Blockchain y protección de datos.

Blockchain es la tecnología definida en 2009 por quien dijo llamarse Satoshi Nakamoto, personaje del que existen dudas sobre su verdadera identidad, para crear la moneda virtual bitcoin (Hoy en día, Satoshi Nakamoto es reconocido como el alias de la persona o grupo de personas que crearon Bitcoin, una figura o figuras invisibles).

Su diseñador definió dos características básicas: una primera que impide que el poseedor de una moneda pueda gastarla dos veces y una segunda consistente en la no existencia de un banco central que dé sustento a la misma actuando de tercero de confianza.

La ausencia en el bitcoin de esta figura de tercero de confianza se suple con el registro y anotación de todas y cada una de las transacciones que tienen lugar con la moneda en un "libro mayor contable" del que existen multitud de copias públicamente disponibles, de forma que es posible rastrear por qué identidades del blockchain ha pasado cada bitcoin.

La existencia de múltiples copias distribuidas del libro mayor es lo que proporciona seguridad a la moneda ya que, si alguien pretendiera manipular una transacción de pago o cobro, tendría que manipular la mayoría de las copias del libro mayor y ello requeriría de esfuerzos desproporcionados, tanto mayores cuanto mayor sea el número de copias del libro.

A pesar de que todas las transacciones realizadas con bitcoins quedan registradas en el libro mayor y éste se encuentra replicado en infinidad de ubicaciones, la privacidad de los intervinientes en las transacciones queda garantizada en la medida en que cada interviniente opera con un identificador, visible en el Blockchain, pero cuya relación con la persona que lo opera sólo es conocida por éste, por lo que es el propio usuario el que mantiene el control sobre su identidad.

El éxito que viene acumulando el bitcoin ha puesto el foco en la tecnología que lo sustenta, de tal manera que están surgiendo múltiples aplicaciones para Blockchain que van más allá de las monedas virtuales. Este efecto se ha visto aumentado tras la incorporación a la tecnología Blockchain de una nueva funcionalidad denominada contratos inteligentes o "**smart contract**", que permite no sólo registrar en el libro mayor una transacción sino un contrato o conjunto de transacciones susceptibles de ser ejecutadas en el futuro si se dan una serie de condiciones que se estipulan en el propio contrato.

El campo de nuevas aplicaciones es tan amplio que cubre todo tipo de sectores como el financiero, seguros, energía, telecomunicaciones, salud, justicia, administración pública, registros públicos y privados, etc; así como tecnología de base para todo tipo de transacciones en el marco del Internet de las cosas. De aquí que se hable del fenómeno blockchain como la "revolución industrial de internet".

Desde el punto de vista de la protección de datos y la privacidad, no cabe duda de que habrá que seguir muy de cerca el desarrollo y expansión de esta tecnología. Si bien por un lado aspectos ya citados y relativos al anonimato, junto con la posibilidad de utilizar múltiples identificadores (en los que algunos pueden ser anónimos pero otros no) puede contribuir a que los usuarios mantengan control sobre su privacidad, no están claros todavía como se podría implantar el derecho de supresión en una tecnología que no permite, en origen, alterar el libro mayor de transacciones.

En este sentido, el Reglamento General de Protección de Datos que será aplicable en mayo de 2018 incorpora mecanismos tales como la protección de datos desde el diseño y por defecto,

así como las evaluaciones de impacto en la protección de datos que serán claves para alinear el desarrollo de la tecnología Blockchain con la protección de datos de carácter personal.

Llegados a este punto, en noviembre de 2024, la Agencia Española de Protección de Datos ha publicado una nota técnica en relación con Blockchain y el derecho de supresión. La Prueba de Concepto que se presenta en este documento demuestra la viabilidad de construir infraestructuras Blockchain que permitan cumplir con el Reglamento General de Protección de Datos (RGPD).

La nota técnica describe los fundamentos de las infraestructuras Blockchain y aclara conceptos utilizados en el marco de esta tecnología desde una perspectiva de protección de datos. También analiza los casos reales de aplicación de cambios y gestión de la gobernanza habituales en dichas infraestructuras. A continuación, se desarrollan políticas, que incluyen medidas organizativas y técnicas, para implementar el derecho de supresión en una infraestructura Blockchain. Finalmente, tras analizar y documentar los componentes de una infraestructura Blockchain real de uso muy extendido, se aplican de forma práctica en un caso de uso de eliminación de la actividad de un usuario, incluyendo la información relativa a los Smart-Contracts.

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, documentado y específicamente orientado al cumplimiento del RGPD, sin pretender ser una solución comercial de aplicación directa en el mercado. 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 AEPD, consciente de la creciente adopción de Blockchain en el ámbito empresarial, ha desarrollado una Prueba de Concepto (PoC) para explorar cómo la eliminación de datos en Blockchain podría ejecutarse de manera que cumpla con el RGPD. La PoC se centra en un caso concreto: la eliminación de una cuenta de usuario en la Blockchain y todas las transacciones asociadas a ella. Este enfoque busca cumplir con el derecho de supresión mediante la alteración de datos en Blockchain a través de un proceso llamado Hard Fork, una bifurcación que permite actualizar las bases de datos de los nodos para reflejar la eliminación solicitada.

Es importante destacar que, al emplear esta técnica, no se restaura la integridad de los bloques originales, sino que se modifica la estructura de datos en la cadena para evitar que la cuenta eliminada siga visible en el historial de transacciones. La PoC propuesta por la AEPD es una aproximación experimental y no se plantea como una solución que pueda aplicarse directamente en infraestructuras Blockchain comerciales o en producción.

Dicho de otra manera, la AEPD demuestra que es técnicamente posible eliminar datos en Blockchain, pero reconoce que esta práctica va en contra del principio de inmutabilidad de la cadena. Para implementar el derecho de supresión, se necesita modificar directamente la estructura de datos, algo que, en una red de Blockchain diseñada de manera tradicional sería altamente disruptivo.

Nota técnica AEPD: https://www.aepd.es/guias/anexo-tecnico-blockchain.pdf