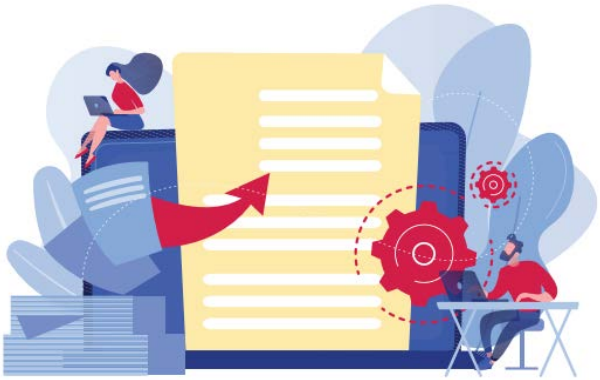
Acelera la transformación digital de tu PYME



INFORME TECNOLÓGICO – Enero 2023

Blockchain – Aplicación a la trazabilidad en el transporte de mercancía peligrosa

Elaborado por: AIDIMME

GOBIERNO DE ESPAÑA
VICEPRESIDENCIA PRIMERA DEL GOBIERNO
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL
red.es
UNIÓN EUROPEA
Fondo Europeo de Desarrollo Regional
"Una manera de hacer Europa"

1 Introducción

La tecnología Blockchain permite dejar constancia de eventos y transacciones en un registro fiable en el que se puede verificar la autenticidad de los datos. Tiene múltiples aplicaciones, y en este informe se describe un caso de aplicación para gestionar la documentación vinculada al transporte de mercancías peligrosas, en el marco del proyecto GESTABLOCK.

2 La tecnología Blockchain

La tecnología Blockchain (o cadena de bloques) se empleó por primera vez con la criptomoneda Bitcoin. La cadena de bloques emplea una base de datos distribuida, es decir, no está centralizada como sí lo está el registro civil, por usar un ejemplo que todos conocemos. En el caso del registro civil, hay que acudir a una ventanilla del registro con la solicitud de inscripción del nacimiento de nuestra hija, la persona detrás de la ventanilla recoge nuestra solicitud y nos dice que debemos volver en unos días para obtener una copia del registro. Pasados los días, volvemos a la ventanilla con nuestro justificante, se lo entregamos a la persona que está detrás de la ventanilla y nos devuelve la copia del folio del registro. En dicha copia del folio del registro vemos que hay un número de folio y un indicador de tomo del registro donde quedaron escritos los datos de nuestra solicitud. Esta copia del folio del registro tiene validez legal como certificado de nacimiento registrado por las autoridades públicas. El registro civil está centralizado y nadie, salvo las personas que trabajan en él, pueden introducir o modificar los datos. Dichas personas también deciden quienes, y bajo qué circunstancias, pueden pedir una copia del registro. Esto hace que el registro civil sea muy seguro ante intentos fraudulentos de acceder ilegalmente a sus datos y hace virtualmente imposible la adulteración fraudulenta de los datos registrados.

En la tecnología Blockchain, los datos no están centralizados, sino que están distribuidos entre los miembros de un consorcio. El consorcio decide cuándo y cómo se añade un nuevo bloque a la cadena de bloques. Para esto se cuenta con aplicaciones informáticas especializadas, que emplean la encriptación asimétrica de la información para hacerla invulnerable a los intentos fraudulentos de alterar los datos, y exige el uso de la firma digital y clave secreta de los usuarios del sistema para verificar la identidad de los usuarios que quieran acceder al sistema.

Como la tecnología Blockchain nació para servir a la criptomoneda Bitcoin, tiene la estructura de un libro mayor de contabilidad, donde se pueden introducir transacciones de pago y de cobro, junto con cualquier otro tipo de información que deseemos introducir. Es por eso por lo que en inglés se dice que la cadena de Blockchain es un “ledger”, que significa libro mayor de contabilidad. Más aún, está distribuido entre los miembros de un consorcio que se pone de acuerdo, mediante un algoritmo de consenso, para validar las solicitudes de inscripción de transacciones y datos que quieran formar parte de un nuevo bloque y dar de alta a dicho bloque al final de la cadena existente en ese momento. Los usuarios del sistema deberán acreditar su identidad (mediante clave secreta y firma digital) para poder solicitar que se añada al registro una transacción individual que, además de los datos aportados por el usuario, contarán con una marca de fecha y hora de la presentación de la solicitud. Dicha transacción se coloca en una cola

de solicitudes de entrada en el registro hasta que la cola se llena con la capacidad de transacciones que tiene un bloque. Cuando la cola esté llena, un algoritmo retirará una a una las transacciones de la cola siguiendo una especie de lotería, con el objeto de desordenarlas para evitar que una persona maliciosa hubiese enviado una secuencia de transacciones, cuyo contenido es en realidad un conjunto de secuencias numéricas muy reconocibles para quien las ha creado, y que pudieran ser empleadas posteriormente durante el análisis del bloque cifrado para facilitar el descubrimiento del método de cifrado asimétrico empleado. Las transacciones, debidamente reorganizadas al azar (como si se tratase de una baraja de naipes nueva que ha sido barajada muy a conciencia para que las cartas del naipe pierdan completamente el orden perfecto que tenían originalmente), son operadas matemáticamente con un proceso de cifrado asimétrico para crear un nuevo bloque (se emplea el cifrado de clave pública y la criptografía con curvas elípticas, que son lo mejor del estado del arte en criptografía). Una vez alcanzado el consenso entre todos los miembros del consorcio, el nuevo bloque es engarzado al final de la cadena de bloques con medidas adicionales de criptografía. Todos los miembros del consorcio supervisan el proceso y validan la inserción del nuevo bloque. Al acabar este proceso, la cadena de bloques habrá crecido con un nuevo bloque. Así es como la cadena de bloques crece en tamaño. La cadena puede ser consultada (los miembros del consorcio deciden la forma como se lleva a cabo este trámite), pero los bloques existentes en la cadena de bloques no pueden ser modificados.

Cuando se deba corregir un error en una de las transacciones de un bloque que ya estuviese inserto en la cadena, el usuario interesado deberá generar una nueva transacción de enmienda. No se permite alterar la transacción errónea porque está prohibido modificar un bloque de la cadena. En esto se parece al registro civil que, en el caso de detectarse un error, no se borran las anotaciones existentes erróneas, sino que se añade una nota de enmienda en el mismo folio del registro, habitualmente empleando para ello el espacio en blanco que hay en el margen del folio, quedando reflejados tanto el error como su enmienda.

Con esta tecnología Blockchain se consigue algo similar a un registro civil, pero con una base de datos distribuida y sin la burocracia y los costes asociados a él. Cabe recalcar que existen costes para los usuarios de los servicios que emplean la tecnología Blockchain porque alguien tiene que pagar por el sostenimiento y mantenimiento de la infraestructura (sistemas informáticos, trasmisión de datos, y la gestión y administración del consorcio, entre otros gastos).

En el caso de la criptomoneda Bitcoin (origen del Blockchain), una persona tiene en su ordenador un monedero Bitcoin que se llena y se vacía mediante transacciones de la tecnología Blockchain con la requerida presentación de la clave secreta. Todo va bien hasta que la persona pierde su monedero Bitcoin y su clave secreta, en cuyo caso nadie podrá ayudarla a recuperar su dinero porque el sistema no está pensado para revelar sus secretos a nadie (ni tan siquiera a la persona que es la legítima dueña del monedero Bitcoin).

Esto es una fortaleza del sistema porque no se puede suplantar a la persona que es la legítima dueña del monedero Bitcoin para saquear su contenido del monedero Bitcoin. En este sentido, el tristemente célebre James Howells del Reino Unido perdió el disco duro de su ordenador donde estaba su monedero Bitcoin y su clave secreta. Se cree que el valor de lo que se perdió

en el disco duro está en los trescientos millones de dólares. Otro caso similar es el de Stefan Thomas de Alemania que no ha perdido el pendrive súper seguro IRONKEY con el monedero Bitcoin, pero se ha olvidado cuál es la clave secreta para usarlo. Da la casualidad de que el pendrive súper seguro IRONKEY se auto formatea tras diez intentos fallidos de introducir la contraseña secreta (para protegerse contra los ataques de los piratas informáticos) y solamente quedan dos intentos. Dicen algunos teóricos de la informática que, en el futuro, un ordenador cuántico de suficiente potencia podría revelar los secretos del cifrado asimétrico con criptografía de curvas elípticas.

3 El transporte de mercancías peligrosas

Las mercancías peligrosas son aquellas cuyo transporte por carretera supone un riesgo. Según los últimos datos del Ministerio de Transportes (excepto Cataluña y País Vasco) durante 2019 se transportaron en España 773 millones de toneladas de sustancias catalogadas como mercancías peligrosas. En ese período de tiempo se produjeron 135 accidentes con 6 víctimas mortales no relacionadas con la mercancía, y aunque cualquier daño sobre vehículos con productos peligrosos supone un riesgo potencial para la salud humana, la seguridad y las infraestructuras, su logística y transporte cumplen una estricta reglamentación internacional con el fin de minimizar los riesgos de estas operaciones. Y es aquí donde las TIC tienen mucho que aportar. La reglamentación internacional regula el transporte de las mercancías peligrosas y obliga a las partes que participan en estas operaciones a dejar una huella documental.

La actual reglamentación internacional permite que el registro de la información se haga en formato impreso en papel (es decir, con documentación manuscrita) con todos los problemas que eso conlleva (por ejemplo, que se pierda, se manche o se traspapele la documentación) pero no prohíbe el uso de medios informáticos para gestionar la documentación. El uso de la documentación informatizada abre la puerta para la utilización de la tecnología Blockchain, que tiene muchas ventajas con respecto a la documentación manuscrita, dado que ofrece una cadena de custodia de la legitimidad del documento, quedando en evidencia cualquier alteración fraudulenta.

4 Verificación del transporte de mercancía peligrosa mediante Blockchain.

Teniendo en cuenta lo expuesto en los apartados anteriores, el ITI[1] junto con AIDIMME[2] unieron sus fuerzas para dar forma al proyecto GESTABLOCK[3], que nació con el objetivo de minimizar los riesgos en el transporte de mercancías peligrosas.

[1] Centro Tecnológico de Investigación, Desarrollo e Innovación en tecnologías de la Información y las Comunicaciones (TIC). https://www.iti.es/

[2] Instituto Tecnológico Metalmecánico, Mueble, Madera, Embalaje y Afines. https://www.aidimme.es/

[3] https://actualidad.aidimme.es/tag/gestablock-aidimme-iti/

Para conseguirlo, desarrollaron una plataforma que monitoriza las distintas fases del transporte de mercancías peligrosas, utilizando una solución Blockchain para el registro de aquella información considerada relevante y que hace partícipes a todos los actores involucrados.

Para ello, el ITI creó un sistema para la transferencia de documentos con la tecnología Blockchain y una base de datos distribuida DLT para cumplir con el requisito de la normativa vigente relativo a los documentos del transporte de mercancías peligrosas.

Por su parte, AIDIMME desarrollo un dispositivo para control de desperfectos de la mercancía durante el transporte. Se sabe que, durante el transporte, la mercancía puede recibir golpes que la dañen y es importante que se determine quién la tenía en el momento en el que se produjo el desperfecto, para que su seguro cubra los daños. Pero, hasta el momento, el daño se conocía al abrir el embalaje, por lo que quedaba la duda de quién tenía la custodia de la mercancía en el momento del percance. En el proyecto Gestablock se añadió un dispositivo que registra el instante de tiempo (fecha y hora) y la gravedad del desperfecto y, mediante las comunicaciones inalámbricas, se transmite esta información para que sea incorporada a las informaciones documentadas con la tecnología Blockchain. De esta manera, queda registrado con marca de fecha y hora que la mercancía sufrió un percance. Esto permite dilucidar quién era responsable de la mercancía en el momento de producirse el desperfecto.

Adicionalmente, en el proyecto se realizaron ensayos de caída libre de envases y embalajes de mercancía peligrosa para verificar el cumplimiento de la normativa.

4.1 Desarrollo de un dispositivo ciberfísico para registrar incidencias en el transporte.

Este dispositivo integra distintos sensores (temperatura, vibraciones) así como capacidades básicas de computación, almacenamiento y comunicación inalámbrica para conectarse con la plataforma.

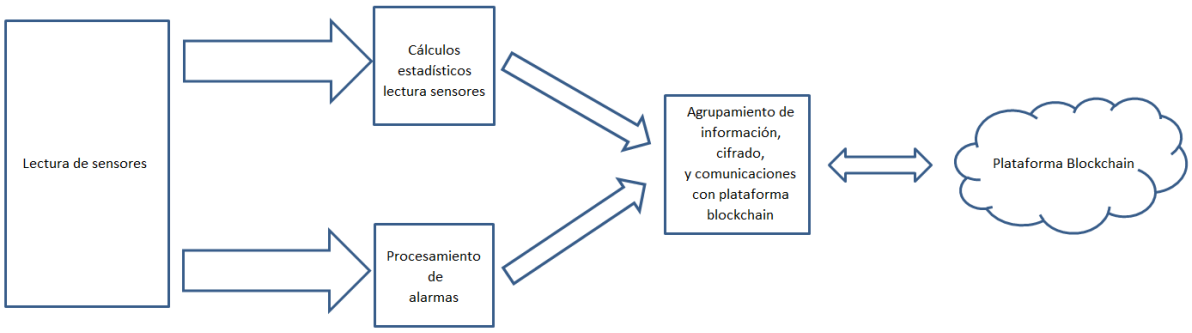
Las características de estos dispositivos incluyen:

- Plug&sense, es decir que no requieren instalación ni configuración.
- Bajo consumo de la batería.
- Inteligentes, que aprenden de su entorno y pueden detectar eventos no habituales.
- Con capacidad de comunicarse entre ellos para incrementar su “inteligencia”.

Dispositivo inteligente autónomo

El fin del dispositivo inteligente autónomo es la lectura de los sensores integrados en el sistema con el fin de detectar anomalías durante el transporte o almacenamiento de un contenedor de carga.

El sistema se compone de varios subsistemas diferentes según se aprecia en la siguiente imagen.



Cada subsistema deposita sus datos en una carpeta del sistema de archivos. Los archivos únicamente se borran del sistema cuando han sido procesados correctamente por la etapa siguiente.

4.2 Cadena Blockchain

Se desplegó una red Blockchain que captura distintos aspectos de la lógica de negocio a través de Smart Contracts, donde se almacena la información proveniente del dispositivo ciberfísico desarrollado y de otras fuentes, de manera inmutable y segura.

Dicho sistema engloba a todos los actores participantes en la cadena de transporte de productos catalogados como mercancías peligrosas. De este modo toda la información queda registrada en su totalidad, desde el almacenamiento de eventos de transporte, hasta caídas o impactos de las unidades de carga, permitiendo a su vez mejorar la trazabilidad de estos o reaccionar más ágilmente ante cualquier evento que afecte a la mercancía.

El consorcio del proyecto realizó un proceso de validación mediante pruebas en un entorno relevante que aplicó las condiciones exigidas para las mercancías peligrosas.

Este sistema está compuesto por:

- Un conjunto de dispositivos ciberfísicos, autónomos, universales e independientes capaces de obtener información fiable de las variables relevantes del proceso que acompañan a la mercancía peligrosa durante el transporte.
- Un sistema Blockchain / DLT que consta de un despliegue básico de red, junto con la política de gobernanza más adecuada, y el conjunto de aplicativos (en forma de Smart Contracts, APIs y aplicaciones externas) que incluye toda la lógica de negocio para su control, gestión y uso.

El sistema posee las siguientes características:

- Una metodología de toma de datos de los procesos de transporte involucrados.
- Un desarrollo de sistemas ciberfísicos para la supervisión de los procesos de transporte.
- Implementación de un sistema de transmisión, almacenamiento, procesado de datos y visualización de resultados.

- Desarrollo del hardware de captura y almacenamiento de datos de los elementos esenciales que conforman el ciclo de transporte, garantizando la veracidad de estos y que a su vez sean compatibles con la arquitectura de red creada.
- Diseño de la red Blockchain / DLT (basada en Ethereum Quorum o red Alastria) y definición de su gobernanza, considerando agentes que deben intervenir, información que debe ser almacenada y privacidad de la información.
- Diseño y desarrollo de los Smart Contracts, APIs y aplicaciones externas para soportar la lógica de negocio: subir y almacenar la información, consultarla y visualizarla.
- Despliegue e interconexión de todos los elementos participativos en el sistema que permita la ejecución de pruebas piloto.
- Prueba piloto del sistema construido y validación de la bondad del sistema completo en un entorno lo más cercano posible a un escenario real.

En la actualidad no existe una solución que aúne la gestión de la extensa documentación legal para este tipo de transporte, y referencie las incidencias del proceso de carga, descarga, y tránsito, con una monitorización en vivo que impediría ocultar los siniestros que son de obligada notificación por parte de la empresa y el Consejero de Seguridad.

GESTABLOCK resuelve las dificultades en la obtención de estadísticas ágiles en esta materia, al plantear una serie de herramientas que, al gestionar la trazabilidad, permiten completar la documentación legal, en forma de Smart Contracts, APIs, y aplicaciones externas, y otros datos computados por un dispositivo acoplado al transporte o sus cargas.

De esta forma, la preservación de la información queda garantizada mediante redes como Alastria o Ethereum Quorum, basadas en plataformas con arquitectura distribuida y descentralizadas de código abierto, que permiten formalizar un sistema de nodos Blockchain o de Tecnología de Registro Distribuido (Distributed Ledger Technology, DLT, por sus siglas en inglés) dando un acceso autorizado a los actores participantes.

GESTABLOCK dispone además de otra herramienta fundamental que completa este sistema único de control de mercancías peligrosas, inicialmente previsto para el transporte por carretera pero ampliable al resto de modalidades, ferroviario, aeronaves y buques.

Se trata de un dispositivo inteligente autónomo incorporado a las unidades de carga o al propio transporte que registra todos los parámetros físicos que sucedan en el trayecto mediante algoritmos de machine learning, como movimientos de carga, impactos, caídas, o posición GPS, entre otros, y que alerta de incidencias graves a los diferentes actores de la cadena de suministro.

Este servicio permite además evaluar, en un laboratorio de ensayos, la adecuación de los contenedores, envases, y embalajes, para sus ajustes y rediseños, y minimizar en caso de accidentes las roturas y los consecuentes derramamientos que pueden originar combustiones espontáneas o en contacto con el agua, entre otros factores de riesgo.

4.3 Validación del dispositivo

Un consorcio de empresas del sector validó el proyecto mediante diferentes pruebas en un entorno controlado, que aplicó las condiciones exigidas según la normativa del Acuerdo Europeo sobre el Transporte Internacional de Mercancías Peligrosas por Carretera conocido

El Instituto Tecnológico ITI lideró el proyecto Gestablock para la utilización de la tecnología Blockchain como elemento de garantía de la custodia de los documentos relacionados con el transporte de mercancías peligrosas.

El ITI trabajó en los algoritmos necesarios para desarrollar la tecnología Blockchain en este proyecto y AIDIMME trabajó en el desarrollo del hardware y software necesarios para disponer de los dispositivos físicos inalámbricos para llevar a bordo del vehículo de transporte junto a los paquetes o bultos que deben ser transportados.

5 OTRAS REFERENCIAS DE INTERÉS

Si le interesa conseguir más información sobre el transporte de mercancía peligrosa, le invitamos a explorar las siguientes referencias:

https://www.boe.es/doue/2008/260/L00013-00059.pdf
https://www.mitma.gob.es/recursos_mfom/pdf/4C02E0BA-8474-499B-9718-4F1F07FCA161/15773/RDGTC21112005.pdf
https://www.mitma.gob.es/recursos_mfom/pdf/3C509EBA-18F9-4095-B123-6C5F4ECBC91B/22177/ORDENFOM29242006.pdf
https://www.mitma.gob.es/recursos_mfom/pdf/A643F37A-69B3-4C85-AA09-63C97F497F08/123586/20140214_RD_97_Tte_Mercs_Peligrosas.pdf
https://bitcoin.org/es/como-funciona
https://www.xataka.com/criptomonedas/315-millones-euros-bitcoins-hombre-que-lleva-anos-buscando-disco-duro-vertedero-1
https://www.xataka.com/criptomonedas/220-millones-dolares-bitcoin-contrasena-perdida-dos-intentos-restantes-tragica-historia-ingeniero-aleman-para-recuperar-su-cartera-2
https://www.xataka.com/seguridad/los-creadores-del-cifrado-de-clave-publica-galardonados-con-el-prestigioso-premio-turing
https://www.xataka.com/espacioutad/criptografia-curvas-elipticas-segura-computacion-cuantica-permita

Las Oficinas Acelera pyme puestas en marcha en toda España por Red.es, entidad pública adscrita al Ministerio de Asuntos Económicos y Transformación Digital a través de la Secretaría de Estado de Digitalización e Inteligencia Artificial, cuentan con un presupuesto global de 8 millones de euros, de los cuales Red.es aportará 6,3 y las entidades beneficiarias el resto. Las actuaciones están cofinanciadas con fondos FEDER de la Unión Europea, en el marco del Programa Operativo Plurirregional de España FEDER 2014-2020 (POPE) bajo el lema “Una manera de hacer Europa”.

Contacto operativo en la Oficina Acelera pyme

Roberto Mateu Ortiz - rmateu@femeval.es // **(+34) 963719761**