UNIÓN EUROPEA

PROYECTO COFINANCIADO POR EL FONDO EUROPEO DE DESARROLLO REGIONAL (FEDER)

Una manera de hacer Europa

MINISTERIO DE INDUSTRIA, TURISMO Y COMERCIO

Bettergy

Entregable 17

CUMPLIMIENTO REQUISITOS DE PROPIEDAD INTELECTUAL Y PROTECCÓN DE DATOS

Impulso Tecnologías Habilitadores Digitales (THD) Expediente: TSI-100907-2019-19

1. Introducción

Una de las actividades más importantes incluidas en este proyecto fue investigar si, y en qué medida, las aplicaciones de Blockchain desarrolladas cumplen con las normas y leyes vigentes en términos del tratamiento de la innovación y los datos que estas realizan. Esta actividad se concibió inicialmente como una subcontratación en su totalidad, no obstante, se ha realizado en su mayor parte de forma interna a partir del aprendizaje alcanzado por el personal dedicado, accediendo a especialistas para su validación.

Las dos materias investigadas en esta actividad, por su impacto en el desarrollo de las aplicaciones de Blockchain son: la propiedad intelectual y la protección de datos. Por un lado, investigamos el impacto potencial de Blockchain en el registro, la protección, la gestión y la observancia de los DPI. Para ello toma como referencia la guía "*Blockchain: Legal & Regulatory Guidance*" en su segunda edición, elaborada por *The Law Society* y *Tech London Advocate*, actualizada en 2020.

Este trabajo explora múltiples facetas de los DPI en el contexto de Blockchain / DLT, haciendo comparaciones con la jurisprudencia actual que sirven para ilustrar la amplia gama de impactos que estas tecnologías podrían tener a través de los derechos de autor, marcas, derechos de diseño, derechos de bases de datos, información confidencial y patentes. También, plantea preguntas interesantes para una mayor consideración con respecto a la subsistencia de la protección de los derechos de autor en la arquitectura DLT, los criptoactivos y los contratos inteligentes, así como puntos auxiliares sobre la jurisdicción y el agotamiento.

Por otro lado, estudiamos modelo de compartición de información de registros en la cadena de bloques. El objetivo es estudiar todas las vías posibles de cumplir con normas de privacidad y manejo de datos de usuario por parte de los clientes. Para ello revisamos la ley vigente sobre protección de datos, el reglamento general de protección de datos (RGPD) y cómo afecta a las características de diferentes tipos de Blockchains, enfrentando conceptos como el de la inmutabilidad con el derecho al olvido.

Finalmente, comentamos la estrategia que estamos llevando desde Bettergy en el desarrollo de las aplicaciones de Blockchain, en particular la que se ha desarrollado como parte del presente proyecto, así como las alianzas que hemos creado para mantenernos actualizados.

2. Propiedad intelectual

La propiedad intelectual (PI) se relaciona con las creaciones de la mente: invenciones, obras literarias y artísticas, así como símbolos, nombres e imágenes utilizados en el comercio[1]. La PI

[1] https://www.wipo.int/about-ip/es/

titulares de marcas. En general, no sabemos si las aplicaciones vinculadas a DLT o incluso las propias Blockchains pueden tener derechos de base de datos. Sabemos que la información confidencial puede almacenarse (y permanecer confidencial) en una Blockchain, dadas las supuestas capacidades de custodia. No obstante, se recomienda revisar la estructura de la Blockchain y si diversas aplicaciones, como los contratos inteligentes, atraen derechos de PI, incluida la idoneidad de la protección por patente.

En el material de referencia se realizan importantes recomendaciones respecto al tratamiento de elementos fundamentales como lo son:

- ☑ **Las bases de datos.** No existe seguridad jurídica para los desarrolladores sobre el nivel de protección de los derechos de base de datos para sus creaciones. Es necesario que un tribunal aclare si, y en qué medida, un derecho de base de datos subsistirá en DLT y en cualquier aplicación basada en DLT.
- ☑ **La información confidencial.** Actualmente existe un riesgo relacionado con si la seguridad criptográfica en DLT es lo suficientemente segura como para permitir que la información confidencial se almacene en la cadena. La orientación sobre esta cuestión aumentaría la confianza en la tecnología. Mientras tanto, las aplicaciones que se creen deben limitar al máximo la cantidad de información confidencial que se almacena en la DLT.
- ☑ **La propiedad intelectual que subsiste en la propia Blockchain.** Hay poca orientación sobre qué elementos de la DLT, como el software o el diseño subyacentes, pueden protegerse. Además, en qué medida la tecnología y las redes (incluidos los contratos inteligentes) estarán protegidas por cada uno de los derechos de autor (por ejemplo, en el código del software), el derecho de base de datos (por ejemplo, en la estructura de la Blockchain) o la patente (por ejemplo, en el proceso de construcción de bloques) sería beneficioso para los profesionales, de modo que pueda haber un entendimiento entre las partes interesadas clave en cuanto al nivel de protección que se puede lograr en el propio marco DLT.
- ☑ **La naturaleza distribuida de la DLT.** Falta orientación sobre si la naturaleza distribuida de la DLT se verá influida por la territorialidad de los derechos de PI, dadas las diferentes jurisdicciones en las que pueden estar basados los diversos actores.
- ☑ **Derechos de autor en Blockchain.** Se debe considerar el marco jurídico existente que protege los derechos de autor digitales, dada la posibilidad de que tanto los titulares de derechos como los infractores permitan el acceso a las obras originales a través de la Blockchain.

3. Protección de datos personales

El RGPD (Reglamento General de Protección de Datos) es la norma europea que regula la protección de los datos personales de las personas que se encuentran en la Unión Europea, independientemente de que los datos sean tratados por empresas establecidas en la UE o en otro Estado. Corresponde por tanto a un marco legal de protección de datos nacido con el propósito de otorgar un mayor nivel de protección a los individuos y promover al propio tiempo la libre circulación de los datos personales dentro de las fronteras de la UE y hacia esos países

que cuenten con un nivel de protección de datos adecuado. Además, es una norma tecnológicamente neutra, porque se aplica a cualquier tratamiento de datos personales que recaiga dentro de su ámbito de aplicación, independientemente de la tecnología utilizada.

Cuando se elaboró el RGPD se estaba pensando en proteger a los ciudadanos frente al poder abusivo de los grandes silos de datos centralizados, y no en tecnologías de libre acceso como BlockChain con nodos distribuidos por todo el mundo que mantienen una copia idéntica de una misma base de datos, por lo tanto, surgen preguntas sobre cómo cumplir la normativa vigente en aplicaciones basadas en esta tecnología.

Entre las características que pueden afectar a las Blockchains y sus capacidades, y por tanto la recomendación es prever su tratamiento, hay que destacar:

- ☑ **El consentimiento**. La LOPD establece que este debe ser expreso, es decir, debe darse con una clara acción afirmativa. En el caso del Blockchain cada usuario verifica y valida los datos antes de que se agreguen a la cadena de bloques y el historial de transacciones proporciona una prueba de consentimiento, por lo que no entra en conflicto con el RGPD de forma directa, pero si indirecta cuando se tiene en cuenta el derecho al olvido.
- ☑ **Información a usuario y consentimiento sobre datos utilizados.** Es obligatorio informar adecuadamente a los usuarios según el (Art. 5 LOPD) Cuando se soliciten datos personales se informará de modo expreso, preciso e inequívoco:
  - Existencia de un fichero o tratamiento
  - Finalidad
  - Destinatarios
  - Obligación o no de su respuesta a las preguntas
  - Consecuencias de suministrarlos o no
  - Sus derechos
  - Identidad y dirección de la empresa que los tratará
- ☑ **Privacidad desde el diseño.** Se han tenido en cuenta diferentes aspectos para poder realizar desde el inicio un buen diseño realizando un ejercicio de análisis de los riesgos que pueden suponer para el derecho a la protección de datos de los afectados cuyos datos se tratan y, como resultado de ese análisis, la gestión de dichos riesgos mediante la adopción de las medidas necesarias para eliminar o atenuar en lo posible aquellos que se hayan identificado.
- ☑ **El responsable del tratamiento de los datos.** El responsable del tratamiento de los datos es quién tiene responsabilidad sobre los datos tratados, y se puede determinar según los primeros artículos del RGPD, particularmente en su artículo 4, que el responsable de tratamiento es “la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o conjuntamente con otros, determina los fines y los medios del tratamiento.” El problema con el Blockchain es que puede estar descentralizado, y es un protocolo, no un software, por lo tanto, no se puede considerar responsable del tratamiento. Sin embargo, el usuario sí se puede considerar como tal. Y con esto, se abre otra cuestión que es la identidad en la red si la red es identitaria o anónima en cuyo caso no se podría saber a ciencia cierta el responsable.
- ☑ **Derecho al olvido.** Un afectado tiene derecho a obtener del responsable del tratamiento la eliminación, tan pronto como sea posible, de sus datos personales. Y el responsable del tratamiento estará obligado a borrar dichos

datos e información personal tan pronto como sea posible. El problema con blockchain es que esto se encuentra en contraposición con la idea de inmutabilidad de blockchain, por lo que se procura que los datos sensibles no persistan en la cadena, de esta forma el responsable puede actuar sobre ellos sin alterar la red BlockChain.

- ☑ **Conservación limitada de los datos.** El artículo 5 del RGPD, enuncia que los datos personales solo deben mantenerse durante un periodo que no sea superior al necesario para los fines por los cuales se recogen. Esto entra en conflicto claro con una de las principales características del blockchain, que es la inmutabilidad de los datos. Por ejemplo, los datos no se eliminan después de cada transacción (que es la finalidad para la que se recogen). Si no que quedarán para siempre en la cadena de bloques para que se puedan revisar y como modo de prueba. Por lo expuesto, desde el punto de vista de la limitación del tratamiento, tampoco cumpliría con el RGPD y la solución es la misma que se contempla para el derecho al olvido, poder referenciar esos datos sin que las cadenas de bloques contengan información privada o sensible.

Las soluciones más comunes para adaptar las aplicaciones basadas en Blockchain a la normativa vigente son los datos referenciados y la anonimización. Por un lado, se plantea como solución persistir en blockchain solamente una referencia a datos personales. De esta forma los datos personales estrían custodiados de una forma tradicional y en la Blockchain existiría una referencia que haría de conexión entre Blockchain y BBDD centralizada.

Por otro lado, la anonimización, plantea como solución la ofuscación y el cifrado de datos de los datos personales que se almacenan en la Blockchain. La ofuscación consigue encubrir el significado de una comunicación haciéndola más confusa y complicada de interpretar. Las técnicas de ofuscación más habituales son el servicio de direccionamiento indirecto de terceros y las firmas de anillo. La primera consiste en pedir a un tercero que agregue muchas transacciones de Blockchain y las publique en la cadena utilizando su clave pública propia, encubriendo el significado de una comunicación haciéndola mucho más difícil de comprender. Mediante la segunda opción, llamadas firmas de anillo, múltiples partes firman una transacción de manera que alguien externo pueda estar seguro de que una de las partes es el firmante legítimo, sin saber cuál.

En cuanto al cifrado de datos personales, este puede ser reversible y o no reversible. En el primer caso, se busca cifrar una información de tal manera que sus contenidos no puedan ser entendidos y que solo la persona en posesión de la clave de cifrado puede descifrarla. En cifrado no reversible o hashing, no es posible descifrar la información. El uso que tiene este método es más bien el de verificar la información usando el mismo procedimiento de cifrado y comparando. Lo más destacable es que, si cambia incluso el dato más pequeño, el hash será radicalmente diferente. Esta es una forma de superar las limitaciones del derecho al olvido y la limitación de datos en el tiempo.

Habría que conocer por tanto si un dato personal hasheado está o no sujeto a la normativa, esto es, se ha seguido un proceso de anonimización correcto. En este sentido, la comunidad blockchain ya está relizando sobre múltiples técnicas criptográficas avanzadas que podrían permitir implementar enfoques de anonimización de datos aún más sólidos, como por ejemplo las Zero-knowledge proofs (ZKP) o Pruebas de Conocimiento Cero o la llamada encriptación homomórfica. Estas técnicas permiten presentar pruebas de una declaración sin revelar los

datos que subyacen a la misma. El sistema basado en blockchain más prometedor y que utiliza pruebas de conocimiento cero es ZCash (https://z.cash/es/).

4. Tratamiento de la PI y el RGPD en Bettergy

La forma en que gestionamos la propiedad intelectual y protegemos los datos sensibles es una cuestión importante en el diseño de aplicaciones de Blockchain. La inmutabilidad es uno de los aspectos fundamentales de esta tecnología que hacen cuestionarse si estamos cumpliendo varios de los derechos y legislaciones vigentes.

En especial, necesitamos introducir normas regulatorias a nivel europeo, y que afectan a todas las organizaciones nacionales de hace necesaria para viabilizar el desarrollo de aplicaciones. Cuestiones como el derecho al olvido o la portabilidad de los datos son algunos de los aspectos más complejos que deberán incluir estas nuevas normas.

En los proyectos realizados en Bettergy se han estudiado vías de abordar estos problemas tomando aproximaciones más comunes. Las soluciones adoptadas pasan por no persistir datos de carácter privado dentro de las Blockchain ya que la premisa de derecho al olvido o la limitación de los datos en el tiempo hacen que el borrado de datos no sea posible sin romper la cadena y el concepto de inmutabilidad asociado a Blockchain. Adicionalmente, se han buscado soluciones a este problema con la finalidad de encontrar algún sistema que sea capaz de mantener las propiedades de blockchain y a la vez se ajuste a la legalidad.

Los datos referenciados y la anonimización son los métodos más usados en estos casos. Siempre que se pueda, se recomienda optar por procesar los datos de la Blockchain. Si hay que registrar los datos en la Blockchain, se debe hacer en forma de anonimizada o hasheada usando una función muy segura. Por ejemplo, en el caso de uso de gestión de contratos PPA que hemos desarrollado no se registran datos personales de los participantes en la Blockchain. En su lugar, se mantiene una referencia al registro en la base de datos y solo se almacena en el Blockchain los datos estrictamente necesarios para implementar los contratos inteligentes.

Los aplicativos del ámbito de la energía y otros que se implementen deberán aplicar estos procedimientos para garantizar el cumplimiento de la normativa vigente cuando se desarrollen aplicaciones que registran o gestionan información en la Blockchain. Sobre todo, en aquellas aplicaciones que manejan datos sensibles y necesitan tener los límites muy definidos para crear confianza ante los clientes.

Finalmente, en la búsqueda de formas adecuadas para el tratamiento de la propiedad intelectual y la protección de datos en aplicaciones de Blockchain nos hemos unido a consorcios especializados como es el caso de Alastria, donde pretendemos estar al día en cuanto a las nuevas normativas y aproximaciones que puedan proponerse en la comunidad de expertos en relación con estos temas. El objetivo es desarrollar aplicaciones que no solo aporten un valor adicional desde el modelo de negocio, sino que también cumplan con las normativas y leyes vigentes así como se adapten a los cambios que estas tendrán en un futuro próximo debido a la novedad de la tecnología Blockchain.