(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 759 536**

(21) Número de solicitud: 201831082

(51) Int. CI.:

***H04W 4/029*** (2008.01)

(12) SOLICITUD DE PATENTE A1

(22) Fecha de presentación:

**08.11.2018**

(43) Fecha de publicación de la solicitud:

**11.05.2020**

(71) Solicitantes:

**UNIVERSIDADE DA CORUÑA (100.0%)**
**OTRI-Edificio de Servizos Centrais de Investigación Campus de Elviña**
**15071 A CORUÑA ES**

(72) Inventor/es:

**FERNÁNDEZ CARAMÉS, Tiago Manuel y**
**FRAGA LAMAS, Paula**

(74) Agente/Representante:

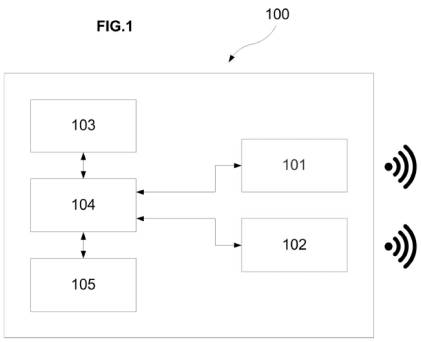
**CONTRERAS PÉREZ, Yahel**

(54) Título: **PROCEDIMIENTO, MÓDULO DE CONTROL Y PRODUCTO DE PROGRAMA DE ORDENADOR PARA CONTROLAR UN DISPOSITIVO CON MÓDULO DE GESTIÓN DE BLOCKCHAIN PARA REALIZAR LA IDENTIFICACIÓN Y EL SEGUIMIENTO DE UNA PERSONA, VEHÍCULO, PRODUCTO, SUBPRODUCTO, ACTIVO O ELEMENTO FÍSICO**

(57) Resumen:

La descripción se refiere a un procedimiento para controlar, mediante un módulo (104) de control, un dispositivo (100) para realizar la identificación y el seguimiento de al menos una persona, vehículo, producto, subproducto, activo o elemento físico, comprendiendo el dispositivo un módulo (101) de identificación pasiva, un módulo (102) de identificación activa y el módulo de control, configurado cada módulo de identificación pasiva para comunicarse con un lector (201) de identificación pasiva y configurado cada módulo de identificación activa para comunicarse con un lector (202) de identificación activa, comprendiendo el procedimiento: el módulo (104) de control, a través del módulo (101) de identificación pasiva, recibe una solicitud de identificación del lector (201) de identificación pasiva; el módulo de control activa el funcionamiento del módulo (102) de identificación activa: el módulo de control, mediante el módulo de identificación activa, lleva a cabo comunicaciones con el lector (202) de identificación activa.

FIG.1




ES 2 759 536 A1

## DESCRIPCIÓN

# Procedimiento, módulo de control y producto de programa de ordenador para controlar un dispositivo con módulo de gestión de Blockchain para realizar la identificación y el seguimiento de una persona, vehículo, producto, subproducto, activo o elemento físico

La presente descripción se refiere a un procedimiento para controlar un dispositivo para realizar la identificación y el seguimiento de una persona, vehículo, producto, subproducto, activo o elemento físico. También se refiere a un módulo de control y a un producto de programa informático adecuados para llevar a cabo el procedimiento.

ESTADO DE LA TÉCNICA ANTERIOR

En los últimos años el uso de sistemas para realizar la identificación y seguimiento de personas, productos, subproductos, activos o elementos físicos ha cobrado notable presencia debido a su utilidad en campos como la logística, el guiado de personas o la monitorización de activos dentro de la industria. Otro ejemplo de dichos campos es el transporte público, en el cual los sistemas basados en tarjetas inteligentes para transporte urbano e interurbano han experimentado un crecimiento notable en todo el mundo. El objetivo de dichos sistemas es esencialmente el ofrecer un sistema de monedero electrónico, existiendo escasos ejemplos de sistemas en los que se haya diseñado la tarjeta inteligente de manera explícita para proveer información adicional que permita optimizar el sistema de movilidad.

La mayoría de las entidades administradoras de los sistemas de tarjetas inteligentes pueden conocer determinados datos sobre los usuarios analizando sus interacciones con el sistema: la frecuencia con qué viajan, su ruta habitual o en qué momento acceden a un vehículo. Estos datos pueden ser obtenidos en tiempo diferido o en tiempo real. A pesar de ello, sería conveniente tener acceso a otros datos tales como la parada en la que se baja cada usuario, cuántas plazas disponibles/ocupadas tiene el vehículo o la ubicación exacta del medio de transporte en cada instante.

En el caso de la localización de un vehículo en exteriores, la solución más habitual consiste en utilizar sistemas GNSS (*Global Navigation Satellite System*) como el sistema

norteamericano GPS (*Global Positioning System*), el ruso GLONASS (*Global'naya Navigatsionnaya Sputnikovaya Sistema*) o el sistema europeo Galileo.

La localización de usuarios da pie a que diversas tecnologías puedan ser utilizadas.

Existen igualmente otras soluciones que no se apoyan estrictamente en la tecnología de la tarjeta de transporte, sino en otros elementos portados por los usuarios. Dichas soluciones se enmarcan en el campo de estudio denominado "identificación pasiva de flujos de personas" e incluye el uso de las tecnologías como Bluetooth, WiFi o GSM/3G/4G. En el caso de Bluetooth ha sido posible su uso para monitorizar el comportamiento de uno de los mayores flujos de personas que existen: la peregrinación a las ciudades de La Meca y Medina. En dicho evento cerca de tres millones de personas se congregan durante diversos rituales religiosos. Para controlar, estudiar e inferir el comportamiento de los peregrinos se han utilizado balizas móviles Bluetooth (portadas por peregrinos), a través de las cuales se han podido estimar los movimientos de las personas y la afluencia en los momentos críticos del evento (sobre todo durante los cinco rezos). Sistemas similares basados en Bluetooth también han sido usados para estimar con bastante precisión la afluencia en festivales de música, partidos de fútbol, la *Oktoberfest* o el *Tour de Flandes*.

Es también posible hacer uso de interfaces basadas en WiFi para realizar la identificación y seguimiento de personas, bien sea a través de la detección de la potencia de transmisión del interfaz WiFi de dispositivos que porten los usuarios (por ejemplo, teléfonos móviles o tabletas) o mediante la monitorización del tráfico de datos de los puntos de acceso WiFi.

Como se ha comentado anteriormente, en el caso de los vehículos de transporte público, además de determinar la cantidad de personas que circulan en el vehículo, es de interés localizar a los usuarios, obtener el número de plazas libres en un vehículo, determinar el número de subidas y bajadas del vehículo, y saber la identidad de dichos usuarios.

En el caso de la determinación de la ocupación del vehículo ya existen soluciones comerciales basadas en la utilización de sensores, pero el problema de estos sistemas es que no son capaces de determinar qué persona concreta sube o baja en cada instante, tan sólo contabilizan dichas acciones. En concreto, los dispositivos que contabilizan las subidas y bajadas de manera automatizada se denominan APC (*Automated Passenger Counter*) y

se han venido utilizando desde hace tiempo para complementar la información del tránsito de pasajeros, pudiendo obtener patrones de uso y determinar las acciones oportunas.

En cuanto a la determinación de qué usuario concreto sube o baja, existen sistemas que fuerzan al usuario a que pase la tarjeta inteligente tanto en las subidas como en las bajadas, pero no se tiene constancia de ningún sistema que realice tales tareas de manera completamente autónoma sin intervención del usuario y basándose exclusivamente en una tarjeta inteligente. Adicionalmente existen también sistemas basados en análisis de vídeo, pero su uso suele limitarse más al conteo de usuarios que a su seguimiento y monitorización.

La información de la identificación y seguimiento de personas, productos, subproductos, activos o elementos físicos se puede almacenar de distintas formas. El almacenamiento local (por ejemplo, discos duros) puede ser barata, pero está sujeta a problemas técnicos (por ejemplo, fallos de disco) y factores externos (por ejemplo, caídas), que pueden dañar y provocar la pérdida de los datos almacenados. Los sistemas de almacenamiento remoto (por ejemplo, cloud, NAS) proporcionan acceso remoto y redundancia, pero su gestión depende habitualmente de compañías externas no necesariamente fiables y que pueden estar expuestas a vulnerabilidades o ciber-ataques, como pueden ser ataques de denegación de servicio que afectan a la disponibilidad de los datos almacenados. En los últimos años, Blockchain, una tecnología de tipo DLT (*Distributed Ledger Technology*), ha surgido como una nueva forma de almacenar los datos (o la prueba de esos datos) de forma que puedan transferirse de forma segura y entre entidades entre las que no exista confianza. Blockchain puede considerarse bajo desarrollo en ciertos aspectos, pero algunas de sus aplicaciones donde la confianza es imprescindible (por ejemplo, finanzas) se encuentran ya en funcionamiento en entornos reales.

Como se ha comentado, la identificación y seguimiento de usuarios y ciertos objetos se ha convertido en una necesidad en múltiples aplicaciones actuales. Volviendo a las tarjetas de transporte, en los sistemas de transporte público, los sistemas basados en tarjetas inteligentes para transporte urbano e interurbano han experimentado un crecimiento notable. El objetivo fundamental de dichas tarjetas inteligentes es ofrecer un sistema de monedero electrónico, con lo que son capaces de realizar la identificación del usuario dueño de la tarjeta y realizar cierto seguimiento de éste de forma similar a como lo hacen las grandes superficies con las tarjetas de fidelización, pero las tecnologías actualmente usadas por

dichas tarjetas tienen una serie de limitaciones relevantes a la hora de realizar el seguimiento en tiempo real en muchas ubicaciones.

Los sistemas de tarjeta inteligente como los usados para transporte urbano e interurbano se clasifican en sistemas de contacto, inalámbricos e híbridos. Todos estos sistemas tienen en común que, aunque su función primaria es la de facilitar a los usuarios el pago del billete en los distintos medios de transporte, algunas tarjetas han añadido funcionalidades adicionales relacionadas con servicios turísticos (por ejemplo, acceso a museos) o ciudadanos (por ejemplo, préstamo bibliotecario, alquiler de bicicletas...).

Las tarjetas de contacto incluyen a las tradicionales tarjetas de banda magnética y las tarjetas basadas en chip. Las primeras, muy utilizadas todavía hoy en día en el sector bancario, se limitan a ofrecer un medio barato y sencillo de identificación de los usuarios ante una entidad. Sin embargo, la seguridad de dichas tarjetas es manifiestamente mejorable (i.e. su información es muy fácil de copiar), el desgaste de su banda las obliga a ser sustituidas cada cierto tiempo o número de usos, y ofrecen un número muy limitado de servicios. Debido a todo ello, las tarjetas de banda magnética están siendo sustituidas progresivamente por tarjetas basadas en chip.

La primera generación de tarjetas basadas en chip supuso un claro avance respecto a las tarjetas de banda magnética, pero siguen adoleciendo del desgaste en los cabezales, los cuales están asociados al proceso de lectura y que, tras cierto número de usos, dan lugar a fallos en las transacciones que obligan al usuario a cambiar de tarjeta.

La que puede ser considerada como segunda generación de tarjetas chip inteligentes opta por comunicaciones inalámbricas o híbridas. En el primer caso las tarjetas se comunican con un lector a una distancia corta, evitando el proceso de desgaste asociado a la lectura, y acelera dicho proceso, al no obligar al usuario a tener que sacar la tarjeta de la cartera. En el caso de las tarjetas de tipo híbrido, además de la interfaz inalámbrica se mantiene la interfaz de contacto basada en chip, con lo que cubren los servicios en los que se usen tanto lectores de contacto como inalámbricos. Existen también tarjetas híbridas que incluyen adicionalmente una banda magnética (por ejemplo, la tarjeta MOBIB usada en Bruselas), aunque el uso de esta banda se encuentra prácticamente extinguido debido a la ganancia de velocidad que ofrece el interfaz inalámbrico.

Un parámetro importante a la hora de poder monitorizar y localizar a los usuarios es la distancia a la que pueden ser leídas sus tarjetas. El avance de las tecnologías de identificación ha permitido pasar de las tarjetas de contacto a incrementar la distancia de lectura hasta varias decenas de metros. Este incremento de la distancia ha mejorado el nivel de automatización y la posibilidad de ofrecer nuevos servicios, pero conlleva un incremento en la inteligencia de la tarjeta, que debe añadir seguridad adicional para evitar lecturas o cancelaciones indeseadas.

Lo más habitual es utilizar tecnologías RFID en distintas bandas de frecuencia, las cuales ofrecen diferentes distancias de lectura:

- Banda LF (entre 120 KHz y 140 KHz): distancias de lectura muy corta (entre 1 y 5 cm).
- Banda HF (13,56 MHz): distancias de lectura corta (suele alcanzar unos 30 cm).
- Banda UHF (en Europa, alrededor de 868 MHz): distancias medias (varios metros de distancia).
- Banda SHF (generalmente, en 2,4 GHz): larga distancia (pueden alcanzar varios centenares de metros).

La inmensa mayoría de tarjetas inteligentes se sitúan en la banda de HF debido a que ofrece un buen compromiso entre distancia de lectura, seguridad y coste. Ejemplos de tarjetas de este tipo son la actual Tarxeta de Transporte Metropolitano de la Xunta de Galicia (TMG), la tarjeta Millennium del ayuntamiento de A Coruña, la tarjeta MOBIB de Bruselas, la Navigo Pass de París, la Octopus Card de Hong Kong o la Troika Card de Moscú.

A este respecto cabe mencionar que, la Unión Europea, a través de un consorcio formado por la Comisión Europea sobre tarjetas inteligentes, realizó en 2011 un estudio centrado en las posibles acciones a tomar a nivel europeo de cara a fomentar y apoyar la interoperabilidad entre los sistemas de transporte presentes y futuros a través del uso de tarjetas inteligentes. Los representantes del consorcio contactaron con gestores de sistemas de transporte de todo el mundo de cara a obtener una mejor visión del estado actual y las futuras mejoras, concluyendo que las tecnologías del futuro más inmediato pasan por una tecnología HF: NFC.

Sin embargo, las tarjetas HF, al tener una distancia de lectura tan pequeña (que se ve notablemente reducida al interponer obstáculos entre la tarjeta y el lector), dificulta la

posibilidad de monitorizar de manera automatizada el proceso de subida y bajada de los vehículos. De hecho, debido a dicha dificultad, no se tiene constancia de ningún desarrollo científico o comercial que utilice tarjetas HF para recoger de manera automatizada la información adicional citada anteriormente. Eso sí, los gestores de sistemas basados en tarjetas HF pueden optar por forzar al usuario a pasar la tarjeta por determinados puntos de lectura del autobús (típicamente a la entrada y salida), lo cual puede dar lugar al rechazo del usuario.

En cuanto a la banda SHF, aunque permite recoger información a gran distancia, tiene el inconveniente de que en la gran mayoría de los casos suele requerir de baterías para alimentar la tarjeta inteligente. Dichas baterías pueden tener una duración de unos pocos años y suelen ser bastante más voluminosas que las tarjetas inteligentes más habituales.

La banda de frecuencia en donde se están moviendo las últimas investigaciones es la de UHF, aunque apenas existen ejemplos de desarrollos.

En todo caso, cabe destacar que las tarjetas inteligentes con interfaz inalámbrico mejoran notablemente la robustez respecto a la versión de contacto, pero, si no son encapsuladas correctamente, son susceptibles a deteriorarse con el uso: si la unión entre el chip y la antena se corta debido a golpes o a el acto de doblar la tarjeta, ésta comenzará a fallar y, en último caso deberá ser sustituida.

Por otro lado, la mayor parte de tarjetas inteligentes usadas por sistemas de transporte público han sido diseñadas como meros monederos electrónicos utilizados para pagar el billete. Por ejemplo, en el caso de la tarjeta MOBIB belga, ésta vale para pagar el metro, los tranvías y los autobuses. Tras la implantación de la tarjeta en Bruselas se le añadió otra funcionalidad adicional: el acceso al sistema de vehículos compartidos de la compañía Cambio.

El resto de las tarjetas inteligentes también ha añadido servicios al monedero de transporte básico. Por ejemplo, en París, la tarjeta Navigo Pass permite alquilar bicicletas del sistema Vélib', el pago de trenes Thalys y el uso de ciertas zonas de aparcamiento.

Probablemente el caso más extremo en el que una tarjeta inicialmente concebida como monedero de transporte se ha generalizado en múltiples ámbitos ha sido la Octopus Card en

Hong Kong. Dicha tarjeta permite pagar en tiendas, supermercados, restaurantes, parquímetros, parkings públicos, máquinas de vending, puntos de venta con un TPV Octopus e incluso es utilizada en escuelas para préstamo de libros o para controlar la asistencia a clase de los estudiantes.

Sin embargo, debido a que la gran mayoría de las tarjetas inteligentes de transporte han sido concebidas como monederos, apenas se encuentran ejemplos de tarjetas diseñadas explícitamente para facilitar la adquisición de datos relacionados con el flujo de pasajeros en flotas de transporte público o en eventos donde dicho flujo sea de interés.

Es también relevante destacar la importancia de la privacidad y seguridad en este tipo de dispositivos: su proliferación ha conllevado numerosas ventajas al ofrecer la posibilidad de procesar mayor información pero diversos colectivos han denunciado que determinadas tarjetas permiten obtener datos presuntamente anónimos.

Por ejemplo, en Bélgica dos organizaciones de derechos ciudadanos denunciaron que la tarjeta que gestiona la compañía de transportes de Bruselas (tarjeta MOBIB) vulneraba el derecho a la privacidad de los ciudadanos que se encuentra regulada en dicho país por una ley de 1992. A pesar de que la compañía aseguraba que la tarjeta cumple con la legalidad, investigadores de la Universidad Católica de Louvain demostraron que la tarjeta puede ser leída por cualquier persona a distancias relativamente cercanas pudiendo obtenerse datos personales (tales como nombre y apellidos, año de nacimiento o código postal) y la traza de los últimos viajes realizados. En 2013 un usuario denunció a la empresa de transportes por esta vulneración de privacidad (al final la empresa llegó a un acuerdo económico extra-judicial para evitar tener que exponer el funcionamiento interno de MOBIB).

En Francia, la tarjeta Navigo Pass sufrió una situación similar en la que tuvo que intervenir el Comité Nacional para la Informática y las Libertades, provocando que la empresa de transportes parisina crease una versión anónima de la tarjeta ("Navigo Découverte") que, aunque ha recibido ciertas críticas por su sistema de adquisición no anónimo, garantiza en gran medida el anonimato del usuario al desvincularlo de cualquier dato que posea la compañía.

Un informe presentado por un consorcio formado por la Comisión Europea indicaba que las entidades administradoras de sistemas basados en tarjetas inteligentes pueden actualmente

monitorizar el comportamiento de los pasajeros y que, aunque su uso puede ayudar a mejorar la movilidad y ser aplicado a estrategias de marketing, dichos administradores deben proteger la privacidad y los datos personales de los usuarios. Dicho consorcio destacó que la legislación de protección de datos está generalmente regulada por los distintos países de la Unión y que difiere en gran medida de un lugar a otro debido a la amplia variedad social, cultural, económica y legal de los territorios. Sin embargo, los principios generales que regulan este aspecto son comunes y son proveídos por regulaciones como la Data Protection Directive de la Unión Europea, el APEC Privacy Framework y las guías de 1980 de la OCDE (Organización para la Cooperación y el Desarrollo Económico) sobre la protección de la privacidad y los datos personajes en flujos migratorios transfronterizos.

Respecto a la seguridad en sí, en los últimos años han surgidos diferentes polémicas relacionadas con la debilidad de los sistemas de seguridad de los sistemas de identificación de basados en tarjetas. El caso que probablemente haya tenido mayor impacto fue el acceso y manipulación de las tarjetas MIFARE Classic que controlaban los sistemas de transporte de Londres (Oyster Card), de los Países Bajos (OV-chipkaart), del condado de Miami-Dade en Estados Unidos (Easy Card), de Estambul (Istambulkart) o de Buenos Aires (tarjeta SUBE). En todos estos casos era posible clonar tarjetas, obtener los datos privados de otros usuarios y alterar el crédito disponible.

De todas formas, hay otros sistemas que, a pesar de ser utilizados de manera masiva, declaran no haber tenido ningún problema de seguridad gracias a un buen diseño. Por ejemplo, la Octopus Card presume de ser un sistema que, a pesar de ser usado masivamente en Hong Kong (por el 95% de la población entre 16 y 65 años), su seguridad no ha sido nunca amenazada. Para ello la tarjeta lleva a cabo un proceso de autenticación de triple pase con el lector basado en el estándard ISO 9798-2. De esta manera, las comunicaciones de datos sólo se establecen cuando la tarjeta y el lector están perfectamente autenticados. La única forma de alterar los datos de la tarjeta que se conoce a día de hoy sería mediante el uso no autorizado del software y un lector oficial Octopus.

En consecuencia, hay una necesidad de un dispositivo que resuelva al menos parcialmente los problemas mencionados anteriormente.

EXPLICACIÓN DE LA INVENCIÓN

En un primer aspecto, se proporciona un procedimiento para controlar, mediante un módulo de control, un dispositivo para realizar la identificación y el seguimiento de al menos una persona, vehículo, producto, subproducto, activo o elemento físico. El dispositivo puede comprender al menos un módulo de identificación pasiva, al menos un módulo de identificación activa y el módulo de control. Cada módulo de identificación pasiva puede estar configurado para comunicarse con al menos un lector de identificación pasiva de un sistema externo. Cada módulo de identificación activa puede estar configurado para comunicarse con al menos un lector de identificación activa del sistema externo. El procedimiento puede comprender:

- el módulo de control, a través del módulo de identificación pasiva, recibe una solicitud de identificación por parte del lector de identificación pasiva del sistema externo;
- el módulo de control, tras recibir la solicitud de identificación, activa el funcionamiento del módulo de identificación activa;
- el módulo de control, mediante el módulo de identificación activa, lleva a cabo comunicaciones con el lector de identificación activa del sistema externo, para realizar la identificación y el seguimiento de la persona, vehículo, producto, subproducto, activo o elemento físico.

De este modo, se consigue un procedimiento que permite obtener de manera automática datos de identificación y seguimiento de una persona, vehículo, producto, subproducto, activo o elemento físico y enviarlos a un sistema de gestión, para hacerlos accesibles a un tercero. Esta gestión puede estar relacionada simplemente con proporcionar información al propio usuario o proporcionar información a un tercero responsable o que tiene relación con la persona, vehículo, producto, subproducto, activo o elemento físico. Por ejemplo, es posible controlar el movimiento de un menor que se mueve en transporte público, conociendo los tiempos en los que sube (cuando valida su tarjeta de transporte) y baja del transporte (cuando se pierde la comunicación entre el módulo de identificación activa del dispositivo (en este caso en forma de tarjeta de transporte) y el lector de identificación activa presente en el vehículo de transporte), la localización en la que sube y/o baja del vehículo de transporte, así como información asociada con el propio vehículo de transporte, tal como el número de plazas ocupadas o disponibles o la localización exacta de vehículo de transporte en cada instante.

De acuerdo con algunos ejemplos, el procedimiento puede comprender:

- el módulo de control envía datos de identificación y seguimiento de la persona, vehículo, producto, subproducto, activo o elemento físico generados en las comunicaciones entre el módulo de identificación activa y el lector de identificación activa, a un sistema de gestión.

Además, este sistema de gestión puede permitir la configuración remota y la gestión de los diferentes dispositivos desplegados.

En cualquier caso, el sistema de gestión puede ser, por ejemplo, un servidor remoto que ejecute al menos un back-end, un front-end y una base de datos. El back-end puede encargarse de la recolección de los datos recibidos sobre la identificación y el seguimiento de los múltiples dispositivos desplegados en los escenarios monitorizados. El front-end puede facilitar la interacción de los usuarios remotos para realizar tareas de gestión y para la visualización de los datos recibidos. El repositorio o base de datos puede almacenar los datos recolectados y la información requerida para llevar a cabo la configuración y monitorización de los dispositivos.

El envío al sistema de gestión de los datos de identificación y seguimiento de la persona, vehículo, producto, subproducto, activo o elemento físico puede realizarse a través del módulo de identificación activa del dispositivo. Complementaria o alternativamente, el dispositivo puede comprender un módulo de comunicaciones, de manera que el envío al sistema de gestión de los datos de identificación y seguimiento de la persona, vehículo, producto, subproducto, activo o elemento físico puede realizarse mediante este módulo de comunicaciones.

Básicamente, el envío de los datos de identificación y seguimiento de la persona, vehículo, producto, subproducto, activo o elemento físico puede realizarse a través del módulo de identificación pasiva/activa del dispositivo y del lector de identificación pasiva/activa del sistema externo. Este último, mediante un módulo de comunicación, ya sea de largo o corto alcance, puede mandar los datos al sistema de gestión. También es posible, si el dispositivo presenta un módulo de comunicaciones propio, que los datos sean enviados directamente al sistema de gestión, sin pasar por ningún módulo o lector.

Por otro lado, el dispositivo puede comprender un módulo de gestión de Blockchain. El procedimiento puede comprender:

- el módulo de control, mediante el módulo de gestión de Blockchain, sube (descarga o intercambia) datos de identificación y seguimiento de la persona, vehículo, producto, subproducto, activo o elemento físico generados en las comunicaciones entre el módulo de identificación activa y el lector de identificación activa, a una Blockchain.

Esta subida (descarga o intercambio) a la Blockchain de los datos de identificación y seguimiento de la persona, vehículo, producto, subproducto, activo o elemento físico puede realizarse a través del módulo de identificación activa del dispositivo y/o, en el caso de que el dispositivo comprenda un módulo de comunicaciones, la subida a la Blockchain puede realizarse mediante este módulo de comunicaciones.

A pesar de que el dispositivo es capaz de almacenar los datos relevantes localmente (por ejemplo, en una memoria EEPROM), los datos también pueden subirse a una Blockchain para almacenarlos de forma más segura. El experto en la materia entenderá que también es posible hacer uso de otras tecnologías similares a Blockchain de tipo distribuido (DLT, *Distributed Ledger Technology*), como puede ser DAG (*Directed-Acyclic Graph*).

El dispositivo, además de interactuar con una Blockchain, también puede participar en Smart Contracts, entendidos como código descentralizado autosuficiente que se ejecuta de manera autónoma cuando se cumplen ciertas condiciones de un proceso de negocio.

Según unos ejemplos, el procedimiento puede comprender:

- el módulo de control detiene el funcionamiento del módulo de identificación activa tras transcurrir un tiempo predeterminado sin que se hayan mantenido comunicaciones con algún lector de identificación activa del sistema externo.

De acuerdo con unos ejemplos, el procedimiento puede comprender:

- el módulo de control mantiene al dispositivo en estado apagado o de bajo consumo hasta recibir, a través del módulo de identificación pasiva, una solicitud de identificación por parte del lector de identificación pasiva del sistema externo.

De este modo, con el objetivo de minimizar el consumo del dispositivo, el módulo de control puede configurar el módulo de identificación activa para que permanezca la mayor parte del

tiempo apagado o en modo de bajo consumo. Debido a que el dispositivo puede llegar a mandar datos con una periodicidad muy baja, la mayoría del hardware del dispositivo debe permanecer en un estado de ultra-bajo consumo hasta que se precise activar el módulo de identificación activa para adquirir y/o enviar datos. La tasa de refresco no se considera crítica, pudiendo ser de minutos o incluso de horas en determinados escenarios de aplicación.

Adicionalmente, el dispositivo puede comprender un módulo de señalización. El procedimiento puede comprender:

- El módulo de control, mediante el módulo de señalización, señaliza la persona, vehículo, producto, subproducto, activo o elemento físico.

El módulo de señalización puede tener un doble objetivo. Por un lado, permite señalizar la localización de la persona que porta el dispositivo, o la localización del vehículo, producto, subproducto, activo o elemento físico al que está asociado el dispositivo, ya sea de manera sonora, visual o háptica. Por otro lado, el módulo de señalización también puede ser usado para proporcionar información a un usuario. Así, por ejemplo, el módulo puede comprender una pluralidad de diodos emisores de luz, también conocidos como LEDs, que utiliza para codificar determinada información (por ejemplo, el envío de datos al sistema de gestión, la falta de batería, etc.) mediante un código de colores.

De acuerdo con un segundo aspecto, se proporciona un programa informático. Este programa informático puede comprender instrucciones de programa para provocar que un módulo de control realice o ejecute un procedimiento para controlar un dispositivo para realizar la identificación y el seguimiento de al menos una persona, vehículo, producto, subproducto, activo o elemento físico, tal como el descrito anteriormente. El programa informático puede estar almacenado en unos medios de almacenamiento físico, tales como unos medios de grabación, una memoria de ordenador, o una memoria de sólo lectura, o puede ser portado por una onda portadora, tal como eléctrica u óptica.

De acuerdo con un tercer aspecto, se proporciona un módulo de control de un dispositivo para realizar la identificación y el seguimiento de una persona, vehículo, producto, subproducto, activo o elemento físico. El dispositivo puede comprender al menos un módulo de identificación pasiva, al menos un módulo de identificación activa y el módulo de control. Cada módulo de identificación pasiva puede estar configurado para comunicarse con al

menos un lector de identificación pasiva de un sistema externo. Cada módulo de identificación activa puede estar configurado para comunicarse con al menos un lector de identificación activa del sistema externo. El módulo de control puede comprender:

- medios para, a través del módulo de identificación pasiva, recibir una solicitud de identificación por parte del lector de identificación pasiva del sistema externo;
- medios para, tras recibir la solicitud de identificación, activar el funcionamiento del módulo de identificación activa;
- medios para, mediante el módulo de identificación activa, llevar a cabo comunicaciones con el lector de identificación activa del sistema externo, para realizar la identificación y el seguimiento de la persona, vehículo, producto, subproducto, activo o elemento físico.

De acuerdo con otro aspecto, se proporciona un módulo de control de un dispositivo para realizar la identificación y el seguimiento de una persona, vehículo, producto, subproducto, activo o elemento físico. El módulo de control puede comprender una memoria y un procesador, en el que la memoria almacena instrucciones de programa informático ejecutables por el procesador, comprendiendo estas instrucciones funcionalidades para ejecutar un procedimiento para controlar un dispositivo para realizar la identificación y el seguimiento de al menos una persona, vehículo, producto, subproducto, activo o elemento físico, tal como el descrito anteriormente.

Según otro aspecto, se proporciona un módulo de control de un dispositivo para realizar la identificación y el seguimiento de una persona, vehículo, producto, subproducto, activo o elemento físico. El dispositivo puede comprender al menos un módulo de identificación pasiva, al menos un módulo de identificación activa y el módulo de control. Cada módulo de identificación pasiva puede estar configurado para comunicarse con al menos un lector de identificación pasiva de un sistema externo. Cada módulo de módulo de identificación activa puede estar configurado para comunicarse con al menos un lector de identificación activa del sistema externo. El módulo de control puede estar configurado para:

- recibir, a través del módulo de identificación pasiva, una solicitud de identificación por parte del lector de identificación pasiva del sistema externo;
- activar el funcionamiento del módulo de identificación activa, tras recibir la solicitud de identificación;

- llevar a cabo, mediante el módulo de identificación activa, comunicaciones con el lector de identificación activa del sistema externo, para realizar la identificación y el seguimiento de la persona, vehículo, producto, subproducto, activo o elemento físico.

De acuerdo con aún otro aspecto, se proporciona un dispositivo para realizar la identificación y el seguimiento de una persona, vehículo, producto, subproducto, activo o elemento físico. El dispositivo puede comprender un módulo de identificación pasiva, un módulo de identificación activa y un módulo de control tal como el anteriormente descrito.

De acuerdo con unos ejemplos, el dispositivo puede ser un dispositivo móvil, tal como un teléfono inteligente o una tableta. En este caso, el módulo de identificación pasiva puede ser implementado por, por ejemplo, un tag NFC, mientras que el módulo de identificación activa puede implementarse mediante Bluetooth o Wifi.

Según unos ejemplos, el dispositivo puede comprender un módulo de gestión de Blockchain configurado para gestionar intercambios de datos de identificación y seguimiento obtenidos en las comunicaciones entre el módulo de identificación activa y el lector de identificación activa, con una Blockchain.

Por otro lado, el dispositivo puede comprender un módulo de alimentación configurado para proporcionar energía a diferentes módulos del dispositivo. El módulo de alimentación, dado que el dispositivo es portable, puede comprender como fuente principal de alimentación baterías embebidas, aunque también puede permitir la inclusión de fuentes de energía alternativas, por ejemplo, obtenida mediante técnicas de recolección de energía (en inglés, “*energy harvesting*”).

De acuerdo con unos ejemplos, el dispositivo puede comprender un módulo de señalización. El módulo de señalización puede comprender al menos uno de los siguientes elementos de señalización: un elemento de señalización configurado para generar una señal audible (por ejemplo, un altavoz, un timbre o un zumbador), un elemento de señalización configurado para generar una señal visual (por ejemplo, una pantalla de visualización, tal como LCD, OLED, etc., o una pluralidad de LEDs), o un elemento de señalización configurado para generar una señal háptica (por ejemplo, un motor vibrador).

Además, el dispositivo puede comprende un encapsulado o carcasa. El encapsulado puede tener forma de al menos uno de los siguientes elementos: un tarjeta inteligente (por ejemplo, una tarjeta bancaria, de transporte o similar); una pulsera; un reloj; una funda; o textil. El encapsulado o tarjeta puede permitir que el dispositivo sea portado con facilidad por un usuario o que sea añadido o acoplado con facilidad a cualquier producto, subproducto, activo o elemento físico, con un funcionamiento totalmente inalámbrico.

De acuerdo con otro aspecto, se proporciona un sistema para realizar la identificación y el seguimiento de una persona, vehículo, producto, subproducto, activo o elemento físico. El sistema puede comprender un dispositivo, tal como el descrito anteriormente; un sistema externo que puede comprender un lector de identificación pasiva configurado para comunicarse con el módulo de identificación pasiva del dispositivo y un lector de identificación activa configurado para comunicarse con el módulo de identificación activa del dispositivo.

El lector de identificación activa puede estar configurado para comunicarse con un sistema de gestión para intercambiar datos de identificación y seguimiento de la persona, vehículo, producto, subproducto, activo o elemento físico. Los datos pueden haber sido generados en las comunicaciones entre el módulo de identificación activa del dispositivo y el lector de identificación activa del sistema externo.

Según unos ejemplos, el dispositivo puede comprender un módulo de gestión de Blockchain configurado para gestionar intercambios de datos de identificación y seguimiento de la persona, vehículo, producto, subproducto, activo o elemento físico, a través del módulo de identificación activa y del lector de identificación activa, con una Blockchain. Estos datos pueden haber sido generados en las comunicaciones entre el módulo de identificación activa del dispositivo y el lector de identificación activa del sistema externo.

De acuerdo con algunos ejemplos, el sistema externo puede comprender un módulo de gestión de Blockchain configurado para gestionar intercambios de datos de identificación y seguimiento de la persona, vehículo, producto, subproducto, activo o elemento físico generados en las comunicaciones entre el módulo de identificación activa del dispositivo y el lector de identificación activa del sistema externo.

Por otro lado, el sistema externo puede comprende un módulo de gestión de Blockchain configurado para gestionar intercambios de datos de identificación y seguimiento de la persona, vehículo, producto, subproducto, activo o elemento físico generados en las comunicaciones entre el módulo de identificación pasiva del dispositivo y el lector de identificación activa del sistema externo.

La presencia de este módulo de gestión de Blockchain en el sistema externo puede producirse cuando el dispositivo no es lo suficientemente potente o no tiene los recursos computacionales suficientes para soportar el módulo de gestión de Blockchain. De este modo, tanto el lector de identificación pasiva como el lector de identificación activa pueden estar conectados al módulo de gestión de Blockchain del sistema externo, de manera que es posible el envío a una Blockchain de los datos generados en las comunicaciones entre el módulo de identificación pasiva y el lector de identificación pasiva, y entre el módulo de identificación activa y el lector de identificación activa (o el envío de información derivada del procesado de estos datos).

Otros objetos, ventajas y características de realizaciones de la invención se pondrán de manifiesto para el experto en la materia a partir de la descripción, o se pueden aprender con la práctica de la invención.

## BREVE DESCRIPCIÓN DE LOS DIBUJOS

A continuación, se describirán realizaciones particulares de la presente invención a título de ejemplo no limitativo, con referencia a los dibujos adjuntos, en los cuales:

La Figura 1 muestra un diagrama de bloques de un dispositivo para realizar la identificación y el seguimiento de una persona, vehículo, producto, subproducto, activo o elemento físico, de acuerdo con algunos ejemplos;

La Figura 2 muestra un diagrama de bloques de un sistema para realizar la identificación y el seguimiento de una persona, vehículo, producto, subproducto, activo o elemento físico, del que podría formar parte el dispositivo de la Figura 1.

## EXPOSICIÓN DETALLADA DE MODOS DE REALIZACIÓN

Como puede verse en la Figura 1, un dispositivo 100 para realizar la identificación y el seguimiento de una persona, vehículo, producto, subproducto, activo o elemento físico puede comprender, por ejemplo, los siguientes módulos:

- un módulo 101 de identificación pasiva configurado para comunicarse con un lector 201 de identificación pasiva de un sistema externo (ver Figura 2);
- un módulo 102 de identificación activa configurado para comunicarse con un lector 202 de identificación activa del sistema externo (ver Figura 2);
- un módulo 104 de control configurado para controlar al menos el módulo de identificación pasiva y el módulo de identificación activa, así como el flujo de datos de identificación y seguimiento generados a partir de estas comunicaciones.

La arquitectura de la invención permite la utilización de varias tecnologías de identificación, tanto activas como pasivas, en función del entorno de aplicación. Algunas de las tecnologías potencialmente utilizables por el dispositivo 100, podrían ser:

- Ejemplos de tecnologías pasivas:
  - Códigos de barra. Es un sistema de codificación basado en la representación de un conjunto de líneas paralelas de distinto grosor y espaciado que, en su conjunto contienen una determinada información. Los lectores de códigos de barras son equipos que traducen impulsos ópticos en eléctricos, por ello es imprescindible colocar el código de forma que se consiga buena visibilidad y legibilidad, por ejemplo, con un buen contraste de colores (negro sobre blanco es lo más común). La distancia de lectura habitual es de decenas de centímetros, aunque hay equipo especializado que puede llegar a varios metros. La correspondencia (o "*mapping*") entre caracteres y barras se denomina simbología. La especificación de dicha simbología implica definir la codificación de los caracteres del mensaje, así como las marcas de principio, fin y espacio intermedio. Pueden clasificarse atendiendo a dos propiedades:
    - Continua vs Discreta. En una simbología discreta n caracteres ocupan n barras y n-1 espacios. En una simbología continua n caracteres ocupan n barras y n espacios, donde un carácter termina con un espacio y el inicio del siguiente carácter.
    - Bidimensional vs Multidimensional. En una simbología bidimensional existen las barras anchas y estrechas, mientras que en una multidimensional los anchos de barra son múltiplos de una anchura determinada.

- Códigos QR. Código de barras bidimensional, diseñado originalmente para la industria del automóvil japonesa, que tiene mayor capacidad que los códigos lineales y que usa 4 modos de codificación (numérico, alfanumérico, binario y kanji). El código consta de cuadros negros distribuidos a través de una cuadrícula con fondo blanco que puede ser leído por un dispositivo óptico. Los cuadros grandes situados en las esquinas permiten detectar la posición del código, existiendo un cuarto para la alineación y orientación. Los lectores de códigos QR usan un sensor de imágenes digital de dos dimensiones, el cual contiene un procesador que busca los cuadros de las esquinas y luego el cuarto cuadro se usa para normalizar el tamaño de la imagen, la orientación y el ángulo de visión. A partir de ahí los cuadros más pequeños se transforman en binario y se valida con un algoritmo corrector de errores. La distancia de lectura depende del tamaño del código, de forma que a medida que se aumente la distancia de lectura el tamaño del código debe aumentar en proporción (tamaño del código = distancia de escaneo/10). Según esta norma un código que vaya a leerse a unos 20 metros debería tener 2 metros de tamaño. El almacenamiento posible en un QR depende del tipo de datos usado, la versión (de 1 a 40 indicando la dimensión de los símbolos) y el nivel de corrección de errores (*Low, Medium, Quartile, High*).
- Tecnologías RFID (*Radio Frequency Identification*) pasivas. Sistemas de comunicación inalámbrica que utilizan ondas de radio para identificar objetos. Un sistema RFID se compone de lectores (transceptores) y etiquetas (tags, transpondedores). Dichas etiquetas son componentes de muy bajo consumo que reaccionan a las ondas de radio emitidas por los lectores, proporcionando la información almacenada. De hecho, un sistema RFID se denomina “pasivo” cuando toda la energía de la que hace uso la rectifica a partir de las ondas electromagnéticas emitidas por un lector RFID remoto inalámbrico, con lo que una etiqueta RFID pasiva no hace uso de baterías para llevar a cabo las comunicaciones con un lector. En función de la frecuencia, los sistemas RFID pueden clasificarse a su vez en función de la longitud de onda que utilizan, diferenciándose principalmente entre:
    - LF (entre 120 KHz y 140 KHz). Ofrecen distancias de lectura muy corta (entre 1 y 5 cm). Pueden usarse para comunicaciones en entornos desfavorables (presencia de metales y líquidos) debido a la mayor longitud de onda. Presentan una velocidad de lectura bastante baja y no son recomendables para entornos en los cuales hay muchas etiquetas en un espacio reducido.

- HF (13,56 MHz). Permite distancias de lectura cortas (suele alcanzar unos 30 cm). Presenta mayores interferencias en entornos desfavorables que LF, pero permite un rango de lectura mayor, una velocidad de transmisión mayor y espacio para más información.
- UHF (en Europa, alrededor de 868 MHz). Ofrece distancias de lectura medias (varios metros de distancia). Presenta mayor rendimiento, tanto en velocidad de transmisión como distancia, con respecto a LF y HF. Sin embargo, los sistemas RFID UHF suelen consumir más potencia, son más sensibles a entornos desfavorables y en general almacenan menos información que las etiquetas HF.
- SHF (generalmente, en 2,4 GHz). Ofrecen comunicaciones consideradas como de larga distancia (pueden alcanzar centenares de metros). Las etiquetas llevan una batería incluida (aunque no sean considerados como dispositivos activos) y puede ser necesario añadir una alimentación local. Presentan grandes problemas ante entornos desfavorables (metales, líquidos, personas) y, en general, la propagación es muy directiva.
- NFC. Tecnología que evoluciona de RFID y que está pensada para comunicar dispositivos que se encuentren a poca distancia. Existen dispositivos NFC pasivos (*tags*) y activos (teléfonos inteligentes, por ejemplo). Los activos usan la inducción para generar un campo magnético que alimenta la circuitería de los pasivos, de forma que se codifica y emite la información. NFC opera en la frecuencia de 13,56 MHz, con una potencia que permite comunicar elementos que estén a menos de 20cm.

- Ejemplos de tecnologías activas:
  - Tecnologías RFID activas. Prácticamente idénticas a las pasivas, pero hacen uso de baterías para llevar cabo las comunicaciones.
  - Bluetooth y sus variantes (BLE, Bluetooth 5.0). Se trata de una tecnología WPAN (Wireless Personal Area Network), es decir, orientada a aplicaciones de corto alcance (entre 10 y 100 metros) y pequeños dispositivos. Utiliza la banda de 2,4 GHz, usando 79 canales de 1 MHz. La tecnología Bluetooth no ha sido diseñada para una aplicación concreta: define una serie de perfiles que representan una solución por defecto para un uso concreto y establecen los requisitos para la interoperación entre dispositivos. Cada dispositivo Bluetooth puede soportar uno o más de estos perfiles, siendo los más comunes los que permiten establecer enlaces

entre dispositivos y el envío de datos entre ellos. Entre esos dispositivos se encuentran los *beacons* (balizas), pequeños objetos que emiten información periódica (por ejemplo, un identificador único) con el objetivo de poder ser localizados en el espacio de forma que sirvan de referencia en un escenario de localización de objetos en interiores.

- WiFi (IEEE 802.11 b/g/n/ac). Tecnología inalámbrica para redes de área local (WLAN) que permite la interconexión de dispositivos y que utiliza las bandas de frecuencia de 2,4 GHz y 5 GHz. Los dispositivos (PCs, móviles, tabletas, etc.) se conectan a la red a través de puntos de acceso, que tienen un rango en torno a los 20 m en interiores y de entre 100 y 200 metros en exteriores.
- Infrarrojos. La radiación infrarroja es un tipo de radiación electromagnética y térmica, de menor frecuencia que la luz visible y no sensible por el ojo humano. Los transceptores de infrarrojos son dispositivos opto-electrónicos capaces de medir dicha radiación de los cuerpos presentes en su campo de visión (es decir, requiere de línea de visión directa entre el lector y el objeto).
- Ultra-Wide Band (UWB). Tecnología de radio de corto alcance que permite la transmisión de grandes cantidades de información sobre un amplio espectro de frecuencias, consiguiendo una densidad de potencia muy baja y pulsos de duración muy corta.
- Ultrasonidos. Transmiten ondas de sonido (mecánicas) cuya frecuencia está por encima del umbral de audición del oído humano. Los transceptores de ultrasonidos son dispositivos capaces de convertir las señales de sonido a señales eléctricas y a la inversa.
- Otras tecnologías potencialmente utilizables por la invención como solución activa serían ZigBee, Dash7, ANT+, Z-Wave, WirelessHART, LoRA, LoRAWAN, SigFox, Weightless, Ingenu o RuBee.

Por consiguiente, el módulo 101 de identificación pasiva puede estar basado en tecnologías pasivas tales como códigos de barra, códigos QR, RFID pasivo o NFC. En todo caso, esta misma tecnología sería empleada por al menos un lector de identificación pasiva 201 (ver Figura 2).

El módulo 102 de identificación activa puede hacer uso de tecnologías tales como RFID, Bluetooth, WiFi, infrarrojos, UWB, ultrasonidos, ZigBee, Dash7, ANT+, Z-Wave, WirelessHART, LoRA, LoRAWAN, SigFox, Weightless, Ingenu o RuBee. La elección de

dicha tecnología es altamente dependiente del escenario, existiendo tecnologías de corta distancia (por ejemplo, ANT+), media distancia (por ejemplo, Bluetooth) y larga distancia (por ejemplo, LoRA, SigFox). Igualmente, el consumo de cada tecnología varía notablemente de una a otra, siendo las más adecuadas las de menor consumo (y, por tanto, menor tamaño de batería y menor tamaño físico del dispositivo). En todo caso, las mismas tecnologías pueden ser utilizadas por cada lector de identificación activa 202 (ver Figura 2).

Con respecto al módulo 104 de control, puede implementarse con una configuración totalmente informática, totalmente electrónica o mediante una combinación de ambos.

En el caso de que el módulo 104 de control sea puramente informático, el módulo puede comprender una memoria y un procesador (por ejemplo, un microprocesador), en el que la memoria almacena instrucciones de programa informático ejecutables por el procesador, comprendiendo estas instrucciones funcionalidades para ejecutar un procedimiento para controlar el dispositivo 100, cuyo procedimiento será descrito más adelante.

La memoria descrita puede estar comprendida en el procesador o puede ser externa. En el caso de que sea externa, puede ser, por ejemplo, unos medios de almacenamiento de datos tales como discos magnéticos (por ejemplo, discos duros), discos ópticos (por ejemplo, DVD o CD), tarjetas de memoria, memorias flash (por ejemplo, pendrives) o unidades de estado sólido (SSD basadas en RAM, basadas en flash, etc.). Por otro lado, estos medios de almacenamiento pueden formar parte del propio dispositivo 100 y/o pueden estar dispuestos remotos al mismo, conectados alámbrica o inalámbricamente. En el caso de estar dispuestos remotos, la comunicación establecida entre el dispositivo 100 y los medios de almacenamiento puede asegurarse mediante, por ejemplo, nombre de usuario/contraseña, claves criptográficas y/o mediante un túnel SSL establecido en la comunicación entre el dispositivo 100 y los medios de almacenamiento.

Por lo tanto, el conjunto de instrucciones de programa informático ejecutables por el procesador (tal como un programa informático) puede estar almacenado en unos medios de almacenamiento físico, tales como los citados, pero también puede ser portado por una onda portadora (el medio portador puede ser cualquier entidad o dispositivo capaz de portar el programa), tal como eléctrica u óptica, que puede transmitirse vía cable eléctrico u óptico o mediante radio u otros medios. De este modo, cuando el programa informático está contenido en una señal que puede transmitirse directamente mediante un cable u otro

dispositivo o medio, el medio portador puede estar constituido por dicho cable u otro dispositivo o medio.

Alternativamente, el medio portador puede ser un circuito integrado en el que está encapsulado (*embedded*) el programa informático, estando adaptado dicho circuito integrado para realizar o para usarse en la realización de los procedimientos relevantes.

El programa informático puede estar en forma de código fuente, de código objeto o en un código intermedio entre código fuente y código objeto, tal como en forma parcialmente compilada, o en cualquier otra forma adecuada para usar en la implementación de los procedimientos descritos.

Con respecto al procesador, puede ser, por ejemplo, un microprocesador, tal como un STM32F107VC de la empresa *ST Microelectronics*. Este microprocesador contiene un núcleo ARM Cortex M3 a 72 MHz y viene acompañado de una pequeña memoria EEPROM (es decir, la memoria descrita anteriormente es interna y se corresponde con el modelo M24512, también de la empresa *ST Microelectronics*), que permite almacenar datos y que permite también actualizar el firmware del microcontrolador desde, por ejemplo, un ordenador personal, preferiblemente a través de un puerto USB o mini USB. La capacidad de esta memoria es de 512 Kbytes y puede comunicarse mediante líneas de comunicación I2C con el microcontrolador.

Adicionalmente, puede montarse un circuito integrado para proteger el microcontrolador contra posibles descargas electrostáticas.

El firmware del microcontrolador puede definirse como el software que gobierna el comportamiento del módulo de control, es decir, se corresponde con el conjunto de instrucciones de programa informático descrito con anterioridad.

El hardware directamente asociado a este microcontrolador puede constar al menos de un cristal de cuarzo, por ejemplo, de 25 MHz, necesario para generar la señal de reloj del microcontrolador, un conector JTAG (*Joint Test Action Group*, norma IEEE 1149.1-1990) para implementar tareas de programación y depuración, y todo un conjunto de condensadores de desacoplamiento necesarios para reducir los niveles de ruido de conmutación.

El hardware asociado a la memoria EEPROM consta únicamente de dos resistencias de polarización para elevar la tensión de las líneas de comunicación I2C, que van directamente conectadas al microcontrolador.

Por otro lado, el módulo 104 de control puede tener una configuración puramente electrónica, por lo que podría estar formado por un dispositivo electrónico programable tal como un CPLD (*Complex Programmable Logic Device*), un FPGA (*Field Programmable Gate Array*) o un ASIC (*Application-Specific Integrated Circuit*).

A partir de lo descrito, el módulo 104 de control puede hacer uso de distintos tipos de circuitos integrados, como CPUs (Central Processing Units), microcontroladores, FPGAs (Field-Programmable Gate Arrays), CPLDs (Complex Programmable Logic Devices), ASICs (Application-Specific Integrated Circuits), SoCs (System-on-Chips) o PSoCS (Programmable SoCs). Una CPU suele ser flexible y potente, pero su consumo no suele ser adecuado para un dispositivo móvil o portátil que haga uso de baterías limitadas. Los microcontroladores son menos potentes que las CPUs, pero ofrecen un mucho menor consumo de energía y pueden ser reprogramados fácilmente. En cuanto a las FPGAs y CPLDs, pueden llegar a implementar diseños de manera más eficiente y potente que una CPU, pero, en general, el desarrollo de dichos diseños es más complejo que con CPUs y microcontroladores, y su consumo energético es habitualmente mayor que estos últimos debido a la corriente de alimentación que precisan para alimentar permanentemente la lógica embebida. Respecto a los ASICs, son dispositivos diseñados prácticamente ad-hoc para resolver unas tareas muy concretas, con lo que son muy potentes y su consumo puede ser optimizado. Sin embargo, el problema de los ASICs es su coste de desarrollo (casi siempre por encima del millón de euros), con lo que estos desarrollos sólo compensan económicamente cuando se produce una cantidad muy alta de unidades de un producto con lo contiene. Finalmente, los SoCs y PSoCs suelen integrar en un mismo circuito un microcontrolador potente y varios periféricos (por ejemplo, transceptores de comunicaciones), lo que los convierte en sistemas más potentes que muchos microcontroladores, pero con un consumo más elevado que estos.

Finalmente, el módulo 104 de control podría presentar también una configuración híbrida entre informática y electrónica. En este caso, el módulo debería comprender una memoria y un microcontrolador para implementar informáticamente una parte de sus funcionalidades,

así como determinados circuitos electrónicos para implementar el resto de las funcionalidades.

Además, el dispositivo 100 puede comprender también un módulo 105 de gestión de Blockchain configurado para gestionar el intercambio de datos de identificación y seguimiento obtenidos en las comunicaciones entre el módulo 102 de identificación activa del dispositivo 100 y el lector 202 de identificación activa del sistema externo 200, con una Blockchain 205 (ver Figura 2).

Cuando el dispositivo 100 no es lo suficientemente potente o no tiene los recursos computacionales suficientes para soportar el módulo de gestión de Blockchain, el sistema externo 200 puede contener un módulo de gestión de Blockchain configurado para gestionar el intercambio de datos de identificación y seguimiento obtenidos en las comunicaciones entre el módulo 102 de identificación activa del dispositivo 100 y el lector 202 de identificación activa del sistema externo 200, con una Blockchain 205 (ver Figura 2); o el intercambio de datos de identificación y seguimiento obtenidos en las comunicaciones entre el módulo 101 de identificación pasiva del dispositivo 100 y el lector 201 de identificación pasiva del sistema externo 200, con una Blockchain 205 (ver Figura 2).

La tecnología Blockchain, originaria de la criptomoneda Bitcoin, permite crear aplicaciones descentralizadas capaces de rastrear y almacenar transacciones realizadas por una gran cantidad de usuarios y dispositivos simultáneos. Blockchain puede agregar valor a muchas aplicaciones al abordar algunos de los desafíos más relevantes de la actualidad:

- Descentralización. Es una característica deseable en muchas aplicaciones que actualmente dependen de servidores centralizados costosos de implementar y mantener. Además, muchas empresas subcontratan su infraestructura de servidores a terceros (principalmente porque no consideran dicha infraestructura como su negocio principal), por lo que pagan a los intermediarios el coste de una solución centralizada subcontratada.
- En ciertos escenarios, el proceso de actualización de software/firmware de dispositivos requiere realizar tareas manuales en múltiples dispositivos distribuidos. Por lo tanto, es necesario encontrar una manera de aliviar tales tareas tediosas e ineficientes y distribuir actualizaciones de software simultáneamente a tantos dispositivos inteligentes como sea posible.

- Es necesario asegurar la autenticidad de las transacciones realizadas con ciertos socios, proveedores de servicios, fabricantes e incluso gobiernos. Debido a estas razones, se requiere una tecnología que proporcione mecanismos para verificar la responsabilidad y agregar confianza.
- La información intercambiada con terceras empresas es clave para algunas empresas, por lo que deben protegerse y anonimizarse. Lo mismo ocurre con los datos recopilados por los dispositivos, que deben estar protegidos y seguir siendo privados para las partes no autorizadas.
- Muchas empresas dependen de código fuente cerrado, lo que también aumenta la falta de confianza, ya que en realidad no es transparente su funcionamiento. Por lo tanto, para brindar confianza y seguridad, es esencial fomentar enfoques de código fuente abierto. No obstante, debe enfatizarse que el código de fuente abierto también puede sufrir errores y vulnerabilidades, pero como ha sido verificado por muchos desarrolladores, es menos susceptible a modificaciones maliciosas.

En la invención, se aprovechan las ventajas mencionadas anteriormente de modo que los datos recopilados por el dispositivo 100 se envían, verifican y almacenan de forma segura en una Blockchain 205. Además, la Blockchain se puede configurar para determinar quién puede acceder a la información: todos los que tienen acceso a la cadena de bloques o solo un subconjunto de entidades autorizadas. Por lo tanto, la invención puede hacer uso de diferentes tipos de Blockchains:

- Blockchain públicas: no requieren la aprobación de una entidad para unirse a la Blockchain. Cualquiera puede publicar y validar transacciones. Las cadenas de bloques públicas pueden ser útiles en ciertos escenarios donde es necesario un grado alto de transparencia o donde se requiere la interacción masiva del dispositivo del consumidor.
- Blockchain privadas: la participación en la Blockchain está regulada por el propietario. Por lo tanto, este propietario decide sobre temas como las recompensas de minado o quién puede acceder a la red.
- Blockchain federadas: un grupo de propietarios opera la Blockchain. Restringen el acceso de los usuarios a la red y las acciones realizadas por los participantes. De hecho, el algoritmo de consenso generalmente es ejecutado por un grupo de nodos preseleccionados, lo que aumenta la privacidad de la transacción y acelera la validación de las transacciones.

Además de interactuar con una Blockchain 205, la invención también puede participar en contratos inteligentes 206 (en inglés, *smart contracts*). Un smart contract se puede definir como un código descentralizado autosuficiente que se ejecuta de manera autónoma cuando se cumplen ciertas condiciones de un proceso de negocio. El código puede traducir a términos legales el control sobre objetos físicos o digitales a través de un programa ejecutable. Las condiciones de los smart contracts se basan en datos que dependen de servicios externos que obtienen datos del mundo real y los almacenan en la Blockchain (o viceversa).

El módulo 105 de gestión de Blockchain (y/o smart contracts) es un módulo que puede implementarse con software o hardware y es responsable de gestionar los intercambios de información con la Blockchain 205 (y/o los smart contracts 206) de forma segura. Dichos intercambios se pueden realizar a través del módulo de identificación activa 202 y a través de Internet o de una red de área local (LAN) 204, y consistirían esencialmente en la subida de información a la Blockchain 205 o la consulta de cierta información almacenada en ella. Igualmente, los resultados en la resolución de smart contracts 206 pueden generar intercambios de información con un dispositivo 100 o con el sistema de gestión 203, permitiendo automatizar la respuesta a ciertos eventos. La Blockchain 205 puede ser pública, privada o federada, existiendo en ella al menos un minero o un controlador de la Blockchain.

Además, el dispositivo 100 puede comprender un módulo 103 de alimentación, el cual se encarga de proveer de energía a los componentes electrónicos que lo requieren. Dado que el dispositivo diseñado es portable, la fuente principal de alimentación son baterías embebidas, pero el módulo permite la inclusión de fuentes de energía alternativa recolectadas mediante técnicas de *energy harvesting* (por ejemplo, recarga de la batería mediante sensores piezo-eléctricos de movimiento).

Con el objetivo de minimizar el consumo, el módulo 101 de identificación activa y el módulo 104 de control pueden permanecer la mayor parte del tiempo apagados o en un modo de bajo consumo. Debido a que el dispositivo 100 puede llegar a mandar datos con una periodicidad muy baja, la mayoría del hardware debe de permanecer en un estado de ultra-bajo consumo hasta que se precise activar el módulo 102 de identificación activa para adquirir y/o enviar datos. La tasa de refresco no se considera crítica, pudiendo ser de minutos o incluso de horas en ciertos escenarios de aplicación.

Además, la transmisión de los datos de posicionamiento del dispositivo 100 puede realizarse bajo demanda, es decir, es el sistema de gestión 203 quien solicita los datos al dispositivo.

Por consiguiente, con respecto al módulo 103 de alimentación, para proporcionar puede comprender una batería, los reguladores necesarios para cada módulo a alimentar, así como un cargador y una placa solar, con la intención de aumentar su autonomía. La batería puede ser, por ejemplo, de ion-litio o de níquel-cadmio.

Por otro lado, el dispositivo 100 puede comprender también un módulo de señalización (no mostrado) que puede incluir al menos uno de los siguientes elementos de señalización:

- un elemento de señalización configurado para generar una señal audible, tal como un altavoz, un timbre o un zumbador;
- un elemento de señalización configurado para generar una señal visual, tal como una pantalla de visualización (por ejemplo, LCD, OLED, etc.) o una pluralidad de LEDs (Light Emitting Diode o Diodo Emisor de Luz);
- un elemento de señalización configurado para generar una señal háptica, tal como un motor vibrador.

De acuerdo con unos ejemplos, este módulo de señalización puede comprender una pluralidad de indicadores visuales de estado, por ejemplo, LEDs. De este modo, el módulo de señalización puede comprender un conjunto de diodos LED (por ejemplo, tres: uno rojo, uno verde y uno amarillo), todos ellos conectados al módulo 104 de control. El dispositivo 100 puede utilizar estos LEDs para transmitir cierta información, que codifica a través de un código de colores. Así, por ejemplo, puede codificarse el envío de datos al sistema de gestión 203, la falta de batería, etc.

Por otro lado, este módulo de señalización puede permitir también señalizar el dispositivo 100, para que sea fácilmente localizable, siendo a su vez fácilmente localizable la persona que lo porta o el producto, subproducto, activo o elemento físico al que está asociado.

Además, el dispositivo 100 puede comprender un encapsulado o carcasa, por ejemplo, estanca, que permite portarlo con facilidad por un usuario o añadirlo o acoplarlo con facilidad a cualquier producto, subproducto, activo o elemento físico, con un funcionamiento totalmente inalámbrico. Este encapsulado o carcasa debe tener en cuenta los siguientes

factores inherentes al uso diario del dispositivo o, en ciertos casos, a los relacionados con su uso en aplicaciones industriales, para su correcta configuración:

- Adecuación al entorno de desarrollo. Implica que los sistemas de identificación y seguimiento (es decir, el dispositivo 100) deben tener un tamaño lo más pequeño posible para no causar incomodidad durante su manejo diario o cuando sea adherido a productos, subproductos, activos u objetos que vayan a ser manipulados;
- Presencia de metales. Idealmente, el dispositivo 100 debe soportar la presencia de metales en el entorno;
- Presencia de agua en el ambiente. El dispositivo 100 debe soportar la transmisión en entornos marítimos-costeros donde la humedad relativa puede ser muy elevada;
- Presencia de ácidos y sustancias corrosivas. En entornos industriales el encapsulado del dispositivo 100 debe ser capaz de resistir ácidos, salinidad, combustible y demás sustancias que puedan crear corrosión;
- Interferencias. El dispositivo 100 debe poder transmitir en presencia de las fuentes más habituales de interferencia electromagnética;
- Tolerancia a temperaturas. En entornos industriales el dispositivo 100 debe soportar las temperaturas que los productos, subproductos, activos o elementos físicos puedan alcanzar en ciertos momentos de su vida útil;
- Presión soportada. El dispositivo 100 debe ser capaz de soportar la presión ejercida durante su uso diario o, en el caso de un entorno industrial, durante el procesado habitual de los productos, subproductos, activos o elementos físico (por ejemplo, apilado de objetos en pallets).

Además, es necesario tener en cuenta, en ciertas aplicaciones, la relevancia del encapsulado en el grado de aceptación y usabilidad del dispositivo por parte de los usuarios de determinados colectivos (por ejemplo, niños).

Tradicionalmente el formato de encapsulado utilizado por sistemas similares ha sido el de una tarjeta parecida a las bancarias, pero existe la posibilidad de embeber el dispositivo 100 en objetos que hagan más atractivo su uso. Por ejemplo, es posible variar el encapsulado en función del grupo de edad o permitir personalizarlo incluyendo una foto del usuario. Igualmente, el dispositivo 100 podría encapsularse en forma de wearable: pulseras para niños, relojes (de muñeca, de bolsillo y llaveros) o fundas para el móvil, o incluso dentro de los textiles, creando un dispositivo e-textile (textil electrónico).

Como puede verse en la Figura 2, un sistema para realizar la identificación y el seguimiento de al menos una persona, vehículo, producto, subproducto, activo o elemento físico puede comprender un dispositivo 100, tal como el descrito anteriormente, un sistema externo 200 y un sistema de gestión 203.

El sistema externo 200 puede comprender:

- Un lector 201 de identificación pasiva configurado para comunicarse con el módulo 101 de identificación pasiva del dispositivo 100;
- Un lector 202 de identificación activa configurado para comunicarse con el módulo 102 de identificación activa del dispositivo 100;
- Un módulo (no mostrado) de gestión de Blockchain.

Tanto cada lector 201 de identificación pasiva como cada lector 202 de identificación activa puede comunicarse además de manera cableada o inalámbrica con el sistema de gestión 203 a través de una red de datos local interna (LAN interna) o de Internet 204, para, por ejemplo, el intercambio de datos de identificación y seguimiento obtenidos en sus comunicaciones con el módulo 101 de identificación pasiva del dispositivo 100 y con el módulo 102 de identificación activa del dispositivo, respectivamente. En el caso de una comunicación cableada (alámbrica), la conexión puede realizarse mediante puertos serie, tales como USB, micro USB, mini USB, Firewire o Ethernet. En el caso de comunicaciones inalámbricas, la conexión puede realizarse mediante módulos de comunicaciones inalámbricas de corto alcance, por ejemplo, Bluetooth, NFC, Wifi, IEEE 802.11 o Zigbee, aunque pueden presentar un consumo energético excesivo para el objetivo que se persigue. Si las comunicaciones son de largo alcance, la conexión puede realizarse mediante módulos de comunicaciones basados en tecnología GSM, GPRS, 3G, 4G, 5G o tecnología por satélite (por ejemplo, si la comunicación se realiza a través de una red global de comunicación, tal como Internet), aunque también tienen un consumo energético excesivo, o incluso a través de la red de comunicaciones para IoT descrita anteriormente.

Para que toda la información obtenida por los dispositivos 100 sea de utilidad, debe transmitirse en tiempo real o casi-real al sistema de gestión 203 para que éste la filtre, procese y haga disponible a los potenciales usuarios externos (por ejemplo, los padres de un escolar que deseen saber si éste ha llegado correctamente al colegio o si se ha bajado del vehículo en cierta parada).

En el caso de que al menos un lector 201 de identificación pasiva y al menos un lector de 202 identificación activa se encuentren embarcados en un vehículo o similar, puede ser necesario dotarles de interfaces de comunicación basados en tecnológicas de telefonía móvil de tipo 2G/3G/4G/5G (e.g., GSM, GPRS, UMTS, LTE, LTE-A). Según ha avanzado la tecnología, la velocidad de transmisión que permiten estos interfaces es cada vez mayor. Las comunicaciones GSM/GPRS sólo permiten transmitir a velocidades relativamente bajas (GSM llega a 9,6 Kbps, GPRS hasta unos 170 kbps), pero suficientes para la transmisión de los datos relacionados con los usuarios y sus transacciones. Sin embargo, en el caso de que precise la transmisión de datos de identificación y seguimiento de múltiples usuarios simultáneamente, pueden ser necesarias las comunicaciones de tipo UMTS (hasta 2 Mbps), LTE (hasta 20 Mbps) o LTE-A (hasta 300 Mbps). Existen igualmente otras tecnologías de transmisión de datos adecuadas para vehículos, pero actualmente no existe garantía de despliegue de la infraestructura inalámbrica adecuada que garantice un flujo de datos en tiempo real. Algunas de estas tecnologías son las redes WLAN (IEEE 802.11 a/b/g/n/ac), WiMAX fijo (IEEE 802.16), Mobile WiMAX (IEEE 802.16e), las redes basadas en balizas RFID o las redes de sensores basadas en IEEE 802.15.4 (ZigBee o 6LoWPAN).

Un ejemplo que ilustra el uso de los componentes descritos anteriormente es el caso de la identificación y seguimiento de un usuario dependiente en un autobús (por ejemplo, un niño o una persona mayor con alguna dependencia). En dicho caso es interesante conocer cuándo dicha persona dependiente se ha subido y bajado del autobús. En este ejemplo se asumiría que el autobús estaría equipado con al menos un lector 201 de identificación pasiva y al menos un lector 202 de identificación activa. Igualmente, se asume que se ha realizado previamente un proceso de asociación de la información personal del usuario (por ejemplo, identidad, saldo, etc.) a un dispositivo 100 como el descrito. El usuario, al subir al autobús, procedería de manera similar a cómo se realiza hoy en día para el pago con tarjeta inteligente en el metro o en autobuses públicos: acercaría el dispositivo 100 a un lector 201 de identificación pasiva. El dispositivo, que, hasta ese momento, por norma general, debería de estar en un modo de bajo consumo, remitiría un identificador al lector 201 de identificación pasiva. A continuación, el dispositivo 100 activaría el módulo 102 de identificación activa, el cual comenzaría a comunicarse con el lector 202 de identificación activa del autobús. De esta manera, mientras el usuario estuviese dentro del autobús, la comunicación entre el dispositivo 100 (a través de su módulo 102 de identificación activa) y el lector 202 de identificación activa continuaría, pero, en el momento en que el usuario descendiese del autobús y se encontrase a cierta distancia, la comunicación entre el módulo

102 de identificación activa del dispositivo 100 y el lector 202 de identificación activa del autobús cesaría, reconociéndose entonces la bajada del autobús por parte del usuario.

Como se puede observar a raíz del ejemplo anterior, existen múltiples escenarios dónde se podría replicar la forma de proceder de cara a identificar y realizar el seguimiento de usuarios, sobre todo cuándo dichos datos son de alto interés, como es el caso de eventos con altas aglomeraciones de gente (por ejemplo, peregrinaciones, eventos deportivos, festivales de música o conciertos). Igualmente podría aplicarse, por ejemplo, en escenarios industriales en los que puede ser necesario, por ejemplo, conocer la localización de determinados productos fabricados o necesarios para la fabricación.

El sistema de gestión 203 puede consistir básicamente en un servidor remoto que ejecuta al menos un back-end, un front-end y una base de datos. El back-end puede encargarse de la recolección de los datos recibidos sobre la presencia de los múltiples dispositivos 100 desplegados en uno o más de los escenarios monitorizados. El front-end puede facilitar la interacción de los usuarios remotos de cara a realizar tareas de gestión y para la visualización de los datos recibidos. La base de datos puede almacenar la información recolectada y la necesaria para llevar a cabo la configuración y monitorización de los dispositivos.

El sistema de gestión 203 puede ser un servidor en rack o un ordenador personal, bien una torre con una placa de formato reducido, como puede ser una “micro ATX”, o bien un ordenador portátil. Cualquiera de estas opciones aporta una potencia y capacidad de almacenamiento que puede ser suficiente para gestionar las necesidades de datos precisadas para la gestión y control de números no muy elevado de usuarios, productos, subproductos, activos o elementos físicos.

Por consiguiente, el sistema de gestión 203, una vez recibidos los datos referentes a la identificación y seguimiento de un dispositivo 100, los procesa, almacena y pone disponibles a terceros, ya sea, por ejemplo, a través de una aplicación web, un API REST o un acceso simple a una base de datos.

En consecuencia, el sistema de gestión 203 puede presentar una interfaz de usuario intuitiva que permita la visualización en todo momento de la posición de los elementos monitorizados (persona, vehículo, producto, subproducto, activo o elemento físico) a través de cada

dispositivo 100, permitiendo obtener la trazabilidad temporal y de ruta de cualquier elemento y ofreciendo la posibilidad de consultar y explotar los datos históricos de posicionamiento del mismo.

Los datos de identificación y localización obtenidos (es decir, los datos de identificación y seguimiento) pueden almacenarse en un repositorio de datos (por ejemplo, en una base de datos) para su posterior visualización y análisis. Esto permite incluir técnicas de procesado y análisis de datos. Además, pueden presentarse alertas automatizadas, gráficas dinámicas en tiempo real u obtener estadísticas a partir de los registros históricos.

Estos datos pueden almacenarse en el sistema de gestión 203 de manera segura, por ejemplo, mediante el uso de un nombre de usuario/contraseña o encriptados. Así, por ejemplo, en el caso de que se encripten, puede obtenerse una huella electrónica que puede comprender un valor de hash criptográfico, al aplicar una función hash criptográfica sobre los datos almacenados. Básicamente, una función hash criptográfica es un procedimiento determinista que toma los datos almacenados y devuelve una cadena de bits de tamaño fijo, el valor del hash, de manera que un cambio accidental o intencional de los datos provoca un cambio en el valor del mismo.

Una función hash que se puede usar es la SHA-256 (un algoritmo de criptografía universal de la Agencia de Seguridad Nacional (NSA/CSS) de los Estados Unidos) que pertenece al conjunto de funciones hash criptográficas SHA-2 estándar, aunque podría utilizarse otra función hash si, por ejemplo, en un futuro se demuestra que SHA-256 no es lo suficientemente segura. Por ejemplo, SHA-1 y MD5 fueron inicialmente consideradas en el contexto de estos ejemplos, pero finalmente fueron descartados debido a algunos fallos de seguridad reportados. De este modo, a pesar de que SHA-256 puede utilizarse actualmente en el contexto de estos ejemplos (la probabilidad de colisión para dicha función hash es de aproximadamente 1 a 1015, mientras que la probabilidad de que un archivo dado genere dos códigos hash diferentes es cero), puede ser sustituido en el futuro por otra función hash con mejor resistencia a las colisiones (es decir, más segura), tal como, por ejemplo, SHA-3, que es un nuevo estándar de hash actualmente en desarrollo.

En cualquier caso, el módulo 104 de control de un dispositivo 100, tiene que estar configurado para ejecutar un procedimiento tal como el siguiente:

- el módulo 104 de control, a través del módulo 101 de identificación pasiva, recibe una solicitud de identificación por parte del lector 201 de identificación pasiva del sistema externo 200;
- el módulo 104 de control, tras recibir la solicitud de identificación, activa el funcionamiento del módulo 102 de identificación activa;
- el módulo 104 de control, mediante el módulo 102 de identificación activa, lleva a cabo comunicaciones con el lector 202 de identificación activa del sistema externo 200, para realizar la identificación y el seguimiento de la persona, vehículo, producto, subproducto, activo o elemento físico.

Cuando, el módulo 104 de control recibe la solicitud de identificación a través del módulo 101 de identificación pasiva, puede enviar datos de identificación del dispositivo 100 al lector 201 de identificación pasiva. Este, a si vez, puede hacer llegar los datos al sistema de gestión, tal como se ha comentado anteriormente.

Del mismo modo, el módulo 104 de control puede enviar datos de identificación y seguimiento de la persona, vehículo, producto, subproducto, activo o elemento físico generados en las comunicaciones entre el módulo 102 de identificación activa y el lector 202 de identificación activa, a un sistema de gestión 203, tal como se ha comentado también anteriormente.

Este envío al sistema de gestión 203 de los datos de identificación y seguimiento de la persona, vehículo, producto, subproducto, activo o elemento físico puede realizarse a través del módulo 102 de identificación activa del dispositivo 100, cuyo módulo de identificación activa envía los datos al lector 202 de identificación activa, el cual los hace llegar al sistema de gestión 203.

Alternativamente, el dispositivo 100 puede comprender un módulo de comunicaciones (el cual puede comprender al menos una interfaz de comunicaciones y puede seleccionarse la más adecuada al entorno en el que se encuentra el dispositivo), y el envío al sistema de gestión (203) de los datos de identificación y seguimiento de la persona, vehículo, producto, subproducto, activo o elemento físico puede realizarse mediante este módulo de comunicaciones.

Por otro lado, en el caso de que el dispositivo 100 comprenda un módulo 105 de gestión de Blockchain, el procedimiento puede comprender:

- el módulo 104 de control, mediante el módulo 105 de gestión de Blockchain, sube (o intercambia) datos de identificación y seguimiento de la persona, vehículo, producto, subproducto, activo o elemento físico generados en las comunicaciones entre el módulo 102 de identificación activa y el lector 202 de identificación activa, a una Blockchain 205.

Esta subida o intercambio de datos con la Blockchain 205 puede realizarse a través del módulo 102 de identificación activa del dispositivo 100, a través de un módulo de comunicaciones comprendido en el dispositivo, tal como se ha descrito también para el envío de los datos al sistema de gestión 203, o a través del módulo de gestión de Blockchain del sistema externo 200.

Además, el procedimiento ejecutado por el módulo 104 de control del dispositivo 100 puede comprender:

- el módulo 104 de control detiene el funcionamiento del módulo 102 de identificación activa tras transcurrir un tiempo predeterminado sin que se hayan mantenido comunicaciones con algún lector 202 de identificación activa del sistema externo 200.

En este caso, dado que se ha perdido la comunicación del dispositivo 100 con el sistema externo 200, se entiende que la persona que porta el dispositivo o el vehículo, producto, subproducto, activo o elemento físico que tiene asociado el dispositivo ya no se encuentra dentro de la cobertura de dicho sistema externo. Volviendo al ejemplo del usuario dependiente en un autobús, podría entenderse que el usuario (previamente identificado) se ha bajado del autobús, de manera que puede comunicarse a su familia toda la información obtenida (datos de identidad y seguimiento tales como la identidad del usuario, hora del evento, parada en la que se ha bajado, etc.). Además, también puede saberse si ha quedado un sitio libre, a partir del flujo de usuarios que bajan y suben al autobús.

Adicionalmente, el procedimiento puede comprender:

- el módulo 104 de control mantiene al dispositivo 100 apagado o en estado de bajo consumo hasta recibir, a través del módulo 101 de identificación pasiva, una solicitud

de identificación por parte del lector 201 de identificación pasiva del sistema externo 200.

A pesar de que se han descrito aquí sólo algunas realizaciones y ejemplos particulares de la invención, el experto en la materia comprenderá que son posibles otras realizaciones alternativas y/o usos de la invención, así como modificaciones obvias y elementos equivalentes. Además, la presente invención abarca todas las posibles combinaciones de las realizaciones concretas que se han descrito. El alcance de la presente invención no debe limitarse a realizaciones concretas, sino que debe ser determinado únicamente por una lectura apropiada de las reivindicaciones adjuntas.

## REIVINDICACIONES

1. Procedimiento para controlar, mediante un módulo (104) de control, un dispositivo (100) para realizar la identificación y el seguimiento de al menos una persona, vehículo, producto, subproducto, activo o elemento físico, comprendiendo el dispositivo al menos un módulo (101) de identificación pasiva, al menos un módulo (102) de identificación activa y el módulo de control, estando configurado cada módulo de identificación pasiva para comunicarse con al menos un lector (201) de identificación pasiva de un sistema externo (200) y estando configurado cada módulo de identificación activa para comunicarse con al menos un lector (202) de identificación activa del sistema externo, comprendiendo el procedimiento:

- el módulo (104) de control, a través del módulo (101) de identificación pasiva, recibe una solicitud de identificación por parte del lector (201) de identificación pasiva del sistema externo;
- el módulo de control, tras recibir la solicitud de identificación, activa el funcionamiento del módulo (102) de identificación activa;
- el módulo de control, mediante el módulo de identificación activa, lleva a cabo comunicaciones con el lector (202) de identificación activa del sistema externo (200), para realizar la identificación y el seguimiento de la persona, vehículo, producto, subproducto, activo o elemento físico.

2. Procedimiento según la reivindicación 1, que comprende:

- el módulo (104) de control envía datos de identificación y seguimiento de la persona, vehículo, producto, subproducto, activo o elemento físico generados en las comunicaciones entre el módulo (102) de identificación activa y el lector (202) de identificación activa, a un sistema de gestión (203).

3. Procedimiento según la reivindicación 2, en el que el envío al sistema de gestión (203) de los datos de identificación y seguimiento de la persona, vehículo, producto, subproducto, activo o elemento físico se realiza a través del módulo (102) de identificación activa del dispositivo (100).

4. Procedimiento según la reivindicación 2, en el que el dispositivo (100) comprende un módulo de comunicaciones, y en el que el envío al sistema de gestión (203) de los datos de identificación y seguimiento de la persona, vehículo, producto, subproducto, activo o elemento físico se realiza mediante el módulo de comunicaciones.

5. Procedimiento según una cualquiera de las reivindicaciones 1 a 4, en el que el dispositivo (100) comprende un módulo (105) de gestión de Blockchain, comprendiendo el procedimiento:

- el módulo (104) de control, mediante el módulo (105) de gestión de Blockchain, sube datos de identificación y seguimiento de la persona, vehículo, producto, subproducto, activo o elemento físico generados en las comunicaciones entre el módulo (102) de identificación activa y el lector (202) de identificación activa, a una Blockchain (205).

6. Procedimiento según la reivindicación 5, en el que la subida a la Blockchain (205) de los datos de identificación y seguimiento de la persona, vehículo, producto, subproducto, activo o elemento físico se realiza a través del módulo (102) de identificación activa del dispositivo (100).

7. Procedimiento según la reivindicación 5, en el que el dispositivo (100) comprende un módulo de comunicaciones, y en el que la subida a la Blockchain (205) de los datos de identificación y seguimiento de la persona, vehículo, producto, subproducto, activo o elemento físico se realiza mediante el módulo de comunicaciones.

8. Procedimiento según una cualquiera de las reivindicaciones 1 a 7, que comprende:

- el módulo (104) de control detiene el funcionamiento del módulo (102) de identificación activa tras transcurrir un tiempo predeterminado sin que se hayan mantenido comunicaciones con algún lector (202) de identificación activa del sistema externo (200).

9. Procedimiento según una cualquiera de las reivindicaciones 1 a 8, que comprende:

- el módulo (104) de control mantiene al dispositivo (100) en estado de bajo consumo hasta recibir, a través del módulo (101) de identificación pasiva, una solicitud de identificación por parte del lector (201) de identificación pasiva del sistema externo (200).

10. Procedimiento según una cualquiera de las reivindicaciones 1 a 9, en el que el dispositivo (100) comprende un módulo de señalización, comprendiendo el procedimiento:

- El módulo (104) de control, mediante el módulo de señalización, señaliza la persona, vehículo, producto, subproducto, activo o elemento físico.

11. Producto de programa informático que comprende instrucciones de programa para provocar que un módulo (104) de control realice un procedimiento según una cualquiera de las reivindicaciones 1 a 10 para controlar un dispositivo (100) para realizar la identificación y el seguimiento de al menos una persona, vehículo, producto, subproducto, activo o elemento físico.

12. Producto de programa informático según la reivindicación 11, que está almacenado en unos medios de grabación.

13. Producto de programa informático según la reivindicación 11, que es portado por una señal portadora.

14. Módulo (104) de control de un dispositivo (100) para realizar la identificación y el seguimiento de una persona, vehículo, producto, subproducto, activo o elemento físico, comprendiendo el dispositivo al menos un módulo (101) de identificación pasiva, al menos un módulo (102) de identificación activa y el módulo (104) de control, estando configurado cada módulo de identificación pasiva para comunicarse con al menos un lector (201) de identificación pasiva de un sistema externo (200) y estando configurado cada módulo de identificación activa para comunicarse con al menos un lector (202) de identificación activa del sistema externo, **caracterizado** por el hecho de que comprende:

- medios para, a través del módulo (101) de identificación pasiva, recibir una solicitud de identificación por parte del lector (201) de identificación pasiva del sistema externo;
- medios para, tras recibir la solicitud de identificación, activar el funcionamiento del módulo (102) de identificación activa;
- medios para, mediante el módulo (102) de identificación activa, llevar a cabo comunicaciones con el lector (202) de identificación activa del sistema externo (200), para realizar la identificación y el seguimiento de la persona, vehículo, producto, subproducto, activo o elemento físico.

15. Módulo (104) de control de un dispositivo (100) para realizar la identificación y el seguimiento de una persona, vehículo, producto, subproducto, activo o elemento físico, **caracterizado** por el hecho de que comprende una memoria y un procesador, en el que la memoria almacena instrucciones de programa informático ejecutables por el procesador,

comprendiendo estas instrucciones funcionalidades para ejecutar un procedimiento según una cualquiera de las reivindicaciones 1 a 10 para controlar un dispositivo (100) para realizar la identificación y el seguimiento de al menos una persona, vehículo, producto, subproducto, activo o elemento físico.

16. Módulo (104) de control de un dispositivo (100) para realizar la identificación y el seguimiento de una persona, vehículo, producto, subproducto, activo o elemento físico, comprendiendo el dispositivo al menos un módulo (101) de identificación pasiva, al menos un módulo (102) de identificación activa y el módulo (104) de control, estando configurado cada módulo de identificación pasiva para comunicarse con al menos un lector (201) de identificación pasiva de un sistema externo (200) y estando configurado cada módulo de identificación activa para comunicarse con al menos un lector (202) de identificación activa del sistema externo, **caracterizado** por el hecho de que está configurado para:

- recibir, a través del módulo (101) de identificación pasiva, una solicitud de identificación por parte del lector (201) de identificación pasiva del sistema externo (200);
- activar el funcionamiento del módulo (102) de identificación activa, tras recibir la solicitud de identificación;
- llevar a cabo, mediante el módulo de identificación activa, comunicaciones con el lector (202) de identificación activa del sistema externo (200), para realizar la identificación y el seguimiento de la persona, vehículo, producto, subproducto, activo o elemento físico.

17. Dispositivo (100) para realizar la identificación y el seguimiento de una persona, vehículo, producto, subproducto, activo o elemento físico, **caracterizado** por el hecho de que comprende:

- un módulo (101) de identificación pasiva;
- un módulo (102) de identificación activa;
- un módulo (104) de control según una cualquiera de las reivindicaciones 14 a 16.

18. Dispositivo (100) según la reivindicación 17, que comprende:

- un módulo (105) de gestión de Blockchain configurado para gestionar intercambios de datos de identificación y seguimiento obtenidos en las comunicaciones entre el módulo (102) de identificación activa y el lector (202) de identificación activa, con una Blockchain (205).

19. Dispositivo (100) según una cualquiera de las reivindicaciones 17 o 18, que comprende:

- un módulo (103) de alimentación configurado para proporcionar energía a diferentes módulos del dispositivo.

20. Dispositivo (100) según una cualquiera de las reivindicaciones 17 a 19, que comprende:

- un módulo de señalización.

21. Dispositivo (100) según la reivindicación 20, en el que el módulo de señalización comprende al menos uno de los siguientes elementos de señalización:

- un elemento de señalización configurado para generar una señal audible;
- un elemento de señalización configurado para generar una señal visual;
- un elemento de señalización configurado para generar una señal háptica.

22. Dispositivo (100) según una cualquiera de las reivindicaciones 17 a 21, que comprende un encapsulado o carcasa.

23. Dispositivo (100) según la reivindicación 22, en el que el encapsulado tiene forma de al menos uno de los siguientes elementos:

- una tarjeta inteligente, tal como una tarjeta bancaria, de transporte o similar;
- una pulsera;
- un reloj;
- una funda;
- textil.

24. Sistema para realizar la identificación y el seguimiento de una persona, vehículo, producto, subproducto, activo o elemento físico, **caracterizado** por el hecho de que comprende:

- un dispositivo (100) según una cualquiera de las reivindicaciones 17 a 24;
- un sistema externo (200) que comprende:
    - un lector (201) de identificación pasiva configurado para comunicarse con el módulo (101) de identificación pasiva del dispositivo;
    - un lector (202) de identificación activa configurado para comunicarse con el módulo (102) de identificación activa del dispositivo.

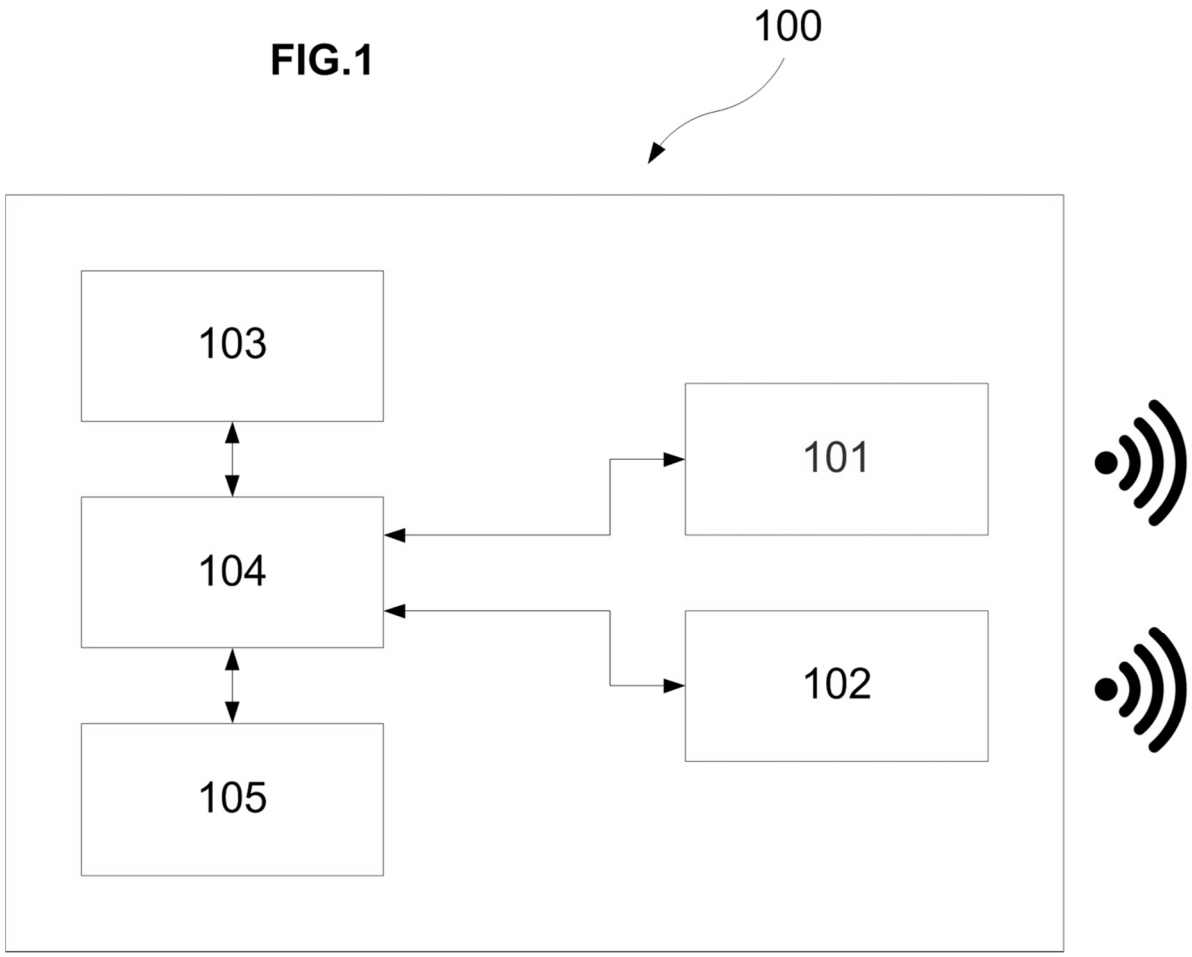
25. Sistema según la reivindicación 24, en el que el lector (202) de identificación activa está configurado para comunicarse con un sistema de gestión (203) para intercambiar datos de identificación y seguimiento de la persona, vehículo, producto, subproducto, activo o elemento físico, siendo generados estos datos en las comunicaciones entre el módulo (102) de identificación activa del dispositivo y el lector (202) de identificación activa del sistema externo (200).

26. Sistema según una cualquiera de las reivindicaciones 24 o 25, en el que el dispositivo (100) comprende un módulo (105) de gestión de Blockchain configurado para gestionar intercambios de datos de identificación y seguimiento de la persona, vehículo, producto, subproducto, activo o elemento físico, a través del módulo (102) de identificación activa y del lector (202) de identificación activa, con una Blockchain (205), siendo generados estos datos en las comunicaciones entre el módulo de identificación activa del dispositivo y el lector de identificación activa del sistema externo (200).

27. Sistema según una cualquiera de las reivindicaciones 24 o 25, en el que el sistema externo (200) comprende un módulo de gestión de Blockchain configurado para gestionar intercambios de datos de identificación y seguimiento de la persona, vehículo, producto, subproducto, activo o elemento físico generados en las comunicaciones entre el módulo (102) de identificación activa del dispositivo (100) y el lector (202) de identificación activa del sistema externo (200).

28. Sistema según una cualquiera de las reivindicaciones 24 o 25, en el que el sistema externo (200) comprende un módulo de gestión de Blockchain configurado para gestionar intercambios de datos de identificación y seguimiento de la persona, vehículo, producto, subproducto, activo o elemento físico generados en las comunicaciones entre el módulo (101) de identificación pasiva del dispositivo (100) y el lector (102) de identificación pasiva del sistema externo (200).

FIG.1



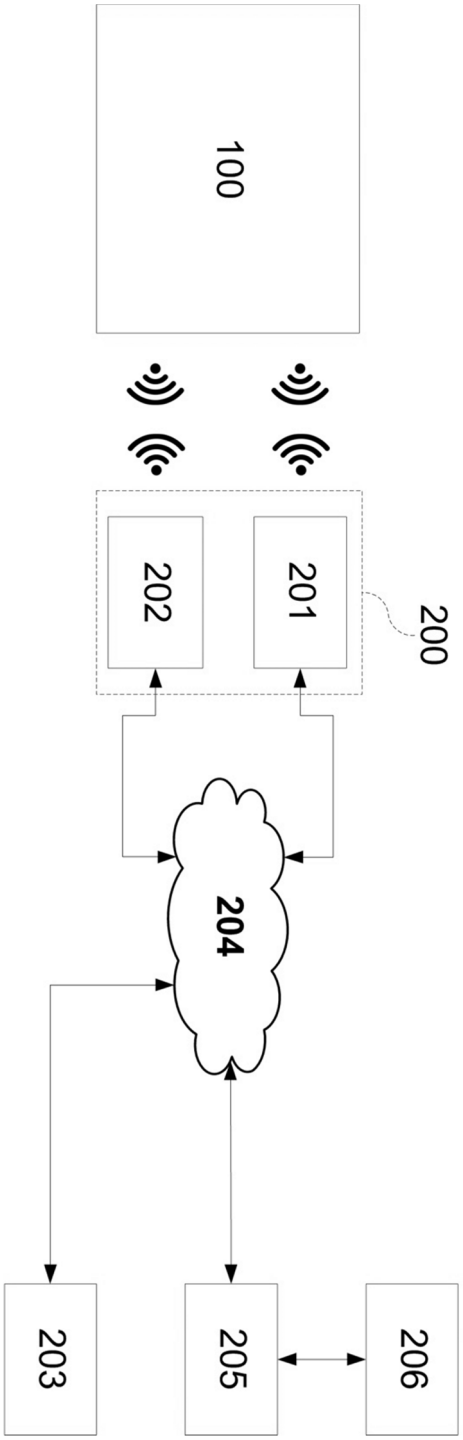



FIG.2

OFICINA ESPAÑOLA
DE PATENTES Y MARCAS

ESPAÑA

(21) N.º solicitud: 201831082

(22) Fecha de presentación de la solicitud: 08.11.2018

(32) Fecha de prioridad:

# INFORME SOBRE EL ESTADO DE LA TECNICA

(51) **Int. Cl. :** ***H04W4/029*** (2018.01)

DOCUMENTOS RELEVANTES

| **Categoría** | (56) **Documentos citados** | **Reivindicaciones afectadas** |
|---|---|---|
| X | US 2018220278 A1 (TAL NIR et al.) 02/08/2018,<br>Párrafos 0008-0010, 0023, 0039-0049, 0061-0065, 0072-0078, 0083, 0095;<br>Figuras; Reivindicaciones. | 1-28 |
| A | US 2008150698 A1 (SMITH GEOFF et al.) 26/06/2008,<br>Párrafos 0047, 0057, 0082, 0084 | 1-28 |
| A | WO 2018126077 A1 (INTEL CORP) 05/07/2018,<br>Párrafos 0017, 0205, 0577, Figura 10 | 1-28 |
| A | US 2017161517 A1 (SHAH SHAHID N) 08/06/2017,<br>Todo el documento | 1-28 |

Categoría de los documentos citados
X: de particular relevancia
Y: de particular relevancia combinado con otro/s de la misma categoría
A: refleja el estado de la técnica
O: referido a divulgación no escrita
P: publicado entre la fecha de prioridad y la de presentación de la solicitud
E: documento anterior, pero publicado después de la fecha de presentación de la solicitud

**El presente informe ha sido realizado**

☒ para todas las reivindicaciones ☐ para las reivindicaciones nº:

| **Fecha de realización del informe** | **Examinador** | **Página** |
|---|---|---|
| 21.06.2019 | F. Diaz Madrigal | 1/2 |

Documentación mínima buscada (sistema de clasificación seguido de los símbolos de clasificación)

H04W

Bases de datos electrónicas consultadas durante la búsqueda (nombre de la base de datos y, si es posible, términos de búsqueda utilizados)

INVENES, EPODOC, WPI, Internet