Oportunidades y desafíos de *blockchain* en el sector público de España

Existen diversas definiciones técnicas de *blockchain*, pero su utilidad práctica puede comprenderse mejor con un ejemplo de aplicación.

ALEXANDER ZLOTNIK

Imaginemos que queremos organizar una apuesta sobre el resultado de un partido de fútbol de manera presencial y en papel. Las reglas son sencillas: (i) todos los participantes realizan una apuesta monetaria ante una persona de confianza –el responsable del registro de apuestas–, que las apunta junto con la fecha y la hora en la que se han realizado; (ii) una vez celebrado el partido de futbol, el responsable del registro le entrega el premio a la persona que haya ganado la apuesta; (iii) si nadie acierta, se devuelve el dinero de las apuestas; (iv) si dos o más personas aciertan el resultado, el premio lo recibe la persona que haya hecho la apuesta primero; (v) el responsable del registro de apuestas hace una fotocopia del registro de apuestas y la distribuye a todos los participantes para que el proceso sea transparente.

El problema de este planteamiento es la confianza y la escalabilidad. Por ejemplo, el responsable del registro de apuestas podría apuntar algunas apuestas con fechas y horas equivocadas o quedarse con los fondos recaudados y no efectuar el pago al ganador. Asimismo, este esquema difícilmente puede extenderse a miles o millones de participantes, que no se conocen y que no confían unos en otros, ni en el responsable del registro de apuestas.

Un sistema *blockchain* permite resolver esta situación al sustituir el sistema centralizado del ejemplo anterior (responsable del registro de apuestas) por un sistema descentralizado basado en la confianza criptográfica, que se ejecuta de manera distribuida en varios nodos, con replicación de la información y resistencia a fallos. Así, un sistema *blockchain* podría registrar las apuestas de manera inalterable y transparente para todos los participantes (sustituyendo a la fotocopia del registro de apuestas). También sería capaz de reaccionar (realizar el pago al ganador) ante un evento del mundo exterior (el resultado del partido de fútbol) mediante la ejecución de un programa (o *smart contract*) que se ejecutaría sobre el sistema

blockchain. Además, sería un sistema escalable, dado que podrían participar en él millones de personas.

Tras este ejemplo podemos enumerar de una manera más formal las características principales de los sistemas *blockchain* actuales: (i) un registro de información inalterable; (ii) lógica de negocio contenida en *smart contracts*, que se ejecuta sobre el sistema *blockchain*, y que es capaz de responder a estímulos externos; (iii) un sistema redundante y computacionalmente distribuido, que seguiría en funcionamiento a pesar de la caída de algunos de los nodos conectados en red que componen el sistema *blockchain*.

Cabe destacar que estos sistemas presentan una serie de limitaciones. Para su comprensión es muy recomendable la lectura de la guía sobre tecnologías *blockchain* publicada recientemente por el *National Institute of Standards and Technology* (NIST) [1]. En primer lugar, la capacidad de almacenamiento es más limitada y la velocidad de las transacciones es más reducida que en un sistema de información centralizado conectado a una base de datos relacional. Por otra parte, la lógica de negocio contenida en los *smart contracts*, al ejecutarse sobre toda la red, imprime una carga computacional sobre todos los nodos. Por tanto, es necesario algún mecanismo que limite dicha carga computacional y garantice la disponibilidad del sistema. Una solución es el uso de sistemas *blockchain* en los que únicamente algunos nodos autorizados pueden participar en la red (leer y escribir información, así como ejecutar *smart contracts*). Este esquema se suele denominar *blockchain* privado o "permisionado" [2]. Si la red es más reducida y controlada, su funcionamiento es mucho más rápido y flexible que el de un *blockchain* público de gran tamaño (como Bitcoin o Ethereum), en el que cualquier participante puede efectuar operaciones de lectura y escritura. Por otra parte, el hecho de que la grabación de la información sea inalterable[1] puede generar dificultades operativas. Por ejemplo, el ejercicio del derecho al olvido y del derecho a la portabilidad de datos (artículos 17 y 20 del Reglamento UE 679/2016) imponen, en la práctica, la imposibilidad de grabación de datos personales sobre un sistema *blockchain*. Una posible solución es la grabación de pruebas criptográficas (p.ej. *hashes*[2]) con firmas electrónicas sobre *blockchain* y el almacenamiento de los propios datos en repositorios externos (almacenamiento *off-chain*). De esta manera, la verificación de autenticidad e integridad de dichos datos y documentos se podría seguir realizando sobre *blockchain*, sin comprometer su confidencialidad y portabilidad.

"Cabe destacar que en las Administraciones Públicas de España ya existen algunos pilotos de sistemas *blockchain* para la participación ciudadana y para la contratación pública. Desde el punto tecnológico, el uso de blockchain en estas aplicaciones no es imprescindible, pero tiene el potencial de aportar mayor transparencia y confianza."

En el caso de las aplicaciones al sector público es importante que realicemos un breve análisis jurídico en el ámbito del derecho administrativo. Desde una interpretación posibilista, los sistemas *blockchain* son compatibles con la legislación básica en materia de identificación y firma electrónica de ciudadanos en su actuación ante las administraciones públicas (artículos 9.2.c y 10.2.c de la Ley 39/2015) y de firma electrónica de empleados públicos (artículo 43.2 de la Ley 40/2015). Asimismo, los sistemas *blockchain* en general pueden considerarse compatibles con los requisitos de nivel bajo y medio de las medidas relativas a la identificación y firma electrónica establecidos en el Real Decreto 3/2010, por el que se regula el Esquema Nacional de Seguridad (epígrafe 5º de la medida [op.acc.1] y medida [mp.info.4] del Anexo II). Por otra parte, algunas arquitecturas *blockchain* pueden entrar en conflicto con ciertos conceptos de la Ley 40/2015 (tales como la sede electrónica del artículo 38) y del Esquema Nacional de Interoperabilidad definido en el Real Decreto

[1] Cabe destacar que, aunque en este artículo se he usado el término "registro inalterable", en realidad la mayor parte de los sistemas *blockchain* actuales son susceptibles de un ciberataque bastante sencillo en su concepción: si una única entidad controla más del 51% de la potencia computacional de la red, el registro de información y los *smart contracts* pueden ser falsificados por dicha entidad. Por ello, en todo sistema *blockchain* es esencial que exista un equilibrio de potencia computacional entre los nodos que controla cada una de las entidades que forman parte de un sistema *blockchain*.

[2] Siendo esencial asegurarse de la fortaleza criptográfica a largo plazo de los algoritmos empleados.

4/2010. Asimismo, podría ser necesaria la modificación de la legislación y normativa sectoriales para su adaptación a *blockchain*.

Cabe destacar que en las Administraciones Públicas de España ya existen algunos pilotos de sistemas *blockchain* para la participación ciudadana (p.ej. en el Ayuntamiento de Alcobendas [3]) y para la contratación pública (siendo relevante el proyecto de la Dirección General de Contratación, Patrimonio y organización del Gobierno de Aragón [4]). Desde el punto tecnológico, el uso de *blockchain* en estas aplicaciones no es imprescindible, pero tiene el potencial de aportar mayor transparencia y confianza.

Otra área de aplicación relevante son los registros de accesos a información sensible, tales que ni el propio administrador del sistema pueda alterarlos. Un ejemplo de sistema en producción es el registro de accesos a historias clínicas de Estonia [5]. Otros ejemplos potenciales son los registros de actuaciones realizadas sobre las listas de espera quirúrgica, de consultas y técnicas diagnósticas gestionadas por los servicios regionales de salud o los de accesos a la información tributaria. Asimismo, la idea de una lógica de negocio crítica (contenida en *smart contract*) que se ejecutara de manera distribuida sobre pequeños *blockchain* privados y fuera inalterable por virus o *malware* podría tener aplicaciones en el software de ciberseguridad, de infraestructuras críticas o del ámbito militar.

Por último, una de las aplicaciones potenciales más interesantes de *blockchain* en el sector público es la interoperabilidad de los sistemas de administración electrónica a nivel nacional e internacional [6]. Seguramente sea una visión a medio o largo plazo, dada la falta de madurez de la tecnología en algunos aspectos y debido a la existencia de desafíos jurídicos todavía por resolver. Sin embargo, podría establecerse un sistema *blockchain* privado con nodos distribuidos por las administraciones públicas de España y de la Unión Europea, en el que se definieran, mediante *smart contracts*, una serie de reglas de interoperabilidad e intermediación de datos de ciudadanos. Un sistema así podría simplificar notablemente los procesos de verificación y reconocimiento mutuo de datos y documentos en poder de las distintas administraciones públicas, además de ofrecer amplias garantías de disponibilidad y trazabilidad, sin que existiera dependencia de una entidad central.

En definitiva, a pesar de las limitaciones enunciadas, el uso de los sistemas *blockchain* ya es posible en las Administraciones Públicas de España, existiendo varios proyectos en fase de pruebas y diversas aplicaciones potenciales futuras. ✱

Bibliografía

[1] D. Yaga, P. Mell, N. Roby, and K. Scarfone, "NISTIR 8202. Blockchain Technology Overview." ed: National Institute of Standards and Technology, 2018.

[2] P. Jayachandran. (2017). *The difference between public and private blockchain,* URL: https://www.ibm.com/blogs/blockchain/2017/05/the-difference-between-public-and-private-blockchain/

[3] M. Sierra. (2017). *Un ayuntamiento español permitirá a sus ciudadanos votar con 'blockchain',* URL: https://www.clubdeinnovacion.es/ayuntamiento-espanol-permitira-ciudadanos-votar-blockchain/

[4] (2018). *El Gobierno de Aragón impulsará un proyecto de contratación pública utilizando 'blockchain',* URL: http://aragonhoy.aragon.es/index.php/mod.noticias/mem.detalle/id.216059

[5] (2018). *e-Estonia -- e-Health Records,* URL: https://e-estonia.com/solutions/healthcare/e-health-record/

[6] P. Marchionni, "Next Generation Government Service Bus-The Blockchain Landscape", 2018.