

BLOCKCHAIN EN EL SECTOR PÚBLICO, UNA PERSPECTIVA INTERNACIONAL

BLOCKCHAIN IN PUBLIC SECTOR, AN INTERNATIONAL VIEW

Magdalena Cordero Valdavidá

Directora de Información, Entorno de Trabajo
e Innovación
Tribunal de Cuentas Europeo*
Magdalena.cordero@eca.europa.eu

Recibido: 05/03/2019

Aceptado: 11/04/2019

© 2019 IVAP. Este es un artículo de acceso abierto distribuido bajo los términos de la licencia Creative Commons Reconocimiento – NoComercial – SinObráDerivada (by-nc-nd)



Laburpena: Eraldaketa digitalak, besteren artean Interneten iraultzarekin sustatu denak, arriskuarekin zerikusia duten automatizazio- eta efizientzia-aukera berriak eskaintzen ditu; segurtasunaren eta elkarreragingarritasunaren ingurukoak, adibidez. Bloke-katearen (blockchain) teknologia disruptiboa eta berritzailea da, eta sektore publikoko arduradunen arreta atzeman du, zerbitzu berriak sortzeko eta daudenak hobetzen laguntzeko gaitasuna baitu, gardentasuna areagotzearekin eta herritarren konfiantzari eustearekin bat. Artikulu honetan, teknologia horren sarrera egiten da, teknologia horrek sektore publikoan dituen ezarpenak azaltzen dira, Europar Batasunaren ekimenak kontatzen dira, eta Europako Kontuen Auzitegiaren adibide zehatz bat aurkezten da.

Gako-hitzak: *bloke-katea, erregistro banatuetaarako teknologia, kriptotxanponak, adimendun kontratuak, gobernu irekia, administrazio elektronikoa, blockchain-a, gardentasuna.*

Resumen: La transformación digital, impulsada entre otras cosas por la revolución de internet, ofrece nuevas oportunidades de automatización y eficiencia que van unidas a riesgos, como la seguridad, o la interoperabilidad. La tecnología de cadena de bloques (*blockchain*), de naturaleza disruptiva e innovadora, ha captado la atención de los responsables del sector público por su capacidad de generar nuevos servicios, y de contribuir a mejorar los existentes, aumentando la transparencia y manteniendo la confianza de los ciudadanos. Este artículo introduce la tecnología, describe sus aplicaciones en el sector público, relata las iniciativas de la Unión Europea y presenta un ejemplo concreto del Tribunal de Cuentas Europeo.

Palabras clave: *cadena de bloques, tecnología de registros distribuidos, cripto-monedas, contratos inteligentes, gobierno abierto, administración electrónica, transparencia.*

Abstract: The digital transformation, driven by, amongst other things, the Internet revolution, offers new opportunities for automation and efficiency that go together with risks such as security and interoperability. The disruptive and innovative nature of *Blockchain* technology has not been overlooked by the public sector decision-makers for its ability to generate new services and to contribute to improving existing ones, increasing security, transparency and maintaining the confidence of citizens. This article introduces the technology, describes its applications in the public sector, explains the initiatives at the European Union level and presents a use case of the European Court of Auditors.

Keywords: *blockchain, distributed ledger technology, crypto-currencies, smart contracts, open government, electronic administration, transparency.*

* Este texto expresa la opinión personal de la autora y no la del Tribunal de Cuentas Europeo.

Sumario

1. Introducción.—2. La administración pública y la transformación digital.—3. Descripción de la cadena de bloques, tipos y propiedades.—4. Principales casos de aplicación en el sector público.—5. *Blockchain* y el esfuerzo de liderazgo de la Unión Europea.—6. Panorama internacional y desarrollos en España en el sector público.—7. La experiencia del Tribunal de Cuentas Europeo.—8. Metodología para el desarrollo del *blockchain*.—9. Consideraciones finales.—10. Referencias

1. Introducción

El mundo está cambiando muy rápidamente y una gran parte de este cambio se debe a la presencia de las tecnologías de la información que han tenido una radical influencia en cómo nos comunicamos y gestionamos los procesos. La digitalización ha llegado a nuestras vidas cambiando la forma en que vivimos y trabajamos.

Para el sector público en particular, este momento entraña tanto un gran reto como una gran oportunidad. Por un lado, las administraciones públicas sufren más y más presiones de transformación ya que son responsables de múltiples tareas: implementar las políticas, ofrecer nuevos servicios, recaudar impuestos, proteger a los ciudadanos, empresas y otras agencias gubernamentales. Por otro lado, se les exige mayor transparencia, agilidad y apertura para facilitar la participación ciudadana en los procesos. Y todo esto haciendo frente a restricciones presupuestarias constantes, y con continuas exigencias de rapidez de reacción.

Hasta ahora, la solución ha consistido en implementar herramientas basadas en tecnologías de la información que han permitido desarrollar lo que se ha conocido como gobierno electrónico y/o administración electrónica. Este cambio, significativo, ofrece posibilidades de ser más eficientes, pero también comporta riesgos relacionados con la capacidad de transformar los servicios mientras hay que controlar el coste, justificar un buen ratio calidad-precio, garantizar el éxito y la aceptación del nuevo servicio generado, con medidas estrictas para proteger la información, asegurar el cumplimiento de legislación. Y todo ello con el problema, si bien cada vez menor, de la brecha digital.

Este proceso se ha visto amplificado gracias a la revolución de internet, que ha pasado en un tiempo récord

de ser un lugar de consumo de información a ser el sitio donde realizamos muchas de las tareas de nuestra vida cotidiana. Esta evolución hace que internet se esté reinventando para que podamos compartir y hacer negocios de forma segura y fiable. Para ello es necesario un estándar que permita a todas las industrias y a la comunidad de desarrolladores trabajar con una misma base. La potencia de internet en el mercado digital necesita de una capa de seguridad que «proteja» la red.

Por otro lado, el enorme y exponencialmente creciente número de datos disponibles nos enfrenta a otros problemas: los sesgos, las conclusiones erróneas, las noticias falsas y la pos-verdad. Por ello, identificar y evaluar las fuentes de información es crucial, convirtiéndose en un proceso clave la determinación de su grado de fiabilidad, señalando hasta qué punto son de confianza.

Las administraciones públicas han tenido siempre el papel, entre otros, de almacenar y custodiar información fiable acerca de los individuos, las organizaciones, los activos, y las actividades. Los distintos organismos tienen tendencia a almacenar su información en silos, fijar sus propios procedimientos de gestión «protegiendo» la información e impidiendo a otros organismos su uso. En muchos casos, el tradicional modelo de los ficheros de papel se ha reproducido en las redes informáticas.

Muchos de los datos producidos por las administraciones se convierten en datos públicos, publicados en sus páginas de internet, o alimentando fuentes de datos abiertos. En esos datos hay que confiar, pero estos repositorios no están exentos de ataques para manipular la información, tanto por agentes externos como desde dentro, debido a las demandas de transparencia cada día más exigentes¹.

La crisis de la calidad de los datos va acompañada de la oportunidad de crear nuevos sistemas basados en la confianza.

En este contexto, no es de extrañar que la cadena de bloques o «*blockchain*», considerada por algunos autores como una de las tecnologías más disruptivas desde la llegada de internet, se haya colado en la agenda de los administradores públicos. Hay varias razones para esto. Primero, es una tecnología que se caracteriza por generar **confianza** en la información y los procesos en circunstancias donde el número de actores, o usuarios, es grande y heterogéneo. Segundo, *blockchain* crea trazas que facilitan el control y permiten saber quién ha hecho qué y cuándo; convirtiéndose así en una herramienta para contribuir a la **transparencia**. Tercero, no necesita de una autoridad de certificación centralizada para gestionar los accesos y el uso de los servicios por grandes poblaciones. Finalmente, el desarrollo de sistemas basados en *blockchain*, si se completan con éxito, podría llevar a ahorros de coste significativos.

Hoy en día, las agencias gubernamentales de todo el mundo exploran las posibilidades de *blockchain* para hacer que sus servicios sean más eficientes, más rentables, más seguros, más transparentes. Y, por supuesto, están buscando la forma en que *blockchain* pueda aumentar la confianza en los procesos gubernamentales.

Dicho esto, la tecnología de cadenas de bloques no es la solución a todos los problemas. De hecho, el gran optimismo y ambición quizá sean los principales riesgos ligados a este sistema, ya que muchos actores (entre ellos los gobiernos europeos) están intentando por todos los medios que triunfe esta tecnología, lo que puede llevar a invertir recursos significativos sin alcanzar los resultados esperados.

En cualquier caso, se puede comenzar a hablar de «internet del valor», una plataforma nueva, distribuida, con un gran potencial para ayudarnos a reformular el trabajo y a transformar para mejor el vigente orden de los negocios.

2. La Administración Pública y la transformación digital

En el caso de las administraciones públicas existen elementos de contexto que facilitan y promueven la implementación de proyectos de tecnologías de la información, entre ellos la e-administración o *gobierno digital* y el llamado *gobierno abierto*.

2.1. Gobierno abierto

Según el portal de la transparencia de la Administración General del Estado², el gobierno abierto es una nueva forma de actuar mediante la que las Administraciones Públicas, a través de Planes de Acción, ofrecen información sobre lo que hacen con transparencia, rinden cuentas, promueven la participación y tienen en cuenta la opinión de los ciudadanos en la gestión de los asuntos públicos. Este concepto está sustentado por tres pilares básicos. Primero, la **transparencia**, ya que la administración debe poner a disposición del ciudadano toda la información sobre lo que está haciendo y cómo lo está haciendo, siempre cumpliendo con las leyes y normas establecidas. Segundo la **colaboración** para facilitar el trabajo conjunto entre la sociedad civil, las empresas y la administración. Finalmente, la **participación**, directa o indirecta, de la ciudadanía, lo que requiere un acceso a una información que las administraciones públicas deberán poner a su disposición.

Transparencia

Todos los gobiernos han elaborado sus normativas sobre la transparencia como un pilar fundamental no solo de un gobierno abierto, sino como elemento esencial de una democracia madura. Y, como no solamente los datos deberán ponerse a disposición del ciudadano, sino que el control del acceso a esa información tendrá también que estar regulado, surgen las leyes de protección de datos. El mismo ciudadano que quiere acceder a la información requiere que sus datos personales estén protegidos. El equilibrio correcto entre estos dos principios está aún por llegar.

Al hilo de estas leyes sobre transparencia, han proliferado los portales de acceso a la información. Aun así, no se puede decir que ello haya erradicado problemas como la corrupción o las irregularidades.

Colaboración

Un gobierno colaborativo implica y compromete a ciudadanos y demás agentes en el propio trabajo de la Administración. La colaboración supone la cooperación no sólo con la ciudadanía, sino también con las empresas, las asociaciones y otros actores. Y permite el trabajo conjunto dentro de la propia Administración, entre sus empleados, así como entre diferentes administraciones.

Participación

La participación ciudadana es una pieza fundamental para el desarrollo de un buen gobierno democrático, capaz de promover una sociedad activa que ayude al gobierno a impulsar aspectos económicos, sociales, culturales y políticos. Este derecho del ciudadano enriquece al sistema gubernamental en todos sus procesos administrativos para que sean más competentes, y genera una relación de respeto entre la administración y la ciudadanía.

Los mecanismos de participación ciudadana están estrechamente ligados a las nuevas tecnologías que se están implantando para mejorar las vías democráticas y los procesos conjuntos instituciones-sociedad (Shermin, 2017). De este modo, se pretende desarrollar herramientas eficaces y accesibles a la participación mejorando la comunicación entre ambas partes. Una de las formas de participación política tradicional son las elecciones. Y es un reto para el gobierno encontrar soluciones seguras para el voto electrónico.

Una consecuencia del gobierno abierto es la apertura de *datos públicos* a los ciudadanos, lo que implica la publicación de información del sector público en formatos que permitan su reutilización por terceros para generar nuevo valor. Toda la información que se facilita —que debe ser completa, accesible para todos, gratuita y no restringida, es decir, legible, no discriminatoria y libre— constituye el insumo para la innovación, además de incrementar la transparencia del gobierno y la rendición de cuentas a la ciudadanía.

Ya en 1970 Alvin Toffler escribió que la única forma de salvar los sistemas políticos de representación era la democracia participativa: permitir a los ciudadanos, previamente informados, tomar las decisiones. Su editor, Clem Bezold, en 1978 escribió en *Anticipatory Democracy* que la democracia se va a componer de ciber-administración, ciber-voto, ciber-participación, ciber-agenda y ciber-infraestructura (Lander, Cooper, 2017). El paso del tiempo ha confirmado lo visionario de esta afirmación.

2.2. Gobierno digital o administración electrónica

La e-Administración o Administración Electrónica es la incorporación de las tecnologías de la información en la administración pública. Tiene dos vertientes. Desde un punto de vista intra-organizativo, implica transformar las oficinas tradicionales, convirtiendo los procesos en papel en procesos electrónicos, con el fin de

crear una oficina sin papeles. Desde una perspectiva de las relaciones externas, implica habilitar la vía electrónica como un nuevo medio para la relación con la ciudadanía y empresas. Interesa resaltar que es una herramienta con un elevado potencial de mejora de la productividad y simplificación de los diferentes procesos del día a día.

Desde 2001, el desarrollo de la Administración Electrónica en la Unión Europea ha partido del consenso alcanzado entre los Estados miembros en declaraciones ministeriales. La última de ellas adoptada en la ciudad de Tallín el 6 de octubre de 2017, a iniciativa de la Presidencia estonia de la UE, con el apoyo de la Comisión Europea, refuerza el compromiso con los principios del Plan de Acción de Administración Electrónica 2016-2020. Esta declaración va dirigida tanto a la Unión Europea como a los países EFTA (32 países en total), sus líneas de actuación política están detalladas en la Tabla 1.

Estos dos modelos de gobierno y administración, justifican por qué la tecnología *blockchain* que pasamos a describir, ha suscitado tanto interés en el sector público, ya que parece dar respuesta a una parte de los retos que se señalan.

3. Descripción de la cadena de bloques, tipos y propiedades

En septiembre de 2008, Lehman Brothers sufrió la quiebra más importante en la historia de los Estados Unidos originando la crisis financiera mundial. En octubre de ese mismo año, una persona o grupo desconocido, utilizando el nombre de Satoshi Nakamoto, publicó «*Bitcoin: A Peer-to-Peer Electronic Cash System*» donde se define un protocolo por el que se propone un sistema descentralizado para la transferencia de valor, que no se basaría en la ética de los seres humanos ni en la confianza en las instituciones, sino en matemáticas y cálculos informatizados sólidos. Nace *blockchain* o la cadena de bloques. La criptomoneda Bitcoin fue la primera aplicación de la cadena de bloques.

Una década después, el ecosistema desarrollado en torno al proyecto *blockchain* incluye cientos de aplicaciones en distintos ámbitos: de las financieras al voto electrónico, la identidad o el mercado de valores.

Tabla 1

Líneas de actuación política de la Declaración de Tallín sobre Administración Electrónica

Línea de actuación política	Descripción
Digital por defecto, inclusión y accesibilidad	Asegurar que la ciudadanía y las empresas europeas interactúen digitalmente con las administraciones públicas y de la manera más accesible posible, desarrollando sus capacidades digitales así como promoviendo los servicios públicos digitales disponibles.
Principio de solo una vez	Evitar que la ciudadanía tengan que suministrar constantemente los mismos datos a las diferentes administraciones. Se pretende impulsar la colaboración y el intercambio de datos entre las distintas administraciones, tanto a nivel regional como nacional y europeo.
Confianza y seguridad	Asegurar la implementación a tiempo y promover el uso de la Regulación sobre identificación electrónica y de los servicios de confianza para las transacciones electrónicas en el mercado interior. Asegurar que los requisitos de privacidad se tienen en cuenta a la hora de diseñar servicios públicos y soluciones basadas en tecnologías de la información.
Apertura y transparencia	Mejorar la gestión que la ciudadanía y empresas pueden hacer de sus datos personales recogidos por las administraciones públicas.
Interoperabilidad por defecto	Impulsar la reutilización de soluciones tecnológicas compartidas y estandarizadas, en temas como la identidad, la firma electrónica, o los contratos, y hacer más uso de soluciones y software abierto.
Medidas políticas horizontales	Establecer un conjunto de medidas que faciliten la transformación digital de las organizaciones en términos de competencias, planificación, experimentación, intercambio de buenas prácticas, etc.

Fuente: Elaboración propia.

3.1. Que es blockchain?

Pensar en *blockchain* es pensar en transacciones que tradicionalmente se registran en el libro contable que se guarda a buen recaudo. La cadena de bloques es un registro compartido por millones de ordenadores conectados, donde se inscriben y archivan las transacciones de dos partes de manera verificable, permanente y anónima sin necesidad de intermediarios. Está diseñada para evitar su modificación, ya que, una vez que ha sido publicado un contenido, se usa un sellado en el tiempo, fiable, enlazado a un bloque anterior, y distribuido. Por esta razón es especialmente adecuada para almacenar de forma incremental datos ordenados en el tiempo y sin posibilidad de modificación ni revisión.

La denominación «cadenas de bloques» es el resultado de una combinación de dos tecnologías, por un lado la *tecnología de registros distribuidos* y por otro la *cadena de bloques*, aunque esta última es la que ha dado identidad al conjunto. La Figura 1 presenta la arquitectura de *blockchain* de forma esquemática.

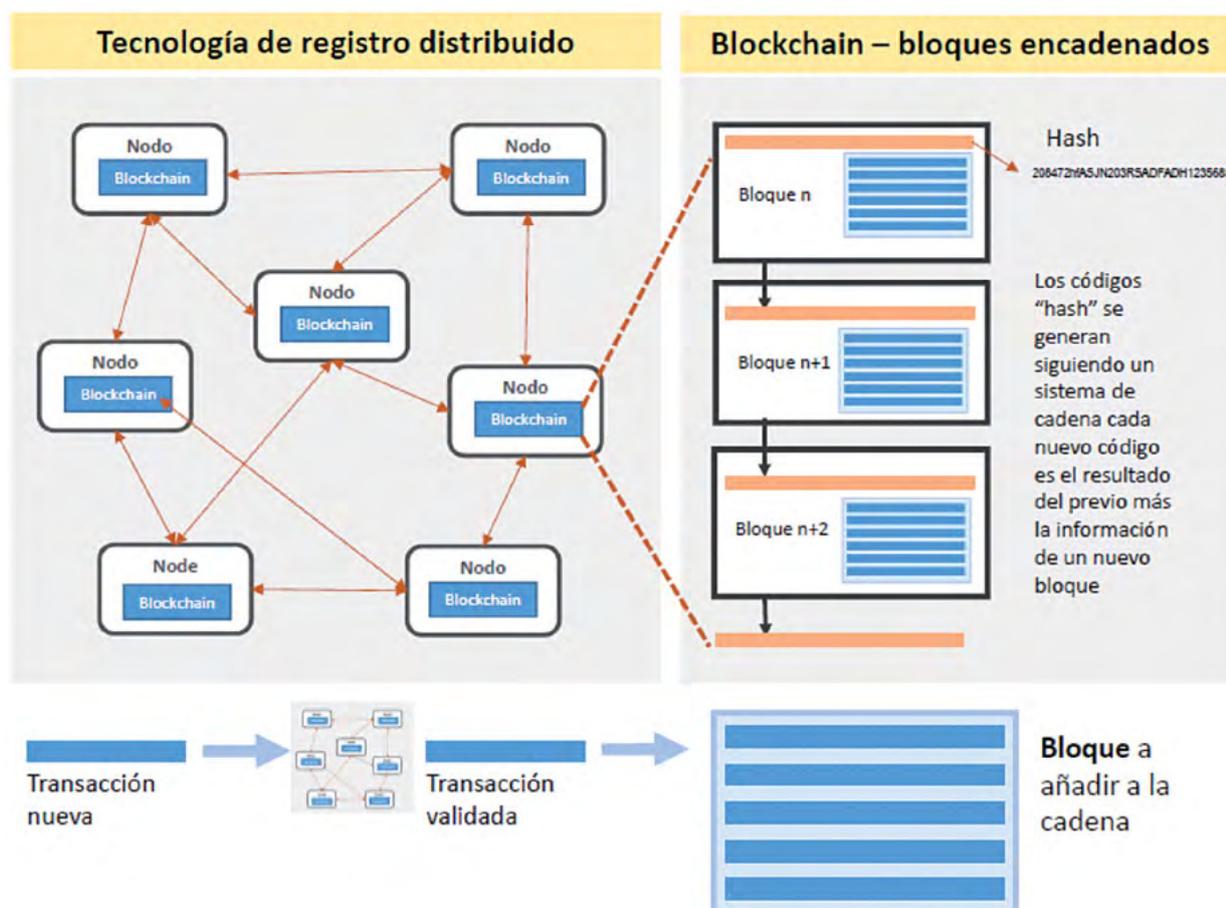
Un registro distribuido

Blockchain es un *registro distribuido* porque la información se encuentra repetida en diferentes ordenadores (**nodos**) que están repartidos por todo el mundo y sincronizados a través de un mecanismo de consenso. Todos los nodos comparten la responsabilidad y los beneficios del mantenimiento, las desviaciones con respecto a las reglas son fácilmente detectables. El sistema se auto-controla de forma que, ante ataques, es suficiente que un 51% de los nodos contengan aún la información para que esta se siga considerando válida. Dado el gran tamaño de la red pública, ataques de mayor envergadura son, hoy en día, difíciles de imaginar.

Es un *registro electrónico* en que no hay intermediarios lo que disminuye el riesgo de fraude, además de permitir una mayor transparencia y un aumento de la confianza (Parlamento Europeo, 2018).

Figura 1

Cómo funciona blockchain. Arquitectura



Fuente: Junstrand (2018) y elaboración propia.

Un conjunto de bloques encadenados

Literalmente, *blockchain* es una cadena de bloques, cada bloque contiene un grupo de transacciones validadas. Los bloques se añaden a la cadena de forma lineal y cronológica y cada bloque está inextricablemente unido al previo utilizando un proceso de «hashing»³. Cada bloque tiene un único código hash que se calcula a partir de la información del bloque y del hash del bloque previo, generando una secuencia de códigos encadenados.

Si se altera el contenido de una transacción, aunque sea mínimamente, se cambiará completamente el código hash del bloque. Esto ocasionaría efectos cascada en todos los bloques subsiguientes conectados. Los nodos se darían cuenta inmediatamente y lo rechazarían.

3.2. Propiedades

Las principales propiedades de la cadena de bloques distribuida es que es descentralizada, verificable, inmutable y segura.

En un sistema **descentralizado** no hay un punto único de decisión. En cada nodo se toma la decisión que más conviene en función de las reglas de consenso que el operador del nodo ha elegido libremente. El resultado del conjunto del sistema es la respuesta colectiva. Cada transacción es firmada digitalmente por el iniciador y debe ser **validada** por la mayoría de los otros nodos. El registro es transparente: todos los agentes pueden ver todas las transacciones y verificar su validez.

Una de las claves de la tecnología es la criptografía, un algoritmo que transforma un mensaje sin alterar su contenido. En el *blockchain* es esencial para que el mecanismo de codificación sea **seguro** y evitar la manipulación o el hurto, protegiendo así la integridad de los registros.

Cuando se añaden a la cadena de bloques, las transacciones no pueden suprimirse ni modificarse, quedan grabadas de forma permanente. Los algoritmos criptográficos que confirman la validez de las transacciones están **sellados temporalmente**, el sistema es **inmutable**.

3.3. Tipos de redes *blockchain*

Atendiendo a la libertad de los nodos para integrarse en el sistema, las cadenas de bloques de pueden clasificar en tres grandes grupos: públicas, privadas e híbridas.

Las redes *blockchain* **públicas**, según Preukschat (2017), pueden definirse como una red descentralizada de ordenadores (nodos) que utilizan un protocolo común asumido por todos los usuarios y que permite a éstos registrar transacciones. En este tipo de *blockchain* no existe limitación en cuanto al número de usuarios participantes que podrán siempre descargar en su ordenador la tecnología necesaria para constituir un nodo que se unirá a la red. Estos usuarios participan también en el proceso de consenso. Cuantos más nodos participan en la cadena de bloques, esta es más segura y menos vulnerable frente a intentos fraudulentos de alterarla. Las redes públicas más conocidas son Bitcoin, Bitcoin Cash, Ethereum y Litecoin.

Como las cadenas de bloques públicas están compartidas de forma abierta entre todos los usuarios, se ha visto la necesidad, por motivos de confidencialidad o por razones regulatorias, de crear las cadenas privadas. Las redes **privadas** o **permisionadas** son aquellas en las que el proceso de consulta, validación y participación están limitados a unos nodos determinados. Una autoridad central concede las autorizaciones para realizar transacciones, ejecutar programas o acceder a la información. Con ello, se pierde la propiedad de la descentralización como elemento característico de la tecnología *blockchain* tal y como fue concebida. Además, el buen funcionamiento del sistema dependerá de la honestidad de esta autoridad central.

Para mitigar los problemas de las redes públicas sin perder sus propiedades (como ocurre con las privadas) las entidades financieras han impulsado so-

luciones híbridas, que no permiten que cualquier usuario pueda participar en el proceso de validación de las transacciones, sino que las restringen a los miembros de un determinado colectivo, pudiendo ser el acceso a los bloques tanto público como restringido.

Las administraciones públicas, al igual que las entidades financieras, deberán buscar la solución que se adapta mejor a sus requisitos. Una de estas soluciones pasa por integrar *blockchain* público con los sistemas de información existentes, la información reside en los sistemas de la administración y la huella digital de las transacciones se almacena en la cadena de bloques de forma que puedan disfrutar de sus beneficios y mitigar sus problemas.

Sin menospreciar las soluciones basadas en infraestructuras privadas, es pertinente recordar en este punto la frase de Forde (2017) «The answer lies with the public - public *blockchains*, to be specific» («la solución está en el público, en el *blockchain* público, para ser exactos»).

3.4. Las limitaciones de *blockchain*

El *blockchain* no deja de tener sus limitaciones. Como apuntan Lander y Cooper (2017), la adopción de esta tecnología será lenta por diversas razones. La primera es la propia **lentitud** del sistema: los beneficios en seguridad que proporciona un registro descentralizado, replicado y distribuido tienen como contrapartida su **ineficiencia** si se compara con una base de datos clásica, no solo en tiempo de proceso, sino también en recursos de cálculo, siendo así la gran cantidad de recursos energéticos que consume una de las críticas más importantes. Además, ante una nueva versión del sistema, es preciso migrar todos los datos para preservar la historia lo que hace que las actualizaciones sean muy lentas.

Todo ello se ve aún más dificultado por los problemas ligados a la **privacidad**, la encriptación es una solución, pero requiere garantías de preservación. Todo esto sin olvidar las cuestiones de **legalidad** como ¿cuál es el valor de los contratos inteligentes? ¿pueden las trazas de *blockchain* utilizarse en un tribunal de justicia? Es necesario, sin duda, un marco normativo común.

En la actualidad, la utilización del *blockchain* de forma generalizada para muchas transacciones puede resultar muy **costoso**.

Todas estas limitaciones invitan a la prudencia. Y prudencia es también la conclusión del informe del EU *Blockchain* O. F. (2018a) que presenta los cuatro prin-

cipios que constituyen la regla de oro que deben guiar a las organizaciones que se lanzan a utilizar *blockchain*:

- *Principio 1.* Comenzar observando el panorama general: ¿Cómo se crea valor para los usuarios? ¿Es necesario realmente utilizar *blockchain*?
- *Principio 2.* Evitar almacenar datos personales en una cadena de bloques a menos que se haga uso completo de las técnicas de ofuscación, encriptación y agregación de datos para anonimizarlos.
- *Principio 3.* Almacenar los datos personales fuera de la cadena o, si no se puede evitar, en redes de cadenas privadas permitidas. Considerar cuidadosamente los datos personales al conectar cadenas de bloques privadas con las públicas.
- *Principio 4.* Continuar innovando, pero de manera responsable con la privacidad, y siendo muy transparente con los usuarios.

3.5. Los campos de aplicación de la tecnología

La tecnología *blockchain* tiene, fundamentalmente, tres campos de aplicación: las **criptomonedas**, los **contratos inteligentes** y las funciones de **notaría**.

En el campo de las *criptomonedas*, o de la transferencia de valor, la cadena de bloques se usa como notario público no modificable de todo el sistema de transacciones a fin de evitar el problema de que una moneda se pueda gastar dos veces.

También se utiliza como base de plataformas descentralizadas que permiten soportar la creación de acuerdos de *contratos inteligentes*⁴ entre pares.

Por último, la cadena de bloques puede utilizarse como servicio de *notaría* al registrar la huella digital de los documentos y sus metadatos. Las huellas digitales son un identificador único generado por el contenido de un documento, un pequeño cambio de contenido alteraría completamente la huella, por lo que se proporciona un mecanismo para verificar la integridad. Una impresión registrada en la cadena de bloques está «escrita en piedra» y sirve como futura referencia para demostrar que un documento no ha sido modificado desde su registro. Si a ello le añadimos el sellado temporal, su utilización es muy variada y permitirá, entre otras aplicaciones, mejorar la función de *registro* de documentos en las relaciones entre las administraciones públicas, los ciudadanos y las empresas.

4. Principales casos de aplicación en el sector público

Blockchain tiene el potencial de contribuir a la transparencia, seguridad, y eficiencia de los servicios públicos existentes; de crear nuevos; de contribuir a disminuir la corrupción de la administración pública; de romper los silos entre los distintos departamentos y aumentar la interoperabilidad y, en definitiva, de recuperar la confianza en los gobiernos y el sector público. No obstante, como indica el EU *Blockchain O. F.* (2018b), *blockchain* no es la solución a todos los problemas; en muchos casos, una base de datos centralizada operada por una agencia del gobierno fiable dará los resultados deseados sin tener que recurrir a tecnologías más complejas.

Para obtener beneficios hay que desarrollar esa tecnología en aplicaciones pertinentes. Para ilustrar sus múltiples posibilidades pasamos a describir a continuación algunos casos de uso prometedores.

4.1. Gestión de la identidad

Las administraciones públicas no son solamente la fuente de información de identidad clave para la ciudadanía (desde el certificado de nacimiento al de defunción), sino que también necesitan identificarlos sin ambigüedad para ofrecerles servicios. Esto se aplica también a empresas o asociaciones y cada vez más a máquinas y otros agentes.

Algunos países han desarrollado sistemas de identidad digital, en general costosos y de difícil gestión, ya que dependen de autoridades de certificación. Lo ideal es que cada actor en la economía digital tenga una identidad digital única y verificable, segura y privada sin tener que recurrir a una autoridad externa, esto no es fácil de obtener con la tecnología existente, y las administraciones están lanzando proyectos para ver si la cadena de bloques puede contribuir a implementar soluciones en esa línea.

4.2. Registros de títulos y/o activos

Debido al sellado temporal, a su imposibilidad de modificación, y a su capacidad de verificación por el público, registrar un título o un activo es una de las fun-

ciones básicas más obvias de la cadena de bloques, y esta tecnología está siendo utilizada para la digitalización del registro de la propiedad en algunos países. El mismo proceso se puede utilizar para cualquier tipo de registro: empresas, automóviles, armas de fuego, etc.

El proceso actual, usualmente basado en papel, es lento, y requiere la verificación entre diferentes entidades: bancos, notarios, abogados, agencias del gobierno y las partes interesadas. Suecia y Reino Unido han realizado proyectos piloto utilizando *blockchain*.

4.3. Salud

En muchos países, los ficheros médicos están guardados en los archivos de los médicos y en las bases de datos de los hospitales, la información no está fácilmente accesible y los ficheros se comparten de forma manual. Encontrar soluciones digitales es muy delicado al tratarse de datos sensibles de carácter personal.

Estonia, que ha establecido un registro Electrónico de Salud, está pensando en utilizar un registro basado en *blockchain* para garantizar una manipulación correcta de datos médicos sensibles al generar una traza de auditoría sobre cómo los datos han sido utilizados. En Suecia hay una iniciativa para crear un registro sanitario para otorgar a la ciudadanía más control sobre sus datos. En estos ejemplos, lo que se propone no es el almacenamiento de los datos en *blockchain*, sino que se use la cadena de bloques para almacenar las pruebas de que son genuinos los datos que están almacenados fuera de la cadena.

4.4. Certificados y diplomas en el campo de la enseñanza

Los diplomas en la enseñanza son un ejemplo de datos almacenados en silos, que son las instituciones académicas. Los diplomas papel pueden falsificarse fácilmente y dar acceso a estos datos para probar la autenticidad de las credenciales puede ser muy difícil. Por otro lado, los títulos universitarios tardan tiempo en ser emitidos con el sello oficial y los certificados de estudios, utilizados para comprobar datos y evitar currículos falseados, implican un farragoso papeleo y tiempo de espera. Todo esto sin tener en cuenta que cada país utiliza un sistema diferente y que el reconocimiento de la equivalencia del diploma no es una tarea trivial.

Por todo esto, si hay un campo en que se pueden identificar fácilmente los beneficios de la implementación de la tecnología *blockchain* es el de la enseñanza. Según Grech y Camilleri (2017) las siguientes áreas es muy probable que utilicen la cadena de bloques en el futuro próximo de forma generalizada: (a) emisión de certificados y transferencia de créditos, (b) validación de los títulos o certificados sin contactar con organismo emisor, (c) utilización de las criptomonedas para realizar pagos y recibir ingresos (becas) dentro de la institución.

En resumen, *blockchain* puede ayudar a los individuos que pueden tomar las riendas de sus credenciales académicas a través del registro, por otro lado, esas credenciales pueden fácilmente verificarse por empleadores u otras entidades que requieren contrastar la veracidad del diploma.

La universidad de Nicosia ya emite certificados que pueden verificarse en línea. Malta lo está iniciando a nivel gubernamental. En España, la escuela de negocios ISDI y la Universidad Carlos III de Madrid certifican sus títulos de forma instantánea utilizando esta tecnología.

4.5. Voto electrónico

El voto electrónico es una tentadora perspectiva para el gobierno abierto puesto que la ciudadanía podría votar de forma fácil y segura, desde cualquier sitio, utilizando dispositivos de uso común (teléfono móvil, ordenador personal) siendo éste el paso fundamental para el verdadero desarrollo de la democracia participativa.

Si hay un sistema que solamente puede funcionar si la confianza es absoluta es el voto electrónico. La sospecha de una posible manipulación invalida el sistema, y por esto se utilizan los observadores (interventores) en los procesos basados en el papel. Soluciones basadas en *blockchain* contribuyen a diseñar un sistema de voto electrónico transparente y fiable, manteniendo la confidencialidad. A través de la tecnología sería posible automatizar el recuento asegurándose la unicidad del conteo de cada voto.

Esta transformación representa un gran cambio cultural: pasar de confiar en la autoridad electoral a creer en protocolos y algoritmos. Esta dificultad no ha impedido que algunas iniciativas vayan adelante como la de Zug, en Suiza y algunas experiencias en Estonia o Australia. Por otro lado, para llegar a un modelo de participación y cohesión social, las plataformas tienen que ser accesibles a toda la población, no se pueden construir sistemas para las élites, por ello hay que tener en cuenta la, aun existente, brecha digital.

El voto electrónico es una de los campos de actuación que se detallan en la Resolución del Parlamento Europeo (2018).

4.6. Seguimiento y regulación de mercados

Para proteger a los consumidores, una de las tareas clave del gobierno es regular y supervisar los mercados asegurando su viabilidad y garantizando la legalidad. Esta supervisión es de particular importancia en los suministros e infraestructuras críticas. Para hacer este seguimiento hace falta conocer la realidad y esto a través de datos que, en la actualidad, o son auto-declarados o se obtienen vía inspecciones.

Ambos métodos presentan problemas. En el caso de datos auto-declarados, los gobiernos dependen de la entidad que informa para la exactitud de la información y esto deja la puerta abierta al fraude, al error y a los retrasos, lo que dificulta la tarea del regulador y del supervisor. Por otro lado, realizar inspecciones y auditorías es costoso y, como se basan en controles al azar, solo proporcionan una imagen parcial de lo que está sucediendo, siendo difícil, además, integrar los datos procedentes de diferentes entidades.

La tecnología de *blockchain* podría ayudar a abordar tales problemas. Tener un registro distribuido puede simplificar la recopilación de datos ya que los reguladores podrían solicitar más fácilmente informes en tiempo real de instituciones como bancos o fabricantes, bien conectándose directamente a sus sistemas o desarrollando una plataforma compartida para una industria determinada donde se unan empresas reguladoras y otras partes interesadas.

En las cadenas de producción y suministro, tales plataformas podrían hacer un buen uso de la automatización a través de sensores que envían sus datos directamente al registro. Esto permitiría a los reguladores reemplazar las inspecciones con el seguimiento directo y en tiempo real de los productos durante su ciclo de vida.

Dichas capacidades podrían ser particularmente efectivas en cadenas de suministro «críticas», como alimentos y productos farmacéuticos, cuya protección es esencial para la salud pública. Con datos en tiempo real sobre los mercados financieros, por ejemplo, las administraciones pueden identificar más rápidamente problemas con un banco o una empresa de seguros.

Transparencia es la clave y muchos de los actores actuales pueden no sentirse cómodos con ello. Participantes honestos van a aceptar entrar en el sistema,

de forma que el no ser parte de él se traducirá en una pérdida de confianza de los usuarios.

4.7. Impuestos

En Europa, el Impuesto al Valor Añadido (IVA) es una fuente importante de ingresos para los Estados Miembros y la Unión Europea, el sistema de recaudación tiene deficiencias y se estima que se pierden anualmente unos 150.000 millones de euros en fraude de IVA, en parte, porque el IVA tiene que ser auto-declarado (EU *Blockchain* O. F. (2018b)). El control *a posteriori* es costoso y lento, y solo se examina una pequeña parte de las declaraciones.

Una empresa holandesa está construyendo una plataforma basada en *blockchain* que tiene como objetivo combatir el fraude del IVA. La solución se basa en un *blockchain* permissionado que contiene un registro de facturas confidencial y con sellado temporal, aportando transparencia y eficiencia en el proceso del IVA. Su solución, dice la empresa, mejorará la detección del fraude, y permitiría la automatización del IVA.

4.8. Gestión de compras, contratos y proveedores

La contratación pública es un caso de uso en el que un registro basado en una cadena de bloques puede aportar muchos beneficios al proceso al poder facilitar la transparencia total de los gastos públicos.

Por ejemplo, el registro de todos los documentos digitalizados que presentan las empresas que licitan podría hacerse a través de una cadena de bloques que garantizaría la hora y la exactitud de cada elemento del contenido. Cualquier añadido o modificación no sería reconocido por la cadena. De la misma forma, otras etapas del proceso pueden registrarse incluyendo los mensajes que se intercambien entre la administración y las empresas en este contexto.

Si imaginamos un futuro en que todos los registros administrativos estuviesen basados en una cadena de bloques, los documentos como escrituras de la empresa, certificaciones, o referencias, ya estarían registrados en la cadena con lo que introducir la repuesta a una licitación se reduciría a señalar unas entradas al registro ya existentes, y a registrar la propia respuesta al pliego de especificaciones. Los beneficios son múltiples: reducción de los riesgos de falta de conformidad con el proceso, aumento de la seguridad y la

transparencia, automatización de la confirmación de fechas y plazos, eliminación de la necesidad de una verificación por terceras partes, etc. Y por supuesto, añadiendo el de una menor carga de trabajo para las empresas.

Además, para licitaciones sencillas, la atribución puede automatizarse utilizando la tecnología de contratos inteligentes.

El modelo no se reduce solo a la fase de licitación, sino que se extiende a todos los documentos generados en el proceso: contratos, facturas, documentos de aceptación, albaranes, entregas, etc.

4.9. Las ciudades inteligentes

Una sociedad en constante cambio hace que las ciudades de hoy en día se enfrenten a muchos retos: el crecimiento de la población, la contaminación y el tráfico, la seguridad, el control de la corrupción, la transparencia, el aumento del turismo, el consumo energético. La única respuesta razonable a todos estos retos es el uso de las tecnologías de la información. Al uso integrado y totalmente desplegado de las tecnologías de la información y las comunicaciones en la gestión de las ciudades se le denomina «ciudades inteligentes».

En el mundo, son numerosas las plataformas para gestionar ciudades inteligentes. En todos los casos la funcionalidad es generalmente buena, pero adolecen de los problemas de integración, interoperabilidad, transparencia, seguridad y la robustez. En ese contexto, las plataformas basadas en *blockchain* pueden ser una buena solución.

4.10. Contenidos y publicaciones inmutables

Uno de los riesgos de la transformación digital de las organizaciones es garantizar que los contenidos difundidos de forma electrónica son los originales, que no han sido manipulados.

Registrar los contenidos y/o las publicaciones en una cadena de bloques permitirá, en todo momento, y a cualquier usuario o ciudadano, comprobar si un contenido o una publicación es la originalmente emitida por una institución, ciudadano o empresa. También impide que el propio emisor o autor cometa fraude reemplazando contenidos o eliminándolos, ya que el nuevo contenido no se correspondería con el ya registrado.

5. Blockchain y el esfuerzo de liderazgo de la Unión Europea

No hay duda de que la Unión Europea ha abrazado *blockchain* como una herramienta importante para fomentar la innovación y apoyar el mercado único digital. Una década después de su creación, diversas acciones han llegado a las agendas de los distintos actores públicos, entre ellas cabe destacar la creación en 2018 del *Observatorio y Foro Blockchain de la Unión Europea* gestionado por la Comisión Europea, el *Partenariado Europeo en Blockchain* en que participan los Estados Miembros firmado en Abril 2018 y la *Resolución del Parlamento Europeo sobre la cadena de bloques* publicada en noviembre del mismo año.

Tanto las instituciones de la Unión Europea, como los Estados Miembros, manifiestan así su clara intención y ambición de liderar la implementación de esta tecnología en lugar de ser simplemente seguidores.

5.1. Observatorio y Foro en Blockchain de la UE

En febrero 2018 la Comisión Europea lanza el Observatorio y Foro *Blockchain* de la Unión Europea con la misión de *destacar las principales iniciativas existentes en Europa (y más allá), promover los agentes europeos y reforzar el compromiso europeo con múltiples partes implicadas en las actividades de blockchain*. El observatorio se crea para hacer seguimiento de las tendencias de desarrollo, abordar problemas emergentes, y convertirse en un centro de conocimiento en la cadena de bloques.

El observatorio representa una importante oportunidad de comunicación para que Europa exponga su visión en la escena internacional y trata de inspirar acciones comunes basadas en casos de uso específicos de interés europeo.

5.2. Declaración para la creación de Partenariado Europeo en Blockchain

El 10 de abril de 2018, 22 Estados Miembros firmaron la *Declaración para un Partenariado Europeo en Blockchain*, con la intención de que sea un vehículo para la cooperación entre los Estados Miembro, con

el fin de intercambiar experiencias y conocimientos en los ámbitos técnico y reglamentario y con el objetivo ambicioso de identificar casos de uso, desarrollar especificaciones y preparar el lanzamiento de aplicaciones de *blockchain* en toda la UE, en todo el mercado único digital. En la actualidad, 27 países ya han firmado la declaración.

En el acto de firma la comisaria Gabriel declaró: «En el futuro, todos los servicios públicos utilizarán la tecnología blockchain. Blockchain es una gran oportunidad para Europa y los Estados Miembros para repensar sus sistemas de información, para promocionar la confianza de los usuarios y la protección de los datos personales, para ayudar a crear nuevas oportunidades de negocio y establecer nuevas áreas de liderazgo, beneficiando a la ciudadanía, los servicios públicos y a las empresas. El Partenariado lanzado hoy, permite a los Estados Miembros trabajar juntos con la Comisión Europea para convertir el enorme potencial de la tecnología blockchain en mejores servicios para la ciudadanía.»

5.3. La Resolución sobre *blockchain* del Parlamento Europeo

En 3 de octubre de 2018, el Parlamento Europeo contribuyó al debate existente en el seno de la Unión Europea adoptando la Resolución sobre las tecnologías de registros distribuidos y las cadenas de bloques: fomentar la confianza con la desintermediación.

Bajo la hipótesis de que la tecnología de registros distribuidos no solo contribuye a la generación de confianza, sino que también reduce costes de intermediación y puede contribuir a una mejora de los servicios, el Parlamento plantea la necesidad de adoptar iniciativas estratégicas en distintos campos. Entre esos campos están: energía y aplicaciones respetuosas del medio ambiente, transporte, sector sanitario, cadena de suministro, educación, industria creativa y derechos de autor, y financiero. La Resolución dedica también un capítulo a las ayudas a las PYMES.

La Resolución alude a la seguridad de la infraestructura insistiendo en la necesidad de garantizar la sostenibilidad de las plataformas *blockchain* en el marco del programa del Observatorio y Foro *Blockchain* de la UE, y considera esta seguridad como un aspecto muy importante para mejorar los servicios y la gestión del sector público.

El Parlamento Europeo, aun cuando pide a la Comisión Europea que evalúe y desarrolle un marco jurídico para solventar posibles problemas legales que puedan plantearse en caso de fraude o delitos,

apunta en una dirección que no implicaría, por el momento, regular los nuevos fenómenos, sino más bien eliminar las barreras para su desarrollo, con la ambición de hacer de la UE el líder mundial en la era de la cuarta revolución industrial.

6. Panorama internacional y desarrollos en España en el sector público

Sin pretender ser exhaustiva, y con el objetivo de ofrecer una visión de conjunto de la situación internacional en el uso de la cadena de bloques en el sector público, paso a describir experiencias de diferentes países usando esta tecnología.

Si se tiene en cuenta la reacción de todos los actores ante el *blockchain*, no cabe duda de que esta tecnología está siendo una revolución. Su grado de penetración en el panorama mundial varía mucho; los países con un desarrollo en tecnologías de la información limitado, han visto la oportunidad de ofrecer de forma rápida servicios seguros basados en la infraestructura pública de registros distribuidos. Por el contrario, países con sistemas de información mucho más sólidos, con un nivel de interoperabilidad elevado, con una estructura pública digital (identidad digital, por ejemplo) largamente desarrollada, son más escépticos acerca de las ventajas que la nueva tecnología, «a la mode» puede ofrecer. A ello hay que unir el diferente nivel de tradición democrática, y de exigencias de transparencia. La Tabla 2 presenta ejemplos de aplicación en distintos países.

Un caso particular es el de Estonia, un país con larga tradición en administración electrónica que, sin embargo, no se ha quedado atrás en la introducción de *blockchain* y en 2012 se convierte en el primer país en desplegar esta tecnología en producción para su registro de sucesiones (testamentos). En sus aplicaciones, los datos reales no se almacenan en el *blockchain*, lo que significa que no hay problemas de privacidad, y el sistema permite al usuario saber quién ha actuado en el fichero (incluidas visualizaciones). Estonia tiene un registro e-salud respaldado con *blockchain* que se puede utilizar para hacer recetas electrónicas, y la legislación (el boletín del Estado) está también publicada en *blockchain*, proporcionando una prueba irrefutable de los textos legales en el tiempo.

Tabla 2

Ejemplos de aplicaciones de *blockchain* en el sector público en distintos países

País	Algunos ejemplos de uso de la cadena de bloques
Suiza	En Zug, credencial de identidad para residentes y se ha utilizado para el voto electrónico y para el alquiler de las bicicletas públicas.
Finlandia	Sistema de identidad para los refugiados en los campamentos finlandeses, vinculada a tarjeta de crédito para comprar alimentos y otras necesidades.
Estonia	Registro de sucesiones, e-Salud, publicación del Boletín oficial, registro de la huella digital de los activos.
Suecia	Registro de la propiedad inmobiliaria en <i>blockchain</i> privada, permite la realización de transacciones entre todos los actores comprador, vendedor, y bancos, en móviles.
Georgia	Aplicaciones para teléfonos inteligentes para la adquisición y la transmisión de títulos de propiedad de forma rápida y a un coste limitado.
USA	En el Estado de Delaware, donde muchas compañías se establecen, pilota un registro corporativo para los impuestos, y están explorando seguros compartidos. Wyoming tiene un marco legal.
Emiratos Árabes	Explorando casos de uso que incluyen, no solo el registro, la logística, sino también las operaciones de los bancos centrales. Smart Dubai.
Australia	Mejora de la transparencia de la cadena del comercio de agua, automatización de los derechos de autor, y desarrollo de una aplicación de voto electrónico.
Dinamarca	Almacenamiento del ciclo de vida de los automóviles (revisiones, averías, seguros, cambios de propietario), uso en compraventas y en la administración de los impuestos.
Ghana	Administración del territorio, la existencia legal de las parcelas y sus propietarios. La solución combina una red <i>blockchain</i> pública y tecnología de satélites.
Ucrania	Licitación pública con componentes en <i>blockchain</i> y últimamente, explorando la utilización del voto electrónico y el uso de las criptomonedas.
Italia	Búsqueda de modelos de certificación en las universidades.

Fuente: Elaboración propia.

La mayoría de los países de nuestro entorno han creado redes nacionales con el objetivo de desarrollar conocimiento sobre esta tecnología, en particular en el sector público; de poner en contacto expertos en distintas áreas de la administración; de facilitar la colaboración entre administraciones; y de ayudar a crear una cultura de la experimentación a largo término. Estas redes han catalizado las iniciativas y en muchos casos han encontrado financiación para realizar pilotos. Tal es el caso de Finlandia, Italia o España, entre otros.

En octubre de 2017, el gobierno de Eslovenia anunció su intención de posicionar al país como el destino líder de la tecnología *Blockchain* la Unión Europea. Siguiendo adelante con sus intenciones en octubre de 2018 Eslovenia inaugura el European *Blockchain* Hub con el objetivo de promocionar a alto nivel, crear y

distribuir conocimiento, e iniciar, coordinar y ejecutar proyectos en el área de *blockchain*.

El problema del marco legal está presente en todos los países, así como la falta de garantías de gobernanza de una infraestructura pública sin estructuras centrales de toma de decisiones.

Fuera del entorno europeo hay que mencionar el caso de Australia que, en 2016, fundó una compañía, Civic Layer, de *blockchain* con el propósito de ayudar a los gobiernos a resolver procesos de negocio complejos mediante la digitalización de las operaciones y los servicios utilizando tecnologías de contratos inteligentes y *blockchain*. En la actualidad, a través de su Digital Transformation Agency, realizan estudios de viabilidad y aconsejan en el uso de la tecnología.

Los Emiratos Árabes han realizado una gran apuesta por la tecnología de la cadena de bloques, en particular Dubai con su iniciativa Smart Dubai, una agencia creada con el objetivo de convertir Dubai en la ciudad del mundo más avanzada tecnológicamente y en particular desarrollar un gobierno basado en *Blockchain*. En la actualidad están desarrollando 20 casos de uso piloto en el área de las carreteras y el transporte, la energía, la educación o la salud.

En Canadá se ha creado la Cámara del Comercio Digital con el objetivo de centralizar las actividades en torno a *blockchain*. Una de sus líneas de acción es trabajar con los departamentos y líderes gubernamentales para que el gobierno entienda y acepte la cadena de bloques, proponiendo educación y orientación, y apoyando la creación e implementación de políticas, programas y financiación.

En los Estados Unidos de América existe una gran diferencia entre Estados. Cabe destacar el Estado de Wyoming, el único Estado con un marco legal para activos digitales, y el pionero Delaware con su aplicación de registro de empresas. A nivel federal, algunas agencias están implementando iniciativas como, por ejemplo, el Departamento de Seguridad Nacional con su aplicación en tareas de control de aduanas, la inmigración y el transporte.

Un caso particular es Japón, un país que depende enormemente del dinero físico y que no realiza apenas pagos electrónicos. El Primer Ministro japonés declaró que para 2025, el 40% de los pagos se realizaría sin efectivo, y el mejor método para que Japón realice esta transformación es mediante la tecnología Bitcoin (Orcutt, 2019).

6.1. Los desarrollos en España en el sector público

En el año 2016, España crea la red Alastria, un consorcio multisectorial promovido por empresas e instituciones que nace para acelerar la creación de ecosistemas digitales en torno a *Blockchain*, poniendo a disposición de los socios una plataforma colaborativa común. Desde su origen, su objetivo es trascender el ámbito empresarial, e incluir también las administraciones públicas, la comunidad de desarrolladores y la comunidad académica. El Consorcio está abierto a cualquier organización que quiera disponer de una herramienta fundamental para desarrollar su propia estrategia *Blockchain* pensando en la distribución y organización de productos y servicios para el mercado español.

Se puede resumir Alastria como una red *Blockchain* semipública, independiente, permissionada y neutral, diseñada para ser conforme con la regulación existente, que permite a los asociados experimentar estas tecnologías en un entorno cooperativo. Fue la primera red regulada basada en *blockchain* del mundo.

Al certificarse la identidad de cada socio, se pueden ofrecer servicios que utilizan la tecnología de contratos inteligentes, y explotar en España aplicaciones en un entorno con plenas garantías legales.

El gobierno regional de Aragón, socio de Alastria, ha sido pionero en España en lanzar un proyecto para controlar la licitación pública mediante la cadena de bloques. El objetivo es eliminar los intermediarios, permitir a licitadores presentar sus ofertas y respetar la integridad de la información que proporcionan. Su ámbito de aplicación serán los procedimientos abiertos simplificados, es decir, aquellos en que la evaluación se basa en una fórmula y no en un juicio de valor.

El proyecto se realizará en dos fases. La primera consiste en registrar las huellas de las ofertas con todos los documentos asociados. La generación de la huella digital utiliza tecnología *blockchain* pública. La segunda, más ambiciosa y que requiere más programación, consiste en utilizar los contratos inteligentes para evaluar automáticamente las propuestas. En todo el proceso se garantiza la integridad y la transparencia contribuyendo así a una mejora de la eficiencia. La fase I coincide con el piloto realizado por el Tribunal de Cuentas Europeo que se describirá más adelante.

Otras comunidades autónomas, como por ejemplo Cataluña, están desarrollando una estrategia formal para implementar *blockchain* en la administración pública.

Además de los ya mencionados ejemplos de uso en el sector académico, en pocos años, será realidad la red universitaria *blockchain* española para formalizar las titulaciones e intercambiar expedientes de forma automática. El primer paso se ha dado ya, con la entrada de la Conferencia de Rectores de las Universidades Españolas (CRUE) en Alastria.

En el año 2018 la Comisión Nacional del Mercado de Valores, tras enfrentarse a un creciente número de consultas sobre la regularidad de proyectos de inversión en criptomonedas e intercambios decide, junto con el Banco de España, y la Dirección General de Seguros instaurar un «Sandbox» para que los emprendedores probaran sus proyectos con usuarios reales y así el regulador pudiera conocer cuáles son los problemas para poder actuar en consecuencia y avanzar en la regulación.

7. La experiencia del Tribunal de Cuentas Europeo

El Tribunal de Cuentas Europeo (TCE) se creó para auditar las finanzas de la UE, principalmente en ámbitos relacionados con el crecimiento y el empleo, el valor añadido, las finanzas públicas, el medio ambiente y la acción por el clima. Los auditores seleccionan, vía muestreo, las transacciones a auditar que se corresponden con beneficiarios en los Estados Miembros o en países terceros o con otras instituciones.

Como indican Dai y Vasarhelyi (2017), la metodología común de auditoría basada en el muestreo genera muchos errores debido a la gran cantidad de datos que no llegan a ser auditados. La certeza al final de una auditoría es solo razonable, lo que no es muy eficiente teniendo en cuenta la gran cantidad de recursos invertidos en auditar. La tecnología *blockchain* podría transformar este proceso, haciendo que su incorporación en los procesos del negocio pueda facilitar el *control por diseño*.

Para poder auditar una transacción, se necesita recopilar *evidencias* que permitan saber si los fondos se han utilizado para el propósito original y si se han seguido las normas y procedimientos. Y precisamente, la información almacenada en la cadena de bloques ofrece una traza de contenidos lista para ser analizada por los auditores ya que está encriptada, ha sido aprobada por un protocolo de consenso, está disponible para todos los participantes, no puede alterarse, y cuenta con una marca temporal y con una huella digital única.

7.1. Proyecto piloto del TCE

Por todo esto, como parte de la actividad de vigilancia tecnológica del TCE, y con el objetivo de **estimular** el progreso de la tecnología de cadena de bloques en el ámbito de la auditoría de la UE y **explorar** la aplicación práctica, el ECALab⁵ inició, en marzo de 2018, un proyecto piloto para explorar las capacidades y los beneficios de la aplicación de un sistema de registro electrónico basado en la tecnología de la cadena de bloques. El piloto se realizó utilizando Compepio, un software que utiliza *Blockchain* (tecnologías de registros distribuidos) para registrar, verificar y rastrear los documentos y cualquier otra información digitalizada. El ECA Registry actúa como servicio nota-

rial permitiendo (a) registrar y relacionar las huellas digitales de los documentos y sus metadatos, (b) el control de plazos, (c) verificar los documentos y cualquier otra información digitalizada, y (d) intercambiar bidireccionalmente huellas digitales (hash) con otros sistemas.

En el ámbito de aplicación de este proyecto piloto, el TCE seleccionó tres casos de uso: auditoría de fondos europeos, contratación pública y protección de las publicaciones.

Dentro de las especificaciones se incluyeron (1) obtener resultados rápidos, (2) presentar usos concretos de las tecnologías de cadena de bloques en el ámbito de la auditoría, (3) usar una aplicación web, interfaz intuitiva para el simple uso como registro, (4) basarse en una plataforma pública de *blockchain*, (5) permitir la interoperabilidad entre estas plataformas públicas de cadena de bloques y los sistemas informáticos internos.

Durante el piloto se creó un sistema, listo para la producción, que permite a los usuarios registrar documentos digitales en la cadena de bloques pública, verificar su autenticidad y crear una traza de auditoría segura. Los trabajos concluyeron en junio de 2018.

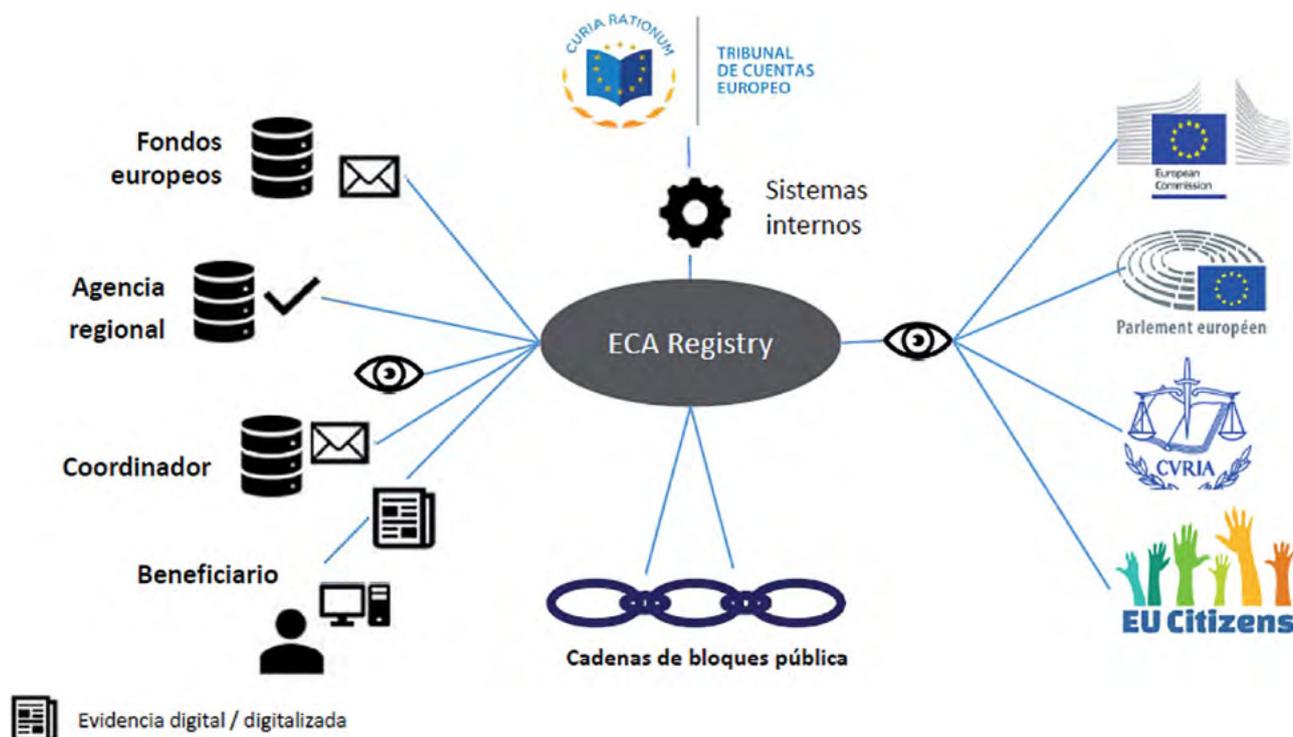
La Figura 2 presenta la solución. El **ECA registry** calcula la huella digital de cada uno de los documentos o informaciones registradas conteniendo esta huella digital toda la información de la transacción que se registra en la cadena de bloques públicas. Como comentábamos antes al hablar de las redes públicas y privadas, la solución adoptada fue almacenar la huella digital en la cadena de bloques pública, y conservar el documento en un recurso privado en este caso el ECA registry.

Los beneficios de esta solución son varios. Primero, evita los problemas de incumplimiento de la ley de protección de datos. Segundo, la cantidad de información registrada es pequeña lo que abarata los costes. Y tercero, el sistema se ocupa del registro en la *blockchain* pública con lo que el usuario no percibe problemas de lentitud del sistema. Para mitigar el riesgo ligado a las faltas de garantías de la disponibilidad de la infraestructura, la inscripción se hace en las 4 plataformas públicas existentes.

En el caso de la auditoría, el principio es que las evidencias son registradas por el beneficiario en el momento en que se generan. Así el resto de actores del proceso como coordinadores, agencias regionales, y cualquier otro organismo de control, no necesitan más que acceder al registro para registrar nuevas informaciones, o para consultar y verificar la información en el registro.

Figura 2

ECA Registry



Fuente: Tribunal de Cuentas Europeo.

El ECA Registry podría integrarse con los sistemas de información existentes en el TCE y con otros organismos de control y facilitar la captura de evidencias fiables introduciendo el concepto de **control-por-diseño**; esto podría contribuir a una importante reducción del coste de la auditoría que beneficiaría tanto a los organismos auditores como a los auditados a todos los niveles (europeo, nacional, regional o local), creando así valor añadido tanto estratégico como operacional, en términos de optimización del proceso, reducción del fraude y aumento de la transparencia generando confianza. Además, el TCE estaría en condiciones de mostrar su liderazgo en innovación en de los procesos de auditoría de la administración pública.

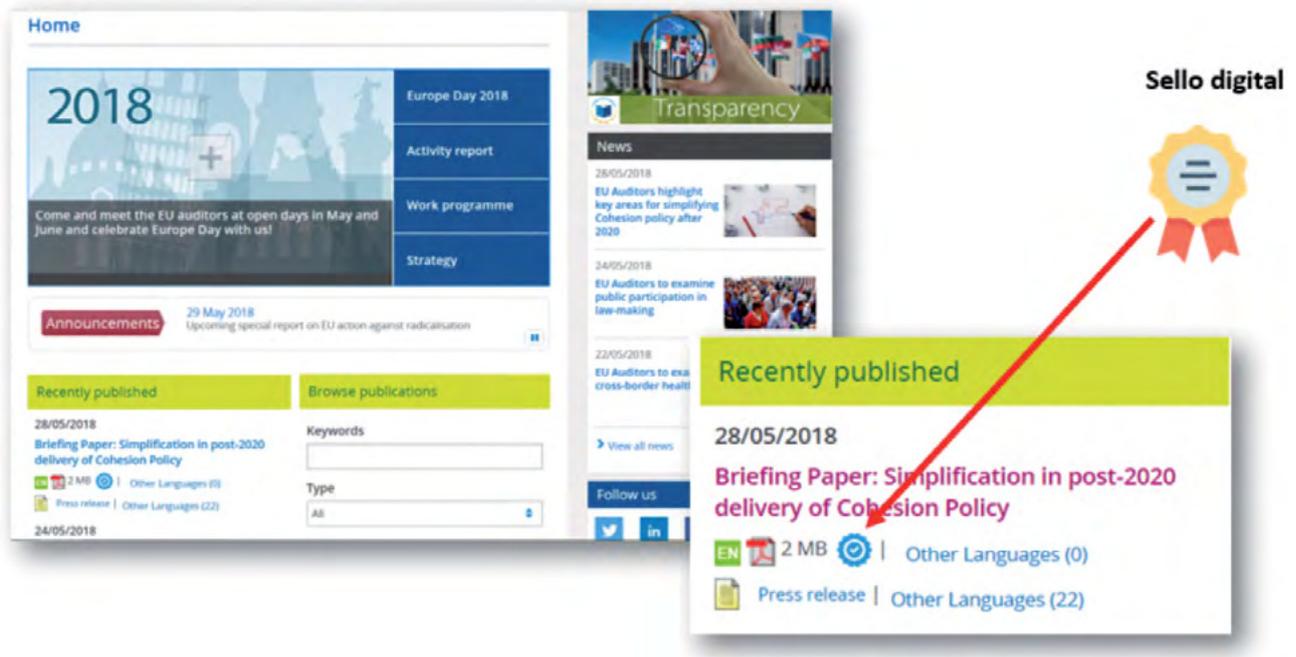
En lo referente al caso del uso *contratación pública*, el piloto ha mostrado cómo la utilización del registro ayuda a tener garantías sobre la integridad de los documentos y el cumplimiento de los plazos.

El tercer ejemplo consistió en registrar los informes oficiales que hoy se publican en el sitio internet del TCE, para garantizar la autoría y la integridad del contenido. A esas publicaciones se les asoció un icono que indica que la publicación es la original (ver Figura 3). El sistema permite, a cualquier usuario futuro, comprobar si el texto es realmente el original del TCE o, por el contrario, ha ido modificado.

El ECA Registry, en su aplicación para la auditoría ha sido uno de los proyectos seleccionados por el Partenariado Europeo en *Blockchain* para investigar su posible implementación a nivel europeo, utilizando los procesos de gestión de los fondos de cohesión. El TCE está trabajando con varias Direcciones Generales de la Comisión Europea para hacer realidad el proyecto, que representa una innovación disruptiva del proceso de auditoría, y en el que se deberá contar con la participación de ciertos estados miembros.

Figura 3

Solución para el sellado de las publicaciones del TCE integrada en el sitio internet



Fuente: Tribunal de Cuentas Europeo.

7.2. Auditar en un entorno post-blockchain

Como indica Cordero (2018), el futuro de la auditoría va a transformarse dramáticamente debido a la implementación de *blockchain*, junto con el uso de la tecnología de automatización de los procesos con robots y el ya creciente uso de la inteligencia artificial, haciendo del auditor un nuevo actor que pasará a jugar un papel más estratégico, como socio de negocio o consejero, ayudando realmente a la toma de decisiones.

una velocidad vertiginosa, y requiere unas inversiones considerables.

Este crecimiento supone un reto para las organizaciones públicas que tienen que tomar decisiones sobre el uso de esta tecnología. La falta de estándares para *blockchain* dificulta la evaluación de la calidad de una u otra solución, y la integración con sistemas existentes. Por otro lado, los proveedores de servicios *blockchain* son pequeñas empresas start-up, cuya contratación no es evidente debido a las exigentes reglas del sector público en cuanto a la licitación oficial.

Como indica Chen, Matthias, Domeyer y Lundqvist (2017), las organizaciones públicas tienen que adoptar un modelo de **incubadora** para poder moverse y sobrevivir en este mundo de la cadena de bloques.

¿Qué quiere decir esto? Deben formar un pequeño equipo que se ocupe primero de hacer un *inventario de ideas*, identificando las áreas en que esta tecnología puede ser de utilidad.

Una vez hecho esto, se deben *identificar* las aplicaciones que pueden dar mayores beneficios. El equipo se concentra en esas aplicaciones y realiza una prueba de concepto para validar la idea.

8. Metodología para el desarrollo de *blockchain*

Las organizaciones que quieren adoptar soluciones basadas en *blockchain* tienen que entender que se introducen en un mundo cambiante que evoluciona a

Las ideas buenas se pueden exportar, ofrecérselas a compañías tecnológicas para que las implementen en *partenariado*. El primer prototipo, deberá discutirse e intercambiarse con otros actores del propio país para conseguir una implementación más global. Una vez hecho esto, se puede pensar en extender la idea al contexto internacional.

Los gobiernos pueden y deben intercambiar experiencias, incluir socios internacionales, compartir tecnología y promover estándares globales.

9. Consideraciones finales

El potencial de la cadena de bloques para contribuir a la transformación digital del sector público es indudable. La capacidad de generar un sistema sin intermediarios que permite aumentar la confianza de los ciudadanos, la eficiencia en situaciones en que la madurez digital no está presente, la gran transparencia que puede brindar a democracias digitalmente maduras y la seguridad de los datos, son razones suficientes para creer en la tecnología.

Sin embargo, hay otros elementos a poner en la balanza. El primero, el gran esfuerzo que se ha invertido en hacer de la tecnología un éxito por todos los actores públicos europeos, que evidencia que no se ha crecido de forma natural, como ocurrió con la expansión de internet, sino más forzada. El segundo, la falta de marco normativo que esperamos se solucione pronto al menos a nivel europeo. Y, por último, no debemos dejar de pensar que otras tecnologías que están a la cola, serán también disruptivas y que pueden poner en peligro las propiedades de *blockchain*. Hablo en particular del *quantum computing*, que podría hacer repensar todos los sistemas basados en la criptografía.

10. Referencias

- Chen, S. *et al.* (2017). Using blockchain to improve data management in the public sector. *Digital McKinsey*. McKinsey&Company. Recuperado de <https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/using-blockchain-to-improve-data-management-in-the-public-sector>
- Cordero, M. (2018). Auditoría digital: el reto del siglo XXI. *Pre-supuesto y Gasto Público*. 91, 135-151.
- Dai, J. and Vasarhelyi, M. (2017). Toward Blockchain-Based Accounting and Assurance. *Journal of Information Systems*, Vol. 31 (3), 5-21.
- Forde, B. (2017, march, 31). Using Blockchain to keep public data public. [Entrada blog]. Recuperado de <https://hbr.org/2017/03/using-blockchain-to-keep-public-data-public>
- Grech, A. and Camilleri, A. F. (2017). Blockchain in Education. Luxembourg, Publications Office of The European Union. doi: 10.2760/60649
- Junestrand, S. (2018). A blockchain-based governance model for public services in smart cities. *Open Access Government*. Recuperado 5 octubre 2018, de <https://www.openaccessgovernment.org/a-blockchain-based-governance-model/52928/>
- Lander, L., Cooper, N. (2017). Promoting public deliberation in low trust environments; Australian use cases. *Social Science Research Network (SSRN)*. Recuperado 26 noviembre 2017, de <http://dx.doi.org/10.2139/ssrn.3077474>
- Orcutt, M. (2019). La apuesta de sustituir el efectivo por *blockchain* se decide en Japón. *MIT Technology Review*. Recuperado de <https://www.technologyreview.es/s/10900/la-apuesta-de-sustituir-el-efectivo-por-blockchain-se-decide-en-japon>
- Parlamento Europeo (2018). Tecnologías de registros distribuidos y cadenas de bloques: fomentar la confianza con la desintermediación. Resolución del Parlamento Europeo de 3 de octubre de 2018. P8_TA-PROV(2018)0373.
- Preukschat, A. (2017). Los fundamentos de la tecnología blockchain. En Preukschar, A. (Coords.), *Blockchain: la revolución industrial de internet*. Barcelona: Ediciones Gestión 2000.
- Resolución del Parlamento Europeo, de 3 de octubre de 2018, sobre las tecnologías de registros distribuidos y las cadenas de bloques: fomentar la confianza con la desintermediación. (2017/2712 (RSP)).
- The European Union Blockchain Observatory and Forum. (2018a). *Blockchain and the GDPR*. European Commission. Recuperado de https://www.eublockchainforum.eu/sites/default/files/reports/20181016_report_gdpr.pdf
- The European Union Blockchain Observatory and Forum. (2018b). *Blockchain for Government and Public Ser-*

vices. European Commission. Recuperado de https://www.eublockchainforum.eu/sites/default/files/reports/eu_observatory_blockchain_in_government_services_v1_2018-12-07.pdf

Toffler, A. (1970). *Future Shock*. Londres: Pan Books Great Britain.

Vivas Augier, C. (2017). Aplicaciones transversales de la blockchain. En Preukschat, A. (Coords.), *Blockchain: la revolución industrial de internet*. Barcelona: Ediciones Gestión 2000.

Voshmgir S. (2017). Disrupting governance with blockchains and smart contracts. Strategic Change. *John Wiley & Sons*, 26, 499-509. Recuperado de doi.org/10.1002/jsc.2150

Notas

- 1 La administración Trump borró datos del sitio web de la Casa Blanca. Volkswagen engañó en las pruebas de emisiones. Uber mostró información falsa sobre los conductores disponibles a los empleados del gobierno. Airbnb intentó limpiar más de 1.000 listas que violaban la ley del Estado de Nueva York, justo antes de compartir sus datos con el público como parte de un compromiso «para construir una comunidad abierta y transparente» (Forde, 2017).
- 2 Fuente: http://transparencia.gob.es/transparencia/transparencia_Home/index/Gobierno-abierto/bIVPlanAccion/Que_es_IV_Plan.html
- 3 Hashing es una función de encriptación que convierte un *input* (texto, imagen, etc.) en un código de longitud fija. El mismo *input* resulta en el mismo código, pero el mínimo cambio modificará completamente el código.
- 4 Siguiendo a Vivas Augier (2017), un *contrato inteligente* es un código informático que actúa como un acuerdo vinculante entre dos o más partes, sin necesidad de un intermediario, y se auto-ejecuta validando así el cumplimiento de las condiciones de las cláusulas. Un contrato inteligente tiene que ser totalmente digital, debe tener capacidad sobre activos digitales, debe poder validar el cumplimiento de las condiciones acordadas y debe ejecutarse de forma autónoma y automática.
- 5 El ECALab es una red interna de personal del TCE que está interesada en el uso innovador de la tecnología para la auditoría. También es un espacio físico en el que pueden someterse a ensayo las nuevas tecnologías así como un centro de aprendizaje. El ECALab está preparando el camino hacia la creación de servicios de datos adaptados a la auditoría en el TCE.