ARI 105/2019
12 de noviembre de 2019

La seguridad y privacidad del blockchain, más allá de la tecnología y las criptomonedas

Javier Alonso Lecuit | Miembro del Grupo de Trabajo de Ciberpolítica del Real Instituto Elcano.

Tema

El artículo ofrece un recorrido sobre los retos en la seguridad y la regulación de la protección de datos de carácter personal que plantea la tecnología blockchain.

Resumen

La tecnología *blockchain* vive un momento prometedor en el campo de las inversiones (7.400 millones en *startups* en 2018, según la Comisión Europea) y las expectativas (gestionará un 10% del PIB mundial en 2025, según el Foro Económico Mundial), a lo que habría que añadir el uso de criptomonedas tales como Bitcoin, Ethereum, Litecoin y Monero. A pesar de esta prometedora perspectiva, el *blockchain* es una tecnología en construcción que presenta notables retos tecnológicos, jurisdiccionales y jurídicos. Aun siendo conceptualmente segura, su implementación no tiene por qué serlo en igual medida, según evidencian diversos incidentes registrados hasta la fecha, así como los retos que en ocasiones plantea la interpretación y la aplicación de la regulación de datos personales, tales como el derecho a la rectificación o el derecho al olvido.

Análisis

La tecnología *blockchain* permite realizar transacciones de valor entre usuarios sin que intervengan intermediarios en el proceso, es decir, descentraliza la gestión de las transacciones y presenta a todos sus participantes un mismo libro de registro o base de datos descentralizada (*distributed ledger*). Las transacciones pueden ser monetarias (criptomonedas) o de otra naturaleza (bienes, información, servicios, etc.) y se desarrollan sobre plataformas cuyos nodos se comunican mediante redes de pares iguales (P2P [1]) a través de conexiones a Internet. El *blockchain* ofrece una representación o registro dinámico e inalterable de esas transacciones a lo largo del tiempo que sustituye a intermediarios y autoridades centralizadas de confianza (p. ej. notarios, bancos, aseguradoras, etc.) que respalden las transacciones por la confianza digital que los usuarios han depositado en esta tecnología.

El *blockchain* ofrece transparencia (todos los participantes pueden ver la totalidad de la información contenida en la base de datos distribuida), compartición y descentralización (una misma copia de la base de datos en todos los nodos), irreversibilidad (una vez

[1] Red P2P (*peer-to-peer*) o 'red de pares' cuyos nodos se comportan como iguales entre sí, sin clientes o servidores fijos.

registrado un dato, no puede ser modificado o borrado) y desintermediación (sin árbitro central, los participantes toman las decisiones por consenso). La cadena de bloques enlaza la secuencia de transacciones e incorpora una marca de tiempo que da transparencia y trazabilidad a las operaciones sin por ello quebrantar *a priori* la privacidad de los usuarios (puede conocerse el camino[2] y el contenido aunque no siempre sea factible inferir la identidad del usuario). Los actores pueden adoptar tres roles: usuarios con derecho a tener y consultar una copia de la base de datos distribuida (*accessors*), participantes con derecho a realizar transacciones (*participants*) y usuarios encargados de validar las transacciones y crear bloques (*miners*). Todos ellos disponen de una copia validada y única de la base de datos.

Cada plataforma establece sus reglas de participación, operación y gobernanza. Las plataformas pueden ser abiertas (públicas) si son accesibles sin restricciones (*permissionless ledgers*), como, por ejemplo, la criptomoneda Bitcoin. Son semipúblicas o autorizadas (*permissioned ledgers*) cuando se condicionan la participación, el derecho a veto de nuevos miembros o la posibilidad de decidir el protocolo de consenso al inicio de la cadena. También pueden ser privadas cuando un actor establece las reglas; en este caso, se desdibuja la diferencia entre una cadena de bloques y un base de datos descentralizada convencional.

El *blockchain* emplea mecanismos criptográficos de seguridad para acceder, firmar y cifrar las transacciones, los bloques y su encadenado. Las claves privadas pueden estar vinculadas a la identidad de los usuarios o a elementos intermedios; por ejemplo, las carteras digitales con las que la plataforma ofrece el anonimato de las operaciones. Las reglas que ejecutan las transacciones pueden estar establecidas mediante contratos inteligentes[3]; en el *blockchain* Ethereum, por ejemplo, aseguran un entendimiento común de la transacción entre las partes, en particular sobre las obligaciones contraídas, ofreciendo una visibilidad probatoria limitada a los interesados (las terceras partes del *blockchain* ajenas al contrato no tienen acceso a sus estipulaciones o a su cumplimiento).

Determinados nodos de la red se especializan en validar la transacción y escribirla cifrada en el bloque, encadenándolo a los preexistentes una vez completado. Antes de que un nuevo bloque pueda ser agregado a la cadena, su autenticidad ha de ser verificada por un proceso de validación por consenso. El mecanismo de consenso asegura que todas las copias del libro distribuido comparten el mismo estado. Validada la transacción, los nodos “mineros” actualizan la base de datos distribuida mediante la agregación de la transacción al bloque de transacciones en curso (todavía no está definitivamente registrado); cuando este bloque alcanza un número dado de transacciones validadas, los “mineros” proceden a sellarlo e incorporarlo a la cadena, quedando estas transacciones registradas permanentemente.

[2] Determinadas criptomonedas (por ejemplo, *monero*) ofrecen también intrazabilidad.

[3] Los *smart contracts* son contratos cuyas estipulaciones se programan informáticamente para que se puedan ejecutar de forma automática cuando se cumplan las condiciones programadas.

Los nodos mineros utilizan algoritmos matemáticos para convertir la información de un bloque en un código alfanumérico o *hash* que enlace al *hash* del bloque anterior y encadenar los bloques entre sí. Por cada bloque añadido a la cadena, el nodo minero percibe una remuneración en criptomonedas o una participación en el negocio objeto de la transacción; una vez agregado un bloque, éste es inmutable. La participación de los nodos mineros sigue las reglas definidas por cada plataforma relativas al mecanismo de consenso, el cual determina en gran medida la seguridad, fiabilidad, velocidad y coste computacional y energético del proceso.

Los retos tecnológicos

La complejidad, la velocidad de crecimiento, la proliferación de un gran número de plataformas distintas o su alto potencial de negocio dificultan la resolución de retos tecnológicos significativos tales como la escalabilidad, la estandarización o la interoperabilidad, aspectos estos de especial incidencia en la seguridad.

La necesidad de escalabilidad se ve acentuada por el crecimiento exponencial de las principales plataformas públicas (por ejemplo, Bitcoin creció el 450% entre julio de 2012 y julio de 2016). A medida que la red crece, aumenta la competencia para realizar las validaciones, se tarda más tiempo y se incrementa el coste unitario por transacción. Por consiguiente, son necesarios nuevos mecanismos de consenso que reduzcan el tiempo de procesamiento sin comprometer la seguridad.

La necesidad de interoperabilidad se acentúa dadas la proliferación de distintas soluciones y la necesidad de compartir datos entre plataformas o de utilizar monederos electrónicos comunes. El intercambio de datos exige la traducción entre protocolos y la conciliación de distintos mecanismos de consenso, que se ve dificultado por la ausencia de estándares. Más allá de los aspectos técnicos, la interoperabilidad entre plataformas habrá de dar respuesta también a necesidades tales como la facilidad de uso de las aplicaciones y la capacidad para transferir activos, limitar el volumen de transacciones, impedirlas o establecer salvaguardas ante cambios de propiedad fraudulentos.

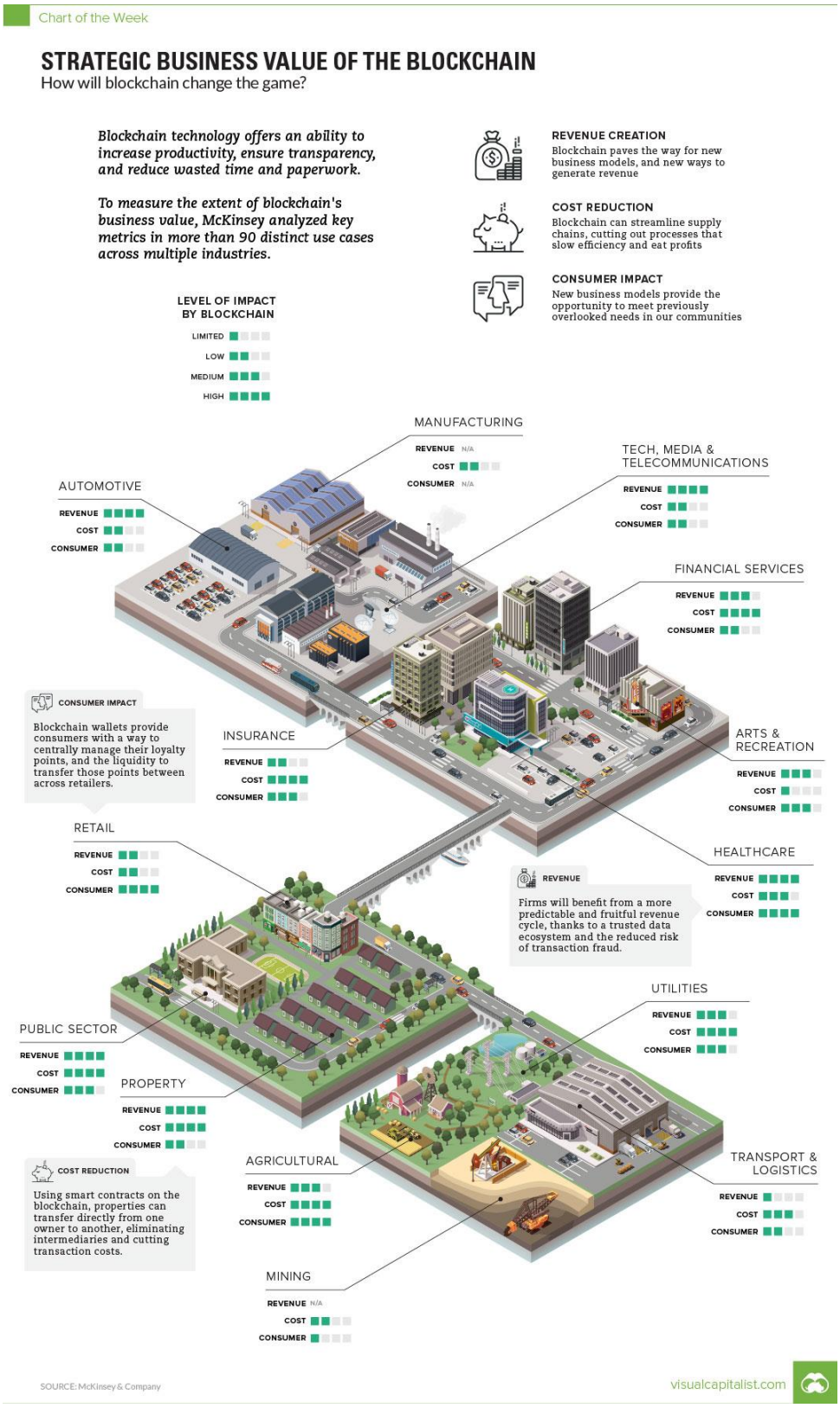
Un reto tecnológico en permanente debate es la eficiencia energética, dado el elevado consumo intrínseco al *blockchain* y el significativo coste oculto vinculado a los mecanismos de consenso para la validación y cálculo de bloques realizados por los nodos mineros. Estos factores guardan una relación directa con el impacto medioambiental[4] y determinan la necesidad de protocolos de validación más eficientes y seguros que faciliten la participación en la plataforma *blockchain* de dispositivos autónomos de limitado consumo, por ejemplo, IIoT en el ámbito industrial.

[4] Christian Stoll, Lena Kaarssen y Ulrich Gallersdörfer, “The Carbon Footprint of Bitcoin”, MIT Working Paper 18, 2018, http://ceepr.mit.edu/files/papers/2018-018.pdf.

Blockchain, más allá de las criptomonedas

Existen infinidad de aplicaciones de *blockchain* actualmente en desarrollo con usos distintos a las criptomonedas en la práctica totalidad de los sectores, lo cual evidencia la transversalidad de esta tecnología, según se refleja en la figura 1. A título de ejemplo, cabe citar el sector financiero (transacciones bancarias entre entidades, medios de pago, pólizas de seguros), el logístico (trazabilidad y gestión de las mercancías), el energético (integración de medios de generación a la red eléctrica), el sanitario y farmacéutico (historiales, gestión médica, trazado de medicamentos), la industria audiovisual (gestión de los derechos a través de la cadena de valor de la obra), el turismo (gestión de reservas, contrataciones, tarifas, acciones de fidelización, gestión de la identidad, seguimiento de equipajes), la industria 4.0 (construcción de comunicaciones seguras en las redes industriales mediante el registro actualizado en tiempo real de los dispositivos IIoT fiables integrados a la red operaciones) o la Administración Pública (gestión de licencias, transacciones, eventos, movimiento de recursos y pagos, gestión de propiedades, gestión de identidades).

Figura 1. Oportunidades estratégicas para el *blockchain*



Fuente: Jenny Scribani, "The Business Value of the Blockchain", *Visual Capitalist*, 30/XI/2018, https://www.visualcapitalist.com/business-value-blockchain/.

Cabe señalar la aplicación del *blockchain* en el ámbito de la identidad digital como sistema para validar identidades de forma irrefutable, segura e inmutable, lo que permitiría a los ciudadanos el control del uso de sus datos por terceros. En el ámbito jurídico y regulatorio, esta tecnología permite trazar el cumplimiento de obligaciones contractuales y normativas, por ejemplo para evidenciar ante el regulador el cumplimiento de las obligaciones de los controladores de datos en el marco del Reglamento General de Protección de Datos (RGPD). En cada sector y empresa, la proliferación de plataformas *blockchain* tendrá importantes implicaciones económicas (inversión, escala mínima, economías de escala), organizativas (incorporación al diseño de los departamentos de ciberseguridad, cumplimiento y responsables de privacidad) y de gobernanza, así como formativas al ser una tecnología compleja y de uso transversal. En este sentido, el rol de las autoridades públicas y la colaboración público-privada desempeñan un papel clave, tal como evidencian las iniciativas de la Comisión Europea, el Gobierno, las Autonomías o el sector privado con ejemplos como Alastria o entornos de colaboración y supervisión conjunta público-privada con las autoridades regulatorias (*regulatory sandboxing*).

La seguridad del *blockchain*

El *blockchain* es una tecnología conceptualmente segura gracias a su naturaleza distribuida, la irreversibilidad de las transacciones y el uso intensivo de cifrado. Las vulnerabilidades surgen habitualmente como resultado de la implementación de las plataformas y aplicaciones, es decir, se vinculan al desarrollo del código informático, de los protocolos de comunicación o de la simplificación de los mecanismos de validación y consenso de los bloques.

El *blockchain* es una tecnología reciente y compleja. A pesar de un diseño y revisión exhaustivos del código, no pueden excluirse las vulnerabilidades a consecuencia de errores de programación. Identificadas éstas, resultan especialmente complicadas de parchear sin afectar al servicio debido a la arquitectura distribuida y la inmutabilidad de la cadena de bloques. Las vulnerabilidades se ven acentuadas por la multiplicidad de lenguajes de programación y protocolos, esto es, por la ausencia de estándares tecnológicos. Esta fragmentación ralentiza la curva de madurez de esta tecnología, reduce las posibilidades de detección de errores y de implantación de controles sobre el código y dispersa la experiencia de los desarrolladores, sometidos a una presión constante para acortar los tiempos de entrega.

Asimismo, la integración de las plataformas de *blockchain* con los sistemas de información que apoyan los procesos de negocio de la empresa o la interoperabilidad entre distintas plataformas de cadenas de bloques es todavía muy incipiente, lo cual limita la eficiencia e incrementa los riesgos de ciberseguridad. Puede tardarse años en alcanzar un grado de madurez y consenso técnico que facilite la convergencia de estándares de seguridad y la interoperabilidad entre plataformas. Por consiguiente, desarrolladores y empresas han de incorporar ineludiblemente metodologías de seguridad por diseño desde las primeras fases de desarrollo contando con la participación de los departamentos de sistemas de información y ciberseguridad.

Las plataformas, servicios y redes comparten riesgos de seguridad con las tecnologías de la información, tales como los de confidencialidad, privacidad, gestión de claves, criptografía, identificación y parcheado de vulnerabilidades o concienciación ante amenazas de ingeniería social. Pero además ofrecen riesgos específicos:

- secuestro del mecanismo de consenso mediante la coalición de usuarios (*51% attack*) o adquisición puntual de gran capacidad de computación en la nube con el fin de alterar la validación (por ejemplo, denegando transacciones o reasignando un activo ya gastado);

- minado de cadenas laterales o paralelas (*sidechains*[5]) al contar con menos capacidad de minería o ante la posibilidad de ataques que puedan bloquear una cadena lateral y revertir la carga transaccional sobrecargando el *blockchain* raíz;
- ataques de denegación de servicio distribuidos mediante la inyección de un alto número de transacciones *spam* (vulnerabilidad acentuada ante la posibilidad de almacenamiento en el *blockchain* de datos y algoritmos);

- ataques centrados en las capacidades de la entidad gestora (única) de un *blockchain* autorizado (*permissioned*).

A medida que aumenta el número de bloques de una cadena, los nodos mineros tienden a agruparse (*pools*), ya que disminuye la posibilidad de que un nodo individual selle un bloque y obtenga la recompensa. Esta concentración puede plantear vulnerabilidades de cara a obtener un consenso fiable si la preponderancia de unos pocos *pools* es dominante en la plataforma.

En relación con el empleo generalizado de *smart contracts* para llevar a cabo transacciones, éstos se ven expuestos a los errores y vulnerabilidades –más probables en la medida en la que los *smart contracts* son más complejos– derivados de su codificación y de los de la plataforma de cadena de datos en la que se ejecutan[6]. Además de errores de programación, las tecnologías *blockchain* se enfrentan a riesgos que tienen que ver con las técnicas criptográficas que aseguran la confidencialidad y la integridad del registro de las transacciones, tales como la custodia de las claves de acceso del usuario, el alojamiento de los monederos[7] o la hipotética ruptura de algoritmos criptográficos mediante computación cuántica en un futuro.

[5] Las cadenas *de bloques* laterales son piezas de *software* conectadas a la cadena de bloques que se emplean para ejecutar determinadas aplicaciones en la plataforma y evitar que la saturación de una cadena afecte al *blockchain* en su totalidad. Asimismo, facilita añadir funcionalidades al *blockchain* a través de una cadena de bloques lateral que, una vez validada, se incorpora al *blockchain* principal.

[6] David Arroyo, Álvaro Rezola y Luis Hernández, "Principales problemas de seguridad en los *smart contracts* de Ethereum", XII Jornadas STIC CCN-CERT, diciembre de 2018, https://www.ccn-cert.cni.es/pdf/documentos-publicos/xii-jornadas-stic-ccn-cert/3422-m22-02-smart-contracts-ethereum/file.html.

[7] El programa que implementa la función de monedero electrónico en el equipo del usuario debe proteger las claves durante la operación y en su almacenamiento y evitar accesos no autorizados, ya que, en caso de sustracción, sería imposible revertir las transacciones fraudulentas realizadas durante el intervalo de tiempo en que la situación pase inadvertida.

(cont.)

La Agencia Europea de Seguridad de las Redes y de la Información (ENISA, por sus siglas en inglés) proporciona recomendaciones pormenorizadas y buenas prácticas para afrontar las amenazas y retos reseñados[8]. La mayoría de los incidentes registrados no están directamente vinculados al diseño conceptualmente seguro del *blockchain*. Por consiguiente, se debería partir de la base de que las plataformas *blockchain* se ven expuestas a riesgos de ciberseguridad y operativos similares a los de cualquier sistema de información, tal como evidencian numerosos ciberincidentes de gran impacto para los clientes, como los contenidos en el "Informe de Amenazas contra *blockchain* 2018" de McAfee o el informe de CipherTrace que analiza la actividad delictiva en el mercado de las criptomonedas.

A continuación se hace referencia a algunos incidentes a título de ejemplo:

- En agosto de 2010, un *hacker* generó 184.467 millones de *bitcoins* en una transacción utilizando una vulnerabilidad del código conocida como "incidente por desbordamiento de valor", solucionada al cabo de horas.

- En enero de 2018, Coincheck, uno de los operadores de cambio más populares de Japón, perdió 532 millones de dólares en monedas NEM, lo que afectó a 260.000 inversores. Un ciberdelincuente había accedido al ordenador de un empleado e instalado *malware* para obtener claves de los monederos digitales utilizados en transacciones *online* inmediatas (*hot wallet*) y vaciar las cuentas.

- En marzo de 2018, *Schneier on Security* se hizo eco de las vulnerabilidades de los *smart contracts* de plataformas *blockchain* como Ethereum[9].

- En mayo de 2019, la plataforma Binance sufrió el robo de 41 millones de dólares en *bitcoins*. Los *hackers* utilizaron varias técnicas, desde virus hasta *phishing*, para introducirse en el sistema y acceder a una cartera de *bitcoins* de la compañía desde la que sus clientes realizaban transacciones.

- En 2019 el fallecimiento del CEO de un fondo de gestión de criptoactivos provocó la desaparición de las credenciales para acceder a las criptomonedas que administraba, por valor superior a 150 millones de dólares, que se volvieron irrecuperables.

Resulta significativa la gran variedad de incidentes ajenos al diseño conceptual del *blockchain*, así como el fuerte crecimiento de delitos denunciados: las criptomonedas sustraídas de sitios de intercambios y estafadas a inversores aumentaron más de un 400% en 2018, alcanzando alrededor de 1.700 millones de dólares al cambio. De los 1.700 millones de dólares, 950 millones constituían robos a servicios de intercambio de

[8] Enisa, "Distributed Ledger Technology & Cybersecurity. Improving information security in the financial sector", 18 de enero de 2017.

[9] Nicholic et ál., "Finding the Greedy, Prodigal and Suicidal Contracts at Scale", 14/III/2018, https://arxiv.org/pdf/1802.06038.pdf; y P. Vessenes, "Ethereum Contracts are Going to be Candy for Hackers", 18/V/2016, https://vessenes.com/ethereum-contracts-are-going-to-be-candy-for-hackers/.

criptomonedas e infraestructura, como carteras, lo que representa un aumento de casi el 260% frente a los 266 millones de dólares robados en 2017 (Corea del Sur y Japón acaparan el 58% de los robos de sitios de intercambios).

Llegados a este punto, es importante reiterar la importancia de cuidar los aspectos no tecnológicos derivados de incorporar una plataforma *blockchain* a los procesos de negocio u operaciones, en particular los relativos a los impactos organizativos y de procesos de negocio. Por ejemplo, el departamento de seguridad de la información de la compañía habrá de participar en el diseño de la solución desde su inicio, así como en la implantación, al igual que con cualquier otra plataforma tecnológica.

En un ámbito distinto, la creciente aceptación y el anonimato que caracterizan las transacciones de las nuevas criptodivisas han propiciado el *cryptojacking* o uso ilegítimo por cibercriminales de la capacidad de procesamiento de equipos informáticos ajenos al *blockchain* para la obtención fraudulenta de criptomonedas. El *cryptojacking* detrae recursos (computacionales, de memoria, energéticos) del equipo del usuario afectado para apropiarse de activos de una plataforma *blockchain*. Se estima[10] que en enero de 2018 el número de muestras de este tipo de código dañino rondaba los 94.000, mientras que sólo tres meses más tarde esta cifra llegó a incrementarse un 74%.

El diseño de la privacidad

El *blockchain* plantea nuevas y complejas cuestiones en torno a la protección de los derechos de la privacidad en el uso de datos de carácter personal y en particular en la aplicación del RGPD cuando las transacciones gestionan datos de carácter personal o bien la información de los bloques hace referencia a datos de carácter personal de los participantes[11.]

Características tales como la descentralización del procesado y del almacenamiento de los datos dificultan la interpretación del Reglamento. Las autoridades nacionales de regulación e instituciones europeas promueven el análisis regulatorio y emiten directrices e informes que son referencia obligada para desarrolladores. En este ámbito hay que mencionar la contribución del Observatorio y Foro sobre Blockchain de la UE (EU Blockchain Observatory and Forum).

Es importante indicar que el RGPD no evalúa una tecnología en materia de privacidad, sino la manera en que la utilizan los distintos casos de uso y aplicaciones. Por consiguiente, es ineludible iniciar todo diseño de una plataforma o aplicación *blockchain* realizando un exhaustivo análisis sobre los impactos en privacidad, evaluando la conveniencia de adoptar soluciones alternativas al *blockchain* más apropiadas o la necesidad y proporcionalidad de las opciones de diseño que se hayan elegido. Por ejemplo, habrá de evaluarse la conveniencia de utilizar un *blockchain* público, ya que los autorizados y privados plantean menores dificultades regulatorias (por ejemplo, en

[10] Informe CCN-CERT IA-25/18 sobre *cryptojacking*, septiembre de 2018, pág. 4, https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/3027-ccn-cert-ia-25-18-cryptojacking/file.html.

[11] Michèle Finck, “Blockchain and data protection in the EU”, *EDPL* 1, 2018, https://edpl.lexxion.eu/data/article/12327/pdf/edpl_2018_01-007.pdf.

los *blockchain* públicos todo usuario puede trazar las transacciones de origen a destino o descargarse el libro de registro, lo que dificulta el ejercicio del derecho al olvido o de rectificación). Igualmente sensible es el uso de contratos inteligentes que puedan ser origen de fugas de datos de carácter personal.

Un *blockchain* puede contener dos categorías de datos personales: los que permiten la identificación de emisor y receptor de la transacción mediante claves públicas y la información incluida en la transacción relacionada con terceras personas. A partir de esta distinción es de aplicación la metodología de análisis del RGPD (identificación del controlador de los datos, derechos y salvaguardas, gestión de riesgos, etc.). A grandes rasgos, las tensiones regulatorias sobre el RGPD que capitalizan el debate entre autoridades y desarrolladores giran en torno a la identificación de los roles de controlador y de procesador de los datos o qué implicaciones tiene que varios participantes decidan procesar las transacciones conjuntamente junto a las obligaciones derivadas, a la anonimización de los datos de carácter personal y al ejercicio de derechos tales como la rectificación, el borrado, derecho al olvido, la objeción al tratamiento o la portabilidad de datos de carácter personal. Asimismo, el diseño debe prestar especial atención a las obligaciones derivadas de la subcontratación o a las reglas de gobernanza en la transferencia internacional de datos, en particular entre *blockchain* públicos.

En este sentido, el Observatorio y Foro sobre Blockchain de la UE indica a los desarrolladores cuatro directrices de aplicación general:

- Iniciar el diseño a alto nivel evitando que el *blockchain* se convierta en una solución innovadora en busca de problema: ¿cuál es la aportación de valor de la solución para el usuario? ¿Es realmente necesaria una plataforma *blockchain*? ¿Cómo gestionar los datos?

- Evitar almacenar datos de carácter personal en el *blockchain*; utilizar técnicas de ofuscación, cifrado y agregación para anonimizar estos datos.
- Mantener los datos personales fuera de los bloques siempre que sea posible o utilizar *blockchain* autorizado o privado; analizar la transferencia de datos de carácter personal al conectar *blockchain* privados con públicos.

- Ofrecer total transparencia ante los usuarios sobre el tratamiento de los datos.

Conclusión

El *blockchain* es una de las tecnologías de la información más disruptivas, complejas e incipientes, cuyo vertiginoso crecimiento es transversal a todos los sectores de actividad del ámbito público y privado. Más allá de las criptomonedas, cuenta con enorme potencial como paradigma de la descentralización y empoderamiento de personas físicas y jurídicas, junto a no pocos retos regulatorios, jurisdiccionales y tecnológicos tales como la escalabilidad, la interoperabilidad o el impacto medioambiental.

El *blockchain* es una tecnología conceptualmente muy segura que se ve expuesta en el curso de su implementación a errores y vulnerabilidades propios de cualquier sistema

de información, añadidos a los específicos de esta tecnología. A esto se suman los retos de seguridad, interoperabilidad y tecnológicos derivados de su progresiva madurez, complejidad, falta de estandarización y diversidad de protocolos, a los que se superponen las exigencias propias de un vibrante entorno competitivo.

El alineamiento con la regulación del RGPD en este ámbito es una labor compleja y abierta a estudio con el necesario apoyo de las autoridades regulatorias. Ha de ofrecer respuesta, entre otros aspectos, a la identificación de los roles de controlador y de procesador de los datos, la anonimización, el ejercicio de derechos tales como la rectificación, el borrado, derecho al olvido, la objeción al tratamiento o la portabilidad, las obligaciones derivadas de la subcontratación o la transferencia internacional de datos.

En consecuencia, la aplicación de los principios de la seguridad y la privacidad por diseño son ineludibles desde las fases iniciales del diseño junto a consideraciones resultado de integrar la plataforma *blockchain* a los procesos de negocio u operaciones, como los impactos en la organización y en los procesos de negocio. Afrontar estos retos exige la constitución de equipos multidisciplinares que cuenten con la participación desde el inicio del área jurídica/regulatoria, de ciberseguridad y de sistemas de información de las empresas.