



Artículo doctrinal

**THE EUROPEAN BLOCKCHAIN SERVICE
INFRASTRUCTURE (EBSI)
Y EL DESARROLLO DE BLOCKCHAIN EN
EL MARCO INSTITUCIONAL EUROPEO
CASOS DE USO**

**MONTAÑA MERCHÁN ARRIBAS
ÁNGEL LUIS MARTÍN BAUTISTA**

MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL
SECRETARÍA GENERAL DE ADMINISTRACIÓN GENERAL - SGAD

20 de agosto de 2020

BLOCKCHAIN INTELLIGENCE

www.blockchainintelligence.es

COTENIDO:

1.	LA IMPORTANCIA DE LA TECNOLOGÍA BLOCKCHAIN.....	2
2.	LA APUESTA EUROPEA EN BLOCKCHAIN.....	4
3.	LA RED DE SERVICIOS BLOCKCHAIN: EBSI.....	5
4.	LA GOBERNANZA ES UN PUNTO CLAVE DEL PROYECTO.....	8
5.	LA PARTICIPACIÓN ESPAÑOLA.....	10
7.1.	IDENTIDAD DIGITAL AUTO-GESTIONADA.....	13
7.2.	CASO DE USO DE DIPLOMAS.....	14
7.3.	CASO DE USO DE NOTORIZACIÓN.....	16
7.4.	CASO DE USO DEL GRUPO TAXUD.....	18
7.5.	NUEVOS CASOS DE USO.....	19
7.5.1.	Número de la Seguridad Social Único Europeo.....	19
7.5.2.	Solicitantes de Asilo.....	19
7.5.3.	Financiación de la PYMES.....	20
7.6.	NUEVO GRUPO DE GOBERNANZA TÉCNICA DE LA RED.....	21
8.	ARQUITECTURA DE LA EBSI.....	22
9.	ESTUDIOS DE ASESORAMIENTO LEGAL EN CURSO.....	24
9.1.	SITUACIÓN DEL ANÁLISIS DE CUMPLIMIENTO DE LA RED EBSI CON EL REGLAMENTO DE PROTECCIÓN DE DATOS.....	24
9.2.	SITUACIÓN DEL ANÁLISIS DE CUMPLIMIENTO DE LA RED EBSI CON EL REGLAMENTO EIDAS.....	24
10.	PRÓXIMOS PASOS DE EBSI.....	26
	REFERENCIAS.....	27

1. LA IMPORTANCIA DE LA TECNOLOGÍA BLOCKCHAIN

Una Blockchain es un libro mayor digital que se distribuye entre varias ubicaciones para garantizar la seguridad y facilidad de acceso a nivel mundial, permitiendo a consumidores y proveedores conectarse directamente, eliminando la necesidad de un tercero”

Blockchain se conoce fundamentalmente por ser la tecnología utilizada en la creación de la moneda virtual Bitcoin, pero no todos los proyectos que utilizan blockchain giran alrededor de bitcoin desde que Ethereum pareció en 2015. Bitcoin se centra en las transacciones financieras mientras que Ethereum tiene una alta aplicación en otros ámbitos, incluido el ámbito de los servicios públicos.

Satoshi Nakamoto, el creador del bitcoin, se inspiró en soluciones propuestas por la cultura Cypherpunks, que se formó a finales de los ochenta en EEUU. Un movimiento anarco capitalista tecnológico cuyo manifiesto incluye frases como;

‘La privacidad es necesaria para una sociedad abierta en la era electrónica’.

Satoshi quería crear Bitcoin como un dinero que funcionara entre pares (P2P o Peer to Peer). Y por ello, Bitcoin y, por consiguiente, la blockchain es mucho **más que una tecnología, es un instrumento de cambio social.**

Diez años antes, 1998, Nick Szabo, jurista y criptógrafo, había diseñado un mecanismo para una moneda digital descentralizada a la que llamó "bit gold". Un trabajo conceptual que no llegó a implementarse pero es considerado como el precursor de bitcoin. En 1997, Szabo también escribió un documento donde detallaba el funcionamiento de lo que en 1995 se había denominado los **Smart Contracts**.

El concepto de smart contract es fundamental en la historia de blockchain pues si bien en 1997 no pudo implementarse, 15 años después con la tecnología blockchain se hace realidad y es partir de entonces cuando esta tecnología se revela viable para una amplia gama de aplicaciones.

Las características de blockchain: descentralización, inmutabilidad a prueba de manipulaciones, trazabilidad, transparencia, seguridad, son la causa del interés que esta tecnología ha despertado en muchos sectores y ámbitos, desde el control de alimentos o trazabilidad de

mercancías, el ámbito financiero y de registros (registro de la propiedad, validación de documentos, notarios digitales, etc); aportando valor en todos los ámbitos que son descentralizados y hay múltiples actores.

Para el sector público blockchain también tiene beneficios como son la capacidad de implementar una identidad autogestionada que cumple con el Reglamento General de Protección de Datos, mayor confianza en los gobiernos y una mejor automatización, transparencia y auditabilidad. En algunos casos aporta beneficios realmente de valor como en el registro de apoderamientos o la contratación, registros sanitarios, sellos de confianza. De hecho, tiene un gran potencial en ámbitos en los que se necesita trazabilidad.

Indudablemente la OCDE (Organización para la Cooperación y el Desarrollo Económico) y la Comisión Europea se han interesado por esta tecnología creando sendos grupos de trabajo específicos. La OCDE ha creado el Blockchain Expert Policy Advisory Board (BEPAB), un equipo global de referencia para formular las políticas sobre blockchain y otras DLTs (Distributed Ledger Technology); mientras que la Comisión Europea creó un consorcio de países para desarrollar una red de servicios blockchain. El Ministerio de Asuntos Económicos y Transformación Digital participa en los dos grupos. También cada vez más diversas administraciones públicas de todo el mundo, están incluyendo esta tecnología en sus planes estratégicos.

2. LA APUESTA EUROPEA EN BLOCKCHAIN

Con el objetivo de que la Unión Europea se convierta en líder mundial en esta tecnología, la Comisión Europea está apostando decididamente por la tecnología blockchain.

Así en octubre de 2017, el Consejo de Europa solicitó a la Comisión Europea adoptar medidas en relación a blockchain con iniciativas que permitan que la Unión Europea explore nuevos mercados y consiga posicionarse como líder en los mismos. Con este mandato, en febrero de 2018 la Comisión puso en marcha el Observatorio y Foro Europeo de Blockchain (EU Blockchain Observatory and Forum <https://www.eublockchainforum.eu/>) con el ánimo de acelerar la innovación y el ecosistema de desarrollo en blockchain dentro de la Unión Europea. Se trata de un foro para compartir conocimiento, identificar obstáculos y encontrar soluciones para el establecimiento de esta tecnología. En la actualidad el número de países firmantes de esa declaración asciende a 30: todos los países de la UE más Noruega y Liechtenstein.

Dos meses más tarde, el 10 de Abril de 2018, durante la celebración del Digital Day en Bruselas, 22 países europeos, incluyendo a España, firmaron **una Declaración de Cooperación para establecer una asociación europea de Blockchain** reconociendo el compromiso de estos países con el potencial de esta tecnología para transformar los servicios digitales tanto en el sector público como en el privado. El principal objetivo de la European Blockchain Partnership (EBP) es **crear una infraestructura europea de servicios basados en blockchain** (European Blockchain Services Infrastructure –EBSI).

Es en la séptima reunión de este grupo donde se da un gran impulso al proyecto, y comienza a acordarse un calendario muy apretado y también coincide con la fecha de incorporación de los autores de este artículo al proyecto.

3. LA RED DE SERVICIOS BLOCKCHAIN: EBSI

¿Qué es lo que se quiere conseguir con el desarrollo de EBSI? **El objetivo de EBSI es mejorar la provisión de servicios transfronterizos para el ciudadano y favorecer la movilidad ciudadana y empresarial, garantizando el cumplimiento de la normativa de la UE.** Como consecuencia se reducirá el impacto ambiental del papel y el transporte y se desarrollarán proyectos innovadores europeos.



Ilustración 1 Objetivos de la EBSI

Veamos algunas de los principios que guían la infraestructura de la red de servicios blockchain europea (EBSI):

- Ha de ser una red de tipo **pública y permitida**, por tanto, cada nodo está identificado y entra a formar parte de la red tras ser aceptada su solicitud de participación. Todos los nodos pueden realizar transacciones y ver el registro de transacciones de la cadena de bloques, pero solo un número limitado de nodos participa en el mecanismo de consenso.
- Ha de ser **escalable** de manera que permita un alto número de transacciones y de nodos.
- **Ha de ser una red abierta** utilizando sistemas open-source.
- Debe ser **sostenible** marcándose altos objetivos de eficiencia energética.
- Ha de ser una red **interoperable** que se base en **estándares y especificaciones técnicas reconocidos**.



Ilustración 2 Características de EBSI

Sobre esta infraestructura blockchain se implementarán los casos de uso propuestos por los países miembros considerando los siguientes criterios:

- A. basarse en una **necesidad claramente identificada** de las autoridades públicas,
- B. **tener una dimensión transfronteriza** con transacciones u operaciones que involucren a varias administraciones de los Estados Miembros,
- C. **que la tecnología blockchain aporte valor añadido a la solución.**

En base a estos criterios y para la primera fase de la EBSI se han seleccionado tres casos de uso, al que se añadió Intercambio de datos confiables y para la segunda fase programada para 2021, recientemente se han aprobado otros tres casos. En total se implementarán los siguientes siete casos de uso en dos años:

1. **Notarización** de documentos
2. **Identidad digital soberana o autogestionada 1**
3. **Diplomas Académicos**
4. **Intercambio de datos confiables²**

¹ European Self-Sovereign Identity Framework – ESSIF

² A estos casos se ha unido el de "Intercambio de datos de confianza", en el marco de la Directiva 2006/112/EC conocida como "One-Stop-Shop", consistente en el pago de IVA en

5. Número único de la Seguridad social
6. Identidad para los refugiados
7. Financiación de las PYMES

El **éxito** de este proyecto depende en gran medida de la capacidad de los estados miembros para integrar sus servicios en EBSI y proporcionar a los ciudadanos las credenciales verificables oportunas. Para ello, la Comisión ha desarrollado un Kit de despliegue de nodos y una API para la integración de los servicios en EBSI.

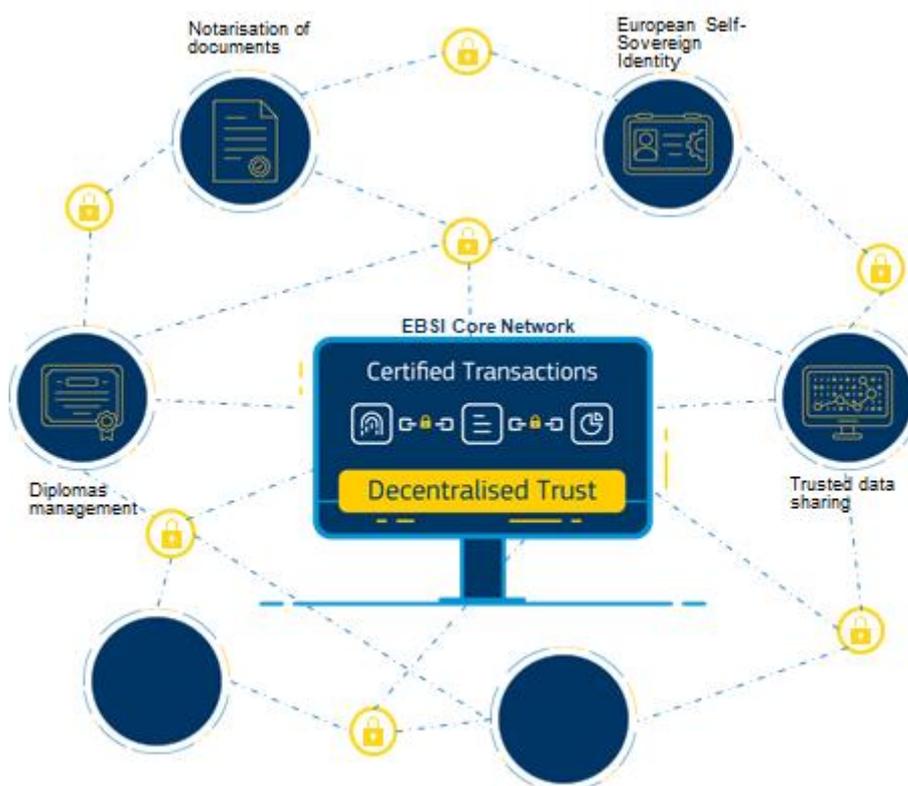


Ilustración 3 Esquema de la EBSI

envíos procedentes de países extracomunitarios con valor inferior o igual a 150 euros y que entrará en vigor el próximo 1 de enero de 2021. Un caso especificado en la DGTAXUD de pago de aduanas.

4. LA GOBERNANZA ES UN PUNTO CLAVE DEL PROYECTO

La coordinación del proyecto está a cargo de la Dirección General de Redes de Comunicación, Contenido y Tecnología (**DG Connect**), responsable de la gestión de la Agenda Digital y de la Dirección General de Informática (**DG DIGIT**) responsable de las infraestructuras y los servicios digitales en la Comisión, y como hemos mencionado se ha unido la **DG TAXUD** responsable de las políticas de la Comisión sobre fiscalidad y unión aduanera.

Para ejecutar el proyecto se han creado **cinco grupos de trabajo**, en los cuales participan los representantes de cada país.

- El grupo "**Policy**" que se orienta a la gobernanza general del proyecto y realiza la selección de nuevos de casos de uso a implementar en la plataforma entre otros aspectos;
- el grupo "**Technical**" que tiene la función de definir los requisitos técnicos de la red de manera que dé cabida a los casos de uso elegidos y sea lo suficientemente flexible como para acoger otros casos de uso en el futuro;
- **los grupos de los casos de uso que** tienen como misión definir el modelo de información y el *Smart contract* correspondiente a cada caso.

El interés de la Comisión Europea en este proyecto se ha puesto de manifiesto en la apretada hoja de ruta que estableció a principios de 2019 y el apoyo que ha dado al I Congreso Mundial de blockchain celebrado en Málaga en noviembre de 2019. La Comisión Europea espera que exista una **estrecha colaboración** entre los países miembros del **EBP** para desarrollar la red EBSI con servicios públicos transfronterizos. Impulsa la colaboración público-privada apoyando la **creación de un consorcio**, International Association of Trusted Blockchain Applications (**INATBA**), formado por organizaciones del sector privado y sector público. La Comisión Europea considera clave la colaboración público-privada para lograr el objetivo de que Europa sea una referencia en esta tecnología y considera que para ello es necesario que se produzca un diálogo fluido entre el sector privado y las instituciones públicas que permita definir el futuro marco regulatorio de las tecnologías de registro distribuido de forma que surja una **convergencia** que evite la aparición de enfoques fragmentados.

El **Observatorio y el Foro Europeo de blockchain** es el espacio en el que los países pueden **compartir los conocimientos** en esta materia y ofrecer soluciones a posibles problemas que puedan aparecer. Por otro lado a través de los programas Horizonte 2020 y *Connecting Europe Facility* (CEF), la Comisión facilita **la inversión en investigación e innovación y la promoción de un entorno legal y regulatorio**, con estándares interoperables.

EU Strategy
Blockchain holistic approach

European Commission

ESTABLISHING GLOBAL LEADERSHIP IN BLOCKCHAIN AND DISTRIBUTED LEDGER TECHNOLOGIES

- 

JOINED-UP POLITICAL VISION (EU-MS)
JOINT DECLARATION ON THE ESTABLISHMENT OF THE **EUROPEAN BLOCKCHAIN PARTNERSHIP** [EBP] AND THE DEVELOPMENT OF THE **EUROPEAN BLOCKCHAIN SERVICES INFRASTRUCTURE** [EBSI] FOR CROSS-BORDER DIGITAL SERVICES OF PUBLIC INTEREST
- 

PUBLIC-PRIVATE PARTNERSHIP
SUPPORTING THE CREATION OF THE **INTERNATIONAL ASSOCIATION OF TRUSTED BLOCKCHAIN APPLICATIONS** [INATBA]: A MULTISTAKEHOLDER ORGANISATION TO PROMOTE TRUST AND INTEROPERABILITY AT GLOBAL LEVEL
- 

CONNECTING GLOBAL and EUROPEAN EXPERTISE
THE **EU BLOCKCHAIN OBSERVATORY AND FORUM** BRINGS TOGETHER THE LEADING GLOBAL EXPERTS TO IDENTIFY OBSTACLES, INCENTIVES AND PRACTICAL SOLUTIONS TO PROMOTE BLOCKCHAIN UPTAKE.
- 

INVESTING IN EU RESEARCH, INNOVATION AND START-UPS
THROUGH THE **CONNECTING EUROPE FACILITY** AND H2020 PROGRAMMES, THE EU IS CO-INVESTING IN THE MOST ADVANCED DIGITAL INFRASTRUCTURE AND THE MOST INNOVATIVE EU START-UPS
NEW EU INVESTMENT SCHEME FOR AI AND BLOCKCHAIN + SUPPORT PROGRAMME
- 

PROMOTING AN ENABLING DSM LEGAL FRAMEWORK, INTEROPERABLE STANDARDS and SKILLS DEVELOPMENT

Ilustración 4 Puntos de éxito de la EBSI

5. LA PARTICIPACIÓN ESPAÑOLA

España firma la Declaración de Cooperación para establecer una asociación europea de Blockchain el 10 de abril de 2018 y desde entonces ha asistido a todas las reuniones del EBP hasta el día de hoy.

España participa en los grupos de trabajo: "Policy", "Technical", "ESSIF" y "Diploma". Los organismos de la Administración que participan en el proyecto son: la Secretaría de Estado de Telecomunicaciones e Infraestructura Digital (anteriormente SEAD) con representantes en el grupo Policy en materia de estandarización; la Fábrica Nacional de Moneda y Timbre (FNMT) que nos representa en el grupo técnico y en el de identidad auto-gestionada; la Secretaría General de Administración Digital (SGAD) con representantes en el Policy, en el técnico y un observador en el de identidad auto-gestionada; el Ministerio de Universidades a través de la Secretaría General de Universidades y el Consejo Rector de las Universidades Españolas (CRUE) que participan en el grupo de Diplomas y finalmente un experto en blockchain e identidad soberana del consorcio Alastria que participa en el grupo de identidad auto-gestionada.

Hay que destacar que las experiencias previas en blockchain de las Universidades españolas en el intercambio de acreditaciones académicas y todo el trabajo realizado por el consorcio Alastria en la identidad digital auto-gestionada, han permitido a España ser uno de los países tractores del proyecto y situar un "convinor" (redactor de las especificaciones) en tres de los grupos de trabajo: el Técnico, Diplomas y el de Identidad.

Con el propósito de llevar a las reuniones europeas una única voz y una estrategia común, la SGAD creó un grupo de coordinación, denominado **GT-EBSI**, compuesto únicamente por los representantes involucrados en los grupos de trabajo anteriormente citados. Un segundo grupo de difusión, se estableció al amparo Comité de Dirección de las Tecnologías de Información y Comunicaciones, al objeto de tener informados a todos los Departamentos Ministeriales del avance del proyecto.

6. EL AVANCE DEL PROYECTO EBSI

A pesar del apretado calendario que propuso la comisión europea a principios de 2019, los plazos se están cumpliendo con pequeñas variaciones. El principal hito ha sido la puesta en marcha de una versión de pruebas de la red EBSI, sobre la **que están funcionando los tres casos de uso** seleccionados. Además se está trabajando en la incorporación de uno más denominado “Intercambio de datos de confianza”, en el marco de la Directiva 2006/112/EC conocida como “One-Stop-Shop”, consistente en el pago de IVA en envíos procedentes de países extracomunitarios con valor inferior o igual a 150 euros y que entrará en vigor el próximo 1 de enero de 2021. Este proyecto, liderado por la DG-TAXUD, se va a desplegar también sobre la red EBSI aunque se ha utilizado diferente tecnología blockchain que en el resto de casos de uso.

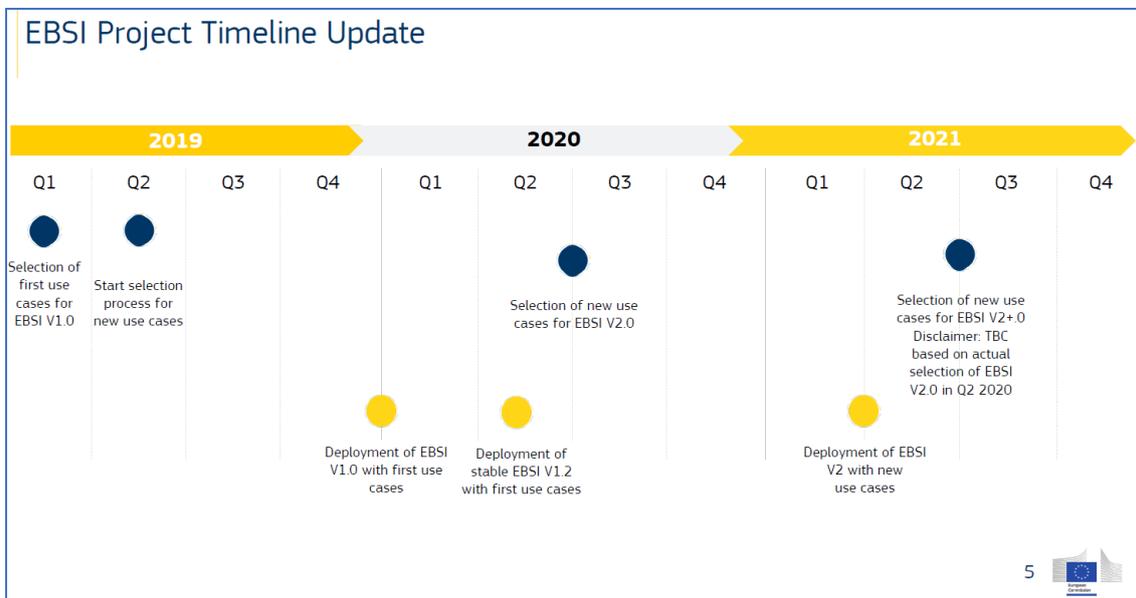


Ilustración 5 Principales hitos del proyecto.

A finales de febrero de 2020, se publicó el “kit de despliegue” del nodo EBSI que los países voluntarios han utilizado para configurar uno o varios nodos de EBSI y poner en marcha la red. A fecha de junio de 2020, 19 estados miembros están en proceso de albergar al menos 1 nodo. En total hay 36 desplegados o en proceso de conexión, 19 de los cuales están funcionando correctamente, y el resto en el proceso. España va a instalar **tres nodos pilotos EBSI**: un nodo en la SGAD, otro en la FNMT y el tercero en Red Iris. Este último con el objetivo de que la iniciativa BLUE de la CRUE y otras iniciativas de las Universidades pueda interoperar con EBSI.

La Comisión ha desplegado seis nodos en Bruselas y durante la reunión del grupo “Policy”, el 12 de febrero, realizó una demostración del funcionamiento del “Viaje de Eva”.

“El viaje de Eva” es la historia de usuario definida por la Comisión Europea para probar los casos de uso. El video de “El viaje de Eva” está disponible en <https://youtu.be/m2uj7fgb2Jl>. Igualmente, está a disposición de la ciudadanía una página dónde es posible comprobar el funcionamiento permitiendo realizar todos los pasos de ese itinerario.

<https://ec.europa.eu/digital-single-market/en/blockchain-technologies>

De acuerdo a la estrategia de compartir información con el sector privado la Comisión Europea ha publicado el proyecto EBSI como un componente de reutilización de la Comisión Europea, “*building block*”. Es decir, ha publicado los componentes centrales de la EBSI, los casos de uso, los proyectos demostradores, el entorno de producción y una API para que el mercado pueda estudiar esta información y conectar sus redes blockchain siendo lo que se denomina “EBSI compliant”. La documentación sobre el proyecto se puede consultar en:

- <https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/Get+Start+ed+EBSI>
- <https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/EBSI>

El trabajo continuará durante 2020 para cerrar los puntos pendientes, tales como la revocación de información en blockchain y mejoras en torno al “Wallet EBSI”. Según el cronograma previsto en 2021 la red EBSI pasará a producción con información real proveniente de múltiples fuentes de datos de las administraciones públicas (universidades, ministerios, organismos públicos, etc) de los EEMM.

España ha presentado una propuesta ambiciosa, en el marco del programa CEF que le permitirá completar tres subproyectos:

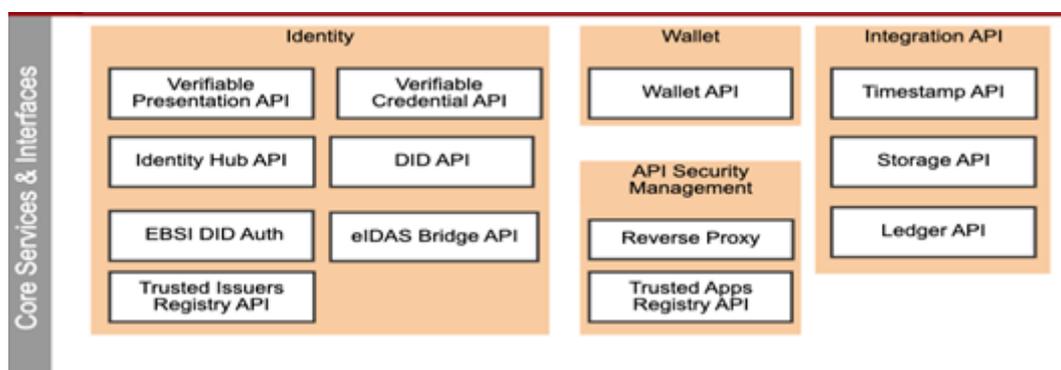
1. Gestión del nodo-SGAD y conexión con el Registro Nacional de Títulos Universitarios. Esto supone que el Ministerio de Universidades puede otorgar credenciales verificables con datos reales a los ciudadanos que lo soliciten para hacerla valer ante cualquier administración o empresa europea.
2. Gestión del nodo-FNMT y piloto de identidad auto-gestionada.
3. Gestión del nodo-RedIris e interoperabilidad con la red BLUE. Esto supone que la red blockchain de Universidades Españolas (BLUE) será EBSI compliant.

7. LOS CASOS DE USO

7.1. IDENTIDAD DIGITAL AUTO-GESTIONADA

Se trata de implementar una identidad autogestionada (European Self-Sovereign Identity ESSIF), que permita a los ciudadanos gestionar su propia identidad sin depender de autoridades centralizadas con vocación de ser transfronteriza.

Casi desde el inicio del proyecto, se hizo patente que este caso de uso es transversal y necesario para la implementación de los otros casos de uso seleccionados como servicios de administraciones públicas a sus ciudadanos. Por tanto, ESSIF se ha planteado como un “building block, ya que en todos los casos es necesario conocer quién es el sujeto de cualquier credencial sin ningún género de dudas, y sería más complejo abordar una identidad para cada caso. De manera que cualquier otra credencial verificable será un atributo de la identidad de un sujeto. Los elementos de identidad, tal y como aparecen en el diagrama, forman parte del “core” de la red EBSI.



La identidad es un punto clave para el intercambio de diplomas y por ello estos dos casos de uso ahora se trabajan juntos.

El sistema de identidad digital autogestionada basado en blockchain podría formar parte del ecosistema de medios de identificación con las administraciones públicas siendo compatible con los actuales sistemas de identificación. Así lo expuso la Comisión en la última reunión trimestral.

Algunos de los principales elementos que se han definido en este caso de uso son:

- Acceso al "Wallet" EBSI.
- Creación de un identificador descentralizado (DID).
- Solicitud de una credencial de identidad.
- Envío de una credencial de identidad.
- Almacenamiento de credenciales de identidad.



La historia de usuario: **Eva, estudiante Belga, obtiene la credencial de identidad**

Eva instala y configura su *wallet* EBSI (monedero o llavero). Eva puede seleccionar un *wallet* de entre varios que estén disponibles. **Además** obtiene un DID-EBSI (*Decentralized Identifier*). Un DID es un identificador con dos claves asociadas (privada y pública), que no contiene ningún dato personal.

Eva solicita al gobierno federal de Bélgica la emisión de una credencial de identidad verificable que se asocia a su DID y se guarda en su *wallet*.

7.2. CASO DE USO DE DIPLOMAS

El caso de uso de **Diplomas** se define como la expedición de un grado universitario o cualquier titulación oficial reconocida, en forma de credencial verificable expedida y firmada por la institución autorizada en cada país. El ciudadano podrá presentar esta credencial en cualquier Universidad Europea o cualquier empresa que se lo solicite. La implementación en blockchain de las credenciales académicas es una de los casos de uso más claros y con más soluciones implementadas desde que el MIT lanzara su plataforma Blockcerts, para registrar diplomas universitarios y publicara en abierto el código software para

que cualquier persona pudiera unirse a la comunidad de desarrolladores.

Con este caso de uso se solucionan varios problemas asociados con los diplomas académicos:

- Disminuir considerablemente el fraude existente en materia de falsificación de títulos académicos ya que blockchain proporciona una naturaleza inalterable.
- Permitir a las personas mantener el control total de su propio historial académico y hacer valer su título académico en otro país sin la burocracia asociada a validar el título por una autoridad intermedia.
- Facilitar que se pueda utilizar también por el sector privado o incluso desde países fuera de la órbita de la Unión Europea.

En este caso, como extensión de la identidad autogestionada, se han definido, esencialmente, las credenciales académicas con el conjunto de los metadatos asociados a la credencial que definen un título académico.

En la fase 1 y dependiendo de los requisitos de cumplimiento de GDPR, el contenido podría almacenarse fuera de la cadena y solo se almacenaría un puntero en la cadena de bloques.

Historia de usuario: Eva se matricula en una Universidad española para hacer un máster.

Eva descubre un programa interesante en ingeniería de seguridad informática e Inteligencia artificial en una Universidad española y decide matricularse como estudiante. Para matricularse a través de la página web de la Universidad, Eva debe cumplir con dos requisitos: presentar su identidad y su grado. Eva solicita al gobierno regional de Flandes la emisión de una *certificación verificable* correspondiente a su título de grado que es firmada por dicho gobierno y lo guarda en su wallet-EBSI.

Eva presenta a través de su *wallet-EBSI* las dos credenciales que le son requeridas y firmadas con la clave de EVA. Por su parte, tras formalizar la matrícula, la Universidad española podría dar a Eva una *credencial con su Número de Registro Universitario (NRU)*, que podrá hacer valer en las librerías o eventos culturales.

En este caso España está en una posición privilegiada pues, a diferencia de muchos de sus vecinos, dispone de un registro centralizado de títulos oficiales, el Registro Nacional de Titulados Universitarios Oficiales (RNTUO) creado por el artículo 4 del Real Decreto 1002/2010, de 5 de agosto, sobre expedición de títulos universitarios oficiales. Lo cual simplifica el trabajo de forma significativa conectando este registro RNTUO a la EBSI para disponer de todos los títulos oficiales en forma de credencial verificable. Cuando un ciudadano lo solicite se le podrá expedir su título académico en el formato que se ha definido en diplomas EBSI, además de los formatos que ya emite. Sin embargo, todavía existe el escollo de modificar el Real Decreto 1002/2010, de 5 de agosto, sobre expedición de títulos universitarios oficiales en cuanto a admitir un formato de expedición digital más allá del papel que es el que se establecen en la norma.

El resto de titulaciones académicas de las Universidades españolas podrán ser expedidas igualmente en blockchain EBSI si se adhieren a la red BLUE, dado que en el caso de uso de Diplomas también se trabaja para poder incorporar al Wallet del ciudadano títulos y certificaciones académicas más allá de los oficiales.

7.3. CASO DE USO DE NOTORIZACIÓN

Este caso de uso fue propuesto inicialmente por el Tribunal de Cuentas Europeo para proporcionar a los beneficiarios de fondos y subvenciones europeas un sistema basado en blockchain que permitiera registrar todos los documentos que justifican el gasto de una subvención, típicamente facturas y comprobantes de pago, contratos, etc. De modo que se facilitara la realización de auditorías de manera ágil, transparente, digital y transfronteriza, que además estuviera vinculada al gasto presupuestario de la UE.

Notarización es el caso más sencillo de los implementados pues se trata de un registro en la blockchain EBSI que almacena huellas (hashes) de documentos relevantes y de sus metadatos asociados. Estos hashes son la prueba de autenticidad de documentos que posteriormente se pueden utilizar en una auditoría.

En el caso de notarización en la blockchain sólo se almacenan los hashes de los documentos y pueden ser verificados directamente en la blockchain. No es necesario mantener un sitio centralizado para cotejar el documento, ni acceder al organismo correspondiente.

Se pretende que este caso de uso se extienda a todo tipo de documentos, en particular a aquellos que constituyen títulos habilitantes emitidos por administraciones públicas o títulos-valores. Este tipo de documentos están vinculados a un derecho privado patrimonial y hasta ahora sólo existen en soporte papel, porque quien tiene el documento físico también tiene el valor que soporta el documento, cosa que no se puede implementar en digital porque un documento electrónico, aunque esté firmado electrónicamente, tiene infinitas instancias de sí mismo y no se puede traspasar porque el emisor no puede deshacerse del documento electrónico. Por ese motivo en estos casos existen registros centrales que es donde se realizan las anotaciones respecto a quien es el que poseedor del documento en cuestión.

En el caso de la administración española, este caso podría agilizar las numerosas apostillas que emite el Ministerio de Justicia.

Dado que blockchain permite traspasar valor entre entidades, puede resolver este problema gracias a proyectos como el que se está desarrollando en este caso de uso de "Notarización" en el que la red EBSI contendría la información sobre quién es el actual poseedor de un documento concreto.

Historia de usuario: Eva finaliza su máster y solicita una subvención para montar una startup.

Cuando Eva completa sus estudios, recibe de la universidad española la *credencial verificable* que representa su Diploma de máster (credencial firmada digitalmente por la Universidad) que Eva almacenará en su *wallet-EBSI* con las otras *credenciales*.

Eva solicita una subvención FEDER de la UE para crear una Startup en Italia. Las autoridades italianas le conceden la subvención. El acuerdo de subvención se realiza a través del Componente de Notarización.

Para justificar cómo se gasta la subvención ante la Autoridad de Gestión de forma electrónica, Eva utiliza el componente de Notarización con el que la autoridad de Gestión podrá validar las facturas y demás documentación.

Posteriormente y en el contexto de una auditoría, los auditores de la UE pueden verificar la integridad y la marca de tiempo de los documentos almacenados en la blockchain.

7.4. CASO DE USO DEL GRUPO TAXUD

El objetivo de intercambio de datos confiables (trusted data shared, TDS) consiste en desarrollar una infraestructura de plataforma blockchain, que técnicamente permita a las entidades de los Estados miembros compartir datos de manera pública o privada y verificar la validez, propiedad y/o autenticidad de estos datos.

Las entidades de los Estados miembros podrán compartir datos (por ejemplo, los números de identificación del IVA de la IOSS (Import One Stop Shop) e importación de ventanilla única) en una plataforma segura y confiable, compatible con GDPR, entre las autoridades aduaneras y fiscales de la UE y sin usar un intermediario y sin tener un solo punto de fallo.

Historia de usuario: **Entidad pública comparte un nuevo contenido y otra lo consulta.**

Una entidad identificada publica contenido nuevo para un servicio de intercambio de datos de confianza específico con la estructura de datos definida por el administrador del grupo. Tras la recepción de la solicitud enviada, TDS verifica su formato y valida cada entrada en la solicitud de publicación recibida, le añade una marca de tiempo y almacena el contenido recién publicado y luego envía una respuesta de reconocimiento de validación a la entidad de publicación. A continuación, el contenido publicado se sincroniza en todos los nodos del TDS. Dependiendo de los requisitos de cumplimiento de GDPR, el contenido podría almacenarse fuera de la cadena y solo se almacenaría un puntero en la cadena de bloques.

Otra entidad identificada puede consultar contenido existente para un servicio de intercambio de datos de confianza específico. Al recibir la solicitud de consulta enviada, TDS verifica su formato y valida cada atributo específico solicitado para una entrada identificada y existente en particular. Para cada entrada de contenido especificada en la solicitud de consulta, TDS creará la respuesta correspondiente, incluyendo los atributos solicitados.

7.5. NUEVOS CASOS DE USO

7.5.1. Número de la Seguridad Social Único Europeo

Este caso fue propuesto simultáneamente por Italia y España. Finalmente y a petición de la Comisión los institutos de seguridad social español e italiano llegaron al acuerdo de que España apoyaría la propuesta italiana por ser esta última más avanzada, madura y coincidir esencialmente con la propuesta española.

El caso de uso ESSIN (Número de identificación de la seguridad social europea) propuesto permite a cada Estado miembro de la UE crear un Pasaporte de bienestar digital de ciudadanos de la UE móviles y prevenir fraudes o errores al garantizar una comunicación e intercambio de datos más fáciles entre los países e instituciones europeos.

Este caso de uso trata de resolver uno de los problemas transfronterizos en la Unión Europea consistente en regularizar y consolidar con facilidad los derechos adquiridos por aquellos ciudadanos que han estado cotizando en varios países durante su vida laboral (por ejemplo, la pensión, beneficios de desempleo, etc.), comprobación que en blockchain sería accesible con facilidad y bajo el control del ciudadano.

7.5.2. Solicitantes de Asilo

El derecho de asilo ha sido propuesto por Alemania y es quizá el paradigma de caso de uso de identidad autogestionada por excelencia, consiste precisamente en darle un DID EBSI a un refugiado y asociarle una nueva identidad, ya que no dispone de ninguna o al menos no es posible preguntarle a su país de origen si los datos que aporta son ciertos o no. Al menos esta nueva identidad que se le proporciona ya no se le podrá negar o eliminar del registro distribuido y podrá utilizarla a través de las fronteras.

El derecho de asilo de las personas perseguidas políticamente está consagrado en Grundgesetz, la constitución de la República Federal de Alemania. Al llegar a Alemania, los solicitantes de asilo deben presentarse inmediatamente a la policía federal o estatal para solicitar asilo que les proporciona un documento de prueba de entrada que les otorga un derecho de estancia temporal. Los solicitantes de asilo también pueden registrar su solicitud en la Oficina Federal de Migración y Refugiado que determinará si otro estado miembro de la UE ha registrado previamente a este mismo solicitante. Si este fuera el caso, el refugiado debe, de acuerdo con el Reglamento de Dublín, regresar al

estado miembro donde se registró por primera vez. Sin embargo, el proceso de revisión puede tardar varios días.

Este caso de uso permitirá una coordinación más eficaz, entre Estados miembros, del proceso de la transferencia de solicitantes de asilo. Actualmente, este proceso de regularización de las transferencias de solicitantes de asilo entre los Estados miembros todavía se basa en correos electrónicos y listas de Excel. La tecnología Blockchain es un medio mucho más eficaz para coordinar estos procesos de transferencia. Específicamente, una aplicación EBSI respaldaría el cumplimiento de GDPR, reduciría los gastos administrativos y mejoraría la armonización de las fechas de transferencia con respecto a los límites de capacidad en los cruces fronterizos o aeropuertos individuales.

Una solución EBSI permitiría una cooperación eficaz entre los estados miembros. Agilizará el intercambio de datos, minimizará la duración, los gastos administrativos y el coste de los procesos de transferencia y contribuiría al cumplimiento de los plazos. Todo ello sin olvidar que contribuiría a apoyar uno de los derechos fundamentales de las personas: disponer de una identidad.

7.5.3. Financiación de la PYMES

El objetivo de este caso es la creación de una plataforma de valores para toda la UE con el objetivo de financiar la transformación digital y la modernización de las PYMES. La plataforma blockchain serviría como una herramienta para emitir, y en etapas posteriores para comprar, bonos en los estados miembros. La clásica financiación bancaria es de una complejidad innecesaria para este tipo de financiación. La emisión y negociación de valores/bonos permitiría a los proveedores privados construir servicios sobre la infraestructura blockchain proporcionada y crear un mercado transfronterizo completamente nuevo.

Este caso de uso presenta una gran oportunidad para implantarlo en el sandbox que recientemente ha creado Consejo de Ministros en el Anteproyecto de Ley para la transformación digital del sistema financiero.

Sin duda este caso, tendrá mucho interés en el ámbito financiero dónde varias entidades financieras se están posicionando adquiriendo capacidades para introducir en el mercado financiero sus soluciones de medios de pago sobre blockchain.

7.6. NUEVO GRUPO DE GOBERNANZA TÉCNICA DE LA RED

Recientemente se ha creado un subgrupo de trabajo para definir la gobernanza técnica, y cuyo objetivo fundamental es redactar el conjunto de protocolos de actuación, procedimientos y guías de trabajo ante diversas situaciones exclusivamente técnicas como puedan ser dar de alta un nuevo nodo, acciones a tomar en caso de caída de un nodo, etc. En definitiva todas aquellas acciones de gobernanza que no caen en el ámbito de la gobernanza política. Por ejemplo, en este grupo no se decide cómo dar permiso a un solicitante para desplegar un nodo, sino una vez concedido ese permiso, cómo ha de desplegarlo.

8. ARQUITECTURA DE LA EBSI

El diagrama de la **arquitectura de la red** se muestra en la siguiente ilustración con las cinco capas de servicio que la definen.

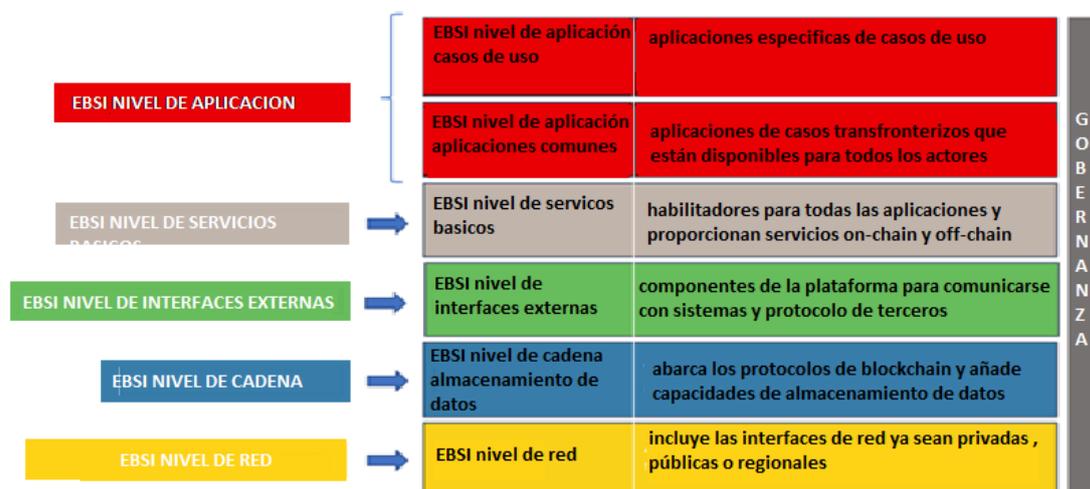


Ilustración 6 Arquitectura de EBSI

Hay cinco capas en la arquitectura y cada capa da servicio a las capas superiores: En la capa más baja, el nivel de red en amarillo, incluye la interface de red sean públicos o privados; la capa en azul abarca los protocolos de blockchain y el **almacenamiento**; la capa en verde se corresponde con los componentes para comunicarse con los sistema de terceras partes (contiene por ejemplo las API de las credenciales verificables, el DID, elDAS Bridge para sellar credenciales con un alto nivel de confianza o Identity Hub para almacenar credenciales, entre otros componentes); el wallet; la API de gestión de seguridad y las API de integración (que permiten escribir en el ledger de Hyperledger Besu o Hyperledger Fabric, de almacenamiento o de timestamping para fechar documentos); el siguiente nivel es de los servicios centrales y es el que se ofrece a las aplicaciones; y por último se encuentra la capa correspondiente a los **casos de uso**, que es la capa de aplicaciones de negocio que consumen los servicios de la EBSI.

Desde un punto de vista técnico, un nodo debe cumplir con los requisitos establecidos en las especificaciones técnicas y garantizar un Acuerdo de Nivel de Servicio predefinido. Además, el equipo técnico de la entidad debe formar parte de la red del equipo de soporte tecnológico de EBSI.

El modelo de consenso de EBSI debe ser tolerante a fallos y continuar funcionando incluso si hasta el 33% (un tercio) de sus nodos están desconectados o comprometidos. En el caso de EBSI es un algoritmo de consenso del tipo tolerante a fallos Bizantino (PBTF) especialmente apropiado para su aplicación en blockchains permissionados. Es un algoritmo tipo Trebizond con sucesión rotatoria de líder. De acuerdo con el principio de separación de responsabilidades (separación de las fases de acuerdo y ejecución), se ha adoptado una arquitectura estructurada en dos capas, delegando la gestión de la comunicación a la capa inferior, denominada controlador de red.

9. ESTUDIOS DE ASESORAMIENTO LEGAL EN CURSO

La Comisión Europea encargó la realización de estudios sobre la compatibilidad de la red EBSI con el reglamentos GDPR y el reglamento eIDAS, en el marco del programa CEF, a un conjunto de expertos en estas áreas. El pasado febrero de 2020 en Bruselas se anticipó la conclusión de los mismos que se resume a continuación.

9.1. SITUACIÓN DEL ANÁLISIS DE CUMPLIMIENTO DE LA RED EBSI CON EL REGLAMENTO DE PROTECCIÓN DE DATOS

No se puede tratar la tecnología blockchain, como una unidad en sí misma a la hora de hacer este estudio, ya que el impacto en la privacidad depende de la implementación de cada caso de uso y cada uno de ellos tiene sus propias peculiaridades y necesidades legales en función del análisis de riesgos. Por ejemplo, el caso de uso “Intercambio de datos de confianza” tiene una legislación propia que hay que tener en cuenta.



En el estudio se están examinando dos aspectos principales, por una parte los diferentes actores que intervienen en la red EBSI y sus responsabilidades en términos de protección de datos (actores como los nodos nacionales, los nodos de la Comisión Europea y los usuarios de la red EBSI); por otro lado se está examinando el ámbito de aplicación del GDPR. En este último apartado se señaló, por ejemplo, que sobre los hashes (huellas) no puede decirse a priori que sean o no un dato personal, sino que depende de nuevo de la implementación en un contexto concreto.

9.2. SITUACIÓN DEL ANÁLISIS DE CUMPLIMIENTO DE LA RED EBSI CON EL REGLAMENTO EIDAS

Desde la perspectiva de la Unión Europea, del Mercado Único Digital, la confianza en las transacciones en internet es una de las principales necesidades. El Reglamento eIDAS constituye el marco principal de confianza en la Unión Europea y el Espacio Económico Europeo para personas físicas y jurídicas en Internet. Los servicios de identificación electrónica y de confianza permiten el establecimiento de relaciones

electrónicas transfronterizas en el ámbito de la administración electrónica.



Por otra parte, uno de los casos de uso más interesantes de la DLT se refiere a la llamada identidad soberana (SSI), que da a cada persona el control sobre sus datos personales, sin la intervención de terceros. La SSI se propone como el paso siguiente en la evolución de la gestión de identidades, porque reduce dos de los principales riesgos asociados con los sistemas de delegación de autenticación: la gestión de los datos de identidad dependiente del proveedor de identidad y, lo que es más

importante, el seguimiento del comportamiento del usuario por parte del proveedor de identidad, algo que puede llevar a la creación de perfiles de usuario.

Diseñar soluciones de identidad SSI alineadas con el Reglamento eIDAS es una necesidad clave en el marco del Mercado Único.

En el estudio se describen los diferentes escenarios de ISS alineados con la regulación eIDAS:

1. Escenarios a muy corto plazo. Consiste en utilizar los aspectos que encajan con el reglamento actual sin necesidad de cambiar la regulación. Por ejemplo utilizar los certificados cualificados para emitir credenciales verificables (VC); utilizar los certificados cualificados para firmar / sellar VC con eIDAS Bridge; utilizar los nodos eID actuales para emitir afirmaciones SAML basadas en un VC/VP (Presentación verificable)
2. Escenarios a corto plazo. Consiste en adoptar nuevas especificaciones técnicas de eID basadas en ESSIF para identificación. Como emitir certificados cualificados basados en un método de identificador descentralizado (DID) + especificación de VC.

Escenarios a medio largo plazo. Consiste en adoptar nuevas regulaciones para permitir el uso de DID sobre DLT como un servicio de confianza.

10. PRÓXIMOS PASOS DE EBSI

Se presenta en este punto un resumen de los próximos pasos marcados por la Comisión Europea en el entorno del EBSI.

- En septiembre la Comisión Europea va a presentar una “Estrategia Europea de Blockchain” en la que el EBP jugará un papel fundamental.
- También en septiembre comenzará a trabajarse en los tres nuevos casos de uso que han sido elegidos en los grupos de trabajo formados por los expertos enviados por los distintos países en cada una de esas tres temáticas.
- Durante 2021 se espera que los EEMM aporten datos reales provenientes de sus sistemas legacy en relación a los casos de uso en que se está trabajando.
- Se está analizando el componente eIDAS BRIDGE en cuanto a la posibilidad de que aumente el valor legal de las credenciales verificables y el reconocimiento de las mismas de forma transfronteriza.
- Al mismo tiempo se estudiará que las credenciales verificables puedan utilizarse como certificados cualificados o que su utilización sirva también para transmitir otros atributos de identidad confiables, lo cual requeriría la gestión de emisores de confianza y una extensión del capítulo II del reglamento eIDAS.

La Comisión espera que la liberación de las especificaciones y desarrollo de EBSI influyan en el modo de desarrollar redes blockchain en los EEMM, de forma que éstas sean “EBSI compliant” e interoperables.

Algunos puntos adicionales que se están analizando son:

- La naturaleza legal de los DID activos frente a un tipo especial de seudónimo; el régimen legal de claves y de los *wallets*, etc.
- Los deberes y responsabilidades de los emisores, titulares y verificadores de las credenciales verificables y los aspectos legales del ciclo de vida de las mismas (emisión, suspensión y causas de revocación, etc.).

REFERENCIAS

C.E. WIKI DEL PROYECTO EBSI (2020): [HTTPS://EC.EUROPA.EU/CEFDIGITAL/WIKI/X/71D6DG](https://ec.europa.eu/cefdigital/wiki/x/71d6Dg)

C.E. MEET: EUROPEAN BLOCKCHAIN SERVICES INFRASTRUCTURE (PPT)

C.E. (2018, 10 ABRIL). EBP. [HTTPS://EC.EUROPA.EU/DIGITAL-SINGLE-MARKET/EN/NEWS/EUROPEAN-COUNTRIES-JOIN-BLOCKCHAIN-PARTNERSHIP](https://ec.europa.eu/digital-single-market/en/news/european-countries-join-blockchain-partnership)

C.E. (2020, 20 MARZO). EBSI. [HTTPS://EC.EUROPA.EU/CEFDIGITAL/WIKI/DISPLAY/CEFDIGITAL/EBSI](https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/EBSI)
CITA EN EL TEXTO

MONTAÑA MERCHÁN (2020, FEBRERO 22). VIAJE DE EVA.
[HTTPS://DIGITALREVOLUTION.INFO/2020/02/22/EL-VIAJE-EUROPEO-DE-EVA/](https://digitalrevolution.info/2020/02/22/el-viaje-europeo-de-eva/)