Grant Thornton

RGPD y Blockchain

Soluciones blockchain para el
Reglamento General de Protección de Datos

Contenido

Claves del Reglamento General de Protección de Datos (RGPD)

La tecnología de registros distribuidos (DLT, por sus siglas en inglés), más conocida como Blockchain ha logrado despertar un importante interés en gran cantidad de sectores económicos gracias a su potencial transformador. Esta repercusión se debe a la posibilidad que blockchain brinda para revolucionar el papel de los intermediarios en las transacciones, debido a su capacidad para mejorar la eficiencia de procesos existentes y para crear nuevos modelos de negocio. Gracias a sus características, esta tecnología ayuda a disminuir significativamente los costes y a aumentar los beneficios de las compañías que la adoptan.

La tecnología blockchain introduce propiedades que hasta ahora no habían sido posibles, como la posibilidad de mantener inmutable la información almacenada en la red o la descentralización de los registros informacionales, lo cual aporta ventajas como la trazabilidad de las transacciones a tiempo real o la reducción de las vulnerabilidades del sistema. Sin embargo, estas propiedades, y particularmente el hecho de que la información vertida en la red no pueda editarse ni eliminarse (inmutabilidad), plantean algunos interrogantes legales que deben abordarse desde el punto de vista de la protección de datos personales.

Gestión de los retos legales

Dado que la tecnología blockchain todavía se encuentra en una fase inicial en su desarrollo, no se ha alcanzado un consenso en cuanto a su enfoque regulatorio, llegándose a plantear, en algunos casos, incluso la posibilidad de elaborar regulación específica al respecto.

La normativa de protección de datos y la llegada del nuevo RGPD plantean desafíos que deben examinarse con el objetivo de diseñar redes que mantengan las propiedades que hacen de blockchain una tecnología atractiva (inmutabilidad y descentralización), pero que, a su vez, sean capaces de cumplir con la legislación aplicable.

Resulta positivo en este sentido, que algunos organismos como la Comisión Europea, estén respondiendo con agilidad a esta tendencia tecnológica. Esto lleva, al menos, a la existencia de algunas certezas mínimas en lo que respecta al tratamiento de blockchain en relación con la protección de datos personales o la privacidad. Gracias a ello, las compañías que empiezan a operar con tecnología blockchain más allá de Pruebas de Concepto comienzan a contar con cierta seguridad en esta materia.

El objetivo de este documento es desarrollar las soluciones a los desafíos que plantea el RGPD en relación con la tecnología blockchain.

Reglamento General de Protección de Datos (RGPD)

El instrumento más reciente en materia de protección de datos es el Reglamento (UE) 2016/679, también conocido como RGPD. Su objeto es amplio y trata de ofrecer una protección integral a las personas físicas en relación con sus datos de carácter personal. Este reglamento, que será aplicable en mayo de 2018, refuerza algunos derechos, incluye nuevas figuras, y desarrolla principios cuya aplicación deberá ser homogénea en toda la Unión Europea.

¿Por qué surge RGPD?

La Directiva 95/46 CE derogada por el RGPD, contemplaba una serie de objetivos generales de protección de datos que los Estados miembros debían cumplir. Sin embargo, dicha Directiva contaba con una serie de puntos débiles, como el amplio margen otorgado a los legisladores nacionales para articular sus legislaciones de protección de datos personales, siempre y cuando cumpliesen con los objetivos establecidos en la Directiva.

Esta libertad producía divergencias entre los Estados miembros a la hora de interpretar y aplicar la norma. El resultado era una evidente falta de homogeneidad entre países que, en muchos casos, llevaba a la restricción de actividades en el mercado comunitario. Esta falta de homogeneidad regulatoria en la libre circulación de datos generaba obstáculos dentro la economía digital europea.

Aspectos principales del RGPD

A diferencia de su predecesora, el RGPD es aplicable a los datos personales de cualquier persona física, con independencia de su nacionalidad o lugar de residencia, siempre que se cumplan los requisitos que estipula el artículo 3.

El RGPD define los datos personales como “toda información sobre una persona física identificada o identificable (el interesado)”. Se considerará persona física identificable a toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular, mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona.

Técnicas de anonimización para cumplir con el RGPD

La distinción entre datos personales y no personales es de crucial importancia en una red en la que la información vertida permanece inmutable, ya que los datos no personales quedan fuera del alcance de la legislación sobre protección de datos, y por tanto del RGPD.

Para poder convertir datos personales en no personales –y evitar así su sujeción al RGPD–, es necesario aplicar técnicas de anonimización que impidan la posibilidad de identificación del titular de los datos.

Cómo utilizar la tecnología blockchain para lograr cumplir el RGPD

1. **Legitimidad del tratamiento (y el derecho de cancelación y olvido):** el tratamiento de datos personales será legítimo, entre otros, cuando el interesado haya prestado su consentimiento. Revocar el consentimiento deberá ser tan sencillo como concederlo.

   Desafío: poder eliminar los datos personales de la red blockchain en caso de que el interesado revoque su consentimiento.

2. **Principio de exactitud (y el derecho de rectificación):** los datos personales deberán ser precisos y, si fuera necesario, actualizados. Deberán tomarse todas las medidas razonables para que los datos personales inexactos (en función de los fines previstos) se supriman o rectifiquen sin demora.

   Desafío: poder modificar la información almacenada en una red blockchain.

3. **Limitación del plazo de conservación:** los datos personales deben mantenerse de tal forma que se pueda identificar a los interesados solo durante el tiempo necesario para los fines previstos.

   Desafío: poder eliminar los datos personales en el futuro, cuando concluyan los fines para los que fueron recogidos.

4. **Integridad y confidencialidad:** los datos personales se tratarán de forma tal que se garantice su seguridad, incluida su protección frente a tratamientos no autorizados o ilícitos, pérdidas accidentales, destrucción o daños, utilizando para ello medidas técnicas u organizativas adecuadas.

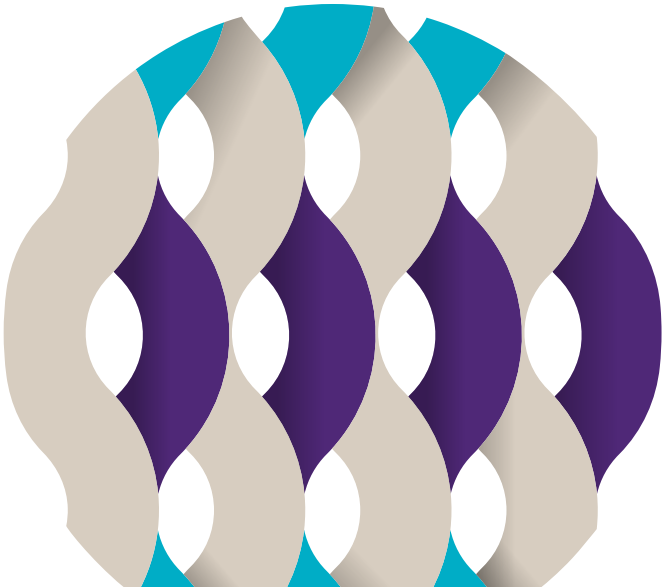
   Desafío: todos los nodos participantes de una red blockchain tienen acceso a los datos almacenados en ella (al tratarse de una red distribuida todos los nodos poseen una copia exacta de cada transacción realizada), con independencia de la autorización otorgada por el interesado.

Solución de Grant Thornton

En Grant Thornton consideramos que existen soluciones para los retos que plantea el RGPD en relación con la tecnología blockchain, permitiendo que sus principios sean compatibles con la utilización de esta tecnología. Dichas soluciones pueden dividirse en dos grupos: **función hash** y **canales privados** con datos cifrados. Analizamos ambas a continuación.

***Hashing* criptográfico**

Canales privados



Soluciones de la tecnología blockchain para los principios del RGPD

Hashing criptográfico

¿Qué es la función hash?

La función hash es una técnica criptográfica que permite generar, para cualquier tipo de documento, información o dato, un identificador (código alfanumérico) único. Mientras el dato no se modifique, este identificador resultante será siempre idéntico; en caso de la menor variación, el identificador será diferente. Por ello, el hash puede ser considerado como la huella digital de un dato específico.

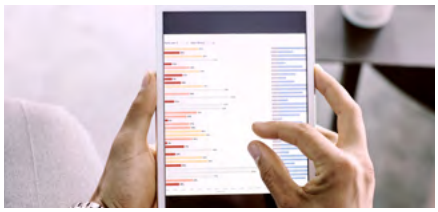
Partiendo de esta base, la solución hash en blockchain consiste en la generación de hashes o identificadores únicos para los datos personales. Dicho hash quedaría almacenado en la red blockchain mientras que los datos personales, por su parte, se mantendrían en una base de datos externa, gestionada por el responsable de tratamiento que corresponda.

¿Cómo funciona la solución hash?

Eliminación de datos: Cuando deban eliminarse los datos personales, de acuerdo con los principios de legitimidad del tratamiento o limitación del plazo de conservación, el responsable del tratamiento eliminará los datos de la base de datos externa, mientras que el hash correspondiente permanecerá en blockchain. Al eliminar los datos correspondientes con este hash, éste se convierte en un número aleatorio sin correspondencia, de modo que la información almacenada en blockchain pasa a ser ininteligible y, por tanto, irrelevante.

Modificación de datos: Cuando deban modificarse los datos, de acuerdo con el principio de exactitud, el responsable del tratamiento los modificará en la base de datos externa. El registro actualizado sustituirá al anterior registro de la base de datos externa y recibiendo un nuevo hash, que se almacenará en blockchain. El hash de los datos personales antiguos pasará a ser, nuevamente un número aleatorio carente de significado por no tener correspondencia con ningún dato de la base de datos externa.

Confidencialidad: Dado que los hashes se almacenan en blockchain y los datos personales permanecen almacenados en una base de datos fuera de la red, los nodos solo tendrán acceso a los hashes –números aleatorios sin significado para ellos–, cumpliendo así los principios de integridad y confidencialidad.



Mayor protección: "*Hashes* con salt"

Todas las soluciones anteriores se basan en el supuesto de que la función hash sea suficiente para garantizar la imposibilidad de identificar al propietario del dato, sin embargo, existe un escenario que podría poner en entredicho este enfoque. Pensemos en el siguiente ejemplo:

Si se conoce el conjunto de hashes utilizados por la compañía y se dispone del conjunto de datos a los que dichos hashes se encuentran asociados, podrían introducirse todas las posibilidades de ambos conjuntos hasta acertar y dar con el hash correspondiente a cada dato. Esto hace que el hash se considere sometido al RGPD (se trata de un dato pseudoanonimizado y por tanto un dato personal), por permitir la identificación de los interesados en ciertos supuestos. Por ello, es necesario reforzar los hashes utilizando "salt". Se entiende por "salt" un conjunto de valores aleatorios que se añaden al hash del dato personal en concreto, dificultando de esta forma la identificación del propietario de dicho dato.

Es importante utilizar la función hash con "salt" para garantizar, en la medida de lo posible, la anonimización de los datos personales, sobre todo, teniendo en cuenta que el hash, permanecerá almacenado en blockchain de forma indefinida. A este respecto, destaca la Opinión 5/2014 del Grupo de Trabajo del Artículo 29 en la que señalan los tres aspectos clave que deben analizarse para verificar que la anonimización es correcta:

- **Singularización:** ¿es posible extraer de un conjunto de datos algunos registros que identifiquen a una persona física?
- **Vinculabilidad:** ¿es posible vincular como mínimo dos registros de un único interesado o grupo de interesados?
- **Inferencia:** ¿es posible deducir con una probabilidad significativa el valor de un atributo a partir de los valores de un conjunto de otros atributos?

En conclusión, la técnica del hashing implica almacenar los hashes correspondientes a cada dato personal en la red blockchain. Por su parte, los datos personales se almacenan por separado en una base de datos gestionada por el responsable de tratamiento. De esta forma, se pueden modificar o eliminar datos personales – y garantizar que el interesado pueda ejercitar sus derechos de conformidad con el RGPD – conservando al mismo tiempo los beneficios inherentes a la inmutabilidad, propiedad básica de la tecnología blockchain.

Soluciones de la tecnología blockchain para los principios del RGPD

Canales privados

¿Qué son los canales privados?

Los canales privados son vías de transmisión de información creadas por dos o más nodos que quieren compartir información en privado dentro la red blockchain, es decir, sin que los demás nodos sepan qué contenido comparten. El resto de nodos (los que se encuentran fuera del canal privado) solo podrán conocer el hash de la información que se comparta en el canal privado.

Cómo compartir información en un canal privado: cifrado

Los datos que se comparten a través de los canales privados deben cifrarse. El cifrado es una medida de seguridad que aporta confidencialidad a un canal de comunicación entre partes identificadas, evitando la interceptación o revelación involuntaria del contenido de la información. El cifrado implica que las partes dispongan de una clave de descifrado para acceder a la información. En este caso, los nodos A y B de la red blockchain dispondrán de esta clave y serán también los encargados de su custodia.

¿Por qué datos cifrados?

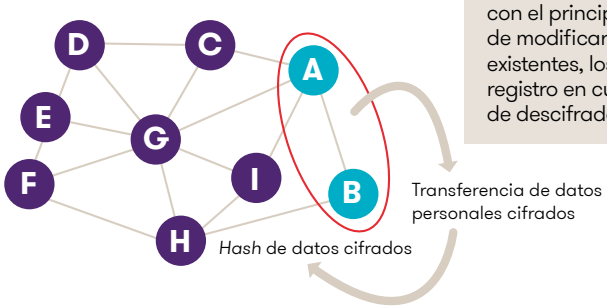
Los canales privados forman parte de la red blockchain y, aunque son privados, cuentan con todas las propiedades de la tecnología– por tanto, la información que se almacena en ellos es inmutable. La solución para los desafíos que plantea la inmutabilidad en este caso, pasa por cifrar los datos personales. Si se cifran los datos personales, cada vez que los nodos A y B tengan que eliminar o actualizar la información del canal privado conforme a los principios del RGPD, solo tendrán que suprimir la clave de descifrado de los datos personales en cuestión. Los datos cifrados permanecerán en el canal privado, pues la información almacenada en blockchain no puede eliminarse ni modificarse, pero ni A ni B podrán visualizarla al haber eliminado la clave.

Canales privados con datos cifrados: funcionamiento

1 Los nodos A y B crean un canal privado en la blockchain

2 Los datos personales cifrados se comparten en el canal privado entre A y B

3 El *hash* de datos cifrados se almacena en la blockchain "común", es decir, el resto de los nodos (C, D, E, F, G, H e I) saben que A y B han compartido información en un momento concreto, pero no pueden visualizar el contenido: solo ven el *hash*.



¿Cómo funciona esta solución?

Eliminación de datos: Cuando deban eliminarse datos personales (de acuerdo con los principios de legitimidad del tratamiento o limitación de almacenamiento), los nodos A y B eliminarán la clave de descifrado de los datos personales. Así se consigue que el registro de datos sea inidentificable e inaccesible (para todas las partes, incluidos A y B), pues la clave queda eliminada.

Modificación de datos: Cuando los datos deban modificarse (de acuerdo con el principio de exactitud), en lugar de modificar los registros de datos existentes, los nodos A y B bloquearán el registro en cuestión (eliminando la clave de descifrado). El registro actualizado sustituirá al anterior al recibir una nueva clave de cifrado. El registro anterior se vuelve inidentificable e inaccesible sin la correspondiente clave de descifrado (que ha sido eliminada).

Confidencialidad: Dado que los hashes se almacenan en la blockchain "común" y los datos personales siguen almacenados en un canal privado, los participantes de la red blockchain (nodos C, D, E, F, G, H e I) solo podrán acceder a los hashes de la información cifrada compartida en el canal privado (números aleatorios sin sentido aparente para ellos).

Referencias
- Parlamento Europeo. *Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos). Abril de 2016.*
- Grupo de Trabajo del Artículo 29. *Dictamen 05/2014 sobre técnicas de anonimización, adoptado el 10 de abril de 2014. Abril de 2014.*
- Hogan Lovells. *A guide to blockchain and data protection. Septiembre de 2017.*
- Guy Zyskind, Oz Nathan y Alex 'Sandy' Pentland. Privacy: *Using Blockchain to Protect Personal Data.*
- Chainfrog. *Blockchain and GDPR, 2017.*
- Pablo Fernández Burgueño. *La obligación legal de cifrar información y datos personales. Enero de 2017.*

Conclusiones

Protección de datos desde el diseño y por defecto

El uso de blockchain, al igual que cualquier otra tecnología innovadora, exige una valoración jurídica exhaustiva previa a fin de abordar los desafíos que pueda implicar. El RGPD incluye el principio de "protección de datos desde el diseño y por defecto". La aplicación de este principio a la tecnología blockchain exige la necesidad de diseñarla de forma que sea compatible con la legislación de protección de datos desde un primer momento, es decir, desde el diseño del proyecto.

Soluciones caso por caso

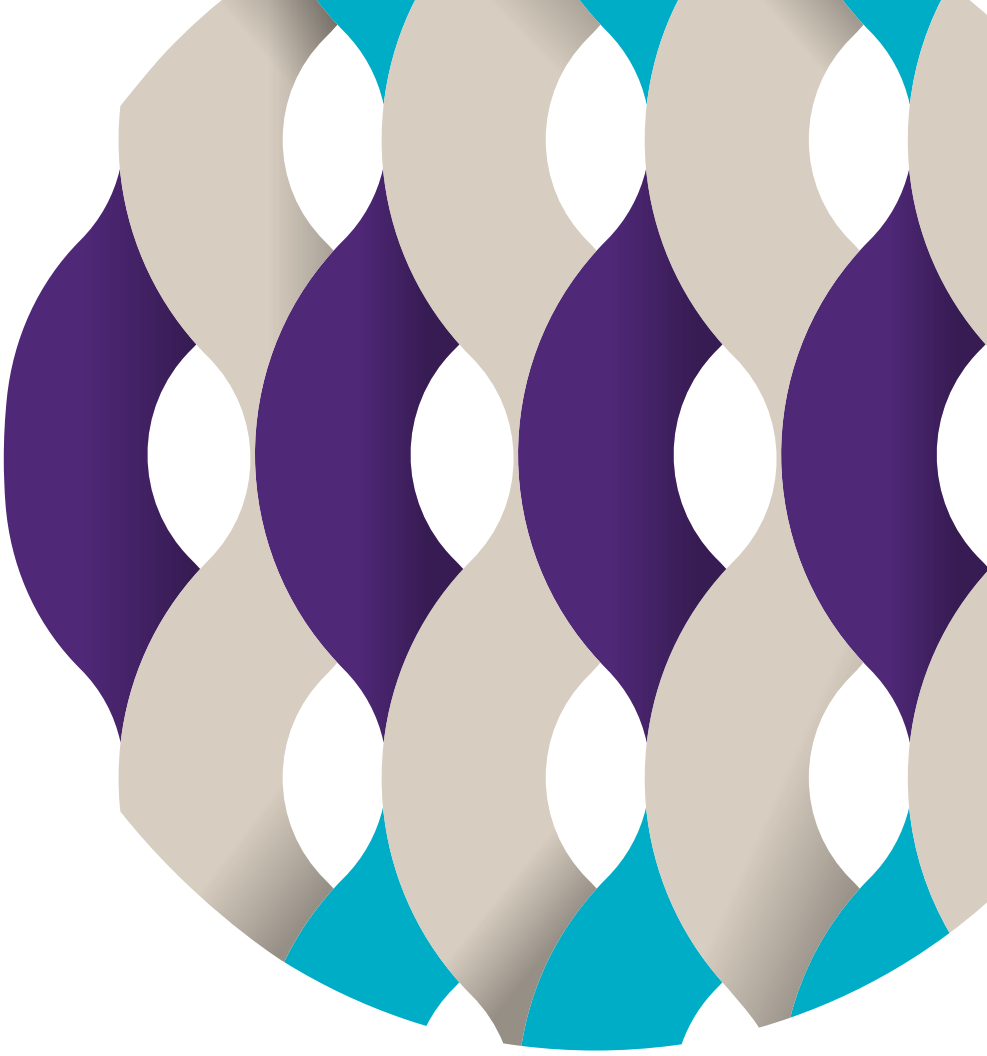
Se puede proteger la privacidad utilizando tecnología blockchain a través de diferentes métodos: función hash, canales privados o una combinación de ambos. Deberán valorarse estos métodos antes de diseñar la solución blockchain, a fin de determinar cuál responde mejor a los objetivos planteados y al modelo de negocio de la entidad – teniendo especialmente en cuenta la importancia de evitar desnaturalizar las principales características de la tecnología blockchain.

Contactos

Luis Pastor
Socio, Head of Blockchain
+34 638 184 482
Luis.Pastor@es.gt.com

Adrian White
Responsable de proyectos internacionales de blockchain
+34 659 639 467
Adrian.White@es.gt.com

Sara Esclapés Membrives
Abogada especialista en blockchain
+34 676 644 691
sara.esclapes@es.gt.com



Grant Thornton

An instinct for growth™

grantthornton.es