El difícil equilibrio entre riesgo y oportunidad en el contexto blockchain

David Arroyo Guardeño // Grupo de investigación en Criptología y Seguridad de la Información.
Instituto de Tecnologías Físicas y de la Información.
Consejo Superior de Investigaciones Científicas (CSIC)

Las tecnologías de registro distribuido (DLT), cuya expresión más conocida es la *blockchain*, se han ido postulando como la solución a un grueso muy significativo de los grandes problemas del espacio cibernético. Los casos de aplicación más conocidos abarcan la digitalización del dinero (criptomonedas y otro tipo de criptoactivos), el seguimiento de productos y mercancía en cadenas de suministros (como realiza el sistema Tradelens de IBM y Moller-Maerks para la logística de contenedores de mercancía), la notarización de títulos académicos (e.g., los sistemas desplegados por parte de algunas universidades españolas), certificados oficiales u otros documentos (donde encontramos Stampery o Guardtime).

Si bien en su origen *blockchain* fue desplegándose al hilo de una suerte de corriente contracultural, lo cierto es que paulatinamente ha ido ganando terreno en el ámbito institucional. Así, es de especial relevancia la iniciativa The European Blockchain Services Infraestructure (EBSI), entre cuyos objetivos figura el impulso del estudio (y eventual implementación) de casos de usos de interés para *blockchain* y de relevancia para la ciudadanía europea. De esta forma, y en el tenor de la sentencia de Schopenhauer sobre la aceptación de "una nueva verdad", *blockchain* ha pasado del rechazo frontal tras su aparición, a la ridiculización por suponer una tecnología ineficiente (considérese el tono jocoso de los comentarios sobre la compra de dos pizzas por 10 000 bitcoins en 2010), a recibir el apoyo de una institución como la Comisión Europea.

A pesar del entusiasmo en su adopción, las DLTs presentan una serie de limitaciones y disfuncionalidades que pueden poner en riesgo la sostenibilidad del ecosistema digital. En muchas ocasiones se confunde el uso de DLT como un medio al servicio de la resolución de un problema, con su adopción como fin en sí mismo. Son múltiples los casos de aplicación de DLT que llevan a forzar determinadas asunciones y requisitos sobre el contexto de operación. El estado de desarrollo de la tecnología DLT hace que, al ser aplicada en problemas complejos, acabe convirtiéndose en parte del problema sin aportar una ventaja objetiva sobre planteamientos tecnológicos previos, maduros y ampliamente adoptados en la industria. Es más, el uso de tecnologías que no garanticen una buena experiencia de usuario puede desembocar en su desprestigio y, finalmente, en el rechazo por parte de sus potenciales receptores. El no garantizar un despliegue de soluciones estables, escalables y robustas puede derivar en una quiebra de la confianza del ciudadano respecto a la tecnología. De ser así, nos encontraríamos en la situación paradójica de que la "máquina de la confianza" (como a veces se nombra a la DLT) no goza del crédito de sus potenciales usuarios.

¿Por qué entonces adoptamos DLT o deberíamos hacerlo? Una ventaja de estas tecnologías es que proporcionan un medio de almacenamiento de evidencias que es resistente frente posibles manipulaciones. En el caso de DLTs en las que no todos los usuarios pueden escribir y leer la información almacenada, el estudio pormenorizado de las características de ese medio de almacenamiento pone de relieve toda una metodología de control de acceso y de autorización cuya importancia se extiende muchos más allá de la misma DLT. Este medio permitiría revisar todo el conjunto de acciones efectuadas en un cierto entorno de colaboración, lo que facilitaría la puesta en marcha de procesos de auditoría, así como de procedimientos de depuración de responsabilidad.

Por otro lado, la aparición en su momento de Bitcoin permitió integrar todo eso conjunto de tecnologías en un producto de alto impacto y transcendencia social. La criptografía asimétrica y las funciones hash, combinadas con una red de comunicación entre pares, permiten generar un esquema colaborativo basado en una suerte de interés común tutelado por restricciones algorítmicas y de cómputo. Bitcoin, de este modo, consigue crear un marco de confianza algorítmico que permite eludir la necesidad de bancos centrales para el intercambio de dinero. Más tarde, con la aparición de Ethereum, surge la primera concreción con éxito de los denominados contratos inteligentes o *smart contracts*. Al margen de lo preciso de su consideración como contratos y su cualificación como inteligentes, los *smart contracts* permiten almacenar código ejecutable en una DLT, de forma que, si se dan ciertas condiciones,

dicho código (que es incorruptible gracias a la inviolabilidad del medio de persistencia representando por la DLT) se ejecuta automáticamente. Así, la ocurrencia de una serie de condiciones garantiza la ejecución de código *software* y la consiguiente acción sin que exista intervención humana.

La inviolabilidad de la DLT como medio de almacenamiento, así como la automatización de la toma de decisión mediante contratos inteligentes, en efecto, pueden constituirse en pilares de nuevos esquemas de gobernanza digital. Pero ello ha de llevarse a término teniendo en cuenta que tal gobernanza no surge única y exclusivamente de la absorción de toda modalidad de gobernanza en términos de gobernanza algorítmica. Dicho de otro modo, y yendo más allá –o más acá– de Lawrence Lessig, conviene evitar los cantos de sirena del pensamiento analógico, y no caer en la tentación de asumir acríticamente isomorfismos entre código *software* y código normativo/jurídico. Hemos de tener bien presente que pueden darse circunstancias contingentes que, por ejemplo, obliguen a modificar la inmutabilidad de una *blockchain* o una DLT para resolver algún problema (como ocurrió en 2016 con TheDao). En estas coyunturas ha de existir un marco de gobernanza corporativo, institucional o social que defina de modo claro y evidente el tipo de decisiones a tomar, así como los responsables de las mismas. Estas reglas han de ser conocidas por un conjunto representativo de los actores de un ecosistema DLT, ya que lo contrario erosionaría el supuesto espíritu de transparencia de esta tecnología. Es más, esas reglas deben determinar el marco de restricciones para consensuar la escritura de información en una DLT. Este marco demanda la correcta formalización de los distintos algoritmos de consenso y los protocolos de comunicación correspondientes.

Por otro lado, la gobernanza algorítmica determinada por la DLT es muy dependiente de la fiabilidad de sus protocolos y procesos. Como todo *software*, los contratos inteligentes tienen vulnerabilidades que deben ser debidamente contempladas, de acuerdo con modelos de atacante suficientemente precisos, y con vistas a acercarse al principio maximalista de "seguridad por diseño y por defecto". Y no solo seguridad y robustez, sino que también se debe proteger el acceso a datos personales sensibles cuya explotación por parte de terceros puede implicar fallas de privacidad. Los criterios maximalistas (derecho al olvido, minimización de datos, seguridad por defecto, etc.) deben ser debidamente dimensionados de acuerdo con las posibilidades de la tecnología, las necesidades del ámbito de aplicación y perceptivas restricciones legales o normativas. Soluciones avanzadas de criptografía pueden contribuir a minimizar el volumen de datos a compartir en procesos de verificación de contenido, así como a reforzar la protección de la identidad mediante modalidades adecuadas de anonimato que hagan factible tanto la detección de abusos en la utilización de la tecnología, como su personalización para cada tipo de usuario de cara a desplegar estrategias de fidelización.

La inviolabilidad de la DLT como medio de almacenamiento, así como la automatización de la toma de decisión mediante contratos inteligentes, en efecto, pueden constituirse en pilares de nuevos esquemas de gobernanza digital

La contribución de la DLT y la *blockchain* a la gestión del ciberriesgo pasa por afrontar de modo exhaustivo sus riesgos tecnológicos y legales, lo que supone la puesta en marcha de una hoja de ruta con un *pathos* tecnológico y otro jurídico. Ambos deben articularse de modo solidario (tal que vasos comunicantes), de forma discursiva y con una fuerte componente pedagógica. Hace falta desarrollar *curricula* universitarios y de postgrado que abarquen comprehensivamente las disciplinas de la ingeniería criptográfica, las comunicaciones en sistemas asíncronos y las tecnologías de consenso y confianza digital. Al mismo tiempo, el derecho digital y las ciencias sociales y humanidades deben nutrirse de egresados universitarios con capacidad de innovar en el plano normativo-jurídico, en consonancia con las modalidades y ritmos ínsitos en la construcción del sujeto e instituciones sociales en el actual mundo ciberfísico. Unos y otros no deben olvidar que en el centro de sus esfuerzos y denuedos está el ser humano, ese ente *(Dasein)* que aspira a ser ciudadano y sin el cual las instituciones devienen en un esclerótico complejo institucional carente de la savia de lo instituyente. La aceptación institucional y por parte del público de la DLT se presenta, pues, como una gran oportunidad (una estancia de ese *Laboratorium* possibilis *Salutis* de Ernst Bloch) para emprender el diseño de una sólida estrategia en pos del ansiado caso de éxito en la gobernanza digital mediante la des-intermediación y la des-centralización de la configuración y toma de decisiones. ●