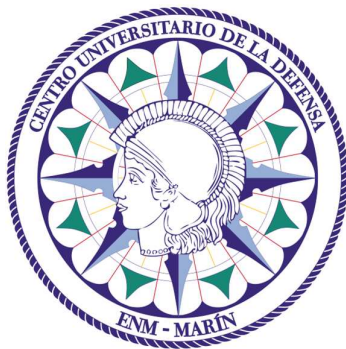




Centro Universitario de la Defensa en la Escuela Naval Militar

TRABAJO FIN DE MÁSTER

Garantizando la integridad de la información en la Cadena de Custodia de evidencias judiciales: Aplicación de la Tecnología Blockchain para su preservación.

Máster Universitario en Dirección TIC para la Defensa

ALUMNO:

D. I. J. Morales Molero

DIRECTORES:

D. J. P. González Coma

D. L. M. Álvarez Sabucedo

CURSO
ACADÉMICO:

2023-2025

UniversidadeVigo



Centro Universitario de la Defensa en la Escuela Naval Militar

TRABAJO FIN DE MÁSTER

Garantizando la integridad de la información en la Cadena de Custodia de evidencias judiciales: Aplicación de la Tecnología Blockchain para su preservación.

Máster Universitario en Dirección TIC para la Defensa
Especialidad de Sistemas y Tecnologías de la Información

Universida_{de}Vigo

RESUMEN

La cadena de custodia de las evidencias judiciales es uno de los pilares fundamentales en cualquier proceso judicial. Muchos procedimientos son sobreseídos porque, en algún punto, la cadena de custodia de las pruebas ha sido comprometida o se ha roto. Sin embargo, es importante señalar que la ruptura de la cadena de custodia no necesariamente invalida la evidencia, aunque sí puede afectar significativamente su credibilidad ante el tribunal, ya que la confianza en su integridad se ve reducida.

Es crucial preservar la integridad de las evidencias durante todo el proceso judicial, independientemente del ámbito en el que se desarrolle. Para garantizar esta integridad, es posible establecer un procedimiento en la cadena de custodia que sea completamente fiable, donde la trazabilidad de las pruebas quede claramente determinada, asegurando en todo momento que no han sido manipuladas, desde su recolección hasta su presentación ante el tribunal correspondiente.

Una manera efectiva de asegurar esta integridad y trazabilidad es mediante el uso de nuevas tecnologías, en particular, a través de la tecnología Blockchain. Este sistema puede garantizar que las evidencias judiciales sean completamente inviolables, registrando de manera inmutable no solo por dónde y por quién ha pasado la evidencia, sino también qué información ha sido añadida por cada interviniente a lo largo del proceso. Así, cada interacción con la evidencia queda registrada de forma transparente e incorruptible, lo que refuerza tanto su validez como su credibilidad ante los tribunales, aun cuando la cadena de custodia se ponga en duda.

El objetivo de este trabajo será realizar un análisis exhaustivo de las posibles situaciones y escenarios donde la cadena de custodia pueda verse comprometida, y cómo la tecnología Blockchain podría aplicarse para mitigar estos riesgos, garantizando no solo la integridad de las pruebas, sino también la trazabilidad precisa de cada intervención y cualquier información añadida a lo largo de todo el proceso.

PALABRAS CLAVE

BLOCKCHAIN, EVIDENCIAS, JUDICIALES, CADENA, CUSTODIA

AGRADECIMIENTOS

Mi más profundo agradecimiento a mi mujer y a mi hijo por su infinita paciencia y apoyo durante todo el transcurso de este máster, siempre brindándome fuerza para continuar. Asimismo, agradezco a mis directores del trabajo fin de máster por sus valiosas sugerencias y recomendaciones, que fueron fundamentales para su desarrollo.

Contenido

1	Introducción y objetivos	7
1.1	Exposición inicial.....	7
1.2	Relevancia de Blockchain en el contexto legal.....	7
1.3	Blockchain y la cadena de custodia	8
1.4	Objetivos específicos	10
1.5	Organización del documento	10
2	La tecnología Blockchain	13
2.1	Origen de Blockchain.....	13
2.2	Fundamentos de Blockchain	14
2.2.1	Estructura de Bloque.....	14
2.2.2	Mecanismo de consenso	15
2.2.3	Criptografía en Blockchain.....	16
2.2.4	Tipos de Blockchain	16
2.3	Contratos Inteligentes (<i>Smart Contracts</i>)	17
2.4	Aplicaciones de Blockchain.....	18
2.4.1	Criptomonedas y Finanzas.....	18
2.4.2	NTFs (Token no Fungibles).....	18
2.4.3	Cadena de suministros	19
2.4.4	Sistemas de votación electrónica	19
2.4.5	Aplicaciones en el Sector de la Salud.....	19
2.4.6	Propiedad Intelectual y Derechos de Autor	19
2.4.7	Seguros	20
2.4.8	Adopción en Nuevas Áreas	20
3	La cadena de custodia: caracterización y fundamentos.....	21
3.1	Análisis jurisprudencial.....	21
3.1.1	Doctrina General de Tribunal Supremo (TS) sobre la cadena de custodia.....	21
3.1.2	Presunción de validez en la conservación de la cadena de custodia	23
3.1.3	Cadena de custodia aplicada a la prueba electrónica	23
3.2	Aportaciones de la doctrina científica respecto a la cadena de custodia	25
3.3	La normativización de la cadena de custodia.....	26
4	El reconocimiento jurídico de las tecnologías de registro distribuido	29
4.1	Uso de las tecnologías de registro distribuido en el sector público	31
4.2	La regulación del libro mayor electrónico como servicio de confianza	32

5 Consideraciones de protección de datos de carácter personal.....	35
6 Iniciativas sobre tecnología Blockchain en el sector público.....	39
6.1 Iniciativa Europea de Infraestructura de Servicios Blockchain (ESBI).....	39
6.1.1 Arquitectura basada en Blockchain permitida.....	40
6.1.2 Mecanismos de interoperabilidad	41
6.1.3 Infraestructura descentralizada	41
6.1.4 Seguridad y privacidad.....	41
6.2 El Proyecto de la Fábrica Nacional de Moneda y Timbre (FNMT-RCM)	43
6.2.1 Características Técnicas de la Solución	43
6.2.2 Beneficios de la Solución.....	44
6.3 <i>Hyperledger Fabric</i> : Características y Capacidades.....	44
6.3.1 Estructura técnica	44
6.3.2 Cumplimiento con la normativa de protección de datos europea y española	46
7 Propuesta de solución	49
8 Conclusiones	53
9 Bibliografía.....	55

1 INTRODUCCIÓN Y OBJETIVOS

1.1 Exposición inicial

La cadena de custodia es un proceso crítico en el sistema de justicia penal, donde cada paso de la manipulación de una evidencia debe ser rigurosamente documentado para asegurar que dicha evidencia no ha sido contaminada, alterada o manipulada desde el momento en que fue recogida hasta su presentación en un tribunal. La integridad de la cadena de custodia es crucial para garantizar que la evidencia sea admisible en un proceso judicial y para proteger los derechos de todas las partes implicadas.

Diferentes unidades de la Guardia Civil, en su labor de investigación de hechos delictivos, en el ejercicio de sus funciones como Policía Judicial, tanto genérica como específica, requiere de una solución para apoyar la operativa de estas unidades. De esta forma, la toma de evidencias y su custodia durante la realización de su servicio de inspección técnica ocular (ITO), hasta que sea presentada ante las autoridades judiciales, garantizaría la integridad, y seguridad necesaria para que sean consideradas válidas en el proceso judicial correspondiente.

Es aquí donde podría integrarse la tecnología Blockchain, pues ésta no solo presenta una revolución en campos como el mundo de las criptomonedas, sino que su aplicación en el campo legal, y en particular en la gestión de la cadena de custodia de evidencias judiciales, ofrece una oportunidad para mejorar la integridad, transparencia y seguridad de los procesos judiciales. Con la tecnología basada en Blockchain, el sistema de ITO,s puede avanzar hacia un futuro donde la confianza en las evidencias presentadas sea más robusta, y mejorando la integridad de las evidencias que se presentan ante los juzgados. Es decir, que las evidencias judiciales no se han visto comprometidas en ningún estadio de la cadena de custodia.

1.2 Relevancia de Blockchain en el contexto legal

La tecnología Blockchain ha emergido como una de las innovaciones tecnológicas más disruptivas del siglo XXI, revolucionando la manera en que se manejan las transacciones y los datos en un mundo cada vez más digitalizado. Originalmente concebida como la tecnología subyacente del Bitcoin, la primera criptomoneda, Blockchain ha trascendido su aplicación en las finanzas para ofrecer soluciones a una variedad de problemas en múltiples sectores, incluyendo la cadena de suministro, la salud, la administración pública, y, especialmente, en el ámbito legal.

En su esencia, Blockchain es un libro mayor digital distribuido que permite a las partes mantener un registro compartido e inmutable de transacciones. Este sistema descentralizado elimina la necesidad de intermediarios de confianza, como bancos o notarios, y ofrece una solución para el almacenamiento y transmisión de datos que es resistente a manipulaciones [1]. Cada transacción, una vez validada y registrada en un bloque, se convierte en parte de una cadena que no puede ser alterada sin el consenso de la red, lo que asegura la integridad y autenticidad de la información almacenada [2].

El potencial de Blockchain se extiende de manera significativa al ámbito legal, donde la integridad, transparencia y trazabilidad de la información son fundamentales. Una de las áreas donde Blockchain puede tener un impacto transformador es en la cadena de custodia de evidencias judiciales.

1.3 Blockchain y la cadena de custodia

Blockchain ofrece una solución robusta para los desafíos asociados con la cadena de custodia de evidencias judiciales al proporcionar un registro inmutable y verificable de cada interacción con la evidencia. En un sistema tradicional, la cadena de custodia se mantiene a través de registros escritos o bases de datos centralizadas, que son susceptibles a errores humanos, manipulaciones intencionales o no intencionales, y pérdida de registros. Con Blockchain, estos riesgos pueden mitigarse significativamente, ya que el uso de esta tecnología, alineado con principios legales, refuerza la autenticidad y admisibilidad de las evidencias digitales en los tribunales. [3]

A continuación, se describen las ventajas clave que Blockchain aporta a la cadena de custodia de evidencias judiciales:

1. Inmutabilidad y Transparencia:

- Una de las principales fortalezas de Blockchain es su capacidad para registrar transacciones de manera inmutable. Una vez que una evidencia es registrada en la Blockchain, cada transacción relacionada con esa evidencia (como transferencias de custodia, acceso, o análisis) queda registrada de forma permanente y no puede ser alterada sin que toda la red lo detecte. Esta inmutabilidad asegura que cualquier intento de manipulación o alteración en la cadena de custodia sea fácilmente detectable.
- Además, la naturaleza transparente de Blockchain permite que todas las partes involucradas (incluidos los defensores, fiscales, jueces y, en algunos casos, el público) tengan acceso a un registro auditable de la cadena de custodia, lo que refuerza la confianza en la integridad del proceso judicial.

2. Trazabilidad:

- Blockchain permite la trazabilidad completa de cada evidencia desde el momento en que es recogida hasta su presentación en el tribunal. Cada cambio de custodia, cada acceso por parte de un investigador o analista forense, y cada transferencia entre instituciones se registra en la Blockchain, creando un historial detallado y verificable.
- Este nivel de trazabilidad es crucial en casos complejos donde las evidencias pasan por múltiples manos o requieren de análisis en diferentes laboratorios. La capacidad de rastrear el recorrido completo de una evidencia aumenta la confianza en que se ha mantenido la integridad durante todo el proceso.

3. Automatización a través de Contratos Inteligentes:

- Los contratos inteligentes, que son programas autoejecutables almacenados en la Blockchain, pueden automatizar aspectos clave de la cadena de custodia. Por ejemplo, un contrato inteligente podría activarse automáticamente cuando una evidencia es recibida por un laboratorio, registrando automáticamente la hora y el lugar de la recepción, así como la identidad del responsable.

- Además, los contratos inteligentes pueden garantizar que solo personas autorizadas puedan acceder a la evidencia y que cualquier acceso o manipulación sea registrado de manera automática en la Blockchain, sin intervención humana, reduciendo así el riesgo de errores o manipulaciones.

4. Seguridad y Privacidad:

- Aunque Blockchain es transparente, también puede ofrecer altos niveles de seguridad y privacidad. Las identidades de los responsables de la custodia y los detalles específicos de las evidencias pueden cifrarse en la Blockchain, asegurando que solo personas autorizadas puedan acceder a información sensible, mientras que la trazabilidad y la integridad de la cadena de custodia permanecen aseguradas.
- Esta seguridad adicional es especialmente importante en casos donde las evidencias son de naturaleza delicada o involucran información privada que debe ser protegida durante todo el proceso judicial.

5. Reducción de Disputas y Aumentos en la Eficiencia:

- Al proporcionar un registro claro y auditable de todas las interacciones con una evidencia, Blockchain puede reducir las disputas relacionadas con la manipulación de evidencias. Cualquier desacuerdo sobre la autenticidad o la manipulación de la evidencia puede resolverse fácilmente mediante la consulta del registro en la Blockchain.
- Además, la automatización y la trazabilidad ofrecidas por Blockchain pueden mejorar la eficiencia del proceso judicial, reduciendo el tiempo necesario para verificar cadenas de custodia y permitiendo a los investigadores y fiscales concentrarse en el análisis sustantivo de las evidencias.

En resumen, el futuro de Blockchain en el ámbito judicial y, específicamente, en la cadena de custodia de evidencias, es extremadamente prometedor. A medida que las tecnologías Blockchain continúan evolucionando y madurando, es probable que se vea un incremento en su adopción en los sistemas de justicia de todo el mundo. Esta adopción podría llevar a un sistema judicial más transparente, eficiente y justo, donde la integridad de la evidencia esté garantizada y donde los litigios relacionados con la manipulación o pérdida de evidencia sean significativamente reducidos.

Además, la evolución de las regulaciones y la colaboración entre gobiernos, empresas tecnológicas y el sector judicial será clave para superar los desafíos actuales y aprovechar al máximo los beneficios de Blockchain en este ámbito. La implementación de estándares y mejores prácticas en el uso de Blockchain para la cadena de custodia podría establecer un nuevo paradigma en la administración de justicia, brindando mayor confianza al público y fortaleciendo el estado de derecho.

En conclusión, Blockchain no solo es una tecnología con el potencial de transformar industrias comerciales, sino que también tiene un papel crucial que desempeñar en la mejora de la justicia y la gobernanza. La adopción de Blockchain en la cadena de custodia de evidencias judiciales representa un avance significativo hacia un sistema judicial más transparente, seguro y eficiente. A medida que se continúa explorando y desarrollando nuevas aplicaciones de Blockchain, es fundamental que los profesionales del derecho, los tecnólogos y los reguladores trabajen juntos para integrar esta tecnología de manera que maximice sus beneficios y minimice sus riesgos. Con un enfoque cuidadoso y colaborativo, Blockchain podría convertirse en un pilar fundamental de la administración de justicia en el siglo XXI.

No obstante, uno de los principales retos de esta tecnología en el ámbito legal es que sea admitida por las autoridades judiciales que tendrán que validar su uso y confiar en su fiabilidad e inmutabilidad para declarar sin ningún tipo de duda, que la cadena de custodia realizada a través de

Blockchain cuenta con las características y las funcionalidades que deben estar presentes en este proceso.

1.4 Objetivos específicos

El presente trabajo tiene como objetivo general explorar y evaluar el potencial de la tecnología Blockchain en el ámbito de la cadena de custodia judicial, abordando los aspectos legales significativos para garantizar su implementación efectiva y admisibilidad en los procesos judiciales. Para ello, se definen los siguientes objetivos parciales:

1. Análisis legal y normativo:
 - Realizar un estudio exhaustivo de las normativas nacionales e internacionales aplicables a la gestión de evidencias y la cadena de custodia, con especial énfasis en su aplicación dentro del sistema judicial español y europeo.
 - Evaluar las funcionalidades y procesos asociados al uso de Blockchain para garantizar que se cumplan los requisitos legales de trazabilidad, integridad y autenticidad de las evidencias en el contexto judicial.
2. Revisión del impacto de esta tecnología en el marco jurídico y legal actual:
 - Garantía de aceptación en tribunales:
 - ✓ Analizar la viabilidad legal del uso de tecnologías de libros mayores distribuidos (DLT), como Blockchain, para certificar la integridad y autenticidad de las evidencias judiciales, garantizando su aceptación en tribunales como un proceso válido.
 - ✓ Validar cómo la tecnología Blockchain puede cumplir con los estándares legales para asegurar el no repudio de la información registrada en la cadena de custodia.
 - Cumplimiento de normativas de privacidad y protección de datos:
 - ✓ Examinar la adecuación del uso de Blockchain con respecto al Reglamento General de Protección de Datos (RGPD) y la legislación española de protección de datos, asegurando que se respeten los derechos de privacidad de las partes involucradas.
 - ✓ Análisis de las capacidades de plataformas basadas en tecnología Blockchain que hagan viable el cumplimiento de esta normativa.
3. Proponer las bases de una plataforma válida para el contexto actual de la Guardia Civil:
 - A través del análisis de plataformas en desarrollo como la iniciativa europea de servicios de Blockchain (ESBI) y otros proyectos piloto en el ámbito nacional, proponer una plataforma que satisfaga tanto las exigencias normativas como las necesidades de las unidades de la Guardia Civil en cuanto a la preservación de la cadena de custodia de las evidencias que deban ser puestas a disposición judicial.

1.5 Organización del documento

El desarrollo del presente trabajo se estructura en las siguientes secciones, diseñadas para abordar de manera integral los objetivos planteados en el punto anterior:

1. Estado del arte:
 - Revisión de la literatura existente sobre el uso de Blockchain en el ámbito legal, con un enfoque en la gestión de evidencias y la cadena de custodia. Esto permite resolver el Objetivo parcial 1.

2. Definición de cadena de custodia:

- Explicación detallada del concepto de cadena de custodia, sus principios fundamentales y su importancia en el sistema judicial.
- Identificación de las etapas clave en la cadena de custodia y los desafíos actuales en su gestión.

3. Marco normativo de los libros mayores distribuidos:

- Estudio del marco normativo aplicable al uso de tecnologías de libros mayores distribuidos en España y la Unión Europea.
- Análisis de la aceptación legal de registros basados en Blockchain como evidencia en tribunales, considerando precedentes legales y normativa específica. Esto permite resolver parcialmente el Objetivo parcial 2.

4. Cumplimiento de la normativa estatal y europea sobre protección de datos:

- Evaluación del cumplimiento del Reglamento General de Protección de Datos (GDPR) y la legislación española en relación con la gestión de información sensible en Blockchain. Esto permite resolver parcialmente el Objetivo parcial 2

5. Propuesta de solución

- Se abordará a nivel teórico una posible solución para la implementación de la tecnología Blockchain en el ámbito policial. Esto permite resolver el Objetivo parcial 3

6. Conclusiones:

- Resumen de los hallazgos más relevantes del trabajo y su aplicabilidad práctica en la cadena de custodia.

2 LA TECNOLOGÍA BLOCKCHAIN

2.1 Origen de Blockchain

La historia de Blockchain se remonta a la década de los 90 del siglo XX, cuando Stuart Haber y W. Scott Stornetta propusieron por primera vez una solución práctica para el uso de una cadena de bloques para asegurar la integridad de los registros digitales. En 1991, estos científicos publicaron un artículo, titulado "*How to Time-Stamp a Digital Document*", en el que describían un sistema en el cual los documentos digitales podían ser registrados para que no se pudieran manipular ni retroceder en el tiempo, utilizando un sellado de tiempo (*timestamping*). Sin embargo, este concepto no se desarrolló completamente hasta años más tarde, cuando se combinó con la criptografía moderna.

En 2008, una figura anónima o grupo de personas bajo el pseudónimo "Satoshi Nakamoto" revolucionó la tecnología al introducir una aplicación práctica del Blockchain en el famoso documento titulado "*Bitcoin: A Peer-to-Peer Electronic Cash System*" [2]. Este sistema propuso la creación de una moneda digital descentralizada, Bitcoin, que operaría sin la necesidad de intermediarios como bancos, utilizando la tecnología de Blockchain para mantener un registro público y seguro de todas las transacciones. Nakamoto usó la idea de Haber y Stornetta [1], pero la mejoró con un mecanismo de consenso distribuido llamado "*proof of work*" (*PoW*), lo que permitió que la tecnología fuera segura y escalable.

La primera aplicación del Blockchain fue en el campo de las criptomonedas, concretamente con el Bitcoin, lanzado en 2009. A partir de ahí, el uso de esta tecnología se ha expandido a múltiples sectores, incluyendo finanzas, logística, salud y otros. Blockchain ha demostrado ser útil para garantizar la transparencia y seguridad en sistemas descentralizados, facilitando el registro inmutable de datos. La popularidad del Bitcoin ayudó a que muchas otras criptomonedas y aplicaciones basadas en Blockchain emergieran en los años posteriores, convirtiendo esta tecnología en una de las más disruptivas del siglo XXI.

2.2 Fundamentos de Blockchain

Blockchain, frecuentemente descrita como una tecnología revolucionaria y disruptiva, es esencialmente una base de datos distribuida que permite el registro seguro, transparente e inmutable de transacciones. La tecnología subyacente se basa en principios de criptografía, redes distribuidas y mecanismos de consenso, lo que garantiza que los datos sean resistentes a manipulaciones y accesibles para todos los participantes de dicha red. Con el objeto de un mejor entendimiento del funcionamiento de Blockchain, es primordial estudiar y explorar sus componentes fundamentales y la forma en que estos interactúan para ofrecer una solución robusta a una variedad de problemas respecto a la confianza y seguridad en sistemas distribuidos.

¿Y qué se entiende por sistema distribuido? Un sistema distribuido es un conjunto de computadoras independientes que aparecen como un único sistema unificado para los usuarios. Cada computadora en el sistema colabora entre nodos de forma transparente, con el objeto de mejorar la eficiencia, la confiabilidad y la escalabilidad de los procesos [4].

2.2.1 Estructura de Bloque

Cada bloque en una cadena de bloques (Blockchain) es como una página en un libro mayor digital. Esto es, una base de datos distribuida y consensuada, compartida en una red de múltiples ubicaciones, donde se registran de manera segura y permanente las transacciones o activos de una organización o sistema. Su tecnología subyacente permite que cada participante en la red tenga una copia sincronizada del registro, promoviendo la transparencia y reduciendo la necesidad de intermediarios [5].

De esta forma, contiene un conjunto de transacciones que han sido verificadas y registradas por los participantes en la red. A continuación, se nombrarán los elementos clave que componen un bloque en una plataforma como Bitcoin:

- Datos de las transacciones: este es el contenido central del bloque, que incluye todas las transacciones que han sido realizadas y verificadas dentro de un tiempo específico. En el caso de las criptomonedas como Bitcoin, por ejemplo, los datos consisten en detalles de transacciones como el emisor, el receptor y la cantidad transferida.
- Hash del bloque anterior: Un hash es una cadena alfanumérica única generada por una función criptográfica a partir de los datos del bloque anterior. Este hash actúa como un identificador digital que asegura la integridad del bloque anterior y enlaza los bloques entre sí en una secuencia continua. Si se altera el dato en un bloque anterior, el hash cambiará, lo que haría evidente cualquier intento de manipulación.
- Hash del bloque actual: Similar al hash del bloque anterior, el hash del bloque actual es generado a partir de los datos del propio bloque. Este hash es único y actúa como la “huella digital” del bloque. Es esencial para el proceso de validación y para garantizar que el bloque no ha sido alterado una vez ha sido registrado en la cadena.
- *Nonce* (Número Arbitrario): El *nonce* es un número que los mineros, es decir, los participantes de la red de Blockchain que compiten entre sí para introducir el siguiente bloque en la cadena, desean hallar, en el caso de Blockchains que utilizan el mecanismo de consenso *Proof of Work (PoW)*. El mencionado *nonce* es un número tal que, una vez añadido al bloque, hace que el hash resultante empiece por, como mínimo, una cierta cantidad de ceros. El único modo de buscarlo es por fuerza bruta. Este número necesario de ceros iniciales en el *nonce* es el grado de dificultad del minado y es ajustado cada cierto tiempo para mantener una tasa constante de generación de bloques.

2.2.2 Mecanismo de consenso

El mecanismo de consenso es el protocolo que define cómo los nodos de la red acuerdan sobre una única versión de la verdad en la Blockchain. Definido de otro modo, permite que todos los participantes en la red se pongan de acuerdo sobre el estado actual de la cadena y sobre cuáles transacciones deben ser añadidas al siguiente bloque.

Los mecanismos de consenso más comunes son:

- *Proof of Work (PoW)*: Este mecanismo de consenso es uno de los primeros y más conocidos, utilizado por Bitcoin. En PoW, los mineros, o participantes en la red, compiten para resolver problemas matemáticos complejos, proceso que es conocido como minería. El primer minero en resolver el problema tiene el derecho de añadir un nuevo bloque a la cadena, siendo recompensado con una cierta cantidad de criptomoneda.

La dificultad del problema matemático asegura que solo se pueda añadir un bloque aproximadamente cada diez minutos, en el caso de Bitcoin, haciendo que la red sea segura, aunque también costosa en términos de energía.

- *Proof of Stake (PoS)*: este mecanismo fue introducido como una alternativa más eficiente energéticamente al PoW. En PoS, en lugar de competir para resolver problemas matemáticos, los validadores son seleccionados para crear nuevos bloques y validar transacciones en función de la cantidad de criptomoneda que han “apostado” como garantía en la red.

Inciendo en la palabra “apostado” de la frase anterior, se hace referencia al proceso en el cual los validadores “bloquean” o depositan una cantidad de criptomonedas en la red como una garantía o compromiso de que actuarán de manera honesta y responsable al validar transacciones y crear nuevos bloques en el sistema de consenso *Proof of Stake (PoS)* [6]

Esta “apuesta” de criptomonedas se denomina también “*staking*”, y sirve como incentivo para que los validadores se comporten correctamente. Si un validador intenta manipular o comprometer la red, podría perder parte o la totalidad de la criptomoneda que ha apostado.

Cuanto mayor es la cantidad de criptomoneda que un validador ha apostado, mayor es la probabilidad de ser seleccionado para validar un bloque, lo que crea una relación entre la cantidad apostada y el nivel de participación y confianza en la red.

Los validadores que actúen de manera deshonesta pueden perder parte o la totalidad de su apuesta, incentivando el comportamiento honesto, para generar confianza.

PoS, aun cuando es más eficiente en términos de consumo energético, plantea diferentes desafíos en términos de diseño, referido a aspectos arquitectónicos y estructurales del sistema de consenso *Proof of Stake (PoS)*. Estos incluyen cómo se eligen y gestionan los validadores, cómo se manejan los depósitos o “*stakes*” de criptomonedas, y cómo se garantiza la descentralización de la red.

Pero también en cuanto a la seguridad, en cuanto a mecanismos necesarios para proteger la red contra ataques y abusos específicos de PoS. Debe emplear métodos de seguridad, como el “*slashing*” (penalización de validadores deshonestos), medidas contra ataques de larga duración, o el ataque del “nada en juego” (donde los validadores podrían validar múltiples cadenas sin penalización).

- *Delegated Proof of stake (DPoS)*: Una variación del PoS, que permite que los participantes voten por un pequeño número de delegados que son responsables de validar las transacciones y mantener la cadena de bloques.

Este mecanismo puede mejorar la eficiencia y la velocidad de las transacciones, pero, a menudo, es criticado por su tendencia a centralizar el poder en un pequeño grupo de actores.

- Prueba de Autoridad (*Proof of Authority*, PoA): Es el mecanismo de consenso utilizado en Blockchains privadas, donde se selecciona validadores en función de su identidad o reputación en lugar de su participación financiera o poder computacional. Es un mecanismo útil en entornos donde se requiere un alto grado de control y confiabilidad, como pueden ser redes corporativas o gubernamentales.

2.2.3 Criptografía en Blockchain

La seguridad de Blockchain se basa principalmente en la criptografía, definido como el arte de crear códigos y cifrados para proteger la información. En este sentido, existen varios métodos criptográficos que son fundamentales para el funcionamiento de Blockchain.

Estos son:

- *Hashing*: Es un proceso criptográfico que convierte cualquier bloque de datos en una cadena de longitud fija, denominada *hash*. Una característica crucial de los algoritmos de *hash*, como SHA-256 utilizado en Bitcoin, es que, incluso, un pequeño cambio en los datos originales genera un *hash* completamente diferente, lo que hace que sea prácticamente imposible alterar un bloque sin que esa manipulación sea detectada.
- Criptografía de Clave Pública y Privada: Cada usuario de una red Blockchain tiene un par de claves criptográficas: una clave pública, que es visible a todos, y una clave privada, que debe mantenerse secreta.

La clave pública se utiliza para recibir transacciones, mientras que la clave privada se utiliza para encriptar digitalmente las transmisiones que se envían.

- Firmas Digitales: Una firma digital es un mecanismo criptográfico que se utiliza para validar la autenticidad e integridad de un mensaje, software o documento digital.

En el contexto de Blockchain, las firmas digitales se emplean para firmar transacciones, asegurando que solo el propietario de una clave privada puede transferir los fondos asociados a una clave pública, en el caso de que se traten de Blockchains públicas dentro del mundo de las criptomonedas, o que, en el caso de Blockchains privadas, aseguran que solo los participantes autorizados puedan validar y ejecutar transacciones, lo que agrega una capa de control de acceso sobre quién puede participar activamente.

2.2.4 Tipos de Blockchain

A medida que Blockchain ha evolucionado, han surgido diferentes tipos de Blockchains para satisfacer las necesidades de distintos casos de uso. En este apartado, se enumerarán los distintos tipos de cadenas de bloque existentes actualmente:

- Blockchain Pública: Son las más comunes y están abiertas a cualquiera que desee participar. Cualquier persona puede leer o enviar transacciones o participar en el proceso de consenso. Bitcoin y Ethereum son ejemplos de Blockchains públicas. Estas Blockchains son completamente descentralizadas, lo que significa que ninguna entidad central tiene el control sobre la red de participantes. Sin embargo, esta apertura también las hace más susceptibles a problemas de escalabilidad y consumo de energía.
- Blockchain Privada: A diferencia de las Blockchains públicas, las privadas están controladas por una organización o grupo central que decide quién puede leer y escribir en la cadena. Este tipo de Blockchains se utiliza generalmente en entornos empresariales donde se requiere privacidad y control sobre quién tiene acceso a los datos.

Como ejemplo, se puede citar *Hyperledger Fabric*. Se utiliza principalmente en aplicaciones empresariales donde la privacidad, el rendimiento y la capacidad de personalización son cruciales. Algunos sectores donde se implementa incluyen:

- Cadena de suministro: Permite un seguimiento seguro y transparente de productos desde su origen hasta el consumidor final, con control de acceso a datos específicos en cada etapa.

- Finanzas: Facilita transacciones rápidas, seguras y transparentes entre instituciones financieras, respetando la privacidad de los clientes y cumpliendo con regulaciones.
- Atención médica: Permite compartir registros médicos entre hospitales, laboratorios y aseguradoras de manera segura, protegiendo la privacidad del paciente.
- Gobierno y servicios públicos: Optimiza procesos administrativos, aumenta la transparencia y mejora la colaboración entre diferentes departamentos y agencias. [7]
- Blockchain Permisionada (Consortio): Estas Blockchains combinan características de las públicas y las privadas. Aunque son accesibles solo para un grupo selecto de participantes, pueden ser gestionadas por múltiples organizaciones en lugar de una solo. La Blockchains permisionadas son comunes en consorcios empresariales, donde varias empresas necesitan colaborar de manera segura y eficiente.

Un ejemplo de este tipo de Blockchain es R3 Corda, diseñada para instituciones financieras [8].

- Blockchain Híbrida: Combina elementos de Blockchains públicas y privadas. Permiten que una parte de la cadena sea pública, accesible a todos, mientras que otra parte permanece privada, controlada por un grupo específico de participantes en la red. Esto permite a las organizaciones disfrutar de la transparencia de una Blockchain pública mientras mantiene un control privado sobre ciertos datos sensibles.

En este caso, un ejemplo destacado de Blockchain híbrida es Dragonchain, una plataforma inicialmente desarrollada por Disney que permite a las empresas decidir qué datos quieren mantener privados y qué información hacer pública. Combina privacidad y seguridad en un entorno empresarial, permitiendo cumplir con regulaciones y proteger datos sensibles, mientras se beneficia de la transparencia y verificabilidad de una red pública. Esto la hace adecuada para aplicaciones en sectores como la cadena de suministro, finanzas y propiedad intelectual [9].

Cada uno de estos tipos de Blockchain tiene sus propias ventajas y desventajas, lo que los hace adecuados para diferentes aplicaciones y casos de uso. La elección del tipo de Blockchain depende de factores como el nivel de descentralización requerido, la necesidad de privacidad, y las consideraciones de rendimiento y escalabilidad.

2.3 Contratos Inteligentes (*Smart Contracts*)

Los contratos inteligentes son una de las innovaciones más revolucionarias de la tecnología Blockchain. Estos permiten que ciertos procesos contractuales se realicen de forma automática, sin necesidad de intermediarios, lo que abre un abanico de posibilidades para múltiples sectores.

1. Programas Autoejecutables: Los contratos inteligentes son básicamente programas que funcionan automáticamente cuando se cumplen ciertas condiciones. Al estar almacenados en la Blockchain, se garantiza que estos contratos se ejecuten exactamente como fueron programados, sin posibilidad de interferencia externa, manipulación o fraude.
2. Inmutabilidad: Una vez que un contrato inteligente se despliega en la Blockchain, no puede ser modificado. Esto significa que las condiciones que lo activan siempre serán las mismas, brindando una seguridad y confianza muy alta para todos los involucrados.
3. Activación por Condiciones: Un contrato inteligente actúa como una serie de "si sucede esto, entonces haz aquello". Por ejemplo, podría liberar un pago automáticamente cuando se cumpla una fecha específica o cuando un producto sea entregado y confirmado por ambas partes.
4. Descentralización: Al operar en una Blockchain, los contratos inteligentes no dependen de un intermediario para ejecutarse. Esto ahorra tiempo y costos que usualmente se destinan a terceras partes en los contratos tradicionales.

En conclusión, los contratos inteligentes ofrecen una forma eficiente y segura de ejecutar acuerdos de manera automática, sin depender de terceros y con un alto nivel de confiabilidad. Gracias a su versatilidad, están transformando sectores como las finanzas, los seguros, la votación y la logística, estableciendo una nueva forma de hacer negocios en el ámbito digital. [10]

2.4 Aplicaciones de Blockchain

La tecnología Blockchain ha extendido sus aplicaciones mucho más allá de las criptomonedas, sirviendo como base para una nueva generación de sistemas y servicios digitales. Su capacidad para ofrecer transparencia, seguridad y descentralización ha permitido la creación de innovadoras aplicaciones en áreas como almacenamiento de archivos, aplicaciones descentralizadas, activos digitales únicos y servicios gubernamentales. A continuación, se presentan algunas de las aplicaciones más destacadas de esta tecnología.

2.4.1 Criptomonedas y Finanzas

El sector financiero fue el primero en adoptar Blockchain, gracias al surgimiento de Bitcoin en 2008. Las criptomonedas son quizás la aplicación más conocida de esta tecnología, pero las finanzas descentralizadas (DeFi) están llevando esta innovación aún más lejos.

Criptomonedas:

- Bitcoin: La primera y más conocida criptomoneda, Bitcoin, utiliza Blockchain para permitir transacciones peer-to-peer sin la necesidad de intermediarios como bancos. Cada transacción es registrada en una cadena de bloques, lo que asegura su inmutabilidad y transparencia.
- Ethereum: A diferencia de Bitcoin, que fue diseñado principalmente como una moneda digital, Ethereum introdujo la idea de los contratos inteligentes y aplicaciones descentralizadas (dApps) que se ejecutan en su Blockchain. Esto ha abierto la puerta a una amplia gama de aplicaciones financieras automatizadas.

Finanzas Descentralizadas (DeFi):

- Préstamos y Créditos: Las plataformas DeFi permiten a los usuarios prestar y tomar prestados activos digitales sin necesidad de intermediarios tradicionales. Los contratos inteligentes automatizan todo el proceso, desde la aprobación del préstamo hasta el cobro de intereses.
- Intercambios Descentralizados (DEXs): Los DEXs permiten a los usuarios intercambiar criptomonedas directamente entre sí, sin la necesidad de una plataforma centralizada. Esto reduce el riesgo de manipulación y hackeos asociados con los intercambios tradicionales.
- *Stablecoins*: Estas criptomonedas están vinculadas a activos estables como el dólar estadounidense, lo que las hace menos volátiles. Son ampliamente utilizadas en el ecosistema DeFi para realizar transacciones y mantener valor.

2.4.2 NTFs (Token no Fungibles)

Los NFTs o Tokens No Fungibles representan activos digitales únicos e indivisibles en la Blockchain. A diferencia de las criptomonedas, los NFTs no son intercambiables uno a uno, ya que cada uno tiene un valor y características únicas. Esto los convierte en una herramienta ideal para representar propiedades digitales exclusivas, como obras de arte, coleccionables, música, y otros activos digitales.

- Características de los NFTs:
 - Únicos: Cada NFT tiene un identificador único en la Blockchain, lo que garantiza su autenticidad.
 - Indivisibles: No se pueden dividir en partes, a diferencia de las criptomonedas.

- Transferibles: Pueden ser transferidos o vendidos entre usuarios.
- Escasez Verificable: Su escasez se garantiza y se verifica en la Blockchain, ya que el número total de NFTs puede ser limitado.

2.4.3 Cadena de suministros

La Blockchain se ha convertido en una herramienta crucial para la cadena de suministro, permitiendo la trazabilidad y autenticidad de productos en tiempo real desde su origen hasta el consumidor final. Al registrar cada paso del proceso de producción y distribución en la Blockchain, las empresas pueden garantizar la transparencia y verificar que los productos sean auténticos.

- Ventajas para la Cadena de Suministro:
 - Trazabilidad y Transparencia: Los productos pueden ser rastreados a lo largo de toda la cadena de suministro, lo cual es crucial para sectores como alimentos y bienes de lujo.
 - Prevención de Fraude: Al registrar cada transacción en la Blockchain, es mucho más difícil introducir productos falsificados en la cadena de suministro.

2.4.4 Sistemas de votación electrónica

Los sistemas de votación basados en Blockchain permiten que los procesos electorales sean transparentes, seguros y verificables. En estos sistemas, cada voto se registra en la Blockchain como una transacción inmutable, lo que dificulta la manipulación o el fraude electoral.

- Características de los Sistemas de Votación en Blockchain:
 - Inmutabilidad: Los votos no se pueden alterar ni eliminar una vez registrados.
 - Transparencia: El recuento de votos es accesible y verificable por cualquier observador, garantizando la confianza en el sistema electoral.

2.4.5 Aplicaciones en el Sector de la Salud

En el sector salud, Blockchain se utiliza para crear un sistema seguro y transparente de intercambio de información médica. La tecnología permite a los hospitales, médicos y pacientes compartir registros médicos de manera segura, protegiendo la privacidad de los datos sensibles y facilitando un acceso rápido en situaciones de emergencia. Como casos de uso, se pueden nombrar, por ejemplo, los siguientes:

- Historia Clínica Electrónica (EHR): Blockchain permite que los registros médicos se almacenen de forma descentralizada, permitiendo a los pacientes controlar quién accede a su información.
- Trazabilidad de Medicamentos: La Blockchain permite rastrear medicamentos desde su *Fabricación* hasta el paciente, lo que ayuda a reducir el problema de los medicamentos falsificados.

2.4.6 Propiedad Intelectual y Derechos de Autor

Blockchain ofrece una solución efectiva para la protección de propiedad intelectual y derechos de autor, permitiendo a los creadores registrar sus obras de manera segura y transparente. Los derechos sobre las creaciones (música, arte, escritos, etc.) se pueden almacenar en la Blockchain, lo cual facilita la verificación de la autoría y evita el plagio.

Esto ofrece ventajas para la Propiedad Intelectual, ya que permite:

- Verificación de Autenticidad: Cada obra registrada en la Blockchain puede ser rastreada y verificada como original.

- Transparencia en la Distribución de Derechos: La Blockchain permite realizar pagos automáticos y justos a los creadores por el uso de sus obras.

2.4.7 Seguros

La Blockchain también se emplea en el sector de los seguros para simplificar y automatizar los procesos de reclamaciones, reduciendo el fraude y mejorando la eficiencia. Los contratos inteligentes en Blockchain permiten la ejecución automática de pagos de seguros al cumplir ciertas condiciones, eliminando la necesidad de intervención manual.

- Aplicaciones en Seguros:
 - Automatización de Reclamaciones: Los contratos inteligentes permiten que las reclamaciones se procesen automáticamente, reduciendo el tiempo de espera y minimizando el fraude.
 - Transparencia y Verificación: Cada póliza y transacción se registra en la Blockchain, permitiendo a los asegurados y aseguradoras verificar el estado de las reclamaciones y las condiciones de la póliza.
- Ejemplo: Aseguradoras como AXA han implementado contratos inteligentes para el pago automático de indemnizaciones en casos de retrasos de vuelos.

2.4.8 Adopción en Nuevas Áreas

La tecnología Blockchain está extendiendo su impacto a diversos sectores más allá de las criptomonedas, demostrando su potencial para transformar procesos, mejorar la transparencia y aumentar la seguridad en distintos ámbitos. Blockchain se está convirtiendo en una herramienta fundamental para abordar problemas de confianza, ineficiencia y seguridad en un mundo cada vez más interconectado.

En este sentido, se puede destacar como área clave donde Blockchain está comenzando a ofrecer soluciones innovadoras y a habilitar nuevas oportunidades para el desarrollo y la eficiencia, su uso en el área conocida como internet de las cosas (IoT), de tal modo que la combinación de Blockchain con IoT promete mejorar la seguridad y la gestión de datos en un entorno donde miles de millones de dispositivos están interconectados. Blockchain puede proporcionar un marco seguro para la comunicación y la transacción entre dispositivos IoT, facilitando el desarrollo de "ciudades inteligentes" y sistemas autónomos.

Como se puede ver, la capacidad de Blockchain para proporcionar seguridad, transparencia, y eficiencia ha llevado a su adopción en una amplia gama de industrias, desde las finanzas hasta la cadena de suministro, la salud, y más allá. A medida que la tecnología sigue evolucionando, es probable que se vea un crecimiento continuo en su adopción y la aparición de nuevas aplicaciones que aprovechen las propiedades únicas de Blockchain. Esta tecnología tiene el potencial de transformar profundamente la forma en que operan las industrias y gestionar datos y transacciones, abriendo nuevas posibilidades para la innovación y la eficiencia en una economía cada vez más digital y globalizada.

3 LA CADENA DE CUSTODIA: CARACTERIZACIÓN Y FUNDAMENTOS

3.1 Análisis jurisprudencial

3.1.1 *Doctrina General de Tribunal Supremo (TS) sobre la cadena de custodia*

La Sentencia del Tribunal Supremo (STS) 241/2024, de 13 de marzo, Fundamento Jurídico (FJ) 3, sintetiza la reiterada doctrina recogida en la sentencia núm. 513/2018, de 30 de octubre, con referencia expresa a las sentencias núm. 6/2010, de 27 de enero; 1045/2011, de 14 de octubre; 776/2011, de 20 de julio y 347/2012, de 25 de abril sobre la cadena de custodia. En este sentido, dice lo siguiente:

"El problema que plantea la 'cadena de custodia' es garantizar que, desde que se recogen los vestigios relacionados con el delito, hasta que llegan a concretarse como pruebas en el momento del juicio, aquello sobre lo que recaerá la inmediación, publicidad y contradicción de las partes y el juicio del tribunal, es lo mismo. Es a través de la cadena de custodia como se satisface la 'mismidad' de la prueba, pues al tener que pasar la sustancia intervenida por distintos lugares para que se verifiquen los distintos exámenes, es necesario tener la seguridad de que lo que se traslada y analiza es lo mismo en todo momento, desde que se intervienen hasta el momento final que se estudia y analiza y, en su caso, se destruye.

Lo hallado debe ser descrito y tomado con las debidas garantías, puesto en depósito y con las debidas garantías, y analizado con las debidas garantías. El art. 318 LECrim. previene que 'los instrumentos, armas y efectos a los que se refiere el art. 334 se sellarán si fuera posible y se acordará su retención, conservación o envío al organismo adecuado para su depósito. (...)

Ahora bien, existe la presunción de que lo recabado por el juez, el perito o la Policía se corresponde con lo presentado el día del juicio como prueba, salvo que exista una sospecha razonable de que hubiese habido algún tipo de posible manipulación.

Por ello, en STS 4.6.2010 hemos dicho que la irregularidad de la cadena de custodia, de ser ese el caso, no constituye, de por sí, vulneración de derecho fundamental alguno que tan solo vendría dado por el hecho de admitir y dar valor a una prueba que se hubiera producido sin respetar las garantías esenciales del procedimiento y especialmente, el derecho de defensa, y en segundo lugar, que las formas que han de respetarse en las tareas de ocupación, conservación, manipulación, transporte y entrega en el

laboratorio de destino de la sustancia objeto de examen, que es el proceso al que denominamos genéricamente ‘cadena de custodia’, no tiene sino un carácter meramente instrumental, es decir, que tan sólo sirve para garantizar que la analizada es la misma e íntegra materia ocupada, generalmente, al inicio de las actuaciones. De modo que, a pesar de la comisión de algún posible error, ello no supone, por sí solo, sustento racional y suficiente para sospechar siquiera que la analizada no fuera aquella sustancia originaria, ni para negar el valor probatorio de los análisis y sus posteriores resultados, debidamente documentados”.

Continúa el Alto Tribunal mencionando que, “en cuanto a la cadena de custodia, hemos manifestado –entre otras, la STS 277/2016, de 6 de abril– que ‘la cadena de custodia no es un fin en sí mismo, sino que tiene un valor instrumental, lo único que garantiza es la indemnidad de las evidencias desde que son recogidas hasta que son analizadas, lo que en caso de quiebra puede afectar a la credibilidad del análisis, pero no a su validez.

Constituye un sistema formal de garantía que tiene por finalidad dejar constancia de todas las actividades llevadas a cabo por cada una de las personas que se ponen en contacto con las evidencias. De ese modo la cadena de custodia sirve de garantía formal de la autenticidad e indemnidad de la prueba pericial. No es prueba en sí misma. La infracción de la cadena de custodia afecta a lo que se denomina verosimilitud de la prueba pericial y, en consecuencia, a su legitimidad y validez para servir de prueba de cargo en el proceso penal. Por ello la cadena de custodia constituye una garantía de que las evidencias que se analizan y cuyos resultados se contienen en el dictamen pericial son las mismas que se recogieron durante la investigación criminal, de modo que no existan dudas sobre el objeto de dicha prueba pericial. A este respecto resulta evidente la relación entre la cadena de custodia y la prueba pericial, por cuanto la validez de los resultados de la pericia depende de la garantía sobre la procedencia y contenido de lo que es objeto de análisis.

Por otro lado, hemos manifestado que ‘la cadena de custodia sirve para acreditar la ‘mismidad’ del objeto analizado, la correspondencia entre el efecto y el análisis o informe, su autenticidad. No es presupuesto de validez sino de fiabilidad. Cuando se rompe la cadena de custodia no nos adentramos en el campo de la ilicitud o inutilizabilidad probatoria, sino en el de la menor fiabilidad (menoscabada o incluso aniquilada) por no haberse respetado algunas garantías. Son dos planos distintos. La ilicitud no es subsanable. Otra cosa es que haya pruebas que por su cierta autonomía escapen del efecto contaminador de la vulneración del derecho (desconexión causal o desconexión de antijuricidad). Sin embargo, la ausencia de algunas garantías normativas, como pueden ser las reglas que aseguran la cadena de custodia, lo que lleva es a cotejar todo el material probatorio para resolver si han surgido dudas probatorias que siempre han de ser resueltas en favor de la parte pasiva; pero no a descalificar sin más indagaciones ese material probatorio’ (STS 277/2016, de 6 abril con cita de la STS 777/2013, de 7 de octubre)”. [11]

El ATS 3443/2024, de 8 de febrero, ECLI:ES:TS:2024:3443A, FJ Único, considera “que el reproche en cuanto a una posible ruptura de la cadena de custodia solo surte efecto sobre el valor probatorio, cuando se acredita que existe un lapso, más o menos largo, en el que los efectos o instrumentos del delito (en este caso las tijeras) han estado fuera del control policial o judicial, ...”.

Por tanto, la doctrina del Tribunal Supremo sobre la cadena de custodia establece un marco claro y riguroso para asegurar la autenticidad e integridad de las pruebas desde su recolección hasta su análisis en juicio. Según el Tribunal, la cadena de custodia tiene un rol instrumental y no constituye una prueba en sí misma, sino un medio para garantizar que la evidencia analizada es la misma que fue inicialmente recogida. La ruptura en la cadena de custodia no implica automáticamente la invalidez de la prueba, sino que afecta su fiabilidad y credibilidad. Solo en casos donde haya una justificación razonable para dudar de la autenticidad de la evidencia o una sospecha concreta de manipulación se cuestionaría su validez. De este modo, la cadena de custodia se interpreta como una garantía formal de la “mismidad” de la prueba, asegurando la legitimidad del análisis pericial en el proceso penal, pero sin llegar a invalidar la prueba en caso de fallos menores que no afecten de manera sustancial a su autenticidad.

No obstante, recurrir a la ruptura o a la vulneración de la cadena de custodia es una de las principales estrategias de la defensa en los procedimientos del ámbito penal, sobre todo en lo que respecta al tráfico de drogas. En este sentido, en 2024, de los 50 autos del tribunal supremo en los que se alude la ruptura de la cadena de custodia, un 84% estaban relacionados con este tipo de delito [12].

3.1.2 Presunción de validez en la conservación de la cadena de custodia

La presunción de validez en la conservación de la cadena de custodia refuerza la confianza en la integridad de las pruebas bajo custodia judicial, partiendo del principio de que dicha cadena ha sido respetada salvo prueba en contrario.

Así se recoge en la STS 131/2024, FJ 3, en la que considera lo siguiente:

“En cuanto a la cadena de custodia, en principio hay que suponer que se ha respetado: es quien alega lo contrario quien deberá expresar por qué duda de su corrección. Es absurdo especular con extravagantes hipótesis consistentes en una trama policial que hubiera sustituido el colchón realmente usado o la toalla por otros elementos en los que -no se sabe cómo- hubiesen podido dejar restos biológicos inculpativos y, además, absurdamente, no del todo concluyentes cuando nada impedía que fuesen definitivos. Si fuese así, lo sencillo era contaminar esos efectos y documentar de forma tan burocrática como inútil el traslado de esos elementos (con impresos en que constasen los agentes que las portan y a quien las entregan). Esa tarea no aportaría nada: si la alternativa es que la Guardia Civil pudo manipular los efectos o sustituirlos por otros, entonces que hubiesen escondido esa actuación - ¡delictiva! - con unos protocolos bien rellenos y firmados, tampoco garantizaría nada.

La imprecisión o no plasmación minuciosa del sucesivo traslado de objetos incautados no es fórmula que por sí misma sirva para negar virtualidad probatoria a esos efectos. Será necesario que surjan dudas de que no se ha respetado esa garantía suficiente para desvirtuar la fiabilidad probatoria del concreto elemento. Ningún esfuerzo argumentativo hace en ese sentido el recurrente”.

La presunción de validez en la conservación de la cadena de custodia establece que, en principio, debe asumirse que dicha cadena se ha respetado, y corresponde a quien la impugna demostrar razones concretas para dudar de su corrección. El Tribunal rechaza hipótesis infundadas o especulaciones sobre posibles manipulaciones de la evidencia por parte de las autoridades sin pruebas que sustenten tales acusaciones. La simple falta de documentación detallada de cada paso en el traslado de los objetos incautados no es suficiente para invalidar su valor probatorio. Para cuestionar la fiabilidad de la evidencia, es necesario aportar argumentos sólidos que generen dudas razonables sobre la integridad de los elementos custodiados.

3.1.3 Cadena de custodia aplicada a la prueba electrónica

El Auto del TS (ATS) 3522/2024, de 14 de marzo, FJ 1, aporta un análisis detallado sobre la cadena de custodia aplicada a la prueba electrónica, subrayando los procedimientos legales y las garantías técnicas empleadas para preservar la integridad de las evidencias. En este caso, relacionado con delitos de pornografía infantil, se cuestionó la validez del manejo de los equipos informáticos incautados por la Guardia Civil, argumentando posibles irregularidades en el desprecinto, clonado y nuevo precinto de las pruebas sin presencia judicial. El TS inadmite el motivo con el siguiente razonamiento:

“En lo que respecta a que la Policía ha tenido bajo su control los equipos informáticos incautados y que los han precintado y desprecintado a su voluntad sin autorización ni presencia judicial, el Tribunal Superior de Justicia dispone que las actuaciones realizadas han sido ajustadas a lo dispuesto por el art. 588 sexies c) LECRIM y el auto habilitante de la entrada y registro de 23 de mayo, que dispuso que ‘se faculta expresamente a la fuerza actuante para que se adopten medidas de investigación tecnológica limitativas de derechos fundamentales, así, la intervención de cuanta documentación, material o soporte informático, teléfonos móviles, *tablets*, agendas, cartas, fax, correo electrónico y otros que puedan servir, para acreditar la autoría del delito investigado; la práctica del clonado de cuantos soportes de

almacenamiento digital sean intervenidos durante el registro, llevándose a cabo esta práctica en sede policial de forma inmediata a su intervención con el fin de proceder al análisis del contenido de los dispositivos intervenidos con la mayor celeridad posible'. De esto, se infiere, razona el órgano de apelación, que no solo se autoriza a recoger esa información, sino que a la par se acuerda que los efectos incautados queden bajo la custodia de los agentes intervinientes, lo cual no es objetable, ya que no existe obligación legal de que los equipos incautados queden bajo la custodia del Letrado de la Administración de Justicia (LAJ) o deban ser depositados en dependencias judiciales.

El Tribunal Superior de Justicia esgrime que lo que realmente está alegando el recurrente (aunque en el recurso de casación lo niegue) es una ruptura de la cadena de custodia, ya que, si cuestiona que se hayan precintado y desprecintado los equipos intervenidos en la entrada y registro sin la presencia de un Letrado de la Administración de Justicia (LAJ), es que, en definitiva, está denunciado que, con ese proceder, se ha podido alterar el contenido de los discos y demás material informático.

[...]

El Tribunal Superior de Justicia analiza dicha cadena de custodia y llega a la conclusión fundada de que ninguna irregularidad se produjo. Así, dispone que la Fuerza actuante, bajo cuya custodia quedaron los elementos incautados, estaba facultada en consecuencia para proceder a su precinto y desprecinto, de lo que se da cuenta en el 'Acta de desprecinto, clonado y nuevo precinto de evidencias', en la que, al describir el procedimiento llevado a cabo como garantía de esa identidad, se indica que 'para cada una de las evidencias, se realiza un desprecinto de la bolsa o sobre que la contiene, se extrae, se realiza el proceso de clonado o extracción de información, y por último se precinta de nuevo. En el acta se incluyen fotografías del precinto previo, la evidencia extraída de la bolsa o sobre, y del nuevo precinto realizado'.

El Tribunal Superior de Justicia analiza el sistema mediante el cual se garantiza que el contenido de los equipos incautados no ha sido alterado (el 'hash', que es una cadena alfanumérica, obtenida como resultado de aplicar una fórmula matemática al contenido del dispositivo, de modo que, si se repite el procedimiento de forma idéntica, se obtendrá el mismo resultado, lo que garantiza que la evidencia no ha sido alterada), y resalta que, si la defensa tenía cualquier reserva sobre la autenticidad de tal contenido, pudo a través de esa serie numérica comprobar hasta qué punto pudo haber sido objeto de algún tipo de alteración.

Finalmente, el Tribunal Superior de Justicia desataca un aspecto muy relevante, como es que, en todo caso, lo recogido fueron imágenes, tanto del acusado como de otras personas, que han podido ser identificadas y reconocidas visualmente durante la celebración del juicio.

Desde todo lo anterior, el Tribunal Superior de Justicia ha dispuesto razonada y lógicamente que no existe evidencia ninguna de que la Policía manipulase el contenido de los equipos incautados, por lo que ninguna indefensión se le ha provocado porque tales equipos se custodiasen en dependencias policiales en vez de judiciales, ni porque se desprecintasen y precintasen sin la presencia del Letrado de la Administración de Justicia, lo cual, en todo caso, no es exigible legalmente...".

De la sentencia expuesta se puede inferir que el Tribunal Superior de Justicia justifica que las actuaciones de la Policía respecto a la custodia de los equipos incautados se ajustaron al artículo 588 sexies c) de la Ley de Enjuiciamiento Criminal (LECRIM), que regula la autorización judicial para acceder a la información contenida en dispositivos electrónicos incautados durante una investigación, y al auto habilitante de la entrada y registro. Este auto autorizaba a los agentes, no solo a intervenir los dispositivos y clonar su contenido de manera inmediata, sino también a mantenerlos bajo su custodia. Además, aclara que no existe obligación legal de que dichos equipos sean custodiados por el Letrado de la Administración de Justicia o depositados en dependencias judiciales.

El Tribunal destaca que el procedimiento incluyó medidas para garantizar la integridad de las pruebas, como el registro en actas de cada desprecinto, clonado y nuevo precinto, acompañado de fotografías. También subraya el uso del sistema hash para verificar la autenticidad de las evidencias, permitiendo a la defensa comprobar la inalterabilidad del contenido, y, por tanto, la preservación de la

cadena de custodia en prueba electrónica. En conclusión, se considera que no hubo manipulación de las pruebas ni se causó indefensión al acusado, ya que el procedimiento fue ejecutado conforme a la normativa aplicable.

3.2 Aportaciones de la doctrina científica respecto a la cadena de custodia

En ausencia de una definición normativa de cadena de custodia, la doctrina científica ha aportado diversas caracterizaciones del concepto. En este sentido, (López-Valera, 2019) [13] desgana las notas características de la cadena de custodia de muestras de ADN, con base en reiterada jurisprudencia:

“Control de la prueba; o mecanismo tendente a comprobar, inspeccionar e intervenir legalmente las fuentes de prueba conforme a un protocolo preestablecido para todo el íter de la prueba dando validez y fiabilidad a la misma.

Trazabilidad de las evidencias; o tracto sucesivo o continuado en todo momento de los objetos y muestras biológicas custodiadas y analizadas, dejando constancia de todas las actividades llevadas a cabo por cada una de las personas que han estado en contacto con las muestras de ADN.

Acreditación documental; de todas las operaciones y personas que individualmente recogieron, transportaron, custodiaron, conservaron, analizaron, depositaron y destruyeron las evidencias o los resultados de su análisis.

Mismidad de la prueba; garantía o certeza de que lo que se traslada y analiza es idéntico en todo momento, o que las evidencias sujetas a los principios procesales de inmediación, publicidad y contradicción de las partes para constituirse en prueba a juicio de los juzgadores, es lo mismo en todo momento.

Autenticidad, Integridad e Indemnidad de las evidencias; encontrándose siempre acreditadas o ciertas, de forma completa en todas sus partes y sin sufrir daño alguno o menoscabo que las pueda contaminar, alterar, sustituir, deteriorar o destruir.

Licitud, Legitimidad y Validez de las pruebas; obteniendo y manipulando las muestras respetando escrupulosamente la legalidad vigente, así como los derechos fundamentales de las personas afectadas.

Fiabilidad; empleando los medios técnicos y científicos correctos y más idóneos para análisis de las muestras, incluidos los informes o resultados periciales finales resultantes de éstos.

Verosimilitud de las evidencias; de forma que las muestras y resultados de sus análisis custodiados sean fiables y creíbles, con la finalidad de que sirvan de prueba de cargo o de descargo en el proceso penal.

Vigilancia o Custodia; cuando las evidencias se hallan bajo posesión u observación de una persona física idónea, o guardada en un lugar seguro y accesible sólo a personas autorizadas para su manipulación”.

Por su parte, (Soleto-Muñoz, 2009) [14], en relación con las pruebas de ADN, indica que “la norma ISO/IEC 17025 para laboratorios de ensayo [...] establece normas que garantizan la cadena de custodia: cada muestra recibida debe estar perfectamente identificada y relacionada con el ensayo y los resultados obtenidos, y se anotan detalles correspondientes al análisis, como los lotes de reactivos utilizados, métodos y equipos empleados, fecha y firma de la persona que realiza el análisis y cualquier incidencia que haya acontecido durante el proceso”, lo que refuerza diversas de las características anteriormente mencionadas.

Así, (López-Jara, 2020) [15] entiende por cadena de custodia “el proceso que transcurre desde que los agentes policiales intervienen un efecto del delito que puede servir como prueba de cargo, hasta que se procede a su análisis, exposición o examen en la instrucción o en el juicio. Proceso que debe garantizar que el efecto que se ocupó es el mismo que se analiza o expone y que no se han producido alteraciones,

manipulaciones o sustituciones, intencionadas o descuidadas (SSTS 581/2017, de 19 de julio y 491/2016, de 8 de junio, entre otras muchas)”, tratándose por tanto de un concepto material y no formal, “orientado a una finalidad muy concreta, –el *mimismo*– debiendo dejarse constancia en las actuaciones de todos los eslabones, de todos los pasos –al menos los más relevantes– de bien o muestra de que se trate, así como de la identificación de todos –agentes, otros profesionales y particulares– que de una u otra forma hayan actuado o participado en esa cadena” [15].

Este autor reseña que “la cadena de custodia no es una prueba en sí, es un instrumento al servicio de la prueba”, añadiendo que “la quiebra de la cadena de custodia no determina la nulidad de la prueba, sino que afecta a su credibilidad, de modo tal que, si se duda del *mimismo*, será apartada del material probatorio del que dispone el tribunal para sustentar una condena. Aunque no toda irregularidad en la cadena de custodia tendrá esa consecuencia. Sólo aquellas más significativas capaces de infundir esas serias dudas en el tribunal” [15].

Y recuerda que “no es suficiente la mera sospecha o alegación de ruptura de la cadena, quien lo alegue deberá concretar en qué momento, con qué intensidad y qué consecuencias habría tenido la irregularidad denunciada, pues se parte de la presunción de que las fuerzas policiales y los tribunales actúan con respeto a la Ley, sin que el derecho a la presunción de inocencia se extienda a presumir una actuación ilegal de aquellos” [15].

Desde la óptica de la práctica, (Luque et al, 2018) presentan una propuesta concreta para elaborar el documento de cadena de custodia en las investigaciones sobre antropología forense teniendo en cuenta diversos formularios consultados, argumentando que es frecuente que este documento no se realice, o se cumpla de forma insuficiente, y ello puede suponer problemas en la garantía y trazabilidad de las muestras. Realizan una propuesta por la que los laboratorios forenses deban disponer de protocolos generales de actuación y también específicos para la toma de muestras, además de unos sistemas de registro que sean adecuados a las exigencias del ámbito judicial. Considerando que el documento relativo a la cadena de custodia de las evidencias es imprescindible en todos los casos, realizan una propuesta de contenidos muy completa.

3.3 La normativización de la cadena de custodia

Hasta la fecha no se ha regulado en el derecho español con carácter general la cadena de custodia, si bien se puede encontrar alguna norma sectorial, como la Orden JUS/1291/2010, de 13 de mayo, por la que se aprueban las normas para la preparación y remisión de muestras objeto de análisis por el Instituto Nacional de Toxicología y Ciencias Forenses, que viene a referirse a la cadena de custodia en los casos sujetos a su ámbito, de la que se dice que “registra todos los intervinientes en la toma y cadena de custodia de las muestras”.

Los recientes Anteproyecto de Ley de Enjuiciamiento Criminal de 2011 y el de 2020 [16] contienen propuestas relevantes, alineadas con la jurisprudencia, que cabe considerar. Más en concreto, el Anteproyecto de 2020 [16] regula, en relación con el “cuerpo del delito”, el tratamiento de la cadena de custodia, que “comienza con la misma obtención de la fuente de prueba, distinguiéndose, en particular, los procedimientos de gestión de muestras –que, por su carácter técnico, deben ser objeto del correspondiente desarrollo reglamentario– de los datos que, en todo caso, han de quedar expresamente registrados para asegurar la integridad de la muestra a lo largo del procedimiento. De esta forma, ha de quedar en todo caso garantizado que el tracto de la muestra pueda ser perfectamente reconstruido sin solución de continuidad” (preámbulo).

A la cadena de custodia dedica los artículos 444 a 447, que se reproducen a continuación:

“Artículo 444. *Garantías de las fuentes de prueba.*

1. Todas las actuaciones tendentes a la localización, recogida, obtención, análisis, depósito y custodia de las fuentes de prueba deberán realizarse en la forma prevista en esta ley y en las demás disposiciones que resulten aplicables.

2. Todas las fuentes de prueba obtenidas durante la investigación de los hechos delictivos serán debidamente custodiadas, a fin de asegurar su disponibilidad en el acto del juicio oral con los efectos que esta ley establece.

Artículo 445. *Cadena de custodia.*

1. La cadena de custodia se inicia en el lugar y momento en los que se obtiene o encuentra la fuente de prueba.

2. Corresponde a todos cuantos tengan relación con la fuente de prueba, sean funcionarios públicos o particulares, la obligación de constituir, aplicar y mantener la cadena de custodia, garantizando la inalterabilidad de la fuente de prueba.

3. Si por la naturaleza de la actuación o por las técnicas que hayan de aplicarse para su recogida, inspección, análisis o depósito hubieran de producirse alteraciones en el estado original de las muestras o efectos intervenidos, se dejará debida constancia de ello en las actuaciones.

Artículo 446. *Procedimiento de gestión de muestras.*

1. A fin de garantizar su debida conservación, se establecerán reglamentariamente los procedimientos de gestión y custodia de muestras.

Estos procedimientos habrán de ser observados por las instituciones y las personas que tengan relación con las fuentes de prueba.

2. En todo caso, se dejará constancia de los siguientes particulares:

- a) La persona y el lugar en el que se localizó la muestra y la documentación del hallazgo.
- b) Todas las personas que la hayan tenido a su cargo y los lugares en los que haya estado guardada, depositada o almacenada.
- c) El tiempo que haya estado en poder de cada persona o depositada en un determinado lugar.
- d) El motivo por el que la fuente de prueba ha sido enviada a otro lugar o ha pasado a manos de otras personas.
- e) Las personas que hayan accedido a las fuentes de prueba, detallando en su caso las técnicas científicas aplicadas y el estado inicial y final de las muestras.

3. Para el cumplimiento de lo dispuesto en el apartado anterior, cada una de las personas o instituciones que hayan intervenido en la gestión y custodia de la muestra documentará su intervención en la cadena de custodia.

Artículo 447. *Efectos de la cadena de custodia.*

1. El cumplimiento de los procedimientos de gestión y custodia determinará la autenticidad de la fuente de prueba llevada al juicio oral y, en su caso, justificará sus alteraciones o modificaciones.

2. El quebrantamiento de la cadena de custodia será valorado por el tribunal a los efectos de determinar la fiabilidad de la fuente de prueba.

3. La cadena de custodia podrá ser impugnada en el trámite de admisión de la prueba alegando el incumplimiento de los procedimientos de gestión y custodia de las muestras”.

Mientras no se regule con carácter general la cadena de custodia, y “ante la ausencia de dicho marco legal, la jurisprudencia admite que la regularidad de la cadena de custodia pueda acreditarse documentalmentemente o mediante testimonio”, por lo que “en muchas ocasiones las omisiones o deficiencias en la cadena de custodia podrán ser salvadas, subsanadas o aclaradas por el testimonio –una explicación razonable o atendible- de los agentes que hubieran intervenido, para ello es preciso que sean propuestos como testigos y traídos a juicio” [15].

4 EL RECONOCIMIENTO JURÍDICO DE LAS TECNOLOGÍAS DE REGISTRO DISTRIBUIDO

Las tecnologías de registro distribuido (*distributed ledger technologies*, o DLT) y, en particular, la tecnología Blockchain, como viene reseñándose a lo largo de este trabajo, permite la creación de un registro inalterable y gestionado de forma descentralizada, que permite nuevas aplicaciones con potencial transformador. Por este motivo, se considera una tecnología de tipo disruptivo, que ofrece oportunidades de innovación en diversos campos, pero siempre que reciba reconocimiento jurídico. Hay que tener en cuenta que, en el ámbito judicial, deben ser los jueces y tribunales los que determinen que el procedimiento que sea utilizado en la preservación de la cadena de custodia es admitido en derecho.

Desde este punto, en primer lugar, conviene presentar algunas nociones terminológicas, tanto relativas a los libros mayores electrónicos distribuidos (la categoría general que agrupa los diferentes enfoques tecnológicos), como de las cadenas de bloques (una categoría concreta de implementaciones tecnológicas de libro mayor electrónico distribuido, que, como se verá, encadena los registros del libro mayor electrónico distribuido). Todos los conceptos que se mencionan en adelante proceden de la norma internacional ISO 22379, segunda edición. [17]

Un libro mayor electrónico (*electronic ledger*) es un almacén de información que contiene registros (*records*) de transacciones (*transactions*) que se pretenden finales, definitivos e inmutables. Hay que señalar que por *record* se entiende la definición contenida en la norma internacional ISO 30300 [18], donde este término se encuentra traducido como “documento”, siendo la información creada, recibida y conservada como evidencia y como activo para una organización o individuo, en el desarrollo de sus actividades o en virtud de sus obligaciones legales, lo que potencia la visión del libro mayor electrónico como soporte de verdaderos documentos. Más abstracta es la definición de transacción, que se caracteriza como la unidad más pequeña de un proceso de trabajo, que consiste en una o más secuencias de acciones requeridas para producir un resultado que cumple con las reglas de gobierno (de la transacción).

Las transacciones documentadas mediante el libro mayor electrónico se orientan a ser finales, definitivas e inmutables. Esta última (*immutability*) es definida como una propiedad de un libro mayor electrónico distribuido en cuya virtud los registros del libro mayor no pueden ser modificados o eliminados una vez añadido a dicho libro mayor distribuido. La definición anota que no forma parte de la propiedad de la inmutabilidad, de forma necesaria, que el libro mayor electrónico mantenga el orden

de las transacciones. Por su parte, respecto al carácter definitivo de un libro mayor electrónico (*finality*) se entiende el estado de un registro en el libro mayor electrónico que ha devenido irreversible y no puede ser modificado o eliminado.

Por fin, se llega a la definición de libro mayor electrónico distribuido (*distributed ledger*), que es el libro mayor compartido entre un conjunto de nodos de tecnología de libro mayor electrónico y sincronizado entre dichos nodos mediante un mecanismo de consenso. Esta definición contiene la nota de que un libro mayor electrónico distribuido se encuentra diseñado para ser inmutable y resistente a modificaciones, para permitir detectar las modificaciones y para permitir exclusivamente la adición de registros, debiendo contener registros de transacciones confirmadas y validadas. Una transacción confirmada es la que ha sido aceptada por consenso para su incorporación al libro mayor electrónico distribuido, mientras que una transacción validada es aquella en relación con la que se han comprobado y cumplen las condiciones exigibles de integridad.

Generalmente, un libro mayor distribuido almacena sus entradas en una serie de nodos en una red, en vez de en una sola ubicación, por lo que la idea general, por tanto, es que las transacciones documentadas mediante el libro mayor electrónico distribuido resultan confiables precisamente por la presencia de las propiedades que se acaban de mencionar, objetivo que puede lograrse empleando diversos enfoques técnicos, entre los cuales se encuentra el uso de la cadena de bloques (*Blockchain*), que la mencionada norma ISO define como un libro mayor electrónico distribuido con bloques confirmados organizados en una cadena secuencial de sólo adición, utilizando vínculos criptográficos. *Blockchain* no es un simple algoritmo, sino un constructo tecnológico y un protocolo habilitador que facilita la intermediación descentralizada de datos entre participantes. [19]

Como se ha venido exponiendo a lo largo de este documento, los bloques son estructuras de datos que contienen una cabecera de bloque y datos del bloque, variando en función de la tecnología de cadena de bloques empleada. La cabecera debe obligatoriamente incluir el vínculo criptográfico al bloque anterior, y puede incluir otros datos como sellos de tiempo o árboles de resúmenes criptográficos de las transacciones incorporadas al bloque.

Un protocolo válido debe garantizar que cada bloque esté vinculado criptográficamente a un bloque inmediatamente anterior que forme una secuencia única de bloques en el tiempo. La secuencia completa de bloques asociados criptográficamente forma una estructura de datos de solo adición accesible globalmente, la cadena de bloques, que proporciona la versión canónica del historial de transacciones global. En el ejemplo anterior, estas informaciones se contienen en la cabecera del bloque. [20]

Para garantizar que el proceso de actualización del libro mayor produzca como resultado un solo estado del libro mayor para un bloque determinado, los protocolos de Blockchain, como sucede en todo libro mayor electrónico distribuido, incluyen un mecanismo de consenso que proporciona un orden total de todas las transacciones dentro del bloque. La acción colectiva de todos los nodos en el sistema Blockchain funciona como un servidor de marca de tiempo que valida las transacciones pendientes y actualiza el estado actual del libro mayor agregando bloques secuencialmente al Blockchain.

Para implementar un libro mayor distribuido, por tanto, los sistemas de cadena de bloques requieren un mecanismo para distribuir nuevos bloques a todos los nodos, un mecanismo para validar transacciones y un mecanismo para garantizar la coherencia de todas las copias de la cadena de bloques.

Se habla de una Blockchain programable cuando la misma ofrece soporte a los denominados contratos inteligentes (*Smart contracts*). Como ya se ha comentado, un contrato inteligente es un programa definido por el usuario que se despliega y ejecuta en un sistema Blockchain, que puede expresar desencadenantes, condiciones y lógica de negocio para permitir transacciones programables complejas. Los contratos inteligentes se pueden implementar e invocar a través de transacciones, y todos los nodos conectados los ejecutan a través de la red Blockchain.

La firma del remitente de la transacción autoriza la carga útil de datos de una transacción para crear o ejecutar un contrato inteligente. La confianza en la correcta ejecución de los contratos inteligentes se

extiende directamente desde las transacciones regulares, ya que (i) se despliegan como datos en una transacción y, por lo tanto, son inmutables; (ii) todas sus entradas son a través de transacciones y del estado actual; (iii) su código es determinista; y (iv) los resultados de las transacciones se capturan en los árboles de estado y recibos, que forman parte del consenso.

En definitiva, las soluciones Blockchain permiten a las organizaciones de una red Blockchain mantener el control sobre sus actividades pero, al mismo tiempo, les permiten establecer una "verdad compartida y persistente" sobre el estado del proceso en un momento dado, verdad que permite la resolución de posibles conflictos que puedan surgir en un momento posterior, así como el uso de actualizaciones en la cadena de bloques como desencadenantes confiables para actividades posteriores [21].

4.1 Uso de las tecnologías de registro distribuido en el sector público

Como sucede con otras tecnologías, la tecnología de Blockchain ha ido evolucionando a lo largo del tiempo, que se puede segmentar considerando la Blockchain 1.0, o moneda digital, con Bitcoin como paradigma; la Blockchain 2.0 de los contratos y otras aplicaciones de mercados financieros; y la Blockchain 3.0 de las aplicaciones en general, incluyendo en particular el gobierno [5].

En relación con la moneda digital, debe señalarse que, hasta la fecha, solamente dos estados han implantado las criptomonedas como monedas de curso legal. Este es el caso de El Salvador (en el año 2021) y la República Centroafricana (en el año 2022). Este paso ha generado debate global y ha puesto a ambas naciones en el centro de la discusión sobre el futuro de las criptomonedas en las economías nacionales.

La adopción de Bitcoin por El Salvador y la República Centroafricana representa un experimento audaz en el panorama financiero global. Sin embargo, el éxito a largo plazo dependerá de cómo aborden los desafíos relacionados con la infraestructura, la educación financiera y la volatilidad de las criptomonedas.

Las Administraciones Públicas han empezado a introducir las tecnologías Blockchain en áreas en que los actores deben registrar transacciones descentralizadas; en particular, en entornos en que no todas las partes resultan dignas de confianza.

Respecto a los factores que determinan la adopción de Blockchain en el sector público, diversos autores [22] emplearon la teoría de la difusión de la innovación para examinar a los principales adoptantes de Blockchain a nivel del gobierno nacional en 2018. En su trabajo probador, enumeran seis factores para la adopción de Blockchain utilizando regresión logística: ciberseguridad, control de la corrupción, desarrollo del gobierno electrónico, eficacia gubernamental, estabilidad política y participación democrática. Su análisis mostró que la ciberseguridad, la eficacia del gobierno y la estabilidad política son predictores significativos. Los altos niveles de ciberseguridad y eficacia gubernamental aumentan la probabilidad de que los países adopten Blockchain, mientras que, paradójicamente, un mayor grado de estabilidad política disminuye la probabilidad de una adopción temprana de Blockchain.

Durante 2018, otros autores [23] realizaron un análisis relativo a la experimentación del uso de Blockchain por parte de los gobiernos, con el objetivo de mejorar la comprensión de cómo la tecnología de Blockchain puede afectar al sector público de forma práctica. Los proyectos analizados venían referidos a transferencias sociales y pensiones; documentos de ciudadanos y registros públicos y a componentes fundacionales relativos a la identidad digital y el cumplimiento regulatorio. En todos los casos, se emplearon las capacidades de notarización, base de datos compartida y automatización de flujos de trabajo, operando de forma mayoritaria en Blockchains permissionadas.

Estos autores consideran que, en general, los proyectos donde la transacción de Blockchain hace uso de datos procedentes de bases de datos gubernamentales centralizadas o de carteras criptográficas en

poder de los ciudadanos, han mostrado el valor de los libros mayores electrónicos distribuidos para superar cuellos de botella en procesos administrativos en que la certificación y verificación de datos se realiza tradicionalmente de forma manual, sin constituir una amenaza para los servicios públicos, sino un complemento de los mismos.

Concluyen que las implementaciones de Blockchain en el sector público buscan principalmente mejoras de eficiencia en el mantenimiento de registros y la gestión financiera; que los proyectos existentes experimentan con la aplicación automatizada de transacciones y nuevos modelos de prestación de servicios, que utilizan interfaces móviles y bases de datos compartidas; y que los resultados son prometedores y demuestran la capacidad de las cadenas de bloques para reducir la burocracia y los costos de los procesos administrativos y romper los silos entre las agencias gubernamentales. Asimismo, el estudio constata que estos habilitadores de eficiencia están disponibles principalmente en entornos permisionados, y que no necesitan reproducir la confianza, sino automatizar el intercambio de información entre nodos conocidos pertenecientes a diferentes socios del ecosistema.

Una forma de ver las aplicaciones gubernamentales y de servicio público basadas en Blockchain es considerar que las características inherentes de una Blockchain se pueden aprovechar para lograr dos servicios primitivos: un servicio notarial para sellar el tiempo y una plataforma de gestión de datos (entre múltiples partes) con una única fuente de verdad facilitada por la trazabilidad. Además, se ejecutan ciertos componentes básicos como la identidad digital, el registro digital, los certificados digitales, el servicio de contabilidad para almacenar interacciones o transacciones. Se trata de aplicaciones por derecho propio, pero además se apoyan entre sí, lo que da lugar a un cierto grado de entrelazamiento entre los módulos, por ejemplo, la identificación digital y los servicios de registro son interdependientes; además, habilitan otras aplicaciones superpuestas que aprovechen estas primitivas y bloques de creación subyacentes [24].

La tecnología de registro electrónico distribuido resulta particularmente apropiada para la gestión de registros y de documentos, presentando un potencial significativo para la transformación de la gestión documental segura en el sector público, en especial en lo relativo a las firmas digitales, los certificados y la autenticación de documentos [25], consideración que resulta aplicable también a otros sectores. Sin embargo, no se puede olvidar que esta tecnología presenta limitaciones inherentes, tanto tecnológicas como socioeconómicas, especialmente en función del mecanismo de consenso utilizado y del modelo de gobernanza de la red, que deben ser objeto de consideración antes de adoptar su uso generalizado [26].

Las tecnologías de registro distribuido ofrecen importantes posibilidades de innovación en la gestión de documentos, en especial en relación con las transacciones de datos y de los documentos, externos a esta, que las mismas sustentan. Sin embargo, el libro mayor electrónico es también un objeto con valor documental, que se debe tratar adecuadamente, y sujeto a necesidades de conservación, igual que sucede con los documentos electrónicos, lo que exige la adopción de las correspondientes prácticas, por ejemplo, para su conservación.

4.2 La regulación del libro mayor electrónico como servicio de confianza

La acreditación de la existencia de transacciones y de documentos con base en el libro mayor electrónico distribuido puede transformar la forma en la que se generan, intercambian y capturan los documentos y, lo que es más importante, las evidencias acerca de los eventos acerca de los documentos, que en la actualidad se encuentran centralizadas en bases de datos o, en demasiados casos, simplemente no se capturan. Más aún, nos encontramos ante una tecnología que realmente permite innovaciones disruptivas, también en el sector público.

Sin embargo, para que se pueda confiar en estas tecnologías, es ineludible que las mismas ofrezcan garantías apropiadas, y a pesar de que existen diversas opciones para “regular lo desconocido”, resulta oportuno y conveniente proceder al establecimiento de un marco regulatorio.

El 3 de junio de 2021, la Comisión presentó la propuesta de modificación del Reglamento eIDAS, para establecer un marco para la Identidad Digital Europea (COM (2021) 281 final, en adelante, “Reglamento eIDAS 2”), y que viene, entre otras cuestiones, a regular los libros mayores electrónicos, incluyendo aquellos basados en Blockchain. El Reglamento eIDAS 2 ha sido aprobado por el Parlamento Europeo y el Consejo, mediante su firma el 11 de abril de 2024.

De forma novedosa, el Reglamento eIDAS 2 contiene una regulación del libro mayor electrónico (*electronic ledger*). La necesidad de establecer este régimen jurídico se viene a mencionar en la memoria que acompaña a la propuesta de Reglamento eIDAS 2, que describe cómo los libros mayores electrónicos proporcionan a los usuarios una evidencia confiable y una pista de auditoría permanente para la ordenación de transacciones y registros, asegurando la preservación de la integridad de los datos.

Entre los casos de uso que se citan se encuentra la inscripción de la propiedad de bienes inmuebles en registros descentralizados de la propiedad inmobiliaria, el voto electrónico y la cooperación transfronteriza de las autoridades aduaneras o de las instituciones académicas. Asimismo, la propuesta enfatiza que, al objeto de prevenir la fragmentación, es necesario definir un único marco paneuropeo que permita el reconocimiento transfronterizo de los servicios de confianza que ofrezcan soporte a la operación de los libros mayores electrónicos, algo que es especialmente relevante cuando el enfoque técnico sea el de un libro mayor electrónico distribuido como Blockchain.

No es la primera vez que se propone una regulación generalista de *Blockchain* como tal, como en Italia con el decreto-ley 135/2018 (convalidado por Ley 12/2019) otorgando a estas tecnologías efecto jurídico equivalente al sello electrónico de tiempo, pero se trata de la primera ocasión en la que se propone una visión completa, con un enfoque neutral que también incluye soluciones centralizadas, incluyendo la definición del concepto, de un servicio de confianza (el registro de datos electrónicos en un libro mayor electrónico), y el establecimiento de los requisitos y de los efectos jurídicos de dicho servicio, además de la aplicación de las exigencias comunes a todos los servicios de confianza.

La definición del libro mayor electrónico se refiere a una secuencia de registros electrónicos de datos, asegurando su integridad y la exactitud de su orden cronológico, en una aproximación tecnológicamente neutral, que permite sistemas centralizados y distribuidos, como el Blockchain.

El Reglamento eIDAS 2 establece los requisitos que deben cumplir los libros mayores electrónicos cualificados; a saber, que los mismos sean creados y gestionados por uno o varios proveedores de servicios de confianza cualificados; que establezcan el origen de los registros de datos en el libro mayor; que garanticen el orden cronológico secuencial único de los registros de datos en el libro mayor; y que registren los datos de tal manera que cualquier cambio posterior en los datos sea inmediatamente detectable, asegurando su integridad a lo largo del tiempo.

Siguiendo la lógica normativa y el enfoque de doble nivel propio del Reglamento eIDAS [27], se garantiza, en primer lugar, que todo libro mayor electrónico se beneficiará del principio de no discriminación, por lo que podrá acceder al procedimiento y, en su caso, producir efectos; mientras que, en el caso de que el libro mayor electrónico sea cualificado, gozará de la presunción de su orden cronológico secuencial único y preciso y de su integridad (artículo 45 *duodecies* del Reglamento eIDAS modificado).

Este marco puede suponer la superación de algunas de las problemáticas que están impidiendo el despliegue de las soluciones basadas en Blockchain, en especial desde la óptica del uso de Blockchain como instrumento acreditativo y de transferencia de responsabilidad legal.

A diferencia de lo expresado por autores como (Anguiano-Jiménez, 2018) [28]., que se refiere a la necesaria decisión judicial en caso de controversia, atendiendo a la posible aceptación “*ad mathematicatem*” del procedimiento, es decir, por su carácter técnico y verificable, sin que sea preciso un análisis interpretativo adicional, el Reglamento eIDAS 2 presenta un enfoque radicalmente diferente

orientado a facilitar la adopción de estas tecnologías mediante su regulación como servicio de confianza, y el establecimiento de las correspondientes presunciones jurídicas.

La regulación del libro mayor electrónico es un imperativo en orden a su adopción fiable, en especial debido a la sustitución de los protocolos de consenso basados en prueba de trabajo por otros protocolos que no se basan en pruebas matemáticas intensivas, que además plantean desafíos de sostenibilidad medioambiental, como sucede con prueba de autoridad o prueba de participación.

Por otra parte, el Reglamento eIDAS 2 no aborda más que una pequeña parte de los desafíos jurídicos que plantea el uso de estas tecnologías, de los que da buena cuenta (Ibáñez-Jiménez, 2018) [29], por lo que, como se reconoce en el Reglamento eIDAS 2, esta norma paneuropea se aplicará sin perjuicio de otra legislación secundaria de la UE, por lo que, por ejemplo, cuando se utilicen libros mayores electrónicos para respaldar la emisión o negociación de bonos, o para criptoactivos, los casos de uso deberán ser compatibles con todas las normas financieras aplicables, como puede ser la Directiva sobre mercados de instrumentos financieros, la Directiva sobre servicios de pago y la Regulación de los mercados de criptoactivos.

Al hilo de esta cuestión, es necesario comentar la iniciativa europea sobre el euro digital. Junto con los bancos centrales nacionales de la zona del euro, se está estudiando la posibilidad de emitir un euro digital. Sería una moneda digital de banco central: un equivalente electrónico al efectivo. Ofrecería una opción adicional para realizar pagos que complementaría a los billetes y a las monedas. [30]

Y, por supuesto, cuando los casos de uso involucren datos personales, los proveedores de servicios deberán cumplir con la correspondiente normativa reguladora, posiblemente una de las cuestiones que más debate está generando, en particular desde la perspectiva de la posibilidad qué datos pueden ser considerados como no personales o datos seudonimizados, algo muy relevante cuando los mismos deben ser escritos en una Blockchain pública o pública permissionada. Otras discusiones relevantes en este contexto se refieren a la posibilidad de editar la *Blockchain* para retirar datos sensibles. No obstante, en el siguiente capítulo se abordará la cuestión de la protección de datos de carácter personal.

En conclusión, desde la entrada en vigor del Reglamento eIDAS 2, el acceso a los Tribunales de los registros de datos incorporados a un libro mayor electrónico (como es el caso de una *Blockchain*) se encuentra plenamente garantizado, siempre que, por supuesto, resulte útil y pertinente a efectos de prueba, lo que corresponde apreciar al órgano judicial, sin poder sufrir discriminación por razón de la tecnología empleada.

Y cuando se trate de un libro mayor electrónico, disfrutará de una presunción legal que traslada la carga de la prueba a quien cuestione la ordenación cronológica única o la integridad del libro mayor electrónico, lo que siempre resulta conveniente.

5 CONSIDERACIONES DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

Los tratamientos de datos personales relativos a la cadena de custodia se encuentran sujetos a la normativa reguladora correspondiente, si bien con particularidades que deben reseñarse.

El marco jurídico general está establecido en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, sobre la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, que derogó la Directiva 95/46/CE. También se encuentra regulado en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

Sin embargo, hay que referirse también a la Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales, cuyo artículo 1 establece que la Ley “tiene por objeto establecer las normas relativas a la protección de las personas físicas en lo que respecta al tratamiento de los datos de carácter personal por parte de las autoridades competentes, con fines de prevención, detección, investigación y enjuiciamiento de infracciones penales o de ejecución de sanciones penales, incluidas la protección y prevención frente a las amenazas contra la seguridad pública”.

A tenor del artículo 2.1 de la LO 7/2021, la ley “será de aplicación al tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero, realizado por las autoridades competentes, con fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales, incluidas la protección y prevención frente a las amenazas contra la seguridad pública”, mientras que, conforme al epígrafe 2 del propio artículo 2, “el tratamiento de los datos personales llevado a cabo con ocasión de la tramitación por los órganos judiciales y fiscalías de las actuaciones o procesos de los que sean competentes, así como el realizado dentro de la gestión de la Oficina judicial y fiscal, en el ámbito del artículo 1, se regirá por lo dispuesto en la presente Ley Orgánica, sin perjuicio de las disposiciones de la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial, las leyes procesales que le sean aplicables y, en su caso, por la Ley 50/1981, de 30 de diciembre, por la que se regula el Estatuto Orgánico del Ministerio Fiscal”.

Entre las autoridades competentes a los efectos de la LO 7/2021 se citan a las Fuerzas y Cuerpos de Seguridad (artículo 4.1.a) de la LO 7/2021).

La definición de tratamiento de datos recogida en el artículo 5.b) de la LO 7/2021 (“cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción”) incluye, como no puede ser de otra forma, las operaciones referidas a la cadena de custodia.

Respecto a la licitud del tratamiento, dispone el artículo 11.1 de la LO 7/2021, que “el tratamiento sólo será lícito en la medida en que sea necesario para los fines señalados en el artículo 1 y se realice por una autoridad competente en ejercicio de sus funciones”, por lo que el responsable del tratamiento ciertamente deberá poder justificar dicha necesidad. A estos efectos, juega un papel fundamental la ya mencionada jurisprudencia del Tribunal Supremo.

Además, también en este ámbito resultan aplicables los principios de protección de datos, recogidos en el artículo 6.1 de la LO 7/2021: principio de licitud del tratamiento, principio de finalidad, principio de proporcionalidad, principio de calidad, principio de minimización y principio de seguridad.

Particularmente relevante para las ulteriores operaciones de la cadena de custodia resulta el artículo 6.3 de la LO 7/2021, que autoriza que “los datos personales podrán ser tratados por el mismo responsable o por otro, para fines establecidos en el artículo 1 distintos de aquel para el que hayan sido recogidos, en la medida en que concurran cumulativamente las dos circunstancias siguientes: a) Que el responsable del tratamiento sea competente para tratar los datos para ese otro fin, de acuerdo con el Derecho de la Unión Europea o la legislación española. b) Que el tratamiento sea necesario y proporcionado para la consecución de ese otro fin, de acuerdo con el Derecho de la Unión Europea o la legislación española”.

En general, puede considerarse que la necesidad de sustentar la cadena de custodia en un libro mayor electrónico deriva de sus propiedades y efecto jurídico, resultando un sistema más idóneo para la protección de la información, como se ha expuesto anteriormente. Esto es especialmente así en el caso del libro mayor electrónico cualificado.

A la luz de las anteriores previsiones normativas, resulta especialmente necesario evaluar la viabilidad jurídica de registrar datos de carácter personal en un libro mayor electrónico, en especial tratándose de una Blockchain, en la medida en que dicha tecnología no permita borrar la información incorporada a la misma.

Hay que tener en cuenta que, en este sentido, también la LO 7/2021 prevé el derecho de supresión de los datos, si bien sólo “cuando el tratamiento infrinja los artículos 6, 11 o 13, o cuando los datos personales deban ser suprimidos en virtud de una obligación legal a la que esté sujeto” el responsable (artículo 23.2 de la LO 7/2021), pudiendo ser limitado el tratamiento de los datos que debieren ser suprimidos cuando “los datos personales hayan de conservarse a efectos probatorios” (artículo 23.3.b) de la LO 7/2021).

Este derecho de supresión (al igual que el de acceso) podrá ser denegado, total o parcialmente, “siempre que, teniendo en cuenta los derechos fundamentales y los intereses legítimos de la persona afectada, resulte necesario y proporcional para la consecución de los siguientes fines: a) Impedir que se obstaculicen indagaciones, investigaciones o procedimientos judiciales. b) Evitar que se cause perjuicio a la prevención, detección, investigación y enjuiciamiento de infracciones penales o a la ejecución de sanciones penales. [...]” (artículo 24.1 de la LO 7/2021), como ocurriría en el caso de la cadena de custodia.

En todo caso, no puede soslayarse que, en cierto momento, conforme a la normativa, deberá procederse a la supresión de la información de la cadena de custodia, lo que deberá permitir el sistema en cuestión, incluido el de *Blockchain*.

En este sentido, existen plataformas de Blockchain, como *Hyperledger Fabric*, que se abordará con mayor detenimiento en el capítulo 6, que ofrecen diversas capacidades técnicas en soporte de la implementación de controles de protección de datos, que pueden ser empleadas para garantizar el pleno cumplimiento de las exigencias de la normativa. (Brotsis et al, 2020) se refieren a dos de ellas:

- Uso de canales (*channels*): Un canal es una partición de estado con sus propias reglas de política de acceso y mecanismo de ordenación de transacciones. Cada canal es gestionado por un conjunto de pares y está asociado a algunas políticas que proporcionan acceso a los recursos correspondientes (como el estado del libro mayor, las transacciones incluidas en él y los códigos de cadena correspondientes). Cuando un par se registra en un canal, que se caracteriza por un identificador único, a continuación, se crea el libro mayor correspondiente y se ejecuta en este par, lo que le permite gestionar un almacén de datos idéntico y coherente con el resto de los pares del canal. Por lo tanto, los mecanismos de preservación de la privacidad, como los canales, son muy importantes en los casos de proporcionar soluciones de Blockchain en un entorno de consorcio (donde el consorcio está compuesto por una serie de organizaciones o partes con objetivos comerciales comunes).
- Recopilación de datos privados (*private data collection* o PDC): Si bien los canales se dedican a la preservación de la privacidad de la información, al permitir que la información se almacene por separado, la recopilación de datos privados (PDC) puede preservar la privacidad de los datos desde otra perspectiva. El PDC permite que solo un conjunto establecido de pares en un canal conserve los datos reales, mientras que los pares restantes solo acceden a su prueba de existencia. El PDC se crea para proporcionar a los pares las capacidades de respaldar, confirmar o consultar datos privados sin verse obligado a crear un nuevo canal y agregar sobrecarga adicional.

El PDC es en realidad una suma de los siguientes elementos: 1) los datos privados reales, que se envían desde/hacia pares autorizados por medio de un protocolo de propagación, almacenados en las bases de datos de estado privadas del par y solo pueden ser vistos por este conjunto de nodos, y 2) el hash de datos privados que se ejecuta ordena y almacena en el libro mayor de cada par como evidencia de la existencia de la transacción. En algunos casos de uso, cuando un par de un PDC desea compartir datos privados con otros pares, por ejemplo, para transferir cualquier activo a un tercero de confianza (TTP), el TTP puede producir el hash de los datos privados y, posteriormente, examinar si la salida del valor hash es consistente con el hash que se almacena en el libro mayor del canal y, por lo tanto, probar la existencia de la transacción. Es decir, el hash se utiliza como una prueba criptográfica de la existencia y la integridad de los datos privados asociados.

El "derecho al olvido" se puede utilizar en las transacciones privadas, ya que cada par puede borrar su propia base de datos privada en cualquier momento, eliminando los datos de forma irreversible, pero manteniendo el hash apuntando a la información privada subyacente. Un aspecto adicional que se implementa con las transacciones privadas es la limitación de uso. Se puede definir una política "*BlockToLive*" para cada PDC para determinar la cantidad de tiempo que debe transcurrir con la base de datos privada oculta para que se borre automáticamente.

La política "*BlockToLive*" se define como el período durante el cual un bloque de transacciones es considerado válido o útil en el contexto de su sistema.

En conclusión, un diseño adecuado de la solución basada en tecnología Blockchain que contemple estas capacidades puede dar satisfacción a las exigencias de la normativa de protección de datos. No

obstante, parece claro que en lo que a la protección de datos se refiere, la gobernanza de la red de Blockchain es primordial, en cuanto debe haber un exhaustivo control de quién debe acceder y a qué información debe acceder, una opción muy similar a las medidas que se adoptan respecto a los antecedentes policiales de los menores. Al contrario que los antecedentes policiales de personas mayores de edad, a los que cualquier Guardia Civil puede acceder, claro está siempre que sea necesario conocer, respecto a los menores, los datos no aparecen, debiendo solicitar al responsable del tratamiento de manera explícita, el acceso a los datos de un menor.

6 INICIATIVAS SOBRE TECNOLOGÍA BLOCKCHAIN EN EL SECTOR PÚBLICO

En este capítulo se va a profundizar en las iniciativas y proyectos piloto que se considera de mayor interés para la aplicación de la tecnología Blockchain en la cadena de custodia, dadas las funcionalidades que ofrecen estas soluciones. En concreto, se expondrán las principales características y capacidades de dos iniciativas, una a nivel europeo, y otra a nivel nacional, ambas opciones de gran interés para la propuesta de este trabajo.

6.1 Iniciativa Europea de Infraestructura de Servicios Blockchain (ESBI)

La Iniciativa Europea de Infraestructura de Servicios Blockchain (ESBI) es un proyecto en el que participan diferentes estados europeos y liderado por la Unión Europea que busca establecer una plataforma Blockchain para fomentar la cooperación digital entre los países miembros.

Según el informe "*Blockchain Strategy for Europe*" publicado por la Comisión Europea en 2018, Blockchain es clave para consolidar la soberanía digital y fomentar la confianza entre los Estados miembros (Comisión Europea, 2018). En este sentido, el principal objetivo de ESBI es proporcionar una infraestructura interoperable y sostenible que sirva como base para aplicaciones Blockchain a nivel europeo. Esto incluye garantizar que los Estados miembros puedan compartir datos y realizar transacciones de manera segura y eficiente, promoviendo la confianza y la innovación tecnológica en toda la región.

La ESBI pretende construir una red Blockchain de última generación que conecte a los Estados miembros, sus administraciones públicas y otros actores relevantes. Esta infraestructura estará diseñada para soportar aplicaciones tanto públicas como privadas, permitiendo una amplia gama de usos, desde la trazabilidad de productos hasta la gestión de identidades digitales. Uno de los mayores desafíos del uso de Blockchain a nivel paneuropeo es la interoperabilidad entre distintas soluciones tecnológicas. ESBI busca crear estándares comunes que permitan que diferentes sistemas interactúen sin problemas. Según un informe técnico del Centro Común de Investigación (JRC) de la UE, la falta de interoperabilidad es una barrera clave para la adopción de Blockchain a gran escala (JRC, 2020).

Garantizar la protección de los datos personales y la seguridad de las transacciones es fundamental para la confianza en esta tecnología. Por ello, ESBI se construirá bajo estrictos lineamientos de seguridad

y conformidad con el Reglamento General de Protección de Datos (GDPR), lo que asegura un enfoque europeo en la protección de los derechos digitales de los ciudadanos.

Se espera que la plataforma soporte una variedad de casos de uso, como identidades digitales soberanas, certificados académicos digitales, registros empresariales, trazabilidad de productos y contratos inteligentes. Esto impulsará tanto la eficiencia administrativa como la innovación en el sector privado. Un ejemplo notable es el proyecto piloto de certificados académicos digitales desarrollado en colaboración con universidades europeas, que demostró ser eficiente y seguro (Comisión Europea, 2021).

La ESBI es un esfuerzo colectivo en el que participan todos los países de la Unión Europea, junto con Noruega y Liechtenstein. Cada uno de estos países contribuye al desarrollo, implementación y gobernanza de la plataforma. Además, los Estados miembros tienen la oportunidad de integrar sus propias soluciones Blockchain dentro de la infraestructura común. Un aspecto central de esta colaboración es el "Nodo Nacional Blockchain", una instancia dedicada en cada país para garantizar la integración con los sistemas locales y la interoperabilidad a nivel europeo. Un estudio del Parlamento Europeo sobre el impacto de Blockchain en la gobernanza pública destaca que esta tecnología podría ahorrar hasta 27.000 millones de euros anuales en costos administrativos (Parlamento Europeo, 2020).

A pesar de sus promesas, la iniciativa enfrenta varios desafíos. Entre ellos, destacan:

- Adopción tecnológica:

Algunos Estados miembros pueden carecer de los recursos técnicos y financieros para implementar plenamente la tecnología Blockchain. Según la consultora tecnológica Gartner, existe una "brecha de madurez tecnológica" entre países europeos que podría dificultar la adopción uniforme de ESBI (Gartner, 2021).

- Regulación y gobernanza:

Establecer un marco legal y regulatorio armonizado a nivel europeo es esencial para el éxito del proyecto. La Comisión Europea ha señalado la necesidad de un marco legislativo claro para evitar discrepancias entre jurisdicciones nacionales.

- Escalabilidad:

La tecnología Blockchain enfrenta limitaciones en términos de capacidad y velocidad, aspectos que deben ser resueltos para manejar un gran volumen de transacciones. La ESBI está explorando soluciones como el uso de "Blockchains de segunda capa" para mejorar la escalabilidad sin comprometer la seguridad (Comisión Europea, 2021).

De cara al futuro, la ESBI tiene el potencial de convertirse en un modelo global para la adopción de Blockchain en servicios públicos. Su éxito dependerá de la cooperación continua entre los Estados miembros, la inversión en innovación y la resolución de los desafíos tecnológicos y regulatorios. Seguidamente, se describe someramente cómo se está construyendo técnicamente la plataforma ESBI.

6.1.1 Arquitectura basada en Blockchain permissionada

La ESBI utiliza una arquitectura de Blockchain permissionada, en la que los nodos participantes son entidades verificadas, como administraciones públicas y actores privados acreditados. Esto garantiza un entorno confiable y controlado.

- Tecnología base: La plataforma está basada en protocolos Blockchain adaptados, lo que permite flexibilidad en la implementación según los casos de uso. Es decir, ha sido adaptada o personalizada para cumplir con necesidades específicas o casos de uso concretos.
- Permisos y acceso: El control de acceso se gestiona mediante un sistema de identidades digitales verificadas que asigna roles específicos a cada participante.

6.1.2 Mecanismos de interoperabilidad

Uno de los objetivos clave de ESBI es garantizar la interoperabilidad entre los diferentes sistemas Blockchain nacionales y de terceros. Para lograrlo:

- Estándares comunes: Se están definiendo estándares europeos para garantizar que las diferentes soluciones Blockchain puedan comunicarse sin problemas.
- APIs abiertas: La infraestructura está desarrollando interfaces de programación abiertas que permiten a aplicaciones externas interactuar con la red.
- Puentes Blockchain: Se están implementando mecanismos de "*cross-chain*" para permitir el intercambio de datos y activos entre diferentes redes Blockchain.

Cross-chain es un término que se refiere a la capacidad de diferentes redes de Blockchain para interactuar, comunicarse y transferir información o activos entre sí. Dado que cada Blockchain suele operar de forma aislada con su propio conjunto de reglas, tokens y mecanismos de consenso, las soluciones cross-chain buscan superar estas barreras, permitiendo la interoperabilidad entre múltiples cadenas.

6.1.3 Infraestructura descentralizada

La red de ESBI está formada por nodos distribuidos entre los Estados miembros y otras entidades participantes. Estos nodos tienen funciones específicas:

- Nodos de validación: Verifican y validan las transacciones.
- Nodos de almacenamiento: Almacenan registros inmutables de datos.
- Nodos intermedios: Gestionan la comunicación entre diferentes redes y actores.

El enfoque descentralizado garantiza que ningún participante pueda monopolizar el control de la red, promoviendo transparencia y confianza.

6.1.4 Seguridad y privacidad

La EBSI adopta tecnologías y prácticas avanzadas para garantizar la protección de los datos personales, alineándose estrictamente con los requisitos del Reglamento General de Protección de Datos (RGPD) y otras normativas europeas relevantes. Estos mecanismos aseguran que la infraestructura Blockchain de la EBSI no solo cumpla con las regulaciones, sino que también establezca estándares de confianza y seguridad en el ecosistema digital europeo. A continuación, se exponen los puntos clave sobre los que se basará estos aspectos:

6.1.4.1 Cifrado de extremo a extremo:

La EBSI emplea cifrado de extremo a extremo (E2EE) para proteger la confidencialidad de los datos mientras están en tránsito (durante su transferencia entre nodos) y en reposo (almacenados en servidores o dispositivos).

Este mecanismo utiliza algoritmos de cifrado avanzados, como AES (*Advanced Encryption Standard*) o cifrado basado en curvas elípticas, garantizando que solo las partes autorizadas puedan acceder a los datos.

Impacto en la seguridad: Evita que actores malintencionados puedan interceptar o descifrar la información, incluso si logran acceder al canal de comunicación o almacenamiento.

6.1.4.2 Anonimización y Pseudonimización

La EBSI asegura que los datos sensibles se transformen de manera irreversible en un formato que no pueda vincularse a un individuo específico. Este proceso garantiza que, incluso si los datos almacenados en la Blockchain son accesibles, no se puede identificar a las personas relacionadas con esos datos.

Como, por ejemplo, se puede llevar a cabo la eliminación de identificadores como nombres, direcciones IP o números de identificación antes de registrar datos en la Blockchain.

En casos donde los datos necesitan mantenerse rastreables (por ejemplo, para validar identidades o autorizaciones), se utilizan técnicas de pseudonimización. Aquí, los identificadores directos se reemplazan por seudónimos o códigos que solo pueden relacionarse con la identidad real mediante información adicional que está estrictamente protegida.

En lo que respecta al impacto en el RGPD, esto permite procesar datos personales con mayores garantías de privacidad y minimiza riesgos en caso de violación de datos.

6.1.4.3 Gestión de Consentimientos

Esta iniciativa integra contratos inteligentes en su arquitectura, que actúan como herramientas automatizadas para garantizar el consentimiento explícito de los usuarios antes de que sus datos sean procesados.

Estos contratos registran el consentimiento de forma inmutable en la Blockchain, asegurando que las operaciones cumplan con los principios de transparencia, responsabilidad y revocabilidad establecidos por el RGPD.

Las funcionalidades principales que ofrece son:

- Gestión dinámica del consentimiento: Los usuarios pueden otorgar, revocar o actualizar su consentimiento en cualquier momento.
- Trazabilidad: Cada interacción relacionada con el consentimiento queda registrada en la Blockchain, creando un historial auditable.
- Automatización de políticas: Los contratos inteligentes verifican automáticamente si el consentimiento requerido está vigente antes de procesar cualquier dato.

6.1.4.4 Principios Adicionales de Seguridad y Privacidad

- Minimización de datos:
 - Se evita almacenar datos personales directamente en la Blockchain. En lugar de ello, se almacenan referencias hash de los datos, que actúan como identificadores únicos sin exponer información personal.
 - Los datos reales se mantienen en sistemas externos protegidos, y solo se vinculan a la Blockchain mediante estos hashes.
- Auditorías automatizadas:
 - La infraestructura permite realizar auditorías automáticas sobre el cumplimiento de los protocolos de privacidad y seguridad.
 - Esto incluye la supervisión de accesos, transacciones y manejo de datos sensibles.
- Cumplimiento con el derecho al olvido:
 - Aunque los datos registrados en una Blockchain pública son inmutables, la EBSI permite cumplir con el derecho al olvido a través de mecanismos de

"revocación de acceso" o anonimización avanzada, asegurando que los datos ya no sean accesibles o rastreables.

6.1.4.5 Gobernanza de la red

La gobernanza de la ESBI se basa en una estructura colaborativa entre los Estados miembros, la Comisión Europea y las organizaciones participantes. Las decisiones técnicas y operativas se toman mediante un modelo de consenso distribuido.

- Consorcio europeo: Cada país miembro gestiona su nodo nacional y participa activamente en el desarrollo y mantenimiento de la plataforma.
- Actualizaciones y mejoras: Se implementan de forma iterativa, permitiendo una evolución constante en base a las necesidades y avances tecnológicos.

6.1.4.6 Integración con tecnologías complementarias

La plataforma ESBI se construye para integrarse con otras tecnologías emergentes:

- Inteligencia artificial: Para análisis avanzados y automatización de procesos.
- Internet de las cosas (IoT): Para registrar datos en tiempo real provenientes de dispositivos conectados.
- *Cloud computing*: Almacenamiento complementario para datos off-chain.

En resumen, la ESBI es una iniciativa ambiciosa que combina tecnologías punteras, estándares europeos y un enfoque descentralizado para construir una infraestructura Blockchain robusta y escalable. Su éxito dependerá de la colaboración entre los Estados miembros, la implementación de estándares interoperables y la resolución de retos tecnológicos.

6.2 El Proyecto de la Fábrica Nacional de Moneda y Timbre (FNMT-RCM)

La FNMT-RCM, en colaboración con PwC, ha desarrollado una plataforma tecnológica que integra la tecnología Blockchain con los certificados de firma electrónica.

La integración de Blockchain con los certificados de firma electrónica busca garantizar una mayor integridad de los datos, ya que Blockchain crea registros inmutables y auditables

La plataforma busca proveer servicios digitales más seguros, transparentes y confiables, al tiempo que impulsa la modernización de la certificación electrónica mediante la tecnología Blockchain.

6.2.1 Características Técnicas de la Solución

1. Integración de Blockchain y Firma Electrónica:

- La plataforma combina la infraestructura de Blockchain con los certificados de firma electrónica emitidos por la FNMT-RCM.
- Cada transacción en la red lleva asociada una firma electrónica, garantizando que todos los registros estén firmados digitalmente por las partes implicadas.

2. Seguridad y No Repudio:

- Las transacciones firmadas digitalmente se almacenan de manera inmutable en la Blockchain, asegurando que no puedan ser modificadas ni repudiadas.

- Este enfoque incrementa sustancialmente la seguridad en la red, ya que cada registro es verificable y auténtico.
3. Servicios para Administraciones Públicas:
- Está diseñada para ser utilizada por diversas Administraciones Públicas, facilitando la implementación de servicios digitales seguros y eficientes.
 - Permite a los usuarios seleccionar qué información compartir y con quién, garantizando la veracidad de los datos compartidos.

6.2.2 Beneficios de la Solución

- Incremento de la Seguridad: La combinación de Blockchain con firma electrónica proporciona una capa adicional de seguridad, asegurando la integridad y autenticidad de las transacciones.
- Transparencia y Confianza: La naturaleza inmutable de la Blockchain, junto con las firmas digitales, ofrece una trazabilidad completa de las operaciones, fomentando la confianza entre las partes involucradas.
- Eficiencia en Procesos: La automatización y digitalización de procesos mediante esta plataforma pueden reducir tiempos y costos operativos en la gestión de servicios públicos.

Esta iniciativa representa un avance significativo en la modernización de los servicios públicos en España, aprovechando las ventajas de la tecnología Blockchain para ofrecer soluciones más seguras y eficientes.

6.3 Hyperledger Fabric: Características y Capacidades

En los puntos anteriores de este capítulo, se ha visto que tanto ESBI como la plataforma que está desarrollando la FNMT-RCM utilizan *Hyperledger Fabric* como la plataforma Blockchain sobre la que se sustentará gran parte de las soluciones en desarrollo.

Esto hace que sea de gran interés profundizar en las capacidades y características de esta plataforma, pues, además, facilitaría que en un futuro ambas soluciones se integrasen y que la FNMT pudiera convertirse en el nodo, o uno de los nodos nacionales de esa plataforma paneuropea objetivo final de la iniciativa ESBI.

Hyperledger Fabric es un proyecto de la fundación Hyperledger, respaldado por la Linux Foundation, que ofrece una arquitectura modular y customizable, lo que lo convierte en una opción popular para los diferentes actores que buscan soluciones Blockchain adaptadas a sus necesidades específicas.

6.3.1 Estructura técnica

6.3.1.1 Arquitectura modular

Hyperledger Fabric está diseñado para ser modular, lo que significa que las organizaciones pueden personalizar diferentes partes de la plataforma según sus requisitos. Estos son:

- Módulos de consenso: Permite elegir entre distintos algoritmos de consenso (Raft, Kafka, etc.), dependiendo de la velocidad, tolerancia a fallos y requisitos de la red.
- Gestión de identidad: Soporte para sistemas de identidad mediante certificados digitales y Autoridades Certificadoras (CAs).
- Privacidad de datos: Permite configuraciones como canales y colecciones privados para controlar la visibilidad de las transacciones.

6.3.1.2 Redes permissionadas:

Esto significa que solo los participantes autorizados pueden unirse a la red. Esto se logra mediante un sistema de gestión de identidades que utiliza certificados digitales emitidos por una Autoridad Certificadora (CA).

- Organizaciones participantes: Cada miembro de la red (organización) debe tener un nodo y un certificado.
- Control de acceso: Se define mediante políticas que regulan quién puede leer, escribir o validar transacciones.

6.3.1.3 Estructura de la red

Una red de *Hyperledger Fabric* se compone de varios elementos clave:

- *Peer Nodes*:
 - Validan transacciones y mantienen el libro mayor (*ledger*).
 - Pueden ejecutar contratos inteligentes (*chaincodes*).
 - Se dividen en nodos de organización según la estructura de la red.
- *Orderer Nodes* (Servicio de orden):
 - Garantizan el ordenamiento de las transacciones antes de que sean añadidas al libro mayor.
 - Soportan múltiples algoritmos de consenso como Raft o Kafka.
- Clientes: Entidades externas que interactúan con la red mediante aplicaciones API.

6.3.1.4 Libro mayor (Ledger)

El libro mayor en *Hyperledger Fabric* está compuesto por dos partes principales:

1. Base de datos de estado (*State Database*):
 - Representa el estado actual del sistema.
 - Utiliza bases de datos como LevelDB o CouchDB para almacenar los datos.
2. Blockchain:
 - Registra todas las transacciones en forma de bloques de manera inmutable.
 - Cada bloque contiene un encabezado, datos de transacciones y un hash para garantizar su integridad.

6.3.1.5 Privacidad y canales

Una de las características distintivas de *Hyperledger Fabric* es su capacidad para manejar la privacidad de datos mediante canales:

- Canales: Subredes dentro de la red Blockchain que permiten que un grupo específico de participantes comparta datos de forma privada.
- Colecciones privadas: Ofrecen un control aún más granular sobre los datos, permitiendo que solo ciertos nodos tengan acceso a información específica.

6.3.1.6 Algoritmos de consenso

Hyperledger Fabric es compatible con múltiples algoritmos de consenso:

- Raft: Un algoritmo de consenso tolerante a fallos y de alto rendimiento.

- Kafka:, aunque no es algoritmo de consenso, se utiliza como mecanismo de consenso en su implementación de tipo "ordenador", es decir, que actúa como un componente esencial para garantizar el ordenamiento de las transacciones en la red de Fabric antes de que fueran validadas y añadidas a un bloque.

El consenso en *Fabric* se separa en dos etapas:

- Validación de la transacción: Los nodos verifican las reglas del contrato inteligente.
- Ordenamiento: Los nodos del servicio de orden garantizan que las transacciones lleguen en el orden correcto.

6.3.1.7 Contratos Inteligentes (chaincodes)

Los *chaincodes* son programas que definen la lógica empresarial en *Hyperledger Fabric*. Se implementan en lenguajes de programación comunes como Go, Java y Node.js.

- Ejecución en contenedores: Cada *chaincode* se ejecuta en un contenedor Docker aislado.
- Validación: Los chaincodes aseguran que todas las transacciones cumplan con las reglas definidas antes de ser aceptadas.

6.3.1.8 Seguridad y criptografía

Hyperledger Fabric utiliza tecnologías avanzadas para garantizar la seguridad de la red:

- Criptografía de clave pública: Todas las transacciones se firman digitalmente.
- Certificados X.509: Gestionados por una Autoridad Certificadora para autenticar nodos y participantes.
- Cifrado TLS: Protege las comunicaciones entre los nodos.

6.3.1.9 Gobernanza

La gobernanza en *Fabric* está diseñada para redes empresariales, donde múltiples organizaciones colaboran. Las políticas se definen mediante archivos de configuración y contratos inteligentes, permitiendo la toma de decisiones distribuida.

6.3.2 Cumplimiento con la normativa de protección de datos europea y española

Llegado a este punto, es de reseñar las capacidades de esta plataforma en cuanto al cumplimiento de la normativa nacional y europea sobre protección de datos de carácter personal, una de las cuestiones que mayor controversia pudiera traer en cuanto a la utilización de la tecnología Blockchain.

Hyperledger Fabric tiene varias características que lo hacen compatible con el cumplimiento del RGPD en Europa y la LOPDGDD en España, características que se pasa a enumerar:

- Control de acceso y consentimiento:
Fabric permite definir roles y permisos específicos para cada participante, asegurando que sólo las partes autorizadas accedan a los datos personales. Además, los contratos inteligentes pueden programarse para garantizar que se obtenga el consentimiento explícito antes de procesar cualquier información.
- Minimización de datos:

En cumplimiento con el principio de minimización de datos, *Fabric* permite almacenar solo los datos estrictamente necesarios para cada operación. Además, los canales privados aseguran que la información sensible esté restringida a los participantes relevantes.

- Trazabilidad y auditoría:
La inmutabilidad de Blockchain garantiza un registro detallado y verificable de todas las transacciones, lo que facilita la trazabilidad y el cumplimiento normativo. Sin embargo, *Fabric* también permite implementar mecanismos para registrar solo datos pseudonimizados o tokenizados, alineándose con los requisitos de privacidad.
- Derecho al olvido:
Aunque Blockchain es conocido por su inmutabilidad, *Hyperledger Fabric* ofrece soluciones técnicas para cumplir con el derecho al olvido, como la eliminación de datos almacenados en *off-chain* o el cifrado revocable de información. No obstante, esta solución se abordará con mayor detenimiento posteriormente.
- Seguridad y cifrado:
Fabric utiliza algoritmos criptográficos avanzados para proteger los datos en reposo y en tránsito, garantizando la confidencialidad e integridad de la información procesada en la red.

Como se ha mencionado con anterioridad, la solución al derecho al olvido es una de las capacidades que mayor interés suscita, puesto que no es fácil comprender cómo puede llevarse a cabo en una red Blockchain, cuando una de las principales características de esta tecnología es la indelebilidad de los bloques que componen la cadena.

El software de "derecho al olvido" en *Hyperledger Fabric* se centra en abordar las exigencias del Reglamento General de Protección de Datos (GDPR), particularmente en torno a la eliminación de datos personales. *Fabric* adopta enfoques técnicos para equilibrar estos requisitos legales con la tecnología Blockchain. Entre estos se encuentran:

1. Almacenamiento *off-chain*: Los datos personales no se almacenan directamente en la Blockchain, sino en bases de datos externas seguras. Solo referencias (hashes o identificadores únicos) de esos datos se registran en la Blockchain. Esto permite eliminar o modificar los datos en el sistema externo, cumpliendo con el derecho al olvido sin afectar la integridad de la Blockchain.
2. Cifrado revocable: *Fabric* permite cifrar los datos sensibles con claves criptográficas específicas. En caso de que se requiera eliminar el acceso a esos datos, las claves de cifrado pueden ser revocadas o destruidas, haciendo que los datos cifrados sean inaccesibles.
3. Uso de colecciones privadas: *Fabric* incluye la funcionalidad de colecciones privadas, donde los datos solo están disponibles para un subconjunto de participantes en la red. Esto permite cumplir con principios de minimización y garantizar que los datos personales sean gestionados dentro de un entorno controlado.
4. Tokenización o pseudonimización: Los datos personales pueden ser representados mediante identificadores únicos generados criptográficamente. Esto asegura que, incluso si los datos quedan almacenados en la Blockchain, no puedan ser vinculados directamente a individuos sin información adicional.

En resumen, *Hyperledger Fabric* destaca por su arquitectura modular, privacidad avanzada y flexibilidad, que lo convierten en una plataforma ideal para aplicaciones empresariales que requieren un control detallado y cumplimiento normativo, como el RGPD o la L.O. 3/2018, a nivel nacional.

7 PROPUESTA DE SOLUCIÓN

En base a lo mostrado hasta el momento, resulta interesante llevar a cabo una propuesta de alto nivel superadora de lo existente. Para ello, se tomará como base un escenario en el que un procedimiento necesita realizar un documento de la cadena de custodia de las evidencias judiciales que se hayan obtenido.

En este sentido, un equipo de Policía Judicial de la Guardia Civil es requerido para que asista a la escena donde se ha cometido un delito. En la escena del crimen aparecen varias evidencias que deben ser tratadas.

En este caso, con una aplicación, se abre un expediente, que corresponderá con las diligencias que se realicen en relación con el delito correspondiente. A este expediente, se le incluirá cada una de las evidencias que se recojan en la escena del crimen. A cada evidencia se le identificará con un código que, a su vez, corresponderá con la etiqueta que se colocará a la evidencia, en caso de ser un objeto material. A cada evidencia se le reseñará fotográficamente, y se incluirán las notas que se considere. Pues bien, cada una de estas evidencias formarán parte de una transacción en la Blockchain, donde debe constar el código de la evidencia, la reseña fotográfica y el agente que realiza la recogida de ésta, sin olvidar que esta tupla pertenecerá a un expediente al que estará relacionada dicha evidencia y todas las que correspondan al mismo hecho, o a las mismas diligencias.

Del mismo modo se procederá con todas las evidencias que se hayan recogido, de tal manera que, aun estando todas las evidencias relacionadas en un mismo expediente, cada una de ellas es independiente en cuanto a su gestión y manipulación.

Por ejemplo, supongamos que en la escena del delito se han recogido muestras de sangre y un arma de fuego. En este caso, la muestra de sangre será enviada a un laboratorio de ADN, mientras que el arma de fuego será derivada al departamento de balística. En cada una, ha de recogerse mediante la aplicación mencionada inicialmente, qué agente ha tenido bajo su responsabilidad cada una de las evidencias. Mediante la integración con la plataforma Blockchain correspondiente, quedará recogida tanto la firma digital del agente que recepciona la evidencia, como el momento en el que lo hace, marcado a través del *timestamp* de la transacción.

Hay que resaltar la importancia de contar con una aplicación con la que se pueda llevar a cabo la firma digital mediante el certificado de seudónimo que posee el personal de la Guardia Civil para que no aparezca sus datos personales de manera abierta, y si a través del número de identificación personal.

A esto hay que añadir que a cada evidencia se le debe poder ir añadiendo no solamente la identificación de cada agente por el que haya pasado la evidencia, sino también otras informaciones sobre procesos de análisis a los que se ha sometido esa evidencia, incluso informes periciales sobre la misma, de modo que aseguren más si cabe la transparencia en la gestión y la cadena de custodia de la prueba.

Una vez finalizado el ciclo de cada evidencia respecto al tratamiento dado por el cuerpo policial correspondiente, puede haber dos alternativas sobre la compartición de la información de la cadena de custodia: Por un lado, podría ponerse a disposición de las partes implicadas (jueces, fiscales, defensa, acusación particular, o cualquier otra parte que se le reconozca como interesado en el procedimiento judicial) a través de una interfaz y que se pudiera consultar directamente a través de los permisos de usuarios correspondientes. No obstante, este aspecto, dada la complejidad que conlleva la gestión de usuarios entre otros aspectos, excede el estudio realizado en este documento.

Por otro, podría descargarse o imprimirse físicamente toda la información referente a cada evidencia para incluirlo directamente en las diligencias que sean puestas a disposición de todas las partes interesadas y obligadas a conocer del asunto, al tiempo que se expida un certificado en el que conste todos los datos técnicos de la tecnología Blockchain utilizada. En este sentido, puede ser algo similar a lo que la Dirección General de Tráfico remite cuando una persona es sancionada por exceso de velocidad, en el que se recogen todas las características técnicas y de homologación del cinemómetro con el que se han obtenido los datos objeto de la infracción correspondiente.

En cuanto a cómo utilizar la tecnología Blockchain, a lo largo de este documento se ha venido recogiendo su funcionamiento, características, que el uso de esta tecnología por parte de organismos policiales es factible en cuanto a que su uso sería aceptado por parte de los tribunales de justicia, que este uso redundaría en la trazabilidad de cualquier transacción o cualquier acción que se desarrolle sobre una evidencia, que los datos obrantes en la misma son inmutables e incluso que es una tecnología que a pesar de que sus registros son imposibles de borrar, hay soluciones que darían cobertura al cumplimiento de la normativa tanto europea como nacional sobre la protección de datos de carácter personal.

Por otro lado, parece evidente que, dado el carácter de los datos que se incluiría en una Blockchain de estas características, debe ser una Blockchain de tipo privada, donde se requiere un alto grado de privacidad y control sobre quién tiene acceso a los datos.

Sin embargo, el desarrollar una plataforma de estas características que pertenezca a un organismo policial, como pueda ser la Guardia Civil, o incluso que pertenezca al Ministerio del Interior y que pueda ser utilizada por los diferentes cuerpos policiales, no se considera adecuado. La razón no es tanto la complejidad técnica, ni el coste que supondría crear una red propia. Parece claro que esta tecnología cumple ampliamente con las características de inmutabilidad, trazabilidad y seguridad de las transacciones. Esta razón estaría más bien relacionada con la percepción de las personas, pues podría ponerse en tela de juicio que el mismo organismo sea quien gestione una Blockchain para certificarse a sí mismos que lo han hecho de manera correcta. En otras palabras, podría no estar bien visto, a los ojos de la opinión pública, ser juez y parte en procesos judiciales.

Por ello, se considera conveniente explorar la posibilidad de consumir soluciones que otros organismos públicos hayan desarrollado, como, por ejemplo, la plataforma EBSI, o la prueba de concepto que está desarrollando la Fábrica Nacional de Moneda y Timbre (FNMT), basada en *Hyperledger Fabric*, ambas ya descritas en el Capítulo 6 de este documento.

En concreto, a priori parece más interesante optar por la opción de la solución de la FNMT, puesto que, aun cuando podría ser más llamativa la opción de EBSI, pues podría certificar o validar la veracidad de las transacciones en un entorno paneuropeo, el camino sería mucho más largo, dado que esta plataforma debería adecuarse a las diferentes legislaciones de los países participantes. Hay que tener en cuenta que en la Unión Europea el avance en la armonización legislativa en campos como el económico o financiero está mucho más avanzado que en el ámbito judicial penal.

Sin embargo, la solución presentada por la FNMT puede ser mucho más factible hoy en día. Es un organismo público, ajeno a la espera del Ministerio del Interior y, por ende, a los cuerpos policiales, es una Blockchain privada, y tanto en España como en el resto de la Unión Europea está considerada como un organismo de confianza. De hecho, es el organismo que expide los certificados de las tarjetas profesionales de los agentes de la Guardia Civil con los que se firma digitalmente. El que la solución que está desarrollando este organismo esté integrada con los certificados digitales gana muchos enteros como alternativa principal. A todo ello hay que unir que la FNMT forma parte de ESBI, por lo que una integración con una plataforma europea sería mucho más sencilla y reduciría los plazos en gran medida.

Así, esta propuesta no solo asegura el cumplimiento legal, sino que también facilita la integración con plataformas internacionales como EBSI, marcando el camino hacia una gestión más eficiente y transparente de las evidencias judiciales en un contexto digitalizado.

En cuanto a su implantación, es interesante tener en cuenta la infraestructura descentralizada que propone ESBI, y que está recogida en el punto 6.1.3, que podría implementarse de la siguiente forma:

- Interacción con Nodos de Validación:

Los nodos de validación de EBSI, o de la plataforma de FNMT podrían encargarse de verificar las transacciones relacionadas con las evidencias judiciales, como el registro inicial de su recogida, el clonado de información y cualquier transferencia entre agentes o laboratorios.

Cada transacción incluiría datos clave como:

- Código único de la evidencia.
 - Firma digital del agente responsable.
 - *Timestamp* de la acción realizada.
 - Hash de integridad para asegurar que los datos no han sido alterados.
- Uso de Nodos de Almacenamiento:

Los registros relacionados con las evidencias, incluidos los informes periciales y datos fotográficos, serían almacenados de forma inmutable en los nodos de almacenamiento.

Estos nodos garantizarían la preservación de los datos durante todo el proceso judicial, permitiendo su consulta en cualquier momento con total transparencia.

Estos nodos de almacenamiento podrían ser bases propias de la Guardia Civil

- Rol de los Nodos Intermedios:

Los nodos intermedios facilitarán la comunicación entre la plataforma de gestión de evidencias policiales y la red EBSI o de la plataforma de la FNMT.

Estos nodos permitirían la interoperabilidad con otras redes o actores, como laboratorios de análisis, tribunales o agencias internacionales, promoviendo una colaboración fluida entre diferentes jurisdicciones.

8 CONCLUSIONES

A lo largo de este documento, se han desarrollado los diferentes epígrafes con el propósito de responder a los objetivos específicos inicialmente planteados, destacando los siguientes aspectos clave:

En el capítulo 2, se ha analizado el funcionamiento de esta tecnología, destacando sus características esenciales como inmutabilidad, trazabilidad y seguridad. Estas propiedades se presentan como una solución confiable para cumplir con las exigencias normativas de la cadena de custodia, consolidando a Blockchain como una herramienta eficaz y segura.

En el capítulo 3, se ha señalado que la normativa actual relacionada con la cadena de custodia es bastante limitada. A pesar de algunos intentos de regulación más precisa, no existe un marco legislativo único que compile los requisitos específicos de este proceso. En consecuencia, se recurre a la jurisprudencia para encontrar una definición y aplicación práctica.

Con los capítulos 2 y 3, se da por cumplido el objetivo parcial 1.

El capítulo 4 aborda la implementación del libro mayor distribuido en el ámbito público, concluyendo que esta tecnología ha sido ampliamente aceptada en este sector, lo que refuerza su idoneidad para procesos sensibles como la cadena de custodia.

Una cuestión crítica tratada en el capítulo 5 y parte del capítulo 6 es la aplicación de la normativa sobre protección de datos personales, tanto a nivel europeo como nacional. Si bien los registros en Blockchain son inmutables y permanentes por diseño, existen soluciones que permiten cumplir con los requisitos normativos de privacidad sin comprometer la integridad de los datos.

Con los capítulos 4, 5 y parte del capítulo 6, se da por cumplido el objetivo parcial 2.

El capítulo 6 analiza las principales plataformas disponibles en el sector público, tanto a nivel europeo como nacional, destacando sus capacidades y características. Estas plataformas cumplen con los requisitos técnicos y normativos necesarios, consolidándose como opciones confiables para implementar una cadena de custodia eficiente y segura.

En el capítulo 7, se ha planteado una propuesta de implementación, concluyendo que una Blockchain de tipo permissionada es la opción más adecuada. Este enfoque no solo garantiza la transparencia y refuerza la imagen de los cuerpos policiales, como la Guardia Civil, sino que también resuelve cuestiones de viabilidad técnica. La propuesta sugiere que un organismo de confianza gestione la plataforma Blockchain, mientras la Guardia Civil actúe como usuaria de los servicios ofrecidos.

Con los capítulos 6 y 7, se da por cumplido el objetivo parcial 3.

Por tanto, se puede afirmar que se han cumplido todos los objetivos planteados inicialmente. En esta investigación, podemos concluir que la implementación de una cadena de custodia basada en tecnología Blockchain, utilizando plataformas como las desarrolladas por la FNMT o EBSI, asegura la integridad, trazabilidad y transparencia en la gestión de evidencias judiciales. Este enfoque no solo satisface los estándares legales y técnicos, sino que también refuerza la confianza de todas las partes implicadas en los procesos judiciales. Al combinar tecnología avanzada con un diseño descentralizado e interoperable, esta propuesta establece una base sólida para una gestión de evidencias eficiente, confiable y adaptada a los desafíos de un entorno digital y globalizado.

Como líneas futuras no abordadas en este trabajo, se pueden señalar varias propuestas que podrían enriquecer y optimizar aún más el uso de Blockchain en la gestión de la cadena de custodia. En primer lugar, el refinamiento de la plataforma para proponer casos de uso más avanzados y específicos, que permitan aprovechar al máximo las capacidades de esta tecnología. En segundo lugar, la implementación de una red Blockchain diseñada específicamente para este propósito, promoviendo el concepto de soberanía digital y garantizando el control autónomo sobre los datos y procesos implicados. Otra línea relevante sería la integración digital de los agentes implicados, facilitando su interacción con el sistema de manera eficiente y segura. Asimismo, se propone desarrollar una estrategia de cambio cultural orientada a implementar nuevos modelos de funcionamiento que adapten a los usuarios y organizaciones a las exigencias de este entorno tecnológico.

Además, se identifican dos áreas específicas de investigación con alto potencial. La primera se centra en la mejora de las interfaces de acceso para las partes implicadas, mediante el diseño de plataformas web seguras, intuitivas y accesibles que permitan interactuar con los datos de la Blockchain, asegurando al mismo tiempo la protección de la información sensible y el cumplimiento de las normativas aplicables. La segunda línea está orientada hacia la digitalización de las evidencias materiales mediante la tokenización, que permite representar digitalmente objetos físicos, o a través del uso de oráculos que conecten los sistemas físicos y digitales. Un ejemplo práctico de esta última propuesta sería la integración de dispositivos como básculas inteligentes en intervenciones de droga, capaces de registrar automáticamente el peso de las mercancías incautadas en un bloque de la Blockchain, garantizando así la inmutabilidad y trazabilidad de los datos desde el momento de la intervención.

Estas líneas no solo complementarían la funcionalidad actual, sino que también abren nuevas posibilidades para consolidar un sistema de cadena de custodia más eficiente, confiable y adaptado a las necesidades del futuro.

9 BIBLIOGRAFÍA

- [1] S. & S. W. Haber, «How to time-stamp a digital document,» *Journal of Cryptology*, vol. 2, nº 3, pp. 99-111, 1991.
- [2] S. Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, 2008.
- [3] S. Mason, Electronic Evidence, University of London, 2017.
- [4] A. S. & V. S. Tanenbaum, Distributed Systems: principles and Paradigms, Prentice Hall, 2007.
- [5] M. Swan, Blockchain: Blueprint for a New Economy, O'Reilly Media, Inc., 2015.
- [6] Binance Academy, «Proof of Stake (PoS) Explained,» s.f.. [En línea]. Available: <https://academy.binance.com/es/articles/proof-of-stake-explained>. [Último acceso: 28 10 2024].
- [7] IBM, «Hyperledger Fabric Overview,» s.f.. [En línea]. Available: <https://www.ibm.com/topics/hyperledger>. [Último acceso: 28 10 2024].
- [8] R. G. Brown, «Corda: An Introduction,» 2016. [En línea]. Available: <https://gondal.me/2016/08/24/corda-an-introduction/>. [Último acceso: 26 10 2024].
- [9] Dragonchain, «What is Dragonchain?,» s.f.. [En línea]. Available: <https://dragonchain.com>. [Último acceso: 26 10 2024].
- [10] Binance academy, «¿qué son los contratos inteligentes?,» 2018. [En línea]. Available: <https://academy.binance.com/es/articles/what-are-smart-contracts>. [Último acceso: 26 10 2024].
- [11] ATS 3635/2024, 2024.
- [12] Centro de Documentación Judicial CENDOJ, [En línea]. Available: <https://www.poderjudicial.es/search/indexAN.jsp>.

- [13] M. López-Varela, La cadena de custodia de las pruebas de ADN, Dykinson, 2019.
- [14] H. Soletto-Muñoz, La identificación del imputado: Rueda, fotos, ADN... De los métodos basados en la percepción a la prueba científica, Tirant lo Blanch, 2009.
- [15] M. Lopez-Jara, «l,» 2020. [En línea]. Available: <https://www.lacaciabogados.com/cadena-de-custodia-en-el-proceso-penal/>. [Último acceso: 26 11 2024].
- [16] «Anteproyecto de Ley de Enjuiciamiento Criminal,» 2011. [En línea]. Available: <https://www.mjusticia.gob.es/es/AreaTematica/ActividadLegislativa/Documents/210126%20ANTEPROYECTO%20LECRIM%202020%20INFORMACION%20PUBLICA%20%281%29.pdf>.
- [17] International Organization for Standardization, *ISO 22739: Blockchain y tecnologías de registro distribuido - Terminología*, Ginebra: ISO, 2020.
- [18] International Organization for Standardization, *ISO 30300: Gestión de documentos - Fundamentos y vocabulario*, Ginebra: ISO, 2011.
- [19] «Hellwig, D., Karlic, G., & HUCHZERMEER, A., Build your own Blockchain.,» *Spring International Publishing*, p. 3, 2020.
- [20] E. Dans, «Enrique Dans,» [En línea]. Available: <https://www.enriquedans.com/>. [Último acceso: 14 12 2024].
- [21] Rieger, A., Stohr, A., Wenninger, A., & Fridgen, G., *Blockchain and the Public Sector: Theories, Reforms, and Case Studies*, Springer International Publishing, 2021.
- [22] «Reddick, C. G., Cid, G.P., & Ganapati, S., Determinants of lockchain adoption in the public sector: An empirical examination,» 2019.
- [23] «Allessie., Maciej Sobolewski & David, Blockchain Applications in the Public Sector: Investigating Seven Real-Life Blockchain Deployments and Their Benefits.,» 2021.
- [24] A. Datta, «Blockchain Enabled Digital Government and Public Sector Services: A Survey,» *Springer International Publishing*, 2021.
- [25] «Olmes, S. & Jansen, A., Blockchain Technology as a Support Infrastructure in e-Government.,» *Springer International Publishing*, pp. 215-227, 2017.
- [26] «Gamage, H. T. M., Weeransiinghe, H. D., & Dias, N. G. J., A survey on Blockchain Technology Concepts, Applications, and Issues,» *SN Computer Science*, vol. 1, p. 114, 2020.
- [27] I. Alamillo-Domingo, Identificación, firma y otras pruebas electrónicas. La regulación jurídico-administrativ de la acreditación de las transacciones electrónicas, Thomson Reuters Aranzadi, 2019.
- [28] J. M. Anguiano-Jiménez, «Blockchain: Fundamentos y perspectiva jurídica. De la confianza al consenso,» 2018.
- [29] J. W. Ibañez-Jimenez, *Derecho de blockchain y de la tecnología de registros distribuido*, Cizur Menor (Navarra): Thomas Reuters Aranzadi, 2019.
- [30] Union Europea, «Euro Digital,» [En línea]. Available: https://www.ecb.europa.eu/euro/digital_euro/html/index.es.html. [Último acceso: 10 enero 2025].

- [31] A. J. Gilliland, «Introduction to metadata,» Getty Research Institute, 2016.
- [32] R. C. Merkle, «A Digital Signature Based on a Conventional Encryption Function,» de *Advances in Cryptology --- CRYPTO '87*, Berlin, Heidelberg, Springer Berlin Heidelberg, 1988, pp. 369--378.
- [33] A. M. Anatopoulos, *Mastering Bitcoin: Inlocking Digital Cryptocurrencies*(2nd ed.), O'Reilly Media, 2017.
- [34] Coinbase, «¿Cómo funcionan los mineros de criptomonedas?,» s.f.. [En línea]. Available: <https://www.coinbase.com/es-es/learn/crypto-basics/how-do-cryptocurrency-miners-work>. [Último acceso: 27 10 2024].
- [35] V. Buterin, «www.ethereum.org,» 2021. [En línea]. Available: <https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/>. [Último acceso: 10 12 2024].
- [36] «Zheng, Z., Xie, S., Dai, H.-N., Chen, X., Wang, H., & Imran, M., Blockchain challenges and opportunities: A survey.,» *International Journal of Web and Grid Services*, nº 15, pp. 99-135, 2020.
- [37] «Luque, M., Rodriguez-Lasarte, A., Etxeberria, F., El documento de cadena de custodia. Propuesta para el ámbito de la antropología y odontología forense en España,» *Revista Internacional de Antropología y Odontología Forense*, vol. 1, nº 2, junio, 2018.
- [38] *ATS 3522/2024, FJ1*, 2024.
- [39] «BROTSIS, S., KOLOKOTRONIS, N., LIMNIOTIS, K., BENDIABY, G., & SHIAELES, S., On the Security and Privacy of Hyperledger Fabric: Challenges and Open Issues.,» de *2020 IEEE World Congress on Services (SERVICES)*, Beijing, China., 2020.