

Prueba de concepto Blockchain y el derecho de supresión

Resumen ejecutivo

Blockchain es una tecnología que permite crear infraestructuras de almacenamiento e intercambio de información. Distintos procesos pueden usar dichas infraestructuras, entre otros sistemas, para implementar servicios. Para la gestión de la propia infraestructura se requiere la ejecución de procesos específicos. Ambos conjuntos de procesos podrían involucrar tratamientos de datos personales.

Los diseños de las infraestructuras Blockchain no han aplicado, de forma general, la protección de datos desde el diseño. En muchos casos, en el desarrollo de las infraestructuras se han utilizado componentes sin documentar exhaustivamente, y que tampoco han sido analizados por sus desarrolladores y gestores. En la mayor parte de las infraestructuras Blockchain se han aplicado medidas de gobernanza de facto, muchas veces motivadas por problemas sobrevenidos, y también poco documentadas.

La Prueba de Concepto que se presenta en este documento demuestra la viabilidad de construir infraestructuras Blockchain que permitan cumplir con el RGPD.

En esta Prueba de Concepto se analizan y documentan los componentes de una infraestructura Blockchain, de amplio uso en el mercado, en el cumplimiento del principio de responsabilidad proactiva. También se analizan los casos reales de aplicación de cambios y gestión de la gobernanza habituales en dicha infraestructura. A continuación, se desarrollan políticas, que incluyen medidas organizativas y técnicas, para implementar el derecho de supresión en una infraestructura Blockchain mediante la gestión de inconsistencias. Finalmente, se aplican de forma práctica en un caso de uso sobre una infraestructura Blockchain real.

Si bien existen trabajos previos para gestionar el borrado de información en una infraestructura Blockchain, la presente Prueba de Concepto constituye un demostrador completamente funcional y documentado que está específicamente orientado al cumplimiento del RGPD. Además, contempla la gestión de la información personal almacenada en todo el conjunto de la Blockchain, es decir, no solo la información en las transacciones de los bloques, sino otras como la registrada en los recibos de las transacciones.

La Prueba de Concepto demuestra que es posible el cumplimiento del RGPD en infraestructuras Blockchain, específicamente en relación con el cumplimiento del derecho de supresión, sin pretender ser una solución comercial de aplicación directa en el mercado. Es importante recalcar que, aunque la Prueba de Concepto se ha desarrollado sobre una infraestructura que no ha aplicado la protección de datos desde el diseño, no pretende validar dicha forma de proceder. Al contrario, tiene el propósito de promover entre los diseñadores, autoridades y organizaciones que tienen algún papel en el diseño o el desarrollo de estas infraestructuras, la adopción de estrategias de protección de datos desde el diseño y por defecto.

El presente documento pretende servir de puente entre el profesional de protección de datos y el de tecnologías Blockchain, por lo tanto, analizará la terminología utilizada y aclara los conceptos para evitar equívocos que se esconden tras descripciones imprecisas. Además, está complementado con [información técnica adicional](#) y [videos demostrativos](#) que están accesibles en la página web de la AEPD, en el apartado de [Innovación y Tecnología](#).

ÍNDICE

I.	INTRODUCCIÓN	5
II.	CONCEPTOS BÁSICOS	8
III.	MARCO TECNOLÓGICO Y LEGAL	12
A.	Descripción de la tecnología Blockchain y su aplicación	12
B.	Equívocos relativos a tecnologías e infraestructuras Blockchain	17
1.	Equívoco: Inmutabilidad	18
2.	Equívoco: La gestión de las infraestructuras Blockchain es completamente descentralizada	18
3.	Equívoco: No existe un marco de gobernanza en las infraestructuras Blockchain, y si existe, es completamente automatizado	19
4.	Equívoco: En una infraestructura Blockchain los nodos actúan de forma automática	19
5.	Equívoco: Todas las infraestructuras Blockchain tienen las mismas propiedades que el modelo ideal sugerido en la definición original de tecnología Blockchain	20
6.	Equívoco: El código es ley	20
7.	Equívoco: Las actuales infraestructuras Blockchain garantizan el control del usuario sobre sus propios datos	21
8.	Equívoco: La tecnología Blockchain es incompatible con el RGPD	21
9.	Equívoco: Los Smart Contract son autónomos e inteligentes	21
10.	Equívoco: En una infraestructura Blockchain los datos solo están en las transacciones y los bloques.	22
C.	Datos personales	22
D.	Tratamientos y responsabilidades	23
E.	Cumplimiento del RGPD	24
IV.	PRUEBA DE CONCEPTO DE LA AEPD	27
A.	Antecedentes	27
B.	Explotación de estrategias ya existentes	27
1.	Gobernanza	27
2.	Hard Fork/ Soft Fork y actualizaciones de software	29
3.	Procedimientos de validación de nuevas versiones	30
4.	Trazabilidad	31
5.	La aplicación de los derechos en el RGPD	32
C.	Diseño de la Prueba de Concepto	33
1.	Procedimiento de detección de registros afectados	33
2.	Procedimiento de generación de una nueva versión de software de la Blockchain	34
3.	Procedimiento de distribución de la nueva versión de software y ejecución de este en los nodos	35

4. Estrategia técnica para implementar un mecanismo de consenso en la nueva versión de la Blockchain	35
5. Medidas organizativas para la gestión de la gobernanza	35
V. EJECUCIÓN Y RESULTADOS DE LA PRUEBA DE CONCEPTO	39
A. Estrategia técnica para la ejecución de la PoC	39
B. Resultados de la PoC	41
1. Transacciones	45
2. Balance	47
3. Almacenamiento de <i>Smart Contracts</i> y recibo de transacciones (<i>receipts/logs</i>)	48
VI. DESARROLLOS FUTUROS	51
VII. CONCLUSIONES	52

I. INTRODUCCIÓN

El despliegue de nuevos tratamientos de datos personales sobre servicios en Internet, como la gestión de la identidad digital, las monedas digitales, el acceso a certificados o la propia historia clínica, se ha planteado utilizando distintas tecnologías. Algunas de las opciones tecnológicas incorporan características de disponibilidad descentralizada de las bases de datos, intercambios mediante protocolos P2P¹ y de gestión de la integridad de la información digital almacenada. Una de esas tecnologías es la denominada Blockchain.

El término “Blockchain” se utiliza de forma aislada para referirse en unas ocasiones a la tecnología tal como se define idealmente, en otras para una materialización concreta en una infraestructura, y en otras para el conjunto de datos que se gestiona en una infraestructura concreta. En este texto diferenciaremos los tres significados con los términos tecnología Blockchain, infraestructura Blockchain, y “cadena/tabla de bloques” respectivamente.

La tecnología Blockchain permite implementar infraestructuras de gestión de datos de forma distribuida y descentralizada. Utilizando esta tecnología, y adaptándola a diferentes casos de uso, se pueden crear infraestructuras Blockchain, que son materializaciones concretas de uso de esta. Distintas infraestructuras Blockchain ajustarán los principios de la tecnología Blockchain y la complementarán con funciones o sistemas adicionales. De esta forma podemos hablar de la infraestructura Bitcoin, o Ethereum entre otras, que son distintas formas de llevar a la realidad las posibilidades de la tecnología Blockchain, pero incompatibles entre sí, y con funcionalidades y objetivos distintos.

La tecnología Blockchain, y muchas de las infraestructuras en las que se materializó, se diseñaron inicialmente para operar en un entorno desregulado, es decir, en un entorno en el que se ignoraban los controles que establece un Estado de Derecho. Además, incorporaban modelos de gobernanza y procedimientos de gestión casi totalmente automatizados, sin recurrir a terceros de confianza ni organismos de supervisión. De esta forma, se podía implementar una infraestructura de almacenamiento y compartición de información en la que todos los intervinientes eran iguales en poderes y funcionalidades (pares), eliminando la asignación de responsabilidades a un organismo centralizado y distribuyendo la responsabilidad en aquellas personas (físicas o jurídicas) que decidían participar en dicha infraestructura. En principio, y sin mediar contratos o actos jurídicos, los intervinientes no adquirirían compromisos como, por ejemplo, los que garanticen algún nivel de calidad de servicio o el cumplimiento de las distintas normativas².

Bitcoin fue la primera infraestructura creada con tecnología Blockchain. A partir de entonces, se han creado distintas infraestructuras que han innovado, desarrollado y modificado los principios de dicha tecnología. Por lo tanto, aunque se puede hablar de las propiedades de la tecnología Blockchain de forma genérica, la implementación concreta en las distintas infraestructuras puede alterar sustancialmente sus características.

Distintos tratamientos de datos pueden utilizar una infraestructura Blockchain para implementar alguna de sus operaciones, como la de almacenamiento de datos. Dichos tratamientos necesitarán incluir otros elementos además de la infraestructura Blockchain para implementar otras operaciones³.

Pero, además, se necesitan algunas operaciones específicas para interactuar con la infraestructura. Ese conjunto de operaciones o sistemas adicionales, al integrarse con la infraestructura Blockchain, es lo que en el ámbito de esta tecnología se ha denominado el

¹ P2P (Peer to Peer): Red entre iguales o entre pares. Los nodos conectados se comportan como iguales entre sí. Permite el intercambio directo de información entre los nodos interconectados. Ejemplos para compartición de archivos son eMule y BitTorrent pero tienen otras aplicaciones (<https://es.wikipedia.org/wiki/Peer-to-peer>)

² De ahí los conflictos con las normativas de derecho de autor o de propiedad intelectual que han originado las redes P2P antes mencionadas.

³ Como sistemas de procesamiento y almacenamiento en la nube, sistemas de IA, etc.

ecosistema Blockchain. Estos pueden ser carteras digitales, emisores de credenciales o atributos, desarrolladores de programas y aplicaciones en la infraestructura, navegadores o visualizadores de datos, mecanismos adicionales de gobernanza, etc. Todos estos elementos introducen operaciones, fortalezas y debilidades que alteran las propiedades teóricas que permite Blockchain. Por ejemplo, aunque algunas implementaciones se han construido como un medio anónimo de intercambio entre personas físicas, la realidad (y el ecosistema) han demostrado que ese anonimato no existe.

Uno de los problemas con los que se enfrentan los tratamientos contruidos sobre infraestructuras Blockchain es que el modelo de gobernanza empleado no ha contemplado como objetivo el cumplimiento de ningún tipo de regulación. En particular no se han tenido en cuenta requisitos para garantizar, y poder demostrar, el cumplimiento del RGPD. Por lo tanto, han sido diseñadas sin tener en cuenta la protección de datos desde el diseño.

En la medida en la que un proceso implementado sobre Blockchain no implique datos personales esto no supone un impedimento para su uso desde la perspectiva del RGPD, sin perjuicio de otras limitaciones regulatorias. Igualmente, si en ciertas operaciones de un tratamiento de datos personales se utiliza Blockchain para implementar funciones que no tienen que ver con datos personales, por ejemplo, mantener un repositorio de datos sobre certificados de entidades que dé soporte a operaciones sobre datos personales, el hecho de usar Blockchain tampoco tendría impacto desde el punto de vista del RGPD.

Sin embargo, cuando el uso de dicha tecnología sea el medio elegido para implementar operaciones de tratamiento de datos personales, entonces, y atendiendo a lo establecido en el considerando 15 del RGPD *“A fin de evitar que haya un grave riesgo de elusión, la protección de las personas físicas debe ser tecnológicamente neutra y no debe depender de las técnicas utilizadas.”*, se ha de garantizar el cumplimiento de dicho reglamento.

La finalidad última de un tratamiento es diferente de los medios seleccionados para implementarlo. El artículo 25 del RGPD establece que el responsable tiene obligación de implementar las medidas técnicas y organizativas apropiadas a fin de garantizar y demostrar que el tratamiento es conforme con el RGPD. A este respecto, el Comité Europeo de Protección de Datos ha manifestado que no puede invocarse la imposibilidad técnica para justificar el incumplimiento de los requisitos del RGPD, especialmente teniendo en cuenta que el artículo 25, apartado 1, del RGPD establece que la protección de datos desde el diseño se tendrá en cuenta en el momento de la determinación de los medios de tratamiento y en el momento del propio tratamiento⁴.

El uso de tratamientos basados en infraestructuras Blockchain ha crecido significativamente en diversos sectores, y con numerosas aplicaciones más allá del ámbito financiero o de las criptomonedas, como pueden ser la gestión de cadenas de suministro, *tokenización* de activos, trazabilidad de bienes, gestión de identidad digital, votación, registros de propiedad, metaverso, etc. La elección por parte de un responsable de una infraestructura Blockchain concreta como elemento de su tratamiento podría generar incumplimientos y riesgos específicos para los derechos y libertades de los interesados. Uno de sus aspectos clave es implementar los principios de protección de datos y permitir el ejercicio de los derechos de los interesados, en concreto, el principio de exactitud, el de conservación y los derechos de rectificación y supresión. En caso de incumplimiento debido a la elección de una infraestructura Blockchain concreta, se ha de cambiar el diseño de dicha infraestructura o del tratamiento.

⁴ EDPB, Report of the work undertaken by the ChatGPT Taskforce de mayo de 2024, párrafo 7: *“In particular, technical impossibility cannot be invoked to justify non-compliance with these requirements, especially considering that the principle of data protection by design set out in Article 25(1) GDPR shall be taken into account at the time of the determination of the means for processing and at the time of the processing itself”*.

Ninguna opción tecnológica es inmutable, y mucho menos las basadas en sistemas digitales. El cumplimiento de la normativa exige adaptaciones de los sistemas y deben estar todos sus componentes debidamente documentados de forma que permitan garantizar y poder demostrar el cumplimiento.

Para demostrar que es posible desarrollar infraestructuras Blockchain que permitan a los responsables de tratamiento el cumplimiento del RGPD, la AEPD ha desarrollado la presente Prueba de Concepto. La Prueba de Concepto incluye la definición de unas medidas de gobernanza, políticas y la implementación de las modificaciones técnicas necesarias para facilitar el cumplimiento del RGPD en los aspectos anteriormente señalados. Para ello, tras un estudio del código fuente de los componentes necesarios para construir una infraestructura Blockchain, se ha llevado a cabo la ejecución de diversos casos de uso sobre la implementación oficial de Ethereum, configurada con el mecanismo de consenso denominado Prueba de Autoridad⁵.

Los casos de uso contemplan un conjunto de transacciones de transferencia de criptomonedas entre diversas cuentas (usuarios), así como la interacción de algunas de ellas con dos Contratos Inteligentes (*Smart Contracts*) programados para la Prueba de Concepto. La Prueba de Concepto hace patente que es posible el derecho de supresión de una de las cuentas participantes en las transacciones.

Esta Prueba de Concepto está dirigida a responsables y encargados de tratamientos que se construyen sobre infraestructuras Blockchain, a los responsables y encargados de los tratamientos que soportan la operación de la infraestructura, y a aquellas autoridades y organizaciones que soportan el desarrollo de proyectos basados en tecnologías Blockchain. En este documento no se entra a valorar la asignación de los roles de responsable o encargado en cada uno de los tratamientos de infraestructuras Blockchain concretas ni en la legitimación de los tratamientos.

⁵ La prueba de autoridad es un algoritmo de consenso basado en la reputación en lugar del mecanismo basado en la participación como es PoS. La prueba de autoridad requiere confiar en un conjunto de firmantes autorizados que se establecen en el bloque génesis (algunas implementaciones permiten incluir nuevos firmantes durante la operación de la Blockchain). En la mayoría de las implementaciones actuales, todos los firmantes autorizados conservan el mismo poder y privilegios a la hora de determinar el consenso de la cadena. La idea detrás del *staking* de reputación es que todos los validadores autorizados sean conocidos por todos a través de mecanismos como conocer a su cliente (KYC) o tener una organización conocida como el único validador; de esta manera, si un validador hace algo mal, se conoce su identidad. Fuente: <https://ethereum.org/es/developers/docs/consensus-mechanisms/poa/>

II. CONCEPTOS BÁSICOS

A la hora de analizar el impacto que pueden tener determinadas opciones tecnológicas desde el punto de vista de protección de datos es fundamental definir con rigor la terminología empleada y asegurarse de comprender con precisión su significado real y técnico. Este conjunto de descripciones tiene como objetivo ofrecer claridad y comprensión sobre esta tecnología⁶:

- a) **Bloque/registro:** Unidad fundamental de información que contiene un conjunto de transacciones validadas y otros datos relevantes, vinculado mediante hash con los bloques anteriores para gestionar la integridad del orden de las transacciones.
- b) **Cadena/tabla de bloques:** Estructura de datos que representa un libro mayor distribuido, con bloques/registros confirmados, organizados secuencialmente, que solo permite añadir bloques/registros vinculados mediante enlaces hash⁷. De ahí el nombre Blockchain. Sin embargo, esta no es la única estructura de datos en las distintas infraestructuras Blockchain. Estas necesitan utilizar varias estructuras adicionales, que permiten su funcionamiento y operación eficiente.
- c) **Consistencia:** Grado en el que los datos están libres de contradicción y son coherentes con otros datos en un contexto de uso específico. Puede ser analizada en datos que se refieran tanto a una como a varias entidades comparables⁸. En tecnología Blockchain se implementan medidas para que la información compartida entre los nodos sea la misma y no existan contradicciones, es decir, todos los nodos en una infraestructura Blockchain concreta comparten el mismo estado en un determinado momento.
- d) **Consenso:** Acuerdo alcanzado entre los nodos sobre que una transacción es válida. También acuerdo sobre que se ha almacenado un conjunto en un orden coherente de transacciones validas. Existen varios mecanismos de consenso para determinar qué nodo añade un nuevo bloque a la cadena. Los más conocidos son el de prueba de trabajo, o *Proof of Work* (PoW) usado en Bitcoin, el de prueba de participación, o *Proof of Stake* (PoS), usado en Ethereum, y el de prueba de autoridad o *Proof of Authority* (PoA), usado por Ethereum en redes privadas y de pruebas⁹.
- e) **Contrato inteligente:** También conocido como *Smart Contract*¹⁰, es un programa que se almacena en la infraestructura Blockchain y ejecuta decisiones automatizadas al cumplirse ciertas condiciones programadas en él cuando son invocados por una transacción. El resultado de las transacciones efectuadas con ellos se refleja en un cambio del estado de la información almacenada en la infraestructura Blockchain, que a su vez se registra de forma automática en la misma. Estos cambios pueden provocar que se ejecuten en cascada otros *Smart Contract*. Su denominación puede resultar engañosa, pues ni son contratos (en el sentido legal del término) ni son inteligentes (son programas de ejecución automática condicionada). El uso continuado de este término se debe más a su arraigo histórico en el campo de la tecnología Blockchain que a una descripción precisa de su funcionalidad¹¹.

⁶ La norma ISO 22739 "Blockchain y tecnologías de registros distribuidos – Vocabulario", contiene definiciones relacionadas con Blockchain. Tiene disponible una versión web en inglés: <https://www.iso.org/obp/ui/#iso:std:iso:22739:ed-2:v1:en>

⁷ ISO 22739.

⁸ ISO 25012.

⁹ Ethereum ha dejado de dar soporte al consenso PoA desde la versión v1.14.0 de 24 de abril de 2024, no obstante, existen varias implementaciones basadas en Ethereum que sí lo contemplan, tales como Hyperledger Besu.

¹⁰ Término acuñado por el criptógrafo Nick Szabo, alrededor de 1993.

¹¹ El artículo 2(39) de la Data Act¹¹ define contrato inteligente en un ámbito más general que el de Blockchain como "programa informático utilizado para la ejecución automatizada de un acuerdo o de parte de este, que utiliza una secuencia de registros electrónicos de datos y garantiza su integridad y la exactitud de su orden cronológico".

- f) **Criptomonedas:** Activo digital que se usa como medio de intercambio o valor. Algunas infraestructuras Blockchain usan criptomonedas como su token nativo, propio de ellas, integrado en su protocolo y fundamental para su operación (no está creado por un *Smart Contract*). No es una moneda, a diferencia de las CBDC (*Central Bank Digital Currency*). No todas las infraestructuras Blockchain implementan criptomonedas propias o nativas. Sin embargo, las criptomonedas representan el caso de uso de mayor éxito de la tecnología Blockchain¹².
- g) **Cuenta o dirección (de una cuenta):** Identificador único obtenido a partir de la clave pública del usuario que permite interactuar y efectuar transacciones en la infraestructura Blockchain. La dirección de un *Smart Contract* es su identificador único en la Blockchain, pero no está basado en una clave pública.
- h) **Distributed Ledger Technology (DLT):** Tecnología de registro distribuido, permite el almacenamiento de los datos en distintos participantes de una red, sincronizados mediante mecanismos de consenso. Blockchain es un caso particular de DLT.
- i) **Ecosistema Blockchain:** Conjunto de tecnologías, plataformas, redes, servicios, aplicaciones, sistemas, bases de datos, organizaciones, desarrolladores, nodos, usuarios y procesos que interactúan en torno a una infraestructura Blockchain y permiten la ejecución de tratamientos.
- j) **Emisor (de una transacción):** Cuenta o dirección del usuario que inicia la transacción. Una cuenta o dirección de un *Smart Contract* no puede emitir transacciones, ya que no está en posesión de una clave privada para poder firmarlas.
- k) **Exchange:** Plataforma privada que facilita y permite a los usuarios la compra, venta, *trading* e intercambio de criptomonedas y otros criptoactivos (*Non Fungible Token* o NFT, etc.)
- l) **Fork o bifurcación de la cadena:** En el contexto de Blockchain, es el mecanismo principal por el cual se implementan actualizaciones de software. Se produce una división en la red y ocurre por modificaciones en el código, en el protocolo, o por toma de decisiones ante situaciones determinadas (un *Hard Fork* origina cadenas separadas e incompatibles).
- m) **Gobernanza:** Ejercicio de la autoridad y control para decidir los objetivos de una organización; priorizar y balancear los objetivos; tomar decisiones, en función de los activos, recursos, contexto y riesgos, para alcanzar dichos objetivos; y monitorizar de forma continua que el progreso de cada una de las acciones tomadas está bien orientado.
- n) **Hash:** Función que a partir de la entrada de un conjunto de caracteres de longitud variable genera como salida otra cadena de longitud fija, que satisface las siguientes propiedades: no existe un procedimiento computacionalmente viable para obtener la entrada a partir de la salida, o para encontrar dos entradas que tengan la misma salida¹³.
- o) **Infraestructura o Sistema¹⁴ Blockchain:** Una instancia concreta de una red de intercambio de información entre pares utilizando tecnologías Blockchain. En muchos casos se confunden las tecnologías para construir una Blockchain con una instancia concreta del uso de dichas tecnologías, más o menos adaptadas

¹² Aunque su mayor éxito es porque se ha usado y se usa con fines dudosos o delictivos tales como pagos en el mercado negro (*silkworm, darkweb, etc.*), pago de rescates (*ransomware*), blanqueo de capitales, sortear prohibiciones, etc. al modo de un “paraíso fiscal” digital.

¹³ Aunque dichas propiedades pueden tener vulnerabilidades en algunos casos. Ver [Introducción al hash como técnica de seudonimización de datos personales](#)

¹⁴ ISO 22739 Sistema que implementa un registro distribuido.

para unos casos de uso concretos. Una CBDC y Bitcoin pueden emplear tecnologías Blockchain, pero son dos infraestructuras radicalmente diferentes.

- p) **Integridad:** Propiedad de exactitud y completitud de los datos¹⁵. En este documento el término se usa en el sentido de que existen medidas que permiten detectar si la información ha sido modificada o alterada unilateralmente. En el entorno de Blockchain se ha confundido la gestión de la integridad con el requisito de inmutabilidad¹⁶ en una Blockchain determinada.
- q) **Nodos:** (ver Participante) dispositivo o proceso que participa en una infraestructura Blockchain y almacena una réplica completa o parcial de la cadena/tabla de bloques¹⁷. Nodo es un concepto técnico. Según su funcionalidad se pueden definir distintas clases de nodos. Los nodos validadores o mineros son aquellos que validan y agregan las transacciones al bloque, y añaden nuevos bloques a los datos registrados en la infraestructura Blockchain mediante el mecanismo de consenso correspondiente. Reciben recompensas y comisiones en forma de la criptomoneda de la Blockchain por esta labor. Las redes privadas pueden configurarse sin incluir estos incentivos.
- r) **Non Fungible Token (NFT):** Token no fungible, significa que algo es único, con propiedades distintas a otro NFT y que no se puede reemplazar. Por el contrario, los tokens que representan criptomonedas son idénticos y tienen las mismas propiedades, es decir, son fungibles¹⁸. Los ejemplos de NFT incluyen ilustraciones, cómics, coleccionables deportivos, cartas coleccionables, juegos y más.
- s) **Participante:** (ver Nodo) Personas físicas o jurídicas que configuran, operan y mantienen procedimientos de gestión, compromisos, potenciales subcontrataciones, dispositivos y programas que implementan uno o más nodos en una infraestructura Blockchain. Podrán actuar en su propio nombre o en nombre de otros. El participante es la persona que será el sujeto obligado de las distintas normativas.
- t) **Peer-to-Peer (P2P):** Infraestructura de compartición de información en la que no hay una relación jerárquica entre los intervinientes, y cada uno es independiente en la toma de decisiones sobre cómo participar en la misma.
- u) **Prueba de Concepto (Proof of Concept o PoC):** Realización de una determinada idea, método o principio con el fin de demostrar su viabilidad, o una demostración con el objetivo de verificar que algún concepto o teoría tiene potencial práctico. Una Prueba de Concepto suele tener un alcance limitado y puede no estar completa.
- v) **Receptor** (de una transacción): Cuenta o dirección destinataria de la transacción. Una cuenta o dirección de un *Smart Contract* es el receptor de la transacción cuando se efectúan llamadas a sus funciones y procedimientos.
- w) **Tecnología Blockchain:** Tecnología que permite el funcionamiento y uso de sistemas Blockchain¹⁹. Es la solución técnica que define las condiciones generales para que intervinientes independientes e iguales (pares) en Internet puedan intercambiar información, con un mecanismo para acordar qué información se va a almacenar, y un mecanismo para gestionar la integridad, tanto de la información como del orden en que se ha almacenado.

¹⁵ ISO 27000:2018

¹⁶ Inmutabilidad se define en ISO 22739:2024 como la propiedad de que los datos no pueden ser modificados o borrados una vez que se han añadido a un registro distribuido. Inmutabilidad se refiere entonces a un requisito u objetivo deseable en una infraestructura Blockchain determinada, antes que a una propiedad de dicha tecnología.

¹⁷ ISO 22739

¹⁸ <https://ethereum.org/es/nft/#what-are-nfts>

¹⁹ ISO 22739

- x) **Token:** Valor digital que representa activos físicos o digitales. Se crea y gestiona en una infraestructura Blockchain usando *Smart Contracts*. Tokenización es el proceso de convertir un activo físico o digital en un token que puede ser registrado, transferido y gestionado en una Blockchain. Este token representa una fracción, propiedad o derecho sobre el activo subyacente. Algunos tokens son usados como criptomonedas.
- y) **Transacción:** Operación que queda registrada en la Blockchain y modifica la información en ella, transfiriendo datos o valor entre el emisor y el receptor. La transacción va firmada digitalmente por el emisor y ha de ser validada por los nodos para su inclusión en un bloque/registro de la Blockchain.
- z) **Trazabilidad de datos:** Capacidad de conocer todo el ciclo de vida del dato: la fecha y hora exacta de extracción, cuándo se produjo su transformación, y cuándo se cargó desde un entorno fuente a otro destino. A este proceso se le conoce como *Data Linage*²⁰.
- aa) **Usuario:** Individuo o entidad que interactúa, en sentido amplio, con la infraestructura Blockchain (efectuar transacciones, acceder a servicios, administrar nodos, obtener información, etc.)

²⁰ <https://datos.gob.es/es/blog/importancia-de-la-catalogacion-de-datos>

III. MARCO TECNOLÓGICO Y LEGAL

Blockchain es una tecnología que surgió en 2009 y que se materializó con la moneda virtual o criptomoneda *Bitcoin*, una infraestructura basada en dicha tecnología que permitía implementar un servicio con garantías de transparencia e integridad de los pagos efectuados. La tecnología Blockchain es un caso particular de las tecnologías de registro distribuido o DLT por sus siglas en inglés (*Distributed Ledger Technology*), término que hace referencia a bases de datos distribuidas, gestionadas mediante mecanismos de consenso por múltiples participantes.

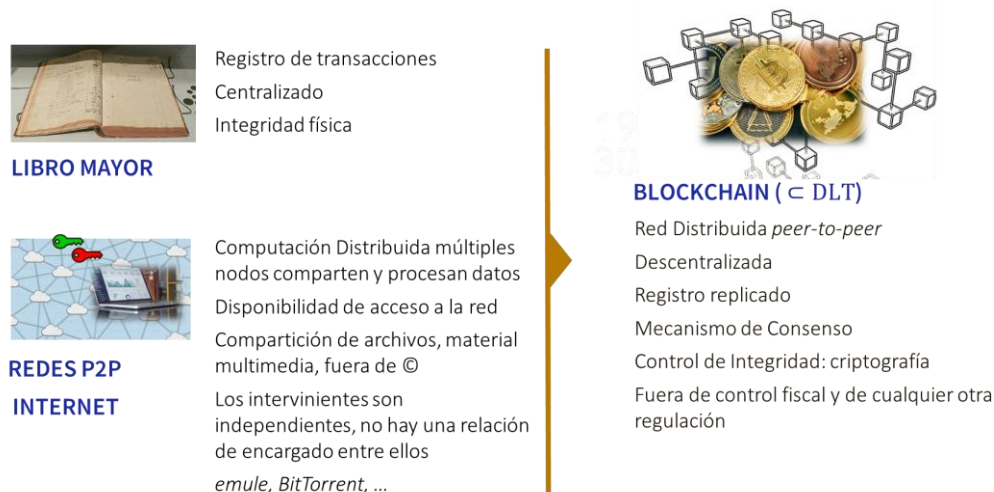


Figura 1. Blockchain no es una tecnología completamente nueva, surge como una evolución del libro mayor combinado con el uso de redes peer-to-peer (P2P) y sin intermediarios.

A. DESCRIPCIÓN DE LA TECNOLOGÍA BLOCKCHAIN Y SU APLICACIÓN

Es importante diferenciar la tecnología Blockchain de las distintas infraestructuras creadas con dicha tecnología, y que pueden ser muy distintas entre sí. En este apartado se van a describir las propiedades de la aplicación teórica de la tecnología Blockchain²¹, tal como se planteaba originalmente. Las implementaciones prácticas han modificado algunas (o muchas) de sus características fundamentales²².

De una forma simple, puede definirse una infraestructura creada con tecnología Blockchain como una red de participantes (personas físicas o jurídicas denominadas pares, *peers* o nodos) que comparten un conjunto de datos de forma distribuida, en el que se anota quién posee qué (activos en forma de datos), donde se negocia con quién se intercambian dichos activos (transacciones) y con medidas para gestionar la consistencia e integridad de los datos.

²¹ Hay que tener en cuenta que en cualquier implementación usando tecnología, hay una gran distancia entre los modelos genéricos o teóricos, y la realidad de las soluciones prácticas y comerciales. Estas no solo adaptan los conceptos a una implementación concreta, sino que se complementan con componentes, funciones y servicios adicionales que afectan a las propiedades ideales del concepto original.

²² En este texto no se explican las soluciones de capa 2, que son las tecnologías que se ejecutan sobre un protocolo de cadena de bloques que mejora la velocidad y la eficiencia de la cadena de bloques subyacente con gastos por comisiones más bajos. La capa 1 se refiere a la propia base de datos distribuida, la red que reúne todos los nodos de la cadena de bloques en un sistema con sus mecanismos de consenso subyacentes. Por ejemplo, la capa 1 de Bitcoin es la red Bitcoin. La capa 2, sin embargo, es una red superpuesta que se asienta sobre la cadena de bloques. Por ejemplo, Lightning Network es una solución de capa 2 para Bitcoin. <https://crypto.com/university/es/what-are-layer-2-scaling-solutions>. En Ethereum existen numerosas soluciones de capa 2, tales como Optimism, Arbitrum o ZKSync. <https://ethereum.org/es/layer-2/>.

Los participantes/nodos pueden entrar a formar parte de una infraestructura Blockchain concreta (p.ej. Bitcoin, Ethereum, una CBDC u otra) por su propio interés o bien por cuenta de otras entidades²³. En el texto se va a utilizar la terminología participante/nodo ya que un participante es la persona física o jurídica que gestionará uno o más nodos en la infraestructura, en su nombre o en nombre de terceros, y será el sujeto obligado en la normativa. Por otro lado, el nodo es un dispositivo o proceso que forma parte de una infraestructura concreta, es decir, un concepto técnico. Los nodos de una misma infraestructura utilizan medios compatibles, no necesariamente los mismos.

Idealmente, cada participante/nodo de la infraestructura Blockchain almacenará una copia de la cadena/tabla de bloques como la que se describe en la Figura 4, además de las estructuras de datos adicionales que implemente la infraestructura Blockchain específica. Será una decisión del participante²⁴, si no actúa por instrucciones explícitas de un tercero²⁵, la forma en la que él almacena la información (algún tipo de base de datos, otro tipo de conjunto de datos, etc.), que recursos dedica al tratamiento de la información, dónde almacena la información (en alguno de los sistemas del participante, en la nube, etc.), cuánta será la cantidad de bloques/registros que almacenará²⁶, y con qué criterios o cuándo se da acceso a dicha información, entre otros.

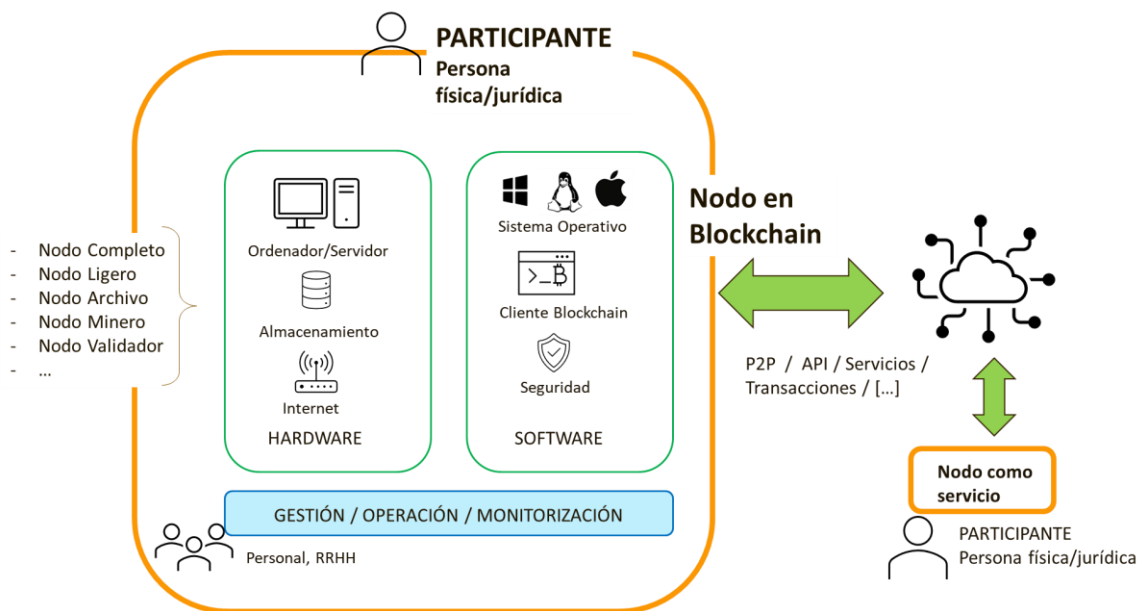


Figura 2 Un nodo de una infraestructura Blockchain es un dispositivo para conectarse a ella. Un participante es la persona que gestiona el nodo y estará sujeto a obligaciones normativas. El participante será quien tome las decisiones sobre en qué infraestructura Blockchain participa y qué/cuántos/cuando recursos físicos y humanos invertirá en el nodo para su operación y funcionamiento.

²³ Por ejemplo, se puede crear una infraestructura Blockchain con nodos bajo el control directo de distintas entidades financieras, aunque alguna de ellas pueda subcontratar esos tratamientos a otras personas jurídicas para que actúen en su nombre gestionando nodos en la misma infraestructura.

²⁴ La selección de los medios que un participante decide (excepto que nos encontramos en el caso de la nota siguiente) incluyen no solo la decisión de en qué infraestructura Blockchain decide participar, sino también la de un software que sea compatible con dicha infraestructura y la forma de implementarlo (como en cualquier sector de negocio), las máquinas en la que se va a ejecutar, la forma de almacenar la cadena de bloques y otros sistemas, facilidades y subcontratas. Hay que tener en cuenta que en infraestructura como Blockchain, y también como en todo sector de negocio, la optimización de dichos recursos es vital para obtener beneficios.

²⁵ En caso de un tratamiento de datos personales, de un responsable que llegue a especificar dichos detalles.

²⁶ En muchas infraestructuras, para que la operación de esta cumpla con casos de uso es necesario generar bloques/registros continuamente, por lo que el número de estos es elevadísimo y muchos participantes/nodos optan por solo almacenar los últimos bloques generados, obviando no solo el almacenamiento, sino el análisis de la integridad de toda la cadena. A esta práctica se le denomina *podado*.

A diferencia de los sistemas de almacenamiento centralizados, en una infraestructura Blockchain idealmente todos los participantes/nodos mantienen una copia del conjunto de datos.

El nombre "Blockchain" proviene de cómo se organiza la estructura de datos replicada en cada uno de los participantes/nodos. Los datos se almacenan en registros en los que a su vez se almacenan transacciones. A los registros se les denomina bloques en la terminología Blockchain, pero mantendremos en este texto la denominación bloques/registros para facilitar la comprensión de las explicaciones.

Los bloques/registros están enlazados cronológicamente mediante el almacenamiento en cada bloque/registro del hash del bloque/registro anterior. Esta es una técnica para gestionar la integridad de la información, ya que, si la información de un bloque/registro cambia, se detectaría por la inconsistencia de los valores de hash almacenados.

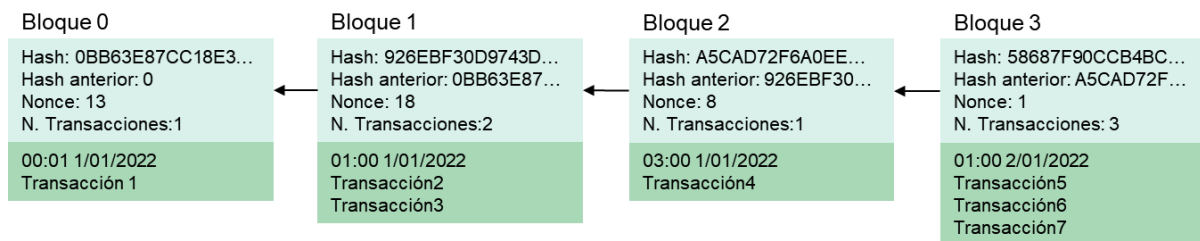


Figura 3. Representación didáctica de un conjunto de bloques/registros como una cadena.

Al conjunto de todos los bloques/registros se le denomina cadena de bloques en terminología Blockchain. Esta denominación puede llevar a confusión sobre cómo y dónde están los bloques. La cadena realmente se almacena en cada nodo como una estructura de datos en la que los bloques/registros están organizados. Esta estructura es una base de datos, que en algunos casos será relacional pero lo más habitual es de tipo clave-valor²⁷. En la Figura 4, se representa la cadena como una tabla, que estaría replicada en los participantes/nodos de la infraestructura Blockchain. Por ello, se utilizará el término cadena/tabla de bloques en este texto.

NºBloque	Hash	Hash bloque anterior	Nonce	N. Transc	Fecha	Transacciones
0	0BB63E87CC18E3...	0	13	1	01/01/2022 0:01	Transacción1
1	926EBF30D9743D...	0BB63E87...	18	2	01/01/2022 1:00	Transacción2 Transacción3
2	A5CAD72F6A0EE...	926EBF30...	8	1	01/01/2022 3:00	Transacción4
3	58687F90CCB4BC...	A5CAD72F...	1	3	02/01/2022 1:00	Transacción5 Transacción6 Transacción7
4						

Figura 4. Representación del almacenamiento de los bloques anteriores en un nodo, en forma de registros en una tabla de una base de datos relacional. Normalmente, los bloques/registro estarán almacenados en una base de datos u otros sistemas para su explotación eficiente. Esta tabla no refleja las estructuras de datos adicionales que es necesario almacenar en el nodo para gestionar otra información.

Además, los participantes/nodos necesitan almacenar varias estructuras de datos adicionales²⁸, distintas de la cadena/tabla de bloques, que permiten su funcionamiento y operación eficiente, como el acceso a la información sin necesidad de procesar toda la cadena desde el bloque inicial o génesis. Algunas de estos conjuntos de datos adicionales son los estados y balances de las cuentas; el almacenamiento de los *Smart Contracts*; un

²⁷ <https://aws.amazon.com/es/nosql/key-value/>

²⁸ <https://ethereum.org/en/developers/docs/data-structures-and-encoding/patricia-merkle-trie/>, <https://github.com/ethereum/go-ethereum/blob/master/core/rawdb/schema.go>, <https://geth.ethereum.org/docs/fundamentals/command-line-options>

registro temporal de transacciones pendientes; recibos de transacción, que proporcionan información sobre el resultado de la transacción, incluyendo los eventos y logs emitidos por un *Smart Contract*; información sobre otros nodos para mantener las conexiones activas y gestionar la comunicación y sincronización; algunos parámetros de configuración de la red y del nodo; estados intermedios y copias del estado de la cadena en momentos específicos para facilitar la sincronización; etc. La implementación exacta puede variar dependiendo de la infraestructura Blockchain específica y de la optimización realizada por cada participante/nodo.

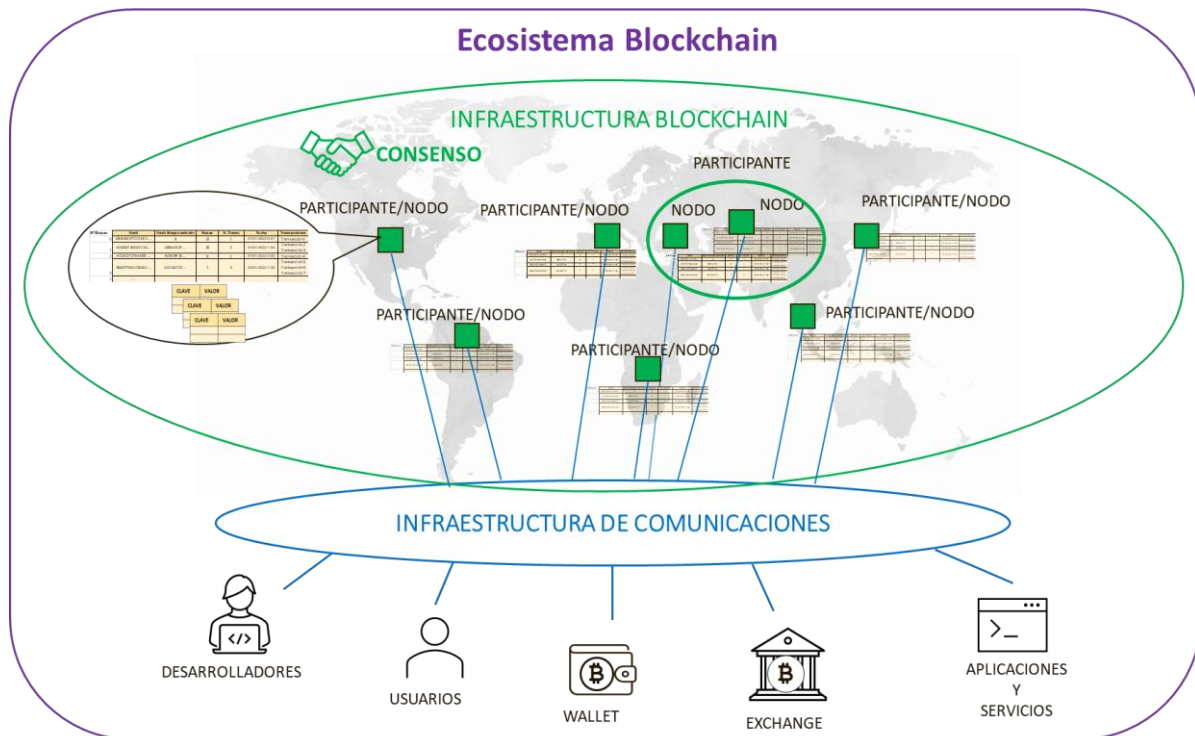


Figura 5. La infraestructura Blockchain está formada por una serie de participantes/nodos, cada uno almacenando los bloques/registros en una estructura de datos denominada cadena/tabla de bloques.

En general, en las infraestructuras Blockchain se supone que no hay una entidad central para verificar y validar transacciones. Por ello es necesario recurrir a mecanismos de consenso entre los participantes para tomar decisiones, actualizar datos y mantener la consistencia de la información almacenada. De esta forma las transacciones se almacenan en registros ordenados de forma temporal que están vinculados cada uno con el anterior, formando una cadena aparentemente "inmutable" y transparente, que incluso puede actualizarse "automáticamente" mediante contratos inteligentes alojados en la propia cadena.

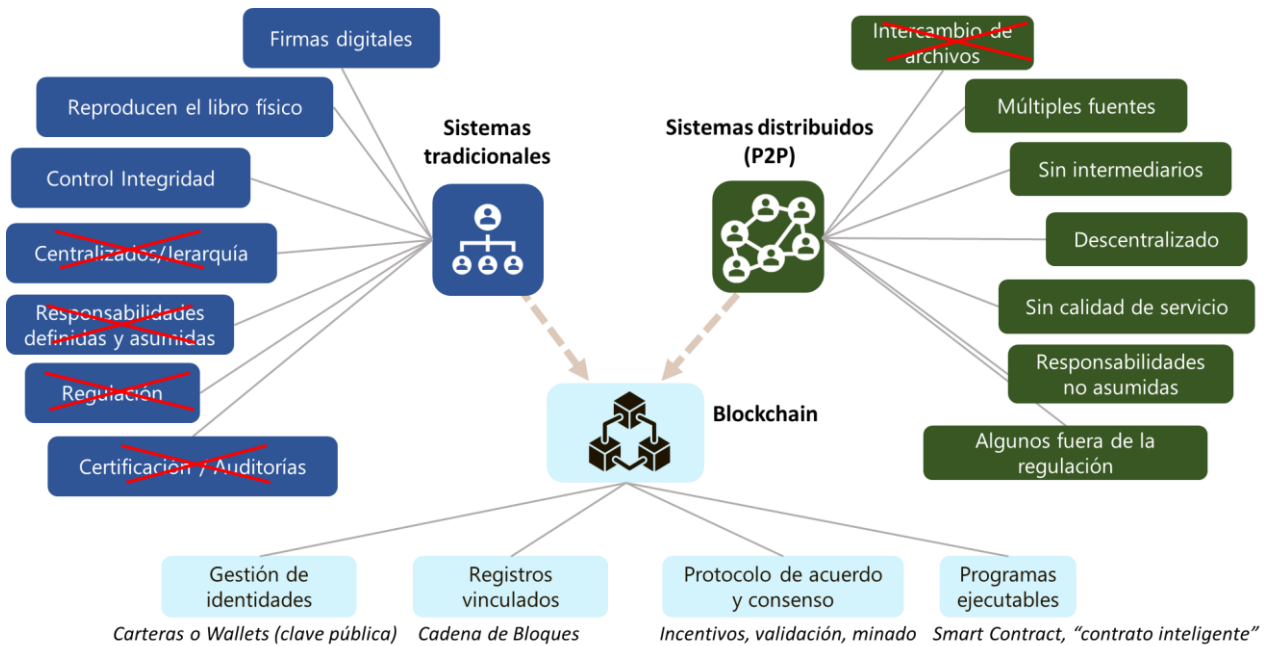


Figura 6. Blockchain hereda algunas características de los sistemas tradicionales y muchas de los sistemas distribuidos P2P, a las que añade nuevos elementos como la gestión de identidades, registros vinculados mediante hash, protocolos de consenso y programas ejecutables (en la figura aparecen tachadas características no heredadas por la tecnología Blockchain genérica).

Los principios generales de las técnicas Blockchain, que se han materializado en las distintas infraestructuras en mayor o menor grado, son:

- **Descentralización:** Los participantes de la Blockchain (nodos) forman una red P2P descentralizada, donde cada uno de ellos tiene una copia replicada de la tabla de registros encadenados. No hay una entidad única que controle y gestione los tratamientos que se realizan sobre los datos. Los nodos son independientes, no hay una relación jerárquica entre ellos y actúan en su propio nombre. No asumen ninguna obligación ni siguen instrucciones y pueden parar su operación en cualquier momento. En muchas infraestructuras Blockchain prácticas la descentralización no existe en determinados aspectos o está limitada.
- **Control de integridad:** Una vez registrados los datos se implementan mecanismos criptográficos para detectar cualquier modificación, borrado o reordenación de los registros.
- **Auditabilidad y transparencia:** Las transacciones son visibles por todos los que pueden acceder a la red. En algunas infraestructuras se establecen límites a esta propiedad, por ejemplo, solo a los participantes/nodos o a terceros seleccionados.
- **Mecanismo de consenso:** El mecanismo de consenso establece la confianza entre los participantes/nodos (todos o algunos asignados como nodos mineros o validadores) para que cooperen en mantener la consistencia e integridad de la tabla y para incorporar nuevos bloques de transacciones como un registro en dicha tabla.

El control de integridad, unido a una replicación masiva de los bloques en distintos nodos, pretenden dar cierta medida de "inmutabilidad" de la información. Sin embargo, la realidad es que hay varios factores que hacen que dicha inmutabilidad pueda verse comprometida, como se ha explicado en el equívoco 1.

Desde la perspectiva de las políticas de acceso, participación y control con los que se diseña e implementa una Blockchain, éstas se suelen clasificar en infraestructuras Blockchain públicas o privadas, y en permissionadas o no permissionadas.

- Una infraestructura Blockchain es pública cuando cualquier participante puede decidir libremente unirse a ella para formar parte de la infraestructura como un nodo, en tanto que una privada incorpora un proceso de gobernanza que la hace accesible solo a un número restringido de participantes, estando generalmente controlada por una entidad privada o consorcio.
- Una infraestructura Blockchain no-permisionada carece de condiciones para unirse a la infraestructura, sin restricciones. Una red permissionada incorpora procesos de gobernanza que la hace accesible a todo participante siempre que supere un proceso de autorización.

Las criptomonedas más conocidas (*Bitcoin, Ethereum, Solana, Tether, etc.*) se corresponden con el caso de infraestructuras Blockchain públicas-no permissionadas. Estas características hacen posible uno de sus principales atractivos, que es la eliminación de intermediarios en el procesamiento de transacciones entre partes, pero es también una de sus principales debilidades cuando se trata de establecer garantías jurídicas a su operación.

Estas debilidades se han hecho manifiestas en casos de desacuerdos en la comunidad y participantes. Por ejemplo, el caso *DAO Fork* de Ethereum²⁹, como respuesta a un ataque que causó pérdidas millonarias, o el *Bitcoin Cash Fork*³⁰, que en esta ocasión fue una decisión proactiva para abordar las limitaciones originales de Bitcoin. En ambos casos, los participantes tuvieron que improvisar un mecanismo de gobernanza que, además, resultó en una bifurcación y separación en dos redes Blockchain y criptomonedas distintas por las diferencias en la toma de decisiones: Ethereum (ETH) y Ethereum Classic (ETC), y Bitcoin (BTC) y Bitcoin Cash (BCH) respectivamente.

La evolución de la tecnología ha hecho que sobre la infraestructura de Blockchain se hayan construido infraestructuras adicionales (al estilo de los servicios *Over The Top* en las infraestructuras de telecomunicaciones), que implementan funcionalidades adicionales o restricciones, conocidas como *Layer 2 Blockchain*, o Blockchain de Capa 2³¹ (canales de estado o pago, *sidechains, rollups, etc.*)

B. EQUÍVOCOS RELATIVOS A TECNOLOGÍAS E INFRAESTRUCTURAS BLOCKCHAIN

Como se ha señalado en el capítulo de Conceptos básicos, a la hora de analizar desde el punto de vista de protección de datos el impacto que puede tener en un tratamiento la elección de determinadas opciones tecnológicas con relación al cumplimiento del RGPD, es fundamental definir con rigor la terminología empleada y asegurarse de comprender con precisión sus implicaciones. La terminología empleada en el ámbito de la tecnología Blockchain puede llevar a equívocos a aquellos que no conocen el detalle de la implementación de la tecnología³². Para poder llegar a conclusiones como implicaciones legales precisas, hay que huir de las generalidades y las etiquetas más o menos comerciales y establecer las definiciones con rigor, para que dichas conclusiones estén basadas en hechos definidos con objetividad³³.

²⁹ <https://ethereum.org/es/history/#dao-fork>

³⁰ https://es.wikipedia.org/wiki/Bitcoin_Cash

³¹ <https://ethereum.org/es/layer-2/>

³² Esto es común en cualquier tecnología, en la que es habitual utilizar términos comerciales, algunos con propósito de marketing, o con un significado muy concreto en dicho contexto y distinto de otros contextos en los que se emplea.

³³ De otra forma, será difícil aplicar rigor jurídico a un ámbito definido con ambigüedad, sin perjuicio de que se generen resúmenes para público no especializado.

En el entorno de Blockchain se emplean muchos términos que pueden llevar a equívocos sobre las implicaciones, posibilidades y limitaciones de esta tecnología. Algunas de las más importantes se desarrollan a continuación.

1. Equívoco: Inmutabilidad

La inmutabilidad se define en ISO 22739:2024 como la propiedad de que los datos no pueden ser modificados o borrados una vez que se han añadido a un registro distribuido. Sin embargo, antes que una propiedad física o tecnológica, es un requisito u objetivo buscado en algunas infraestructuras Blockchain. Como la naturaleza de todo dato digital es la volatilidad, se pretende alcanzar cierto grado de inmutabilidad con medidas técnicas de gestión de la integridad, que permiten detectar datos alterados o eliminados, con un acuerdo supuesto entre todos los participantes/nodos en no alterar la integridad del conjunto de bloques/registros ya consolidado, y con la disposición a una replicación incontrolada de dicho conjunto de bloques/registros con la esperanza de que haya alguien interesado en almacenar la información.

Todas estas circunstancias en algún momento se han alterado. Por ejemplo, puede alterarse la cadena por un acuerdo entre los usuarios para eliminar un bloque o transacción, que, aunque haga manifiesta una inconsistencia, no permite recuperar la información eliminada. Esto es más factible en infraestructuras Blockchain privadas o permissionadas y supone un cambio en el acuerdo entre los participantes/nodos, es decir, una medida de gobernanza.

El recálculo de los valores criptográficos por una mayoría de usuarios también permitiría la alteración de valores en la Blockchain. Hay que tener en cuenta que la infraestructura Blockchain no está libre de ataques y usos no deseados: el comportamiento malicioso de los nodos (si superan la mayoría, conocido como ataque del 51%), vulnerabilidades en el código o errores en la implementación pueden comprometer la integridad de la cadena.

Más simple es el hecho, que ha sucedido múltiples veces, de abandono de los participantes/nodos del proyecto de cadena de bloques³⁴, aquellas levantadas temporalmente para docencia, o la poda³⁵ de bloques antiguos. En estos dos últimos casos, si no hay implementados mecanismos de gobernanza que proporcionen garantías de calidad de servicio sobre la disponibilidad de los datos, estos desaparecen o no estarán accesibles.

Finalmente, muchas Blockchain incorporan mecanismos para implementar actualizaciones planificadas o mejoras en los protocolos, tales como los *Bitcoin Improvement Proposals* (BIP)³⁶ o *Ethereum Improvement Proposals* (EIP)³⁷, que introducen cambios en la red y modificaciones. Por otro lado, la toma de decisiones frente a eventos no previstos, en algunas infraestructuras Blockchain, como el conocido *DAO Fork* de Ethereum, han terminado en cambios en el consenso para revertir los efectos producidos, modificando el estado de la información almacenada.

Por lo tanto, no existe la propiedad de inmutabilidad en una Blockchain. Los datos han desaparecido en ocasiones anteriores.

2. Equívoco: La gestión de las infraestructuras Blockchain es completamente descentralizada

La descentralización es uno de los principios fundamentales del concepto de tecnología Blockchain, y se promueve como una de sus características más importantes. Sin embargo,

³⁴ Infraestructuras Blockchain desaparecidas son: *OneCoin* y *Finiko*, *BitConnect*, *GetGems*, *SpaceBIT*, *PayCoin*, etc.

³⁵ Eliminación de parte de la información de la Blockchain almacenada en un nodo para ahorrar espacio.

³⁶ <https://github.com/bitcoin/bips>

³⁷ <https://eips.ethereum.org/>

en la práctica, incluso las infraestructuras Blockchain de tipo público y no-permisionado son parcialmente centralizadas en ciertos aspectos de su gestión, revelando una concentración de poder en muy pocos intervinientes.

Uno de los ejemplos más claros de esta concentración es la generación de nuevos bloques/registros. En la mayoría de las infraestructuras Blockchain el proceso de añadir bloques a la cadena está dominado por un número reducido de grandes grupos de nodos mineros o validadores, conocidos como *Pools*. Estos grupos, dada su capacidad de procesamiento o participación en la red (según el mecanismo de consenso utilizado) controlan una parte significativa de la capacidad para la creación de bloques, lo que genera un riesgo real de centralización operativa en un sistema que se concibió para ser totalmente descentralizado.

Otro caso se manifiesta en el proceso de toma de decisiones de gobernanza de las infraestructuras Blockchain. Este suele estar concentrada en un pequeño grupo de desarrolladores o entidades que tienen una influencia muy significativa sobre la toma de decisiones clave, como actualizaciones y cambios en los protocolos y software.

3. Equívoco: No existe un marco de gobernanza en las infraestructuras Blockchain, y si existe, es completamente automatizado

Existe una gobernanza de facto en toda infraestructura Blockchain, pero normalmente es incompleta, especialmente desde la perspectiva de protección de datos. Esto es debido a que no se ha contemplado el cumplimiento del RGPD entre los objetivos del marco de gobernanza definidos desde el diseño.

Frecuentemente se argumenta que la gobernanza en infraestructuras Blockchain es automática, democrática, justa y equitativa, pero la realidad difiere bastante. Por ejemplo, en la mayor parte de infraestructuras Blockchain hay una concentración de decisiones en ciertos grupos, como fundadores, desarrolladores o la comunidad más influyente. También, algunos mecanismos de consenso favorecen a los que tienen más participación en cada infraestructura Blockchain concreta.

En particular, ante la toma de decisiones frente a eventos no previstos, en algunas infraestructuras Blockchain se han adoptado mecanismos de gestión específicos de forma sobrevenida. Es decir, se ha tenido que improvisar al no haber desarrollado una gobernanza basada en una gestión de riesgos. Esto ha supuesto crisis muy serias en algunas infraestructuras, originado desacuerdos entre los participantes/nodos con relación a las decisiones adoptadas ante estos eventos, y que han ocasionado la división de la infraestructura³⁸.

4. Equívoco: En una infraestructura Blockchain los nodos actúan de forma automática

Los nodos mineros y validadores no son, como algunas veces se ha querido transmitir, máquinas a las que no se puede reclamar responsabilidad de ningún tipo.

Al contrario, los nodos están formados por un conjunto de recursos, seleccionados y configurados según los intereses específicos de las personas que los gestionan, y puestos a disposición de una infraestructura Blockchain concreta, y de una forma específica, por decisión de dichos gestores. Estos toman decisiones autónomas sobre en qué

³⁸ Además de otros ya referenciados en este documento, Bitcoin Satoshi Vision (BSV) surgió como consecuencia del enfrentamiento entre dos propuestas contenciosas para actualizar Bitcoin Cash, provocando una separación (*Hard Fork*) de Bitcoin Cash.

infraestructura Blockchain participar, qué medios emplear³⁹, qué transacciones incluir en un bloque, ya que los participantes/nodos pueden ordenar o excluir transacciones en un bloque que ellos mismos están produciendo, con el objetivo de obtener un beneficio adicional (*Maximum Extractable Value o MEV*)⁴⁰, y cómo seguir las actualizaciones entre otros.

A menos que actúen en nombre y por encargo de otra entidad, no están obligados a seguir instrucciones específicas y, entre otras cosas, pueden cesar su operación en cualquier momento.

5. Equívoco: Todas las infraestructuras Blockchain tienen las mismas propiedades que el modelo ideal sugerido en la definición original de tecnología Blockchain

El modelo ideal sugerido originalmente en la tecnología Blockchain representa lo que sería una aproximación a una implementación concreta de una infraestructura Blockchain. Incluso la infraestructura Bitcoin original se desvía ligeramente de los principios ideales, por ejemplo, en cuanto a descentralización de la gestión de la gobernanza.

Por otro lado, las distintas infraestructuras Blockchain de uso general adaptan dichos principios a sus propios requisitos⁴¹, lo que las hace incompatibles entre sí. Por ejemplo, las infraestructuras Blockchain privadas-permisionadas se pueden alejar mucho de dichos principios.

6. Equívoco: El código es ley

El código es ley⁴² es una afirmación que simplifica en exceso la realidad de la aplicación práctica de tecnologías Blockchain.

Dicha afirmación pretende establecer que las decisiones están en manos únicamente de un programa de ordenador, en particular, de los llamados *Smart Contracts*. De esta forma, define un entorno en el que, teóricamente, la ejecución de las leyes y principios humanos no sea efectiva, y realizar un desvío de la responsabilidad en la toma de decisiones y de sus consecuencias.

Sin embargo, los *Smart Contracts* son programas realizados por personas, para cumplir objetivos definidos por dichas personas y, además, los eventos que inician la ejecución de los programas son iniciados por personas. Además, los *Smart Contracts*, como todo software, tienen vulnerabilidades que son explotadas por atacantes y existen variantes de *Smart Contract* que permiten modificar su comportamiento (*Proxy*⁴³, Oráculos⁴⁴, etc.).

³⁹ Recursos de conectividad, computación, gestión y humanos. Esto va más allá de utilizar un software compatible con una Blockchain concreta, sino además tomar decisiones qué sistemas se ejecuta los procesos (propios, en la nube, subcontratados, mixtos), la forma en la que él almacena la información (algún tipo de sistema de base de datos, otro tipo de conjunto de datos, etc.), dónde almacena la información (en alguno de los sistemas del participante, en la nube, etc.), cuánta será la cantidad de bloques/registros almacenado, con qué criterios o cuando se da acceso a dicha información, etc., sino actúa por instrucciones explícitas de un tercero.

⁴⁰ <https://ethereum.org/es/developers/docs/mev/>

⁴¹ Las distintas variantes pueden presentar diferentes grados de descentralización (como Ripple, con descentralización limitada), diferentes mecanismos de consenso, o arquitecturas que optimizan rendimiento y escalabilidad (p. ej., Solana o Polkadot).

⁴² <https://ethereumclassic.org/es/why-classic/code-is-law>

⁴³ Un *Smart Contract* de tipo *Proxy* delega las llamadas a otros *Smart Contracts* objetivo, permitiendo la actualización de estos *Smart Contracts* objetivo. El *Proxy* tiene como variable actualizable la dirección del *Smart Contract* objetivo.

⁴⁴ Servicios que proporcionan datos del mundo real a *Smart Contracts* (<https://es.cointelegraph.com/learn/what-is-a-blockchain-oracle-and-how-does-it-work>)

7. Equívoco: Las actuales infraestructuras Blockchain garantizan el control del usuario sobre sus propios datos

La realidad es que la mayoría de las infraestructuras Blockchain, tal y como se han planteado hasta el momento, no permiten al usuario (persona física o jurídica) controlar quién accede a sus datos, cuánto tiempo se almacenan sus datos, cómo ejercer sus derechos y con qué fines se van a tratar.

Este no es un problema de la tecnología Blockchain en sí, sino de cómo se han diseñado las infraestructuras actuales, al no contemplar la protección de datos desde el diseño ni por defecto.

8. Equívoco: La tecnología Blockchain es incompatible con el RGPD

La mayoría de las infraestructuras Blockchain se han construido con el propósito de estar al margen de toda regulación. Por supuesto, si un tratamiento o conjunto de tratamientos se diseñan para que no cumplan una normativa será muy difícil adaptarlos para que así sea. En el caso de las infraestructuras Blockchain esto sucede, generalmente, tanto con la normativa de protección de datos, como con otras normativas como las fiscales o las comerciales.

El hecho de que en una infraestructura Blockchain no se haya contemplado como uno de los objetivos el cumplimiento del RGPD, no es problema de la tecnología en sí, es problema de los objetivos y las decisiones de los diseñadores que la han construido. Si hubieran contemplado objetivos de cumplimiento normativo desde el diseño, se hubieran implementado los mecanismos de gestión oportunos. Y esto es independiente de que nos encontremos con cualquier tipo de infraestructura Blockchain.

9. Equívoco: Los Smart Contract son autónomos e inteligentes

Los *Smart Contracts* son programas almacenados en la infraestructura Blockchain en el que el resultado de cualquier ejecución del programa se registra en la misma⁴⁵. Son programas automatizados que ejecutan acciones predefinidas cuando se cumplen ciertas condiciones que se han programado, ejecutadas al ser invocados mediante transacciones. Su funcionamiento está limitado por su código y los datos que reciben, existiendo además instrumentos que permiten al *Smart Contract* actualizar los estados internos de la Blockchain a partir de información externa (tales como los denominados oráculos⁴⁶).

Es decir, no son "inteligentes" en el sentido de poseer autonomía o capacidad de toma de decisiones. Tampoco puede considerarse como un contrato en sentido jurídico estricto.

La implementación de *Smart Contracts* en escenarios donde se manejan datos personales entra dentro del ámbito definido por el artículo 22⁴⁷ del RGPD y, por tanto, debe ser cuidadosamente evaluada desde el punto de vista del cumplimiento normativo, particularmente en lo que respecta a la protección de los derechos de los individuos frente al tratamiento automatizado de su información.

⁴⁵ ISO 22739

⁴⁶ ISO 22739: Servicio actualiza el estado de la infraestructura Blockchain utilizando datos externos a la tabla/cadena de bloques de la Blockchain.

⁴⁷ El artículo 22 del RGPD establece que las personas tienen derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que produzca efectos jurídicos en ellas o las afecte significativamente de modo similar, con algunas situaciones excepcionales.

10. Equívoco: En una infraestructura Blockchain los datos solo están en las transacciones y los bloques.

La idea de que en una infraestructura Blockchain solo se almacenan los datos en los bloques/registros, y en las transacciones dentro de ellos es incompleta. Esto solo se produce en la descripción teórica de la tecnología Blockchain, sin embargo, la implementación real de una infraestructura concreta es más compleja.

Por ejemplo, los nodos, además de las cadenas/tablas de bloques, necesitan almacenar una variedad de datos adicionales, entre los que se incluyen el almacenamiento propio de los *Smart Contracts* y, los recibos de las transacciones que involucran llamadas a sus funciones y procedimientos. Estos recibos de transacciones, conocidos como *receipts* o *logs*, son registros que se almacenan o enlazan en la infraestructura Blockchain y contienen información sobre el resultado de la transacción y los eventos emitidos por el *Smart Contract*. Estos eventos (programados en el *Smart Contract*) facilitan la comunicación entre los *Smart Contract* y las interfaces de usuario de las aplicaciones desplegadas en la infraestructura Blockchain, y sus propósitos son el de devolver valores a la interfaz de usuario para activar acciones en ella, o como un log o forma de almacenamiento barato (teniendo en cuenta los costes asociados a las transacciones). De esta manera, la infraestructura Blockchain no solo se limita a gestionar transacciones financieras, sino que también se convierte en una plataforma para almacenar información adicional relacionada con la ejecución de *Smart Contracts*.

Otro ejemplo son los almacenamientos *off-chain*. El almacenamiento *off-chain* supone almacenar parte de la información que idealmente estaría en los bloques/registros, en una estructura de datos distinta de la cadena/tabla de bloques. La vinculación entre ambos conjuntos de datos se almacenaría en las transacciones de los bloques. La estructura de datos que conforma la *off-chain* podría ser tecnología de base de datos, o bien otro tipo de cadena de bloques/registros. Además, podría estar replicada también en todos los nodos/participantes, en solo alguno de ellos, o en un almacenamiento centralizado.

En cualquier caso, el almacenamiento *off-chain* forma parte de la infraestructura Blockchain. Los tratamientos para la gestión de dicho almacenamiento, y aquellos que se implementen sobre dicho almacenamiento, también que emplee almacenamiento deben garantizar y poder demostrar el cumplimiento del RGPD. Es decir, los requisitos de cumplimiento del RGPD no desaparecen por desplazar los datos personales de una estructura de datos (la cadena/tabla) a otra. Es más, hay que demostrar que no hay datos personales en la cadena/tabla o en otras estructuras de datos como se ha señalado en este apartado.

Para finalizar, otro ejemplo es toda la información que en copias temporales y de trabajo está almacenada en participantes/nodos, en sus servicios subcontratados, y en cualquier otro interviniente en el ecosistema que permite que una infraestructura Blockchain funcione.

C. DATOS PERSONALES

El uso de una infraestructura Blockchain para el tratamiento de datos exige, de forma general, que el usuario (ya sea persona física o jurídica) disponga de una cuenta. El requisito mínimo para tener una cuenta es estar en posesión de un par de claves pública/privada que le permita firmar las transacciones e identificarse en la Blockchain.

Pueden usarse piezas de software, ajenas a la infraestructura denominadas carteras o *wallets*⁴⁸, para almacenar las cuentas y efectuar transacciones para un usuario. Estas carteras formarían parte del conjunto de aplicaciones del ecosistema de una infraestructura Blockchain concreta.

Cuando un usuario sea una persona física, la clave pública o dirección de una cartera es un dato personal, así como todo identificador único que vincula toda la actividad de dicha persona en la infraestructura Blockchain⁴⁹.

En una infraestructura Blockchain los datos personales⁵⁰ pueden encontrarse en:

- Transacciones (cuenta origen, cuenta destino y datos de la transacción).
- Balances de las cuentas.
- Almacenamiento de los *Smart Contracts* o contratos inteligentes (programas almacenados en la Blockchain que ejecutan acciones sobre su almacenamiento y otros *Smart Contracts* cuando se les invoca mediante una transacción).
- Recibos de transacciones (eventos/logs de *Smart Contracts*).
- Almacenamiento *off-chain*.
- Cualquier otro tipo de almacenamiento que posea el participante/nodo más allá de la propia copia de la cadena/tabla, y los almacenamientos temporales.

D. TRATAMIENTOS Y RESPONSABILIDADES

Una infraestructura Blockchain permite que sobre ella se implementen determinados tratamientos, como, por ejemplo, una consolidación de balances entre sucursales, gestión de certificados, o de acreditación de títulos académicos. Estos tratamientos utilizan la infraestructura Blockchain como parte de las operaciones que conforman el tratamiento. Entre los sistemas adicionales o intervinientes podemos encontrar las carteras⁵¹, los *Exchange*, aplicaciones descentralizadas⁵² (*dApps*), proveedores de interfaces y APIs para interactuar con Blockchain⁵³, oráculos⁵⁴ (servicios que proporcionan datos del mundo real a *Smart Contracts*), Pools de nodos de minería/validación⁵⁵, redes de Internet, etc.

A su vez, la infraestructura en sí misma, independientemente del número de tratamientos que se implementen sobre ella, requerirá la implementación de una serie de tratamientos para su propia gestión⁵⁶ como:

⁴⁸ ISO 22739: Aplicación o mecanismo utilizado para generar, administrar, almacenar o usar claves privadas y claves públicas u otros activos digitales. Una wallet puede implementarse en software, implementarse como un módulo de hardware o escribirse en medios no digitales como papel o metal. Los activos digitales almacenados en wallets pueden incluir, por ejemplo, tokens no fungibles (NFT).

⁴⁹ Existen muchos ejemplos. Se adjunta una declaración de la Real Policía Montada del Canadá que, en una acción de recuperación de dinero por estafa en Bitcoin, declara: "This investigation demystified the fact that cryptocurrency transactions are completely anonymous and that there's no chance of recovery of the victim's funds". <https://rcmp.ca/en/gazette/police-help-victim-crypto-fraud-get-money-back>

⁵⁰ Incluso cuando el usuario no sea una persona física pero las acciones registradas en la cadena se puedan vincular a una persona física por datos que forman parte del tratamiento que se implementa sobre Blockchain.

⁵¹ Las carteras o *wallets* además de almacenar las claves criptográficas permiten operar y efectuar transacciones en Blockchain https://es.wikipedia.org/wiki/Cartera_de_criptodivisa

⁵² https://es.wikipedia.org/wiki/Aplicaci%C3%B3n_descentralizada

⁵³ Por ejemplo, nodos como servicio: <https://ethereum.org/es/developers/docs/nodes-and-clients/nodes-as-a-service/>

⁵⁴ <https://es.cointelegraph.com/learn/what-is-a-blockchain-oracle-and-how-does-it-work>, <https://ethereum.org/es/developers/docs/oracles/>

⁵⁵ Pools de Staking en Ethereum: <https://ethereum.org/es/staking/pools/>, Pools de minería en Bitcoin: <https://miningpools.com/es/bitcoin/>

⁵⁶ De igual forma que otras infraestructuras digitales, por ejemplo, el caso de las redes de telecomunicaciones, pero también en otras infraestructuras no digitales, como es el caso de empresas logísticas. Estas son empresas que manejan muchas contrataciones o están organizadas en forma de cooperativas, que implementan tratamientos para su propia gestión (como el de RR.HH.), y que son utilizadas por otras empresas para implementar otros tratamientos, como venta por Internet, distribución de medicamentos, etc.

- Proporcionar el servicio al usuario final: el correspondiente al conjunto de actividades y recursos para satisfacer las necesidades del usuario y proporcionarle la calidad de servicio adecuada.
- Efectuar transacciones en la Blockchain: transformación de los datos en operaciones válidas para la Blockchain.
- Validar o minar los bloques de transacciones: verificar y añadir transacciones a la Blockchain según el mecanismo de consenso.
- Gestionar la Blockchain según el mecanismo de consenso: verificar y almacenar bloques, aplicar actualizaciones, acceso, etc.
- Implementar cualquier otro tratamiento adicional que un nodo realiza sobre las transacciones, como podría ser reordenar transacciones, administrar las transacciones pendientes (*mempool*), proporcionar datos y servicios a aplicaciones (aplicaciones descentralizadas o *dApps*), almacenamiento de datos históricos, procesar y atender consultas, procesar eventos de los *Smart Contracts*, detectar patrones y comportamientos, etc.

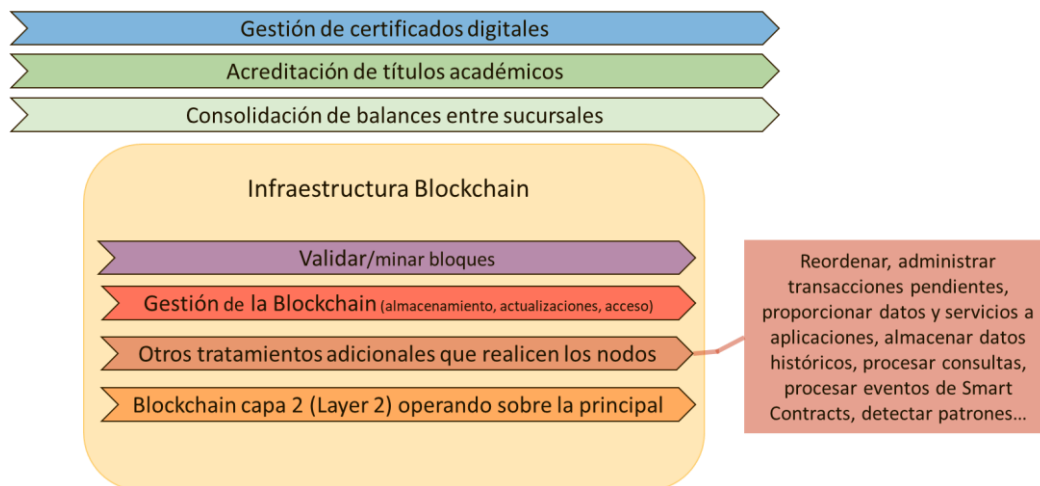


Figura 7. Tratamientos en y sobre una infraestructura Blockchain.

En toda infraestructura Blockchain es crucial establecer claramente las responsabilidades y obligaciones de cada participante en la red, teniendo en cuenta que toda entidad que realice tratamiento de datos personales y no lo haga por cuenta de un responsable, no podrá ser encargado de tratamiento⁵⁷.

E. CUMPLIMIENTO DEL RGPD

Cualquier tratamiento de datos personales debe adecuarse al RGPD. El diseño y características de la gran parte de las infraestructuras Blockchain actualmente implementadas presenta retos significativos para cumplir con los principios del RGPD en los tratamientos que se ejecutan en o sobre la infraestructura Blockchain. Esto es debido a las razones que se desarrollan a continuación.

En primer lugar, en los diseños de la infraestructura no se ha tenido en cuenta la aplicación de la protección de datos desde el diseño. Si bien el artículo 25 del RGPD aplica a responsables de tratamiento, hay que hacer notar que el considerando 78 del RGPD manifiesta que “Al desarrollar, diseñar, seleccionar y usar aplicaciones, servicios y productos que están basados en el tratamiento de datos personales o que tratan datos personales para

⁵⁷ Párrafo 76 de las Directrices 07/2020 sobre los conceptos de «responsable del tratamiento» y «encargado del tratamiento» en el RGPD.

cumplir su función, ha de alentarse a los productores de los productos, servicios y aplicaciones a que tengan en cuenta el derecho a la protección de datos cuando desarrollan y diseñen estos productos, servicios y aplicaciones, y que se aseguren, con la debida atención al estado de la técnica, de que los responsables y los encargados del tratamiento están en condiciones de cumplir sus obligaciones en materia de protección de datos.”. Esto no traslada las obligaciones de los responsables a los productores de servicios y soluciones. Los responsables tienen la obligación de seleccionar los servicios y soluciones que les permitan “garantizar y poder demostrar que el tratamiento es conforme con el presente Reglamento” (artículo 24(1) del RGPD).

Por otro lado, gran parte de las infraestructuras Blockchain se construyen generalmente con módulos o componentes de código abierto⁵⁸. El hecho de usar código abierto no debería implicar, como sucede en muchas ocasiones, que dichos componentes no estén apropiadamente documentados en su diseño y con relación a las pruebas que permitan demostrar lo establecido en el párrafo anterior. De hecho, muchos de estos componentes son de uso libre pero muy opacos en sus funcionalidades, incluyen un alto nivel de dependencias no identificadas, y es muy difícil actualizarlos o incluso garantizar su funcionamiento. Esto último es especialmente crítico a la hora de garantizar y poder demostrar el cumplimiento del RGPD (artículo 24(1) del RGPD), implementar protección de datos desde el diseño (artículo 25 del RGPD) y garantizar la resiliencia de los tratamientos contruidos sobre ellos (artículo 32(1)b) del RGPD).

Cumplir con el RGPD en el tratamiento de datos personales que emplean una o más infraestructuras Blockchain requiere dos fases: 1) garantizar el cumplimiento normativo y, una vez conseguido, 2) evaluar y valorar los riesgos, algunos de los cuales pueden mitigarse con medidas jurídicas, organizativas y técnicas. En caso de alto riesgo, hay que superar la evaluación de la idoneidad, necesidad y proporcionalidad del tratamiento.

En el caso de infraestructuras Blockchain, los aspectos de especial relevancia con relación al cumplimiento del RGPD son los relativos a la exactitud y la limitación del plazo de conservación. Y ello es debido a la falta de medidas de gobernanza que comprometa a los participantes más allá de aquellos que están automatizados en el código. Además, en dichas medidas no se incluye la gestión de la inconsistencia, lo que dificulta la modificación de datos una vez se incluyen en un bloque/registro de la cadena/tabla. Estas circunstancias ponen en serias dificultades el ejercicio de los derechos de rectificación y supresión.

Para resolver estos problemas ha de definirse un marco de gobernanza, desarrollar unos procesos de gestión y adaptar los componentes de utilizados en la infraestructura para facilitar el ejercicio de los derechos de los interesados.

No hay que pasar por alto que las infraestructuras Blockchain ya disponen de mecanismos que pueden involucrar cambios en el protocolo, las reglas de consenso y otros aspectos (incluyendo modificaciones como ocurrió en el *DAO Fork* de Ethereum citado anteriormente) que se materializan en actualizaciones del software, que los participantes/nodos deberían de adoptar. Estos cambios, también llamados propuestas de mejora son, por ejemplo, el *Bitcoin Improvement Proposal* (BIP)⁵⁹ y *Ethereum Improvement Proposal* (EIP)⁶⁰. El proceso de gestión de estos cambios no se lleva a cabo mediante procedimientos formales, sino que son discutidas y valoradas en foros públicos, listas de correo, redes sociales, por la comunidad, los desarrolladores principales y otros actores importantes como los participantes/nodos (en algunos casos los cambios son apoyados y registrados en la Blockchain por un subconjunto de participantes, los que gestionan nodos mineros).

⁵⁸ (pueden existir algunos componentes o versiones empresariales que no).

⁵⁹ <https://github.com/bitcoin/bips>

⁶⁰ <https://eips.ethereum.org/>

Otro factor para tener en cuenta es que la deslocalización de los nodos puede implicar transferencias internacionales de datos personales, que han de cumplir con las disposiciones del RGPD al respecto.

Por último, y como ya se ha mencionado, los *Smart Contracts* son programas que se almacenan en la Blockchain y que ejecutan decisiones automatizadas (aquellas para las que han sido programados). En la medida en que estas decisiones pueden afectar de manera significativa a las personas físicas es esencial que se cumplan desde el diseño los requisitos establecidos en el artículo 22 del RGPD, y que se incorporen las garantías y medidas necesarias para proteger los derechos de los interesados.

IV. PRUEBA DE CONCEPTO DE LA AEPD

La Prueba de Concepto desarrollada muestra el caso de uso, completamente desarrollado, de la eliminación de la actividad de un usuario (persona física) en una infraestructura Blockchain. Para ello, se suprimirá la dirección de una cuenta, que es un identificador y, por tanto, un dato personal. El enfoque escogido implica sobrescribir la dirección de la cuenta, o bien la firma de la transacción desde la que puede derivarse la dirección.

En particular, para garantizar los derechos de rectificación y supresión, lo que supone la eliminación y actualización de datos de transacciones en los registros o bloques, se precisará de mecanismos de gobernanza y medidas técnicas para materializarlas en la Blockchain.

A. ANTECEDENTES

Ya existen diversas investigaciones y proyectos que han explorado estrategias para desarrollar infraestructuras Blockchain “redactables”, es decir, que permitan editar o eliminar datos en determinadas circunstancias, con el objetivo de cumplimiento normativo o de corrección de errores.

Estos proyectos han tenido ciertas limitaciones y se han basado en diseñar protocolos compatibles con la edición y modificación de transacciones mediante operaciones llevadas a cabo por participantes autorizados y buscan mantener la consistencia a nivel de transacción o a nivel de bloque. Los hashes camaleón y variantes criptográficas, modificación de la estructura de datos del bloque, transacciones mutables (varias versiones), almacenamiento *off-chain*, borrado local, técnicas ZKP, técnicas de poda o basadas en mecanismos de consenso, son algunas de estas estrategias⁶¹. No obstante, no se han implementado en las infraestructuras Blockchain más conocidas.

B. EXPLOTACIÓN DE ESTRATEGIAS YA EXISTENTES

La Prueba de Concepto (PoC) de la AEPD no plantea un cambio disruptivo para garantizar el cumplimiento del RGPD, sino que se basa en emplear estrategias ya existentes y conocidas de infraestructuras Blockchain y en los modelos de almacenamiento distribuido de datos.

1. Gobernanza

La gobernanza supone ejercer autoridad y control para decidir los objetivos de una organización, tomar decisiones, en función de los activos, recursos, contexto y una gestión

61

Solanki, A. R. (2024). Redactable Blockchain Solutions for IoT: A Review of Mechanisms and Applications <https://engrxiv.org/preprint/view/3792/6703>

Weiqi Dai et al, (2024) PRBFPT: A Practical Redactable Blockchain Framework With a Public Trapdoor <https://ieeexplore.ieee.org/document/10380599>.

Shams Mhmood A.A et al (2023). Redactable Blockchain: Comprehensive Review, Mechanisms, Challenges, Open Issues and Future Research Directions. <https://www.mdpi.com/1999-5903/15/1/35>.

Xiaoyu Wang et al (2024). A Redactable Blockchain Scheme Supporting Quantum-Resistance and Trapdoor Updates <https://www.mdpi.com/2076-3417/14/2/832>.

Xin-Yu Li et al (2021). Escaping from Consensus: Instantly Redactable Blockchain Protocols in Permissionless Setting <https://eprint.iacr.org/2021/223.pdf>.

Damiano Sartori. University of Twente (2020). Redactable Blockchain. How to change the immutable and the consequences of doing so. http://essay.utwente.nl/82755/1/Sartori_MA_EEMCS.pdf.

Yueyan Dong et al (2023). Redactable consortium blockchain with access control: Leveraging chameleon hash and multi-authority attribute-based encryption <https://www.sciencedirect.com/science/article/pii/S2667295223000661>

Dominic Deuber et al. University of Manchester (2019). Redactable Blockchain in the Permissionless Setting. [https://pure.manchester.ac.uk/ws/portalfiles/portal/211464559/Redactable Blockchain in the Permissionless Setting.pdf](https://pure.manchester.ac.uk/ws/portalfiles/portal/211464559/Redactable%20Blockchain%20in%20the%20Permissionless%20Setting.pdf)

del riesgo, para alcanzar dichos objetivos de forma priorizada y balanceada, y monitorizar de forma continua que el progreso de cada una de las acciones tomadas está bien orientado⁶². La gobernanza se tiene que implementar mediante la definición de roles, políticas, procedimientos, planes, medidas organizativas, jurídicas y técnicas que permitan gestionar la organización.

El éxito de un marco de gobernanza se mide por el éxito de la organización a largo plazo. Un factor que ayudará a dicho éxito será la definición clara y “*accountable*” de los elementos señalados en el párrafo anterior. Entre ellos, podemos señalar la identificación de los objetivos, definición de los roles de toma de decisiones y de gestión, procedimientos bien definidos de toma de decisión y ejecución de estos, así como su trazabilidad, documentación, etc. En función de los objetivos se puede hablar de gobernanza corporativa, estratégica, de los datos, de sostenibilidad, de la IA, etc. Pero, en una organización solo hay una gobernanza, que englobará varios aspectos, y que se traducirá en una única gestión, que estará orientada a conseguir cada uno de los objetivos.

La gobernanza es un elemento básico en toda implementación de una infraestructura Blockchain y además un factor diferenciador en cada una de ellas. De hecho, la principal clasificación de infraestructuras Blockchain se realiza en función de un aspecto de su gobernanza: públicas/privadas y permissionadas/no permissionadas.

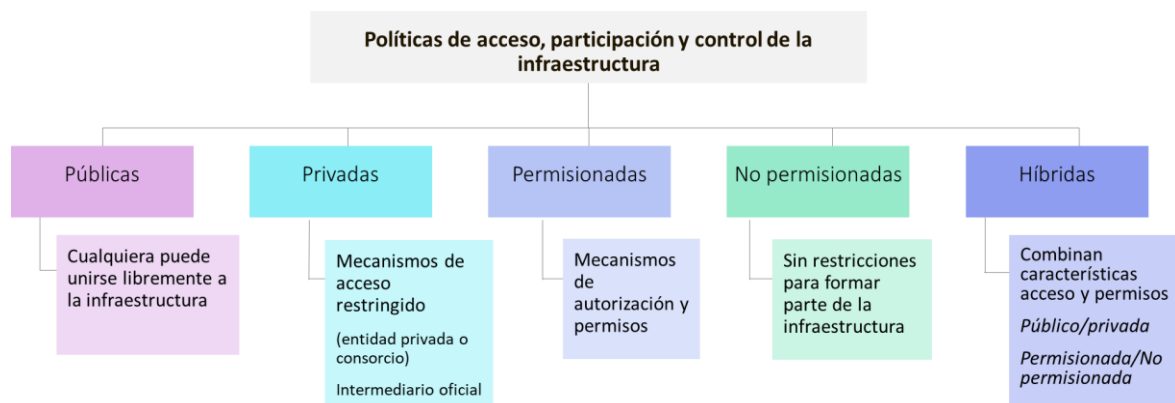


Figura 8. Clasificación de las redes Blockchain en función de las políticas de acceso, participación y control de la infraestructura. Lo habitual es encontrar redes público-no permissionadas (Bitcoin, Ethereum, y la mayoría de las criptomonedas conocidas) y privadas-permissionadas (por entidades privadas y consorcios).

Incluso las infraestructuras Blockchain públicas-no permissionadas incluyen elementos de gobernanza sin los cuales no podrían operar. En primer lugar, una asignación de roles, más o menos distribuidos, sobre quién puede tomar decisiones para alterar la Blockchain. A continuación, unos procedimientos, más o menos asamblearios, de toma de decisiones. Una definición de objetivos marco de la infraestructura⁶³ y otros procedimientos de gestión de más bajo nivel (mecanismos de consenso, versiones de código permitidas, registro de actualizaciones, etc.).

⁶² ITIL4 “the framework of authority, accountability, and decision-making required to achieve an organisation’s objectives and manage risks appropriately, COBIT 2019 “ensures that stakeholder needs, conditions and options are evaluated to determine balanced, agreed-on enterprise objectives to be achieved; that direction is set through prioritization and decision making; and that performance and compliance are monitored against agreed-on direction and objectives”

⁶³ En caso del Bitcoin, el correo electrónico de Nakamoto de 2008 fijaba el objetivo principal de tener una moneda e intercambios económicos fuera del control de una autoridad central. En su publicación original <https://bitcoin.org/bitcoin.pdf>, dedica el capítulo 10 a privacidad, considerando que todos los problemas de privacidad se resolvían utilizando claves públicas, y deduciendo de ello que las transacciones resultaban anónimas. Esto ha resultado en un error. La realidad es que el cifrado no es anonimizar, entre otros porque las claves públicas son identificadores únicos. Los hechos han demostrado que las autoridades reidentifican usuarios, incluso que hay empresas que prestan dichos servicios.

Todos estos elementos estarán más o menos documentados, serán más o menos explícitos⁶⁴, estarán sustentados por medidas jurídicas, organizativas o técnicas, más o menos automatizadas, y se habrán establecido por un proceso de gestión del riesgo o se habrán ido creando en función de los eventos sucedidos⁶⁵.

El hecho de que en una infraestructura Blockchain no se haya contemplado la gestión del cumplimiento normativo, como uno de los objetivos, no es un problema de la tecnología en sí. Pero si no se contempla dicho objetivo, no se implementan los mecanismos de gestión oportunos desde el diseño. Y esto es independiente de que nos encontremos con cualquier tipo de Blockchain, ya sea privada, pública, permitida o no. A ese respecto, el considerando 78 del RGPD explica que *“A fin de poder demostrar la conformidad con el presente Reglamento, el responsable del tratamiento debe adoptar políticas internas y aplicar medidas que cumplan en particular los principios de protección de datos desde el diseño y por defecto.”*. Por lo tanto, al menos desde el punto de vista del RGPD, la gobernanza de una infraestructura Blockchain debe incluir objetivos de cumplimiento de protección de datos y, por lo tanto, definir políticas que desarrollen los procesos de gestión que las implementan.

2. Hard Fork/ Soft Fork y actualizaciones de software

En el contexto de una infraestructura Blockchain una bifurcación o *Fork*, es decir, una división de la cadena/tabla de bloques, es el mecanismo principal por el cual se implementan actualizaciones de software. Puede ocurrir por varias razones, tales como modificaciones en el protocolo, modificaciones en el código para corregir errores o agregar funcionalidades, toma de decisiones ante eventos específicos no previstos, u otros cambios.

En algunos casos las nuevas actualizaciones de software no afectan directamente al funcionamiento y las versiones anteriores son compatibles, es decir aquellos participantes/nodos que no actualicen su software podrán seguir operando, es el caso conocido como *Soft Fork*. Para que un *Soft Fork* sea exitoso es necesario que se actualice en la mayoría de los nodos mineros/validadores.

Por el contrario, se habla de *Hard Fork* cuando la actualización de software no es compatible con las versiones previas y, por tanto, todos los nodos han de actualizar su software para seguir operando. En el caso de que no todos los nodos actualicen su software se originarán cadenas/tablas separadas e incompatibles, surgiendo así nuevas infraestructuras, como ya ha ocurrido en diversas ocasiones, motivadas principalmente por desacuerdos e intereses encontrados.

Se han mencionado anteriormente los mecanismos para introducir cambios mediante los *Bitcoin Improvement Proposal* (BIP) y *Ethereum Improvement Proposal* (EIP), que se incluyen en las actualizaciones de software correspondiente, en ocasiones implementando más de un BIP o EIP en cada actualización.

Actualmente el cliente oficial de Ethereum tiene incorporados más de 100 EIP, alrededor de 60 relativos al consenso, y ha tenido a lo largo de su historia (diez años) unas veinte versiones de tipo *Hard Fork*⁶⁶, es decir, entre una y tres veces por año. Por otro lado, el

⁶⁴ Por ejemplo, toda infraestructura Blockchain, como en todo sector de negocio, requiere de aquellos que quieran participar en el mismo (financieros, telecomunicaciones, farmacéuticos, transporte, etc.) cumplir con normativas, estándares y acuerdos de facto para operar.

⁶⁵ La gestión del riesgo supone identificar qué podría salir mal en el futuro y poner los medios para gestionar los reveses. En el caso del DAO Fork de Ethereum (<https://ethereum.org/en/history/#dao-fork>), no se previó que un Smart Contract pudiera ser manipulado, y cuando así fue, se tuvo que improvisar un procedimiento para gestionar dicho evento con las consecuencias negativas que supuso.

⁶⁶ <https://ethereum.org/en/history/>

cliente oficial de Bitcoin tiene incorporados más de 60 BIP, 17 de ellos relativos al consenso en sus catorce años de historia.

En Ethereum los *Hard Fork* son parte del proceso de su desarrollo y actualización. Generalmente no resultan en cadenas/tablas separadas, ya que la comunidad suele adoptar las actualizaciones. En Bitcoin todas las actualizaciones importantes hasta ahora se han desplegado como *Soft Forks*, varios de ellos con cambios importantes en el consenso. En cualquier caso, un nodo minero o validador que use versiones antiguas a un *Soft Fork* podría tener una funcionalidad limitada y el riesgo de rechazo de los bloques que genera por aquellos que sí han actualizado, riesgo que será mayor si el *Soft Fork* es relativo al consenso.

La PoC que se presenta en este documento hace uso del mecanismo de *Hard Fork* para implementar los cambios en las bases de datos de los nodos necesarios para la ejecución del derecho de supresión, de modo que la nueva versión de la infraestructura Blockchain no contiene los datos personales objeto de la supresión.

3. Procedimientos de validación de nuevas versiones

El *Bitcoin Improvement Proposal* BIP-0009⁶⁷ es uno de los mecanismos implementados en dicha infraestructura para validar una nueva versión del software (*Soft Fork*).

La PoC aquí presentada incorpora de manera simplificada el mecanismo del BIP-0009. Cuando un nodo validador actualiza a la nueva versión, los bloques que va generando incorporan un indicador en uno de sus campos. En el momento en que, en un intervalo de los últimos bloques añadidos a la cadena que está predefinido, un número determinado de ellos (también una mayoría preestablecida) contienen ese indicador, entonces se concluye que la mayoría de los nodos validadores ha actualizado a la nueva versión (está de acuerdo con los cambios) y se da por aceptado el cambio.

Una vez alcanzada esta mayoría, la nueva versión de software hace que cada nodo validador proceda a modificar su base de datos local, haciendo efectivo el derecho de supresión completándose así el *Hard Fork*. A partir de entonces, el campo del bloque que se ha usado para indicar la nueva versión se actualiza, y en los nuevos bloques generados dicho campo contiene también la información sobre el hecho de que la actualización ha sido aceptada y efectuada. Un nodo que se sincronice con la red posteriormente verificará la información en ese campo y modificará también su base de datos local.

⁶⁷ <https://github.com/bitcoin/bips/blob/master/bip-0009.mediawiki>



Figura 9. Esquema del mecanismo simplificado del BIP-0009 usado en la PoC. Se muestra la cadena de bloques que almacena un nodo cualquiera (en todos ocurre lo mismo). En cada bloque un campo indica el estado de la versión usada. Cuando se llega al número predefinido de últimos bloques generados con la nueva versión, se da por acordado el cambio, el nodo modifica su base de datos y los nuevos bloques que genera reflejan el nuevo estado acordado de esta nueva versión. Se ha dado lugar al Hard Fork.

4. Trazabilidad

La trazabilidad del dato en cualquier entorno de compartición de información es la capacidad de conocer todo el ciclo de vida del dato. La trazabilidad es el proceso de gestión que responde a las preguntas sobre quién, cuándo, cómo, dónde y por qué se tratan los datos. La trazabilidad es fundamental para ejecutar un derecho de supresión en organizaciones complejas y tratamientos con múltiples intervinientes (distintos responsables, múltiples encargos y subencargados, etc.). En esos casos es imprescindible conocer los distintos repositorios en los que se encuentra el dato, en qué copias temporales, y en las distintas sedes, encargados o subencargados (artículo 28(3)g del RGPD). La gestión de la trazabilidad, entre otros procesos, sustenta las medidas jurídicas⁶⁸ y organizativas que obligan a cada uno de los intervinientes (y sus departamentos o sucursales) a ejecutar el derecho de supresión de forma efectiva.

La trazabilidad del dato individual, o del conjunto de datos, es una de las funcionalidades imprescindibles en una infraestructura Blockchain. Incluso en las infraestructuras públicas-no permissionadas, el conocer quién está tratando los datos es necesario para la implementación de determinados mecanismos de consenso, para determinar si hay un control de la infraestructura por un grupo mayoritario, o para proporcionar medidas para garantizar la accesibilidad a los datos (aunque sea con procedimientos *Best Effort*⁶⁹), entre otros. En otros tipos de infraestructuras Blockchain cumplirán otras funciones como la gestión de permisos, la facturación de servicios o el control de miembros.

Por lo tanto, los mecanismos de trazabilidad son otra herramienta de gestión necesaria para implementar el marco de gobernanza en una infraestructura Blockchain.

⁶⁸ Independientemente de si se usa Blockchain y otras tecnologías de compartición de datos, las medidas jurídicas son las que imponen a los responsables del tratamiento la obligación de cumplir con los principios fundamentales de protección de datos establecidos en el RGPD. Entre estas medidas, los contratos entre el responsable y los encargados del tratamiento deben garantizar la eliminación de los datos cuando así lo requiera el responsable.

⁶⁹ https://es.wikipedia.org/wiki/Entrega_de_mejor_esfuerzo

En el entorno en línea también es obligado poder determinar los responsables que están tratando datos hechos públicos (considerando 66⁷⁰ del RGPD). Esta obligación viene a dar respuesta a casos que se presentan en redes de naturaleza P2P, como las infraestructuras Blockchain. Un caso característico se produjo en España cuando un centro médico difundió por una popular red P2P⁷¹ de compartición de contenidos un fichero con información muy sensible de pacientes⁷². Esto supuso que la información se distribuyó entre personas⁷³ que se habían sumado a la red pública no permitida y decidieron descargarse el fichero. El responsable de los datos (el centro médico) no había implementado un mecanismo para controlar la distribución de dichos datos a distintos responsables (que no tenían legitimación para tratar dichos contenidos, sentencia TJUE 62006CJ0275⁷⁴), y por supuesto no existía una relación responsable-encargado entre los participantes en la red P2P. Cada participante en la red P2P había elegido libremente participar en la compartición de contenidos (fines y medios) y actuaba en su propio nombre, no bajo las instrucciones del centro médico⁷⁵.

5. La aplicación de los derechos en el RGPD

El RGPD en el art. 12.3 del RGPD establece el plazo máximo de atención de los ejercicios de derechos en un mes, prorrogable a un total de tres meses en caso necesario, atendiendo a la complejidad que puede tener un proceso de atención de dichos derechos:

3. El responsable del tratamiento facilitará al interesado información relativa a sus actuaciones sobre la base de una solicitud con arreglo a los artículos 15 a 22, y, en cualquier caso, en el plazo de un mes a partir de la recepción de la solicitud. Dicho plazo podrá prorrogarse otros dos meses en caso necesario, teniendo en cuenta la complejidad y el número de solicitudes.

Este es un factor que hay que tener en cuenta cuando se plantean estrategias para el ejercicio de derechos en tratamientos de o basados en infraestructuras Blockchain, tanto en los plazos máximos establecidos, como en la consideración de determinadas aproximaciones a la aplicación efectiva de dichos derechos. En el caso que nos ocupa, marcaría el plazo máximo para la ejecución de un *Hard Fork*.

⁷⁰ Considerando 66 del RGPD: “en el entorno en línea, el derecho de supresión debe ampliarse de tal forma que el responsable del tratamiento que haya hecho públicos datos personales esté obligado a indicar a los responsables del tratamiento que estén tratando tales datos personales que supriman todo enlace a ellos, o las copias o réplicas de tales datos. Al proceder así, dicho responsable debe tomar medidas razonables, teniendo en cuenta la tecnología y los medios a su disposición, incluidas las medidas técnicas, para informar de la solicitud del interesado a los responsables que estén tratando los datos personales.”

⁷¹ eMule, que se diferencia de una infraestructura Blockchain en los mecanismos de consenso. Todo el contenido estaba identificado por un hash, lo que le confería un control de integridad a nivel de contenido individual, pero no del conjunto de contenidos ni su orden temporal.

⁷² Procedimiento PS/00059/2008

⁷³ Personas físicas o jurídicas que habían decidido poner sistemas de su propiedad, conexiones y programas para compartir contenidos, de los cuales algunos estaban sujetos a restricciones de uso y por los cuales podrían ser considerados como sujetos obligados por distintas normativas, por ejemplo, de propiedad industrial o intelectual.

⁷⁴ <https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:62006CJ0275> rechazo de la obligación de proporcionar datos personales relativos al uso de internet con objeto de proteger los derechos de autor. En la sentencia se considera que Promusicae intentaba ejercer un derecho legítimo contra personas que habían infringido la normativa de derechos de autor en el marco de un procedimiento civil. Las direcciones IP de las máquinas permitían identificar a las personas responsables de dichas máquinas y tratamientos. Estas personas estaban actuando en nombre propio al infringir la normativa de derechos de autor y no en nombre de terceros. Párrafo 43 “De entrada, procede señalar que las disposiciones de Derecho comunitario mencionadas en la cuestión planteada tienen por finalidad que los Estados miembros garanticen, concretamente en la sociedad de la información, la protección efectiva de la propiedad intelectual y, en particular, de los derechos de autor que Promusicae reivindica en el asunto principal.”

⁷⁵ La AEPD puso en marcha un equipo para localizar los hashes de los ficheros en la red y ordenar a los responsables bajo su competencia la retirada de este de sus sistemas, y solicitar a aquellos que estaban fuera de sus competencias como, por ejemplo, por estar en otro país, su retirada.

C. DISEÑO DE LA PRUEBA DE CONCEPTO

La aproximación a la implementación de la PoC está basada en el empleo del mecanismo de *Hard Fork* para implementar una gestión de las inconsistencias, permitiendo que el sistema continúe operando con garantías.

Para el desarrollo de la PoC se ha usado la implementación oficial de Ethereum⁷⁶, en su versión 1.13.15 de abril de 2024, que incorpora un protocolo de consenso basado en Prueba de Autoridad (denominado '*clique*'⁷⁷, soportado hasta la versión indicada). En esta configuración los nodos validadores son previamente conocidos y autorizados, desde el principio (aunque implementa un mecanismo de aprobación para añadir nodos validadores una vez que la Blockchain está en marcha).

Para ello, en primer lugar, se ha tenido que realizar un análisis de la documentación existente y el código fuente, así como de los procedimientos de gestión implícitos y explícitos que implementan la gobernanza definida en Ethereum.

A partir de ello, se ha trasladado un objetivo al marco de gobernanza de Ethereum: el cumplimiento del RGPD, en particular el del ejercicio del derecho de supresión. Con ese propósito se han desarrollado las herramientas de gestión, organizativas y técnicas necesarias para su implementación. Estas herramientas son:

1. Procedimiento de detección de los registros afectados en los distintos nodos. Se incluyen no solo las transacciones almacenadas en bloques de la cadena, sino también el almacenamiento de *Smart Contracts* y los recibos de las transacciones que los involucran, *receipts/logs*, como se ha explicado en el capítulo III epígrafe B.9.
2. Procedimiento de generación de una nueva versión de software de la infraestructura Blockchain, implementando un *Hard Fork*, tal como se ha explicado en el epígrafe B.2 de este capítulo. La estrategia técnica empleada consiste en implementar en el código fuente un mecanismo de consenso de los nodos validadores en la nueva versión de la infraestructura Blockchain, basado en el BIP-0009, junto con la modificación de la base de datos local del nodo cuando se llega al acuerdo sobre la nueva versión, en donde se ha cumplido el derecho del usuario. Además, se contempla la sincronización posterior de nuevos nodos con la nueva versión.
3. Procedimiento de distribución de la nueva versión de software y ejecución de este en los nodos.
4. Estrategia técnica para implementar un mecanismo de consenso en la nueva versión de la infraestructura Blockchain.
5. Medidas organizativas que se han de incorporar en la gestión de la infraestructura Blockchain para implementar el objetivo de gobernanza de cumplimiento normativo con el RGPD.

1. Procedimiento de detección de registros afectados

La PoC implementa un mecanismo de detección de los registros afectados en la base de datos que componen la Blockchain en los diferentes nodos. Las bases de datos utilizadas por los nodos almacenan información en pares clave-valor, a diferencia de las bases de datos relacionales tradicionales. El proceso se centra en identificar qué información se tiene que eliminar y en reemplazarla.

Este procedimiento consta de los siguientes pasos:

⁷⁶ <https://geth.ethereum.org/>

⁷⁷ Clique es la implementación estándar del consenso PoA en Ethereum, según el EIP-2-5. <https://eips.ethereum.org/EIPS/eip-225>

- Busca en los bloques las transacciones en las que interviene la cuenta del usuario que quiere ejercer su derecho de supresión.
- Comprueba si alguna de estas transacciones está dirigida hacia los *Smart Contracts*, es decir involucra llamadas a algunas de sus funciones o bien si se trata de la transacción de creación del *Smart Contract*.
- Obtiene los árboles de *Merkle*⁷⁸ del estado y balance de las cuentas.
- Sobrescribe la dirección de la cuenta que se desea borrar en las transacciones afectadas.
- Sobrescribe la dirección de la cuenta que se desea borrar en el almacenamiento de los *Smart Contract* afectados.
- Sobrescribe la dirección de la cuenta que se desea borrar en los recibos de las transacciones (*receipts/logs*) de los *Smart Contract*.
- Sobrescribe la dirección de la cuenta que se desea borrar en los árboles de *Merkle* del estado y balance de las cuentas.
- Finalmente, guarda la base de datos modificada en una estructura de datos de tipo JSON, que contiene los pares clave-valor modificados, en los que ya no aparece la dirección de la cuenta a borrar. Esta estructura de datos será incorporada en el procedimiento de generación de la actualización de software del *Hard Fork*.

Por simplicidad, esta PoC lleva a cabo este procedimiento mediante la ejecución en un nodo auxiliar que contiene una copia de la base de datos original. La ejecución del nodo auxiliar facilita la obtención de bloques, transacciones y sus datos mediante consultas a la API que expone un nodo. Adicionalmente, mediante la ejecución de un programa desarrollado en *NodeJS*, se usan librerías de lectura y escritura en las bases de datos del nodo (de tipo *LevelDB*) para acceder al resto de datos necesarios y modificarlos. Este enfoque permite realizar las modificaciones necesarias sin afectar directamente la red principal hasta que se ejecute la actualización del *Hard Fork*.

2. Procedimiento de generación de una nueva versión de software de la Blockchain

Una vez detectados los registros afectados, ha de procederse a la modificación del código fuente oficial de Ethereum (*geth*⁷⁹) para generar la actualización de la versión de software. Para ello se siguen los siguientes pasos:

- Añadir la lógica y funciones para implementar el acuerdo inspirado en BIP-0009 y las modificaciones de las bases de datos de los nodos.
- Añadir los pares clave-valor a modificar en la base de datos, obtenidos en el procedimiento anterior.
- Compilar la nueva versión de software y distribuirla.

La primera etapa en este procedimiento incluye añadir nuevas funcionalidades al código fuente oficial de Ethereum, así como las actualizaciones pertinentes para gestionar la modificación de la base de datos local del nodo y gestionar la posterior sincronización de un nodo. Estos cambios pueden permanecer en sucesivas actualizaciones del software, en donde tan sólo habría que tener en cuenta modificar el número de versión.

La segunda etapa conlleva incluir, como parte del código fuente, los pares clave-valor modificados que reemplazarán a los correspondientes pares clave-valor originales en la base

⁷⁸ ISO 22739: Estructura de datos en árbol en la que cada nodo hoja está etiquetado con el valor hash de un elemento de datos y cada nodo no hoja está etiquetado con el valor hash de las etiquetas de sus nodos hijos.

⁷⁹ <https://geth.ethereum.org/>

de datos local del nodo. Esta operación se realizará cuando se verifique el acuerdo inspirado en el BIP-0009, o bien, cuando se produzca una sincronización de un nodo a la cadena en la que el acuerdo ya se ha alcanzado previamente.

3. Procedimiento de distribución de la nueva versión de software y ejecución de este en los nodos

Una vez completado el procedimiento anterior, se dispondrá de la nueva versión de software. Esta nueva versión se pone a disposición de todos los nodos para que la ejecuten. Los nodos han de estar pendientes de las actualizaciones de software para ejecutarlas, ya que supondrán un *Hard Fork*. La trazabilidad, como se ha indicado en el epígrafe B.4 de este capítulo, sustenta las medidas jurídicas y organizativas que obligan a cada uno de los nodos a ejecutar el derecho de supresión de forma efectiva.

En el contexto de la PoC la nueva versión se distribuye manualmente a cada nodo. Dado que los nodos son gemelos y usan el mismo sistema operativo, el proceso de actualización se simplifica, ya que la versión modificada puede copiarse directamente en cada uno de ellos.

4. Estrategia técnica para implementar un mecanismo de consenso en la nueva versión de la Blockchain

Un segundo pilar fundamental en que se basa la PoC, una vez detectados los registros que se deben modificar, es un mecanismo de acuerdo entre los nodos validadores para adoptar esa actualización del software mediante un consenso y mayoría, registrándolo en la propia Blockchain de la versión actualizada del software que dichos nodos pasan a ejecutar.

Como se ha descrito anteriormente (epígrafe B.3 de este capítulo), la PoC incorpora de manera simplificada el mecanismo del BIP-0009, modificando y adaptando el código oficial de Ethereum para implementarlo. En particular se aprovecha un campo del bloque no usado por el mecanismo de consenso *clique* en Ethereum.

5. Medidas organizativas para la gestión de la gobernanza

Los procedimientos descritos en la presente PoC se tienen que articular como procesos de gestión que implementen los objetivos definidos en el marco de gobernanza. Para ello, se tendría que realizar:

- a) Una definición de roles que intervienen en los procesos de gestión de la ejecución del derecho de supresión.
- b) Una definición de las entidades de la infraestructura Blockchain que ejecutan cada uno de los roles.
- c) La documentación, tanto de las políticas para la ejecución de los procedimientos de borrado, como de la ejecución en sí de los mismos.

Hay muchas soluciones que se pueden dar para la implementación concreta de las medidas de gestión. Una solución podría ser la de delegar en una entidad todos los roles en el proceso de ejecución del derecho de supresión. En el otro extremo, todos esos roles se podrían ejecutar de forma distribuida.

En esta PoC se ha seguido una opción mixta, pues el objetivo principal ha sido demostrar la viabilidad técnica. A continuación, se describe la solución adoptada además de describir otras posibles opciones.

a) Definición de los roles en los procesos de gestión de la ejecución del derecho de supresión

Cada uno de los siguientes procedimientos deberán ser ejecutados por una o más entidades a las que se les ha asignado la obligación de llevarlos a cabo:

1. Documentación de las políticas para la ejecución de los procedimientos de borrado. Las entidades encargadas han de desarrollar y mantener las políticas que describan cómo se van a gestionar las solicitudes de borrado, definiendo los plazos y obligaciones de cada involucrado en el proceso
2. Recogida de solicitudes de ejercicio de derechos. Ha de garantizarse un canal seguro y accesible para que los usuarios puedan enviar sus solicitudes a la entidad/es encargada de la recogida de solicitudes.
3. Evaluación de las solicitudes para garantizar su validez, autenticidad y conformidad. Esta evaluación incluiría las medidas para evitar fraude o usos malintencionados, o determinar si procede o no atender la solicitud, entre otros aspectos.
4. Decisión de arranque del proceso de ejecución de los ejercicios de derechos (que podrían tener en cuenta otros objetivos distintos del RGPD, por ejemplo, cambios para corregir errores). Antes de iniciar el proceso de borrado ha de realizarse una evaluación para considerar los efectos del borrado, ya sea por obligaciones legales o por protección de derechos de terceros.
5. Ejecución del procedimiento de detección de registros. Han de identificarse todos los registros que contengan los datos personales objeto de la solicitud, incluyendo los *Smart Contract* y los recibos de transacciones que los involucran (*receipts/logs*)
6. Ejecución del procedimiento de una generación de la nueva versión de software. La nueva versión ha de incorporar todos los registros a modificar, así como el mecanismo de acuerdo entre los nodos, inspirado en el BIP-0009 en esta PoC. Ha de llevarse un registro y control de versiones de los cambios efectuados.
7. Ejecución del procedimiento de distribución de software. Ha de coordinarse la distribución de la actualización de manera controlada e íntegra, de modo que pueda asegurarse que la nueva versión que un nodo va a usar es la correcta.
8. Validación de la nueva versión de software. Un nodo podría ejecutar el procedimiento de detección de modificaciones y comprobar los cambios en las bases de datos.
9. Ejecución de la nueva versión de software. Los nodos pararán su operación para reiniciarla con la nueva versión.
10. Ejecución de un proceso de purga de bases de datos o almacenamientos temporales, y cualquier otro almacenamiento que contenga los datos a borrar, por ejemplo, almacenamiento de claves del nodo (*keystore*), etc. Es fundamental que no permanezcan copias residuales o de *backup* de los datos en ningún participante en la red.
11. Mantenimiento de los registros de toma de decisiones con relación al ejercicio de supresión.
12. Monitorización de la gestión de la ejecución del derecho de supresión e información al interesado. Finalmente, las entidades han de implementar un sistema de monitorización continua que permita verificar que el derecho de supresión se ejecuta correctamente, incluyendo auditorías y revisión de los procedimientos y políticas.

b) Definición de las entidades de la infraestructura Blockchain que ejecutan cada uno de los roles

En el caso de esta PoC se ha considerado la existencia de una entidad⁸⁰ que asume todos los anteriores roles de gestión, exceptuando los numerados como 8, 9 y 10, que son llevados a cabo por los participantes/nodos de la infraestructura. Esta entidad no ha de ser necesariamente una entidad jerárquicamente superior a los participantes/nodos, sino tan solo una que tiene asignados dichos roles de gestión.

Por otro lado, cada nodo sería responsable de ejecutar los procedimientos de validación del software, gestión de sus copias temporales y cualquier otro almacenamiento que pudiera verse afectado, y ejecución de la nueva versión de software.

Esta aproximación podría darse fácilmente en redes privadas y/o permissionadas en las que ya existan estas entidades. En otro tipo de infraestructura Blockchain pudiera darse el caso que distintas entidades asumiesen los distintos roles. Por ejemplo, que los nodos que fueran responsables de tratamiento tuvieran la obligación de recoger las solicitudes de ejercicios de derechos sin delegarla en un nodo singular o una entidad central. Otra posibilidad es que fuera una entidad (singular) la que gestionase las solicitudes de derechos y que hubiera otra entidad, distinta de la anterior, que gestionase la monitorización del procedimiento⁸¹.

Sin embargo, y en particular en el caso de redes públicas no permissionadas se podrían tener otras aproximaciones. Por ejemplo, se podrían implementar mecanismos distribuidos de la toma de decisión. En este contexto, la gobernanza se distribuye entre los participantes de la red (o un subconjunto seleccionado de ellos), quienes mediante mecanismos como el consenso o votación deciden las reglas y operaciones sobre la Blockchain. En el caso de Bitcoin o Ethereum, es un grupo reducido quien toma las decisiones. En Ethereum, fue una decisión de los desarrolladores el dividir una actualización denominada *Pectra* en dos fases⁸².

c) Documentación de las políticas para la ejecución de los procedimientos de borrado, como de la ejecución en sí de los mismos

En el caso de esta Prueba de Concepto, una entidad determinada tiene asignada la obligación de documentar las políticas y procedimientos de gestión. El capítulo actual podría formar parte de dicha documentación.

También formaría parte de la documentación el establecer la obligación para todos los nodos de ejecutar los procedimientos de detección de registros afectados por el derecho de supresión, el de generación de una nueva versión de software, su distribución y ejecución.

Además, se establecería la obligación para todos los intervinientes en la infraestructura de:

- Establecer canales de comunicación para informar a todos los participantes sobre las actualizaciones. Estos canales han de ser accesibles a los nodos, operadores y otros actores clave, asegurando que se notifique de manera oportuna cualquier actualización. Han de ser canales auditables y verificables.
- Implementar un procedimiento de consulta de actualizaciones, para que los nodos las verifiquen y apliquen. Esto garantiza que las actualizaciones sean legítimas y evita así la implementación de actualizaciones maliciosas o incorrectas.

⁸⁰ En la PoC una misma persona asume esos roles.

⁸¹ También puede darse el caso que un nodo responsable contrate nodos para la operación en la Blockchain, mediante una relación responsable-encargado, que habrá de cumplir con el Art. 28 del RGPD.

⁸² <https://www.fxstreet.es/cryptocurrencies/news/ethereum-sube-mas-del-6-tras-la-decision-de-dividir-la-actualizacion-pectra-en-dos-fases-202409192135>

- Establecer un procedimiento de supervisión para asegurar que el borrado se realice correctamente en toda la red y de acuerdo con las políticas de gobernanza
- Establecer un procedimiento de resolución de conflictos. Debe abordar conflictos entre los participantes, como desacuerdos, problemas de cumplimiento de derechos o disputas sobre obligaciones contractuales entre responsables y encargados.

Las políticas deben incluir el establecimiento de las responsabilidades de los intervinientes, tanto en su actuación como responsables del tratamiento, como las cláusulas específicas en los contratos responsable-encargado para hacer un cumplimiento efectivo del artículo 28(3)g) del RGPD.

V. EJECUCIÓN Y RESULTADOS DE LA PRUEBA DE CONCEPTO

Para la ejecución de los casos de uso de la PoC se han creado varias cuentas de usuario y dos nodos validadores, se ha efectuado el despliegue de dos *Smart Contracts* (sencillos, creando sendos tokens y distintas funciones para cada uno de ellos), se han efectuado transacciones que los invocan, en particular, de creación de tokens, compra de tokens y traspaso de tokens. Adicionalmente, se han efectuado varias transacciones de traspaso de la criptomoneda propia de la Blockchain, *Ether* (que carece de valor económico en esta Blockchain privada), entre usuarios.

Una de las cuentas, perteneciente a un usuario será el objeto de la solicitud de supresión conforme al RGPD, habiéndose por tanto de eliminar cualquier traza de las interacciones de esta en la Blockchain. En la implementación de la PoC se ha tratado de cubrir un amplio abanico de transacciones de esta cuenta: como origen y destino de transacciones de traspaso de criptomoneda *Ether*, destino de una transferencia de tokens en un *Smart Contract*, creador del otro *Smart Contract* y emisor de una transacción de creación de tokens de este.

A. ESTRATEGIA TÉCNICA PARA LA EJECUCIÓN DE LA PoC

Las políticas de gobernanza definen claramente las obligaciones y procedimientos para el tratamiento de datos, que se materializan en una estrategia técnica para dar respuesta a las solicitudes de derechos cuyos pasos son:

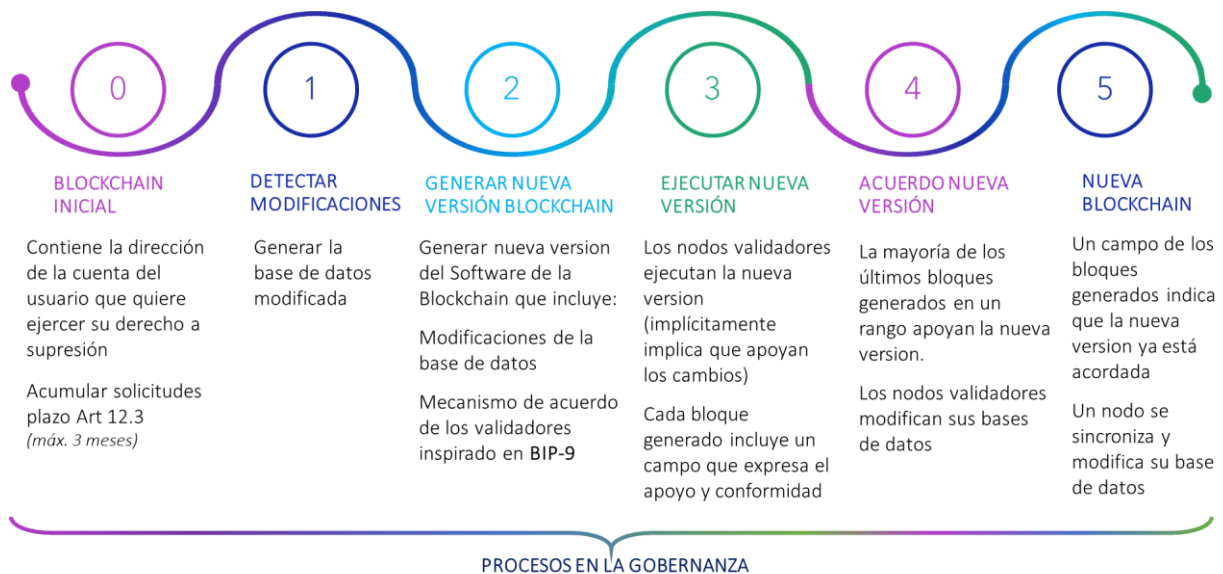


Figura 10. Fases de la PoC, en cada fase se enumeran los procedimientos que se ejecutan.

0. Acumular solicitudes de derechos de forma periódica (cada mes o cada tres meses si está debidamente justificado) para ejecutar en la infraestructura las solicitudes de derechos en ese periodo.

Como se ha indicado anteriormente, en la PoC se contempla la solicitud de supresión de una cuenta por sencillez, contemplar más cuentas simplemente requeriría repetir para cada una de ellas el siguiente paso, el 1.

1. Detectar las modificaciones necesarias que hay que efectuar en las bases de datos de los nodos donde se materializa la tabla de registros y la cadena de bloques, y generar la base de datos modificada (hasta el último bloque necesario).

- Se sobrescriben los datos pertinentes que forman parte de los bloques, almacenamiento de *Smart Contracts*, recibos de transacciones, estado de balances, etc. Para cada bloque se observan las distintas transacciones que se registran en él, y para cada transacción se comprueba si la cuenta en cuestión es origen, destino de esta, o bien está incluida en datos adicionales de la transacción. Cuando una de estas transacciones está dirigida a un *Smart Contract*, se comprueba también su almacenamiento y a los posibles logs o recibos de transacción que se hayan podido generar y almacenar.
- En la PoC se sobrescribe el valor de la cuenta en cuestión (0x17c3b445750221cfc48b1ea6a8d13b1eef1da197) por un valor constante (0xaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa). En el caso de que esta cuenta es la emisora de una transacción, lo que se sobrescribe con el valor constante es uno de los parámetros de la firma de la transacción, ya que los datos almacenados en Blockchain no incluyen explícitamente el campo con la cuenta del emisor (*from*), lo que incluyen es la firma de la transacción, que incorpora la clave pública, desde la que puede derivarse la dirección de la cuenta. En Ethereum se usan tres campos para este cometido 'r', 's', 'v', la Prueba de Concepto sobrescribe 'r'⁸³.
- Para efectuar estas operaciones la PoC, por simplicidad, ejecuta un nodo auxiliar que contiene una copia de la base de datos original. Así se facilita la obtención de bloques, transacciones y sus datos mediante consultas a la API que expone el nodo. Adicionalmente, mediante la ejecución de un programa desarrollado en *NodeJS*, se usan librerías de lectura y escritura en las bases de datos del nodo (de tipo *LevelDB*) para acceder al resto de datos necesarios y modificarlos. Este enfoque permite realizar las modificaciones necesarias sin afectar directamente a la red principal hasta que se ejecute la actualización del *Hard Fork*.
2. Generar la nueva versión del software de la Blockchain, en donde se incorporan los pares clave-valor de la base de datos modificada que reemplazarán a los correspondientes pares clave-valor originales en la base de datos local del nodo, y donde ya no aparecerá la dirección de la cuenta a eliminar. Además, la nueva versión de software incluye el mecanismo de acuerdo de nodos validadores, inspirado en el BIP-0009 de Bitcoin, como se ha descrito anteriormente.
 3. Los nodos validadores actualizan su versión de software. Los bloques que generan incluyen un indicador que refleja su acuerdo con el cambio.
 4. Cuando una mayoría de bloques en un intervalo predefinido incluye el indicador del cambio en el bloque, entonces se da por acordado el cambio. En ese momento, los nodos validadores con la nueva versión de software modifican sus bases de datos, reemplazando los pares clave-valor con los correspondientes que esta versión contiene. En este momento se produce el *Hard Fork* y los nodos validadores modifican desde ese momento en los bloques que generan el indicador, que ahora informa que esta versión ya está aceptada y los cambios en la base de datos implementados.
 5. A partir de este momento cualquier nodo que quiera sincronizarse con la red habrá de actualizar el software a la nueva versión, pues en caso contrario no podría sincronizarse al tratarse de un *Hard Fork*. El nodo, en el proceso de sincronización y descarga de bloques, comprobará que el último bloque existente en la cadena/tabla contiene el indicador que informa que la versión está aceptada y en consecuencia

⁸³ Los valores r y s son los componentes de la curva elíptica ECDSA que genera la clave pública, v es un identificador que facilita la extracción de la clave pública. Si se obtiene la cuenta emisora habiendo sobrescrito r, se obtendrá una cuenta (la que corresponda a los nuevos valores r,s,v, con muy baja probabilidad de que ya exista., en cualquier caso, la transacción no tiene efectos en ella.

actualizará su base de datos. En caso de que la sincronización se produzca antes de que se haya alcanzado el acuerdo, el nodo modificará su base de datos local cuando se alcance.

B. RESULTADOS DE LA PoC

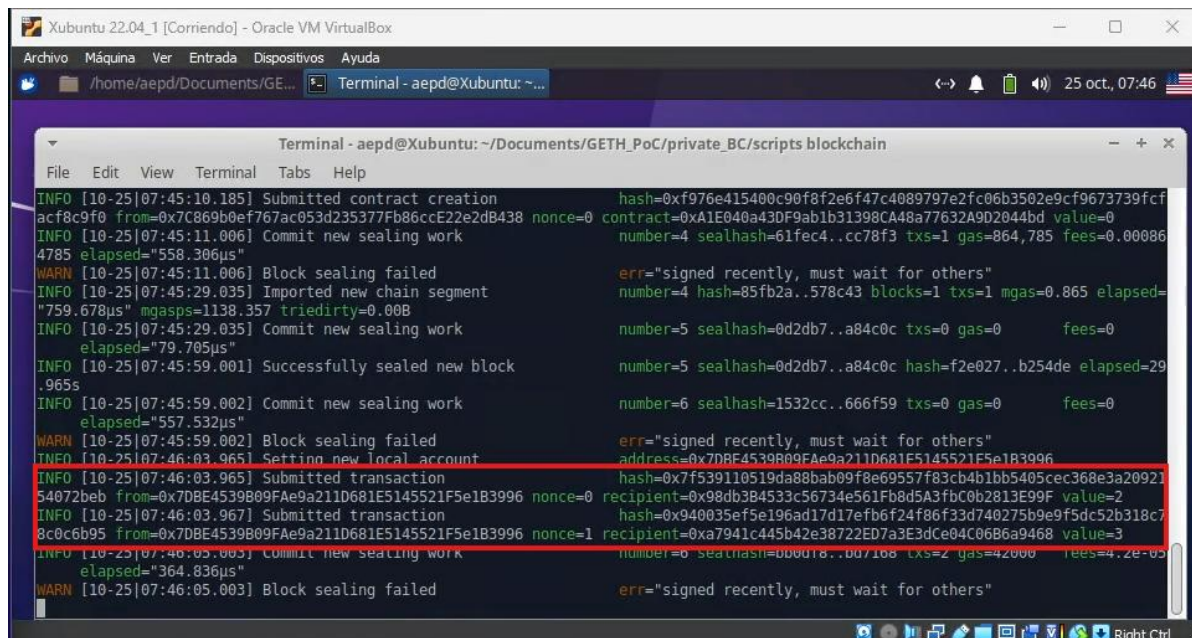
La PoC se ha desarrollado siguiendo la estrategia detallada en el epígrafe anterior, desplegando en un ordenador Windows dos máquinas virtuales que actuarán cada una de ellas como nodo validador, conectadas en una red local. Desde el ordenador Windows se efectúan las transacciones conectándose alternativamente a cada uno de los nodos, reproduciendo un funcionamiento habitual y normal de una infraestructura Blockchain, simulando así la actividad de los usuarios en aplicaciones descentralizadas (*dApps*) u otras aplicaciones (*Wallets*, *Exchanges*, plataformas de compraventa, etc.).

Las dos siguientes figuras muestran la ejecución de las transacciones desde el ordenador Windows y la operación de la infraestructura Blockchain recibiendo y validándolas:

```
"TX de transferencia de ETH entre cuentas"
"Tx transfer ETH Nodo 1"
WARN [10-25|07:46:04.326] Enabling deprecated personal namespace
"0x940035ef5e196ad17d17efb6f24f86f33d740275b9e9f5dc52b318c78c0c6b95"

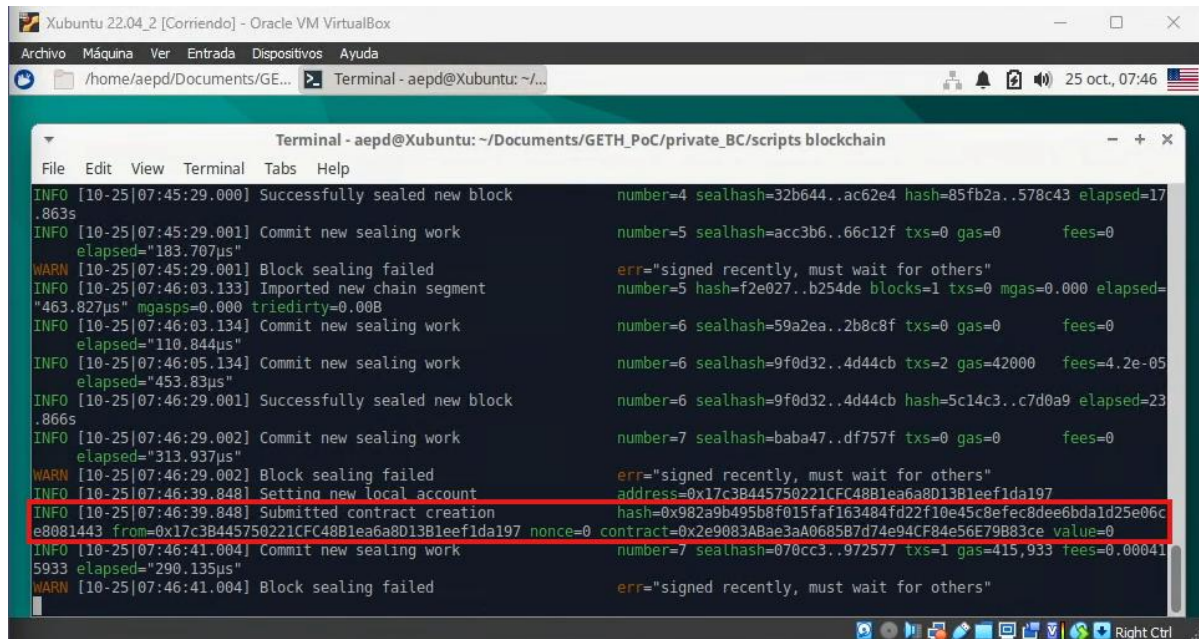
Waiting for 15 seconds, press a key to continue ...
```

Figura 11. Ejecución de las transacciones desde el ordenador Windows.



```
INFO [10-25|07:45:10.185] Submitted contract creation hash=0xf976e415400c90f8f2e6f47c4089797e2fc06b3502e9cf9673739fcf
acf8c9f0 from=0x7C869b0ef767ac053d235377Fb86ccE22e2d8438 nonce=0 contract=0xA1E840a430F9ab1b31398CA48a77632A9D2044bd value=0
INFO [10-25|07:45:11.006] Commit new sealing work number=4 sealhash=61fec4..cc78f3 txs=1 gas=864,785 fees=0.00086
4785 elapsed="558.306µs"
WARN [10-25|07:45:11.006] Block sealing failed err="signed recently, must wait for others"
INFO [10-25|07:45:29.035] Imported new chain segment number=4 hash=85fb2a..578c43 blocks=1 txs=1 mgas=0.865 elapsed=
"759.678µs" mgasps=1138.357 triedirty=0.008
INFO [10-25|07:45:29.035] Commit new sealing work number=5 sealhash=0d2db7..a84c0c txs=0 gas=0 fees=0
elapsed="79.705µs"
INFO [10-25|07:45:59.001] Successfully sealed new block number=5 sealhash=0d2db7..a84c0c hash=f2e027..b254de elapsed=29
.965s
INFO [10-25|07:45:59.002] Commit new sealing work number=6 sealhash=1532cc..666f59 txs=0 gas=0 fees=0
elapsed="557.532µs"
WARN [10-25|07:45:59.002] Block sealing failed err="signed recently, must wait for others"
INFO [10-25|07:46:03.965] Setting new local account address=0x7DBE4539809FAe9a211D681E5145521F5e1B3996
INFO [10-25|07:46:03.965] Submitted transaction hash=0x7f539110519da88bab09f8e69557f83cb4b1bb5405cec368e3a20921
54072beb from=0x7DBE4539809FAe9a211D681E5145521F5e1B3996 nonce=0 recipient=0x98db384533c56734e561Fb8d5A3fbC0b2813E99F value=2
INFO [10-25|07:46:03.967] Submitted transaction hash=0x940035ef5e196ad17d17efb6f24f86f33d740275b9e9f5dc52b318c7
8c0c6b95 from=0x7DBE4539809FAe9a211D681E5145521F5e1B3996 nonce=1 recipient=0xa7941c445b42e38722ED7a3E3dCe04C06B6a9468 value=3
INFO [10-25|07:46:05.003] Commit new sealing work number=6 sealhash=0d0016..007108 txs=2 gas=42000 fees=4.28-05
elapsed="364.836µs"
WARN [10-25|07:46:05.003] Block sealing failed err="signed recently, must wait for others"
```

Figura 12. Operación de la infraestructura Blockchain con los 2 nodos validadores y distintas transacciones en ellos, marcadas dos transferencias de Ether.



```

Terminal - aepd@Xubuntu: ~/Documents/GETH_PoC/private_BC/scripts blockchain
File Edit View Terminal Tabs Help
INFO [10-25|07:45:29.000] Successfully sealed new block      number=4 sealhash=32b644..ac62e4 hash=85fb2a..578c43 elapsed=17
.863s
INFO [10-25|07:45:29.001] Commit new sealing work          number=5 sealhash=acc3b6..66c12f txs=0 gas=0      fees=0
elapsed="183.707µs"
WARN [10-25|07:45:29.001] Block sealing failed            err="signed recently, must wait for others"
INFO [10-25|07:46:03.133] Imported new chain segment      number=5 hash=f2e027..b254de blocks=1 txs=0 mgas=0.000 elapsed=
"463.827µs" mgasps=0.000 triedirty=0.008
INFO [10-25|07:46:03.134] Commit new sealing work          number=6 sealhash=59a2ea..2b8c8f txs=0 gas=0      fees=0
elapsed="110.844µs"
INFO [10-25|07:46:05.134] Commit new sealing work          number=6 sealhash=9f0d32..4d44cb txs=2 gas=42000 fees=4.2e-05
elapsed="453.83µs"
INFO [10-25|07:46:29.001] Successfully sealed new block      number=6 sealhash=9f0d32..4d44cb hash=5c14c3..c7d0a9 elapsed=23
.866s
INFO [10-25|07:46:29.002] Commit new sealing work          number=7 sealhash=baba47..df757f txs=0 gas=0      fees=0
elapsed="313.937µs"
WARN [10-25|07:46:29.002] Block sealing failed            err="signed recently, must wait for others"
INFO [10-25|07:46:39.848] Setting new local account       address=0x17c38445750221CFC48B1ea6a8013B1eef1da197
INFO [10-25|07:46:39.848] Submitted contract creation     hash=0x982a9b495b8f015faf163484fd22f10e45c8efec8dee6bda1d25e06c
e8081443 from=0x17c38445750221CFC48B1ea6a8013B1eef1da197 nonce=0 contract=0x2e9083ABae3aA0685B7d74e94CF84e56E79B83ce value=0
5933 elapsed="290.135µs"
WARN [10-25|07:46:41.004] Block sealing failed            err="signed recently, must wait for others"

```

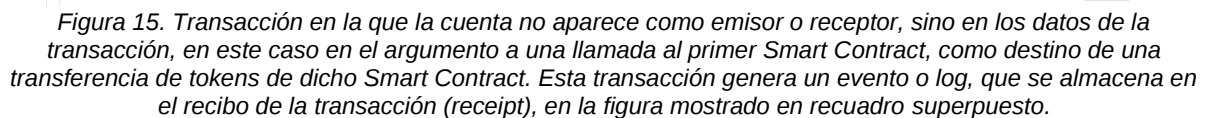
Figura 13. Operación de la infraestructura Blockchain con los 2 nodos validadores. Marcada la transacción de creación de uno de los dos Smart Contract.

Se han considerado todos los casos de uso relacionados con la cuenta que solicita el borrado. Estos casos se agrupan en cinco tipos de transacciones, las cuales cubren todas las posibles situaciones en las que esta cuenta aparece, ya sea como emisor, receptor o argumento de una llamada a una función de un *Smart Contract*.

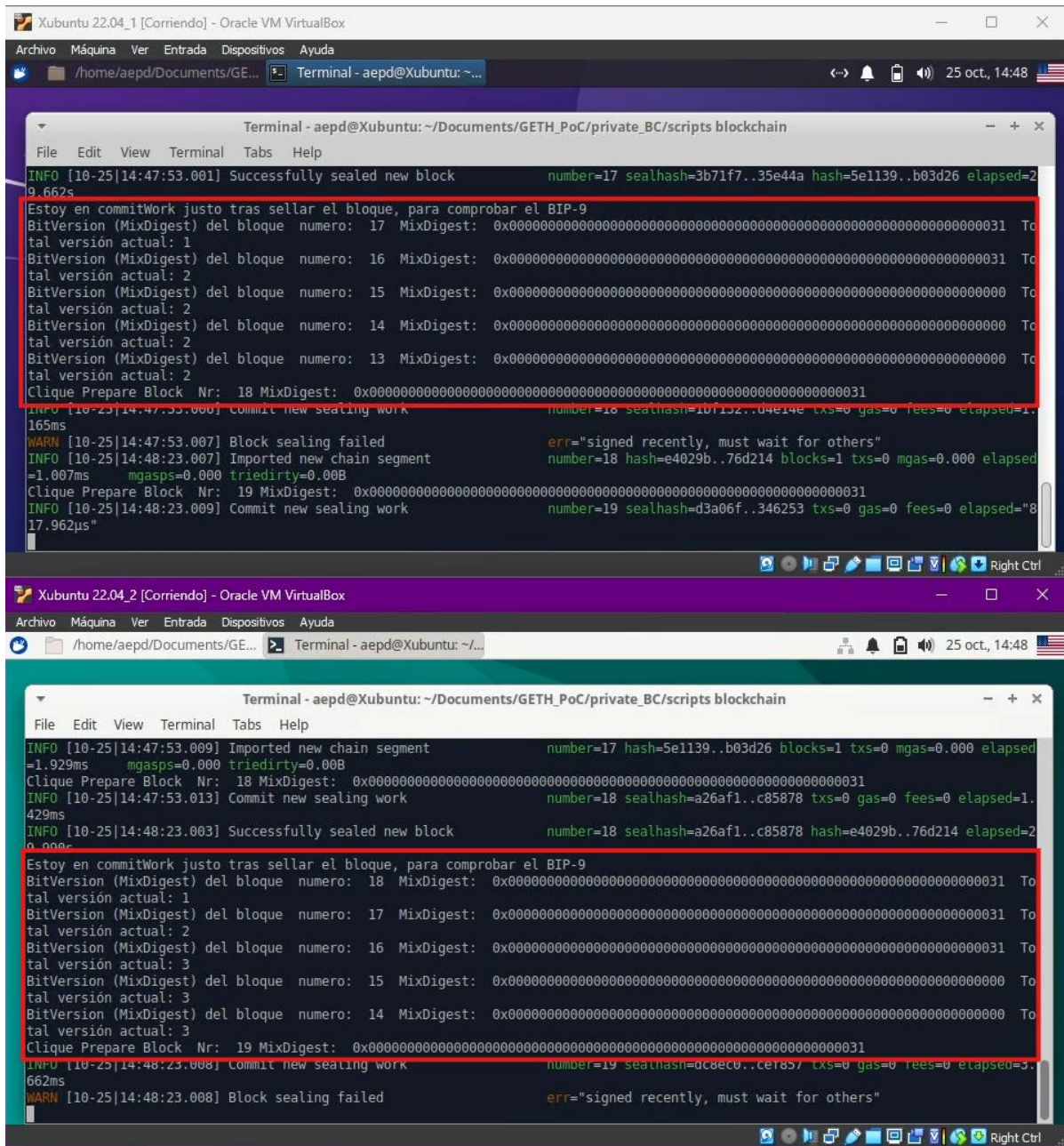
Txn Hash	Method	Block ↓	Mined On	From	To	Value	Fee
FROM en transferencia de ETH							
0x489...e157		12	10/25 10:08:02 AM 4 days ago	self 0x17c3b4...a197	0x7c869b...b438	0.000000000000000001 Ether	0.000021 Ether
FROM en transferencia de tokens en Smart Contract							
0x95c...4de6	0x40c10f19	11	10/25 10:07:32 AM 4 days ago	self 0x17c3b4...a197	0x2e9083...83ce	0 Ether	0.00004421 Ether
0x8da...f789		9	10/25 10:06:32 AM 4 days ago	0x7c869b...b438	self 0x17c3b4...a197	0.000000000000000001 Ether	0.000021 Ether
TO en transferencia de ETH							
0x982...1443	0x60806040	7	10/25 10:05:32 AM 4 days ago	self 0x17c3b4...a197		0 Ether	0.0004159 Ether
Creación Smart Contract							

Explorador de bloques local: <https://app.tryetherl.com/>

Figura 14. Transacciones en las que la cuenta a eliminar aparece como emisor (from) o receptor (to).

[illegible]

En la siguiente figura se observa el proceso de acuerdo de los dos nodos validadores que están ejecutando la versión actualizada del software. En cada bloque que generan comprueban el valor del campo indicador en un rango de bloques prefijado (5 bloques en este caso).



```

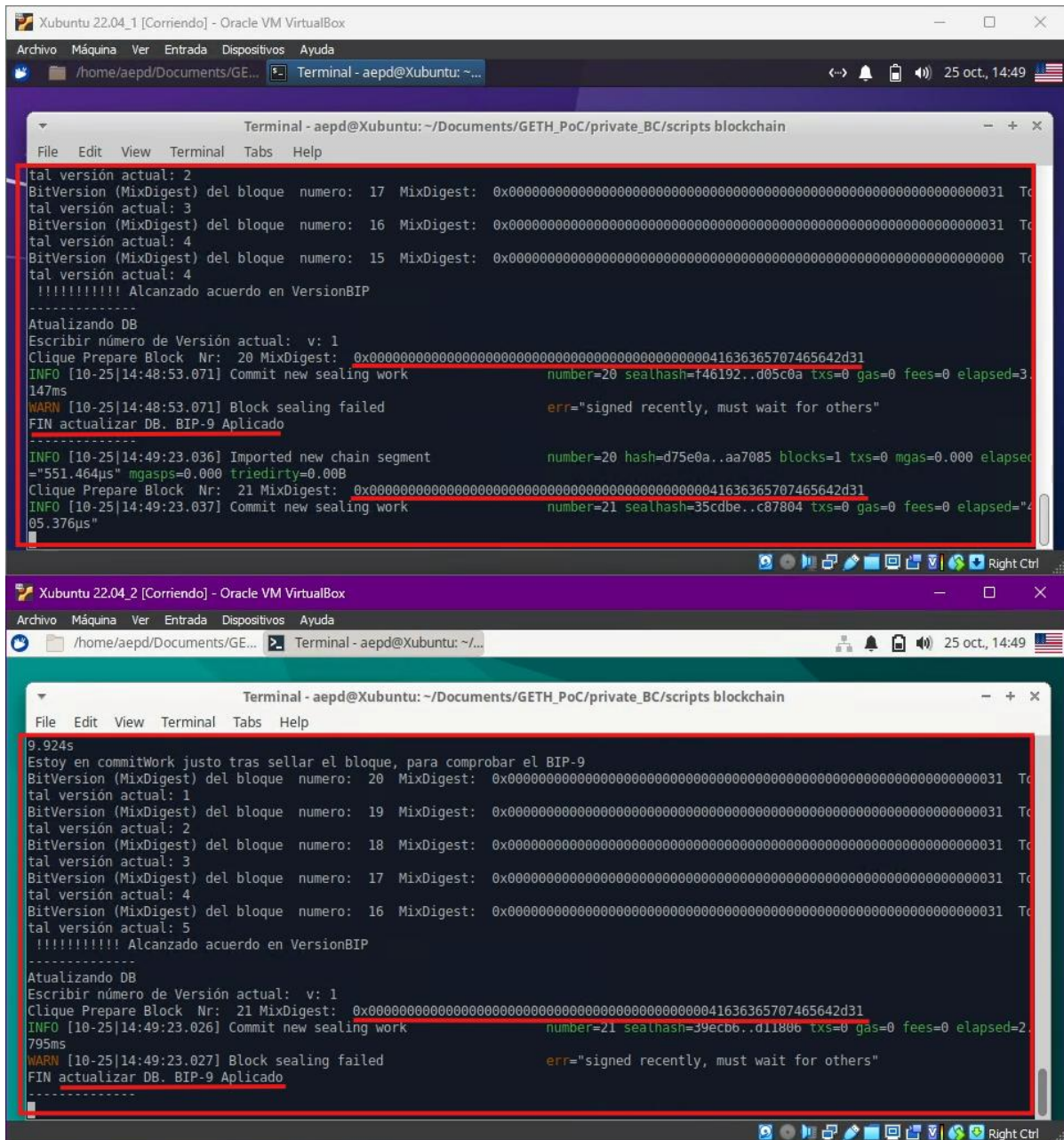
Terminal - aepd@Xubuntu: ~/Documents/GETH_PoC/private_BC/scripts blockchain
INFO [10-25]14:47:53.001 Successfully sealed new block      number=17 sealhash=3b71f7..35e44a hash=5e1139..b03d26 elapsed=2
9.662s
Estoy en commitWork justo tras sellar el bloque, para comprobar el BIP-9
BitVersion (MixDigest) del bloque numero: 17 MixDigest: 0x0000000000000000000000000000000000000000000000000000000000000031 To
tal versión actual: 1
BitVersion (MixDigest) del bloque numero: 16 MixDigest: 0x0000000000000000000000000000000000000000000000000000000000000031 To
tal versión actual: 2
BitVersion (MixDigest) del bloque numero: 15 MixDigest: 0x0000000000000000000000000000000000000000000000000000000000000000 To
tal versión actual: 2
BitVersion (MixDigest) del bloque numero: 14 MixDigest: 0x0000000000000000000000000000000000000000000000000000000000000000 To
tal versión actual: 2
BitVersion (MixDigest) del bloque numero: 13 MixDigest: 0x0000000000000000000000000000000000000000000000000000000000000000 To
tal versión actual: 2
Clique Prepare Block Nr: 18 MixDigest: 0x0000000000000000000000000000000000000000000000000000000000000031
INFO [10-25]14:47:53.000 Commit new sealing work      number=18 sealhash=10f132..d4e14e txs=0 gas=0 fees=0 elapsed=1.
165ms
WARN [10-25]14:47:53.007 Block sealing failed      err="signed recently, must wait for others"
INFO [10-25]14:48:23.007 Imported new chain segment      number=18 hash=e4029b..76d214 blocks=1 txs=0 mgas=0.000 elapsed
=1.007ms mgasps=0.000 triedirty=0.00B
Clique Prepare Block Nr: 19 MixDigest: 0x0000000000000000000000000000000000000000000000000000000000000031
INFO [10-25]14:48:23.009 Commit new sealing work      number=19 sealhash=d3a06f..346253 txs=0 gas=0 fees=0 elapsed="8
17.962µs"

Terminal - aepd@Xubuntu: ~/Documents/GETH_PoC/private_BC/scripts blockchain
INFO [10-25]14:47:53.009 Imported new chain segment      number=17 hash=5e1139..b03d26 blocks=1 txs=0 mgas=0.000 elapsed
=1.029ms mgasps=0.000 triedirty=0.00B
Clique Prepare Block Nr: 18 MixDigest: 0x0000000000000000000000000000000000000000000000000000000000000031
INFO [10-25]14:47:53.013 Commit new sealing work      number=18 sealhash=a26af1..c85878 txs=0 gas=0 fees=0 elapsed=1.
429ms
INFO [10-25]14:48:23.003 Successfully sealed new block      number=18 sealhash=a26af1..c85878 hash=e4029b..76d214 elapsed=2
0.000s
Estoy en commitWork justo tras sellar el bloque, para comprobar el BIP-9
BitVersion (MixDigest) del bloque numero: 18 MixDigest: 0x0000000000000000000000000000000000000000000000000000000000000031 To
tal versión actual: 1
BitVersion (MixDigest) del bloque numero: 17 MixDigest: 0x0000000000000000000000000000000000000000000000000000000000000031 To
tal versión actual: 2
BitVersion (MixDigest) del bloque numero: 16 MixDigest: 0x0000000000000000000000000000000000000000000000000000000000000031 To
tal versión actual: 3
BitVersion (MixDigest) del bloque numero: 15 MixDigest: 0x0000000000000000000000000000000000000000000000000000000000000000 To
tal versión actual: 3
BitVersion (MixDigest) del bloque numero: 14 MixDigest: 0x0000000000000000000000000000000000000000000000000000000000000000 To
tal versión actual: 3
Clique Prepare Block Nr: 19 MixDigest: 0x0000000000000000000000000000000000000000000000000000000000000031
INFO [10-25]14:48:23.008 Commit new sealing work      number=19 sealhash=dc8e0c..c6857 txs=0 gas=0 fees=0 elapsed=3.
662ms
WARN [10-25]14:48:23.008 Block sealing failed      err="signed recently, must wait for others"

```

Figura 17. Proceso de acuerdo entre los nodos validadores (inspirado en el BIP-0009). Los bloques generados con esta nueva versión muestran un valor '0...0031' (texto '1' codificado en hexadecimal), en tanto que los anteriores muestran '0...0000'.

Cuando se alcanza la mayoría de los bloques generados con el indicador de esta nueva versión, este se modifica para indicar que se acepta la modificación a la par que los nodos validadores modifican sus bases de datos, haciendo efectivo el derecho de supresión.



```

Xubuntu 22.04_1 [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
/home/aepd/Documents/GE... Terminal - aepd@Xubuntu: ~...

Terminal - aepd@Xubuntu: ~/Documents/GETH_PoC/private_BC/scripts blockchain
File Edit View Terminal Tabs Help

tal versión actual: 2
BitVersion (MixDigest) del bloque numero: 17 MixDigest: 0x0000000000000000000000000000000000000000000000000000000000000031 Tc
tal versión actual: 3
BitVersion (MixDigest) del bloque numero: 16 MixDigest: 0x0000000000000000000000000000000000000000000000000000000000000031 Tc
tal versión actual: 4
BitVersion (MixDigest) del bloque numero: 15 MixDigest: 0x0000000000000000000000000000000000000000000000000000000000000000 Tc
tal versión actual: 4
!!!!!!! Alcanzado acuerdo en VersionBIP
-----
Atualizando DB
Escribir número de Versión actual: v: 1
Clique Prepare Block Nr: 20 MixDigest: 0x0000000000000000000000000000000000000000000000000000000000000041636365707465642d31
INFO [10-25]14:48:53.071] Commit new sealing work number=20 sealhash=f46192..d05c0a txs=0 gas=0 fees=0 elapsed=3.147ms
WARN [10-25]14:48:53.071] Block sealing failed err="signed recently, must wait for others"
FIN actualizar DB. BIP-9 Aplicado
-----
INFO [10-25]14:49:23.036] Imported new chain segment number=20 hash=d75e0a..aa7085 blocks=1 txs=0 mgas=0.000 elapsed="551.464µs" mgasps=0.000 triedirty=0.00B
Clique Prepare Block Nr: 21 MixDigest: 0x0000000000000000000000000000000000000000000000000000000000000041636365707465642d31
INFO [10-25]14:49:23.037] Commit new sealing work number=21 sealhash=35cdeb..c87804 txs=0 gas=0 fees=0 elapsed="405.376µs"

Xubuntu 22.04_2 [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
/home/aepd/Documents/GE... Terminal - aepd@Xubuntu: ~/...

Terminal - aepd@Xubuntu: ~/Documents/GETH_PoC/private_BC/scripts blockchain
File Edit View Terminal Tabs Help

9.924s
Estoy en commitWork justo tras sellar el bloque, para comprobar el BIP-9
BitVersion (MixDigest) del bloque numero: 20 MixDigest: 0x0000000000000000000000000000000000000000000000000000000000000031 Tc
tal versión actual: 1
BitVersion (MixDigest) del bloque numero: 19 MixDigest: 0x0000000000000000000000000000000000000000000000000000000000000031 Tc
tal versión actual: 2
BitVersion (MixDigest) del bloque numero: 18 MixDigest: 0x0000000000000000000000000000000000000000000000000000000000000031 Tc
tal versión actual: 3
BitVersion (MixDigest) del bloque numero: 17 MixDigest: 0x0000000000000000000000000000000000000000000000000000000000000031 Tc
tal versión actual: 4
BitVersion (MixDigest) del bloque numero: 16 MixDigest: 0x0000000000000000000000000000000000000000000000000000000000000031 Tc
tal versión actual: 5
!!!!!!! Alcanzado acuerdo en VersionBIP
-----
Atualizando DB
Escribir número de Versión actual: v: 1
Clique Prepare Block Nr: 21 MixDigest: 0x0000000000000000000000000000000000000000000000000000000000000041636365707465642d31
INFO [10-25]14:49:23.026] Commit new sealing work number=21 sealhash=39ecb6..d11806 txs=0 gas=0 fees=0 elapsed=2.795ms
WARN [10-25]14:49:23.027] Block sealing failed err="signed recently, must wait for others"
FIN actualizar DB. BIP-9 Aplicado
-----

```

Figura 18. Acuerdo alcanzado entre los nodos validadores (inspirado en el BIP-00009). Los nodos modifican sus bases de datos y el indicador del nuevo bloque se actualiza para indicar que la modificación se ha aceptado (los bloques generados a partir de ahora muestra el valor 'Accepted-1', codificado en hexadecimal).

1. Transacciones

Una vez alcanzado el acuerdo y haciéndose efectivo el *Hard Fork*, se puede comprobar que la dirección de la cuenta en cuestión ya no aparece en las interacciones que tuvo con la infraestructura Blockchain. Para mostrar los resultados de una manera visual y sencilla se ha usado el explorador de bloques local *Ethernal*⁸⁴. El explorador de bloques no muestra datos de las transacciones dado que se han provocado inconsistencias controladas, y, por tanto, no puede decodificar correctamente los datos correspondientes (no obstante, las

⁸⁴ <https://app.tryethernal.com/>

bases de datos de los nodos contienen los datos en bruto de los bloques y las transacciones con las modificaciones efectuadas).

! Some transactions in this block are still being processed (0 / 1).

Block 7

GAS LIMIT	MINED ON	HASH
99,318,416	10/25 10:05:32 AM 4 days ago	0x17ad628883598a2f2d4b12b8410b0240ce22ab644952d3 ce7a157e9db42ac1ac

Transactions

Txn Hash	Method	Block	Mined On ↓	From	To	Value	Fee
No transactions found							
Rows per page: 10 - < >							

Figura 19. El explorador de bloque no puede decodificar la transacción y advierte con un error. La cuenta en cuestión no aparece y no se muestran los datos de la transacción.

Txn Hash	Method	Block ↓	Mined On	From	To	Value	Fee
0x492_d227		13	10/25 10:08:32 AM 4 days ago	0x7dbe45_3996	0xa7941c_9468	0.000000000000000003 Ether	0.000021 Ether
0xa3d_ea18		13	10/25 10:08:32 AM 4 days ago	0x7dbe45_3996	0x98db3b_e99f	0.000000000000000002 Ether	0.000021 Ether
0xa2b_7a70	0xd0679d34	12	10/25 10:08:02 AM 4 days ago	0x98db3b_e99f	0x2e9083_83ce	0 Ether	0.00005239 Ether
0x489_e157		12	10/25 10:08:02 AM 4 days ago	0x17c3b4_a197	0x7c869b_b438	0.000000000000000001 Ether	0.000021 Ether
0x95c_4de6	0x40c10f19	11	10/25 10:07:32 AM 4 days ago	0x17c3b4_a197	0x2e9083_83ce	0 Ether	0.00004421 Ether
0xdb7_a5cd	transfer	11	10/25 10:07:32 AM 4 days ago	0x7dbe45_3996	0xa1e040_44bd	0 Ether	0.00005161 Ether
0x20f_2cbe		11	10/25 10:07:32 AM 4 days ago	0x7dbe45_3996	0xa7941c_9468	0.000000000000000003 Ether	0.000021 Ether
0xf88_d2e5		11	10/25 10:07:32 AM 4 days ago	0x7dbe45_3996	0x98db3b_e99f	0.000000000000000002 Ether	0.000021 Ether
0xd69_a7a2		10	10/25 10:07:02 AM 4 days ago	0x7dbe45_3996	0xa7941c_9468	0.000000000000000003 Ether	0.000021 Ether
0 added_2080		10	10/25 10:07:02 AM 4 days ago	0x7dbe45_3996	0x98db3b_e99f	0.000000000000000002 Ether	0.000021 Ether
0 added_d775	transfer	10	10/25 10:07:02 AM 4 days ago	0x7dbe45_3996	0xa1e040_44bd	0 Ether	0.00005161 Ether
0x8da_f789		9	10/25 10:06:32 AM 4 days ago	0x7c869b_b438	0x17c3b4_a197	0.000000000000000001 Ether	0.000021 Ether
0x509_e6a4		9	10/25 10:06:32 AM 4 days ago	0x7dbe45_3996	0x98db3b_e99f	0.000000000000000002 Ether	0.000021 Ether
0x621_12fa		9	10/25 10:06:32 AM 4 days ago	0x7dbe45_3996	0xa7941c_9468	0.000000000000000003 Ether	0.000021 Ether
0xc47_98fe	0xf088d547	9	10/25 10:06:32 AM 4 days ago	0x7c869b_b438	0xa1e040_44bd	0.007 Ether	0.00006408 Ether
0x982_1443	0x60806040	7	10/25 10:05:32 AM 4 days ago	0x17c3b4_a197		0 Ether	0.0004159 Ether
0x940_6b95		6	10/25 10:05:02 AM 4 days ago	0x7dbe45_3996	0xa7941c_9468	0.000000000000000003 Ether	0.000021 Ether
0x7f5_2beb		6	10/25 10:05:02 AM 4 days ago	0x7dbe45_3996	0x98db3b_e99f	0.000000000000000002 Ether	0.000021 Ether
0xf97_c9f0	0x60806040	4	10/25 10:04:02 AM 4 days ago	0x7c869b_b438		0 Ether	0.0008648 Ether
Rows per page: 100 - <							

Figura 20. En la cadena original se muestran las 19 transacciones en el explorador de bloques

Figura 21. En la cadena modificada se muestran 14 transacciones en el explorador de bloques, las 5 en donde se revelaba la cuenta del usuario que ejerce el derecho de supresión no pueden obtenerse.

[illegible][illegible][illegible]

Página: 49 de 54

Figura 30. Tras el Hard Fork, la dirección de la cuenta eliminada ya no está en la información del recibo de la transacción de transferencia de tokens del primer Smart Contract, ha sido adecuadamente modificada.

VI. DESARROLLOS FUTUROS

La PoC presentada en este documento no pretende ser una solución comercial de aplicación directa en el mercado ni un desarrollo que se pueda poner en producción. Tampoco pretende validar que la forma de conseguir el cumplimiento del RGPD en un tratamiento sea realizando modificaciones después de que el tratamiento ya está diseñado o incluso en explotación. Al contrario, el no contemplar la protección de datos desde el diseño es, en sí mismo, un incumplimiento normativo.

En el momento actual la Prueba de Concepto contempla fundamentalmente la aplicación del derecho de supresión (eliminación de una cuenta y todas sus interacciones acontecidas en la infraestructura Blockchain). Como se ha señalado antes, está basada en el empleo del mecanismo de *Hard Fork* para implementar una gestión de las inconsistencias y permite que el sistema continúe operando con garantías. En esta solución no se recompone la integridad de los bloques con datos borrados y se aprovecha el hecho de que un nodo no valida constantemente el pasado, sino que usa su base de datos local para la validación. No obstante, es posible usar otras aproximaciones, como técnicas basadas en la restauración de la integridad matemática de los bloques de la Blockchain mediante, por ejemplo, hash Camaleón, transacciones mutables (varias versiones de una transacción), nuevas estructuras de bloques, estrategias *off-chain*, pruebas de conocimiento cero ZKP, borrado local, poda (*pruning*), como las usadas en diversas investigaciones y proyectos que han explorado estrategias para desarrollar Blockchain “*redactables*”.

Por último, en la PoC no se ha tenido en cuenta los efectos que pudieran derivarse del derecho de supresión sobre el usuario que ejerce dicho derecho, es decir, la recuperación de sus fondos o balances en *Smart Contracts*, asumiendo que el usuario tendría que gestionar esos efectos antes de realizar su solicitud de supresión, por ejemplo, transfiriendo los fondos y balances a otras cuentas. Desarrollos futuros podrían contemplar este hecho.

VII. CONCLUSIONES

Utilizando tecnologías Blockchain se pueden crear infraestructuras que permiten el almacenamiento e intercambio de información de forma distribuida y descentralizada. Dichas infraestructuras Blockchain adaptan dicha tecnología a sus objetivos concretos y se complementan con sistemas y aplicaciones adicionales. Un tratamiento podría decidir implementar algunas de sus operaciones, por ejemplo, almacenamiento, utilizando dicha infraestructura. A su vez, la infraestructura Blockchain podría dar soporte a operaciones de distintos tratamientos. Finalmente, la gestión de la propia infraestructura podría implicar tratamientos específicos de datos personales.

Cualquier proyecto que implique desarrollar un nuevo tratamiento de datos personales haciendo uso de esta tecnología debe asegurar que el cumplimiento de los principios, derechos y obligaciones establecido por el RGPD no esté limitado por elegir una opción tecnológica concreta. Si el diseño original impide el cumplimiento, dicho diseño ha de modificarse para que garantice y pueda demostrar el cumplimiento del RGPD. Si, tras evaluar su viabilidad técnica y normativa, se decide implementar alguna operación del tratamiento sobre una solución basada en Blockchain, se deberá analizar cuidadosamente el tratamiento, su contexto, alcance e implicaciones para garantizar el cumplimiento. Más allá del cumplimiento de mínimos, si una opción tecnológica implica un alto riesgo para los derechos y libertades de los interesados deberá gestionarse dicho riesgo y someterse a un análisis de idoneidad, proporcionalidad y necesidad en el marco de superar una evaluación de impacto para la protección de datos.

En muchas de las actuales infraestructuras Blockchain no se aplican desde el diseño los principios de protección de datos, en particular, el de responsabilidad proactiva. El hecho de que en el diseño de una infraestructura Blockchain no se haya contemplado la gestión del cumplimiento normativo como uno de los objetivos, no es un problema de la tecnología en sí. El problema reside en que los diseñadores no han contemplado en el marco de gobernanza de la infraestructura dichos objetivos y, por tanto, no se han incluido desde el diseño los mecanismos de gestión oportunos.

En muchos casos se están implementando infraestructuras Blockchain, o tratamientos sobre dichas infraestructuras, con un gran desconocimiento de cómo funcionan los componentes, códigos o aplicaciones que se emplean en dichas infraestructuras. En muchas ocasiones se carece de una documentación mínima que los describa, no se han realizado los análisis necesarios para demostrar que funcionan con la calidad necesaria, y la información es insuficiente para que se puedan adaptar a los requisitos normativos. Ningún tratamiento debería construirse con sistemas, productos, servicios o componentes si los responsables y los encargados del tratamiento no están en condiciones de cumplir sus obligaciones de garantizar y demostrar el cumplimiento en materia de protección de datos (considerando 78 y artículos 24(1), 25 y 32(1)b)).

Sin embargo, es posible, y se debe, cumplir con el RGPD, independientemente de las tecnologías empleadas para la implementación de tratamientos, mediante la implementación de medidas jurídicas, organizativas y técnicas adecuadas (considerando 15 del RGPD).

El Comité Europeo de Protección de Datos ha manifestado que no puede invocarse la imposibilidad técnica para justificar el incumplimiento de los requisitos del RGPD⁸⁷. Especialmente teniendo en cuenta que el artículo 25, apartado 1, del RGPD establece que la protección de datos desde el diseño implica tenerla en cuenta en el momento de la

⁸⁷ EDPB, Report of the work undertaken by the ChatGPT Taskforce de mayo de 2024, párrafo 7: “In particular, technical impossibility cannot be invoked to justify non-compliance with these requirements, especially considering that the principle of data protection by design set out in Article 25(1) GDPR shall be taken into account at the time of the determination of the means for processing and at the time of the processing itself”.

determinación de los medios de tratamiento y en el momento del propio tratamiento. En el caso que nos ocupa, como en otros que ha abordado la AEPD⁸⁸, cabría preguntarse cuándo nos encontramos ante una imposibilidad técnica de proteger los derechos y libertades de las personas, y cuándo nos encontramos ante una resistencia a aplicar soluciones para la protección de tales derechos.

Por ello, es imperativo para los responsables, encargados y desarrolladores conocer las implicaciones, posibilidades y limitaciones reales de los componentes que seleccionan para construir productos, servicios y tratamientos. Este conocimiento ha de partir de la evidencia objetiva obtenida a través de la documentación, certificación y/o auditoría de estos. Responsables, encargados y desarrolladores, incluyendo también a las autoridades de control, han de cuidar la terminología utilizada. La actual terminología genera confusión en los conceptos y sus implicaciones. Hay que evitar el establecer conclusiones sobre términos imprecisos, para evitar equívocos sobre la realidad tecnológica.

La Prueba de Concepto, aquí presentada, desarrolla una aproximación a la implementación de medidas técnicas y de una política de protección de datos en la gobernanza de la infraestructura Blockchain, en la que se demuestra que es posible el cumplimiento del RGPD. Más concretamente, permite el ejercicio del derecho de supresión mediante una gestión de las inconsistencias que permite que la infraestructura continúe operando con las mismas garantías.

Para ello, se han diseñado unos procedimientos para la ejecución del derecho de supresión. A su vez, se ha adaptado el código y las aplicaciones de una infraestructura real, mundialmente empleada, que es la oficial de Ethereum, configurada con el mecanismo de consenso de prueba de autoridad *clique*. Además, se han tenido en cuenta todos los datos personales que se pueden tratar en la infraestructura, como son el remitente y destinatario de una transacción, los datos adicionales que contiene una transacción, el almacenamiento de los *Smart Contract* y los recibos de las transacciones que involucran *Smart Contracts* (*receipts/logs*). Esto ha requerido realizar un trabajo intenso de investigación sobre el código de la infraestructura, de documentación de esta y el despliegue de un caso de uso. Finalmente, se han definido las medidas de gobernanza necesarias para su aplicación.

En este caso concreto, la estrategia técnica empleada sobre una infraestructura Blockchain, que originalmente no tiene en cuenta la protección de datos desde el diseño, obliga a modificar directamente las bases de datos de los nodos. Este tipo de medidas, en cuanto a su impacto en la gestión de la infraestructura, se toman periódicamente en éstas cuando se ha necesitado hacer frente a incidentes críticos en su operación. Los teóricamente rígidos principios de Blockchain se adaptan a las infraestructuras concretas, así como a los incidentes que ocurren en ellas, como los mencionados en el capítulo IV, *DAO Fork* de Ethereum y *Bitcoin Cash Fork*, entre otros muchos casos.

A pesar de haber sido desarrollada sobre una infraestructura Blockchain muy extendida, supone una prueba de laboratorio, ya que el desarrollo de soluciones comerciales está fuera de la competencia de una autoridad de control. En ningún caso la AEPD está imponiendo la utilización de este ejemplo, ni supone un compromiso con relación al ejercicio de los poderes que le otorga el RGPD como autoridad de supervisión.

Para terminar, esta Prueba de Concepto no está validando que la forma de conseguir el cumplimiento del RGPD sea la modificación de infraestructuras Blockchain que han incumplido la protección de datos desde el diseño o el principio de responsabilidad proactiva. En ninguna clase de tratamiento esta es la forma de actuar. Al contrario, tiene el propósito de promover entre los diseñadores, autoridades y organizaciones que tienen algún papel en

⁸⁸ <https://www.aepd.es/areas-de-actuacion/innovacion-y-tecnologia#Menores>

el diseño y desarrollo de estas tecnologías la adopción de estrategias de protección de datos desde el diseño y por defecto que cumplan con los requisitos del RGPD.