno a otro balance en cuestión de segundos en lugar de días.

Seguros

Como es habitual, el sector asegurador ha tardado algunos años más en abrazar la última tecnología disruptiva que el bancario. Por ello, pese a la enorme aplicabilidad de blockchain en toda su cadena de valor, son aún escasas las Pruebas de Concepto (PoC) e investigaciones realizadas.

Su aplicabilidad comienza con la identidad digital a la que se ha hecho referencia, cobrando especial interés en este caso la compartición del historial de siniestralidad entre aseguradores y entidades bancarias para la mejora del *scoring* del cliente.

Asimismo, la automatización que aportan los smart contracts permite crear microseguros que, si antes no eran rentables, ahora sí que pueden serlo. Un ejemplo claro sería el seguro de cancelación de vuelos, en el que estaría automatizado el proceso mediante el que se indemnizaría en caso de que se produjera el evento mediante una simple consulta a las fuentes especificadas. Como también puede ser disruptivo en el caso de los nuevos seguros a los que ha dado lugar la economía colaborativa, vinculando a la identidad digital de un cliente en blockchain su aseguramien-

to al conducir distintos vehículos proporcionados por distintas empresas especializadas en car sharing.

No menos impacto puede tener en la gestión de siniestros, basada en el intercambio de mensajes entre compañías para determinar la culpabilidad a través de una plataforma que ha llegado a estar inoperativa durante 10 días, dando lugar a que ningún asegurado a terceros en España recibiera un volante de reparación en ese plazo. Por el contrario, blockchain garantizaría una plataforma neutral y siempre operativa. Del mismo modo, podría reconciliar la distinta información sobre el cliente que poseen las distintas corredurías, mediadores y filiales. Además, su mecanismo de sellado de tiempo llevaría a la eliminación de gestiones manuales que se llevan a cabo en la actualidad para probar si un asegurado estaba cubierto en un momento exacto del tiempo o no.

Por último, podría revolucionar el mundo del reaseguro, reduciendo drásticamente los plazos de las compensaciones gracias a la trazabilidad de la cobertura; así como suponer el crecimiento exponencial de las cautivas o auto-seguros.

Retos técnicos y legales

Una vez conocidas las cualidades de blockchain y el horizonte tan prometedor que ofrece para transformar industrias y sectores, esta tecnología también debe enfrentarse en el presente y en el futuro a una gran cantidad de retos técnicos y legales.

Técnicos

- Escalabilidad: capacidad que tiene un sistema para responder adecuadamente cuando crece exponencialmente el número de transacciones, de usuarios, datos procesados, etc. sin afectar su rendimiento. Las plataformas blockchain se basan en protocolos P2P (*Peer to Peer,* P2P por sus siglas en inglés) para intercambiar mensajes, conllevan grandes latencias cuando los nodos propagan repetidamente transacciones y bloques de la cadena, pudiendo disminuir notablemente el rendimiento de la plataforma.

  Otro parámetro importante a tener en cuenta es el número de transacciones que puede procesar por segundo: para aumentarlo, las tendencias son aumentar el tamaño del bloque, disminuir el tiempo de generación de bloques y tratar la cadena por fragmentos (sharding).

  En este sentido, hay que destacar la capacidad de almacenamiento requerido por parte de los nodos de la red, dada una cadena de bloques que crece infinitamente. Para ello, se están intentando diseñar estructuras de datos más ligeras y eficientes (con tiempos de acceso más rápidos) y que podrían reemplazar a la cadena secuencial de bloques que conocemos hasta ahora.

- Seguridad: si bien las plataformas blockchain, en general, se han mostrado seguras respecto a la integridad y a la autenticidad de las transacciones (la red pública Bitcoin lleva realizando transacciones con total seguridad 9 años), no ha sido así respecto a la gestión del acceso a la plataforma y la gestión de claves. Los ataques a monederos privados y plataformas de intercambio (donde se cambia dinero fiduciario por criptodivisas), han sido recurrentes durante los últimos años.

  Prueba de ello es el escándalo de Coincheck, plataforma de intercambio japonesa que fue atacada en enero de 2018 y, como resultado, perdió 400 millones de dólares en

criptodivisa XEM. Ya se están tomando medidas y, recientemente, el regulador japonés de mercados financieros (FSA) ha prohibido operar temporalmente a 7 plataformas de intercambio, prohibición que no será levantada hasta que no mejoren sus condiciones de seguridad informática y cumplan más estrictamente con normas de prevención de blanqueo de capitales.

- **Privacidad vs Transparencia:** a día de hoy, hay diferentes tecnologías que ofrecen distintas soluciones de privacidad en las transacciones realizadas sobre blockchain (ZCash, Monero, Quorum, etc.), permitiendo proteger tanto el origen, como el destino, la cantidad y el contenido general de cualquier transacción o estado de una cuenta. La privacidad implica que solo los nodos afectados que comparten esas transferencias confidencialmente puedan validarlas. Es decir, confirmar la validez de los bloques.

  Este hecho, en cierta manera, hace perder a la plataforma la confianza mutua que ofrece una red totalmente transparente. El debate entre transparencia y privacidad debe resolverse en función de la sensibilidad de los datos manejados, las restricciones legales que comporten su manejo y el objetivo de negocio.

- **Coste energético de algunas blockchain públicas:** el consumo de energía eléctrica que supone el minado en la red pública de Bitcoin está, actualmente, por encima del consumo de países como Irlanda o Dinamarca. Es por ello que la línea de trabajo de muchas plataformas blockchain es la migración a modelos menos costosos energéticamente como la Prueba de Participación o de Autoridad, evitando las complejas operaciones criptográficas que dan lugar al citado consumo.

Legales

- **Descentralización:** debido a la ausencia de una figura central en las plataformas blockchain, resulta difícil determinar la competencia para regular las actividades o transacciones que en ella se realizan. La posición legal más aceptada se basa en abordar cada transacción de forma individual, de forma que, en caso de disputa entre las partes, y de conformidad con los principios de derecho internacional que correspondan, pueda determinarse la ley aplicable y el tribunal competente.

- **Inmutabilidad:** la información vertida en blockchain es inmutable. Es decir, no se puede modificar ni eliminar, lo que implica un desafío a las normas sobre protección de datos personales. Particularmente, en lo que se refiere al ejercicio de derechos de acceso, oposición, rectificación o cancelación. También cobran importancia, en este ámbito, algunos principios consagrados en el nuevo Reglamento Europeo de Protección de Datos, como el de limitación del tratamiento o el principio de confidencialidad e integridad.

- **Anonimato:** este problema afecta exclusivamente a las criptodivisas y no a la tecnología blockchain en sí misma. Hasta hace poco tiempo, las plataformas de intercambio no se encontraban obligadas a identificar de forma fehaciente a las personas físicas o jurídicas que realizaban las transacciones con criptodivisas. Esto implicaba una importante falta de control sobre el origen de los fondos con los cuales se adquirían dichas criptodivisas, lo que pronto alarmó a las autoridades nacionales e internacionales.

  Por este motivo, se ha procedido a modificar la Directiva europea 2015/849 relativa a la prevención de blanqueo de capitales y finan-

ciación del terrorismo. Dicha modificación consiste en incluir como sujetos obligados al cumplimiento de la ley a (i) los proveedores de servicios de cambio de monedas virtuales por monedas fiduciarias y a (ii) los proveedores de monederos electrónicos que ofrezcan servicios de custodia de las credenciales necesarias para acceder a monedas virtuales, como sujetos obligados de dicha norma.

- **Smart contracts:** los smart contracts son programas/códigos que permiten que determinados acuerdos se autoejecuten por ellos mismos una vez se han cumplido una serie de condiciones en el mundo real. Por tanto, los smart contracts serán legalmente vinculantes para las partes en la medida en que su ejecución no contradiga ningún acuerdo previo ni ninguna ley aplicable. Para ello, debemos acudir al marco jurídico de referencia que corresponda.
- **Validez de la información almacenada en blockchain:** existen numerosas iniciativas legislativas que reconocen la veracidad de la información almacenada en blockchain. Estas iniciativas han tenido lugar principalmente en Estados Unidos.

Conclusiones

La tecnología blockchain está transformando la manera en la que se intercambia valor entre personas y empresas, gracias a las características únicas que ofrece, tales como la in-

Ideas fuerza

- blockchain ha finalizado la era del Internet de la Información para dar lugar al Internet del Valor.
- blockchain ha permitido que, por primera vez, no sea necesario recurrir a un tercero de confianza para evitar que un activo digital pueda ser gastado dos veces.
- Las criptodivisas son solo la aplicación inicial de la tecnología blockchain, la cual tiene muchas más aplicaciones que ya se están implementando.
- Grandes bancos ya están integrando la tecnología blockchain, tanto para la mejora de procesos internos como para la generación de nuevos modelos de negocio.
- Santander InnoVentures indicó en 2015 que blockchain puede llegar a reducir los costes globales de infraestructura bancaria entre 15 y 22 mil millones de dólares. Hoy, estas previsiones son aún más optimistas.
- La capitalización actual del mercado de criptodivisas a nivel mundial es de 350 MM USD, habiendo alcanzado el máximo de 800 MM en enero de 2018.
- Las aplicaciones potenciales en distintos sectores son enormes, si bien el grado de adopción es menor que en el sector bancario.
- 9 años de funcionamiento exitoso de la red pública de Bitcoin, mostrándose totalmente segura frente a cualquier tipo de ataque.
- El coste energético que supone el minado en la red pública de Bitcoin está actualmente en el tamaño de un país como Irlanda o Dinamarca. La tendencia es pasar a otros mecanismos menos costosos.

mutabilidad y la transparencia. Inicialmente, gracias a la aparición de las criptodivisas, primera moneda en cuya emisión y gestión no interviene ninguna autoridad central. Posteriormente, mediante la aplicación de la tecnología en multitud de sectores, gracias a sus utilidades para la certificación, la tokenización y los smart contracts.

Gracias a estos, en multitud de sectores están desarrollándose aplicaciones totalmente disruptivas que permiten desde el ahorro de costes al mejorar procesos internos hasta la generación de nuevos modelos de negocio. Modelos caracterizados, en muchos casos, por multiplicar la generación de sinergias entre distintas empresas, redundando en una mejora del servicio al cliente.

Sin embargo, el carácter innovador y disruptivo de la tecnología lleva a la necesidad de nuevos retos, tanto desde el punto de vista técnico como del legal. La gran innovación generada alrededor de blockchain está permitiendo encontrar multitud de soluciones a los retos técnicos, mientras que la mayor lentitud del regulador impide que los legales se resuelvan a la misma velocidad. Ello obliga a buscar soluciones que permitan cumplir con la normativa actual por parte de las empresas que desarrollan estas aplicaciones, lo que se está consiguiendo, de manera que el impacto de la tecnología blockchain en distintos sectores es ya una realidad.

Bibliografía

https://coinmarketcap.com/

https://bitinfocharts.com/

https://etherscan.io/

https://blockchain.info/es

https://digiconomist.net/bitcoin-energy-consumption

http://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:52016PC0450&from=ES

https://www.finextra.com/finextra-downloads/newsdocs/the%20fintech%202%200%20paper.pdf

https://asia.nikkei.com/Spotlight/Bitcoin-evolution/Japan-regulator-punishes-7-cryptocurrency-exchanges-over-security

Pablo Serrano Castillo. Ingeniero de Blockchain y Full Stack en Grant Thornton Spain. Con ocho años de experiencia desarrollando proyectos tecnológicos en diferentes sectores, Pablo participa actualmente en la implantación de soluciones Blockchain para las principales entidades financieras de España.

Luis Pastor. Socio Responsable Consultoría Tecnológica e Innovación, Responsable del Blockchain Innovation Center Grant Thornton. Luis es el fundador del Blockchain Lab de Grant Thornton Spain, uno de los centros de innovación en tecnología Blockchain más competitivos a nivel global actualmente, tanto desde el punto de vista tecnológico como de negocio. Luis forma parte del equipo promotor y es líder del Comité de Miembros de la red Blockchain Alastria, consorcio multisectorial nacional de tecnología Blockchain.

Sara Esclapés Membrives. Abogada Blockchain en Grant Thornton Spain. Con experiencia en asesoramiento mercantil, derecho de nuevas tecnologías y protección de datos, Sara participa actualmente en el análisis legal previo de soluciones Blockchain para diferentes sectores económicos. Asimismo, Sara participa en el Consorcio nacional de Blockchain «Alastria» del que Grant Thornton es socio fundador.

Rafael León Alemany. Consultor Blockchain en Grant Thornton Spain. Con experiencia en consultoría estratégica y de innovación, Rafael participa actualmente en la implantación de soluciones Blockchain desde el punto de vista funcional para el sector bancario y asegurador. Asimismo es responsable del Observatorio Permanente de CK-GT de Blockchain.