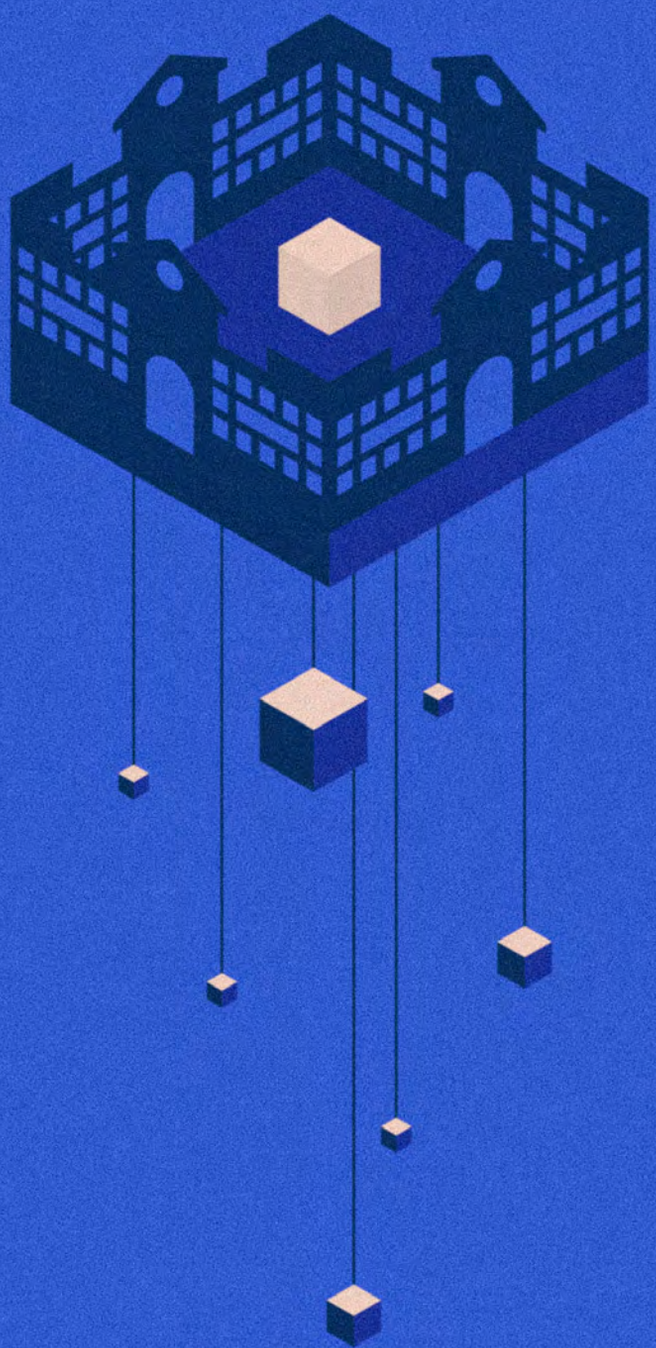
TIC 360 | 2019

Blockchain en la Universidad



crue Universidades Españolas

Depósito legal M-38148-2019
ISBN: 978-84-09-16302-1

Licencia

Me complace presentar la segunda edición del informe TIC 360°, que elabora Crue-TIC, que en esta ocasión está dedicado a la tecnología Blockchain.

Esta colección de informes TIC360° persigue proporcionar a las universidades documentos que les sirvan de referencia y ayuda para afrontar los retos a los que el Sistema Universitario Español tiene que dar respuesta en el ámbito de las TI.

En el anterior informe decíamos en su introducción: "Las tecnologías disruptivas son de importancia central en estos procesos de cambio. Desempeñan un papel decisivo en el rediseño del ecosistema universitario mediante la apertura de nuevas oportunidades para coordinar y vincular las diversas misiones, actividades y procesos de las universidades en formas nuevas y múltiples".

Entre estas tecnologías emergentes aparece de manera recurrente la denominada Blockchain (cadena de bloques), que, entre otras posibles aplicaciones, puede ser utilizada como una nueva forma de emitir, gestionar, verificar y validar las credenciales de la formación universitaria, es decir, una tecnología que puede revolucionar la manera de entender los títulos emitidos en las universidades de todo el mundo.

Esta transformación no solo supondrá un cambio en la forma en la que las universidades gestionan sus títulos, sino que está también ligada a la propia evolución de la oferta formativa universitaria y a la consideración de ésta por parte de los empleadores. El curriculum académico que es valorado para acceder al ámbito laboral tiende a ser configurado como una compilación de formación, competencias y habilidades cuyas acreditaciones estarán sujetas a procesos de validación que deben adaptarse a esta nueva estructura curricular. Además, en una sociedad cada vez más orientada hacia la digitalización, los mecanismos que permitan garantizar la veracidad de estas credenciales deben incorporar procesos digitales que los doten de la fiabilidad y la flexibilidad que demanda este nuevo escenario.

El diploma tradicional ha sido durante generaciones el único mecanismo de acreditación de la educación universitaria y la calificación base para el empleo. El título de Educación Superior aseguraba a los empleadores una disposición para el empleo de los egresados universitarios. Esta garantía se está debilitando en un contexto laboral donde el dominio de otras habilidades, las llamadas *soft skills*, es imprescincible para mejorar la incoporación de nuestros egresados a su primer empleo y también para su progreso profesional, expresando los empleadores, cada vez con mayor claridad, la necesidad de completar la preparación de los graduados con una formación complementaria en estas competencias, lo que exige a su vez la adaptación de los medios para su acreditación. La búsqueda de nuevas formas de emisión de estas credenciales tiene como objetivo disminuir esta brecha, reconociendo que el aprendizaje se lleva a cabo de maneras diversas y emitiendo nuevas formas de credenciales digitales que son apilables, portables, verificables y permanentes. Estas credenciales digitales incluyen títulos, certificados académicos y de la industria, licencias, insignias y microcredenciales.

Blockchain es una de las tecnologías disruptivas que están facilitando la transformación en la forma de entender las certificaciones académicas que son la evidencia que acompaña a todo egresado universitario.

Este escenario que he descrito es el que esta subyacente a los proyectos que dimanan de la Comisión Europea: Europass2, ESCO, caso de uso de diploma del *European Blockchain* Services Infrastructure (EBSI). Su importancia para las universidades españolas ha llevado a la sectorial CRUE TIC a una implicación directa en dichos proyectos y, en colaboración con la Administración General del Estado, a liderar el caso de uso de diploma del proyecto EBSI. Consideramos que nuestra participación decidida en estas iniciativas facilitará la mejor adecuación de nuestras universidades a un más que probable nuevo contexto de los mecanismos y procedimientos para la acreditación universitaria.

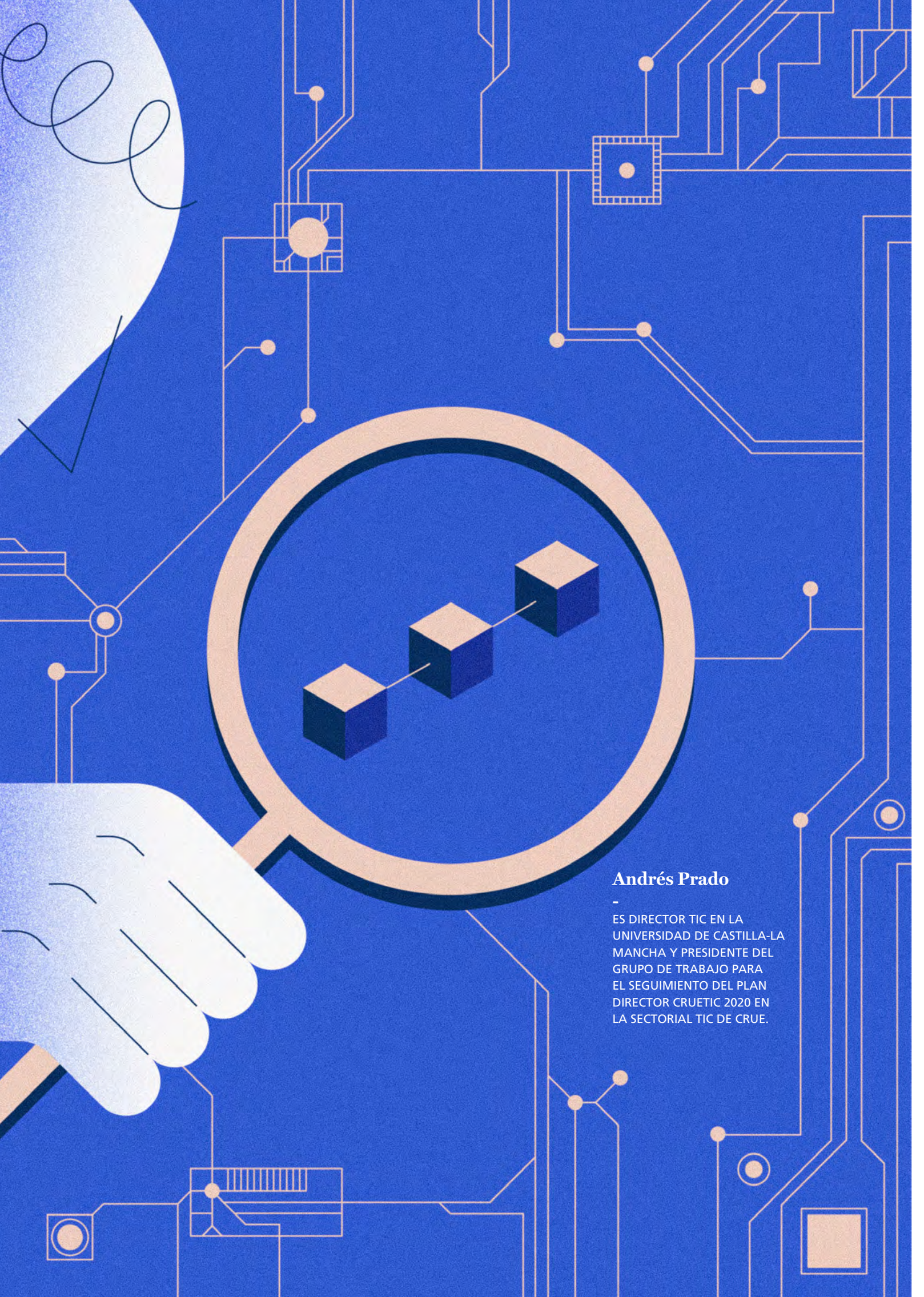
Como resultado del análisis de situación descrito, en el último trimestre de 2018 se decidió impulsar una prueba de concepto generando una red Blockchain denominada Blue (Blockchain Universidades Españolas) para desarrollar y desplegar servicios en ella.

Esta red permitirá la integración en el proyecto EBSI y en un futuro facilitará a los estudiantes agregar de manera complementaria a su certificación formativa convencional un registro distribuido que proporcionaría verificabilidad inmediata de forma integrada en su identidad digital, salvaguardando los requisitos de las regulaciones de protección de datos.

En todo caso, la aplicación de esta red es extensible a otros procesos administrativos universitarios, siendo su gran potencial digno de mención en el contexto del Espacio Europeo de Educación Superior, la movilidad internacional de los estudiantes, así como en la formación continua a lo largo de la vida.

El objetivo de este informe no es otro que proporcionar a los responsables y gestores de las universidades españolas la información básica y esencial necesaria que les permita comprender el potencial y alcance de esta tecnología Blockchain de manera que puedan diseñar sus estrategias en este ámbito y planificar sus actuaciones para incorporarse de la forma más eficaz posible a este nuevo escenario de universidad digital.

Juan Gómez Ortega
PRESIDENTE DE CRUE-TIC
RECTOR DE LA UNIVERSIDAD DE JAÉN



Andrés Prado

-

ES DIRECTOR TIC EN LA UNIVERSIDAD DE CASTILLA-LA MANCHA Y PRESIDENTE DEL GRUPO DE TRABAJO PARA EL SEGUIMIENTO DEL PLAN DIRECTOR CRUETIC 2020 EN LA SECTORIAL TIC DE CRUE.

1.1

EL ANÁLISIS

Análisis estratégico para la adopción de Blockchain en el Sistema Universitario Español

Andrés Prado
UNIVERSIDAD DE CASTILLA-LA MANCHA

En noviembre de 2008 un individuo identificado como Satoshi Nakamoto difunde en un foro de criptografía un documento en formato de paper académico denominado "Bitcoin: *A Peer-to-Peer Electronic Cash System*" (1). Siete años más tarde, la prestigiosa revista The Economist reconoce a Satoshi Nakamoto como merecedor del premio Innovation Awards 2015 en la categoría "No Boundaries"[1], destacando que Bitcoin podría alterar todo el sistema financiero tal y como se encuentra establecido hasta el momento. En el documento de presentación de los premios ese año falta una foto: la identidad de Satoshi Nakamoto es un misterio a día de hoy. Este halo de misterio que rodea sus comienzos es tan solo uno de los ingredientes que generan interés ante Bitcoin y su tecnología subyacente: Blockchain. La génesis de Blockchain es tan incierta como su futuro, si bien existe un amplio consenso en identificarla como una de las tecnologías con mayor capacidad de disrupción en la sociedad actual.

Bitcoin nace con el objetivo de generar un nuevo modelo de intercambio de moneda no sujeto al control de entidades centrales. La propuesta de Bitcoin parte de conceptos y tecnologías ya consolidadas como las redes *Peer-to-Peer* o los elementos criptográficos. Bitcoin basa su funcionamiento en el uso de un libro de registro donde quedan almacenados todos los movimientos que se realizan en torno a la moneda que gestiona. A diferencia de otros modelos de registro que dan fe de las transacciones realizadas, este libro de registro no se encuentra centralizado en un tercero de confianza, sino que el libro se encuentra distribuido en su totalidad. La confianza necesaria se traslada a la propia red, donde cada uno de los nodos participantes contienen una copia completa de ese libro de registro. Ese libro distribuido va incorporando nuevas entradas, pero cada una de ellas es cifrada utilizando información procedente de la anterior, generando de este modo una cadena de bloques de información vinculados consecutivamente. El tamaño de la cadena de bloques superó el Megabyte de información en 2010. En la actualidad supera los 238 MB[2] y las 365.000 transacciones diarias. La seguridad proporcionada tanto por los algoritmos de criptografía utilizados como por el propio modelo conceptual, cuya seguridad se fortalece con el propio crecimiento, ha impedido que la cadena de bloques haya sido comprometida en todo este tiempo.

Si bien Bitcoin irrumpe como un modelo disruptivo en el ámbito financiero, el concepto y la tecnología subyacente se han demostrado exportables a muchos otros ámbitos. En el fondo, el libro de registro distribuido diseñado para permitir el seguimiento fehaciente de las transacciones de monedas virtuales es perfectamente válido para realizar el seguimiento de transacciones de otros bienes materiales o inmateriales. Es precisamente este potencial de Blockchain

[1] https://events.economist.com/events-conferences/asia/innovation-awards-summit-2015/
[2] Fuente: https://www.Blockchain.com/

como tecnología aplicable a una multitud de sectores lo que permite identificarla como elemento disruptivo, llegando incluso a comparar la situación actual de Blockchain con la situación de Internet a principios de los años 90.

Si verdaderamente Blockchain tiene esa capacidad de cambiar modelos en el ámbito económico, en el industrial o incluso en el organizativo, ¿tiene potencial de impacto en el entorno universitario? ¿existen iniciativas piloto en este ámbito a nivel nacional e internacional? ¿se encuentra el Sistema Universitario Español preparado para la adopción temprana de esta tecnología? Este informe, siguiendo la línea editorial planteada en la serie TIC360, no pretende aportar una única respuesta a estas preguntas, sino compartir reflexiones en torno a las mismas que faciliten a las universidades un posicionamiento en torno a una tecnología que plantea un nuevo paradigma de relaciones.

LA PROPUESTA DE VALOR DE BLOCKCHAIN

La aportación de valor de Blockchain está basada en sus principales características. En primer lugar, su naturaleza distribuida y compartida no solo aporta mayor seguridad evitando un único punto de fallo, sino que evita la necesidad de establecer un tercero de confianza. Lo que en Bitcoin permite operar con criptomonedas sin la necesidad de una institución económica central, en el caso de la aplicación de tecnología Blockchain, minimizaría o eliminaría la actividad de agentes o instituciones de intermediación en sectores donde actualmente su participación es necesaria para garantizar el funcionamiento de ese sector.

Evidentemente, la supresión de las actividades de intermediación no viene determinada exclusivamente por la distribución de la información sino, sobre todo, por su inmutabilidad. La vinculación de un bloque de información en Blockchain a la información del anterior impide la modificación de la información ya incorporada a la cadena, puesto que el cambio de un bloque repercutiría directamente en todos los posteriores. Blockchain, por otro lado, define mecanismos de consenso entre los nodos de la red para la incorporación de un nuevo bloque de información. La alteración, por tanto, de un bloque en el momento de su incorporación exigiría al "atacante" tomar el control de más de la mitad de los nodos de la red, lo que se hace cada vez más complejo con el incremento de tamaño de la propia red.

El tercer factor que permite aportar valor a Blockchain en sus múltiples escenarios de uso es la trazabilidad de la información. A diferencia de los habituales modelos de uso de las bases de datos distribuidas, Blockchain opta por replicar toda la información en cada uno de los nodos de la red que integran la plataforma. Todos los nodos, por tanto, disponen de capacidad de verificar todas las transacciones realizadas en el registro de información distribuido que comparte con el resto de nodos de la plataforma.

Además de las características derivadas del diseño de la tecnología Blockchain y sus componentes tecnológicos, existen dos elementos adicionales cuyo análisis es fundamental para la incorporación de esta tecnología a un sector, empresa o institución. Por un lado, los denominados Smart Contracts, que facilitan la generación automática de una transacción incorporada en el registro distribuido en función del cumplimiento de una serie de condiciones que perfectamente pueden darse en el entorno externo de la cadena de bloques. Esta funcionalidad permite que, una vez analizadas las condiciones y automatizada mediante programación de la generación de un evento cuando estas se produzcan, la transacción se realiza y registra de forma inmediata. En general, el uso de Smart Contracts permitirá una reducción de tiempos y de coste en sectores donde se requieren pasos intermedios para, por ejemplo, generar un ingreso debido al cumplimiento de unas condiciones externas a la propia compañía.

Por último, es necesario destacar que la taxonomía de las redes Blockchain es diversa. Además del uso de variantes en la propia tecnología o de criterios de diseño de la propia red, es relevante destacar, de cara a la adopción de Blockchain en un sector concreto, el nivel de apertura de la propia red. Si bien Bitcoin es una red pública, es factible utilizar la tecnología Blockchain en entornos privados, distinguiendo así las redes permisionadas de las no permisionadas. Una red permisionada facilita el uso de Blockchain en un entorno cerrado de uno o varios agentes con capacidad de lectura y escritura en la propia red. A diferencia de las redes no permisionadas, las redes permisionadas se encuentran inaccesibles para agentes externos que requieren de un permiso incluso para acciones de lectura. Este modelo es especialmente relevante para la incorporación de Blockchain en una entidad o en un ecosistema de entidades, donde existe información y transacciones vinculadas a esa información que ha de mantenerse en un entorno no accesible públicamente.

ANÁLISIS DEL ENTORNO EXTERNO

Si bien el objeto de reflexión de este informe es la potencial adopción de Blockchain en el Sistema Universitario Español, es conveniente identificar referencias en otros sectores y los factores externos que tienen influencia en esta adopción.

Casos de uso en otros sectores

El sector financiero está siendo evidentemente afectado por la primera aplicación propuesta sobre Blockchain: en octubre de 2018 se superó el número de 2.000 criptomonedas en circulación[3]. No obstante, más allá de las criptomonedas las entidades financieras están viendo con respeto otras aplicaciones de esta tecnología en un sector con un grado de intermediación y centralización muy elevado. Comienzan también a aparecer iniciativas comerciales, como la emisión de bonos con tecnología Blockchain anunciada en septiembre de 2019 por el Banco Santander (2).

Las pruebas de concepto, experiencias piloto y proyectos con diferente grado de impacto en negocio se han multiplicado en los últimos años tanto en número como en sectores afectados. Los sectores industriales tradicionales están ya invirtiendo en Blockchain de forma decidida. En el sector del automóvil, por ejemplo, los fabricantes, de forma individual o constituyendo consorcios, están invirtiendo en la aplicación de Blockchain para sus líneas de evolución tecnológica, como el desarrollo de concepto de coche autónomos, o para hacer más eficientes procesos actuales vinculados a ese sector, como el pago de seguros en función del uso real.

El sector de la logística es otro de los ámbitos que más está impulsando la adopción de Blockchain, explotando el valor de estas plataformas en términos de trazabilidad. Las iniciativas van desde proyectos para el control de la cadena de suministro hasta proyectos de generación de plataformas dirigidas a ecosistemas de empresas vinculadas comercialmente.

Además de la aplicación en sectores donde la información está vinculada a la trazabilidad de elementos tangibles, Blockchain está aportando soluciones también en sectores donde el elemento clave es la información. Iniciativas en entornos de la salud apuestan no por integrar los datos personales en la cadena de bloques sino por utilizar Blockchain como mecanismo para identificar esos registros así como la posibilidad o no de acceder a los mismos, como en el caso de Estonia.

Factores externos

Más allá del propio entorno de Educación Superior, existen factores que están determinando la evolución y la adopción general de Blockchain en los diferentes sectores productivos. Este informe propone una reflexión en torno a factores políticos, económicos, sociales, tecnológicos, ecológicos y legales, proponiendo así un breve análisis PESTEL.

Factores Políticos

Si, como parece, Blockchain es una de las tecnologías actuales llamadas a cambiar la sociedad de un modo equivalente a cómo lo ha hecho Internet en las últimas dos décadas, no es extraño que este término comience a ser utilizado en ámbitos políticos de esfera nacional e internacional.

Por un lado, la aparición de Bitcoin y otras criptomonedas comienza a impulsar debates y decisiones políticas que van desde declaraciones presidenciales de desprestigio, como las realizadas en verano de 2019 por Donald Trump[4], hasta la posible emisión de criptomoneda por parte de otra potencia mundial como China[5], la Chinese Central Bank Digital Currency o CBDC. En el panorama internacional, existen también decisiones abordadas por países de naturaleza muy diferente a estas dos potencias: Nueva Zelanda, por ejemplo, reconoce desde este verano el pago de salarios en criptomonedas (3). La OCDE identificaba en 2018 hasta 200 iniciativas impulsadas por gobiernos de hasta 46 países en todo el mundo (4). Debates abiertos, proyectos y decisiones que comienzan a tomarse impulsados, entre otros, por el anuncio de lanzamiento de una criptomoneda propia por parte de otra potencia, en este caso empresarial, como Facebook con su "Libra"[6].

Por otro lado, el potencial de Blockchain más allá de la capacidad de generar nuevos modelos económicos basados en criptodivisas, no está pasando desapercibido tampoco para los diferentes ámbitos políticos. En el entorno municipal, las ciudades comienzan a apostar por el desarrollo de proyectos basados en Blockchain para mejorar los servicios ofertados a la ciudadanía. Tal es el caso de Hamburgo que asegura estar probando esta tecnología en ámbitos como el energético, la logística o la seguridad, con el apoyo de universidades y empresas cercanas.

A nivel nacional, por primera vez la campaña electoral de mayo de 2019 incluyó un debate con participación de los cuatro partidos políticos con mayor representación centrado en el uso de Blockchain[7],

[3] https://graphics.reuters.com/CRYPTO-CURRENCIES-CONFLICTS/0100818S2BW/index.html
[4] https://twitter.com/realDonaldTrump/status/1149472282584072192
[5] https://info.binance.com/en/research/marketresearch/CBDC.html
[6] https://libra.org/es-LA/white-paper/#introduction
[7] https://www.Blockchaineconomia.es/debate-Blockchain-politicos-trending-topic/

donde hubo consenso en la necesidad de impulsar esta tecnología. En el entorno europeo la decisión ya está tomada. Blockchain se considera una pieza fundamental para la creación del Mercado Único Digital. Más aún, la UE pretende posicionar a Europa al frente de la innovación basada en Blockchain y lo está confirmando con acciones concretas. En mayo de 2018 se constituyó la *European Blockchain Partnership* que está comenzando el desarrollo de una infraestructura de servicios pan-europea utilizando tecnología Blockchain, denominada *European Blocockchain Services Infrastructure* o EBSI. Como veremos más adelante, el impacto en el sector universitario de estas actuaciones es directo y Crue ya está dando pasos para alinearse con ese reto.

Factores Económicos

Como se comentaba anteriormente, Blockchain está impactando en el sector financiero de forma cada vez más profunda. Este impacto así como su potencial en otros sectores han generado un creciente interés inversor en los últimos años, alcanzándose su máximo crecimiento el pasado año 2018 cuando se superaron los 4.100 millones de dólares invertidos en Blockchain (5). No en vano, el Foro Económico Mundial ya estimaba en 2015 que el 10% del producto interior bruto mundial estaría almacenado en Blockchain para el año 2027.

La posibilidad de una nueva etapa de recesión económica más o menos pronunciada en el futuro próximo está sirviendo también para impulsar el desarrollo y la aplicación de Blockchain. A nivel empresarial, las grandes compañías con actividad en sectores no solo financiero o tecnológico comienzan a desarrollar proyectos con altas expectativas de reducción de costes, incluso por delante de las expectativas de cambio de los modelos de negocio tradicionales.

Factores Sociales

En el propio origen de Bitcoin se plantea una revolución social: la descentralización de la economía y la búsqueda por evitar las entidades financieras centrales. Toda la decisión en manos del individuo, sin intermediarios. Ciertamente, la situación actual no es aún de revolución social, pero en los últimos meses comienzan a atisbarse iniciativas que, si bien quizá no supongan una revolución, impulsarán cambios en los modelos sociales que conocemos. La entrada en el mundo de las criptomonedas de ese otro país virtual que se llama Facebook puede, efectivamente, revolucionar los medios de pago e intercambios económicos.

De nuevo, más allá del ámbito financiero, el potencial de Blockchain aplicado a otros sectores como el industrial, el logístico, la comunicación, la sanidad o la educación podrá suponer verdaderos cambios de modelos de negocio, la aparición de otros nuevos modelos y, también, el empoderamiento del individuo a través del control de su información. Si en épocas anteriores han aparecido revoluciones sociales como respuesta al poder abusivo del estado frente al individuo, la sociedad actual se plantea ya si este poder abusivo no se está ejecutando en la actualidad por las grandes corporaciones que gestionan datos personales a través de sus servicios digitales. La aplicación de Blockchain podría mejorar el limitado control que ahora mismo tienen los individuos de sus datos digitales.

Factores Tecnológicos

A tenor de todo lo expuesto hasta el momento, puede parecer que Blockchain ha emergido como remedio a muchas de las dificultades del sistema socioeconómico actual. Sin embargo, no deja de sorprender las elevadas expectativas que se están depositando en una tecnología o un modelo tecnológico que se encuentra en una situación de inmadurez reconocida .Las estimaciones realizadas por la consultora Gartner exponen que Blockchain no habrá superado los problemas tecnológicos que actualmente plantea hasta 2023 (6) y que no alcanzará un nivel de madurez que permita su uso escalable tecnológica y operacionalmente hasta 2028. (7).

La propia naturaleza de los conceptos sobre los que se basa el modelo Blockchain, el replicado de toda la información entre todos los nodos que componen la red, supone un reto para el rendimiento y escalabilidad de la propia red. Solventar el problema de escalabilidad en Blockchain será fundamental para la adopción en entornos donde las transacciones deban realizarse en tiempo real y a un elevado nivel de concurrencia. Debates al respecto del tamaño de los bloques o del protocolo de consenso utilizado están sobre la mesa al objeto de mejorar el rendimiento en grandes redes (8).

Por otro lado, la aparición de oferta por parte de los grandes actores tecnológicos de plataformas *Blockchain as a Service* (BaaS) permiten en la actualidad a las empresas y administraciones lanzar proyectos y pruebas de concepto de adopción de Blockchain

minimizando el coste de inversión y el riesgo que supone el despliegue de una infraestructura dedicada a una tecnología en fase temprana de desarrollo. Plataformas BaaS como IBM Blockchain Platform[8], Amazon Managed Blockchain[9], Oracle Blockchain Platform[10] o Azure Blockchain Service[11] son ejemplos del desarrollo de esta oferta por parte de las grandes corporaciones tecnológicas. De forma adicional, están surgiendo iniciativas BaaS desde otro tipo de proveedores tecnológicos de menor transversalidad, pero con alto potencial de impacto. Es el caso de la oferta BaaS de Salesforce anunciada en mayo de 2019, donde precisamente uno de los casos de uso mencionados en su nota de prensa (9) es una universidad que identifica valor en el intercambio de información académica entre alumnos e instituciones.

Es necesario destacar también la necesidad de evolución en materia de interoperabilidad entre diferentes cadenas de bloques. La adopción de Blockchain será progresiva en diferentes sectores e incluso en diferentes corporaciones con conjuntos de empresas o administraciones. Será necesario, por tanto, establecer mecanismos que faciliten el intercambio de información entre cadenas de bloques diferentes, cuestión que en la actualidad aún está pendiente de resolución.

Factores Ecológicos

Entre los muchos ámbitos sobre los que la adopción progresiva de Blockchain tiene un impacto directo se encuentra el medioambiental. Se trata quizá de uno de los factores menos analizados en este momento de expectaciones crecientes. La fortaleza de seguridad de la cadena de bloques de información se fundamenta en los algoritmos de cifrado utilizados, lo que requiere una cada vez más elevada capacidad de cómputo y, por consiguiente, requiere de un consumo eléctrico creciente. Los datos actuales solo para el caso de Bitcoin ya son relevantes: en 2017 el consumo eléctrico requerido tan solo para el minado de esa cadena de bloques supuso un 0,13% del consumo eléctrico global. Con esos datos, el consumo de Bitcoin es superior al de 159 países. Visto de otro modo, si Bitcoin fuera un país se situaría en el número 61 dentro del ranking del consumo eléctrico mundial (10).

El sector energético es otro de los más activos en la adopción de Blockchain, pero también aporta iniciativas que, de forma directa, impulsan el consumo de energía renovable. En enero de 2019 Iberdrola anunció un proyecto de aplicación de esta tecnología para garantizar que la energía suministrada a sus consumidores provenía de fuentes completamente renovables (11).

Factores Legales

Blockchain aparece como una tecnología disruptiva, con potencial para cambiar modelos de negocio y hasta sistemas económicos. Los aspectos legales, por tanto, serán otro de los factores a considerar especialmente en esas nuevas áreas o modelos de aplicación. No obstante, de nuevo la naturaleza de Blockchain aporta retos a solventar dentro del marco jurídico existente. La jurisdicción, la identificación y el respeto a los derechos humanos son tres de las cuestiones más relevantes identificadas por Naciones Unidas (12).

En un modelo distribuido como el de Blockchain, sin una base de datos centralizada ni una entidad central, la identificación de la jurisdicción aplicable no es inmediata. En todo caso, no se trata de un tema absolutamente nuevo, puesto que Internet ha roto las barreras geográficas en transacciones entre usuarios distribuidos por el mundo.

La capacidad de interactuar en cadenas de Blockchain de forma completamente anónima es otro de los retos a los que debe enfrentarse el marco jurídico. Para el caso de las criptomonedas más extendidas, la identificación del sujeto que realiza las transacciones se realiza en base a la posesión de la clave privada que permite realizar esas transacciones. La absoluta trazabilidad que aporta Blockchain se pierde, precisamente, en la identificación del usuario.

Esa trazabilidad que facilita Blockchain, a través de la inmutabilidad de la información consignada en la cadena de bloques, supone también un reto frente a la salvaguarda de derechos fundamentales. La información incorporada en una cadena de bloques no puede ser borrada, lo que presenta serios problemas en derechos como el de la privacidad y la protección de datos personales.

En todo caso, los retos legales que Blockchain genera se van multiplicando conforme la tecnología se va adoptando en diferentes sectores. La regulación de las criptomonedas o la regulación de los contratos inteligentes son retos similares a los que debe afrontar el sistema educativo en su adopción de Blockchain como soporte en la certificación académica.

ANÁLISIS DEL SECTOR

Este informe propone adoptar uno de los modelos sistemáticos de análisis estratégico más extendido para identificar los elementos clave en la adopción de Blockchain en el ámbito del Sistema Universitario Español: el modelo de las 5 fuerzas propuesto por Michael Porter (13). Este modelo contempla el potencial

[8] https://www.ibm.com/Blockchain/platform
[9] https://aws.amazon.com/es/managed-Blockchain/
[10] https://www.oracle.com/cloud/Blockchain/
[11] https://azure.microsoft.com/en-us/services/Blockchain-service/

de una industria siempre sujeta a la interacción de cinco grandes fuerzas: el nivel de competencia existente, la capacidad de aparición de nuevas empresas, el poder o influencia de proveedores y clientes, y la existencia de productos o soluciones alternativas.

Competencia

Blockchain es un entorno de alto interés académico para las universidades. En el sistema universitario español el número de titulaciones de posgrado relacionadas de forma directa con Blockchain se ha multiplicado en los últimos tres años. Universidades públicas y privadas, así como escuelas de negocios están ofertando titulaciones sobre Blockchain y Smart Contracts, bien desde el plano tecnológico o bien el plano de negocios, especialmente en forma de máster. Además de esta oferta académica, el propio sector universitario está iniciando proyectos de adopción, tanto de forma individual por parte de universidades concretas, como de forma conjunta bajo el impulso de la sectorial TIC de Crue.

En las jornadas sobre Blockchain celebradas en la sede de Málaga de la Universidad Internacional de Andalucía en octubre de 2018[12], la Universidad Carlos III de Madrid expuso sus primeros pasos con Blockchain, a la que posteriormente se unieron iniciativas en universidades como la Universidad San Pablo-CEU o la Universidad Pontificia Comillas. La jornada permitió también identificar al conjunto de proveedores con mayor actividad e interés en soluciones para el ámbito universitario basadas en Blockchain. Empresas como Cibernos, Ibermática, IBM o SmartDegrees aportaron su visión sobre soluciones centradas especialmente en los certificados académicos.

El evento celebrado en Málaga tuvo consecuencias también en el enfoque conjunto de las universidades frente a Blockchain, puesto que supuso un punto de inflexión para el lanzamiento de la iniciativa conjunta de Crue y RedIRIS denominada Blue (Blockchain Universidades Españolas).

En cualquier caso, en un entorno compuesto por 76 universidades, las iniciativas e incluso los proveedores con ofertas en un estado de madurez razonable son aún limitados. Se trata, por tanto, de un mercado con un alto potencial. Posiblemente un apetecible Océano Azul (14).

Amenaza de nuevos agentes

Un sector con un potencial tan alto como el descrito anteriormente está expuesto a la entrada de nuevos agentes que traten de capitalizar el valor en juego. La irrupción de nuevos competidores depende mucho de las barreras de entrada que se puedan encontrar en el sector. La barrera tecnológica, el conocimiento e incluso el propio estado de madurez de Blockchain y sus elementos asociados, puede parecer demasiado alta como para temer una entrada masiva de soluciones que compitan en el mercado universitario. No obstante, conviene destacar de nuevo la existencia en la actualidad de soluciones BaaS que facilitarían el despliegue de soluciones verticales para el sector universitario con un desacople razonable respecto de la capa de Blockchain. Con estos factores, ha de considerarse seriamente la entrada de nuevos actores en los próximos años, tratando de cubrir las necesidades u opciones que la adopción de Blockchain pueda generar.

Influencia de proveedores

Si bien Blockchain es considerada aún como una tecnología emergente, el impulso que está sufriendo este ecosistema de tecnologías ha favorecido la aparición de proveedores de nicho así como la participación de grandes compañías tecnológicas. El informe que sobre el estado de estas tecnologías ha publicado Gartner en 2019 (7) identifica más de 120 proveedores de referencia en diferentes ámbitos de tecnologías relacionadas con Blockchain. En el ámbito de educación, la consultora HolonIQ publicó en enero de 2019 un informe donde identifica hasta 50 empresas aportando soluciones al mercado de la educación sobre tecnología Blockchain (15). Aunque la presencia de estos proveedores en el mercado español y en su sector universitario es muy limitada, es destacable la presencia de compañías como Amazon, Google, IBM, Intel, Microsoft u Oracle. El interés de estas compañías en el sector educativo es cada vez más intenso. Su presencia gana peso y actividad progresivamente, lo que podría facilitar una integración hacia delante de estas compañías, que tendrían capacidad de ofrecer servicios verticalizados a este sector.

En este momento, la decisión de adopción de un proveedor cualquiera que sea el modelo de adopción de Blockchain escogido por una o varias universidades es una decisión de impacto. El nivel de madurez inicial de estas tecnologías, en las que se estima que el 90% de proyectos actuales necesitarán un reemplazo en 2021 (16), implica que el coste de cambio de proveedor es elevado y, por consiguiente, su influencia es alta en el sector.

[12] https://eventos.crue.org/event_detail/23225/detail/jornada-Blockchain.html

Influencia de clientes

El número de universidades españolas con servicios basados en Blockchain es reducido en la actualidad. Si bien se espera que crezca progresivamente, su influencia individual sobre el sector no tendrá el peso que pueda obtener a través de una iniciativa colectiva como la impulsada en estos momentos por la sectorial TIC de Crue: Blue. Es en este contexto de demanda agregada y servicios compartidos donde la influencia de las universidades como clientes finales puede ser decisiva en el devenir de las soluciones basadas en Blockchain para el ámbito educativo. Esta influencia podría permitir adecuar *roadmaps* de soluciones adaptadas a las necesidades priorizadas por las universidades y facilitaría impulsar conceptos como la apertura y la interoperabilidad.

Sustitutivos

"Blockchain es la Internet del futuro" es una frase habitual en los artículos que identifican esta tecnología como disruptiva. Sin embargo, en la actualidad no todas las comunicaciones utilizan Internet ni todos los servicios que en la actualidad soportan comunicaciones a través de Internet adoptaron esa solución en el nacimiento de la red de redes. Además de identificar adecuadamente el nivel de riesgo asumido por una universidad en la adopción temprana de Blockchain, es necesario identificar claramente el ámbito de adopción. Soluciones tecnológicamente más maduras pueden ser más adecuadas para un buen número de escenarios. Incluso en otros casos, los requisitos de esos escenarios pueden no encajar con las características de Blockchain, como la imposibilidad de borrado de información, o con su nivel de rendimiento, en ámbitos donde la concurrencia o el volumen de transacciones por segundo requerido sea alto.

Análisis interno

El modelo más utilizado para realizar un análisis estratégico interno identifica debilidades, amenazas, fortalezas y oportunidades en un cuadrante denominado DAFO. Este informe propone un análisis en esas cuatro dimensiones desde el punto de vista de la adopción de Blockchain en el sistema universitario español.

Debilidades

Las universidades han sido tradicionalmente un buen sector para el impulso de nuevas tecnologías y servicios tecnológicos. No obstante, la adopción individual por parte de universidades de tecnologías con un nivel de madurez tan temprana como Blockchain es, en estos momentos, bastante moderado. La limitación de recursos económicos, materiales y humanos en los servicios de tecnología de las universidades, así como la gran demanda de nuevos servicios digitales con un alto nivel de disponibilidad y calidad por parte de la comunidad universitaria, deja poco espacio para asumir dedicación y riesgo en la adopción de Blockchain.

La adopción conjunta o colaborativa puede ser una solución razonable a la debilidad actual. En cualquier caso, merece la pena destacar también la limitada experiencia en el uso de servicios compartidos y gobernados por las universidades en su conjunto. Son varias las iniciativas en este sentido. Las más fructíferas se han desarrollado en colaboración con RedIRIS, que asimismo ha destacado la limitación de recursos para no solo la puesta en marcha sino, sobre todo, la operación y sostenibilidad de servicios compartidos destinados al ámbito científico y académico.

Amenazas

De nuevo, la tecnología aparece como factor destacado. El grado incipiente de madurez hace de la tecnología un elemento de riesgo en la adopción de soluciones basadas en Blockchain. Por otro lado, el bajo grado de estandarización y, por tanto, la limitada interoperabilidad entre diferentes cadenas de bloques son elementos que facilitan situaciones a evitar como las de "secuestro tecnológico". Estas situaciones pueden agravarse si alguna de las grandes compañías tecnológicas decide en algún momento irrumpir en el sector de Educación con soluciones basadas en Blockchain. Parece oportuno recordar que la comunidad de estudiantes universitarios españoles está distribuida entre las 87 universidades españolas, pero un elevado porcentaje de esta comunidad se encuentra en lugares comunes como Facebook, que comenzará de forma inminente a ofrecer servicios basados en Blockchain.

Los servicios que sobre Blockchain se encuentran más maduros o al menos más extendidos son los ofertados en el sector financiero, en el ámbito de las Fintech. No en vano, el primer servicio ofertado por Facebook es Libra, una criptomoneda. El sector bancario español comienza también a impulsar esta tecnología entre sus soluciones. Este impulso podría asimismo beneficiar el despliegue de soluciones en el ámbito universitario, aunque será en ese caso necesario medir adecuadamente el nivel de autonomía en la gobernanza de esas soluciones, clave para la adaptación a las heterogéneas situaciones y necesidades del conjunto del sistema universitario.

Fortalezas

Posiblemente la gran fortaleza del sistema universitario español en su ámbito tecnológico es la colaboración, cohesionada y proactiva. La sectorial Crue-TIC aglutina un conjunto de grupos de trabajo integrados por representantes de las universidades españolas que comparten de forma desinteresada esfuerzos para obtener resultados reutilizables por el sistema. Esta actividad originó la primera jornada de trabajo coordinada por el grupo de Dirección TI de las universidades españolas[13], origen de la iniciativa Blue. Esta iniciativa, la prueba de concepto de adopción de Blockchain en actividades universitarias, es en sí misma evidencia de la fortaleza del sistema cuando adopta este tipo de modelos de despliegues colaborativos.

Es necesario destacar en este punto la fortaleza de la colaboración con RedIRIS, la red nacional de I+D que no solo facilita conectividad entre las universidades españolas, sino que ha sido capaz de establecerse como punto neutro ideal para la prestación de servicios tecnológicos compartidos. La iniciativa Blue vuelve a ser un resultado de esta colaboración de éxito donde también destacan los servicios ya establecidos de identificación como SIR[14], de movilidad como eduroam[15] y otros de reciente despliegue en el ámbito de la interoperabilidad como NISUE[16].

Oportunidades

Si el contexto tecnológico no puede aún considerarse una oportunidad, aunque posiblemente haya que incorporarlo en este ámbito en una revisión de este análisis dentro de relativamente poco tiempo, el contexto político, más allá de las situaciones coyunturales, parece propicio a la adopción de tecnologías innovadoras y de potencial disruptivo como Blockchain. En el ámbito nacional ya se ha comentado en este informe el consenso en torno al impulso de Blockchain, pero es en el entorno europeo donde este contexto parece aún más favorable. La iniciativa de Mercado Único Digital[17], prioridad para la Unión Europea en estos momentos, ha identificado ya a Blockchain como una de las tecnologías a impulsar y donde Europa puede posicionarse estratégicamente a nivel mundial. Este impulso pasa por iniciativas como el EBSI[18] que con cuatro millones de euros a invertir entre 2019 y 2020 ha seleccionado cuatro casos de uso, siendo uno de ellos el de las certificaciones académicas.

El entorno social es también favorable a iniciativas que aporten y evidencien más seguridad sobre certificaciones realizadas por las distintas administraciones y, entre ellas, las universidades. Iniciativas que desde las universidades apuesten por incrementar la seguridad y favorecer el intercambio controlado de información académica permitirán satisfacer expectativas de mejora en estos ámbitos demandadas, en general, por parte de la sociedad en su conjunto.

Conclusiones

Este informe, del mismo modo que los informes ya realizados en la serie TIC360, no pretende ofrecer una visión única ni aportar una directriz a seguir por cada una de las universidades, sino servir como punto de partida para reflexiones y debates necesarios. En ese sentido, las conclusiones que se aportan nacen como consecuencia del análisis realizado y han de considerarse en ese sentido.

01

Las aplicaciones de soluciones basadas en Blockchain afectan potencialmente a la mejora de las diferentes misiones universitarias. No solo el ámbito de gestión académica podría beneficiarse en casos como las certificaciones, sino que la potencial mejora en la gestión de la propiedad intelectual puede beneficiar de forma inmediata a otros ámbitos universitarios como el científico.

02

La adopción de soluciones basadas en Blockchain dentro del sistema universitario español, en su conjunto o a nivel discrecional entre sus universidades, ha de contemplar el riesgo asumido que deriva del nivel de madurez de la tecnología utilizada. Será necesario identificar un modelo evolutivo sostenible que permita una evolución tecnológica que tendrá lugar a corto plazo.

[13] http://tic.crue.org/grupos-de-trabajo/direccion-de-ti/
[14] https://www.rediris.es/sir/
[15] http://www.rediris.es/servicios/eduroam/
[16] http://www.rediris.es/nisue/
[17] https://ec.europa.eu/commission/priorities/digital-single-market_es
[18] https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/EBSI

03

Blockchain no es la solución a todas las necesidades tecnológicas. Es necesario identificar claramente el valor de una solución basada en Blockchain en función de las propias características de esta tecnología y adoptarla solo en los casos donde el valor aportado permita asumir los riesgos de adopción.

04

En un escenario como el actual, donde hasta la propia tecnología llamada a ser disruptiva aporta un no despreciable grado de incertidumbre, es necesario poner en valor una de las grandes fortalezas del sistema universitario: la colaboración. La apuesta por infraestructuras y servicios compartidos y gobernados de forma conjunta por las universidades se visualiza como la que aporta mayores garantías de sostenibilidad.

Referencias

1. Nakamoto, Satoshi. Bitcoin: A Peer-to-Peer Electronic Cash System. [Cryptography Mailing list at https://metzdowd.com.] s.l. : Cryptography Mailing list at https://metzdowd.com., 2009.

2. Banco Santander. santander.com. Sala de Comunicación. [En línea] 12 de Septiembre de 2019. [Citado el: 18 de Octubre de 2019.] https://www.santander.com/csgs/Satellite/CFWCSancomQP01/es_ES/Corporativo/Sala-de- comunicacion/2019/09/12/Santander-lanza-el-primer-bono-con-tecnologia-Blockchain-de- principio-a-fin.html.

3. Fernández, Covadonga. Tras el presupuesto de bienestar, la primera ministra de Nueva Zelanda autoriza los salarios en criptomonedas. [Observatorio Blockchain] 14 de Agosto de 2019.

4. Berryhill, J, Bourgery , T y Hanson , A. Blockchains Unchained: Blockchain Technology and its Use in the Public Sector. Paris : OECD Publishing, 2018. OECD Working Papers on Public Governance. 19934351 .

5. CB Insights. Blockchain Trends in Review. 2019.

6. Gartner. Blockchain Technology Spectrum: A Gartner Theme Insight Report. Stamford : s.n., 2018.

7. Hype Cycle for Blockchain Technologies, 2019. 2019.

8. Blenkinsop, Connor . Coin Telegraph. [En línea] 22 de 08 de 2018. [Citado el: 13 de 09 de 2019.] https://cointelegraph.com/explained/Blockchains-scaling-problem-explained.

9. Salesforce. Salesforce Introduces the First Low-Code Blockchain Platform for CRM. Press and News. [En línea] 05 de 2019. [Citado el: 13 de 09 de 2019.] https://www.salesforce.com/company/news-press/press-releases/2019/05/192915-i/.

10. Martinez, Peter. Bitcoin mining consumes more energy than 159 countries. CBS News. [En línea] 27 de 11 de 2017. [Citado el: 13 de 09 de 2019.] https://www.cbsnews.com/news/bitcoin- mining-energy-consumption/.

11. Iberdorla. Iberdrola uses Blockchain to guarantee that the energy it supplies to consumers is 100% renewable. Iberdrola.com Press Room. [En línea] 14 de 01 de 2019. [Citado el: 13 de 09 de 2019.] https://www.iberdrola.com/press-room/news/detail/iberdrola-uses-Blockchain-guarantee-that-energy-supplies-consumers-100-renewable.

12. Legal Aspects of Blockchain. Naves, Jeroen , y otros. s.l. : MIT Press Journals, 2019, Vols. 12:3-4.

13. How Competitive Forces Shape Strategy. Porter, Michael. s.l. : Harvard Business Publishing, Marzo de 1979, Harvard Business Review.

14. Blue ocean strategy. Mauborgne, R y Kim, W C. s.l. : Harvard Business Publishing, Octubre de 2004, Harvard Business Review, págs. 76-84.

15. HolonIQ. Education Blockchain 50. 2019.

16. Gartner. Gartner.com. Newsroom. [En línea] 03 de Junio de 2019. [Citado el: 15 de Septiemrbe de 2019.] https://www.gartner.com/en/newsroom/press-releases/2019-07-03-gartner-predicts-90--of-current-enterprise-Blockchain.

Antonio Tenorio
ES EL INVESTIGADOR PRINCIPAL DE DECENTRALIZED SCIENCE Y PROPIETARIO DE LA COMPAÑÍA EN LA QUE PARTICIPA EN EL PROYECTO LEDGER.

1.2

EL ANÁLISIS

¿Puede Blockchain transformar la financiación y publicación académica?

Antonio Tenorio Fornés
DECENTRALIZED SCIENCE

Bitcoin, la primera moneda electrónica descentralizada, introdujo la tecnología Blockchain en 2009 (1). Esta tecnología ofrece múltiples ventajas para aplicaciones más allá del dinero electrónico, que se están explorando en diversos ámbitos. En el mundo de la academia, se han propuesto múltiples soluciones basadas en Blockchain para resolver alguno de sus problemas.

Esta publicación pretende mostrar alguna de estas propuestas. En particular, se centra en mostrar soluciones centradas en la financiación académica, (Blockchain y dinero van bien de la mano) y en las diferentes fases del proceso de publicación académica, desde la necesaria colaboración entre autores en la fase de escritura, hasta la evaluación de la calidad de las contribuciones académicas una vez están publicadas.

A pesar de la poca madurez de la tecnología, este artículo ilustra el potencial transformador de Blockchain en la academia presentando proyectos existentes y activos. Dejamos fuera del interés y alcance del mismo las especulaciones teóricas que no estén respaldadas por proyectos que las intenten implementar en la actualidad (2).

A continuación, hacemos una breve introducción a Blockchain y sus características, seguida de la presentación de proyectos Blockchain de relevancia para la academia, en concreto para la financiación de la investigación y las transformaciones en la publicación académica.

Para finalizar, se presentan algunas discusiones y conclusiones sobre el material presentado.

BREVE INTRODUCCIÓN A BLOCKCHAIN Y SUS CARACTERÍSTICAS

Blockchain es una tecnología introducida en 2009 por Bitcoin (1). Sus características permitieron por primera vez el desarrollo de una moneda digital distribuida, es decir, que no estuviera controlada por ningún actor central, como podrían ser instituciones (e.g. bancos centrales) o empresas (e.g. Visa o Paypal).

Blockchain puede entenderse como un libro de contabilidad distribuido entre múltiples actores que mantienen y actualizan copias del mismo. De hecho, la tecnología Blockchain y sus evoluciones también se conocen por el nombre de "Distributed Ledger Technologies", i.e. libro de contabilidad distribuido en inglés. Este registro tiene las siguientes características:

- Es compartido, es decir, mucha gente tiene una copia.
- Es abierto, por lo que cualquiera puede obtener una copia, abrir una cuenta en el mismo y realizar transacciones.
- Es transparente, ya que cualquiera puede leer su contenido.
- Es colaborativo, pues cualquiera puede proponer una nueva página (o bloque) del mismo.
- Es inmutable, ya que la información escrita en el mismo no puede borrarse.
- Es verificable, de forma que cualquiera puede comprobar que se están siguiendo las reglas (e.g. que nadie está gastando dinero que no tiene).

- Es seguro, ya que su inmutabilidad está respaldada por un sistema de incentivos que hace extremadamente costosa cualquier modificación del registro.

A pesar de que su diseño original estuviera pensado para permitir monedas descentralizadas, las aplicaciones de Blockchain se han ido generalizado con la aparición de tecnologías que permiten desarrollar otro tipo de aplicaciones (3). Así, hay proyectos Blockchain en ámbitos tan dispares como las redes sociales[19] (4), la logística de la cadena de suministros[20] (5), el entretenimiento[21] (6), o la Academia, como exploramos a continuación.

Aplicaciones de Blockchain en la Academia

Blockchain tiene una gran diversidad de aplicaciones para el mundo académico. En este artículo, presentamos algunos de los proyectos que proponen aplicarlo a la financiación de la investigación y a mejorar las distintas fases de la publicación académica. Dejamos así fuera otros usos interesantes, como por ejemplo el registro de títulos universitarios[22] (7), u otras posibilidades de uso en la educación (8).

Nuevas formas de financiar la investigación

Al igual que muchos proyectos Blockchain, gran parte de las propuestas de uso de Blockchain en la academia también tienen un componente económico. De entre estas propuestas, presentamos aquellas centradas en la financiación de proyectos académicos. Una de las aplicaciones más directas de Blockchain como registro público inmutable es la de garantizar la fecha en la que se hicieron esos registros y que estos no han sido modificados. Así, se puede usar la Blockchain para dejar constancia de la existencia de cierta propiedad intelectual (una contribución académica, un invento, etc.) (9), de quien está registrando la misma y de cuando se hizo el registro. Proyectos como DEIP[23] proporcionan esta funcionalidad a la comunidad académica. El proyecto contempla que este registro no sólo sirva para proteger la autoría o los derechos, sino para facilitar el acceso a financiación de organizaciones interesadas en las contribuciones registradas.

Una propuesta más concreta de cómo puede Blockchain ayudar a obtener financiación tras el registro de propiedad intelectual en la Blockchain es Molecule[24], que propone generar un mercado de derechos sobre la propiedad intelectual de investigación en Farmacia. En su propuesta, esperan facilitar la venta de estos derechos a inversores para que proyectos de investigación puedan obtener financiación y esperan así impulsar el desarrollo de medicamentos.

Existen menos proyectos que exploren formas de financiación académica no ligadas al mercado, aunque se está estudiando el uso de Blockchain para agilizar y mejorar la gestión de la solicitud, evaluación y concesión de subvenciones[25]. Asimismo, en otros ámbitos se están explorando formas de financiación facilitadas por Blockchain como el *crowdfunding* de proyectos en los que los donantes controlan si se cumplen los objetivos[26] que podrían ser aplicados en el mundo académico.

TRANSFORMACIONES EN LA PUBLICACIÓN ACADÉMICA

Afortunadamente, el registro de contribuciones académicas en Blockchain no queda limitado al registro de propiedad intelectual con fines comerciales[27]. El uso de Blockchain se está explorando también para compartir artículos en abierto, dar transparencia al proceso de revisión por pares o mejorar la evaluación de la calidad de las contribuciones publicadas. A continuación, presentamos algunos de estos proyectos, que proponen apoyar la publicación científica en diferentes fases de la misma.

Colaboración y autoría

Proyectos como ARTiFACTS[28] utilizan Blockchain para facilitar la colaboración, permitiendo a los distintos actores registrar sus contribuciones de forma que no teman que se aprovechen de ellas sin la debida atribución.

Revisión por pares

De forma parecida, se pueden registrar en Blockchain los artículos enviados para revisión, quedando constancia de la fecha de la contribución original. Proyectos como Decentralized Science[29] (10) proponen además registrar los informes de revisión por pares en abierto, fomentando la transparencia y la calidad de la revisión por pares, y mejorando el reconocimiento a revisores y la búsqueda de los mismos a editores y organizadores de conferencias. De forma similar, proyectos como Sciencematters[30] o Unified Science[31] exploran formas de incentivar y reconocer el trabajo de revisión, ya sea mediante criptomonedas otras ventajas para los revisores (11).

---

[19] https://steemit.com/, [20] https://www.vechain.com/, [21] https://www.cryptokitties.co/, [22] https://www.smartdegrees.es/
[23] https://app.deip.co, [24] https://molecule.to/,[25] https://gcn.com/articles/2018/12/03/nsf-Blockchain.aspx, [26] https://giveth.io/
[27] Existen formas de registrar la propiedad intelectual para que permanezca en dominio público como http://www.defensivepublications.org/, y Blockchain también podría ayudar a ello, [28] https://artifacts.ai, [29] https://decentralized.science, [30] http://sciencematters.io/, [31] https://mesensei.com/unifiedscience

Publicación y acceso abierto

Tras la revisión de las contribuciones, Blockchain también puede apoyar a su publicación y difusión. Revistas como Ledger[32] y editoriales como Moringa[33], registran en la Blockchain los artículos que publican. El uso de Blockchain junto con otras tecnologías descentralizadas permiten proporcionar acceso abierto a estos artículos y que estos se compartan libremente en una red de pares que no depende de la revista o editorial.

Evaluación y calidad

Una vez publicadas, las contribuciones académicas pueden seguir beneficiándose de las propuestas de proyectos como Aiur 16, que propone combinar el uso de inteligencia artificial con incentivos para evaluar y replicar los estudios publicados.

Discusión y conclusiones

Los proyectos Blockchain presentados en este artículo muestran la diversidad de propuestas en el campo ante algunos de los retos de financiación y publicación académica. Sus propuestas permiten imaginar las mejoras, ventajas y oportunidades que esta tecnología puede ofrecer. Sin embargo, la mayoría de estos proyectos están en un estado de desarrollo bastante inicial, en gran parte por la relativa novedad de la tecnología Blockchain, cuya madurez y grado de adopción tienen todavía mucho camino por recorrer. Tanto es así, que gran parte de los proyectos que estaban activos hace sólo un año (17), parecen no seguir activos. Actualmente nos encontramos en un momento en el que se están comenzando a dar forma a numerosas iniciativas de aplicación de Blockchain en el ámbito académico. Proyectos como Decentralized Science son prueba de ello, donde estaremos encantados de contar con la colaboración, entusiasmo y experiencia de quien quiera acompañarnos en el reto.

Agradecimientos

This project has received funding from the European Union's Horizon 2020 research and innovation programme within the framework of the LED-GER Project funded under grant agreement No825268.

Referencias

1. Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system.

2. Krzysztof Janowicz, Blake Regalia, Pascal Hitzler, Gengchen Mai, Stephanie Delbecque, Maarten Fröhlich, Patrick Martinent, and Trevor Lazarus. On the prospects of Blockchain and distributed ledger technologies for open science and academic publishing. Semantic web, (Preprint):1–11, 2018.

3. Vitalik Buterin et al. Ethereum white paper: a next generation smart *contract & decentralized application platform. First version, 2014.

4. Usman W Chohan. The concept and criticisms of steemit. Available at SSRN 3129410, 2018.

5. Feng Tian. An agri-food supply chain traceability system for china based on rfid & Blockchain technology. In 2016 13th international conference on service systems and service management (ICSSSM), pages 1–6. IEEE, 2016.

6. Tian Min, Hanyi Wang, Yaoze Guo, and Wei Cai. Blockchain games: A survey. arXiv preprint arXiv:1906.05558, 2019.

7. John Rooksby and Kristiyan Dimitrov. Trustless education? a Blockchain. system for university grades. In New Value Transactions: Understanding and Designing for Distributed Autonomous Organisations, Workshop at DIS, 2017.

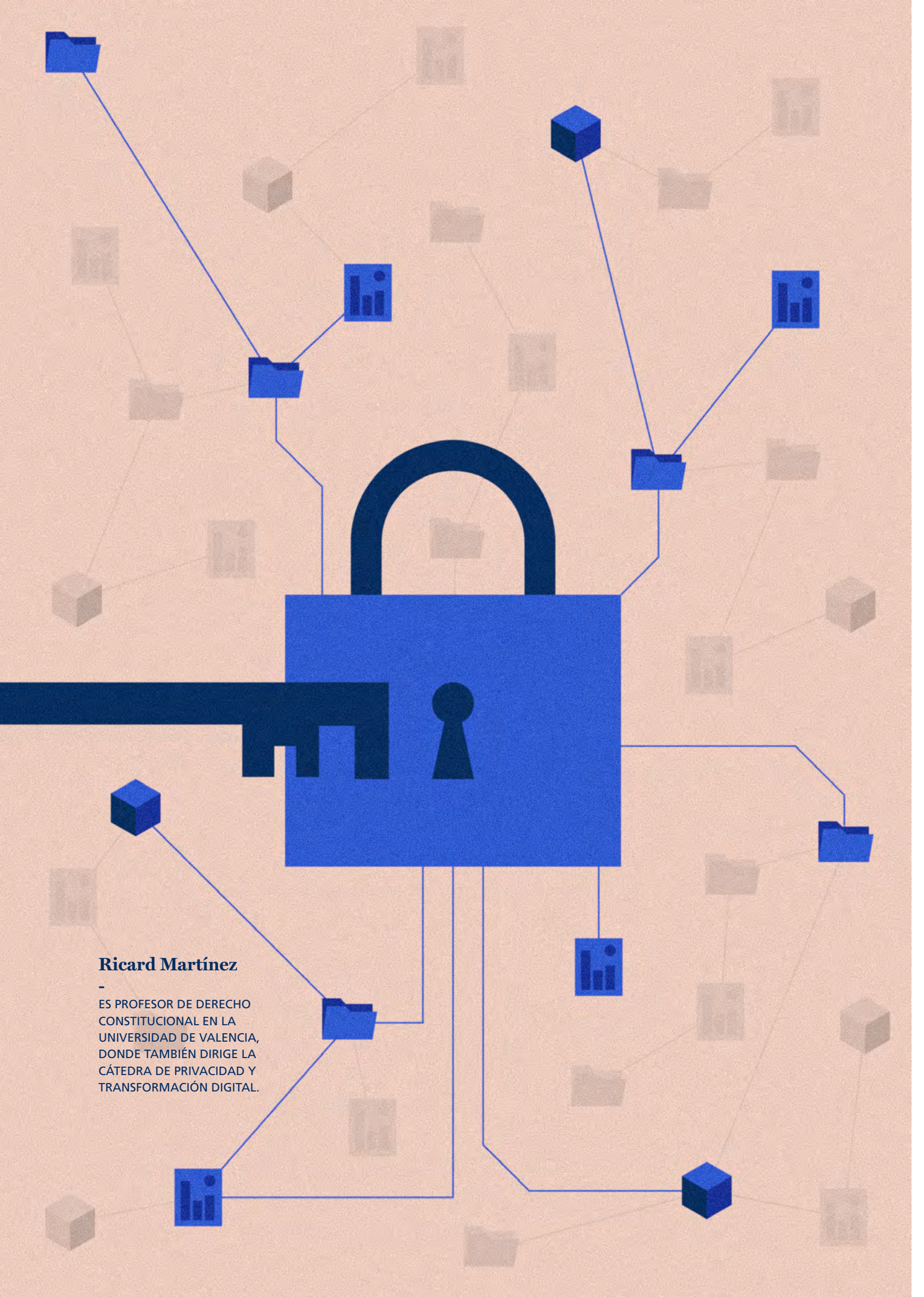
8. Guang Chen, Bing Xu, Manli Lu, and Nian-Shing Chen. Exploring Blockchain technology and its potential applications for education. Smart Learning Environments, 5(1):1, 2018.

9. Martin Zeilinger. Digital art as 'monetised graphics': Enforcing intellectual property on the Blockchain. Philosophy & Technology, 31(1):15–41, 2018.

10. Antonio Tenorio-Fornés, Viktor Jacynycz, David Llop-Vila, Antonio Sánchez-Ruiz, and Samer Hassan. Towards a Decentralized Process for Scientific Publication and Peer Review using Blockchain and IPFS. 2019.

11. Sina Rafati Niya, Lucas Pelloni, Severin Wullschleger, Andreas Schaufelbühl, Thomas Bocek, Lawrence Rajendran, and Burkhard Stiller. A Blockchain-based scientific publishing platform. In 2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), pages 329–336. IEEE, 2019.

[32] https://www.ledgerjournal.org/
[33] https://moringa.pub/



Ricard Martínez

–

ES PROFESOR DE DERECHO CONSTITUCIONAL EN LA UNIVERSIDAD DE VALENCIA, DONDE TAMBIÉN DIRIGE LA CÁTEDRA DE PRIVACIDAD Y TRANSFORMACIÓN DIGITAL.

1.3

EL ANÁLISIS

El cumplimiento del Reglamento General de Protección de Datos en el desarrollo de proyectos universitarios con Blockchain

Ricard Martínez
UNIVERSIDAD DE VALENCIA

Según las definiciones más usuales, Blockchain o cadena de bloques es una base de datos digital compartida y sincronizada que se mantiene mediante un algoritmo de consenso y se almacena en múltiples nodos. Los bloques, pueden incluir o agrupar múltiples transacciones que se agregan a la cadena de bloques existente a través de un proceso de *hashing*. Las funciones de *hash* son funciones criptográficas diseñadas para que sea imposible de revertir. De este modo la información replicada en la cadena resulta imposible de falsificar. Las ventajas que esta tecnología emergente ofrece en términos de seguridad y certeza hacen pensar que en un inmediato futuro cumpla funciones muy relevantes en la adveración y aseguramiento de muy distintas relaciones jurídicas. Entre ellas, la contratación, mediante el uso de los llamados *smart contracts* o el seguimiento de transacciones financieras son las más evidentes. En el sector público, a ellas se podrían unir la emisión de resoluciones y/o actos administrativos, o las certificaciones.

Sin embargo, la propia naturaleza originaria distribuida y abierta a la participación presenta problemas de encaje con las disposiciones del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (RGPD). En las próximas páginas, se abordarán distintos de los problemas que han sido significativamente puestos de relieve por un informe realizado para el Parlamento Europeo (1). Y se adelanta ya una primera respuesta o solución: la aplicabilidad de la cadena de bloques en ámbitos de gestión universitaria exige un diseño jurídico muy preciso para evitar tales inconvenientes. En este sentido, este trabajo se presenta más como la aproximación práctica de un delegado de protección de datos que como un esfuerzo de teorización[34].

1. IDENTIFICANDO PROBLEMAS

Blockchain, la llamada cadena de bloques, es una tecnología emergente que plantea enormes posibilidades para el desarrollo de sistemas de gestión de la información dotados de altas capacidades de trazabilidad. Asegura la certeza de las transacciones y el contenido de la información objeto de las mismas dotando a los entornos de una seguridad particularmente significativa. Sin embargo, es una tecnología cuya complejidad plantea significativas reservas en el mundo del Derecho cuando se enfrenta a la interacción con normas diseñadas sobre la base de una filosofía distinta.

[34] El autor ha sido técnico de protección de datos personales y desarrolla tareas de delegado de protección de datos.

Resultan particularmente significativas las dificultades de encaje del uso de Blockchain en relación con las previsiones de la normativa de protección de los datos de carácter personal.

Conviene, por tanto, tener en cuenta la presencia de distintos elementos de carácter problemático que deben ser salvados para enfocar un proyecto que implique un tratamiento de datos de carácter personal.

1.1 El enfoque de los juristas como problema

Se viene exigiendo, de modo reiterado en distintas publicaciones[35], la necesidad de plantear nuevos enfoques en la metodología jurídica a la hora de implementar proyectos de naturaleza tecnológica. En este sentido, el método jurídico tradicional debe ser complementado con un enfoque basado en el conocimiento de la realidad tecnológica y un modelo operativo que siga los ritmos del propio desarrollo tecnológico. El jurista debe aprender a iterar desde el análisis de requerimientos a la puesta en producción, y mantener la atención durante la vida del sistema.

Es precisamente aquí donde encuentra el primer escollo el propio desarrollo y aplicación de Blockchain. Con notables excepciones, esta tecnología es percibida como amenazante, o al menos contrafactual para una parte del mundo del Derecho. Primero, resulta necesario entender, hasta qué punto la cadena de bloques plantea escenarios muy cercanos a la autorregulación, ya que puede plantear alternativas tecnológicamente significativas a los modelos de regulación tradicional. Por otra parte, venimos de un mundo jurídico con una tradición milenaria de modelos de contratación practicados en el mundo físico y con intervención de fedatarios reconocibles. Y Blockchain, salvo que se apueste por entornos privados controlados, es una tecnología que exige confianza en la interacción de miles de desconocidos en modelos no bilaterales sino multilaterales.

Además, resulta indispensable conocer las rutinas de funcionamiento de una tecnología no necesariamente sencilla, de modo que el rechazo instintivo a lo que no se comprende puede constituir en sí mismo un problema. Por ello, los juristas que aborden Blockchain deben adquirir una cultura tecnológica y científica que les permita ser capaces de afrontar los retos de conocimiento que ello implica. De este modo, el primer prerrequisito para cualquier proyecto que incorpore la cadena de bloques no es otro que proveerse de expertos juristas capaces de afrontar los retos que plantea el mundo tecnológico con predisposición a encontrar soluciones viables para el cumplimiento normativo.

En ese sentido, aunque duela reconocerlo, con muy escasas excepciones, la infraestructura jurídica de las administraciones públicas debe realizar un esfuerzo de adaptación, de actualización de conocimientos, y de adquisición de talento, que difícilmente casa con la filosofía de gestión actual. Una filosofía, basada en mecanismos de selección de personal que atiende más a lo memorístico, que a las capacidades analíticas que permitan enfrentarse a lo desconocido. La obtención de un soporte adecuado puede verse abocada al fracaso cuando la decisión de implementar Blockchain convive con modelos de selección de personal de carácter generalista que considera que cualquier persona posee la capacidad de adaptarse a cualquier tipo de tarea sin considerar la necesidad de una inversión estratégica en la formación de talento y la adquisición de nuevas competencias. O alternativamente, a su desarrollo a espaldas del soporte jurídico de la organización.

1.2 ¿Qué es un dato personal en la cadena de bloques?

Otro de los problemas que se viene planteando respecto de la utilización de la cadena de bloques deriva de las implicaciones del concepto de dato de carácter personal. La razón es obvia: si en Blockchain existen datos personales que son objeto de tratamiento la aplicación del Reglamento General de Protección de Datos deberá producirse en su integridad. Y no sólo esto, deberá tener muy en cuenta los principios de protección de datos desde el diseño y por defecto, y en un entorno tan complejo. Esta no es en absoluto una cuestión banal. Es más, la aplicación del RGPD y la ley española determinarán sin duda decisiones críticas a la hora de definir la tipología de cadena de bloques y los agentes implicados. A tal efecto el art 4 RGPD nos ofrece dos definiciones relevantes:

1)«datos personales»: toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona;

(…)

5) «seudonimización»: el tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas

[35] Por todas véase MARTINEZ, RICARD (2019). "Inteligencia artificial desde el diseño. Retos y estrategias para el cumplimiento normativo", en Revista catalana de dret públic, núm. 58, págs. 64-81.

destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable;

En relación con estos conceptos, y en particular el de pseudonimización, una de las cuestiones que se han planteado reside en establecer si una información protegida del acceso de terceros mediante esta tecnología incluye o no datos de carácter personal. Y la respuesta que vienen dando las autoridades de protección de datos evidencia dificultades significativas para excluir la existencia de datos personales en una cadena de bloques con independencia de que se utilicen de sofisticadas técnicas para ello. En primer lugar, porque el funcionamiento ordinario de la cadena puede generarlos por sí mismo. En este sentido, tanto el uso de la clave pública de un sujeto, como la generación de datos transaccionales con motivo de las operaciones realizadas, puede tener como consecuencia la generación de datos personales.

Por otra parte, la protección de la información mediante técnicas de encriptación, o el uso de algoritmos o funciones de *hash*, no excluye en absoluto la aplicación del RGPD. En la mayor parte de los casos, los datos en realidad no habrán sido anonimizados sino seudonimizados. Desde ese punto de vista, históricamente la posición de los reguladores, y significativamente la del regulador español durante la tramitación de la ley de investigación biomédica, no ha sido otra que considerar que un dato seudonimizado es un dato de carácter personal al que cabe aplicar el conjunto de la regulación. Sin perjuicio de que desde el punto de vista de la seguridad esta técnica ofrezca altas garantías en términos de confianza y seguridad de los tratamientos.

Por otra parte, la posición colectiva de las autoridades de protección de datos sobre la anonimización deja escasos resquicios. El punto de partida cabe encontrarlo en sendos considerandos casi idénticos en la Directiva 45/96/CE[36] y el RGPD que se reproducen a continuación. Así señalaba la Directiva:

(26) Considerando que los principios de la protección deberán aplicarse a cualquier información relativa a una persona identificada o identificable; que, para determinar si una persona es identificable, hay que considerar el conjunto de los medios que puedan ser razonablemente utilizados por el responsable del tratamiento o por cualquier otra persona, para identificar a dicha persona; que los principios de la protección no se aplicarán a aquellos datos hechos anónimos de manera tal que ya no sea posible identificar al interesado; que los códigos de conducta con arreglo al artículo 27 pueden constituir un elemento útil para proporcionar indicaciones sobre los medios gracias a los cuales los datos pueden hacerse anónimos y conservarse de forma tal que impida identificar al interesado;

Y añade el RGPD:

(26) Los principios de la protección de datos deben aplicarse a toda la información relativa a una persona física identificada o identificable. Los datos personales seudonimizados, que cabría atribuir a una persona física mediante la utilización de información adicional, deben considerarse información sobre una persona física identificable. Para determinar si una persona física es identificable, deben tenerse en cuenta todos los medios, como la singularización, que razonablemente pueda utilizar el responsable del tratamiento o cualquier otra persona para identificar directa o indirectamente a la persona física. Para determinar si existe una probabilidad razonable de que se utilicen medios para identificar a una persona física, deben tenerse en cuenta todos los factores objetivos, como los costes y el tiempo necesarios para la identificación, teniendo en cuenta tanto la tecnología disponible en el momento del tratamiento como los avances tecnológicos. Por lo tanto los principios de protección de datos no deben aplicarse a la información anónima, es decir información que no guarda relación con una persona física identificada o identificable, ni a los datos convertidos en anónimos de forma que el interesado no sea identificable, o deje de serlo. En consecuencia, el presente Reglamento no afecta al tratamiento de dicha información anónima, inclusive con fines estadísticos o de investigación.

Es evidente la influencia en la última redacción de las posiciones mantenidas colectivamente por las autoridades de protección de datos. En 2014, el entonces Grupo de Trabajo del Artículo 29[37] estableció un conjunto de rigurosos criterios no siempre compartidos por todas las autoridades. Para el Grupo la anonimización debe ser absolutamente irreversible, esto es equivalente al borrado. En segundo lugar, el análisis del riesgo de reidentificación va a depender, no ya de las capacidades de la entidad que anonimiza sino de dos factores adicionales uno material y otro prospectivo.

Así, no basta con evaluar las capacidades del responsable, sino que entran en juego las capacidades de cualquier tercero. Por tanto, el estándar de riesgo

[36] Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

[37] GRUPO DE TRABAJO DEL ARTÍCULO 29. Dictamen 05/2014 sobre técnicas de anonimización de 10 de abril de 2014. 0829/14/ES WP216.

no vendrá definido por qué hace una entidad sino por el más brillante de los premios "Abel"[38]. Es más, no se considera en el análisis de la capacidad de un "tercero" la propia capacidad de proteger los datos frente a accesos no autorizados. Es decir, unos datos anonimizados resguardados en el bunker del Centro Nacional de Inteligencia, en servidores desconectados de la red y protegidos por una jaula de Faraday, serán datos personales si, desde un punto de vista teórico, un brillante estadístico de la Universidad de Berkeley pudiera ser capaz de reidentificarlos.

El segundo factor es el temporal. El responsable, debe considerar la evolución de la tecnología y, por tanto, la duración del propio tratamiento, y hacer un cálculo probabilístico o prospectivo seguramente de contenido prácticamente imposible. Por tanto, permita el lector una expresión algo coloquial, ya que la conclusión es obvia. Teniendo en cuenta los planteamientos de la Agencia Española de Protección de Datos en sus *guidelines*[39], mejor olvidar cualquier posible recurso a la anonimización. Y aunque los expertos defiendan lo contrario, lo cierto es que habrá que establecer caso a caso bajo qué condiciones se pueden considerar adecuadamente anonimizados los datos. Y, desde el punto de vista de la aplicación defensiva del RGPD al que condena el disuasorio marco regulador, la mejor solución no será otra que considerar la presencia de datos personales como un hecho necesario, así compartan o no las posiciones del regulador.

1.3. Los principios y derechos de la protección de datos

Seguramente, la otra gran dificultad que presenta el uso de esta tecnología en la gestión de la información personal se refiera a las condiciones de conservación de los datos y sus efectos respecto de los derechos de los afectados.

Partamos de que, en principio, una cadena de bloques se orienta a la satisfacción de ciertos objetivos. El primero, la preservación sin límites de la información en el exacto momento en el que esta se encontraba al ser procesada. Esto plantea dos dificultades. La primera reside en el hecho de que el principio nuclear en protección de datos ya desde la Directiva 95/46/CE (2) consistía precisamente en que la finalidad del tratamiento determina el plazo de conservación de los datos. El RGPD ha intensificado este valor imponiendo de modo preciso el deber de determinar este plazo. Este deber se convierte no solo en una decisión interna del responsable del tratamiento y exige trasparencia respecto del titular de los datos, al cual debe informarse del plazo de conservación o de los criterios que determinarán la desaparición de los datos.

Por otra parte, en todos aquellos casos en los que el tratamiento de datos dependa del libre consentimiento de la persona interesada, esta podrá revocar sin límites el consentimiento. Y si bien es cierto que resulta legítimo el tratamiento de datos realizado hasta ese momento, no lo es menos que hay que adoptar las correspondientes decisiones para evitar tratamientos ulteriores. Del mismo, se podrá ejercer el derecho de oposición al tratamiento o, sobre todo, el derecho de rectificación.

Por ello, una tecnología de la que se presume un mantenimiento íntegro e indefinido de los datos casa mal con modelos de gestión de la información que exigen un enfoque dinámico en la modificación y sobre todo en la supresión de aquellos datos cuya inexactitud exige la cancelación.

1.4 Responsables y encargados. ¿La contratación como problema?

La cadena de bloques plantea un problema significativo a la hora de establecer cuáles son las relaciones que se establecen entre sus participantes en términos de protección de datos. La razón para ello deriva del hecho de que las relaciones que se establecen entre los distintos nodos de la cadena no son necesariamente de prestación de servicios. Desde ese punto de vista, entra en juego la definición de responsable del tratamiento y la regulación que el artículo 26 RGPD en esta materia. Partamos de que el RGPD en su artículo 4 define varios posibles roles:

7) «responsable del tratamiento» o «responsable»: la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento; si el Derecho de la Unión o de los Estados miembros determina los fines y medios del tratamiento, el responsable del tratamiento o los criterios específicos para su nombramiento podrá establecerlos el Derecho de la Unión o de los Estados miembros;

8) «encargado del tratamiento» o «encargado»: la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento;

10) «tercero»: persona física o jurídica, autoridad pública, servicio u organismo distinto del interesado, del responsable del tratamiento, del encargado del tratamiento y de las personas autorizadas para tratar los datos personales bajo la autoridad directa del responsable o del encargado;

---

[38] Considerado el equivalente al premio Nobel en matemáticas. Véase https://www.abelprize.no/

[39] Véase la guía "Orientaciones y garantías en los procedimientos de ANONIMIZACIÓN (sic) de datos personales. Disponible el 22/09/2019 en https://www.aepd.es/guias/index.html.

Por otra parte, el art, 26 identifica escenarios de decisión conjunta de varios responsables:

1. Cuando dos o más responsables determinen conjuntamente los objetivos y los medios del tratamiento serán considerados corresponsables del tratamiento. Los corresponsables determinarán de modo transparente y de mutuo acuerdo sus responsabilidades respectivas en el cumplimiento de las obligaciones impuestas por el presente Reglamento, en particular en cuanto al ejercicio de los derechos del interesado y a sus respectivas obligaciones de suministro de información a que se refieren los artículos 13 y 14, salvo, y en la medida en que, sus responsabilidades respectivas se rijan por el Derecho de la Unión o de los Estados miembros que se les aplique a ellos. Dicho acuerdo podrá designar un punto de contacto para los interesados.

2. El acuerdo indicado en el apartado 1 reflejará debidamente las funciones y relaciones respectivas de los corresponsables en relación con los interesados. Se pondrán a disposición del interesado los aspectos esenciales del acuerdo.

3. Independientemente de los términos del acuerdo a que se refiere el apartado 1, los interesados podrán ejercer los derechos que les reconoce el presente Reglamento frente a, y en contra de, cada uno de los responsables.

Desde este punto de vista, lo relevante para que existan corresponsables de un tratamiento es la capacidad de tomar decisiones sobre fines y medios del tratamiento. El Tribunal de Justicia de la Unión Europea ha venido a establecer que un concepto de corresponsabilidad al tratamiento en un sentido amplio[40]. Ha bastado con que existiese un mínimo espacio de decisión con relación a la utilización de un software o los recursos de un tercero para que se considerase que estamos ante la existencia de corresponsables del tratamiento.

Esto plantea una enorme dificultad en los entornos de cadenas de bloques de carácter público, donde múltiples sujetos pueden interactuar libremente para el desarrollo de las actividades propias de la cadena. En estos casos, se ha señalado que el responsable del tratamiento como mínimo toma la decisión de utilizar una determinada cadena como base para el tratamiento de datos.

Otra posibilidad consistiría en presumir que nos encontramos ante una cadena múltiple de prestadores de servicios. Sin embargo, en la medida en que cada uno de sus prestadores puede tomar decisiones sobre la participación a la cadena y sobre la conservación de la información, y, por tanto, sobre la posibilidad de borrar su eslabón en la cadena, tendría un espacio de decisión que lo convierte en corresponsable del tratamiento. Esta complejidad podría ser resuelta mediante condiciones previas de contratación como las definidas en el artículo 26 del RGPD, que establecieran con precisión tanto los requisitos de entrada, como las obligaciones que se asumen en el contexto de la misma.

Existe otro elemento que puede poner en cuestión la aplicación de esta tecnología para la gestión de información personal. La filosofía de la cadena de bloques es abierta y colaborativa. Dicho en términos más propios de un jurista que de un experto en tecnología, lo que se pretende subrayar es que su fortaleza será tanto mayor cuanto mayor sea el número de agentes implicados en la misma. Esto introduce un alto grado de compartición que no se aviene demasiado bien con los principios exigibles para la prestación de servicios en el ámbito del tratamiento de datos de carácter personal.

Ello no sólo se debe a las exigencias propias de la firma del contrato de encargado del tratamiento previsto en el artículo 28 del Reglamento General de Protección de Datos (RGPD) (3) o a la necesidad del artículo 26 del RGPD de establecer cuáles sean las responsabilidades respectivas en el caso de considerar que nos enfrentamos a entornos de corresponsabilidad en el tratamiento. En uno y otro caso, el acuerdo en el que se deben especificar las responsabilidades asumidas individualmente por cada sujeto no es lo más relevante. Precisamente, esta es una de las ventajas que ofrece la cadena de bloques: la posibilidad de servir de plataforma para una contratación dotada de una completa certeza.

El RGPD persigue algo más, persigue asegurar que, en la elección de nuestros socios, sea cual fuere la naturaleza de la relación que establezcamos con ellos, se presuma una diligencia en la comprobación de la capacidad de la otra parte para cumplir con las exigencias de la normativa. El derecho fundamental a la protección de datos sería puesto en riesgo desde el mismo momento en el que no escogimos de modo diligente a nuestra contraparte, o bien convertimos la contratación en una mera formalidad.

Desgraciadamente, este no es un problema sólo imputable la cadena de bloques. Es bien conocido por cualquier experto en protección de datos, cómo y

[40] Véanse los casos C-210/16 Wirtschafsakademie Schleswig-Holstein, C-25/17 Jehovan todistajat, y C- 40/17 Fashion ID.

hasta qué punto, en la contratación de servicios que comporten tratamiento de datos se ha extendido la mala práctica de diseñar contratos de encargado del tratamiento que, sencillamente, ofrecen un trampantojo en el que una versión más o menos extendida del artículo 28 adquiere una apariencia de cumplimiento normativo. De hecho, resulta particularmente inusual encontrar contratos de encargado del tratamiento que incluyan anexos de índole técnica o material en la que especifiquen con precisión cuáles son las condiciones materiales en las que el tratamiento se va realizar y cuáles son las consecuencias en protección de datos. En lo que a Blockchain se refiere, lo cierto es que una cadena abierta en la que cualquier tercero pueda participar sobre la base de la mera formalización de un contrato genérico de encargado se aviene particularmente mal con el estándar mínimo de diligencia.

2. UNA PROPUESTA DE ACCIÓN

A la vista de los problemas constatados, la cadena de bloques plantea dificultades en dos planos: cuando no se tiene control sobre los agentes que procesan los bloques en un entorno público o abierto y, en segundo lugar, cuando se gestiona información personal susceptible de modificación o supresión.

Puesto que lo que se define como cadena de bloques puede construirse de distintas maneras hay que tomar decisiones estratégicas ordenadas a identificar cuál sería el mejor procedimiento aplicable a procesos de colaboración interuniversitaria para finalidades determinadas. Parece bastante claro que debería apostarse por construir cadenas cerradas de naturaleza privada integradas exclusivamente por sujetos autorizados. Este tipo de estructura podría rendir beneficios adecuados, por ejemplo, para transacciones como la certificación de actos administrativos de carácter definitivo no susceptibles de modificación. En este sentido, ciertos procedimientos administrativos llevados a término, que o bien posean valor histórico o bien deban certificarse a lo largo de la vida de la persona interesada, son procesos muy resilientes a la rectificación y a la supresión de los datos.

También podría ser muy útil en aquellos supuestos en los que el procedimiento, incluso cuando se modifican datos exige un grado tal de trazabilidad, que justifique la permanencia de los datos anteriores. De nuevo, el proceso de gestión de las actas de notas se manifiesta como un ejemplo paradigmático[41]. La modificación de un acta definitiva usualmente requiere documentar la nota previa, la decisión de revisión, y la nota definitiva. En nada se impacta al derecho fundamental a la protección de datos por el mantenimiento de la nota antigua a efectos de trazabilidad de un acto cuya manipulación puede ser constitutiva de delito.

Este ejemplo pone de manifiesto que las autoridades de protección de datos deberán plantearse bajo qué condiciones el ejercicio del derecho de rectificación o de supresión debe suponer la rectificación o eliminación de un dato, pero también implicar la conservación de la transacción realizada cuando pueda dotar de trazabilidad a las transacciones realizadas y de seguridad a la información.

En cualquier caso, existen a nuestro juicio dos elementos relevantes desde el punto de vista jurídico y material que deben ser examinados a continuación.

2.1 La apuesta por un modelo basado en un acuerdo, convenio o contrato

Si partimos de la sólida experiencia en el desarrollo de marcos de colaboración interuniversitaria, ya sea entre grupos de Universidades, ya sea en el entorno de la Sectorial de Tecnologías de la Información de la CRUE-TIC, la definición de un marco jurídico común resultaría perfectamente alcanzable.

Por tanto, desde el punto de vista de la conformación de un entorno de Blockchain de las universidades españolas, parece razonable considerar que la base jurídica debiera sustentarse en un modelo jurídicamente regulado en virtud de un contrato o convenio. En este sentido, la naturaleza de la relación jurídica podría ser distinta según se trate de la constitución de una entidad instrumental que integre granjas de ordenadores dedicadas a la prestación del servicio, que en el caso en el que los ordenadores utilizados se encuentren residentes en cada una de las instituciones universitarias.

Corresponderá al soporte jurídico para el desarrollo de un acuerdo de tal naturaleza determinar con precisión si el sistema funciona permitiendo la toma de decisiones autónomas para cada nodo, que incorporen cierto grado de corresponsabilidad, o bien se necesitan instrucciones específicas de cada responsable, de modo que se convierta a cada uno de los participantes a la vez en responsable de sus tratamientos y encargado del tratamiento del colectivo de todas las universidades. Una de las ventajas que ciertamente ofrece el entorno universitario reside en que las tareas que se confíen a una cadena de bloques se relacionarán con el despliegue de las funciones atribuidas por la Ley Orgánica 6/2001, de 21 de diciembre, de Universidades.

[41] Pero no es esta la única área de gestión relevante desde un punto de vista universitario. Pensemos por ejemplo en los traslados de expediente. Un marco colaborativo como el de la cadena de bloques incluso parece funcionalmente idóneo para este tipo de procesos de intercambio de datos.

En nuestra opinión, en este caso lo relevante será sin duda el marco funcional de decisión establecido por esta ley y por los Estatutos y normativa de cada universidad, lo que, en la mayoría de los casos, permitirá definir un marco de relación responsable-encargado que podría resolverse mediante un marco jurídico multilateral de cooperación.

2.2 La protección de datos desde el diseño y por defecto

Las universidades públicas no sólo poseen las capacidades, sino como se ha defendido en otro trabajo, incluso el deber de liderar los procesos de innovación tecnológica al servicio del bien común (4). Pero ello obliga a desplegar un proceso de diseño responsable que con anterioridad se ha expuesto en otros trabajos y del que aquí se aporta una breve síntesis.

Con toda probabilidad, el modelo de referencia sea la metodología de desarrollo de software recomendada por la autoridad noruega de protección de datos (Datatilsynet) (5). Esta autoridad propone procesos de diseño de software con fases diferenciadas:

- Formación
- Toma de requerimientos
- Diseño de la aplicación
- Programación del código
- Prueba o verificación
- Puesta en producción
- Mantenimiento

Se trata de un procedimiento circular, o Ciclo de Deming, orientado a garantizar no sólo un diseño previo adecuado, sino también a mantener el estándar de cumplimiento normativo como compromiso de permanente actualización. De acuerdo con los objetivos de este método resulta recomendable:

2.2.1 Formar ética y jurídicamente al equipo

No se trata de convertir a los desarrolladores ni a los gestores en expertos juristas. Sencillamente, obliga a que exista una cultura de garantía que oriente las decisiones. Y comporta incorporar desde el inicio al proyecto a expertos en materias como la ética y el Derecho.

2.2.2 Identificar los requerimientos del proyecto

Desde esta fase temprana deberán tenerse en cuenta los principios jurídicos aplicables. Y esto implica un enfoque de cumplimiento normativo desde el diseño que tiene significativas consecuencias de orden práctico. En primer lugar, el desarrollo de un proyecto de Blockchain deberá ponerse en el contexto del sector del Ordenamiento en el que se va a desenvolver y deberá considerar la regulación vigente. Será adicionalmente necesario desarrollar un análisis de los riesgos e implicaciones de la tecnología que se está desarrollando. Se trata de una metodología conocida con reglas muy específicas y con criterios de aplicación particularmente precisos. Se trata de establecer cuáles pueden ser las vulnerabilidades intrínsecas al proyecto que se desarrolla y las amenazas a las que se enfrenta. En la metodología de análisis de riesgos debemos establecer una relación entre la probabilidad de que esas amenazas o vulnerabilidades se materialicen en el mundo real y su impacto al afectar, en lo que aquí interesa, al cumplimiento normativo, causar daños a las personas, y muy especialmente, vulnerar sus derechos fundamentales.

2.2.3 Integrar las normas en el diseño y documentar el cumplimiento

Superada la fase de toma de requerimientos y de análisis de riesgos debemos considerar como los principios y valores del artículo 5 del RGPD pueden inspirar de modo muy preciso el desarrollo[42].

2.2.4 De la programación a la fase de producción

Las subsiguientes fases de gestación de un proyecto tecnológico suelen discurrir a través de un proceso ordenado y a la vez creativo. Se produce lo que en la jerga se denomina "iteración". Si bien cada fase de desarrollo incluye un proceso de codificación que genera paquetes entregables, su propia dinámica está muy abierta a la innovación. Así, durante la programación del código, el programador verifica sus posibilidades y problemas y ello le obliga a cambiar su enfoque en muchas ocasiones. Ello implica disponer de un soporte jurídico permanente que asegure el cumplimiento de la norma como un objetivo intrínseco al desarrollo y con una doble función. En primer lugar, no sólo el producto final, sino cada una de las tareas que contribuyen a su gestación debe cumplir

[42] Este dispone que: «1. Los datos personales serán:

el Derecho. No parece razonable considerar adecuado un resultado cuyo proceso de diseño haya vulnerado normas. En segundo lugar, es necesario asegurar en la puesta en producción ofrezca un resultado adecuado desde un punto de vista jurídico.

2.2.5 Un ciclo que se mantiene durante toda la vida de una IA

Ningún proceso de cumplimiento normativo vinculado a la tecnología puede ser estático. Un cumplimiento normativo adecuado obliga a un estado de permanente seguimiento y actualización que se despliega en varios niveles:

1) Aprendiendo del propio funcionamiento de la tecnología. Los resultados obtenidos, los errores de funcionamiento, las incidencias… Cualquier elemento verificado o verificable debería ser indexado y estudiado también por el soporte jurídico. Y no únicamente para prevenir posibles conflictos y responsabilidades sino, sobre todo, para mejorar las condiciones de cumplimiento normativo

2) Profundizando en el diseño de cumplimiento normativo proponiendo mejoras cuando resulte necesario

3) Acompañando cada fase o evolución del producto

Conclusiones

Pretender resolver en un trabajo de esta naturaleza una pregunta del tipo "cómo aplicar Blockchain y cumplir el Reglamento General de Protección de Datos en un entorno universitario" resulta sencillamente ilusorio. Es más, resultaría en sí mismo una contradicción con la propuesta que define este trabajo.

A lo largo de estas páginas, se han apuntado algunos de los problemas que plantea casar el funcionamiento y la filosofía de la cadena de bloques con el Reglamento. No se ha profundizado en elementos de detalle como por ejemplo los procesos relacionados con la portabilidad o el impacto de la "imaginación" de la autoridad española de protección de datos y el legislador al consolidar el instituto del bloqueo de los datos en el artículo 32 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

Cada etapa en el diseño de una cadena de bloques deberá enfrentar estos y otros escollos. Pero aquí no caben soluciones de laboratorio tan queridas a veces en algunas guías y dictámenes. Es necesario encontrar soluciones tecnológicas para cada funcionalidad que se desarrolle.

Sin embargo, quieren apuntarse razones para el optimismo. Existe un punto de partida que dota de viabilidad a un proyecto de esta naturaleza en un entorno universitario. En primer lugar, existe un marco de referencia acotado. Sea un proyecto que implique a dos o a cincuenta universidades existe un marco de referencia funcional y procedimental de finalidades y competencias compartidas. Ello permite construir una cadena de naturaleza cerrada con claros requerimientos técnicos y jurídicos para la entrada y con una filosofía compartida y generalizable en el modo de abordar las necesidades y prestaciones de una plataforma de esta clase.

Por otra parte, la Universidad Española aporta sin duda los recursos humanos y tecnológicos idóneos para afrontar un reto de esta naturaleza. Las capacidades de computación, la experiencia en seguridad, las redes de comunicaciones, y el caudal de programadores e investigadores de alta calidad en distintas áreas, facilita una infraestructura idónea para este tipo de desarrollos. En estos equipos, el cumplimiento normativo por defecto y la incorporación de un equipo jurídico de altas capacidades desde el inicio puede ser sin duda una contribución indispensable. El compromiso de la Universidad con la garantía de los derechos fundamentales no puede sino aportar a un Blockchain universitario el ingrediente ético y jurídico esencial para ofrecer seguridad y protección a las personas.

---

a) tratados de manera lícita, leal y transparente en relación con el interesado («licitud, lealtad y transparencia»);
b) recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines; de acuerdo con el artículo 89, apartado 1, el tratamiento ulterior de los datos personales con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos no se considerará incompatible con los fines iniciales («limitación de la finalidad»);
c) adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados («minimización de datos»);
d) exactos y, si fuera necesario, actualizados; se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan («exactitud»);
(...)
f) tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas («integridad y confidencialidad»). 2. El responsable del tratamiento será responsable del cumplimiento de lo dispuesto en el apartado 1 y capaz de demostrarlo («responsabilidad proactiva»).

No obstante, estas conclusiones no pueden ser sino tenidas como provisionales. Y no sólo por el influjo del cambio tecnológico, sino también por la acción del legislador y del regulador. En primer lugar, el uso de la cadena de bloques ha sido limitado por el Real Decreto-ley 14/2019, de 31 de octubre, por el que se adoptan medidas urgentes por razones de seguridad pública en materia de administración digital, contratación del sector público y telecomunicaciones. Esta norma ha introducido la nueva disposición adicional sexta que señala que para el uso de sistemas de identificación y firma basados en claves concertadas o reconocidos autónomamente por las administraciones no serán admisibles en ningún caso y no podrán ser autorizados cuando se basen en tecnologías de registro distribuido y tampoco los sistemas de firma basados en los anteriores, en tanto que no sean objeto de regulación específica por el Estado en el marco del Derecho de la Unión Europea. Por otra parte, la Agencia Española de Protección de Datos ha publicado unas recomendaciones para aquellos que utilicen técnicas de hash en la seudonimización de datos cuya consulta será obligada[43]. Preocupa, y no poco la escasa rapidez y flexibilidad europea para abordar estas cuestiones. ¿Otra oportunidad perdida?

Referencias

1. FINCK, MICHÈLE (2019). Blockchain and the General Data Protection Regulation. Can distributed ledgers be squared with European data protection law?. EPRS. European Parliamentary Research Service Scientific Foresight Unit (STOA) PE 634.445, July 2019.

2. Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respeta al tratamiento de datos personales y a la libre circulación de estos datos.

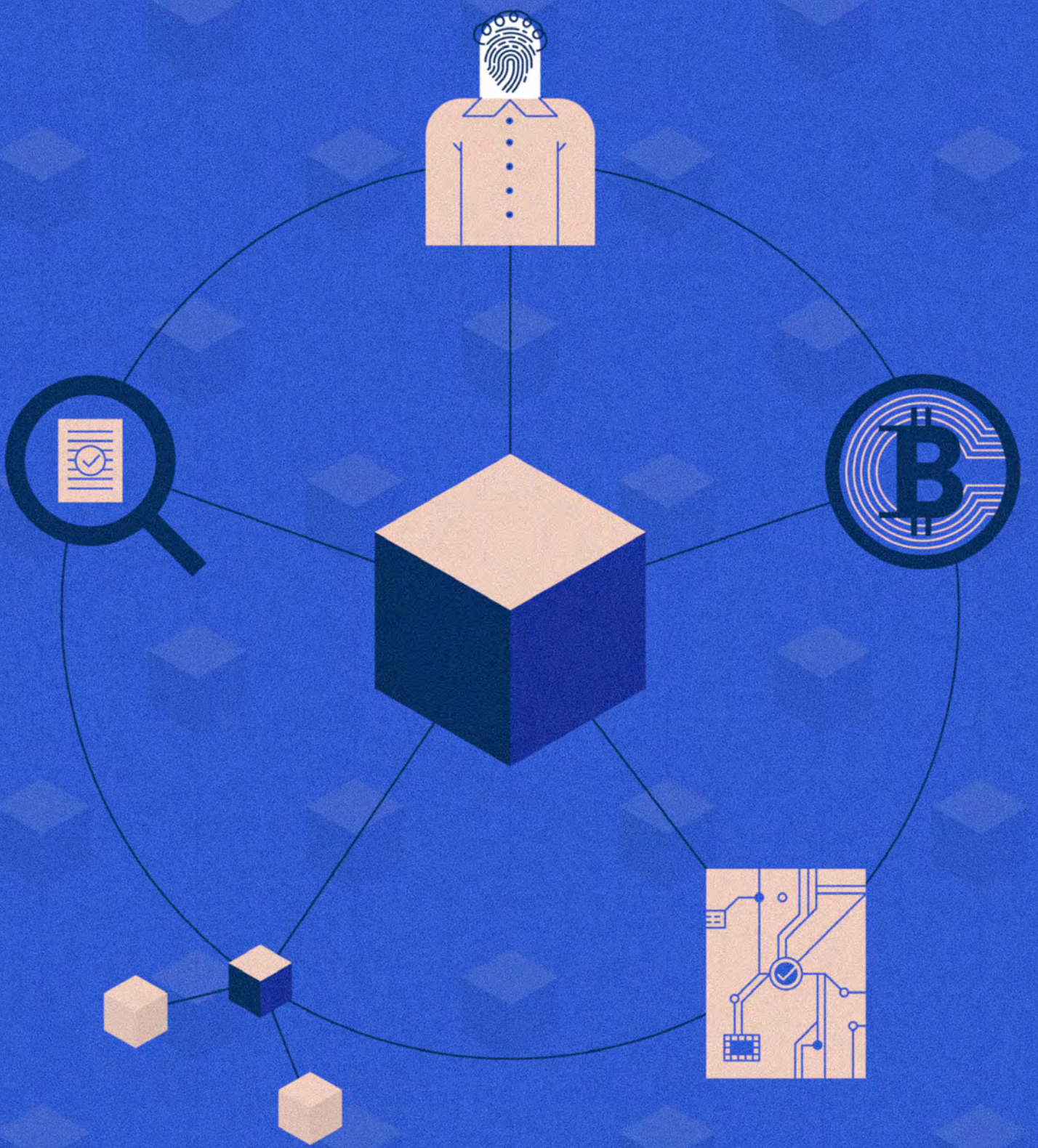
3. Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

4. MARTINEZ, RICARD (2018). "Transformación digital y diseño orientado a la privacidad en la Universidad". RUIDERAe Revista de Unidades de Información. Núm. 13 (2018).

Disponible el 31/07/2019 EN https://ruidera.uclm.es/xmlui/handle/10578/18797

5. Datatilsynet (2018). Software development with Data Protection by Design and by Default. Disponible el 01/05/2019 en http://bit.ly/2V8AG0f

43. Agencia Española de Protección de Datos. Introducción al hash como técnica de seudonimización de datos personales. Disponible el 12/122/2019 en https://www.aepd.es/media/estudios/estudio-hash-anonimidad.pdf"



Diego López

-

ES SENIOR TECHNOLOGY EXPERT EN TELEFONICA
I+D, Y CHAIRMAN DE NFV AND PDL ISGS EN EL ETSI.

1.4

EL ANÁLISIS

Estandarización en el campo de las DLT (o Blockchains por mal nombre). La propuesta del ETSI ISG PDL

Diego R. López
TELEFÓNICA I+D

Las DLT (*Distributed Ledger Technologies*, tecnologías de registros distribuidos), conocidas comúnmente como Blockchains porque la sinécdoque produce uno de esos nombres llamativos que tanto gustan a los que se dedican a las TIC, constituyen una de las aplicaciones recientes de estas TIC con más capacidad disruptiva. Las DLT ofrecen la posibilidad de almacenar cualquier tipo de datos por medio del consenso entre una serie de registros digitales compartidos y replicados en múltiples sitios, sin necesidad de un control central. A esto podemos añadir que las técnicas que soportan las DLT (y de donde viene el término Blockchain) permiten garantizar la inmutabilidad de los datos registrados y de sus relaciones temporales, lo que implica proporcionar pruebas imposibles de repudiar, así como la posibilidad de que las verificaciones puedan ser abiertas y realizadas por cualquier parte.

Estas características permiten considerar un gran número de aplicaciones, la mayoría de las cuales suponen la eliminación de mecanismos de intermediación y del uso registros centrales para realizar tareas como la compensación en transacciones económicas o la verificación de datos. Si bien las DLT son fundamentalmente conocidas por uso en las llamadas criptomonedas hay un amplísimo rango de aplicaciones potenciales, incluyendo los llamados *smart contracts*, la identidad digital, la trazabilidad en cadenas de suministro y la verificación de acuerdos de servicio.

Una distinción esencial en las DLT es si los nodos que mantienen los registros requieren confianza (*permissioned*) o no (*permissionless*) para participar en el consenso que define el registro distribuido. Se podría decir que las DLT *permisionless* proporcionan un soporte más completo a las ideas de descentralización y desintermediación, ya que potencialmente cualquier nodo puede participar en el consenso, y son las que más atención pública han recibido, con el ejemplo paradigmático de Bitcoin. Pero la realidad es que este tipo de DLT presenta serios problemas, tanto en términos técnicos (como los retardos en las actualizaciones del consenso para registrar transacciones) como de los costes que suponen la ejecución de los algoritmos de consenso y actualización, hasta el punto de requerir unos recursos tan altos que en la práctica el sistema queda bajo el control de un número muy limitado de actores. Además, en muchos de los escenarios de aplicación hay requisitos legales que no pueden satisfacerse en un entorno que no requiere un conjunto de requisitos mínimos para los nodos participantes. Por ello, en una gran mayoría de las aplicaciones públicas o comerciales, las DLT *permissioned*, en las que los nodos participantes deben ser aceptados formal y previamente a su participación por los otros nodos (y, típicamente, establecer algún tipo de compromiso contractual), constituyen la elección natural.

El interés en las DLT y las oportunidades de aplicación que suponen se han traducido en una intensa actividad para garantizar la disponibilidad de tecnologías abiertas, tanto en lo que se refiere a implementaciones de código abierto, como en la definición de estándares para favorecer la interoperabilidad a la hora de desplegar infraestructuras y su uso por parte de diferentes aplicaciones.

La aplicación de estándares es poco común en un sector como el de las aplicaciones Internet, donde lo habitual es que un único proveedor tenga una posición de monopolio de-facto y toda la industria se adapte a ellos, como en el caso de los llamados *hexascale cloud providers*. Pero los estándares siguen siendo un componente esencial para garantizar un mercado competitivo y un entorno de innovación abierto en cualquier ámbito tecnológico. Basta con que pensemos en lo que supondría hacer un traslado masivo de cuentas de correo entre dos proveedores globales, o trasladar las aplicaciones que se ejecutan en un proveedor de infraestructura cloud, y lo comparemos con el proceso de cambiar de proveedor de telefonía móvil conservando el número. Los estándares no sólo garantizan la interoperabilidad, sino que facilitan las acciones de regulación necesarias para mantener la competencia y proteger al consumidor. Hay una oferta de "servicios Blockchain" por parte de muchos, si no todos, los grandes proveedores de cloud. Y aquí el término "Blockchain" sí está bien empleado, porque solamente ofrecen el almacenamiento de datos de manera que pueda verificarse su sucesión temporal, pero no los mecanismos de consenso distribuido y abierto, a menos que consideremos que el hecho de que el proveedor esté de acuerdo consigo mismo constituye un nivel de consenso aceptable.

La mayor parte de las actividades de estandarización en este ámbito se ha enfocado al análisis de casos de uso, analizando cómo las DLT podrían incorporarse a prácticas abiertas ya definidas en diferentes escenarios. Pero hasta hace un tiempo no se habían considerado los aspectos operacionales, relativos a la gestión y control de este tipo de infraestructuras y la prestación de servicios basados en ellas. Este es el objetivo del ETSI ISG PDL. Los ISG (*Industry Specification Group*) de ETSI son comunidades abiertas para la discusión y creación de especificaciones que garanticen la interoperabilidad de las tecnologías objeto de trabajo por el grupo. Y es importante resaltar que, aunque el objetivo fundacional de ETSI está relacionado con las comunicaciones (las siglas ETSI corresponden a *European Telecommuncations Standards Institute*), hace tiempo que la convergencia en las TIC ha hecho que cada vez trabaje más en el campo de estas tecnologías en un sentido amplio, extendiendo la base de sus miembros a otros entornos, como la industria informática o la automovilística, por citar dos ejemplos característicos.

El objetivo del grupo PDL (*Permissioned Distributed Ledgers*) de ETSI es analizar los requisitos para la operación de este tipo de registros distribuidos y definir una serie de procedimientos abiertos para ellos, con el propósito de crear un ecosistema abierto de soluciones a nivel industrial y que puedan ser desplegadas por diferentes sectores y con diferentes modelos de gobernanza, de manera que se facilite la aplicación de estas tecnologías y contribuir a la disponibilidad de infraestructuras TIC abiertas, seguras y fiables. Los fundadores de PDL son conscientes no sólo del trabajo ya realizado por otras organizaciones en relación a casos de uso y aplicabilidad, sino también de los resultados disponibles en forma de software libre. El grupo los considera como puntos de partida y sus planes pasan precisamente por considerar los primeros como escenarios de aplicación y los segundos como base fundamental de las especificaciones y recomendaciones que el grupo producirá.

El documento que define los términos y procedimientos para el trabajo del ISG PDL considera los siguientes mecanismos de operación como los primeros objetivos del grupo:

- La validación de los nodos participantes. Un esquema de confianza requiere la definición de mecanismos de participación claros, tanto legales como técnicos, y la realización de una evaluación de los participantes que permita garantizar la futura operación de la infraestructura.
- Los procedimientos de consenso. Como veíamos anteriormente, una de las ventajas de un esquema basado en confianza es la optimización de los costes de registro transacciones, mediante esquemas de consenso adecuados. En infraestructuras distintas, con participantes y esquemas de participación diferentes, podrán establecerse diferentes procedimientos de consenso, y disponer de una descripción de los mismos y su adecuación a diferentes situaciones puede ahorrar mucho esfuerzo (y frustraciones) a los proveedores y usuarios.
- Los mecanismos de transacción. De manera similar al punto anterior, se trata de disponer de un análisis y de recomendaciones relativas a cómo las transacciones deben publicarse y ejecutarse, dependiendo de las características de la infraestructura. En este sentido, es importante resaltar la relevancia de las fuentes y los conductos de datos que proveen la información para ser registrada, tanto en términos de seguridad y fiabilidad como en aspectos relacionados con la privacidad.
- La automatización de las operaciones. Establecer los procedimientos que permitan automatizar la operación y gestión de los nodos participantes en un registro distribuido, y del registro como un todo, sin poner en riesgo los objetivos de interoperabilidad y facilitando el uso de diferentes

modelos de despliegue. Dentro de estos procedimientos de automatización, son especialmente relevantes el intercambio de eventos y la coordinación de las respuestas a los mismos.

- Los requisitos para proveer *PDL-as-a-Service*. En un entorno en que el consumo de servicios "nativos de la cloud" es cada vez más demandado, resulta natural explorar las condiciones en las que estas infraestructuras podrían ser proporcionadas con modelos de servicio nativos. Este objetivo de PDL incluye tanto el alojamiento de nodos en *clouds* públicas como las condiciones para prestar un servicio integral por un proveedor de *cloud*, evitando las condiciones de unilateralidad que señalábamos anteriormente.
- El escalado de las infraestructuras. Hemos visto que uno de las justificaciones esenciales para este tipo de registros es el poder garantizar unas mínimas prestaciones en cuanto a los tiempos necesarios para completar transacciones. Dado que a medida que el número de participantes y el volumen de transacciones aumenten hay un riesgo importante de degradación en este aspecto, el grupo explorará y definirá procedimientos para el adecuado escalado de los registros que permitan garantizar su naturaleza abierta e interoperabilidad entre sus componentes.
- La interconexión entre registros. Es previsible que diferentes registros necesiten el intercambio de datos y transacciones entre ellos, lo cual no implicaría necesariamente su convergencia en un registro único. El grupo pretende ir más allá de garantizar la integración de diferentes participantes dentro de un registro distribuido concreto, y explorar los procedimientos para que pueda darse la interconexión entre registros, analizando los diferentes grados de interconexión y las técnicas para llevarla a cabo.

Creemos que ETSI ISG PDL ha llegado para cubrir un hueco importante en el entorno de las DLT, no sólo en el aspecto de sus objetivos tecnológicos, sino también en lo relativo a demostrar la viabilidad de soluciones abiertas que incluyan una diversidad de implementaciones y estilos de despliegue. Los ISG de ETSI son entornos abiertos, a los que cualquier participante, de cualquier sector, puede unirse, y los requisitos para participar son extremadamente sencillos de cumplir. Los resultados del grupo serán esenciales para la consolidación de un ecosistema realmente abierto en un campo que se prevé será crítico para la evolución de las TIC. Todas las manos son pocas para esta apasionante tarea.

Lluís Alfons Ariño

-

ES DIRECTOR TI EN LA UNIVERSITAT ROVIRA I VIRGILI Y CO-CONVENOR DEL CASO DE USO DE DIPLOMAS DEL EUROPEAN BLOCKCHAIN PARTNERSHIP.

2.1

LOS CASOS DE USO

Proyecto europeo EBSI y Diplomas use case

Lluís Alfons Ariño
UNIVERSITAT ROVIRA I VIRGILI

CONTEXTUALIZACIÓN DE LA INFRAESTRUCTURA EN LA ECONOMÍA DIGITAL

La primera revolución industrial, en el siglo XVIII, impulsada por la energía de vapor, catalizó la creación de las primeras fábricas y la migración del entorno rural al urbano

La segunda revolución industrial, entre los siglos XIX y XX, impulsada por la electricidad catalizó la industrialización y la producción en masa, y gracias a medios de transporte y comunicación más rápidos como el ferrocarril, se propició la recolocación.

La tercera revolución industrial y la primera revolución de la información, a finales del siglo XX, impulsada por la automatización electrónica y el nacimiento de las primeras computadoras, posibilitaron el conocimiento basado en internet.

Estamos inmersos ahora en la cuarta revolución industrial y en la segunda revolución de la información, tenemos el equivalente a las carreteras de alta velocidad para el mundo digital, es decir, la Internet de alta velocidad, y el fenómeno disruptivo para el sector de la información producido por la descentralización del aprovisionamiento de la misma (web 2.0, redes sociales)

Esta cuarta revolución industrial es, sin embargo, fundamentalmente diferente. Se caracteriza por una gama de nuevas tecnologías que fusionan el mundo físico, digital y biológico, impactando a todas las disciplinas, economías e industrias, e incluso desafiando las ideas sobre lo que significa ser humano.

La estrategia de los negocios se basará en la toma de decisiones informada, la información se convierte en la nueva fuente de energía en la economía digital. Disponer de datos fiables y confiables será un punto estratégico para la supervivencia y expansión de las empresas.

Y no debemos olvidar que en este contexto el cliente se convierte en el foco, y el ser humano se convierte en la diferencia

En la economía digital de la Unión Europea, en pro del mercado único digital, existe la necesidad de una nueva infraestructura, digital, de alta velocidad que debe:

- Garantizar la integridad de la información transportada
- Respetar la privacidad de la información, pero poder probar la trazabilidad de la misma
- Garantizar que dicha infraestructura será capaz de transportar todo tipo de información, con independencia de los formatos de la misma y respetando los estándares
- Garantizar la interoperabilidad de la información transportada para garantizar la comunicación transfronteriza
- Estar dotada de inteligencia para facilitar la incorporación y salida de ésta infraestructura de alta capacidad a los sistemas heredados
- Robusta. Más que eso, inmutable

En definitiva, una infraestructura de alta capacidad y digital de confianza ¡Demos la bienvenida a EBSI! El servicio europeo de infraestructura Blockchain.

Según el Massachusetts Institute of Technology, "Blockchain hará por el negocio lo que Internet hizo por la información".

Desde la Unión Europea, el mensaje también es claro. Según Mariya Gabriel, Commissioner for Digital Economy and Society, "Blockchain es una gran oportunidad para Europa y sus Estados miembros para repensar sus sistemas de información, impulsar la confianza de los usuarios y la protección de datos personales, ayudar a crear nuevas oportunidades de negocio y establecer nuevas áreas de liderazgo, beneficiando a los ciudadanos, a los servicios públicos y a las empresas*".*

EBSI -EUROPEANBLOCKCHAIN SERVICE INFRASTRUCTURE

Singularidad y complejidad

Normalmente los proyectos desarrollados des de la Comisión Europea en DG-CONNECT y DIGIT, suelen reflejarse en estándares de referencia o directrices que, una vez fijados, conllevaran un proceso posterior de implementación en productos y/o servicios (normalmente no llevado a cabo por la propia Comisión).

En este caso, el modelo basado en la estandarización a la par que se van desarrollando cuatro casos de uso, que sirven para ir retroalimentando al propio proceso de estandarización, representa un reto añadido. Se puede comprender que la complejidad de gestión de cuatro casos de uso con todos los Estados miembros implicados, no es tarea fácil.

Ejes de trabajo

El proyecto se divide en dos grandes grupos de trabajo: el llamado "*Policy group*" y el llamado "*Technical group*".

El "Policy group" (grupo de políticas), trabajará para lograr el máximo potencial de los servicios basados en Blockchain en beneficio de los ciudadanos, la sociedad y la economía en toda Europa.

En relación a EBSI, el grupo de políticas tiene asignadas las siguientes responsabilidades:

1. Proporcionará orientación general a DG CONNECT sobre el desarrollo y la puesta en funcionamiento de la Infraestructura Europea de Servicios Blockchain (EBSI)
2. En cooperación con la Comisión Europea, identificará y seleccionará nuevos casos de uso adicionales (servicios o procesos digitales transfronterizos) a ser implementados por la Infraestructura Europea de Servicios de Blockchain (EBSI)
3. Contribuirá a establecer las prioridades generales de EBSI, incluida la adopción de directrices para el desarrollo y uso de EBSI
4. Evaluará las necesidades de financiación para la Plataforma de Servicio Central EBSI y sus componentes futuros que se reflejarán en el programa de trabajo del CEF. Hacer propuestas para el Programa de trabajo anual de CEF y financiación para el EBSI que incluirá un análisis de la entrega de "proyectos" en curso del EBSI e identificará los nuevos "proyectos"
5. Trabajará con la Comisión Europea en la supervisión de la gobernanza del EBSI y el desarrollo técnico, y cómo apoya las políticas de la UE a los tomadores de decisiones relevantes
6. Monitorización y mapeo de desarrollos de políticas relevantes (a nivel nacional e internacional) en Blockchain y tecnologías de contabilidad distribuida y análisis del impacto que la infraestructura europea de servicios de Blockchain puede tener en estos desarrollos de políticas y viceversa

El "*Technical group*" (grupo técnico) tiene como objetivo principal la construcción en si de EBSI, dando respuesta a las necesidades identificadas por los diferentes casos de uso, utilizando tecnología *OpenSource*, llevando el estadio de los elementos tecnológicos a un estadio de madurez que posibilite la estandarización de los mismos para su propia adopción.

Casos de uso

Como he mencionado anteriormente, la construcción de EBSI se está haciendo de manera colaborativa, bajo un modelo de desarrollo ágil, con el desarrollo de cuatro primeros casos de uso que están sirviendo como puntos de alimentación para el diseño y construcción final de EBSI.

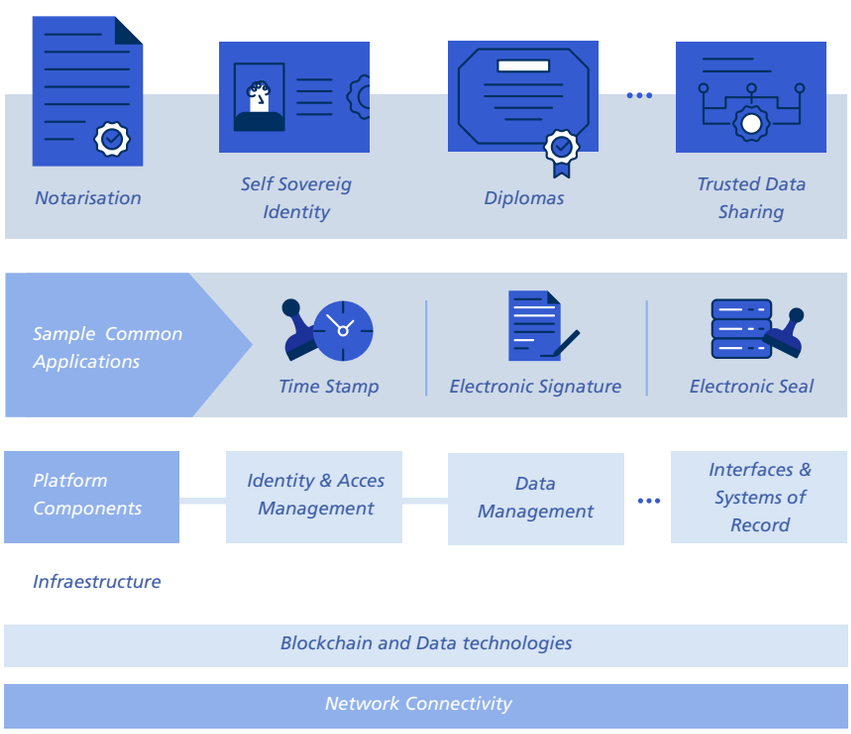
En 2019 se han seleccionado los siguientes cuatro casos de uso:

1. Notarización: gracias a Blockchain posibilitar la creación de trazas de auditoría digital confiables, automatizar las verificaciones de cumplimiento en procesos urgentes y probar la integridad de los datos
2. Diplomas: con el objetivo de devolver el control a los ciudadanos al administrar sus credenciales educativas, reduciendo significativamente los costos de verificación y mejorando la confianza en la autenticidad de las actividades formativas acreditadas
3. Identidad Genérica Soberana: implementando una capacidad genérica de identidad auto-soberana, que permite a los usuarios crear y controlar su propia identidad a través de las fronteras sin depender de autoridades centralizadas
4. Intercambio de datos de confianza: para compartir datos de forma segura (por ejemplo, números de identificación de IVA IOSS e importar ventanilla única) entre las autoridades aduaneras y fiscales en la UE

Para cada caso de uso se ha establecido un grupo de usuarios compuesto y dirigido por un Estado miembro. Estos grupos de usuarios tienen como objetivo entregar una primera versión de EBSI con funcionalidades para cada caso de uso a principios de 2020.

En la Figura 1, se puede observar el esquema conceptual de EBSI, destacando que uno de los grandes valores es que garantizará la interoperabilidad entre diferentes tecnologías de red Blockchain (por ejemplo, Ethereum y Hyperledger), garantizará la independencia de las capas superiores respecto a la tecnología concreta de transporte, respetará la independencia de las aplicaciones o sistemas de información sectoriales de la tecnología y servicios y componentes propio EBSI.

Figura 1 – Esquema conceptual de EBSI y vinculación con los casos de USO



La arquitectura de cada nodo estará compuesta por múltiples capacidades que posibilitan la prestación de servicios, y la capacidad de los Estados miembros para desarrollar más.

¿Por qué es importante este proyecto, además de por las oportunidades que Blockchain brindará?

Porque EBSI pasará a ser un *BuildingBlock* de la Unión Europea y eso implica que pasará a ser un servicio nuclear para la prestación de servicios públicos en la Unión Europea.

Básicamente, EBSI funcionará con la colaboración de los Estados miembros que operarán nodos EBSI a nivel nacional. Estos nodos podrán proporcionar todos los componentes necesarios para crear y transmitir transacciones dentro de la red Blockchain de confianza.

EL CASO DE USO DE DIPLOMAS

¿Qué es el EBSI Diplomas use case?

Es importante contextualizar la palabra Diplomas, puesto que podría llevar a confusión. La palabra Diplomas debe entenderse desde un sentido amplio, no tan sólo el título universitario. Es bajo este concepto que debe entenderse que EBSI ha de poder dar respuesta tanto el llamado aprendizaje a lo largo de la vida (*LongLife Learning*), como a los llamados caminos personales de aprendizaje (*Personal Learning Pathways*).

Principales actores identificados

A continuación, se detallan los principales actores identificados, que proporcionan una visión

más clara de la amplia concepción de educación bajo el acrónimo "Diplomas". Así, identificamos:

1. Estudiante / trabajador / solicitante de empleo / solicitante universitario
2. Roles institucionales educativos estándar
   a. Creador de contenido: crea contenido de aprendizaje que puede estar en formato en línea o combinado
   b. Entrega de contenido: entrega de enseñanza cara a cara, en línea o en formato mixto.
   c. Asesor educativo: evaluación de estudiantes, cursos o calificaciones
   d. Administración educativa: respalda una amplia gama de procesos educativos
   e. Oficial de inscripción educativa: generalmente un registrador responsable de inscribir nuevos estudiantes y atender consultas relacionadas con la validación de diplomas de estudiantes (pasados o presentes)
   f. Gestión de la certificación educativa: gestión general de los certificados ofrecidos por una institución educativa
   g. Finanzas educativas: gestión financiera, como recibir honorarios de estudiantes; pago de consultores externos
   h. Informática educativa (VLE, sistemas de registro de estudiantes, etc.), que deberá vincularse al sistema de acreditación de Blockchain
3. Empresas MOOC y otras plataformas de aprendizaje gratuitas, por ejemplo Moodle, Canvas, Blackboard, edX, Coursera, FutureLearn
4. Empleadores
   a. Gerente de capacitación / RR. HH. - ejecución de programas / plataformas de capacitación corporativa. Cuidar el perfil de habilidades de la empresa
   b. Contratación de personal nuevo o de reemplazo
5. Compañías de reclutamiento - varias
   f. Agencias nacionales / gubernamentales
   g. Agencia Nacional de Acreditación - institución de acreditación; cada programa / curso universitario
   h. Servicio de verificación nacional (por ejemplo, en España): verificación académica controlada centralmente y emisión y renovación de licencias de operación de la institución.
   i. Política educativa / legal: garantizar que las universidades cumplan con las regulaciones nacionales
   j. Verificación de acreditación internacional, por ejemplo comprobar que un título del Este es válido
   k. Agencia de gobierno educativo: responsable del gobierno general de las universidades, por ejemplo para determinar los requisitos previos para las organizaciones que desean ofrecer servicios educativos en varios niveles educativos
   l. Otras agencias gubernamentales. Por ejemplo salud: ¿tiene un médico la calificación adecuada? (Legal, bancario, etc.)
6. Gremios específicos del sector, por ejemplo la capacitación anual para abogados, médicos, salud y seguridad; controles ambientales Muchos de estos están sujetos a regímenes regulatorios en los diferentes Estados miembros

7. Agencias europeas, tanto de la UE como de fuera de la UE
8. Agencias no europeas, por ejemplo para un acuerdo a nivel de la UE sobre reconocimiento de títulos
9. Refugiados: es reconocido que los refugiados constituyen un desafío importante para los estados nación receptores. En este sentido, por ejemplo, las calificaciones existentes no pueden validarse fácilmente por varias razones (incluida la desaparición de la institución original que emite el diploma); la prueba de identidad puede ser difícil (los refugiados pueden no poseer documentos de identidad formales), etc. Los refugiados a menudo tienen que obtener nuevas calificaciones para asegurar el empleo en los países receptores

¿Qué no es el caso de uso de Diplomas?

- Una solución solo para instituciones de Educación superior
- A pesar de las posibilidades de la tecnología para facilitar la interoperabilidad, una solución para los históricos desafíos en el reconocimiento mutuo de diplomas por instituciones y partes interesadas en el mercado laboral en diferentes estados miembros

¿Qué sí es el caso de uso de Diplomas?

- Una oportunidad para todo tipo de educación, la educación a lo largo de toda la vida de una persona, y para los caminos de aprendizaje personalizados
- Una solución para mitigar el fraude
- Una solución para grupos vulnerables y marginados (como los refugiados)

El reto real del caso de uso

Aunque pudiera parecer lo contrario, la tecnología no es, de lejos, el reto mayor del proyecto. Es la falta de HOMOGENEIDAD en el sector educativo europeo, ya que corresponde a los Estados miembros determinar los marcos y regímenes educativos adecuados a los contextos SOCIOCULTURALES y ECONÓMICOS ÚNICOS que prevalecen en cada país.

Por definición, los actores del mundo educativo tienden a ser autónomos y están informados sobre las posibilidades de la tecnología, a pesar de que pueda parecer lo contrario.

Las líneas de investigación (y también los intereses) necesariamente han llevado a una falta de uniformidad en los procesos relacionados con la emisión, el almacenamiento, la validación y el intercambio de información del diploma. Hay muchos proyectos vivos vinculados al concepto de Diplomas en los Estados miembros que están explorando o utilizando diferentes enfoques para abordar las mismas necesidades de negocio.

El caso de uso de EBSI Diplomas (*Diplomas API* + *Self Sovereign Identity* + *Verifiable Credentials*) es una oportunidad real para tratar de asegurar la alineación en los procesos centrales relacionados con los diplomas, particularmente en el caso de las funciones de identidad e interoperabilidad.

Alineación y oportunidades de EBSI para otros proyectos del ecosistema educativo

Lejos de verse como una amenaza, EBSI debe verse como una oportunidad para soportar y alinear diferentes proyectos europeos que, en algunos casos, estaban haciendo aproximaciones diferentes para una misma necesidad. Así, se están trabajando las sinergias con proyectos como *Erasmus Without Papers (EWP), Europass (concretamente Europass Futurism), European Student Card (ESC), EMREX (ELMO), MyAcademicID, EduGAIN*, y otras vinculadas.

Dos elementos tecnológicos disruptivos

En esta oportunidad de salto disruptivo que nos ofrecerá Blockchain al sector educativo, se han identificado dos conceptos que, por un lado y en combinación con Blockchain aportarán y posibilitarán un gran valor a la solución, pero por otro lado impactaran de manera disruptiva en el ámbito educativo en relación a cómo se están gestionando ahora mismo.

Concretamente son los conceptos de identidad soberana autogestionada (*Self Soverign Identity*) y de credenciales verificables (*Verifiable Credentials*).

El primero, la identidad soberana autogestionada, rompe completamente el modelo de gestió de identidad que hasta el momento existe en la Administración pública y el sector educativo (público y privado), donde es la propia institución quién crea y gestiona la identidad del ciudadano (estudiante). En este nuevo modelo es el propio ciudadano quien presenta su propia identidad. Por otro lado, cualquier interacción siempre pasa por la voluntad previa del ciudadano, que además tiene bajo su control exclusivo su propia información, facilitando así aspectos como el cumplimiento del RGPD, a la vez que se empodera de manera real al ciudadano (estudiante).

El segundo concepto, las credenciales verificables, abren la puerta a la estandarización en la manera de serializar la información, asegurar su integridad, su procedencia, etc.

Es en este sentido que la alineación con otros proyectos europeos, concretamente con Europass Digital Credentials, es un punto clave para avanzar en la homogeneización de los modelos educativos en los diferentes estados miembros, y las credenciales verificables serán el medio que circulará sobre esta autopista digital de alta capacidad que será EBSI.

TEMPORALIZACIÓN

Contextualización del proyecto

Hay que entender, al hilo de lo expuesto anteriormente, que el proyecto consta de cuatro grandes vertientes:

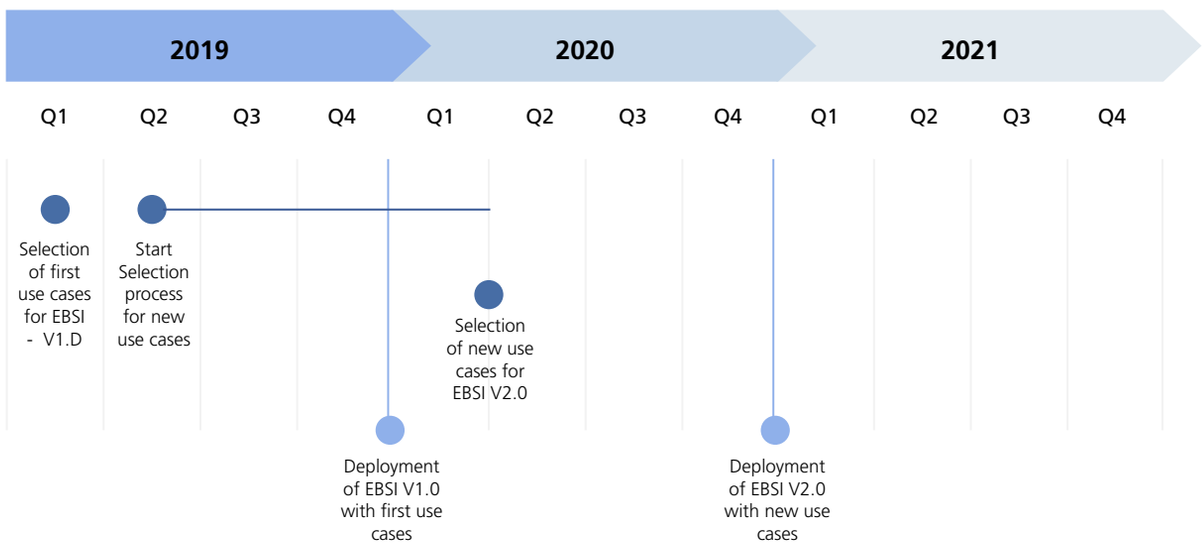
1. la generación de estándares, que requerirán del proceso correspondiente hacia Centro Europeo de Normalización
2. la generación/modificación de directrices legales, que requerirán procesos de adaptación por los estados miembros (por ejemplo, en España para educación superior hay que introducir el formato digital para la emisión del título, y otras oportunidades respecto al reconocimiento de Blockchain en si)
3. la definición y adopción de un modelo de gobernanza, que permita conocer las reglas del juego, requisitos, y garantías para todos los actores
4. la creación en si del eje tecnológico tanto por parte de la Comisión Europea, como por parte de los estados miembros, como de los actores para cada caso de uso

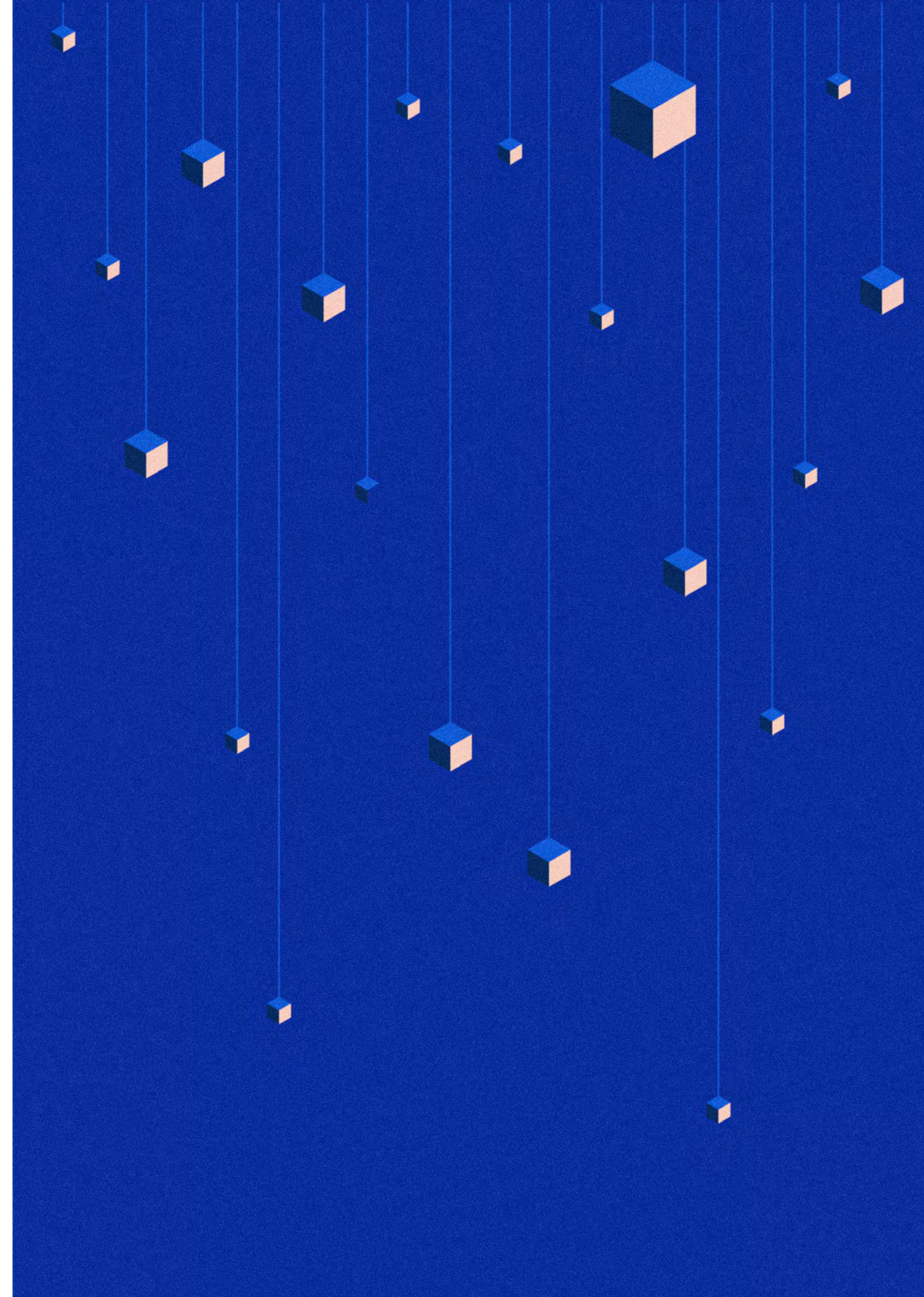
Temporalización de EBSIv1 y proyección de futuras versiones

Teniendo en cuenta que el primer objetivo de EBSIv1 es demostrar la viabilidad tecnológica y establecer los cimientos para la completitud de las historias de usuario de los diferentes casos de uso, se ha establecido un primer y ambicioso objetivo: infraestructura real, servicios reales, componentes reales, modelos de datos reales, pero datos de test.

A continuación, figura 2, observamos la planificación del proyecto para los próximos años. Como puede observarse, EBSIv1 estará ya en producción en Febrero 2020, punto a partir del cual comenzará a establecerse la interconexión con servicios y datos reales de los estados miembros. Cabe destacar la importancia del proyecto a nivel de Comisión Europea, pues los tiempos se están cumpliendo estoicamente.

Figura 2 – Timeline proyectado a 3 años






ALASTRIA

2.2

LOS CASOS DE USO

Alastria, la Blockchain pública permisionada de España

Jesús Ruiz
ALASTRIA

Alastria es un "Consorcio Red" o comunidad de personas que fomentan e implantan la tecnología de registros distribuidos (Blockchain). Con forma legal de asociación (Ley Orgánica 1/2002, de 22 de marzo), tiene plena capacidad de obrar para cumplir sus fines y funcionamiento interno democrático y coparticipativo de sus ya más de medio millar de miembros, personas de derecho público y privadas (empresas tecnológicas, cotizadas y no cotizadas, universidades, fundaciones y asociaciones, e instituciones y Administraciones Públicas).

Además de una comunidad con ecosistemas regionales en territorio nacional, y de una persona jurídica asociativa para cumplir estos fines, Alastria es una red o conjunto de nodos implantados en los servidores de sus miembros asociados. En cuanto red de nodos, Alastria es, por importancia y por su implantación temporal desde octubre de 2017, la primera Blockchain española pública (de libre asociación y baja de miembros) y permisionada (con autorización para proponer y ejecutar transacciones según un protocolo de consenso tipo PoA), cuyo desenvolvimiento operativo inicialmente ha tenido lugar, desde la constitución de la asociación, sobre una versión *Quorum de Ethereum*.

Desde el punto de vista normativo, y en cuanto red permisionada o autorizada para realizar transacciones, los socios o miembros asociados a Alastria cumplen políticas internas para que la red se desenvuelva eficientemente. Tales políticas alcanzan a aspectos relativos a:

- Derecho de la competencia, a fin de evitar y prevenir potenciales actuaciones monopolistas o colusión de determinados nodos en el contexto de los protocolos de prueba de autoridad o PoA que rigen para el cierre de transacciones
- Confidencialidad, a fin de asegurar que los socios cumplen la normativa sobre protección de datos y otras sobre privacidad, preservándose el secreto debido sobre los datos insertos en las transacciones anudadas a la cadena
- Propiedad intelectual e industrial, a fin de proteger la autoría y derechos económicos de los miembros productores de software de código abierto para la asociación y también los signos y activos merecedores de tutela legal que genera la propia Asociación
- Transparencia y gestión de conflictos de interés para garantizar una actuación transparente, legal y de óptimo cumplimiento normativo de asociados y de la propia Asociación, que defienda su reputación y cohesione la propia comunidad
- Limitación de responsabilidad de la Asociación, que previene a terceros que se relacionan con Alastria permitiéndoles conocer la medida de la responsabilidad contractual y extracontractual que contrae y asumen la Asociación y los gestores de los nodos al operar entre sí y con terceros

En los dos primeros años de actividad sin ánimo lucrativo del Consorcio Red, se ha creado una comunidad que ha favorecido y promovido efectivamente

la implantación, estandarización, protección y uso de diferentes tecnologías Blockchain (no solo sobre Ethereum) tanto a nivel nacional como transfronterizo.

En puridad, el Consorcio no ha venido prestando servicios de Blockchain a terceros, sino que se ha limitado a configurar la comunidad de nodos y promover el trabajo colaborativo de todos sobre la infraestructura distribuido. Por esa razón que no asume hoy por hoy responsabilidad por operar, gestionar o poner en funcionamiento redes DLT productivas o donde se presten servicios a terceros. Sin perjuicio de lo cual, quienes autorice la Junta Directiva de la asociación (asociados o no) prestan servicios Blockchain a los asociados, generalmente en el marco de acuerdos de organización de servicios para los asociados y usuarios de la red. En este contexto, los socios, previos informes de los Comités Tecnológico y Legal de la Asociación, aprueban las reglas comunes de tales acuerdos, a los que se adhieren libremente los interesados.

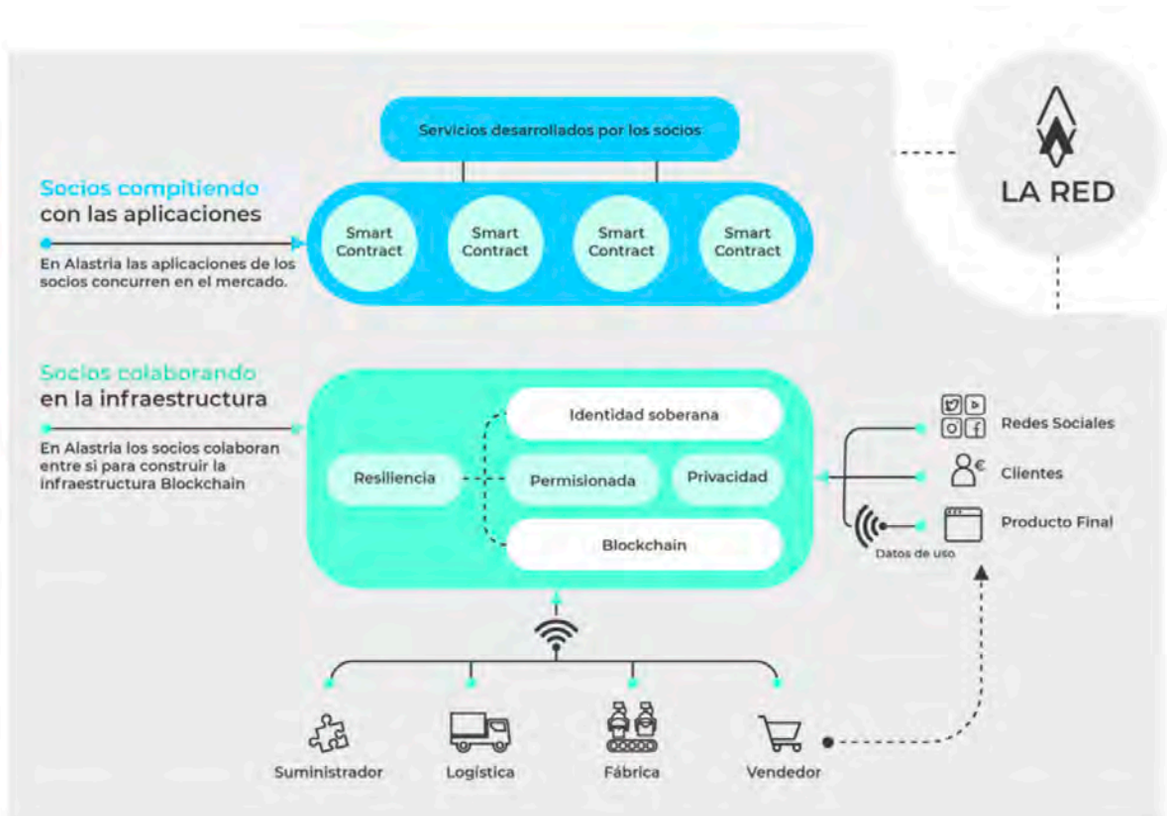
Quizá el mayor logro hasta la fecha de Alastria haya sido su proyección internacional en materia de generación y difusión de estándares sobre la tecnología de registro distribuido. Los Comités de Estándares y otros grupos de trabajo (Legal, Tecnológico, entre otros) han conseguido no solo que Alastria figure en los estándares de Blockchain que están produciendo a escala global las organizaciones ISO o ITU, sino que participe activamente en la propia definición de los conceptos relativos a Blockchain en sus comisiones y grupos de trabajo. Otro tanto está sucediendo a escala europea con los grupos de la Comisión Europea, y de las organizaciones privadas especializadas como INATBA.

En este terreno, las guías básicas y documentos técnicos internos de Alastria (e. g., las Políticas Operativas de Gobierno) constituyen un modelo para la configuración de las redes públicas permisionadas en otras jurisdicciones y también en áreas regionales como Iberoamérica (e. g., proyecto LACChain). Los estándares de la infraestructura sirven tanto para una red principal como para otras redes complementarias o laterales, y las políticas de desarrollo o subpolíticas técnicas de gobierno de los nodos de la red principal (críticos, incluyendo a validadores, y operadores regulares) sirven como modelo de permisionado o autorización de transacciones en Blockchain en cualquier sistema a escala planetaria, sin perjuicio de que la escalabilidad de la operativa de red es limitada a nivel nacional y aún en un ámbito restringido a industrias punteras como la financiera, sanitaria o energética, sin perjuicio de la importancia de determinados servicios de certificación –e.g., en el ámbito académico-. Merece subrayarse a este respecto que en todo momento Alastria ha priorizado el criterio de neutralidad tecnológica y el principio de universalidad, acogiendo protocolos tecnológicos que permiten el mayor uso y adopción posibles de la red. Las guías operativas y demás normas internas van actualizando los requisitos de funcionamiento y los niveles de servicio a los que se vinculan los nodos que habilitan la infraestructura.

No puede olvidarse, por otro lado, que el dinamismo de Alastria lleva continuamente a una adhesión creciente de miembros interesados en ensayar la tecnología distribuida. Si bien solo los nodos más activos tratan de organizar red industrialmente, el principio de no exclusividad y no prohibición de contribución al desarrollo de estándares o tecnologías alternativas hacen del Consorcio un ente vivo, que en dos años ha tenido que superar ya numerosas dificultades derivadas de la heterogeneidad y diversidad de propósito entre los socios. La programación y revisión cooperativa y sin interés comercial de los protocolos informáticos está facilitando el mantenimiento de la red -inicialmente solo de prueba, y hoy preparatoria de producción o preindustrial bajo el nombre Telsius- con medios materiales y humanos aportados por todos, en buena medida de forma desinteresada. Tampoco están escatimando esfuerzos los asesores legales de empresas y despachos asociados para dar consejo legal eficiente en las numerosas materias concernidas al respecto del desarrollo de la comunidad.

Igualmente conviene recordar, por último, que uno de los fines de Alastria es crear un modelo de identidad digital, común e interoperable, idóneo para el uso de los servicios de la Red. Al efecto se han propuesto en los ecosistemas y en varios foros internacionales las hipótesis y elementos que un modelo autogestionado o soberano de identidad digital en la Red (Alastria ID), que está concienciando interna y externamente sobre la viabilidad y utilidad de la firma electrónica y la autenticación digital para preconstituir prueba de las operaciones y gestionar el comercio y las transacciones personales de forma segura en una red distribuida.

Figura 3 – Cómo funciona Alastria



José Luis Hernández

-

ES DIRECTOR TI EN LA UNIVERSIDAD CARLOS III DE MADRID.

Francisco Cruz

-

ES TÉCNICO ESPECIALISTA EN TECNOLOGÍAS EDUCATIVAS EN LA UNIVERSIDAD CARLOS III DE MADRID.

2.3

LOS CASOS DE USO

Usando la tecnología Blockchain para la certificación y acreditación de competencias en cursos SPOCs

José Luis Hernández Fernández
Francisco Cruz Argudo
UNIVERSIDAD CARLOS III DE MADRID

ANTECEDENTES

Los nuevos paradigmas que se vislumbran en los modelos educativos están produciendo que los formatos actuales de títulos completos de larga duración vayan evolucionando a una certificación por competencias adquiridas en periodos de menor duración. Esta desagregación de la Educación hace que cobre un gran valor la posibilidad de tener una certificación digital mucho más dinámica a la hora de generar y de utilizar por parte del usuario/estudiante mediante la creación de una cartera digital (*wallet*) unida a su identidad. Plataformas formativas como edX o Coursera generan certificación digital por un coste adicional que depende del tipo y duración del curso. Así podemos estar hablando de unos cuantos dólares para curso tipo MOOCs tradicionales hasta miles de dólares para micro máster y productos que se extienden algo más en el tiempo. Es en este nuevo entorno es donde se origina y se desarrolla el caso de uso de la utilización de la tecnología Blockchain en el entorno académico de emisión de títulos.

La Universidad Carlos III de Madrid posee una dilatada experiencia en el uso de la tecnología como apoyo a la mejora de la Educación desde sus primeros años de funcionamiento (proyecto ARCA, proyecto AdaMadrid, Mbone,…). Esto ha sido refrendado en los dos últimos planes estratégicos aprobados por la Universidad y en concreto por el último plan estratégico 2016- 2022[44], donde de manera muy clara se apuesta por la digitalización, la innovación docente y el apoyo de las tecnologías en todo lo relacionado con el proceso de enseñanza/aprendizaje. Lo que normalmente se conoce como "EdTech". Para ello, la universidad lleva a cabo distintas iniciativas de manera regular dentro de la comunidad académica como: cursos de formación, seminarios, colaboración con organizaciones de estudiantes….

Dentro de esta línea de trabajo, en el año 2011 se crea una unidad multidisciplinar de apoyo a la innovación docente. Esta unidad que recibe el nombre de UTEID[45] está formada por miembros de varios Servicios de la Universidad: Informática y Comunicaciones, Biblioteca, Audiovisuales y Servicio de Grado. Además, cuenta con varios docentes de departamentos como Comunicación Audiovisual o Ing. Telemática, cuyo campo de trabajo/investigación es precisamente la innovación educativa.

[44] https://planestrategico.uc3m.es
[45] Unidad de Tecnología Educativa e Innovación Docente https://www.uc3m.es/biblioteca/unidad- tecnologia-educativa-innovacion-docente

En el año 2012 se empieza a trabajar en los primeros SPOCs, aunque este término fue acuñado en 2013 por el profesor Armando Fox[46]. Se trata de los 'cursos Cero[47]', cursos que hasta ese momento se daban de manera presencial para alumnos de nuevo ingreso y que empiezan a tener una componente online que se desarrolla durante el mes de agosto. La inclusión de este tipo de iniciativas es un primer intento de uso de la metodología "*Flipped Classroom*". En las primeras ediciones se empieza con una versión libre del software de la "*Khan Academy*". A partir del año 2014 se evoluciona estos cursos a la plataforma *Open edX*.

En todo este contexto, se produce nuestra incorporación a la plataforma de MOOCs *edX*[48] en el año 2014. Siendo una de las tres universidades de España que forman parte de esta plataforma global de enseñanza en la actualidad. Además de la plataforma edX, la Universidad Carlos III de Madrid forma parte también de la plataforma *Miriadax*. Teniendo desde ese momento, una política institucional de creación e impartición de MOOCs.

Además de los 'cursos Cero', La Universidad Carlos III de Madrid empieza a desarrollar un programa de innovación docente más generalizado en el año 2013 para fomentar/extender el uso de nuevas metodologías que mejoran la docencia. Para ello, en ese mismo año dentro de las convocatorias de innovación docente que ya existían en la universidad, se incluyen la creación de SPOCs[49] como cursos de acompañamiento de asignaturas regladas. El objetivo de estos cursos de acompañamiento es llevar parte del contenido teórico de la asignatura a la plataforma de aprendizaje, en nuestro caso *Open edX*, cómo se ha comentado anteriormente. Durante este tiempo se ha consolidado tanto el número de alumnos, como el de sus cursos involucrando a los distintos campus que tiene la universidad. Dentro de este contexto, en la convocatoria de innovación 2015, un grupo de profesores del Dpto. de Electrónica solicitó realizar un curso que habilitase a los alumnos en las competencias para las prácticas en los laboratorios. Este curso es transversal y afecta a distintas titulaciones en las cuales se incluyen este tipo de prácticas. En este curso, para aquellos alumnos que lo superan, se nos pedía poder generar algún tipo de acreditación de superación del curso para poder acceder al laboratorio con esos conocimientos adquiridos y poder entonces realizar las prácticas. En el curso 2016/17 se emiten las primeras acreditaciones digitales que son generadas de forma automática por nuestra plataforma LMS (*OPEN edX*) para todos aquellos estudiantes que superan el curso por encima de la nota que define el profesor. Está plataforma, al ser una plataforma MOOC lleva en origen incluido la generación de este tipo de certificaciones digitales. En ese curso 2016/17 se emitieron un total de 485 certificados digitales.

Incorporación de la tecnología Blockchain

El auge de esta tecnología va unida a la aparición de nuevos paradigmas en la Educación como son los MOOCs, la certificación por competencias, micro-masters, nano-grados, desagregación de la educación, competencias digitales, etc. que hacen que cada vez se vea como una necesidad mayor utilizar las ventajas que aporta su uso dentro del ámbito de la Educación. La idea de utilizar dicha tecnología en temas de certificación hace que muchas universidades y empresas privadas vean este campo con grandes posibilidades de aplicación y crecimiento.

Entre las ventajas que ofrece este tipo de certificación (Grech, y otros, 2017) frente a las tradicionales en papel o las digitales son:

- No pueden falsificarse. Es posible verificar con certeza que el certificado fue emitido originalmente por y para las mismas personas indicadas en el certificado
- La verificación del certificado puede ser realizada por cualquier persona que tenga acceso a la cadena de certificación, con software de código abierto de fácil acceso, no es necesario partes intermedias
- Como no se requieren partes intermedias para validar el certificado, éste aún puede ser validado, incluso si la organización que lo emitió ya no existe o ya no tiene acceso al registro emitido
- El registro de certificados emitidos y recibidos en un Blockchain solo puede ser destruido si se destruye cada copia en cada ordenador del mundo que aloja el software

Con estas ventajas, a nadie se le escapa que se vislumbra un aumento en la utilización de dicha tecnología en el ámbito educativo. Además, los certificados emitidos mediante está tecnología aportan: Seguridad, Privacidad, Transparencia, Validez global y son Auditables.

Desde el año 2016 el Servicio de Informática y Comunicaciones de la UC3M (SDIC)[50] venía siguiendo las iniciativas del uso de la tecnología Blockchain dentro del ámbito de la educación. En concreto, el proyecto

[46] https://www2.eecs.berkeley.edu/Faculty/Homepages/fox.html
[47] https://www.uc3m.es/ss/Satellite/Grado/es/TextoMixta/1371213440582/Cursos_Cero
[48] https://edx.org
[49] https://www.uc3m.es/uc3mdigital/spocs
[50] https://sdic.uc3m.es

Open Source liderado por el MIT y la empresa Learning Machine que recibe el nombre de Blockcerts[51]. En noviembre de 2017 se empezó a trabajar con este software para ver las distintas posibilidades que ofrecía y sus posibles aplicaciones. Entre noviembre de ese año y marzo de 2018 se realizaron tareas de aprendizaje en su uso: instalaciones, configuración y personalizaciones de los distintos componentes del mismo. En marzo de 2018 ya se disponía de los primeros prototipos de acreditaciones utilizando la solución Blockcerts. Durante los siguientes meses estuvo trabajando con el software (traduciendo ciertas partes al idioma Español) y analizando su arquitectura de implantación para poder llevarlo a un escenario de producción real. Esta primera fase del proyecto se terminó con la emisión de los primeros certificados reales en septiembre de 2018 sobre la red pública Bitcoin.

En la primera versión, como se ha comentado anteriormente, las acreditaciones se estaban validando en la red Bitcoin. En la nueva emisión de acreditaciones la red utilizada ha sido Ethereum. *Blockcerts* es una solución "agnóstica" en cuanto a la tecnología de Blockchain que utiliza. Es decir, con la misma capa de usuario es posible emitir un mismo certificado en distintos tipos de redes. Hasta este momento Blockcerts soportaba las redes públicas Bitcoin y Ethereum, pero desde hace unos meses también es posible desplegar *Blockcerts* sobre redes permisionadas mediante la utilización de *Hyperledger Fabric*[52].

Tal y como funcionan *Blockcerts* los datos están "off-chain" es decir, no se guarda ningún tipo de dato de carácter personal dentro de la cadena de bloques. Lo que se valida es un *hash* de la raíz del árbol de *Merkel* que se construyen con los distintos certificados codificados en formato *openbadges*. Es decir, en una única validación es posible validar hasta 2.000 certificados. Estos "ficheros" permanecen en todo momento en la organización emisora de los mismos y son referenciados mediante URLs. Esto hace que la solución cumpla con los requisitos del RGPD[53].

El proyecto *Blockcerts* está fuertemente basado en estándares lo que garantiza y facilita la evolución del mismo.

- *IMS Open Badges*
- *W3C Verificable Claims*
- *W3C Linked Data Signaturas*
- *W3C/ Rebooting web of Trust Decentralized Identifiers*
- *CTDL/Credential Engine registry*

EL PROYECTO

El proyecto tenía por objetivo la generación de acreditaciones mediante la utilización de la tecnología Blockchain que genera nuestra plataforma LMS (OPEN edX) y que ya estábamos emitiendo en formato digital. Para ello, se ha tenido que realizar una serie de tareas previas antes de poder tener un servicio plenamente operativo. Primero, se ha tenido que desplegar un servidor con todos los módulos que incorpora la solución Blockcerts y que está formado por: *cert-issuer, cert-tools, cert-verifier* y los módulos de verificación de acreditaciones. Además, se ha tenido que instalar software adicional ya que parte de este software está basada en la tecnología de Google *(Polymer*). Para servir los certificados se ha instalado un servidor *nginx* y se utiliza el módulo "*verifier*" para diseñar y mostrar los certificados.

Una vez instalado el software, se han tenido que diseñar distintas plantillas donde se fija la parte estática institucional de la acreditación y desarrollar *scripts* para ir rellenando la parte variable de cada uno de las acreditaciones (nombre del curso, nombre del alumno, metadatos del mismo, logo, firma,…). Se ha desarrollado una capa de servicio donde se automatiza todo el proceso: Desde el acceso a los certificados de la plataforma *LMS (OPEN edX)*, hasta procesar dicha información y crear documentos válidos (en nuestro caso *JSON*) que puedan ser procesados por la solución *Blockcerts*. Una vez procesada y generada toda esa información es almacenada en una base de datos (*MongoDB*) para poder tener una correlación entre cada uno de los alumnos y sus certificados.

Además de todo este proceso, se ha tenido que desarrollar una capa de usuario para que el estudiante tenga acceso a sus acreditaciones Blockchain. Para ello se ha utilizado y se han tenido que realizar cambios en el sistema donde en la actualidad se le presentan sus acreditaciones digitales (plataforma LCMS desarrollada por la propia UC3M llamada GEL). Es decir, el usuario dispone en la práctica de dos versiones complementarias de sus acreditaciones, la versión digital y la versión Blockchain pudiendo utilizar cualquiera de las dos de forma independiente. Por tanto el usuario sólo tiene que validarse en la plataforma

[51] https://Blockcerts.org
[52] Implementación de la Universidad del Rosario, red BLUE
[53] Reglamento General de Protección de Datos

de SPOCs de la UC3M (utilizando sus credenciales corporativas) y allí, además del acceso a los cursos en los que está matriculado, tiene acceso a las acreditaciones que ha conseguido.

En las acreditaciones Blockchain se han añadido dos funcionalidades adicionales, por un lado la posibilidad de compartirla en redes sociales (Twitter, Facebook, LinkedIn) y por otro lado la posibilidad de añadir metadatos adicionales como por ejemplo (fecha del curso, horas de esfuerzo/semana, temario, profesorado, competencias adquiridas...). Al utilizar el estándar Blockcerts, todos nuestros certificados pueden ser validados por el validador "universal" del proyecto ubicado en la página web oficial de Blockcerts. Además, también pueden ser cargados, validados y visualizados en la app oficial del proyecto[54] con lo cual le da el valor de la verificación externa a la institución emisora.

Junto al visualizador que se ha personalizado para poder mostrar las acreditaciones de la UC3M, se ha desplegado un validador universal del proyecto *Blockcerts* en nuestra Universidad. Para que cualquier acreditación/certificado que utilice la solución *Blockcerts* pueda ser verificado desde nuestro servicio.

Ilustración 1 Verificador del proyecto en la UC3M

En cuanto a números en el año 2018 se emitieron 590 acreditaciones habilitantes para el acceso al laboratorio de electrónica, esta vez sobre la red Ethereum y en el año 2019 se han emitido 520 acreditaciones del mismo curso. Nuestro objetivo es hacer extensible esta tecnología a más cursos que necesiten este tipo de acreditación y para el curso 2019/2020 la planificación es al menos que sea utilizada en tres cursos adicionales, lo que supondría más de 3.000 acreditaciones.

Por último, se está trabajando actualmente en la adecuación de la infraestructura necesaria para que el servicio pueda ser escalable. Este servicio ya puede ser solicitado por cualquier profesor que despliegue cursos SPOCs a través de la convocatoria de innovación docente. Además, se está trabajando en la creación de una interfaz gráfica para la creación de las plantillas, que en estos momentos se hacen a nivel de *scripts* desde la línea de comando. Esto nos permitirá que personal no técnico tenga la capacidad de emitir este tipo de acreditaciones.

En cuanto a la evolución del proyecto, la línea de actuación es poder desplegar esta tecnología en la nueva red BLUE[55] y el uso de wallet de usuario mediante el uso de la Identidad soberana[56] según lo vaya permitiendo la tecnología. Nuestro objetivo a corto/medio plazo es desplegar este conjunto de servicios y aplicaciones dentro de la red BLUE mediante la utilización de los mecanismos de acceso que proporciona (API).

A continuación, se muestran ejemplos de las acreditaciones que se generan, así como algunas de las funcionalidades de las mismas, como metadatos o la conexión con redes sociales. Además, se puede ver la compatibilidad de nuestros certificados con los del proyecto Blockcerts. Es decir, todos los certificados generados en la UC3M son verificables por el verificador universal del proyecto[57]. Así como por el *wallet* del proyecto (tanto en IOS como Android).

Ilustración 2. Ejemplo acreditación

[54] Blockcerts disponible en IOS y Android
[55] http://tic.crue.org/blue/
[56] https://medium.com/@AlexPreukschat/self-sovereign-identity-a-guide-to-privacy-for-your-digital-identity-5b9e95677778
[57] https://www.Blockcerts.org/

Ilustración 3. Ejemplo redes sociales

Ilustración 4. Ejemplo metadatos

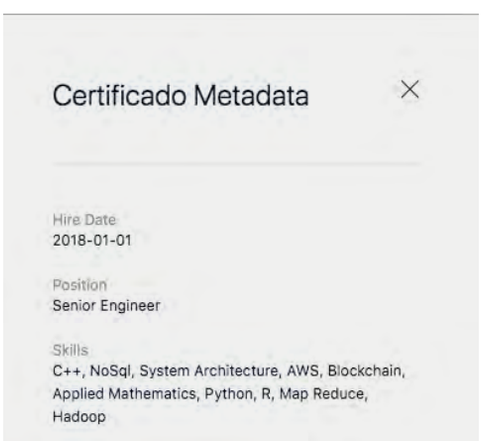


Ilustración 5. Validación verificador Universal proyecto Blockcerts

Carlos Castro-Iragorri

-

ES PROFESOR ASOCIADO DE LA FACULTAD DE ECONOMÍA EN LA UNIVERSIDAD DEL ROSARIO, COLOMBIA. EL AUTOR AGRADECE LA INFORMACIÓN APORTADA POR ANA MARÍA MORENO PROFESORA DE LA UNIVERSIDAD JORGE TADEO LOZANO.

2.4

LOS CASOS DE USO

Experiencia y expectativas de las universidades colombianas con las tecnologías Blockchain

Carlos Castro-Iragorri
UNIVERSIDAD DEL ROSARIO, COLOMBIA

Las tecnologías Blockchain han generado un interés que trasciende las fronteras y los sectores económicos. El reto actual de los profesionales interesados en la tecnología es transformar las expectativas en realidad y garantizar la promesa de valor.

En el ámbito de las instituciones educativas ya existen diagnósticos bastantes completos que indican en qué áreas potencialmente estas tecnologías pueden remplazar el statu quo (Grech, y otros, 2017) (*Blockchain-Based Applications in Education: A Systematic Review,* 2019): administración de certificaciones académicas, acreditaciones, reconocimiento y transferencia de créditos, registro del aprendizaje a lo largo de la vida (*Lifelong Learning*), trazabilidad y generación de valor en las contribuciones científicas, servicios financieros a los estudiantes (pagos y financiación), identidad auto soberana. De acuerdo al diagnóstico realizado algunas de estas iniciativas verán la luz en el corto, mediano o largo plazo. Las universidades, las empresas tecnológicas que proveen servicios en el sector educativo y los emprendedores han prestado atención a la anterior lista de oportunidades.

Actualmente el caso de uso que ha generado mayor interés y desarrollo es el proceso de administración de certificaciones académicas. En las áreas de tecnología y de admisiones y registro de las universidades existe un gran interés por la rápida adopción de la tecnología. La certificación es una convención social que utilizada dentro del ambiente académico representa un reconocimiento o aval ante la sociedad que emite una entidad educativa con respecto al conocimiento y habilidades adquiridas por una persona o un conjunto de personas durante su proceso de aprendizaje. Cualquier certificación digital o no digital consiste en unos componentes y unos procesos. Los componentes mínimos son la afirmación, la evidencia, un emisor y un receptor. Mientras que los procesos son el diseño, la emisión, la socialización y la verificación. El valor agregado de las tecnologías Blockchain desde el punto de vista de componentes y procesos son varios: Primero le concede un mayor control sobre la información y portabilidad al receptor y este sentido complementa la identidad auto-soberana. Segundo, proporciona un medio que garantiza permanencia y trazabilidad sobre las afirmaciones y evidencias. Tercero, proporciona mecanismos alternativos de seguridad, por ejemplo: sistemas de verificación digital colaborativo o procesos de mayor complejidad en el momento de verificación que puedan llevarse a cabo de manera eficiente y automatizada. Cuarto, contar con mecanismos de verificación independientes que faciliten la portabilidad. Por último, concede mecanismos para que el emisor revoque o caduque certificaciones sin incurrir en costos adicionales.

En el dialogo con las áreas de registro y control de las universidades se enfatiza el interés de contar con mecanismos de seguridad y verificación más robustos y eficientes. En general existe la percepción que las tecnologías tradicionales como los certificados en papel o digitales (sin tecnologías Blockchain) cada

vez son más susceptibles a la falsificación. No deja de ser una percepción pues no hay cifras concretas que cuantifiquen la magnitud del riesgo de falsificación de los títulos universitarios, por lo menos en Colombia. Lo que sí existe, tanto en Colombia como en otros países, son casos anecdóticos, registrados por los medios de comunicación donde figuras públicas aseguran contar con unas credenciales académicas que en realidad en la mayoría de los casos corresponden a casos de deserción estudiantil de alto nivel. Si bien para las figuras públicas puede existir un escrutinio mediático que permita una verificación rápida de los antecedentes académicos, para el resto de los ciudadanos no existen mecanismos eficientes de verificación de las afirmaciones con respecto a los logros académicos y profesionales. Es en este sentido que la decisión de adoptar una nueva tecnología debe estar basada en unos beneficios generales que trasciendan las justificaciones anecdóticas y que por el otro lado estén basados en un análisis de costo beneficio. Esto último es un punto que aun adolece en la adopción de las tecnologías Blockchain. Son poco los análisis de costos beneficio de la adopción de la tecnología o su comparación con tecnologías alternativas. En ningún caso de uso este tipo de estudios son evidentes, aun en el contexto de servicios financieros o de cadenas de suministros donde la tecnología parece estar más madura.

Otro diálogo interesante que no solo incluye a las áreas de registro y control académico, sino que también involucra a las áreas de tecnologías, es el que tiene que ver con la capacidad de adopción tecnológica. La introducción de una nueva tecnología no puede desconocer unas prácticas e inversiones que han realizado las instituciones en sistemas de información. Estas prácticas e inversiones son desarrollos propios y/o servicios que adquieren las universidades a proveedores tecnológicos. La adopción de las tecnologías Blockchain deben darse en el ámbito de una interoperabilidad con los sistemas de información de las universidades y unos procesos de transición a unos nuevos modelos de negocios donde esa información pueda ser compartida de una manera segura y que cumpla con la normatividad nacional e internacional con respecto a la custodia y protección de los datos personales (El Reglamento General de Protección de Datos en el contexto Europeo y la Ley 1581 de 2012 en Colombia).

Teniendo en cuenta las anteriores reflexiones los esfuerzos de adopción de las tecnologías Blockchain dentro de las universidades colombianas se ha dado a partir de iniciativas individuales dentro y fuera de las mismas entidades[58]. Hasta el momento no existe un liderazgo ni directrices del sector público sea el Ministerio de Tecnologías de la Información o el Ministerio de Educación.

La Universidad Nacional de Colombia, a través del grupo de investigación InTIColombia y el Vivelab Bogotá, desarrolló un proyecto de emisión de certificaciones académicas para los cursos de educación continuada de la Facultad de Ingeniería. El prototipo utiliza la red no permisionada y pública Ethereum como mecanismo notarial y el InterPlanetary File System (IPFS) como un sistema para almacenar el certificado. Un contrato inteligente genera de manera automática el diploma a partir de los datos de estudiantes y curso, enviando de manera automática a sus correos el pdf del certificado, el *hash* de la imagen del documento y un código QR correspondiente a la información del hash. Además se cuenta con servicio web que funciona como validador del certificado[59].

En la Universidad del Rosario en 2018 se inició una prueba de concepto para la emisión de certificaciones. El propósito de investigación inicial fue la implementación del estándar Blockcerts (desarrollado por MIT y Machine Learning en 2015) en el ámbito de una red Blockchain permisionada. El proyecto Blockcerts se había construido para utilizar las redes públicas y no permisionadas de Bitcoin y Ethereum como mecanismos de notariado en el proceso de emisión de certificados educativos digitales. La prueba de concepto se implementó utilizando Angular, Hyperledger Composer y Fabric. La aplicación proporciona un servicio para que el área administrativa de la universidad genere las plantillas de los certificados y realice posteriormente la emisión individual o en lotes de varios certificados. Adicionalmente, contiene otro servicio que le permite a cualquier usuario verificar y generar una versión en pdf del certificado emitido por la universidad. La aplicación desarrollada es un primer paso a la emisión de diplomas universitarios, pero que considera un caso de uso menos complejo: la emisión de certificaciones por parte del Centro de Atención y Servicio al Estudiante (CASAUR) que administra la emisión de certificados de participación de programa, sanciones y requisitos de idioma para la población universitaria. Desde el área de tecnología de la Universidad se consideró que un piloto en este contexto era más realista que abordar procesos más complejos de emisión de certificados. El prototipo se presentó en el Hyperledger Global Forum en Diciembre de 2018[60] y en primer trimestre del 2019 se puso a consideración del área de tecnología para su implementación. A partir de este

[58] Es importante aclarar que pueden existir proyectos en otras instituciones que el autor desconozca. Por lo tanto se presenta una muestra de aquellos proyectos que han logrado algún nivel de visibilidad en el ámbito universitario local.
[59] https://certificados.bogota.unal.edu.co/

primer desarrollo y atendiendo a la invitación de la RedIRIS y CRUE-TIC, la universidad está participando en la creación del primer nodo internacional de la RedBLUE de universidades españolas para la emisión, registro, verificación y portabilidad de titulaciones universitarias. En paralelo, la Universidad del Rosario viene desarrollando iniciativas con diferentes proveedores tecnológicos para consolidar los procesos de emisión de diplomas digitales que puedan incorporar elementos de tecnología Blockchain. Es el interés de la Universidad apostar de manera simultánea en la investigación de la adopción de nuevas tecnologías pero también en la rápida adopción de estas tecnologías mediante el trabajo colaborativo con proveedores tecnológicos.

La empresa Xertify[61] que cuenta con el apoyo de la Universidad de los Andes ofrece un servicio de emisión y verificación de certificados y mensajes que utiliza el estándar de Blockcerts y la red no permisionada y pública Ethereum como mecanismo notarial. Este proyecto trasciende el caso de uso exclusivamente académico, ofreciendo servicios de administración de credenciales y mensajes certificados o cualquier tipo de documento que pueda verificarse utilizando las tecnologías Blockchain.

La Universidad EAN con el apoyo de la empresa Thomas Signe y a través de la herramienta eTítulo[62] ofrecerá a sus estudiantes la posibilidad de tener una copia autentica y legal del título universitario que aprovecha las ventajas de las tecnologías Blockchain.

En la Corporación Unificada Nacional de Educación Superior (CUN) el grupo de investigación CEBIAC se encuentra desarrollando un prototipo de un sistema de registro de notas utilizando tecnologías Blockchain.

Por otro lado, diferentes asociaciones relacionadas al ámbito académico como la Asociación Colombiana de Universidades (ASCUN), la Red de universidades para fomento de la investigación en tecnologías de la información y la comunicación (UxTIC) y la red Admisiones, Registro y Control Académico (Red ARCA) de las Universidades Colombianas han mostrado un importante interés en las tecnologías Blockchain desarrollando encuentros para explorar los diferentes casos de uso.

Lo anterior presenta un ecosistema atractivo para el desarrollo de soluciones Blockchain en el ámbito educativo y académico en Colombia. Es un ecosistema diverso en diferentes dimensiones. Por un lado, existen desarrollos internos de las universidades así como soluciones aportadas por empresas tecnológicas y emprendedores; por otro, desde el punto de vista de la tecnología hay soluciones Blockchain permisionadas y no permisionadas. El dilema de desarrollar sus propios sistemas, realizarlo en colaboración con los proveedores tecnológicos o adquirir el servicio de titulación digital con tecnología Blockchain es una decisión que tiene desafíos importantes en todo el sistema universitario.

El desafío en la maduración de este ecosistema es lograr un espacio donde se generen bienes públicos y externalidades en la generación del capital humano para la apropiación de estas nuevas tecnologías. La esencia de las tecnologías Blockchain consiste en la descentralización con esquemas de gobernanza colaborativos aun si las diferentes organizaciones, en este caso las universidades, deciden apostarle a desarrollos propios o comprar la tecnología a un proveedor tecnológico. Por lo tanto, hay un espacio importante de diálogo que logre garantizar que el resultado final sea interoperable. Es decir, si el propósito como comunidad académica es obtener unos certificados académicos o compartir cualquier tipo de información académica, es necesario que esa promesa de valor sea completa y que el resultado no sean unas soluciones tecnológicas que permitan la emisión pero se queden cortas en universalizar la verificación y la portabilidad.

Es importante resaltar que la utilización por parte de varios proyectos del estándar Blockcerts, entendido como una estructura de información pero también como unos procesos, es un buen comienzo. Sin embargo lo que queda por recorrer implica: primero, visibilizar los casos exitosos; segundo, escalar el proceso de emisión de certificados de educación continuada a los diplomas académicos; tercero, garantizar la interoperabilidad de estos servicios basados en tecnológicas Blockchain con los sistemas de información de las universidades, y cuarto, empezar un dialogo con las entidades encargadas de la política pública en Educación para definir los criterios que permitan considerar estos mecanismos de administración de las certificaciones en Educación como legalmente válidos y deseables.

Referencias

Blockchain-Based Applications in Education: A Systematic Review. **Alammary, A, y otros**. 2019. 2400, 2019, Applied Sciences, Vol. 9, págs. 1-18.

Grech, A y Camilleri, A. F. 2017. Blockchain in Education. EUR 28778 EN; doi:10.2760/60649. s.l. : Inamorato dos Santos, A. (ed.) EUR 28778 EN, 2017.

[60] Hyperledger supporting Blockcerts compliant digital diplomas across Colombian Universities.
[61] https://xertify.co/
[62] https://portal.etitulo.comw

Coordinación

Andrés J. Prado Domínguez

Director del Área de Tecnología y Comunicaciones de la Universidad de Castilla-La Mancha

Equipo Editorial

Grupo de trabajo de directores TI, del Comité Sectorial de Tecnologías de la Información y la Comunicación de la Conferencia de Rectores de las Universidades Españolas

Lluís Alfons Ariño Martín

Coordinador TIC de la Gerencia y Director del Servicio de Informática de la Universitat Rovira i Virgili

Adelaida Cabrero Bueno

Jefa del Servicio de Informática de la Universidad de Jaén

Joaquín Canca Cuenca

Director Técnico del Servicio de Informática de la Universidad de Málaga

Juan Camarillo Casado

Director Técnico Área de Universidad Digital de la Universidad de Sevilla

Lluís Alfons Ariño Martín

Coordinador TIC de la Gerencia y Director del Servicio de Informática de la Universitat Rovira i Virgili

Santiago Portela García-Miguel

CIO de la Universidad Alfonso X

Andrés J. Prado Domínguez

Director del Área de Tecnología y Comunicaciones de la Universidad de Castilla La Mancha

Autores

Juan Gómez Ortega

Presidente de Crue-TIC
Rector de la Universidad de Jaén

Carlos Alberto Castro Iragorri

Profesor Asociado
Universidad del Rosario

Lluís Alfons Ariño Martín

Coordinador TIC de la Gerencia y Director del Servicio de Informática de la Universitat Rovira i Virgili

José Luis Hernández Fernández

Director TIC
Universidad Carlos III de Madrid

Diego R. López García

Chairman
NFV and PDL ISGS en ETSI

Ricard Martínez Martínez

Director de la Cátedra de Privacidad y Transformación Digital
Universidad de Valencia

Andrés J. Prado Domínguez

Director del Área de Tecnología y Comunicaciones y Profesor Asociado
Universidad de Castilla La Mancha

Jesús Ruiz Martínez

CTO
Alastria

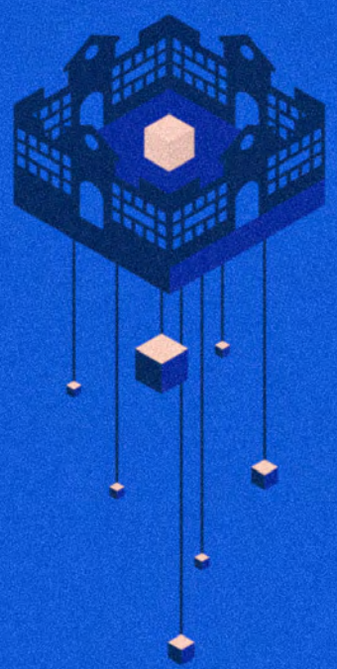
Francisco Cruz Argudo

Especialista en Tecnologías Educativas
Universidad Carlos III de Madrid

Antonio Tenorio Fornés

Investigador Principal
Decentralized Science

Versión digital



crue Universidades Españolas