Centro Universitario de la Defensa en la Escuela Naval Militar

TRABAJO FIN DE MÁSTER

La cadena de custodia mediante tecnología Blockchain

Máster Universitario en Dirección TIC para la Defensa

ALUMNO: Diego Luis Santiago Gutiérrez

DIRECTORES: Luis Modesto Álvarez Sabucedo

CURSO ACADÉMICO: 2022-2023

Universidade Vigo

Centro Universitario de la Defensa
en la Escuela Naval Militar

TRABAJO FIN DE MÁSTER

La cadena de custodia mediante tecnología Blockchain

Máster Universitario en Dirección TIC para la Defensa

Especialidad de Sistemas y Tecnologías de la Información

Universidade Vigo

RESUMEN

Blockchain es considerada una tecnología disruptiva que ofrece un nivel de madurez que permite dar soporte a nuevas aplicaciones de alto valor añadido en, prácticamente, cualquier sector de la sociedad. Sus implicaciones, que superan y trascienden la dimensión tecnológica, afectan a los modelos sociales existentes, adentrándose en el campo jurídico. Este ámbito, que requiere de complejos mecanismos que garanticen aspectos tan relevantes como los derechos fundamentales y las libertades públicas, puede beneficiarse de su potencial; pese a ello, su verdadera capacidad transformadora se encuentra aún por explorar debido a la carencia de soluciones concretas.

Este trabajo explora dicho potencial en una aplicación concreta: el aseguramiento de la cadena de custodia de cualquier evidencia de una investigación. Blockchain permite garantizar su trazabilidad, el registro de acciones, su integridad, su unicidad y su disponibilidad, sin necesidad de un tercero confiable. Este paradigma podrá aportar elementos de prueba altamente fiables, cuestión de suma importancia en el ámbito penal.

Su aplicación requiere valorar multitud de opciones de diseño e implementación. Blockchain engloba gran cantidad de modelos y protocolos específicos con diferencias tan notables que resulta obligatorio estudiarlos y analizarlos minuciosamente. De este modo, es posible seleccionar aquel que cumpla con los requisitos mencionados, permitiendo establecer un modelo que se adapte a las exigencias de un Estado de derecho y a las necesidades de la Guardia Civil. Además, se analizan los casos de uso que habrán de satisfacerse para que hagan de la propuesta una herramienta válida que dé soporte a la cadena de custodia.

PALABRAS CLAVE

Blockchain, evidencia, cadena de custodia, *EBSI*, REST.

AGRADECIMIENTOS

A mi madre.

CONTENIDO

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

1 INTRODUCCIÓN Y OBJETIVOS

1.1 Introducción

El tratamiento de las evidencias y la gestión de sus cadenas de custodia constituyen un asunto de capital importancia en un Estado de derecho, en el que se han de garantizar los derechos fundamentales y las libertades públicas de la ciudadanía. Por ello, el objeto principal de este trabajo es estudiar cómo garantizar el derecho a «*un proceso público sin dilaciones indebidas y con todas las garantías*», «*sin que, en ningún caso, pueda producirse indefensión*» [1], mediante una gestión mejorada de la cadena de custodia.

La correcta realización y posterior gestión de la mencionada cadena de custodia de una evidencia puede significar el éxito procesal. Para ello, cuestiones como la trazabilidad y el registro de acciones llevado a cabo sobre las evidencias, su integridad, su unicidad y su disponibilidad, desempeñarán un papel fundamental.

En la actualidad, los servicios y el funcionamiento de las Administraciones Públicas son objeto de la digitalización [2]. En este panorama, las tecnologías disruptivas y emergentes, como Blockchain, brindan gran cantidad de oportunidades y además mejoran y facilitan los quehaceres de sus empleados. Sin embargo, Blockchain es ya una realidad, que puede ser de interés y utilidad para las Fuerzas y Cuerpos de Seguridad [3], en particular para la Guardia Civil, a fin de que desempeñen sus funciones de forma eficaz, eficiente y segura.

Las Fuerzas y Cuerpos de Seguridad del Estado (Guardia Civil y Policía Nacional [no se encuentran entre ellas las policías autonómicas y locales]) están estrechamente conectadas con el mundo jurídico al realizar labores de policía judicial [3]; por este motivo, «*dependen […] funcionalmente de los Jueces, Tribunales o Ministerio Fiscal que estén conociendo del asunto objeto de su investigación*» [3] «*en sus funciones de averiguación del delito y descubrimiento y aseguramiento del delincuente, en los términos que la ley establezca*» [1]. En este sentido, y gracias a sus propiedades, la tecnología Blockchain puede hacer que los procesos judiciales, en lo que respecta a las Fuerzas y Cuerpos de Seguridad del Estado, se desarrollen con las debidas garantías.

Dentro de este ámbito, se encuentra la figura jurídica de la cadena de custodia, que es la que hace que se tenga la certeza de que los vestigios o efectos –relacionados con el delito– que se recogen son los mismos que llegan a concretarse como pruebas en el momento del juicio; Blockchain, en este caso, se presenta como una herramienta que mejora sus características. Sus propiedades hacen de su empleo una solución óptima para asegurar la cadena de custodia de cualquier evidencia en el marco de una investigación. Con esta tecnología se obtiene, esencialmente, un elemento de prueba altamente fiable, y esto constituye una cuestión de suma importancia en el ámbito jurídico penal.

Esta tecnología presenta diversos y dispares métodos de implementación, con diferencias tan reseñables que resulta preceptivo estudiarlos y analizarlos para lograr seleccionar aquel que cumpla con los rigurosos requisitos del proceso penal. Así, se logrará establecer un modelo que se adapte tanto a las exigencias de un Estado de derecho como a las necesidades de la Guardia Civil y de cada investigación en particular. Con *La cadena de custodia mediante tecnología Blockchain* se tratará de abordar este asunto.

1.2 Motivación

La Ley de Enjuiciamiento Criminal, aprobada mediante Real Decreto de 14 de septiembre de 1882, y esencia de la garantía judicial en el proceso penal, no regula de manera explícita los requisitos que ha de tener la cadena de custodia en este ámbito. Sin embargo, sí se encuentra una primera alusión en su artículo 13 [4]:

> «*Se consideran como primeras diligencias la de consignar las pruebas del delito que puedan desaparecer, la de recoger y poner en custodia cuanto conduzca a su comprobación y a la identificación del delincuente […].*»

Estas primeras diligencias constituyen el inicio de la cadena de custodia, puesto que ya se mencionan las pruebas que se pueden obtener y a su custodia, algo que en última instancia permitirá averiguar el delito y descubrir y asegurar el delincuente [1].

Asimismo, se alude a este procedimiento de manera implícita en los artículos 326, 334, y 338, en los que se dice respectivamente lo siguiente [4]:

> «*Cuando el delito que se persiga haya dejado vestigios o pruebas materiales de su perpetración, el Juez instructor […] ordenará que se recojan y conserven para el juicio oral si fuere posible, procediendo al efecto a la inspección ocular y a la descripción de todo aquello que pueda tener relación con la existencia y naturaleza del hecho.*
>
> *A este fin, hará consignar en los autos la descripción del lugar del delito, el sitio y estado en que se hallen los objetos que en él se encuentren, los accidentes del terreno o situación de las habitaciones y todos los demás detalles que puedan utilizarse […].*»
>
> «*El Juez instructor ordenará recoger en los primeros momentos las armas, instrumentos o efectos de cualquiera clase que puedan tener relación con el delito y se hallen en el lugar en que este se cometió, o en sus inmediaciones, o en poder del reo, o en otra parte conocida. El secretario judicial extenderá diligencia expresiva del lugar, tiempo y ocasión en que se encontraren, describiéndolos minuciosamente para que se pueda formar idea cabal de los mismos y de las circunstancias de su hallazgo.*
>
> *La diligencia será firmada por la persona en cuyo poder fueren hallados, notificándose a la misma el auto en que se mande recogerlos.*»
>
> «*[…] los instrumentos, armas y efectos a que se refiere el artículo 334 se recogerán de tal forma que se garantice su integridad y el Juez acordará su retención, conservación o envío al organismo adecuado para su depósito.*»

En esta segunda parte del texto normativo se detalla con mayor profundidad el proceso de cadena de custodia, en el sentido de que se ha de recopilar todo aquello que guarde relación con la prueba, de manera que se pueda asegurar en todo momento cuál es su estado y cómo ha variado hasta que la prueba es puesta a disposición de la autoridad judicial.

Por su parte, y en el ejercicio de sus competencias, la Sala de lo Penal del Tribunal Supremo, al no estar regulado explícitamente y al poder generarse incertidumbre al respecto, en su sentencia 208/2014, de 10 de marzo, considera que [5]:

«*Se viene entendiendo por la doctrina como "cadena de custodia" el conjunto de actos que tienen por objeto la recogida, el traslado y la conservación de los indicios o vestigios obtenidos en el curso de una investigación criminal, actos que deben cumplimentar una serie de requisitos con el fin de asegurar la autenticidad, inalterabilidad e indemnidad de las fuentes de prueba*».

De esta manera, el Tribunal Supremo, como órgano jurisdiccional superior en el territorio nacional, ha determinado, ante la falta de concreción de la Ley de Enjuiciamiento Criminal, esta definición de cadena de custodia, que sirve para establecer un criterio a la hora de materializarlo.

Tras realizar un breve análisis de los aspectos normativos y jurisprudenciales del concepto de cadena de custodia, puede observarse que en ningún momento se hace referencia a que esta pueda realizarse digitalmente. Sin embargo, por analogía, se trata de un concepto, como otros muchos, que puede extrapolarse a otros ámbitos, en este caso, el digital.

En la práctica, al ser compatibles y proporcionar una mayor garantía y seguridad en relación con la custodia de evidencias, en España se tienen dos tipos de cadena de custodia, que se emplean simultáneamente: la cadena de custodia física y la cadena de custodia digital. En la primera, que se lleva a cabo físicamente, se refleja toda la información de los hechos en formato papel; en la segunda, en formato digital, se reflejan los extremos de la cadena de custodia física en un documento electrónico.

Sin embargo, estos dos tipos de cadena de custodia tienen un claro componente subjetivo, pues toda acción que se lleva a cabo depende exclusivamente de las personas. Esto supone que se puedan dar errores y no exista una seguridad absoluta. Por todo ello, se hace necesario contar con un modelo que sea capaz de soslayar esos errores y que incremente la seguridad de la información relativa a las evidencias; y, como se ha expuesto con anterioridad, la tecnología Blockchain puede dar respuesta a esta problemática.

Por tanto, la motivación de este Trabajo es establecer un modelo de cadena de custodia basado en tecnología Blockchain con el que la Guardia Civil pueda garantizar la trazabilidad, la integridad, la unicidad y la disponibilidad de las evidencias, tanto físicas como digitales, recogidas en el marco de las investigaciones que sus unidades y miembros lleven a cabo, teniendo en cuenta en todo momento lo que la legislación vigente y la jurisprudencia disponen.

1.3 Objetivos

En consonancia con la motivación anterior, puede formularse el objetivo de alto nivel de diseñar una plataforma holística que dé soporte para que se lleve a cabo una adecuada gestión de la cadena de custodia mediante el uso, si así resulta conveniente a la luz del análisis previo, de la tecnología Blockchain.

Se han planteado, para su consecución, los siguientes objetivos:

1) O1: estudiar, debido a su relevancia en un Estado de derecho, el marco legal y jurídico de la cadena de custodia tanto de forma general como desde el punto de vista de la tecnología Blockchain.
2) O2: analizar la tecnología subyacente tras el modelo que se pretende establecer.
3) O3: proponer un modelo de plataforma que ofrezca los servicios necesarios para la adecuada gestión de la cadena de custodia.

1.4 Estructura del trabajo

Atendiendo a la motivación y objetivos expuestos, *La cadena de custodia mediante tecnología Blockchain* se encuentra estructurado, además del presente, en seis capítulos.

En primer lugar, en el Capítulo 2 –*Marco legal y jurídico*–, se tratan los conceptos de cadena de custodia y de tecnología Blockchain tanto desde una perspectiva legal como jurídica, procurando

justificar su uso en la Unión Europea y en España. Con este capítulo se da cumplimiento al objetivo O1.

Una vez tratado este aspecto, en el Capítulo 3 *–Análisis de la tecnología–*, se analiza y estudia la tecnología Blockchain subyacente tras el modelo. En el Capítulo 4 *–Blockchain como modelo de confianza–*, se aborda la importancia y fiabilidad de esta tecnología a través del uso que hace de ella la Unión Europea. Con estos dos capítulos se da respuesta al objetivo O2.

Seguidamente, en el Capítulo 5 *–Modelo propuesto–*, se propone un modelo que sea capaz de cumplir con las exigencias de un Estado de derecho y las necesidades de la Guardia Civil, y en el Capítulo 6 *–Prueba de concepto–*, se implementa parcialmente el modelo propuesto, pues su implementación completa resulta materialmente inviable. De esta forma, se satisface el objetivo O3.

Por último, en el Capítulo 7 *–Conclusiones y líneas futuras–*, se presentan las conclusiones obtenidas y las lecciones aprendidas en el proceso de realización de este documento, así como las líneas futuras para continuar el desarrollo del modelo en posteriores trabajos.

2 MARCO LEGAL Y JURÍDICO

2.1 Cadena de custodia

2.1.1 La cadena de custodia en la Guardia Civil y en el resto de las Fuerzas y Cuerpos de Seguridad

Las Fuerzas y Cuerpos de Seguridad, y en particular la Guardia Civil, han de actuar conforme al ordenamiento jurídico y de acuerdo con las instrucciones que reciban de los órganos judiciales (jueces, tribunales y Ministerio Fiscal) ejerciendo funciones de Policía Judicial.

En su ámbito, la cadena de custodia constituye el conjunto de actuaciones que tienen como fin preservar y garantizar la integridad y permanencia de las pruebas que son objeto de estudio en el marco de una investigación, recogiéndose para ello aquellos indicios o evidencias en el lugar en que se desarrolla el hecho delictivo, ya sea físico o virtual. El objetivo final se reduce a garantizar su validez procesal, es decir, a probar que el indicio presentado ante la autoridad judicial es realmente aquel que fue recuperado en el lugar de comisión del delito.

Este procedimiento se inicia en el lugar en que se encuentra la evidencia, y continúa a lo largo de todo el proceso hasta su presentación ante la autoridad judicial. Por ello, en función de la evidencia y su complejidad, pueden actuar sobre él un número relevante de personas.

Todo miembro de la Guardia Civil que actúe como policía judicial y que participe en el proceso de cadena de custodia debe velar por la seguridad, integridad y preservación de los indicios, por lo que debe evitar, también, cualquier tipo de acción que le afecte y que altere de cualquier forma su estado inicial.

Para garantizar lo anteriormente descrito, se confecciona un documento en soporte papel en el que toda actuación llevada a cabo sobre el indicio queda registrada, haciéndose constar los datos relativos a la remisión; la recogida; la identificación de las evidencias o muestras que se remiten; los estudios que se solicitan; la recepción de esas evidencias o muestras; los agentes intervinientes, y aquellas incidencias, observaciones o comentarios que se estimen relevantes para la investigación.

Las unidades que intervengan han de archivar todo ello para, en su caso, una ulterior actuación o requerimiento de la autoridad judicial.

En la siguiente figura se representa la cadena de custodia empleada en la Guardia Civil, recogida en el documento de toma de evidencias y pruebas:

Cadena de custodia				
TIP y firma	Fecha	Sello de las unidades	Tipo de actuación realizada	Incidencias

Figura 2-1 Ejemplo de ficha de cadena de custodia de la Guardia Civil

Puede observarse, en condiciones ideales, cómo de manera simple se garantiza la inalterabilidad de las evidencias o pruebas, con independencia de si son físicas o digitales; en este segundo caso, teniendo en cuenta que han de estar almacenadas, además, en un soporte físico. Esto significa que, en última instancia, todo ello depende de un medio físico.

A continuación, se muestra un esquema del proceso de cadena de custodia en el ámbito de la Guardia Civil, teniendo en consideración la experiencia en investigación del autor del presente documento:

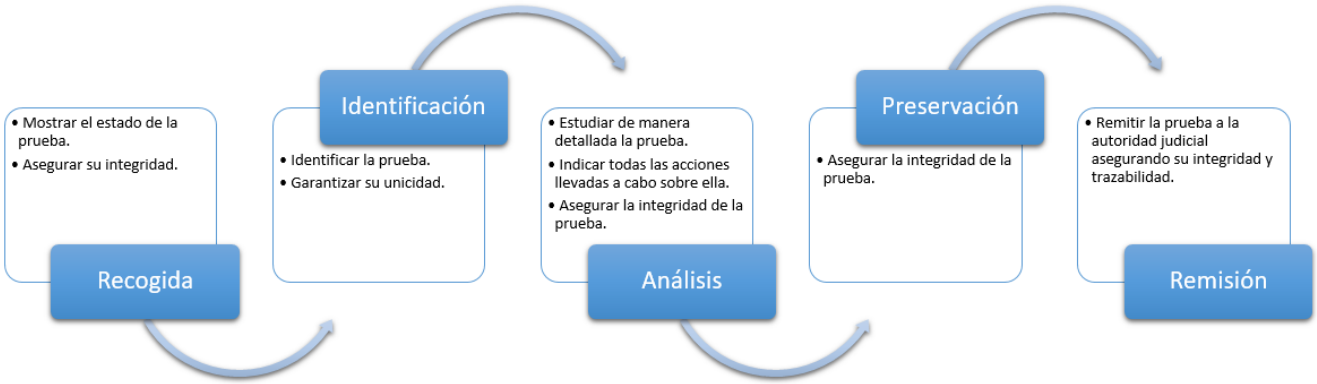

Figura 2-2 Proceso de cadena de custodia

Según se ha reflejado en el apartado *Introducción y objetivos*, se ha indicado que existe la posibilidad de extrapolar este concepto al entorno digital, ya que legalmente las garantías de la cadena de custodia en este entorno podrían ser, al menos, idénticas a las garantías que posee la cadena de custodia tradicional. En este caso, se contaría con las ventajas que proporcionan las tecnologías de la información y las comunicaciones.

Actualmente, la digitalización de la cadena de custodia es un proceso paralelo al tradicional en las investigaciones que llevan a cabo los miembros de la Guardia Civil, y esta situación es similar en el resto de las Fuerzas y Cuerpos de Seguridad.

2.1.2 La cadena de custodia en el ámbito internacional

En el ámbito internacional, si bien no existe una norma de obligado cumplimiento, se tiene el Protocolo de Estambul, mediante el que se establece el "Manual para la investigación y documentación eficaces de la tortura y otros tratos o penas crueles, inhumanos o degradantes" [6].

La primera alusión que se realiza a la cadena de custodia se encuentra enmarcada en los procedimientos para la investigación y casos de tortura, en particular en el aseguramiento y la

obtención de pruebas físicas. Se indica que el investigador deberá reunir aquellas pruebas físicas para documentar un caso o un cuadro de tortura. El acopio y análisis de estas pruebas constituye «*uno de los aspectos más importantes de toda investigación cuidadosa e imparcial de casos de tortura*», por lo que deberá justificar la verdad a través de su cadena de custodia para que puedan utilizarse en procedimientos futuros [6].

Dentro de estos procedimientos para la investigación y casos de tortura, también se incluyen las fotografías que se llevan a cabo de las lesiones de las personas que presuntamente han sido torturadas, de los lugares en que se han producido dichas torturas y de los indicios que, en su caso, se encuentren [6].

Asimismo, en las muestras forenses de aquellos casos relativos a una agresión sexual reciente se ha de garantizar su plena protección, adoptando estrictas precauciones, y documentar la cadena de custodia, «*para evitar toda alegación de contamientación cruzada*» [6].

En el orden comunitario, se encuentra únicamente la Recomendación del Consejo, de 30 de marzo de 2004, sobre directrices para la toma de muestras de drogas incautadas [7]. Con ella se pretende asegurar la cadena de custodia de las evidencias relacionadas con las drogas y sustancias estupefacientes, y que estas sean admitidas como prueba en los procedimientos judiciales con las debidas garantías procesales. Sin embargo, una recomendación, como acto legislativo no vinculante dimanante de instancias europeas, no impone obligación alguna a los Estados miembro.

En definitiva, resulta entonces evidente que el plano extraestatal no profundiza en la regulación de la cadena de custodia, puesto que es, salvo en tratados y acuerdos internacionales suscritos, una cuestión cuya competencia le corresponde a cada estado de manera individual. Además, en el ámbito comunitario, esta situación se ve aún más exacerbada, pues apenas las instituciones y tribunales europeas hacen alusiones a la cadena de custodia.

2.2 Blockchain y cadena de custodia

2.2.1 Blockchain y cadena de custodia

Como se ha tratado con anterioridad, aunque la tecnología Blockchain pueda tener aplicación en multitud de ámbitos, entre ellos la cadena de custodia, es cierto que el concepto de cadena de custodia está íntimamente relacionado con el mundo jurídico, por lo que conviene tratar esta tecnología desde una perspectiva legal, en el sentido de que cuente con todas las garantías procesales y pueda considerarse, así, una prueba válida en un procedimiento judicial.

Para que la cadena de bloques se tenga en cuenta como forma de garantizar la cadena de custodia en un proceso judicial, se ha de tener en cuenta lo dispuesto en la Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil, concretamente en su artículo 299, relativo a los medios de prueba [8]. En este artículo se hace alusión, entre otros, a los documentos públicos y privados, a los dictámenes de peritos, a los medios de reproducción de la palabra, el sonido y la imagen, y a cualquier otro medio que posibilite obtener certeza sobre hechos relevantes, así como a las medidas que en cada caso resulte necesario adoptar [8].

Además de lo anterior, se encuentran aquellos instrumentos que permiten «*archivar y conocer o reproducir palabras, datos, cifras y operaciones matemáticas llevadas a cabo con fines contables o de otra clase, relevantes para el proceso*» [8].

De lo anterior puede deducirse que la tecnología Blockchain, en función del caso y de las medidas que se adopten, puede ser admitida como medio de prueba. Sin embargo, al no estar regulado explícitamente en la ley, su admisión dependerá en última instancia del juez o tribunal competente, que ha de lograr el perfecto entendimiento de esta tecnología, como ocurre con cualquier otro elemento del proceso.

Como muestra de ello, el primer caso en que se aceptó la tecnología Blockchain con esta finalidad en España se dio en 2019. La Sala de lo Penal del Tribunal Supremo, mediante sentencia 2109/2019, de 20 de junio, falló en favor de que la blockchain de bitcoin es una «*red informática verificada*» en la que se emplea «*tecnología informática y criptográfica*» [9]. Si bien únicamente se hace mención expresa de la blockchain de bitcoin, esta explicación podría extenderse, por analogía, a otras cadenas de bloques.

Asimismo, al existir diversas líneas jurisprudenciales, también se ha pronunciado al respecto la Sala de lo Social del mencionado Tribunal, admitiendo que se pueden considerar las pruebas digitales dentro de un concepto amplio de prueba documental. La justificación se basa en que «*el avance tecnológico ha hecho que muchos documentos se materialicen y presenten a juicio a través de los nuevos soportes electrónicos, lo que no debe excluir su naturaleza de prueba documental, con las necesarias adaptaciones (por ejemplo, respecto de la prueba de autenticación). Si no se postula un concepto amplio de prueba documental, llegará un momento en que la revisión fáctica casacional quedará vaciada de contenido si se limita a los documentos escritos, cuyo uso será exiguo*» [10]. De este modo, la tecnología Blockchain podría ser considerada prueba documental.

Aunque cada vez su uso está más extendido en España, el empleo de esta tecnología genera cierta incertidumbre, ya que no se encuentra regulada en este ámbito ni existe jurisprudencia que, en su caso, otorgue seguridad jurídica y lo ampare.

Por otro lado, en países como China, ya las instancias judiciales superiores han elaborado un reglamento en el que se reconoce la legitimidad y apoya el uso de la tecnología Blockchain para recopilar, corregir, proteger y almacenar la información y las evidencias digitales. Así, diferentes ciudades de este país han visto cómo se pueden preservar las evidencias y cómo se han podido facilitar, gracias a esta tecnología, los procedimientos judiciales [11]. Sin embargo, este sistema no está completamente desplegado a lo largo del país, y se espera que en los próximos años la red llegue al nivel local de este ámbito [12].

2.2.2 Panorama de la digitalización y del uso de la tecnología Blockchain en España

Para afrontar de manera eficaz las consecuencias económicas y sociales de la pandemia de la COVID-19, el Consejo Europeo, como institución que define las orientaciones y las prioridades políticas generales de la Unión Europea, acuerda el Fondo de Recuperación *Next Generation EU*, un instrumento de recuperación que cuenta con un presupuesto de 750.000 millones de euros [13].

Dentro de este instrumento se halla el Mecanismo de Recuperación y Resiliencia, que constituye el núcleo del Fondo y cuyo objetivo es apoyar la inversión y las reformas de los Estados miembros para lograr una recuperación sostenible y resiliente, al tiempo que se promueven las prioridades ecológicas y digitales de la Unión Europea [13].

En España, derivado de ese Mecanismo, se encuentra el Plan de Transformación, Recuperación y Resiliencia, elaborado en 2021 por el Gobierno de España y que cuenta con cuatro ejes transversales y diez políticas palanca; en el caso de estudio cabe destacar el eje "Transformación digital" y la política palanca "Una Administración para el siglo XXI", que confluyen en la «*digitalización de los servicios y del funcionamiento*» de las Administraciones Públicas [13], y en particular de la Guardia Civil, ofreciendo «*innumerables oportunidades*» [14].

Asimismo, como uno de los elementos principales del Plan de Recuperación, Transformación y Resiliencia [13], se ha elaborado el Plan de Digitalización de las Administraciones Públicas [2], que constituye el «*marco estratégico global para avanzar en la transformación de la Administración*». En él se contempla «*la creación de servicios públicos personalizados en innovadores que se puedan enmarcar en actuaciones europeas, participando con los Estados miembro de la Unión Europea en proyectos como el European Blockchain Services Infrastructure (*EBSI*)*» [2].

Todo ello crea el ambiente y la situación propicios para que se opte por emplear tecnologías que en su momento fueron disruptivas, ya que están consolidadas e implantadas en numerosos ámbitos [15]. La cadena de bloques y los contratos inteligentes, que pueden llegar a vertebrar [16] aquellas aplicaciones que requieren un mayor nivel de privacidad y de seguridad, son un destacado ejemplo. Además, la implementación de la cadena de custodia mediante Blockchain podría tener cabida en este marco.

3 ANÁLISIS DE LA TECNOLOGÍA

3.1 Introducción

Como se ha expuesto con anterioridad, debido a que en la legislación no se ha determinado forma alguna de implementación o, en términos generales, de llevar a cabo la cadena de custodia, existen múltiples modos de materializarlo. Este documento explora la hipótesis de que el uso de las redes blockchain son el soporte adecuado para llevar a cabo este encargo del legislador. Por ello, el primer paso será realizar un análisis en profundidad de dicha tecnología, para desarrollar un criterio sólido que permita evaluar la pertinencia de su uso.

Esta tecnología posibilita asegurar cuatro propiedades que son inherentes a la cadena de custodia: la trazabilidad y el registro de acciones sobre la evidencia, su integridad, su unicidad y su disponibilidad.

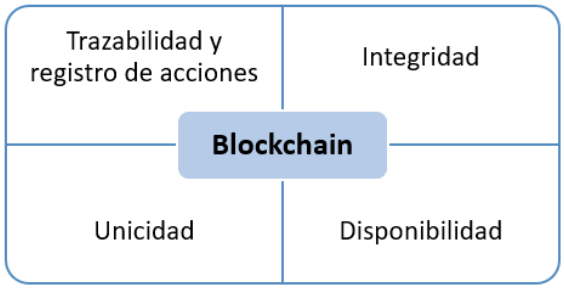

Figura 3-1 Blockchain y propiedades en la cadena de custodia

Asegurando estas propiedades, con independencia de la evidencia de que se trate, se podrá identificar su origen y las diferentes etapas por las que ha pasado, además de hacer constar todas las acciones que se realizan sobre ella. Asimismo, se podrá garantizar que no ha sido modificada, que es única, sin duplicidades, y que se encuentre disponible en todo momento, sin necesidad de un tercero confiable. Este último aspecto puede ser de especial relevancia en caso de cambios de jurisdicción o en lo que respecta a garantizar la auditabilidad de la información registrada. Por ello, se considera que Blockchain se erigirá en una tecnología que tendrá repercusión en el ámbito legal [17].

3.2 Bitcoin

Si bien blockchain es un término empleado con posterioridad, su origen se encuentra en el *White Paper* de Bitcoin [18]. En él se hace alusión a una moneda electrónica, definida como «*una cadena de firmas digitales*» en la que «*cada dueño transfiere la moneda al próximo*» firmando «*digitalmente un hash de la transacción previa y la clave pública del próximo dueño*», y «*agregando estos datos al final*

de la moneda». Así, un beneficiario podría comprobar esas firmas para «*verificar la cadena de propiedad*».

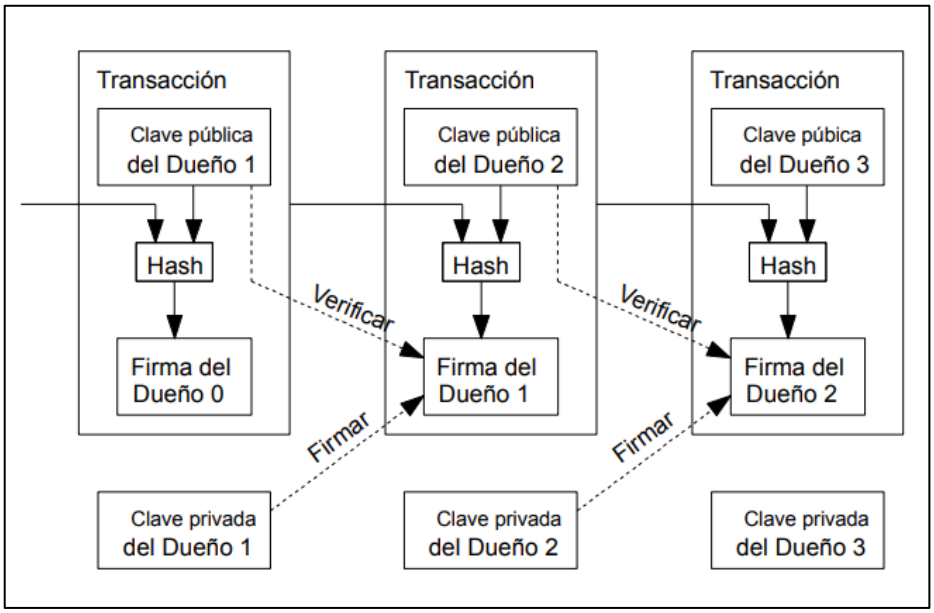

Figura 3-2 Blockchain de Bitcoin [18]

Las transacciones son operaciones mediante las que se incorpora información de diferente índole en la blockchain. En el caso de Bitcoin, se refieren al «*envío o transferencia de valor entre dos partes*» y se reducen al traspaso de bitcoins de una persona a otra dentro de su red [19]. Cada transacción «*se combina con otras para conformar un bloque*», y cuando este se incluye en la cadena, la transacción es definitiva y se considera que se ha completado [20].

Al considerarse Bitcoin de tal forma, su uso principalmente sería el del comercio electrónico, en el que el doble gasto constituye una de las principales preocupaciones. En este sentido, no se puede asegurar que no se ha efectuado un doble gasto de la moneda sin que exista una entidad que certifique que no se ha dado tal circunstancia, es decir, que determine que las transacciones son únicas. Para solucionar este problema, el modelo de blockchain de Bitcoin propone «*un sistema de participantes que estén de acuerdo con una historia única del orden en que estas fueron recibidas*» (algoritmo de consenso), introduciendo un «*servidor de marcas de tiempo*», suprimiendo la necesidad de que exista una autoridad centralizada o terceros confiables que lleven a cabo esta función. De esta manera, gracias a todos los participantes o nodos que lo acordaron, cualquier persona podría verificar que una determinada transacción se efectuó en primer lugar.

Para llevar a cabo esta acción, se toma el hash de un bloque, y se le añade la fecha y la hora de la transacción. Una vez se ha realizado esta operación, se genera un nuevo hash, de manera que «*cada marca de tiempo incluye la marca de tiempo previa en su hash, formando una cadena*»; así, con cada marca de tiempo adicional se refuerzan las anteriores [18].

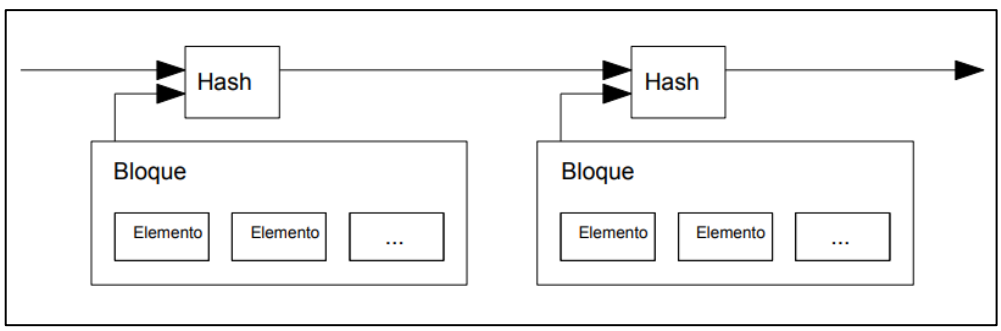

Figura 3-3 Servidor de marcas de tiempo [18]

De este modo, se implementa un libro mayor, replicado y descentralizado en una red *peer-to-peer*[1] (*P2P*), basada en una secuencia de bloques que contienen las transacciones efectuadas, ordenadas cronológicamente, y el hash del bloque anterior, y en la que cada nodo mantiene una copia completa de la blockchain.

Los nodos crean nuevos bloques al recibir transacciones, que son introducidas en la red, y una vez se completan, inician el proceso de consenso ya mencionado, para convencer al resto de nodos e incluirlo en la blockchain. En Bitcoin este proceso se basa en *Proof-of-Work* (*PoW*; en castellano, Prueba de Trabajo), e implica que los nodos compitan entre sí para confirmar las transacciones y crear nuevos bloques calculando *nonces*[2], cumpliendo, así, con las restricciones de dificultad.

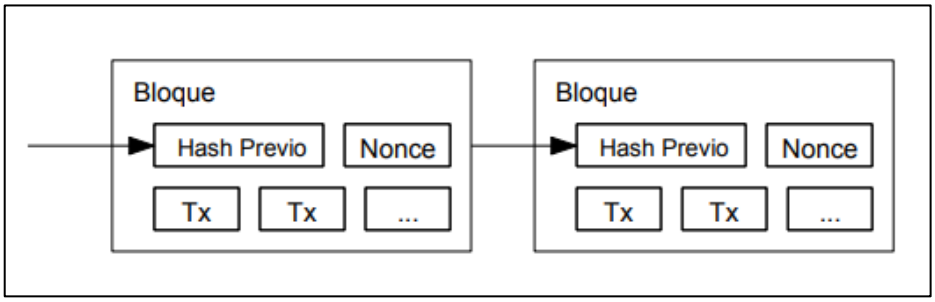

Figura 3-4 Proof-of-Work [18]

El proceso de *PoW* implica hallar un *nonce*, de manera que el hash del bloque completo empiece con un determinado número de bits cuyo valor sea cero. Se trata de un proceso forzado e iterativo, en el que la cantidad de ceros se incrementa progresivamente; así, «*el trabajo promedio requerido es exponencial*». Esto hace de resolver este tipo de problemas una tarea computacionalmente difícil, al contrario que verificar su validación, que requiere una menor cantidad de recursos [18].

Para incentivar la participación, aquellos que crean un bloque, los comúnmente denominados mineros, recibirán una determinada cantidad de bitcoins a modo de recompensa. En ocasiones, diferentes mineros pueden generar un bloque válido, creando así bifurcaciones en la cadena. Las bifurcaciones se resuelven aceptando únicamente la rama con mayor longitud, como continuación de la cadena, y eliminando el resto –pues es la primera la que tiene «*un mayor esfuerzo invertido en ella*» [18]– mediante la votación de los *peers*.

La principal ventaja de *PoW* sobre otros algoritmos de consenso se reduce a que un atacante debe disponer del control de la mayoría de la potencia computacional de la red en lugar del control de la mayoría de los nodos, que es considerado una tarea más compleja y virtualmente imposible en una red pública de grandes dimensiones [18].

Sin embargo, la principal crítica de *PoW* es la excesiva demanda de energía que lleva aparejada, lo que impide que se emplee en determinados contextos. Esto ha hecho que se investigue sobre formas alternativas de consenso, como *Proof-of-Stake* (*PoS*), presentado en 2012 en *PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake* [21] y empleado en Ethereum[3] [22].

Otro problema que puede surgir en la blockchain de Bitcoin es lo que se denomina *fork* (bifurcación). Las bifurcaciones pueden ser de dos tipos: *soft fork* y *hard fork*. Estas se dan cuando se produce una divergencia en la blockchain, esto es, un cambio en el protocolo, lo que afecta a la validez

[1] Una red *peer-to-peer* se trata de una red construida sobre los protocolos TCP/IP, en la que sus integrantes participan de manera descentralizada atendiendo a un protocolo de comunicaciones y consenso común, y pudiendo intercambiar información de extremo a extremo sin necesidad de una autoridad o de terceras partes.

[2] Un *nonce*, que procede de la expresión inglesa "*number that can be only used once*", es un número arbitrario empleado en los protocolos de autenticación criptográficos, y que únicamente puede emplearse una vez.

[3] Conviene reseñar que Ethereum 2.0, actualización de Ethereum, es la blockchain que cuenta con PoS como mecanismo de consenso.

de las reglas. En el primer tipo se produce una actualización gradual de la blockchain, y los nodos pueden crear nuevos bloques si cumplen con las nuevas reglas, al ser compatibles con las versiones anteriores; sin embargo, en el segundo, la blockchain queda dividida en dos, y los nodos han de actualizarse para poder seguir creando bloques, al ser incompatible con las versiones anteriores. Esto implica que se requiera consenso para su resolución, lo que conlleva cierto tiempo para que esta situación se resuelva y que la blockchain funcione con normalidad. Con Ethereum, gracias a *PoS*, este problema se puede evitar o, en caso de que se produzca, reducir dicho tiempo.

3.2.1 Latencia en Bitcoin

Un aspecto que conviene resaltar en la blockchain de Bitcoin es la latencia, puesto que constituye un obstáculo si se quiere emplear para fines que requieran cierta celeridad.

En Bitcoin, no se puede asegurar el éxito de una transacción hasta que no se haya minado en un bloque. Esto supone un tiempo que, por lo general, es de 10 minutos. Además, una vez se haya llevado a cabo, se ha de esperar a que los diferentes nodos de la red reconozcan la transacción e incluyan seguidamente nuevos bloques, para que no sea rechazada. Además, la blockchain de Bitcoin muestra las transacciones como no confirmadas hasta que exista una profundidad de seis bloques[4], si bien en determinados contextos privados, como en plataformas de intercambio de criptomonedas, puede establecerse que este umbral sea mayor [23].

3.2.2 Seguridad en Bitcoin

La seguridad de la blockchain de Bitcoin reside principalmente en la criptografía (también en que se trata de una red distribuida). Particularmente, se emplea la denominada criptografía de clave pública o criptografía asimétrica, y el algoritmo ECDSA (Elliptic Curve Digital Signature Algorithm). Con ella se generan dos claves (una pública y otra privada) que se hallan relacionadas mediante una operación matemática sobre una función de curva elíptica [24], definida mediante el estándar secp256k1 [25].

Concretamente, la clave privada se trata de un número secreto generado de modo aleatorio y conocido únicamente por quien lo generó, mientras que la clave pública es un número generado a partir de la clave privada en la forma especificada en el párrafo anterior, de manera que resulte computacionalmente difícil obtener la primera conociendo la segunda [26].

Con anterioridad se mencionó el concepto de firma digital. Con ella, el receptor de un mensaje puede verificar la autenticidad del origen y que este no ha sido modificado desde que se generó, ofreciendo el soporte para la autenticación e integridad de los datos y el no repudio en origen, ya que el emisor de un mensaje firmado digitalmente no puede argumentar que no lo es [27].

El proceso de firma digital se explica a continuación:

1) A y B disponen de claves públicas y privadas.
2) A genera el hash del mensaje y lo cifra con su clave privada, obteniéndose así la firma digital.
3) A remite el mensaje con la firma digital a B.
4) B emplea la clave pública de A para descifrar el resumen del mensaje.
5) B calcula el hash del mensaje y lo compara con el que proporciona A.
6) Si son idénticos, B verifica que A ha sido quien ha enviado el mensaje y que este no ha sido modificado.

[4] Esta profundidad de seis bloques no viene establecida por la propia red de Bitcoin, sino que se considera una cantidad de bloques prudente para que se lleve a cabo la confirmación del bloque.

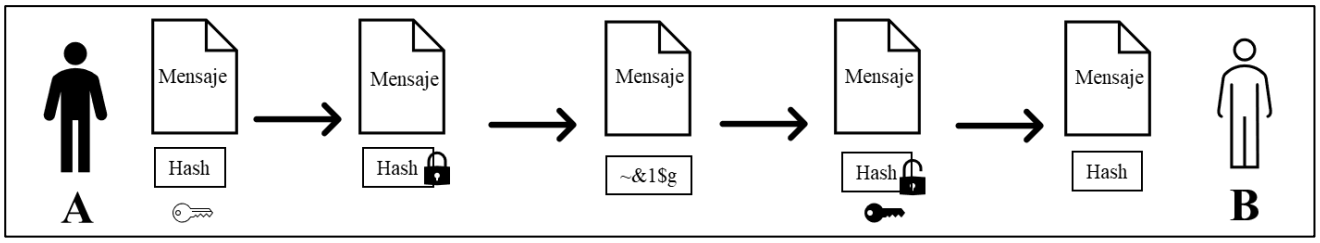

Figura 3-5 Firma digital

Con este sistema criptográfico, que aprovecha «*la naturaleza aparentemente aleatoria de las funciones hash*» [28], se puede generar un hash de 256 bits, pues es su máximo valor posible. Este número de combinaciones es tan elevado que se tardarían varios trillones de años en crear todas las claves con los recursos actuales [24]. Por ello, debido a la gran cantidad de combinaciones (2^{256} combinaciones distintas) y a que es computacionalmente imposible calcular todas ellas, Bitcoin se trata de un sistema seguro, aunque existan otras formas de ataque (ataque del 51 por ciento, minado egoísta, ataque eclipse [Hei+15 y Dot+21], interrupciones de servicio, depuración de responsabilidad [*accountability* y *fair anonymity*] y computación cuántica).

3.3 Ethereum y smart contracts

Una vez analizada la blockchain de Bitcoin, germen de esta tecnología, conviene abordar la blockchain de Ethereum, ya que incluye una serie de funciones y capacidades adicionales, que serán tratadas en este apartado.

Ethereum se trata de una blockchain que permite llevar a cabo acciones adicionales a las que ya hace la red de Bitcoin sin necesidad de que exista una autoridad central. Si bien ambas redes permiten emplear monedas digitales, la principal diferencia reside en que Ethereum es programable, es decir, posibilita la construcción de aplicaciones que usen la cadena de bloques para almacenar datos o controlar lo que estas pueden hacer [22].

El objetivo de Ethereum es crear un protocolo alternativo para construir aplicaciones descentralizadas y que estas cuenten con diferentes utilidades. Las principales aplicaciones a las que se dirige son aquellas en las que el rápido tiempo de desarrollo, su seguridad y la capacidad para interactuar de manera eficiente son fundamentales. Para ello utiliza un lenguaje de programación Turing completo que permite a cualquier persona escribir contratos y aplicaciones descentralizadas, proporcionándoles autonomía y libertad en lo que respecta reglas arbitrarias de propiedad, formatos de transacción y funciones de transición de estado [22].

Esto es posible gracias a que Ethereum cuenta con una máquina virtual que forma parte de su blockchain (*Ethereum Virtual Machine* [EVM]) y que permite ejecutar una amplia gama de instrucciones «*que definen las reglas de cálculo de un nuevo estado válido de bloque a bloque*»; en suma, es el entorno de ejecución de los contratos inteligentes, es decir, en el que las instrucciones se llevan a cabo. Estas instrucciones, que se denominan *smart contracts* o contratos inteligentes, son programas que se ejecutan e implementan en la blockchain de Ethereum a través de un grupo de código (funciones) y de datos (estado) que existe en una dirección específica de la misma [22]; además, en ellas no cabe la interpretación, pues la claridad de los parámetros ha de ser una de sus características.

Específicamente, un contrato inteligente representa uno de los dos tipos de cuenta de Ethereum, por lo que tiene un saldo y puede, además, efectuar transacciones dentro de la red. Al estar implementados en ella, no son controlados por los usuarios, sino que se ejecutan autónoma y automáticamente en la forma en que se hayan programado. El otro tipo de cuenta es la de usuario, y a través de ella se puede interactuar con un contrato inteligente, efectuando transacciones que ejecutan una función definida en él [22].

La red de Ethereum, al igual que la de Bitcoin, está formada por un conjunto de nodos; sin embargo, en este caso, cada uno de ellos cuenta con una EVM local en la que se efectúa la transacción y en la que se almacena junto con su estado. Todo ello consume un recurso virtual denominado *gas*, que sirve de combustible para la EVM y se emplea para incentivar a los mineros, de modo que estos ejecuten las transacciones, que se incluyen posteriormente en la blockchain. De hecho, se recompensa a los mineros con tasas proporcionales a la cantidad total de *gas* consumida en cada transacción [29].

Para evitar que los bloques minados sean demasiado extensos, cuestión que puede tener un impacto severo en la propagación y en el proceso de latencia, cada bloque tiene un límite de *gas*. Este límite representa el número máximo de pasos computacionales que puede realizar un contrato antes de que se anule la transacción, siendo la máxima cantidad de *gas* que pueden consumir todas las transacciones incluidas en el bloque. Por tanto, es posible que una transacción no se incluya en el bloque en cuestión si se excede de este límite; en tal caso, la transacción se incluiría en el siguiente bloque de la blockchain [22].

Por otro lado, como ya se ha mencionado, el algoritmo de consenso de Ethereum es *PoS*, que difiere del de Bitcoin. En este caso, la selección de los nodos validadores a los que se hacía referencia se realiza de forma aleatoria por la propia blockchain, que otorga una mayor probabilidad de asignar la validación a aquellos que cumplan una serie de requisitos, entre los que se encuentran *la cantidad de moneda reservada y el tiempo de participación en la red* [22], si bien pueden definirse otros.

Con *PoS*, un conjunto de nodos, denominados validadores, se turnan tanto en la proposición de nuevos bloques como en la votación. Los validadores, que introducen una participación en la red, son incentivados para actuar de manera honesta y no perder esa participación; si estos realizan comportamientos maliciosos o inapropiados, serían expulsados de la red, perdiendo así su participación. Todo ello se haría constar en un registro de validadores que la propia blockchain posee [22].

Otro aspecto relevante en Ethereum son los oráculos, que constituyen el «*puente entre la blockchain (on-chain) y el mundo real*» (*off-chain*), y su misión es incluir en la propia cadena de bloques información del mundo físico, para que pueda ser tenida en cuenta en las operaciones de la propia blockchain. Su existencia es necesaria, pues permite que cada nodo sea capaz de replicar cada transacción y obtener idéntico resultado: con independencia del nodo que replique la transacción, se emplearán los mismos datos, publicados en la red y que son inmutables. Para ello, el oráculo consultará diferentes API y posteriormente enviará las transacciones, que actualizarán los datos de los contratos inteligentes [22].

3.4 Hyperledger

3.4.1 Hyperledger Fabric

Otra alternativa es Hyperledger Fabric, proyecto de Hyperledger bajo los auspicios de Linux Foundation [30]. Este proyecto se trata una plataforma de código abierto de Tecnología de Contabilidad Distribuida (*DLT*, por sus siglas en inglés), diseñada para contextos empresariales, con una arquitectura modular y extensible para desplegar y operar con blockchains cuyas transacciones únicamente puedan ser procesadas por quienes estén autorizados (*permissioned* blockchains). Conviene, así, diferenciar entre las *permissionless* blockchains y las *permissioned* blockchains: en las primeras cualquiera puede participar sin identificarse, y, además, requieren con frecuencia consenso, una criptomoneda nativa e incentivos económicos; por su parte, las segundas cuentan con un conjunto de participantes conocidos e identificados, y proporcionan una manera segura de interacción entre las entidades que tienen un objetivo común, si bien la confianza no es total [31].

El funcionamiento de una blockchain en Hyperledger Fabric se basa en una arquitectura *execute-order-validate*, y se detalla a continuación [31] [32] [33]:

1) Un cliente emite una transacción a través de una aplicación, tras invocarse una función de un contrato inteligente (*chaincode*), que se ejecuta en un contenedor *Docker*. La transacción es enviada a los pares avaladores, que son los que ejecutan dicha función.
2) Los pares avaladores ejecutan la función, generando un aval, pero no actualizan el libro mayor y devuelven el aval a la aplicación. Este aval cuenta con dos variables: una indica el estado final –modificado– de los datos y la otra, el estado actual –sin actualizar–.
3) La aplicación recopila todos los avales de una transacción y los incorpora en un paquete denominado transacción avalada, que se envía al servicio de ordenamiento. Este servicio recibe las transacciones avaladas, las ordena y las agrupa en un bloque, que remite a los pares confirmadores para que lo añadan al libro. Los pares confirmadores desempeñan un papel fundamental en la política de consenso, pues han de llegar a un acuerdo acerca del orden de los bloques y de las transacciones de cada bloque.
4) Una vez se ha llevado a cabo este proceso de validación, cada par confirmador actualiza los cambios que las transacciones avaladas válidas han generado en su libro local. De esta manera, estos validan, para cada transacción, la política del aval y que no haya habido variaciones en el estado del libro con respecto al actual, es decir, los datos de la variable del estado actual han de coincidir con el estado actual del libro.
5) En caso de que la transacción sea avalada, los cambios que aparecen en la variable del estado modificado deben aplicarse al libro local de cada par. Cada transacción avalada del bloque es etiquetada como válida o inválida, y solo para las primeras se confirma el estado modificado. Cada par confirmador añade el bloque en su libro.
6) Finalmente, se emite un evento para notificar a la aplicación si la transacción fue válida o no.

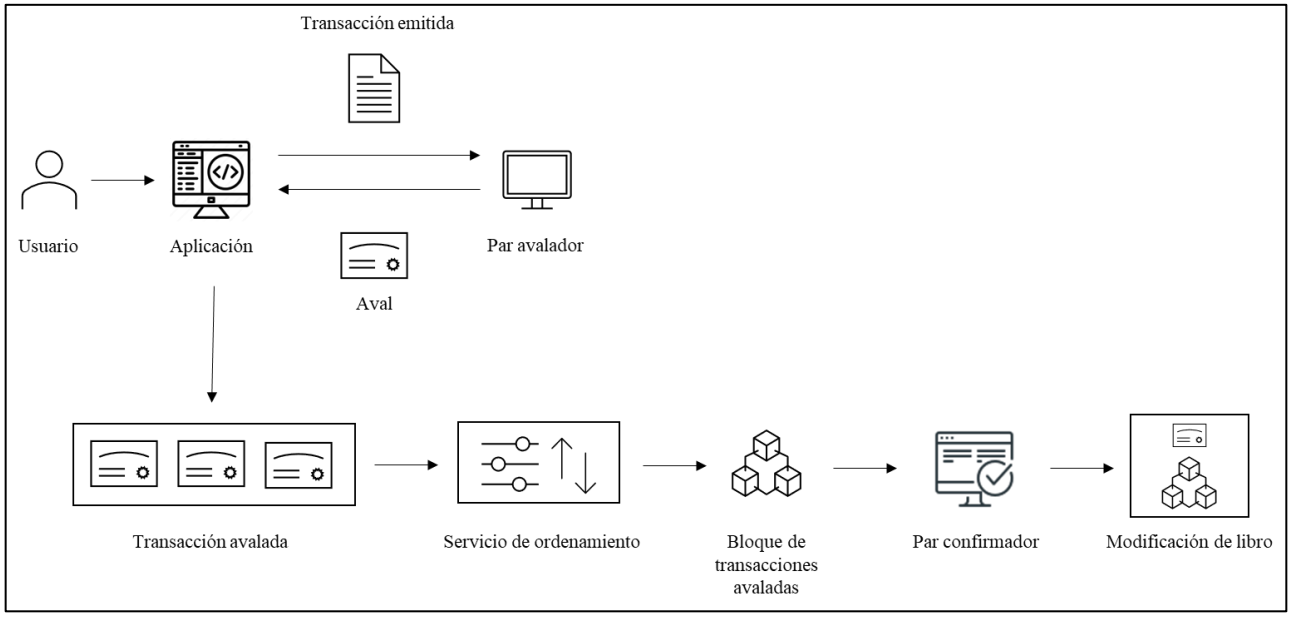

Figura 3-6 Transacción Hyperledger Fabric [32]

Fabric puede adaptarse tanto a entornos de confianza como a aquellos otros en los que puedan existir fallos; en general, se considera que cualquier cliente puede ser malicioso o el origen de esos fallos. Los *peers* se agrupan en organizaciones, y cada organización forma un dominio confiable, en el que cada *peer* confía en el resto de los que se hallan dentro.

En este tipo de redes, existe la figura del proveedor de servicios de membresía (*MSP*, por sus siglas en inglés), que realiza una función esencial: mantiene la identidad de todos los nodos del sistema y es responsable de emitir las credenciales de autenticación y de autorización; al ser del tipo *permissioned*, toda interacción entre nodos se da a través de mensajes autenticados, en particular mediante firma digital. El servicio de membresía comprende un componente en cada nodo, que puede

autenticar transacciones, verificar su integridad, firmar y validar los avales, y autenticar otras operaciones en la blockchain. Para llevar a cabo la autenticación basada en firmas digitales y poder adaptarse a autoridades comerciales de certificación, el *MSP* permite implementar una infraestructura de clave pública (*PKI*, por sus siglas en inglés), si bien ya Fabric incluye su autoridad propia (Fabric-CA).

Fabric posibilita configurar una red blockchain de dos modos: el modo *offline*, en el que las autoridades de certificación general las credenciales y las distribuye a todos los nodos –los *peers* y los nodos del servicio de ordenamiento únicamente pueden registrarse en este modo–, y el modo *online*, en el que se emiten las credenciales criptográficas para los usuarios. La configuración del *MSP* ha de asegurar que todos los nodos, especialmente los *peers*, reconocen la validez de las identidades y autenticaciones.

3.4.2 Hyperledger Besu

Hyperledger Besu es un cliente[5] de Ethereum *open source*, desarrollado bajo la licencia Apache 2.0 [34] y escrito en el lenguaje de programación de propósito general Java, que puede ejecutarse tanto en la red pública de Ethereum como en *permissioned* blockchains. Besu es un software que implementa el protocolo de Ethereum y presenta las siguientes características [35], en consonancia con la Enterprise Ethereum Alliance[6] [36] (*EEA*):

1) EVM: permite el despliegue y ejecución de contratos inteligentes mediante transacciones dentro de la blockchain de Ethereum.
2) Algoritmos de consenso (*Proof-of-Authority* [PoA] –concepto que se explicará en el siguiente capítulo– y *PoW*): empleados en la validación de transacciones y en la creación y validación de bloques.
3) Almacenamiento: utiliza una base de datos para conservar localmente la información de la cadena de bloques. Se tienen, así, dos categorías:
    a. Blockchain: los datos están compuestos por encabezados, que forman la cadena de datos que se utiliza para verificar criptográficamente el estado de la cadena de bloques; por cuerpos, que contienen la lista de transacciones ordenadas incluidas en cada bloque, y por recibos de transacciones, que contienen metadatos relacionados con la ejecución de transacciones, incluidos los registros de estas.
    b. *World State*: cada encabezado de bloque hace referencia a un estado *World State* a través de un hash. Este estado es un mapeo desde direcciones a cuentas, de las que se tienen dos tipos: las cuentas de propiedad externa, que contienen un saldo de Ethereum, y las cuentas de contrato inteligente, que contienen código ejecutable y almacenamiento.
4) Red *P2P*: se usan los protocolos de red de Ethereum para las comunicaciones entre clientes y para la sincronización.
5) API: empleadas para que los desarrolladores de aplicaciones interactúen con la blockchain. Besu proporciona la API JSON-RPC de la red principal de Ethereum y *EEA* a través de los protocolos HTTP (protocolo de transferencia de hipertexto) y WebSocket, así como la API GraphQL.
6) Monitorización: se lleva a cabo una monitorización del nodo y del rendimiento de la red.
7) Privacidad: mantiene las transacciones privadas entre las partes involucradas, de manera que terceras partes no pueden acceder al contenido de la transacción.
8) *Permissioning*: permite que únicamente determinados nodos y cuentas participen en la red mediante una habilitación.

[5] Un cliente de Ethereum es un software que ejecuta la cadena de bloques, comprueba las transacciones y crea nuevos bloques en la red.

[6] La *EEA* es una iniciativa internacional que busca intercambiar experiencias y crear estándares y arquitecturas de referencias basadas en Ethereum.

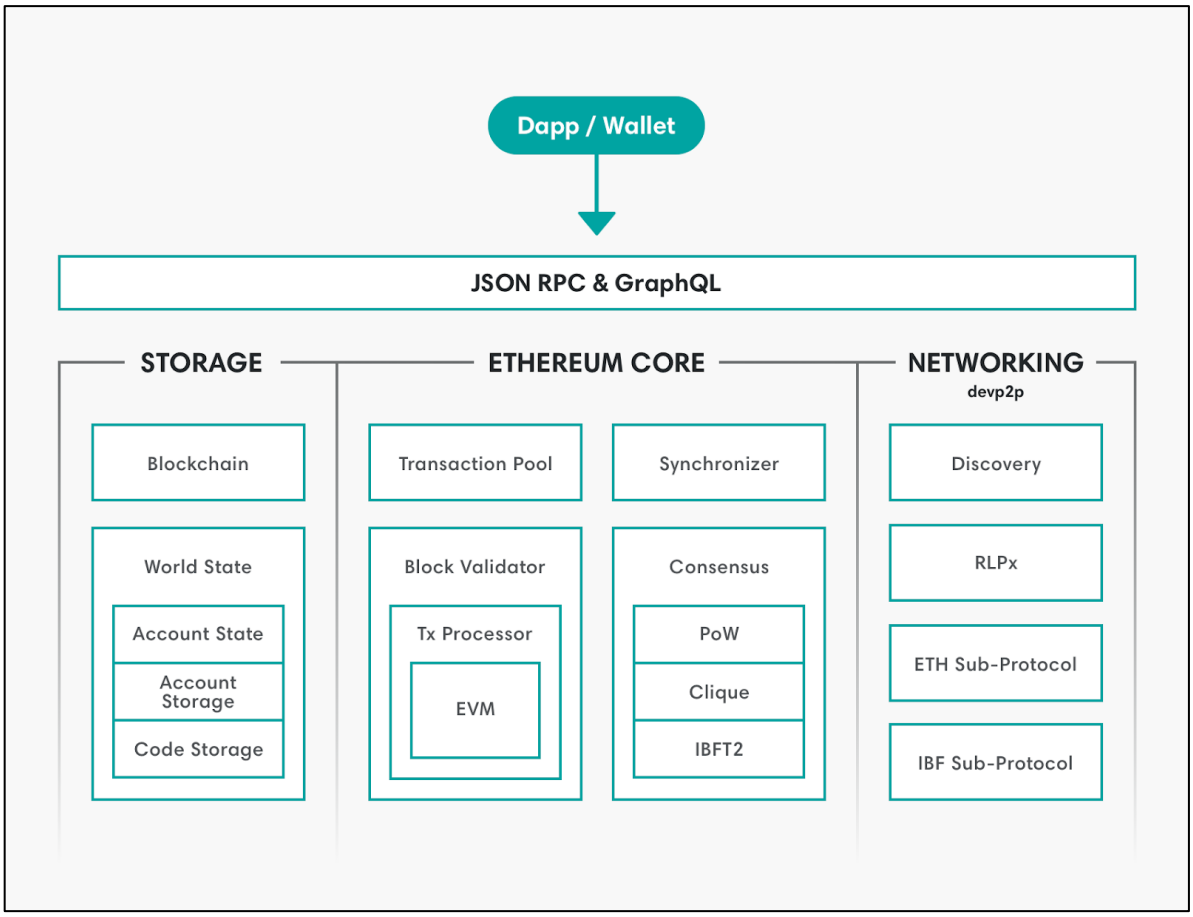

Figura 3-7 Arquitectura de Hyperledger Besu [35]

3.5 API REST

Una API REST permite establecer el «*conjunto de reglas que definen cómo pueden las aplicaciones o los dispositivos conectarse y comunicarse entre sí*», cumpliendo con «*los principios de diseño del estilo de arquitectura REST o transferencia de estado representacional*», que son los siguientes [37]:

1) Interfaz uniforme: las solicitudes para un mismo recurso han de ser idénticas, con independencia de su procedencia, y la interfaz debe asegurarse de que un mismo dato se corresponde con un único identificador uniforme de recursos (URI, por sus siglas en inglés).
2) Desacoplamiento del cliente-servidor: debe existir independencia completa entre las aplicaciones cliente y servidor; el cliente únicamente debe saber el URI, no pudiendo interactuar de otra manera con el servidor.
3) Sin estado: este tipo de interfaz es una API sin estado, lo que significa que cada solicitud ha de incluir la información necesaria para que sea procesada. Además, no se requiere sesión alguna del lado del servidor ni se almacenan datos relacionados con las solicitudes.
4) Capacidad de almacenamiento en memoria caché: los recursos deben poder almacenarse en la memoria caché tanto en el lado del cliente como en el del servidor siempre que sea posible. Las respuestas del servidor han de incluir información relativa a si está permitido este almacenamiento para el recurso entregado.
5) Arquitectura del sistema en capas: las llamadas y las respuestas pasan por diferentes capas, por lo que no se exige que las aplicaciones cliente y servidor se conecten directamente entre sí, pudiendo existir distintos intermediarios en la comunicación, de manera que ni el

cliente ni el servidor puedan reconocer si se comunican con la aplicación final o con un intermediario.

6) Código bajo demanda (opcional): este tipo de interfaz envían normalmente recursos estáticos; sin embargo, las respuestas también pueden contener código, que solo debe ejecutarse bajo demanda.

En una API REST, cuando el cliente o usuario desea acceder a determinada información desde la web, este ha de enviar una solicitud; con ella se pone en contacto con el servidor, que lleva a cabo la autenticación del cliente y confirma que este tiene derecho a acceder a ella. El servidor recibe y procesa la solicitud, proporcionando una respuesta a través HTTP, en formato JSON o XML, al cliente con la información relativa al procesamiento de la solicitud, es decir, con indicación de si se ha efectuado o no de forma correcta y, en su caso, con aquella otra que haya solicitado [38]:

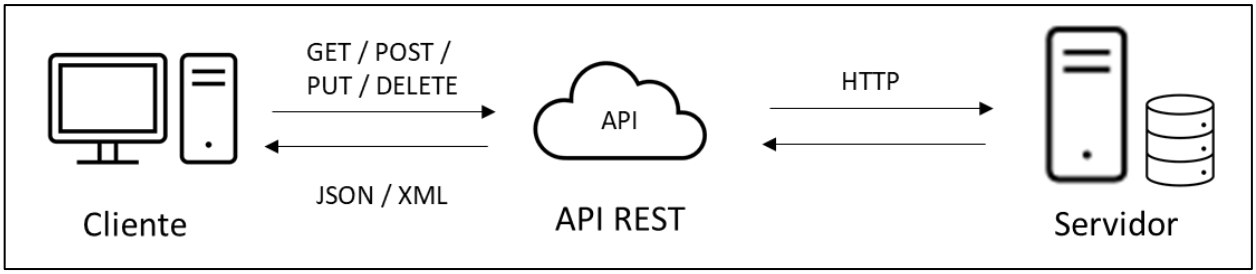

Figura 3-8 Funcionamiento de la API REST

Las solicitudes de los clientes han de contener, esencialmente, los elementos que a continuación se relacionan[7] [38]:

1) Localizador de recursos uniforme (URL, por sus siglas en inglés). El servidor identifica un recurso a través de un URL, pues especifica con claridad y precisión su ruta, mostrando lo que solicita el cliente.
2) Métodos. Un método HTTP informa al servidor lo que debe hacer con el recurso. Los métodos que se emplean son, principalmente, los siguientes:
    a. GET: el cliente accede al recurso solicitado.
    b. POST: el cliente envía datos al servidor.
    c. PUT: el cliente actualiza un recurso existente.
    d. DELETE[8]: el cliente elimina un recurso.
3) Encabezados de HTTP. Los encabezados son los metadatos que se intercambian el cliente y el servidor, y pueden contener:
    a. Datos, para que los métodos funcionen correctamente.
    b. Parámetros, que facilitan al servidor detalles sobre la solicitud. Estos pueden ser de ruta, que especifican detalles del URL; de consulta, mediante los que se solicita más información acerca del recurso, y de *cookie*, que autentican al cliente con mayor rapidez.

Por su parte, la respuesta del servidor de la API REST cuenta con [38]:

1) Línea de estado. Se comunica si la solicitud se ha procesado correctamente o se ha producido un error.
2) Cuerpo. Contiene la representación del recurso. El servidor selecciona el formato adecuado de representación en función de los encabezados de la solicitud.

[7] Otro componente reseñable –y utilizado en este documento– es el cuerpo de la petición HTTP. En él se incluyen los datos de la propia petición.

[8] En lo que respecta a la cadena de custodia, en la que se ha de dejar constancia de toda acción que se lleve a cabo sobre una evidencia, no procede emplear este método, teniendo en cuenta, además, la imposibilidad de eliminar datos de la blockchain.

3) Encabezados. Contienen los metadatos de la respuesta, y proporcionan más información acerca de esta, incluyendo datos relativos al servidor, la codificación, la fecha y el tipo de contenido.

4 BLOCKCHAIN COMO MODELO DE CONFIANZA

4.1 Introducción

El nacimiento de la tecnología Blockchain constituye uno de los cambios más disruptivos que ha tenido lugar en los últimos años en el ámbito de las tecnologías de la información y las comunicaciones, principalmente por su repercusión en la relación y en la confianza entre personas. Gracias a ella, la confianza en un tercero no es necesaria, ya que se tendrá la seguridad de que el registro en la blockchain será legítimo y de que no se modificará.

Esto ha traído consigo que ciertos organismos, como la Unión Europea, apuesten por modelos basados en Blockchain y contratos inteligentes, y confíen en que aspectos tan importantes y críticos como la identidad de una persona dependan de la seguridad de esta tecnología. De esta manera, tendría lugar una digitalización y automatización fiable de los procesos y documentos.

En la cadena de custodia, la gestión tradicional depende, en última instancia, del buen hacer y de la buena fe de la persona que la lleva a cabo, por lo que, intencionadamente o no, pueden cometerse errores que tengan una gran repercusión jurídica. La tecnología Blockchain, y en particular los contratos inteligentes, permiten que se tenga una fiabilidad absoluta, pues son programas informáticos que se ejecutan sin la intervención de terceros cumpliendo las condiciones que en ellos se establezcan, dejando constancia de toda actuación y evitando que se puedan alterar malintencionadamente [39].

4.2 *EBSI*

Un claro ejemplo de lo anterior es el ya mencionado proyecto *EBSI*, una iniciativa conjunta de la Comisión Europea y de la *European Blockchain Partnership*[9] (*EBP*, por sus siglas en inglés) que tiene como objetivo aprovechar la tecnología Blockchain para acelerar la creación de servicios transfronterizos entre administraciones públicas y sus ecosistemas, para verificar la información y hacer que estos gocen de una mayor confianza. Se produce el cambio del modelo tradicional de compartición de información, que es centralizado, por uno de naturaleza distribuida, en el que la cadena de bloques, a través del algoritmo de consenso *PoA*, actúa como una fuente de verdad que facilita la verificación de las entidades involucradas en la transacción y la autenticidad de la información, sin requerir el acceso a su origen en tiempo real [40].

[9] La *EBP* es una iniciativa para desarrollar una estrategia en la Unión Europea sobre Blockchain y construir una infraestructura blockchain para los servicios públicos.

Este protocolo de consenso se basa en la participación como medida de selección y confianza –al igual que sucede en Ethereum–, y en la identidad y la reputación de los nodos. Estos habrán de identificarse voluntariamente y contarán con una reputación. De esta manera, se le otorgará a la red un alto nivel de fiabilidad y de transparencia, ya que en caso de que tenga lugar una acción que atente contra estas cuestiones y afecte al funcionamiento de la blockchain, la responsabilidad recaerá sobre el nodo, y su reputación se verá mermada. En este sentido, a modo de incentivo, los nodos validadores tratarán de que su identidad y su reputación no se vean afectadas, por lo que velarán por el buen funcionamiento de la red [41].

Técnicamente, esta iniciativa consiste en una red blockchain con nodos distribuidos a lo largo de la Unión Europea[10] que prestan apoyo a diversas aplicaciones, centrándose en diferentes casos de uso[11]. Cada miembro de la red aloja un nodo a nivel nacional que puede crear y llevar a cabo transacciones que actualicen el libro mayor de la cadena de bloques, manteniendo, también, una copia de este [40].

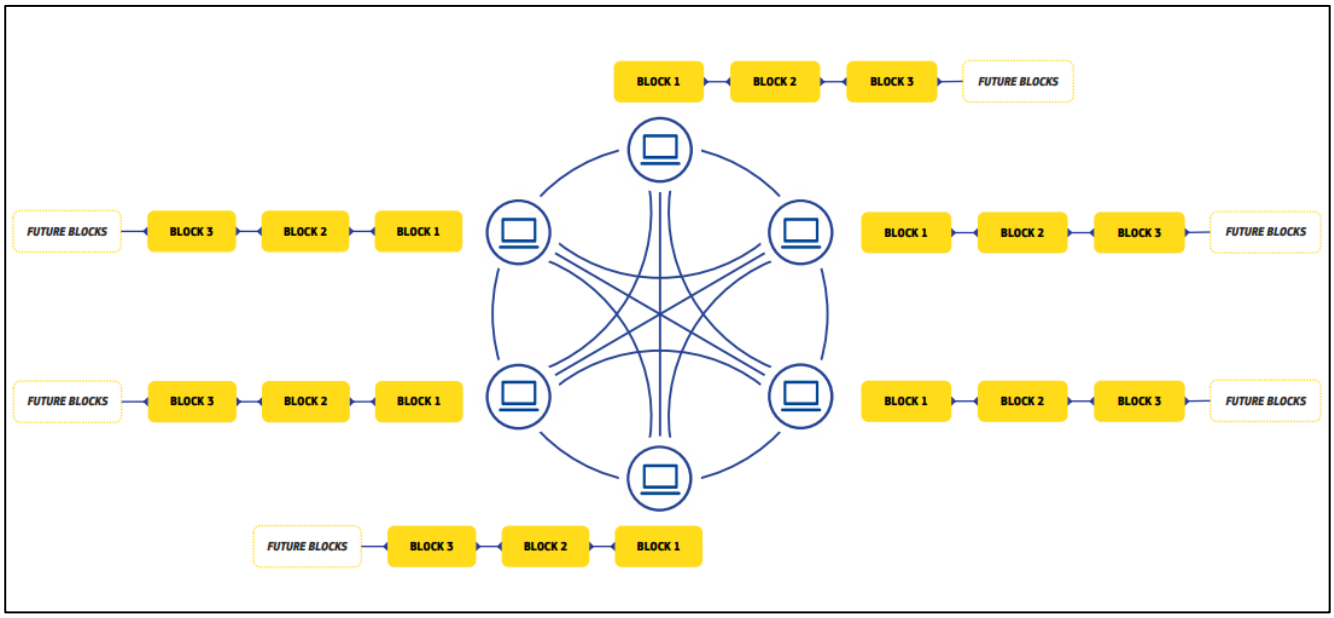

Figura 4-1 *EBSI* [40]

Los nodos a los que se ha hecho referencia se componen de tres capas: infraestructura, cadena y almacenamiento, y núcleo de servicios. Sus funciones son las siguientes [40]:

1) Capa de infraestructura: proporciona capacidades genéricas y conectividad a la red.
2) Capa de cadena y almacenamiento: incluye tanto la cadena de bloques como los protocolos de almacenamiento *off-chain* definidos y aprobados por la *EBP*.
3) Núcleo de servicios: son un conjunto de API que permiten que terceros desarrollen aplicaciones y garanticen el cumplimiento de los principios rectores definidos y aprobados por la *EBP*.

[10] España cuenta con tres nodos pilotos: uno en la Secretaría General de Administración Digital, otro en la Fábrica Nacional de Moneda y Timbre, y un último en RedIRIS [52].

[11] *EBSI* apoya la creación de servicios transfronterizos para que los ciudadanos, por ejemplo, gestionen su propia identidad, credenciales educativas y documentos de registro.

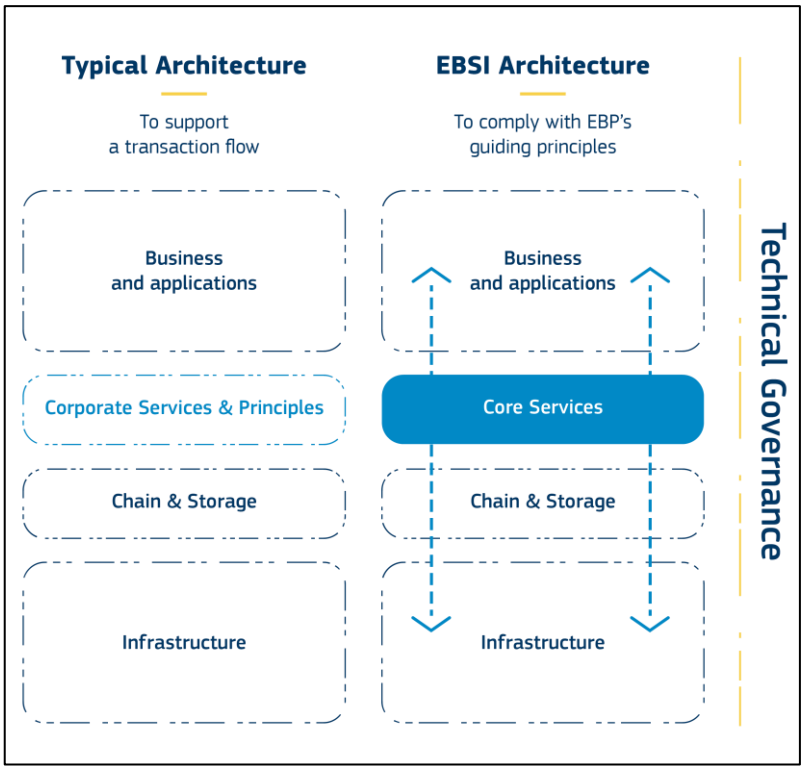

Figura 4-2 Capas de los nodos *de EBSI* [40]

Particularmente, *EBSI* incluye la red Ethereum Enterprise, a la que se accede a través del cliente Besu de Hyperledger y, además, cuenta también con Hyperledger Fabric. Como se ha mencionado en el capítulo anterior, ambos protocolos se ejecutan sobre el algoritmo de consenso de *PoA*, en el que cada nodo de la Comisión y de los Estados miembro cuenta con validadores, salvo en Fabric, que es opcional en el caso de los segundos, pudiendo solicitar tenerlos.

4.3 *eIDAS* 2

Como ya se ha señalado, *EBSI* se trata de una red *peer-to-peer* de nodos interconectados, operados a nivel nacional por autoridades de Estados miembros de la Unión Europea de acuerdo con las políticas de la *EBP*. Está basada en estándares públicos y en un modelo de gobernanza transparente para el que la *EBP* ha definido cinco principios clave: bien público, gobernanza, armonización, código abierto y cumplimiento de la normativa (entre otros, en materia de protección de datos y de identidad digital) [42].

En particular, en el ámbito de la Unión Europea, y especialmente en lo que respecta a la identidad digital, se encuentra el Reglamento (UE) N. 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior, conocido como *eiDAS* (*IDentification, Authentication and trust Services*). El objetivo de este Reglamento es «*garantizar el correcto funcionamiento del mercado interior aspirando al mismo tiempo a un nivel de seguridad adecuado de los medios de identificación electrónica y los servicios de confianza*» [43].

En la actualidad, este Reglamento se halla en un proceso de modificación [44], motivado esencialmente por la relevancia que han adquirido la privacidad y la protección de datos en los últimos años, no lográndose acometer las necesidades de la sociedad en general y de los sectores público y privado en particular. Esta propuesta, conocida como *eiDAS 2*, cuenta con un principal elemento novedoso: el empleo de la tecnología Blockchain y de un sistema descentralizado con el que se pretenden crear las denominadas carteras de identidad soberana propia, basadas en aplicaciones y gestionadas a través de un dispositivo móvil, y que permiten a una persona «*acceder de forma sencilla*

y segura a diferentes servicios públicos y privados con un control total», es decir, esta recuperará la soberanía sobre sus datos. Las personas se identifican a través de una clave pública y otra privada, ambas almacenadas en la cadena de bloques.

Así, tanto una persona física como una persona jurídica gozarán de una identidad digital que estará asociada, respectivamente, a sus identidades, sus datos personales y sus nacionalidades [45], y que podrán gestionar por cuenta propia.

eiDAS 2 constituirá, pues, un claro caso de uso de la tecnología Blockchain en las Administraciones Públicas, quedando probadas su utilidad, su eficacia y su seguridad, y, además, estará amparada legalmente. Por tanto, podrá emplearse igualmente para la gestión de la cadena de custodia.

5 MODELO PROPUESTO

5.1 Elección de la blockchain

Si bien este documento no persigue desarrollar una red propia para el fin seleccionado, sino su uso, se hace necesario valorar cuál es la opción más adecuada para lograr este objetivo. En este sentido, se han de tener en cuenta las opciones existentes, entre las que cabe destacar Ethereum o Hyperledger, puesto que presentan diferencias considerables que permiten dirimir esta cuestión. Otras opciones, como Bitcoin, deben descartarse, ya que, además de que conlleva «*un esfuerzo computacional que establece graves problemas de escalabilidad y eficiencia energética*» [28], las posibilidades se verían considerablemente reducidas, al no proporcionar la misma flexibilidad que otras blockchains. Bitcoin dispone de rígidos y poco personalizables contratos inteligentes, programados en Bitcoin Script y enfocados a las transferencias de sus criptomonedas; básicamente permiten dejar constancia de una transacción e indican las condiciones de pago. En el caso de la cadena de custodia, únicamente permitiría reflejar el hash de un documento que haga alusión a una evidencia sin aportar ninguna información adicional.

Si se compara con Bitcoin, Ethereum se presenta como «*mejor alternativa tecnológica*» [28]. Su minado es más eficiente, y la reputación de las partes que intervienen [46], así como no estar limitado y la posibilidad de crear contratos inteligentes que se adapten a las necesidades del caso de estudio, hacen que su red sea idónea para que se implemente la cadena de custodia.

Por otro lado, se encuentra Hyperledger. En este caso, no es necesaria una criptomoneda nativa para incentivar la minería, cuyo coste es elevado, ni impulsar la ejecución de contratos inteligentes. Evitar el uso de criptomonedas reduce significativamente el riesgo y vectores de ataque, y la ausencia de minería implica que la plataforma pueda desplegarse con aproximadamente el mismo coste operacional que cualquier otro sistema distribuido [32]. Teniendo en cuenta esto, Hyperledger se presenta también como una alternativa para que pueda llevarse a cabo la implementación de la cadena de custodia.

Sin embargo, además de considerar todo lo anterior, conviene tener en cuenta lo expuesto en el Capítulo 4 –*Blockchain como modelo de confianza*–. En él se ha podido comprobar que *EBSI* puede resultar una opción interesante si se quiere implementar la cadena de custodia con las debidas garantías y el respaldo de la Unión Europea.

En este capítulo se propondrá un modelo de cadena de custodia basado en la tecnología Blockchain empleando *EBSI* como infraestructura de confianza al servicio de los Estados miembro de la Unión Europea. De esta manera, se tendrá una infraestructura «*común, compartida y abierta*» que proporcione un «*ecosistema seguro e interoperable*» que permita un tratamiento apropiado de las evidencias [47].

Para lograr el funcionamiento en fase de producción del modelo que se pretende instaurar se ha de contar con una arquitectura en la que se viera involucrada toda la Administración General del Estado (en particular, las Fuerzas y Cuerpos de Seguridad, a través de sus distintas unidades, los diferentes órganos judiciales y aquellos otros organismos o entidades que participaran de manera directa o indirecta en la cadena de custodia), así como las instituciones de la Unión Europea y del resto de Estados miembro. Este documento, que es académico, aborda el diseño de un modelo válido para el marco de una variedad de plataformas.

No obstante, una vez realizado el análisis, se recomienda su eventual despliegue en dicha arquitectura, si bien, en todo caso, conviene indicar que no existen impedimentos que impliquen evitar el uso de Ethereum o alguna solución *Blockchain-as-a-Service* (*BaaS*, por sus siglas en inglés).

Por todo ello, se ha obviado tanto el proceso de incorporación en *EBSI*[12] de la cadena de custodia como la interacción con terceras partes.

5.2 Arquitectura

La red está formada por diversos nodos físicos que se encuentran en los diferentes Estados miembro de la Unión Europea y que se corresponden a su vez con un nodo de la blockchain. Adicionalmente, se cuenta con una base de datos distribuida, que se sincroniza en todos estos nodos. En este sentido, las unidades que necesiten confeccionar la cadena de custodia de una evidencia en el marco de una investigación tendrán que efectuar transacciones dentro de la red, que permitirán actualizar la cadena de bloques y que se almacene una copia de esta también en los nodos.

No obstante, por cuestiones inherentes a la idiosincrasia de la Guardia Civil y a la operatividad de sus unidades, resulta indispensable que el contenido de esa base de datos –relativo a las investigaciones– sea replicado en una base de datos propia, de manera que sea posible su utilización posterior con fines de inteligencia.

Teniendo en cuenta lo anterior respecto a la información que se ha de almacenar, se tienen dos modalidades: en la cadena de bloques permanecerá únicamente aquella información pública e imprescindible, que resulte indiferente que sea conocida o sabida por todos los participantes de la red, y en la base de datos distribuida, a la que exclusivamente tendrán acceso los miembros de la Guardia Civil que realicen labores de policía judicial y que estén habilitados para ello, aquella información que, de acuerdo con la legislación vigente, o porque así lo disponga la autoridad judicial, sea sensible y no deba ser pública. En otros términos, en la cadena de bloques se almacenará el hash asociado a una evidencia y en la base de datos, la propia evidencia y su cadena de custodia[13].

[12] *EBSI* se creó para dar solución a determinados escenarios o casos de uso orientados a la ciudadanía, entre los que no se encuentra la cadena de custodia. No obstante, existen dos formas de incorporar un nuevo caso de uso en *EBSI*: bien a través del Programa de *Early Adopters*, con el que se puede construir y lanzar un proyecto piloto que ha de ser aprobado con posterioridad, bien a través de la Secretaría de Estado de Digitalización e Inteligencia Artificial del Ministerio de Asuntos Económicos y Transformación Digital. Esta segunda forma constituye el conducto que ha de seguir un órgano de la Administración si quiere proponer un caso de uso.

[13] Cuando se hace referencia a las evidencias, estas pueden ser digitales o físicas. Las primeras no suponen problema alguno en cuanto a su gestión en *EBSI*; sin embargo, en las segundas, esto resulta imposible, por lo que se deben digitalizar para que se puedan incluir en el sistema, sin perjuicio de la gestión física –tradicional– que se haga de ellas.

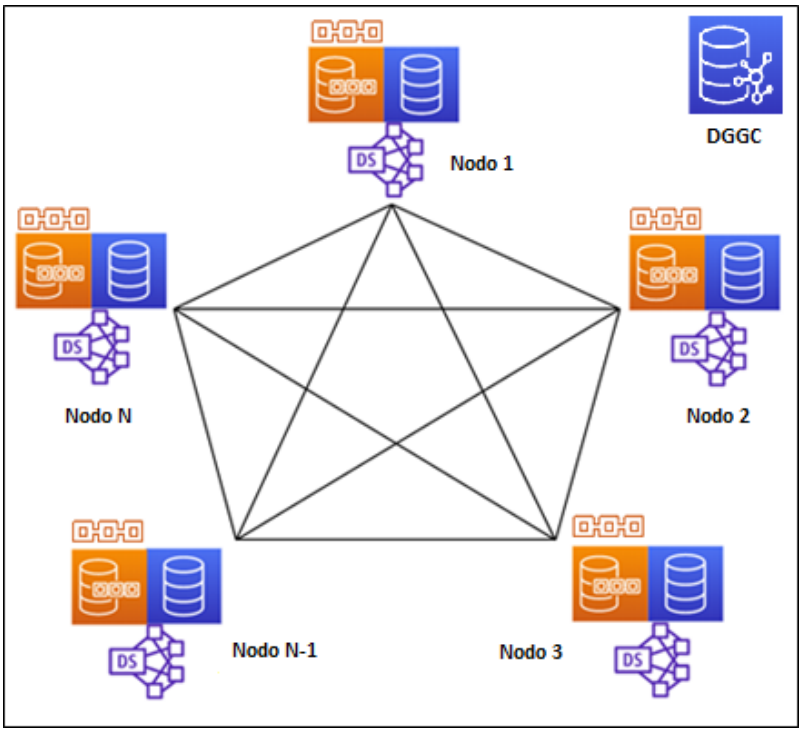

Figura 5-1 Arquitectura de implementación de la cadena de custodia

Al utilizar la infraestructura de *EBSI*, se asume implícitamente el empleo del algoritmo de consenso de *PoA*. Con él, los nodos del sistema seleccionarán a los nodos validadores en función de su identidad y de su reputación en la forma descrita en el capítulo anterior.

Los contratos inteligentes que se han de emplear deben asegurar que la información enviada a través de la API sea grabada correctamente y de manera confiable en la infraestructura.

5.3 Funcionamiento

Quienes ejerzan labores de policía judicial (cuestión que debe quedar convenientemente acreditada a través de una cartera digital o *wallet*) tienen acceso a una aplicación que interactúa con la cadena de bloques a través de una API. Esta interfaz solicita realizar una transacción al contrato inteligente, que queda reflejada en la blockchain. Estas acciones se efectúan en el núcleo de servicios de la infraestructura, que, como se ha mencionado con anterioridad, es la capa de *EBSI* que cuenta con las interfaces que permiten que terceros desarrollen aplicaciones y garanticen el cumplimiento de los principios rectores de la *EBP*.

En la capa de cadena y almacenamiento, en la que se incluyen tanto la cadena de bloques como los protocolos de almacenamiento *off-chain*, los contratos inteligentes controlan y permiten ejecutar las operaciones de forma confiable; de ellas también se deja constancia en la blockchain. Por otra parte, estos contratos se plasman igualmente en registros confiables pertenecientes a la Guardia Civil.

En la capa de infraestructura, en la que se proporcionan las capacidades genéricas y la conectividad a la red, la blockchain valida, autoriza y almacena las transacciones propuestas en la cadena de bloques.

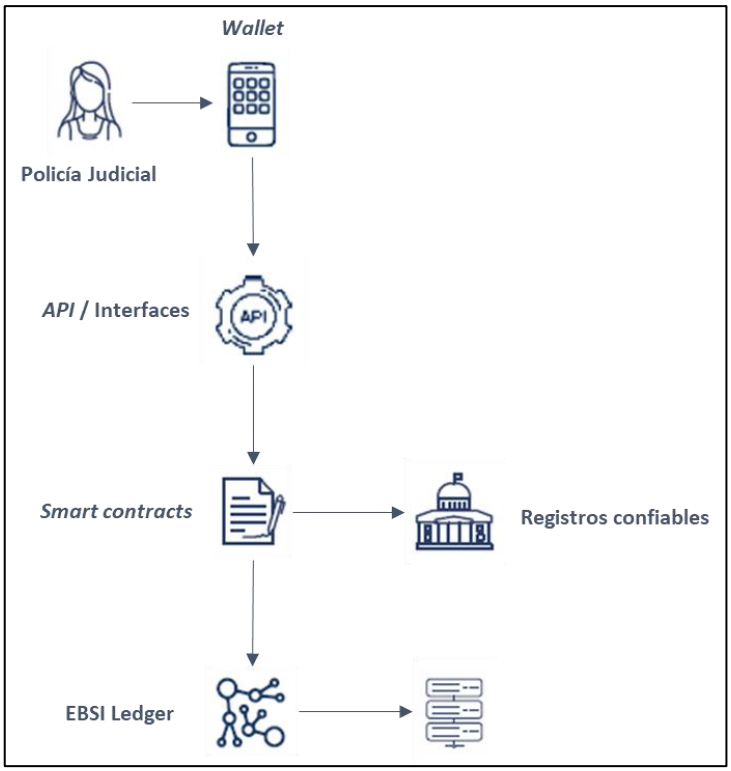

Figura 5-2 Funcionamiento de la infraestructura (1) [40]

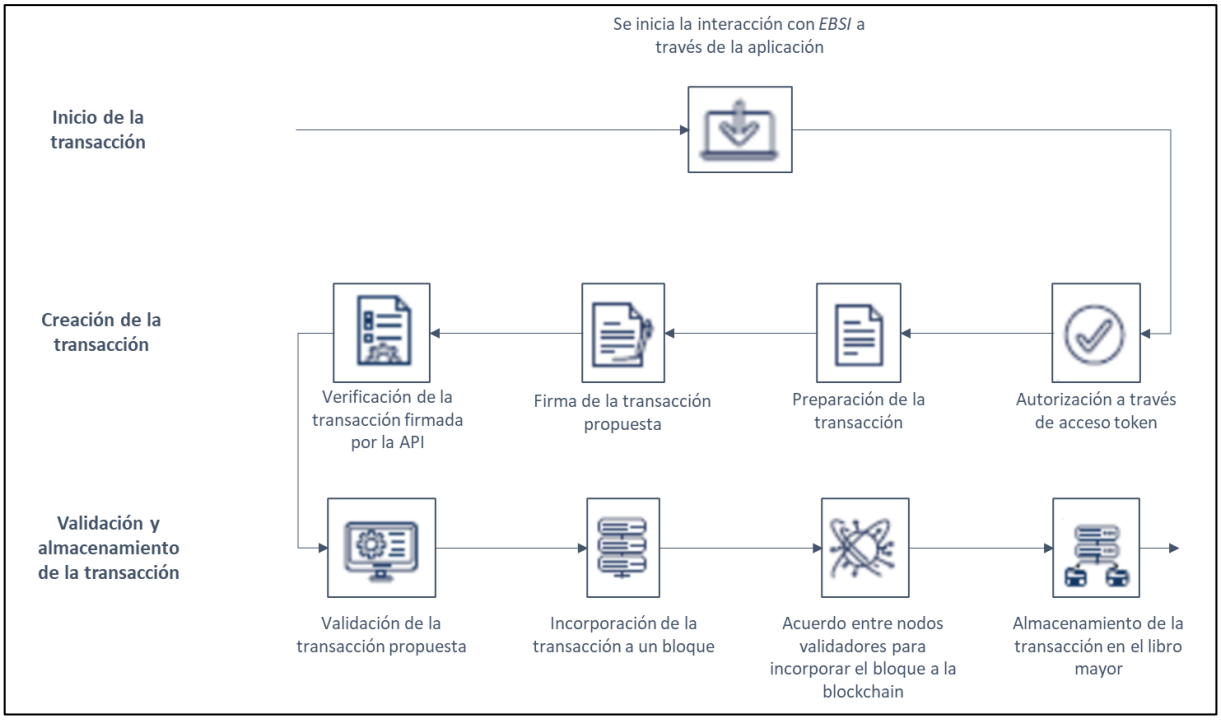

Figura 5-3 Funcionamiento de la infraestructura (2) [40]

En concreto, la transacción se inicia con la interacción del agente de la policía judicial con *EBSI* a través de una aplicación. Entre la aplicación y *EBSI* se encuentra una API, que permite que el agente se identifique con una *wallet*, o mediante el uso de credenciales, y autenticarse a través de un *token* de acceso. Una vez se haya autenticado, puede efectuar llamadas a la interfaz a través de la mencionada aplicación, es decir, puede solicitar realizar una transacción al contrato inteligente, para que esta se prepare y el usuario la firme, y sea verificada posteriormente por el contrato inteligente que existe tras la API.

La siguiente fase consiste en la validación y almacenamiento de la transacción. Para ello, es necesario que la transacción se asocie, en primer lugar, a un bloque candidato y, seguidamente, exista acuerdo entre los nodos validadores para que la incluyan en la blockchain y sea almacenada en el libro mayor.

5.4 Interfaz

A lo largo del presente documento, se ha tratado en diversas ocasiones el empleo de una API como modo de interacción entre aplicaciones y la blockchain. En el modelo propuesto, se utiliza una API REST, debido a la flexibilidad y ligereza que proporciona en la integración de aplicaciones.

Esta interfaz debe ser consecuente con las acciones –y al menos permitir materializarlas– que se llevan a cabo en el proceso de la cadena de custodia tradicional, y dar soporte técnico para su ejecución en el ámbito de la blockchain. Para definir estas acciones en el modelo, se han de tener en cuenta: la evidencia en cuestión, su cadena de custodia y sus registros o *records*[14], y la investigación en la que se enmarca, así como las personas que intervienen en el proceso[15]. Se tienen, por tanto, las siguientes figuras: el agente que realiza labores de policía judicial –que puede pertenecer a cualquier unidad que participe en la investigación–, la investigación, la evidencia, y la cadena de custodia y sus *records*. Así, un agente, por iniciativa propia o por orden de la autoridad judicial, puede iniciar una investigación en la que pueden hallarse una o más evidencias sobre las que se han de confeccionar las respectivas cadenas de custodia, es decir, cada evidencia tiene su propia cadena de custodia.

La estructura de los datos de las investigaciones, de las evidencias y de las cadenas de custodia y sus *records* presentan, respectivamente, la forma que a continuación se muestra:

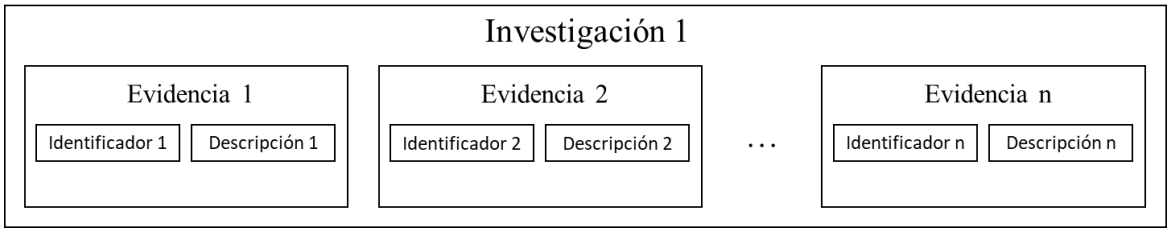

Figura 5-4 Investigaciones

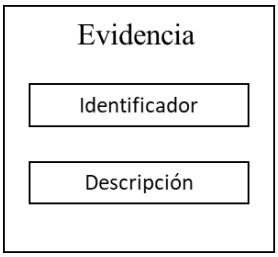

Figura 5-5 Información sobre evidencias

[14] Un *record* de la cadena de custodia, en consonancia con la Figura 2-1, es un registro que se realiza sobre la cadena de custodia. Dentro de estos se incluyen los datos relativos al agente interviniente y su unidad, la actuación efectuada y las observaciones, de forma que se actualiza la cadena de custodia cada vez que se realiza uno.

[15] En cuanto a las personas intervinientes en la cadena de custodia, cabe reseñar que, si bien la autoridad judicial es una figura importante en el proceso, en la práctica son los investigadores quienes realizan y registran todas las acciones que se llevan a cabo sobre una evidencia, ya sea *motu proprio*, porque así corresponda, o acatando las órdenes de la autoridad judicial. De igual manera ocurre con la defensa, quien debe solicitar tener acceso a la cadena de custodia durante la práctica de pruebas que tiene lugar durante el juicio.

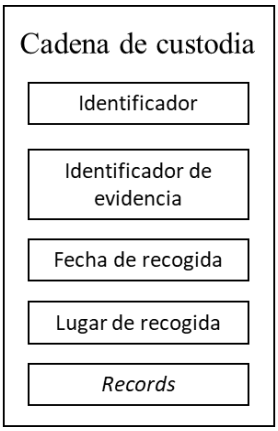

Figura 5-6 Cadena de custodia de una evidencia

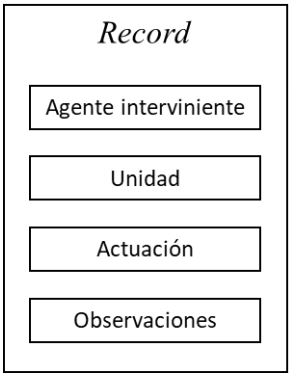

Figura 5-7 *Record* de la cadena de custodia de una evidencia

Para trasladar la realidad al caso de uso, se han de tener en cuenta todas las variables relacionadas con la gestión y el tratamiento de las evidencias:

1) La figura principal es la investigación, pues en ella se enmarcan todas las actuaciones que se realicen, las personas que intervengan y las evidencias que se hallen.
2) La investigación es llevada a cabo por una unidad de policía judicial, que está integrada por diversos agentes. Los integrantes de este tipo de unidades, siempre que resulte pertinente, pueden realizar cualquier actuación con una evidencia en el marco de la investigación.
3) Además de los agentes de policía judicial, se encuentran dos figuras de gran relevancia en las investigaciones: la autoridad judicial y, en caso de que el hecho delictivo se le haya imputado a alguien, la defensa.
4) Por otro lado, se hallan las figuras de la evidencia y de su cadena de custodia, junto con los *records* de esta última. Toda evidencia es objeto de distintas actuaciones, de las que se debe dejar constancia en su cadena de custodia a través de sus *records*.

Teniendo en cuenta lo anterior y las acciones que se pueden llevar a cabo, en la figura siguiente se muestran los casos de uso existentes en el modelo propuesto:

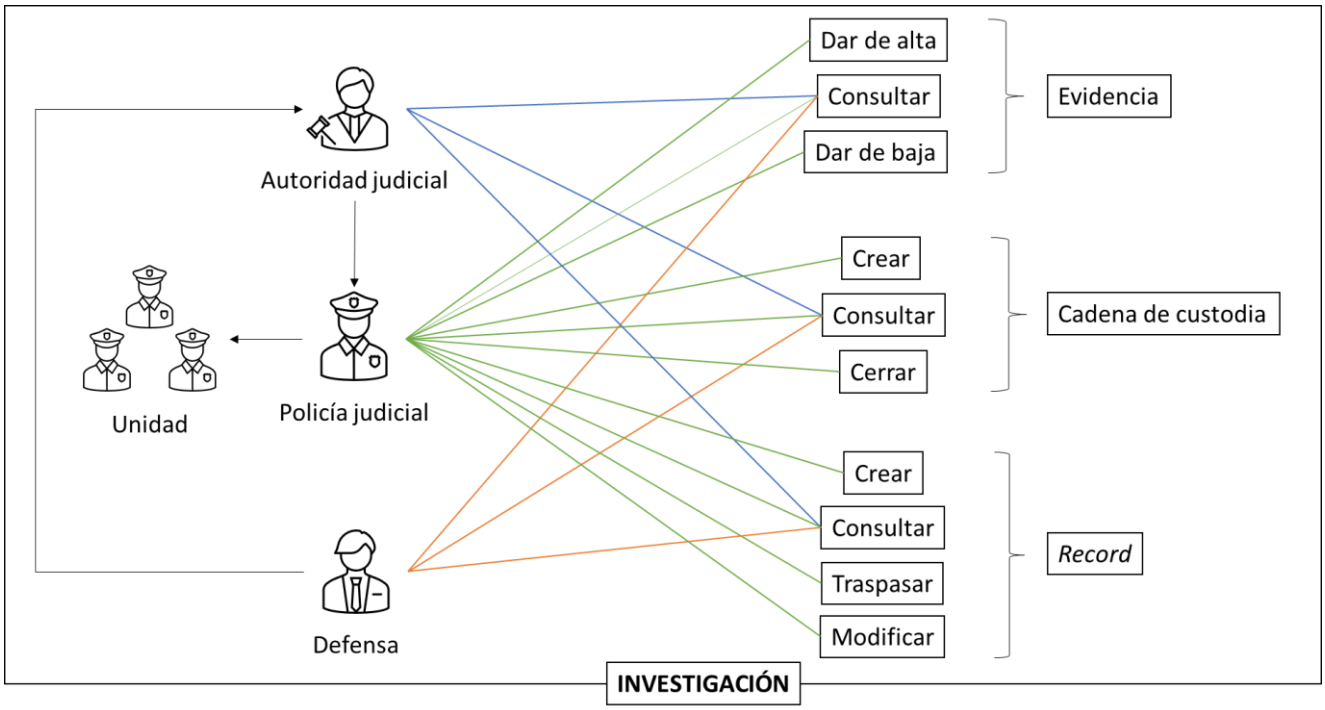

Figura 5-8 Casos de uso del modelo

En la figura puede observarse que, sin perjuicio de las consultas que pueden realizar tanto la autoridad judicial como, en su caso, la defensa sobre la evidencia y su cadena de custodia de acuerdo con la legislación vigente, un agente puede[16] dar de alta una evidencia, consultarla y darla de baja, y además crear su cadena de custodia, consultarla y cerrarla, así como crear, consultar y modificar los diferentes *records* de esta última, y traspasar una evidencia:

1) Respecto a la evidencia se pueden realizar las siguientes actuaciones:
    a. Dar de alta: permite registrar la evidencia en la blockchain, junto con la información pública (metadatos de la petición y el hash de la evidencia –digital o física digitalizada–), además de incluir la información privada (la evidencia en cuestión) en la base de datos distribuida.
    b. Consultar: hace posible obtener la información relativa a la evidencia, ya sea pública o privada.
    c. Dar de baja: posibilita anotar, en el registro, información complementaria de la evidencia que indique que esta se aparta de la investigación, con independencia de la causa.
2) En el caso de la cadena de custodia, las que a continuación se indican:
    a. Crear: permite establecer la cadena de custodia de una evidencia, mediante la que se incluye la información de las acciones realizadas sobre ella en la base de datos distribuida.
    b. Consultar: hace posible obtener la información incluida en la cadena de custodia.
    c. Cerrar: posibilitará dejar constancia de que se han realizado todas las acciones preceptivas sobre la evidencia, sin perjuicio de que, con posterioridad, pueda llevarse a cabo otra actuación a requerimiento de la autoridad judicial.
3) Por último, en relación con los *records*, podrán llevarse a cabo las siguientes acciones:
    a. Crear: incorpora, en la cadena de custodia, información acerca de las actuaciones concretas efectuadas sobre la evidencia, que es almacenada en la base de datos distribuida.

[16] En el *Anexo I: Casos de uso del modelo*, se describe el funcionamiento de los casos de uso del modelo.

b. Consultar: posibilita obtener información acerca de las actuaciones efectuadas sobre la evidencia.
c. Traspasar[17]: permite cambiar la unidad responsable de la evidencia, a fin de que esta realice, a través de sus integrantes, nuevas acciones sobre ella.
d. Modificar: permite subsanar cualquier error que hubiera podido tener lugar.

5.5 Diseño parcial del modelo

Para desarrollar la prueba de concepto, resulta imprescindible diseñar previamente el modelo. Este diseño –parcial–[18] cubre cuatro de los casos de uso del modelo[19][20]: dar de alta una evidencia y crear su cadena de custodia, y consultar tanto la evidencia como la cadena de custodia.

En primer lugar, se han de definir las características de la evidencia y de la cadena de custodia, las relaciones entre ambas y los métodos que se utilizarán, así como los *endpoints*.

Una vez se han definido, se procede a dar de alta la evidencia. Se inserta, así, un recurso denominado "evidence", mediante una petición POST, en cuyo *body* se incluyen tanto los metadatos relativos a la evidencia como la propia evidencia o, en caso de ser una evidencia física, una versión digitalizada de esta:

POST /v1/evidence

Para consultar la información de la evidencia, se utiliza el método GET y se introduce el identificador asignado a la evidencia mediante el método anterior:

GET /v1/evidence/{id}

El siguiente paso es crear la cadena de custodia. En este caso, la información necesaria, incluida en el *body*, es el identificador de la evidencia, la fecha y el lugar de recogida, el agente interviniente, la unidad, la actuación realizada y las observaciones. De este modo, se crea un recurso denominado "custody_chain", que está asociado a una evidencia, mediante una invocación con el método POST:

POST /v1/custody_chain/{id}/evidence

En último lugar, se puede realizar la consulta de la cadena de custodia indicando únicamente su número. El método empleado en este caso es GET:

GET /v1/custody_chain/{id}

5.6 Consideraciones respecto al modelo

En este capítulo se presenta una implementación parcial de la API REST, que muestra de forma somera y superficial las acciones que en última instancia realizan los agentes de la policía judicial al emplear el modelo. No se ha tenido en cuenta la interacción con la blockchain.

No obstante, en función del proceso de implantación de *EBSI* en las Administraciones Públicas, así como de su evolución –en términos tecnológicos–, y al no ser una infraestructura madura y consolidada, este aspecto es susceptible de un estudio pormenorizado que permita definir de forma más precisa estos extremos.

[17] Si bien se podría realizar el traspaso de la evidencia mediante el caso de uso de creación de un *record* desde un punto de vista teórico, resulta recomendable disponer de un caso de uso para tal fin, debido a que se requiere realizar diligencias específicas para llevar a cabo esta actuación.

[18] Para simplificar la prueba de concepto, ya que no influye en la verificación del modelo propuesto para que sea empleado por la policía judicial, la información relativa al *record* se incluye directamente en la cadena de custodia.

[19] Los cuatro casos de uso seleccionados suponen las actuaciones iniciales que se realizan sobre una evidencia en el momento en que es hallada.

[20] En el *Anexo I: Casos de uso del modelo*, se incluye el resto de los casos de uso.

Por otro lado, si bien el acceso a la base de datos distribuida se llevaría a cabo a través de la aplicación, otro aspecto que tampoco se ha considerado es la encriptación de la información, necesaria para evitar acceso no autorizado por parte de terceros y cuestión de interés en una implementación real.

6 PRUEBA DE CONCEPTO

6.1 Introducción

Con el fin de validar la propuesta realizada, se ha desarrollado una prueba de concepto con la que se implementa parcialmente el modelo, para verificar que, efectivamente, es susceptible de ser empleado por la policía judicial y, además, satisface los requisitos técnicos y legales de la gestión de la cadena de custodia.

Para ello, se simula la infraestructura de *EBSI*[21] y únicamente se crea la API REST[22], con la que se interacciona y que cubre las necesidades de la policía judicial en lo que respecta a la cadena de custodia. La interfaz se establece empleando el *framework* de *open source* Flask [48] –por su versatilidad–, y el lenguaje de programación Python [49] –por su flexibilidad y básica sintaxis–. Asimismo, se ha utilizado la plataforma de desarrollo de API Postman [50] para llevar a cabo la prueba de concepto.

6.2 Prueba de concepto

En este apartado, se detalla un ejemplo, a modo de prueba de concepto, en el que se muestra cómo se crea una evidencia, se confecciona su cadena de custodia y, posteriormente, se realiza una consulta sobre ambas.

6.2.1 Creación de la evidencia y consulta de la evidencia

Para la creación de la evidencia se ha empleado el método POST, y se ha añadido la descripción "prueba.doc"[23]. El servidor le ha asignado el identificador "0" de forma automática. Si se continúa dando de alta nuevas evidencias, el servidor asigna, correlativamente, un nuevo identificador. Así, la siguiente evidencia, tendría el identificador "1".

En caso de realizarse una consulta sobre la evidencia con identificador "0", el sistema debería proporcionar la descripción indicada anteriormente.

[21] En la creación de la API REST, se considerará que el modelo propuesto es un caso de uso de *EBSI*, por lo que todo aquello que subyace tras la interfaz funciona en la forma expuesta en el presente documento. Se tiene, así, un escenario ideal de funcionamiento para el modelo.

[22] Como se ha mencionado con anterioridad, las API forman parte de la infraestructura de *EBSI*, concretamente del núcleo de servicios, y son las que permiten a terceros que desarrollen sus aplicaciones, adaptadas a sus necesidades.

[23] En un escenario real, debería incluirse el propio archivo con denominación "prueba.doc" en el *body* del POST.

6.2.2 Creación de la cadena de custodia

Para crear la cadena de custodia de la evidencia con identificador "0", se ha de proporcionar toda la información que ha de incluir la cadena de custodia (identificador de la evidencia, fecha y lugar de recogida, agente actuante y unidad a la que pertenece, actuación realizada y observaciones). Al realizar la petición con dicha información, se incluye esta y, además, se asigna automáticamente otro identificador a la cadena de custodia –en este caso, "0"–. Se observa, también, que la cadena de custodia y la evidencia se encuentran relacionadas.

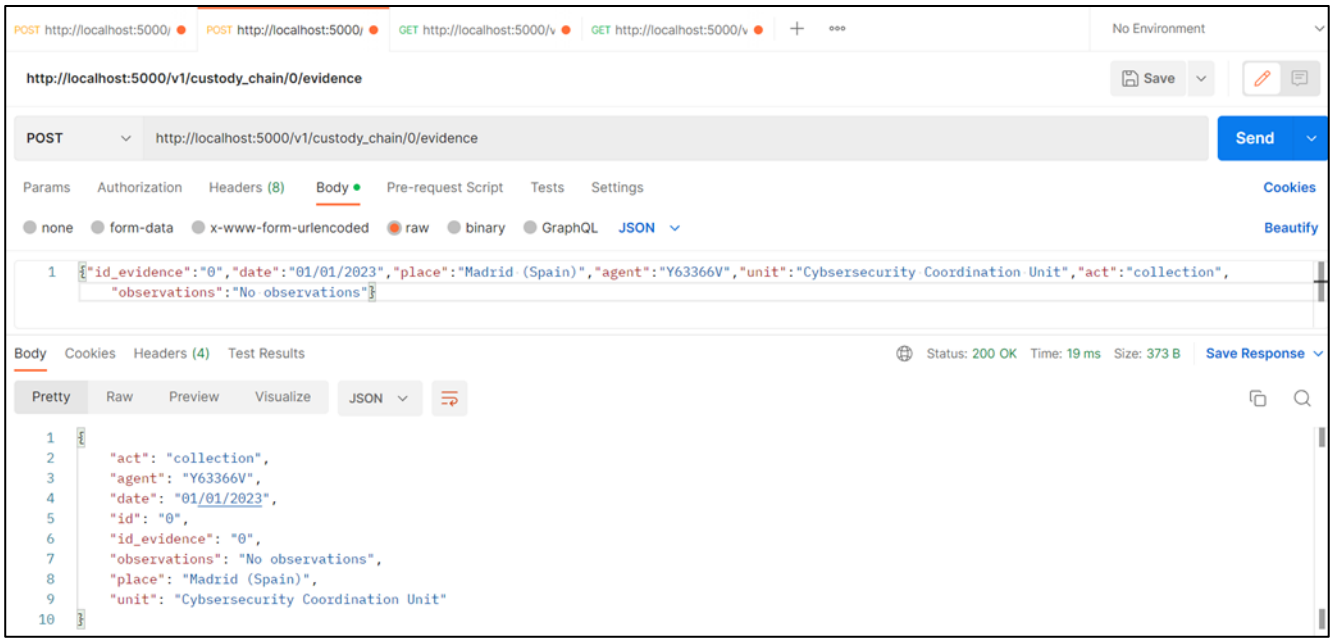

Figura 6-1 Creación de la cadena de custodia (1)

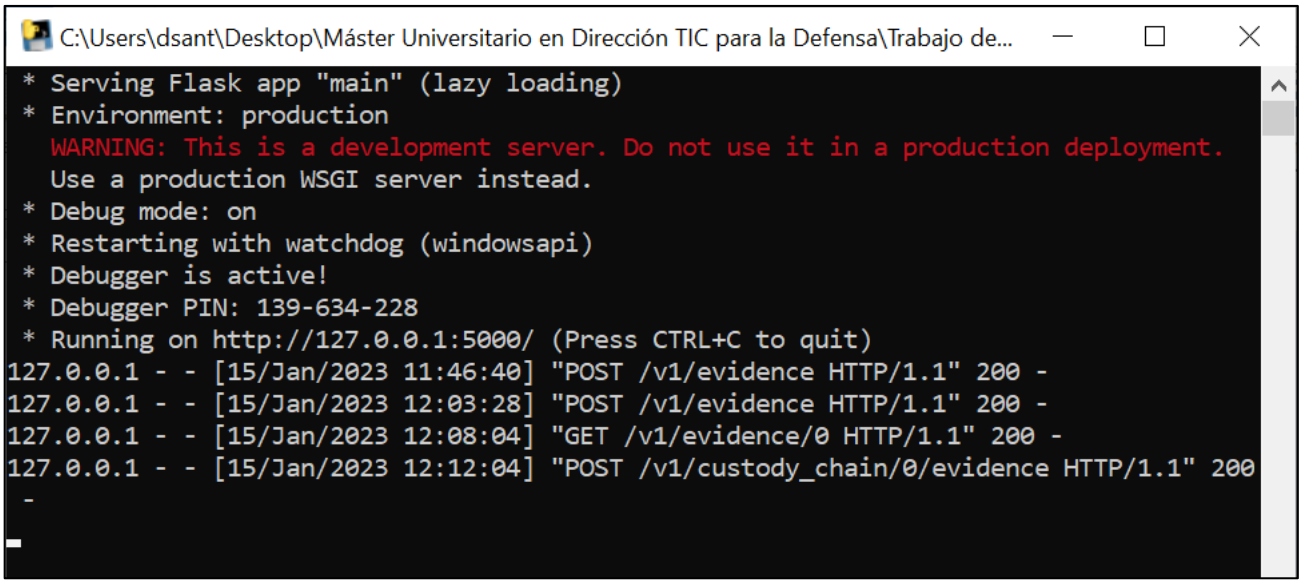

Figura 6-2 Creación de la cadena de custodia (2)

6.2.3 Consulta de la cadena de custodia

Para consultar la información que contiene la cadena de custodia de la evidencia "0", se debe introducir su identificador. De esta manera, introduciendo el identificador "0", se obtiene la información de la cadena de custodia de la evidencia con identificador "0", así como la información de esta última.

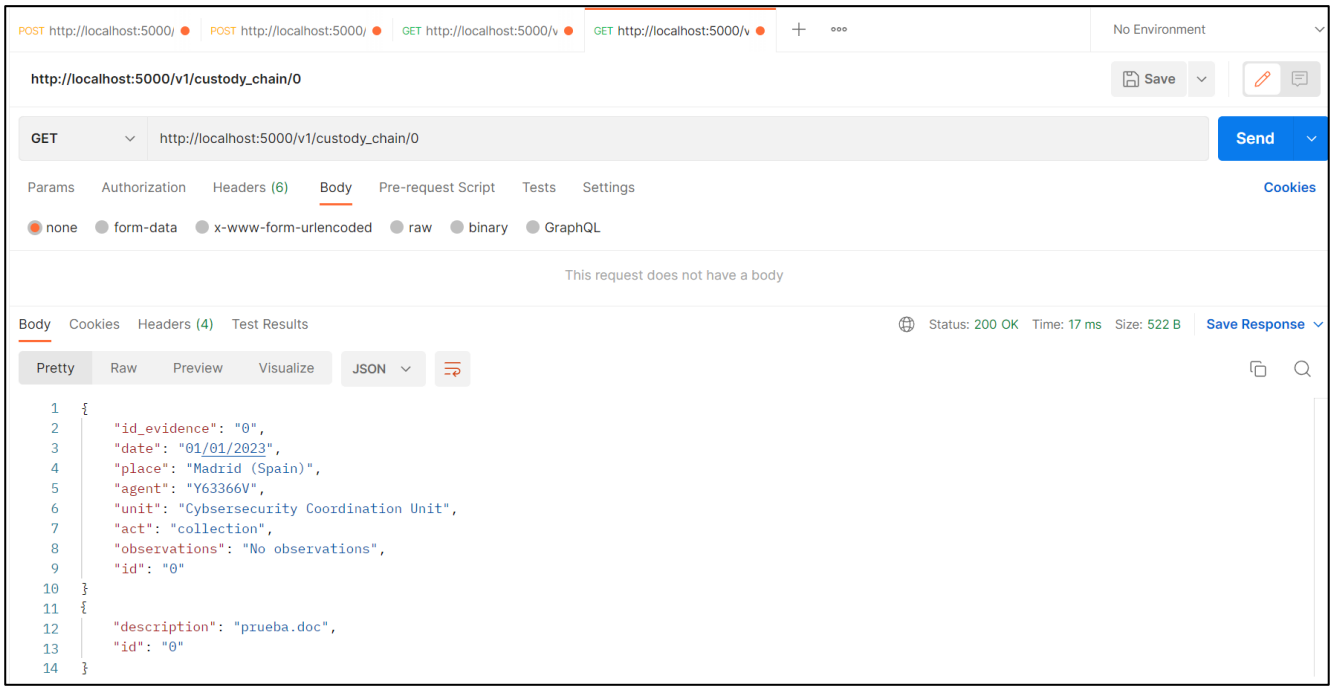

Figura 6-3 Consulta de la cadena de custodia (1)

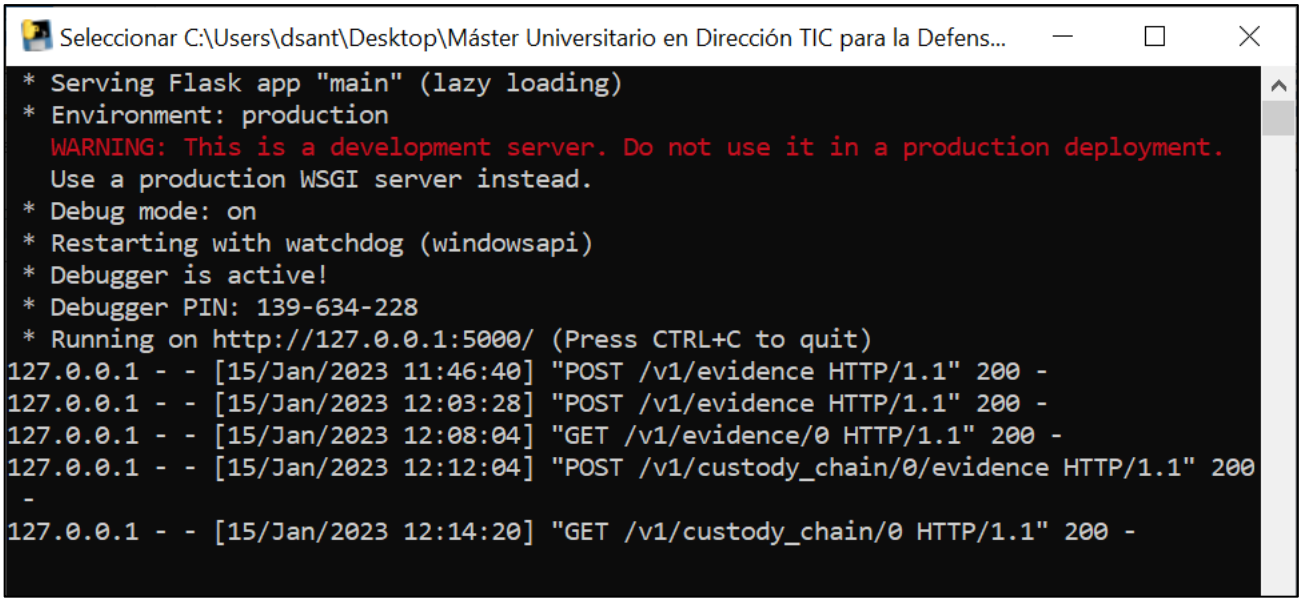

Figura 6-4 Consulta de la cadena de custodia (2)

7 CONCLUSIONES Y LÍNEAS FUTURAS

7.1 Conclusiones

La eficacia procesal constituye un aspecto fundamental en la jurisdicción penal. Esta afirmación implica que aspectos como la cadena de custodia adquieran una importancia significativa para asegurar el normal funcionamiento de esta jurisdicción, sobre todo en lo que respecta a la garantía de los derechos fundamentales y libertades públicas de las personas que se hallan implicadas en el proceso.

En la actualidad, la cadena de custodia se lleva a cabo de forma elemental y básica desde un punto de vista tecnológico. En esencia, se emplean simultáneamente la cadena de custodia física –en formato papel– y la cadena de custodia digital –en documento electrónico, pero con los extremos de la cadena de custodia física–, dependiendo en última instancia del buen hacer y de la buena fe de las personas que participan en su elaboración o gestión.

La constante evolución de las tecnologías de la información y las comunicaciones, así como la digitalización de la sociedad y de la Administración Pública, han creado el ambiente y la situación propicios para que puedan plantearse nuevos escenarios para las figuras legales tradicionales, como la cadena de custodia.

Para ello, las diferentes formas de implementación de la cadena de custodia mediante tecnología Blockchain hacen que sea necesario realizar un profundo estudio que dirima cuáles son las óptimas. Así, a través del análisis de la tecnología efectuado en este documento, y sobre todo teniendo en cuenta el respaldo de instancias europeas, se ha optado por emplear la infraestructura *EBSI* en el modelo propuesto. Esto ofrece al mundo de la investigación y a la cadena de custodia un nuevo paradigma, caracterizado por la descentralización, la escalabilidad y la confianza, así como por el estricto cumplimiento de las normas europeas.

Asimismo, *EBSI* posibilita que cada usuario que interaccione con la red esté debidamente identificado y autenticado, y asegura la trazabilidad y el registro de acciones sobre las evidencias, su integridad, su unicidad y su disponibilidad, lo que garantiza una gestión adecuada de la cadena custodia a través de una única aplicación. De esta manera, se logra una mayor eficiencia y seguridad, además de que la información esté validada y sea inmutable, es decir, que no resulte posible su alteración o supresión tanto legítima como ilegítimamente.

Otra cuestión importante es la redundancia, pues, gracias a este sistema distribuido, se asegura que la información esté duplicada en cada nodo, haciéndola resistente a fallos y ciberataques. Asimismo, en caso de que el sistema no funcione correctamente o se produzca su desconexión por cualquier motivo relacionado con alguno de los nodos de la red, este puede continuar operando sin dificultad alguna, lo que le hace gozar de una mayor seguridad frente a ataques.

La simplicidad y ligereza de REST, así como la flexibilidad que proporciona en la integración de aplicaciones, ha hecho que se opte por este tipo de API en el modelo propuesto. Esta interfaz se convierte en un elemento clave, ya que permite realizar sobre una evidencia, a través de los métodos diseñados, toda acción que se ha de llevar a cabo en la cadena de custodia tradicional.

Por otro lado, la cadena de custodia, implementada mediante Blockchain, facilita al investigador la gestión de las evidencias, evitando los errores y accesos no autorizados que deriven en la comisión de ilícitos penales o en la vulneración de derechos fundamentales, sin perjuicio de la responsabilidad disciplinaria en que pudieren incurrir.

Por todo ello, y gracias a este modelo, se facilita la labor diaria de los investigadores, que pueden centrar su esfuerzo en los aspectos formales y operativos de la investigación en lugar de tener una constante preocupación por las cuestiones burocráticas de la cadena de custodia. Además, la seguridad (confidencialidad, integridad y disponibilidad), característica de trascendental importancia en lo que respecta a la información, así como el cumplimiento de la legislación vigente europea y estatal, se garantizarán en todo momento.

7.2 Líneas de investigación futuras

El modelo propuesto es, en esencia, una aproximación de lo que es el escenario real de la cadena de custodia. Por ello, se plantean las siguientes líneas de investigación futuras:

- Implementar completamente el modelo más allá de la prueba de concepto desarrollada, de manera que sea capaz de proporcionar respuesta a todas las necesidades de la cadena de custodia. La prueba realizada en el Capítulo 6 –*Prueba de concepto*–, si bien comprueba la funcionalidad del modelo, es limitada y solo materializa una parte de él. Por ello, se hace necesario ampliarlo a la totalidad de casos de uso expuestos.
- Estudiar la posibilidad de que se incorporen y empleen oráculos en el modelo, a modo de nexo entre los datos *off-chain* y *on-chain* de las evidencias. Los oráculos consultarán otras interfaces de confianza que contengan información sobre las evidencias y la transmitirán a los contratos inteligentes, de modo que esta se incorpore automáticamente en la cadena de custodia.
- Presentar este modelo como caso de uso en *EBSI*. Al ser una iniciativa de trascendencia estatal, en lo que respecta a las Fuerzas y Cuerpos de Seguridad, y que debe contar con la aprobación del Ministerio del Interior [51], el canal para llevar a cabo la presentación del caso de uso es la Secretaría de Estado de Digitalización e Inteligencia Artificial.
- Extender el uso de este modelo al resto de Fuerzas y Cuerpos de Seguridad y *Law Enforcement Agencies* (LEA, por sus siglas en inglés) de la Unión Europea, de modo que se presente como un ejemplo de cooperación policial y judicial internacional. En general, la delincuencia –y, en particular, la ciberdelincuencia– no entiende de competencia territorial en España, según se dispone en la Ley Orgánica 2/1986, de 13 de marzo, de Fuerzas y Cuerpos de Seguridad[24] [3]. Por este motivo, y a fin de que se facilite la colaboración entre las Fuerzas y Cuerpos de Seguridad y LEA de la Unión Europea, y la eficacia procesal sea mayor, el modelo propuesto habría de adaptarse a esta circunstancia, ya que en determinadas situaciones la evidencia debe ser tratada por diferentes cuerpos policiales.

[24] De acuerdo con la Ley Orgánica 2/1986, de 13 de marzo, las funciones que tienen encomendadas las Fuerzas y Cuerpos de Seguridad del Estado han de ser ejercidas con arreglo a la siguiente distribución territorial:

- Corresponde al Cuerpo Nacional de Policía ejercitar dichas funciones en las capitales de provincia y en los términos municipales y núcleos urbanos que el Gobierno determine.
- La Guardia Civil las ejercerá en el resto del territorio nacional y su mar territorial.

8 BIBLIOGRAFÍA

[1] Cortes Generales, *Constitución Española,* «BOE» núm. 311, 1978.

[2] Ministerio de Asuntos Económicos y Transformación Digital, *Plan de Digitalización de las Administraciones Públicas,* 2021.

[3] Jefatura del Estado, *Ley Orgánica 2/1986, de 13 de marzo, de Fuerzas y Cuerpos de Seguridad,* 1986.

[4] Ministerio de Gracia y Justicia, *Real Decreto de 14 de septiembre de 1882 por el que se aprueba la Ley de Enjuiciamiento Criminal,* 1882.

[5] Tribunal Supremo, *Sentencia del Tribunal Supremo 208/2014 (Sala de lo Penal), de 10 marzo de 2014 (Recurso 836/2013),* 2014.

[6] Naciones Unidas, *Protocolo de Estambul. Manual para la investigación y documentación eficaces de la tortura y otros tratos o penas crueles, humanos y degradantes.*

[7] Consejo de la Unión Europea, *Recomendación del Consejo, de 30 de marzo de 2004, sobre directrices para la toma de muestras de drogas incautadas,* 2004.

[8] Jefatura del Estado, *Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil,* 2000.

[9] Tribunal Supremo, *Sentencia del Tribunal Supremo 2109/2019 (Sala de lo Penal), de 20 de junio de 2019 (Recurso 998/2018),* 2019.

[10] Tribunal Supremo, *Sentencia del Tribunal Supremo 706/2020 (Sala de lo Social), de 22 de julio de 2020 (Recurso 239/2018),* 2020.

[11] Forkast, «Forkast News» [En línea]. Disponible en: https://forkast.news/headlines/china-court-blockchain-cross-examination/.

[12] Forkast, «Forkast News» [En línea]. Disponible en: https://forkast.news/china-has-seen-blockchains-future-and-it-doesnt-include-cryptocurrencies/.

[13] Gobierno de España, *Plan de Recuperación, Transformación y Resiliencia,* 2021.

[14] Departamento de Seguridad Nacional, *Estrategia de Seguridad Nacional,* 2021.

[15] Departamento de Seguridad Nacional, *Estrategia Nacional de Ciberseguridad,* 2019.

[16] Ministerio del Interior, *Instrucción 1/2021, del Secretario de Estado de Seguridad, por la que se aprueba el Plan Estratégico contra la Cibercriminalidad*, 2021.

[17] *M. Fenwick, W.A. Kaal, E.P.M. Vermeulen, Legal Education in the blockchain revolution, J. Ent. & Tech. L., 2017.*

[18] *S. Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, 2009.*

[19] Bit2me, «Bit2me Academy» [En línea]. Disponible en: https://academy.bit2me.com/transacciones-bitcoin/.

[20] Blockchain Federal Argentina, «Blockchain Federal Argentina» [En línea]. Disponible en: https://bfa.ar/blockchain/bloques-y-transacciones.

[21] S. N. S. King, *PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake,* 2012.

[22] V. Buterin, *Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform,* 2014.

[23] Cripto Tendencia, «Cripto Tendencia» [En línea]. Disponible en: https://criptotendencia.com/2018/07/19/como-leer-una-transaccion-en-la-blockchain-de-bitcoin/.

[24] Bit2me, «Bit2me Academy» [En línea]. Disponible en: https://academy.bit2me.com/que-es-ecdsa-curva-eliptica/.

[25] Standards for Efficient Cryptography Group, «Standards for Efficient Cryptography Group» [En línea]. Disponible en: https://www.secg.org/.

[26] Bit2me, «Bit2me Academy» [En línea]. Disponible en: https://academy.bit2me.com/que-es-clave-privada/.

[27] Fábrica Nacional de Moneda y Timbre, «Real Casa de la Moneda. Fábrica Nacional de Moneda y Timbre» [En línea]. Disponible en: https://www.cert.fnmt.es/content/pages_std/html/tutoriales/tuto7.htm.

[28] J. L. D. Lizcano, *Aproximación basada en Blockchain para crear un modelo de confianza en la enseñanza superior abierta y ubicua,* 2019.

[29] M. C. y. C. C. S. Bonomi, *B-CoC: A Blockchain-Based Chain of Custody for Evidences Management in Digital Forensics,* 2019.

[30] The Linux Foundation, «The Linux Foundation» [En línea]. Disponible en: https://www.linuxfoundation.org.

[31] C. Cachin et al., *Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains,* 2018.

[32] The Linux Foundation, «Hyperledger Fabric» [En línea]. Disponible en: https://hyperledger-fabric.readthedocs.io/.

[33] M. Brandenburger, C. Cachin, R. Kapitza, A. Sorniotti, *Blockchain and Trusted Computing: Problems, Pitfalls, and a Solution for Hyperledger Fabric,* 2018.

[34] The Apache Software Foundation, «The Apache Software Foundation» [En línea]. Disponible en: https://www.apache.org/.

[35] The Linux Foundation, «Hyperledger Besu» [En línea]. Disponible en: https://besu.hyperledger.org/.

[36] Enterprise Ethereum Alliance, «Enterprise Ethereum Alliance» [En línea]. Disponible en: https://entethalliance.org/.

[37] IBM, «IBM Cloud Learn Hub» [En línea]. Disponible en: https://www.ibm.com/es-es/cloud/learn/rest-apis.

[38] Amazon, «Amazon Web Services» [En línea]. Disponible en: https://aws.amazon.com/es/what-is/restful-api/.

[39] T. Schrepel, *Smart Contracts and the Digital Single Market Through the Lens of a "Law + Technology" Approach,* 2021.

[40] European Comission, «European Comission» [En línea]. Disponible en: https://ec.europa.eu/digital-building-blocks/wikis/display/EBSI/.

[41] Bit2me, «Bit2me Academy» [En línea]. Disponible en: https://academy.bit2me.com/que-es-proof-of-authority-poa/.

[42] European Comission, «European Comission» [En línea]. Disponible en: https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/EBSI.

[43] Parlamento Europeo y Consejo de la Unión Europea, *Reglamento (UE) N. 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior,* 2014.

[44] Parlamento Europeo y Consejo de la Unión Europea, *Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se modifica el Reglamento (UE) N. 910/2014,* 2021.

[45] Ministerio del Interior, *Real Decreto 1553/2005, de 23 de diciembre, por el que se regula la expedición del documento nacional de identidad y sus certificados de firma electrónica,* 2005.

[46] E. Makriyannis y D. Clow, *Proceedings of the 1st International Conference on Learning Analytics and Knowledge,* 2011.

[47] Gobierno de España, «Portal de la Administración Electrónica» [En línea]. Disponible en: https://administracionelectronica.gob.es/pae_Home/pae_Actualidad/pae_Noticias/Anio2022/Abril/Noticia-2022-04-08-EBSI-la-infraestructura-europea-de-blockchain-en-marcha.html.

[48] Flask, «Flask. Web development, one drop at a time» [En línea]. Disponible en: https://flask.palletsprojects.com/.

[49] Python, «Python» [En línea]. Disponible en: https://www.python.org/.

[50] Postman, «Postman API Platform» [En línea]. Disponible en: https://www.postman.com/.

[51] Ministerio de Política Territorial y Función Pública, *Real Decreto 734/2020, de 4 de agosto, por el que se desarrolla la estructura orgánica básica del Ministerio del Interior,* 2020.

[52] M. Merchán y A. L. Martín, *The European Blockchain Services Infrastructure (EBSI) y el desarrollo de blockchain en el marco institucional europeo. Casos de uso*, 2020.

ANEXO I: CASOS DE USO DEL MODELO

Referencia	Descripción
Nombre	Alta de evidencia
Código	EV1
Método	POST /v1/evidence
Figuras	Unidad y Policía judicial
Acción	Dar de alta una evidencia en el sistema.
Resultado	Se registra el hash asociado a una evidencia en la blockchain, y la evidencia digital o, en caso de que sea física, digitalizada, en la base de datos distribuida.

Tabla 0-1 Caso de uso 1 – Alta de evidencia

Referencia	Descripción
Nombre	Consulta de evidencia
Código	EV2
Método	GET /v1/evidence/{id}
Figuras	Unidad, Policía judicial, Autoridad judicial y Defensa
Acción	Consultar una evidencia que previamente ha sido dada de alta.
Resultado	Se obtiene la información almacenada de una evidencia.

Tabla 0-2 Caso de uso 2 – Consulta de evidencia

Referencia	Descripción
Nombre	Baja de evidencia
Código	EV3
Método	PUT /v1/evidence/{id}
Figuras	Unidad y Policía judicial
Acción	Dar de baja una evidencia del sistema.
Resultado	Se incluye información en el sistema que indique que la evidencia se retira de la investigación. Se trata de una anotación y no de una supresión.

Tabla 0-3 Caso de uso 3 – Baja de evidencia

Referencia	Descripción
Nombre	Creación de la cadena de custodia
Código	CC1
Método	POST /v1/custody_chain/{id}/evidence
Figuras	Unidad y Policía judicial
Acción	Crear la cadena de custodia de una evidencia.
Resultado	Se establece la cadena de custodia, en la que se puede incluir información acerca de las actuaciones efectuadas sobre la evidencia. Se almacena la información en la base de datos distribuida.

Tabla 0-4 Caso de uso 4 – Creación de la cadena de custodia

Referencia	Descripción
Nombre	Consulta de la cadena de custodia
Código	CC2
Método	GET /v1/custody_chain/{id}
Figuras	Unidad, Policía judicial, Autoridad judicial y Defensa
Acción	Consultar la información almacenada acerca de las actuaciones efectuadas sobre la evidencia.
Resultado	Se obtiene la información almacenada en la base de datos distribuida de forma estructurada.

Tabla 0-5 Caso de uso 5 – Consulta de la cadena de custodia

Referencia	Descripción
Nombre	Cierre de la cadena de custodia
Código	CC3
Método	PUT /v1/custody_chain/{id}/evidence
Figuras	Unidad y Policía Judicial
Acción	Finalizar la cadena de custodia.
Resultado	Se completa la cadena de custodia con la última actuación que se había de realizar, indicando tal circunstancia. Se puede abrir la cadena de custodia en caso de que fuera necesario realizar llevar a cabo una nueva actuación sobre la evidencia.

Tabla 0-6 Caso de uso 6 – Cierre de la cadena de custodia

Referencia	Descripción
Nombre	Creación del *record*
Código	REC1
Método	POST /v1/record/{id}/custody_chain
Figuras	Unidad y Policía judicial
Acción	Crear un *record* en la cadena de custodia de una evidencia.
Resultado	Se incorpora, en la cadena de custodia, la información de una determinada actuación realizada sobre una evidencia. Se incluye la apertura de la cadena de custodia en caso de que hubiera sido cerrada.

Tabla 0-7 Caso de uso 7 – Creación del *record*

Referencia	Descripción
Nombre	Consulta del *record*
Código	REC2
Método	GET /v1/record/{id}
Figuras	Unidad, Policía judicial, Autoridad Judicial y Defensa
Acción	Consultar un *record* concreto de la cadena de custodia de una evidencia.
Resultado	Se obtiene la información de una actuación concreta que se encuentra en la cadena de custodia de una evidencia.

Tabla 0-8 Caso de uso 8 – Consulta del *record*

Referencia	Descripción
Nombre	Traspaso de evidencia
Código	REC3
Método	POST /v1/record/{id}
Figuras	Unidad y Policía judicial
Acción	Traspasar la evidencia a otra unidad, que, por competencia o por especialización, ha de realizar alguna actuación sobre la evidencia.
Resultado	Se modifica la unidad responsable de una evidencia y, por tanto, los agentes de policía judicial que intervienen sobre ella.

Tabla 0-9 Caso de uso 9 – Traspaso de evidencia

Referencia	Descripción
Nombre	Modificación del *record*
Código	REC4
Método	PUT /v1/record/{id}/custody_chain
Figuras	Unidad y Policía judicial
Acción	Incluir nueva información o, en su caso, modificar los datos asociados a un *record* concreto de la cadena de custodia de una evidencia.
Resultado	Se incorpora nueva información a la ya existente en un *record* determinado y, en su caso, subsanar cualquier error que hubiera podido tener lugar.

Tabla 0-10 Caso de uso 10 – Modificación del *record*