XV Jornadas de Ingeniería Telemática.
JITEL 2021.
Universidad de A Coruña.

Actas de las XV Jornadas de Ingeniería Telemática (JITEL 2021), A Coruña (España), 27-29 de octubre de 2021.

Mercado de datos IoT sustentado en tecnologías Blockchain

Jorge Lanza, Iván González, Luis Sánchez, Juan Ramón Santana, Pablo Sotres
Departamento Ingeniería de Comunicaciones
Universidad de Cantabria
Avda. Los Castros S/N - Santander - 39005 Cantabria.
{jlanza, igonzalez, lsanchez, jrsantana, psotres}@tlmat.unican.es

El despliegue de infraestructuras de la Internet de las Cosas ha supuesto una revolución en la adquisición de información del contexto alrededor de los servicios provistos para y por los usuarios. Sin embargo, las soluciones globales más comunes se basan en metodologías propietarias que no implementan mecanismos que acrediten y garanticen el origen y futuro uso confiable de los datos generados y compartidos. Estas, además, excluyen al usuario como fuente de los datos de contexto de la cadena de valor. Este artículo describe y evalúa un ecosistema de gestión de datos IoT basado en Blockchain, que garantiza al proveedor el control sobre quién, cómo y cuándo hace uso de los datos, al tiempo que permite explotar nuevos modelos de negocio y monetización de los mismos.

***Palabras Clave*- IoT, Blockchain, prosumer, mercado**

I. INTRODUCCIÓN

El panorama de soluciones de la Internet de las Cosas (IoT, *Internet of Things*), además de altamente fragmentado, está dominado por soluciones verticales propietarias. Las soluciones estándar se restringen al entorno de la investigación y la experimentación [1-3]. Resultado de los escasos esfuerzos de estandarización, los usuarios, emprendedores y PyME se encuentran inmersos en un monopolio comercial que reduce sus expectativas a la hora de afrontar soluciones innovadoras en la plétora de potenciales escenarios ante la dificultad de poder aplicar economías de escala.

Las tradicionales infraestructuras IoT exportan información que, en la mayoría de los casos, no es considerada sensible. Sin embargo, el acercamiento de estas redes al entorno de la empresa o del usuario requieren de políticas claras y robustas en términos de privacidad y protección de datos que garanticen la confianza, extendiendo los actuales paradigmas centralizados basados en entidades de confianza hacia soluciones descentralizadas, federadas y transversales.

Lograr superar estas barreras permitirá, entre otras cosas, ampliar el abanico de actores interesados en el despliegue de soluciones de valor añadido en el ámbito de la IoT. De hecho, la colaboración entre ellos, bajo un modelo de co--creación, podría suponer la creación de un nuevo ecosistema, basado en la confianza y la diversidad, donde se fomente y sea habitual la creación de nuevas aplicaciones disruptivas. Monetizar o incentivar económicamente tanto la cesión de los datos como el uso de los servicios jugará un papel determinante en la sostenibilidad, y, por tanto, en el éxito de este nuevo modelo.

La tecnología Blockchain habilita los mecanismos para desplegar soluciones totalmente descentralizadas que proporcionen trazabilidad garantizada del ciclo de vida de servicios y los datos subyacentes, es decir, que se habilitan los mecanismos para gestionar de forma confiable las transacciones de datos y/o monetarios entre los distintos actores implicados. Por tanto, Blockchain puede suponer una respuesta adecuada a los requerimientos de calidad de la información, de confianza en la fuente de los datos y control del potencial uso de éstos, etc. Todo ello permitirá hacer del ecosistema anteriormente descrito una realidad.

No obstante, ha de evitarse la generación de infraestructuras Blockchain independientes y de carácter vertical que harían emerger nuevamente las problemáticas anteriormente señaladas. Es por esto que exportar la solución como un servicio, bajo el concepto *as a Service*, permitiría integrar cualquier ecosistema existente con necesidades confianza distribuida, de forma rápida y sencilla.

Este artículo presenta una plataforma, basada en Blockchain, que exporta un mercado de datos IoT, el cual habilita intercambios transparentes, seguros y confiables entre productores y consumidores de datos. Este mercado (BIDM, *Blockchain-based IoT Data Marketplace*) genera un ecosistema a través del que no solo se implementa el tradicional contrato de compraventa que establece una compensación (precio) por un servicio o bien, sino que lo extiende para obligar a ambas partes a cumplir unas

condiciones y requerimientos previos y a futuro, desde el punto de vista de reputación, usos del bien adquirido, compensaciones en caso de incumplimiento, etc.

En este sentido, el artículo describe la arquitectura funcional de la plataforma que sustenta el BIDM y los procedimientos para la provisión y consumo de información según las premisas anteriormente expuestas. Además, se incluye la implementación y despliegue de una instancia totalmente funcional del BIDM integrada en el ámbito de una plataforma IoT a gran escala [4], de forma que se pueda evaluar su operativa en condiciones reales.

II. Estado del arte

El acceso a los flujos de datos generados por las infraestructuras IoT puede circunscribirse dentro de los modelos de computación en la nube que consideran que cualquier información está disponible remotamente a través de tecnologías web [5], y más específicamente al modelo sensado como Servicio (SaaS, *Sensing as a Service*) mediante el cual las aplicaciones adquieren la información de contexto necesaria usando estas arquitecturas orientadas al servicio.

Centrado en el ecosistema de las ciudades inteligentes, Diaz et al. [6] plantean una arquitectura funcional para estos escenarios sustentada en tres actores: generadores de datos, proveedores de servicios y consumidores de datos y servicios. El concepto de BIDM se puede extrapolar a este planteamiento puesto que considera el comercio regulado de datos entre los dueños de la infraestructura IoT, aquellos que exponen la información agregada de contexto haciendo uso de servicios, y los que hacen uso inteligente de la información disponible.

Originalmente, la información en crudo, sin procesar, proveniente directamente de los sensores era accesible a través de sistemas centralizados en la nube. Este modelo de mercado de datos, que podría llegar a despertar ciertas reticencias en términos de privacidad para productores de datos que no fueran, a su vez, los propios gestores de esos sistemas centralizados, evolucionó hacia soluciones Peer-to-Peer (P2P) [7], cuyo carácter distribuido minimiza la probabilidad de fallo total del sistema al evitar el potencial único punto de error de las anteriores soluciones. Sin embargo, aunque distribuidas, no daban respuesta a los problemas de escalabilidad que supone proporcionar un registro globalmente compartido e interoperable entre plataformas IoT, aspecto este considerado por la propuesta BIDM presentada en este artículo.

Adicionalmente, otro aspecto a considerar en el despliegue de mercados de datos distribuidos es la necesidad de disponer de un modelo de gestión de la confianza, de forma que las transacciones sean validadas sin necesidad de una entidad de confianza central. Yan et al. [8] y Perera et al. [9] trazan las métricas y propiedades (seguridad, confiabilidad, disponibilidad, precisión, etc.) que los metadatos asociados a la información de contexto generada en el ámbito de la IoT deben incluir en aras de proporcionar confianza necesaria para su uso. Éstas pueden ser fácilmente añadidas al modelo de datos que se considera en el BIDM. Es más, el BIDM amplía la confianza más allá del dato, considerando también a los propios productores y consumidores.

Enfocándose en soluciones más recientes en las que el soporte distribuido se sustenta en tecnologías Blockchain, se observa un creciente interés en las soluciones que exploran la integración de las mismas con la IoT [10][11]. La mayoría de ellas se centran en verticales específicos (vehículos autónomos, salud, trazabilidad alimentaria, etc.) [12]-[15], en lugar de buscar una solución transversal como la que se trata en este artículo.

No obstante, existen diversas arquitecturas para dar soporte a mercados de datos con enfoques similares al descrito aquí. La plataforma MARSA [16], si bien comparte objetivo en tanto en cuanto categoriza los productores y sus datos vinculados y establece los mecanismos para comerciar con ellos, considera el uso de una entidad central que actúa como intermediario de confianza entre las partes involucradas en una transacción. La propuesta descrita por Misura [17] también apuesta por un agente que monitoriza las transacciones, pero en este caso, el intercambio es directo entre las partes. Por tanto, se trata de una solución híbrida en línea con el BIDM, aunque hay que destacar que en el caso del BIDM el agente central actúa únicamente en el almacenaje de los datos, basando el resto de las transacciones en un sistema distribuido sobre Blockchain. Adicionalmente, el BIDM da soporte para la transmisión continua de datos a diferencia de la solución de Misura basada en el modelo petición-respuesta.

Por último, destacar el trabajo de Ozyilmaz et al. [18] que describe un mercado como un conjunto de contratos inteligentes (*smart-contract*) ejecutándose en una red Blockchain Ethereum, que acceden a los datos almacenados en Swarm [19], un entorno distribuido de almacenamiento de información. Si bien la solución presenta grandes similitudes con el BIDM, es en el almacenamiento donde difiere. El BIDM, en su objetivo de lograr la interoperabilidad y la federación entre entornos IoT, se apoya en una solución estándar y de código abierto ampliamente adoptada por la comunidad IoT para el desarrollo de ecosistemas inteligentes como es FIWARE [20].

III. Arquitectura

La plataforma que se presenta en este artículo tiene como uno de sus objetivos principales la integración de la tecnología Blockchain en el ámbito de cualquier ecosistema IoT actual o futuro, y ofrecer a través de ella los mecanismos para gestionar el comercio de datos de forma segura y confiable. Se explotan las propiedades inherentes de Blockchain para permitir la trazabilidad de los datos y las operaciones, logrando así satisfacer las siguientes condiciones fundamentales de diseño:

- Las medidas o datos son generados y exportados por entidades de confianza.
- El pago por el acceso a la información se realiza en un momento específico.
- Los compradores reciben la información adquirida.

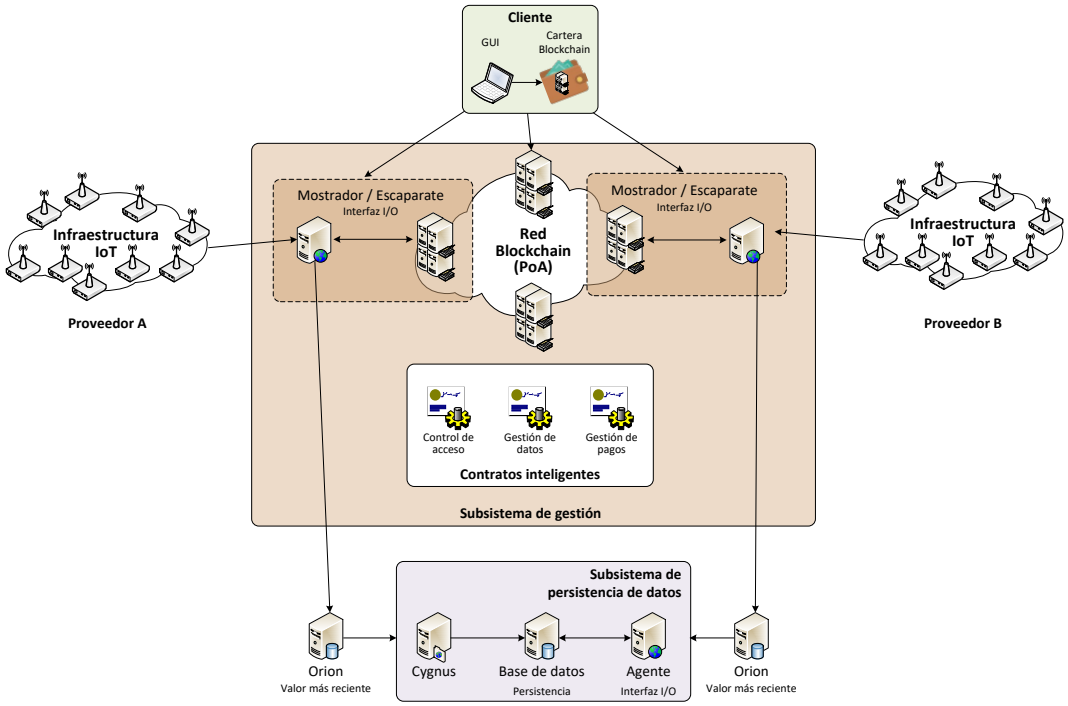

Fig. 1. Arquitectura funcional de la solución

- Sólo aquellas entidades y/o usuarios autorizados podrán acceder de forma segura a la información.

Todo ello redunda en una total transparencia en la operativa del sistema, tanto para los consumidores o clientes como para los productores o infraestructuras IoT.

A. *Arquitectura funcional*

La Fig. 1 muestra la arquitectura funcional del BIDM y las relaciones entre los diferentes elementos que la conforman. Se identifican varios grupos funcionales: por un lado, el subsistema gestor de la plataforma y el de persistencia de datos y, por otro, las entidades externas que estarán vinculadas a los proveedores o a los consumidores de datos. Se ha optado por incluir los elementos que conforman la red Blockchain entre los componentes del subsistema gestor ya que toda la inteligencia de la operativa del mercado tiene como núcleo central esta tecnología. La red Blockchain sobre la que se cimenta el BIDM, ya sea pública o privada, se basa en el protocolo de consenso de Prueba de Autoridad (PoA) y admite la definición de contratos inteligentes. Esta dupla reduce las posibles implementaciones a redes operando con tecnología basada en Ethereum, ya sea la propia Ethereum u otras como Quorum, etc. PoA hace uso de la identidad y la reputación de los validadores como garantía de velar por el buen funcionamiento, la transparencia y confiabilidad de las operaciones dentro de la red. Considerando el objetivo de sustentar el mercado de datos dentro de una federación de infraestructuras IoT, se estima que la opción natural para dar soporte al BIDM es el empleo de este método de consenso unido al despliegue de una red Blockchain permisionada, donde todos los entornos IoT federados tienen el mismo peso y, por tanto, el mismo grado de confianza. Adicionalmente, PoA, frente a otros protocolos de consenso como Prueba de Trabajo (PoW, *Proof-of-Work*), se adapta mejor a la naturaleza asíncrona de la IoT puesto que permite fijar la periodicidad de los bloques minados en función de las tasas máximas y mínimas de publicación de datos, minimizando así el número de bloques vacíos almacenados en la cadena de bloques.

Profundizando en los componentes funcionales principales, encontramos por un lado el mostrador o escaparate como punto de interconexión con el exterior y el subsistema de persistencia de datos:

- Mostrador o escaparate, considerado como un interfaz de I/O, es el elemento a través del cual se recolectan las medidas remitidas por los productores de datos, se publicitan a los potenciales consumidores y, finalmente, las sirve a solicitud de estos últimos. Asimismo, redirige la información al subsistema de persistencia, y la indexa y referencia dentro de la cadena de bloques para facilitar su posterior búsqueda y acceso. Este componente se puede dividir en un proxy de entrada o API que procesa la información recibida y un nodo Blockchain como punto de entrada a red y elemento habilitador de la interacción con los contratos inteligentes que se ejecutan en ella. Podrán existir instancias por cada proveedor y actuarán como cartera de los mismos. La disponibilidad de diferentes puntos de entrada a la red Blockchain reduce los potenciales problemas de escalabilidad. La interfaz visual puede ser adaptada en cada instancia, si bien habilitará el acceso a la información de forma global.
- El Subsistema de persistencia de datos es el almacén de la información, sustentado en habilitadores genéricos del ecosistema FIWARE como Orion y Cygnus. Incluye también una base de

datos indexada por el hash del bloque y accesible a través de un agente web. El uso de los modelos de datos estándar e interoperables permitirá compartir infraestructura entre diferentes proveedores o federar las propias.

B. Procedimientos

Además de estos elementos, se despliegan tres contratos inteligentes que son los que aportan la confianza en el BIDM durante las operaciones de control de acceso, almacenamiento de datos y pago por uso. El primero de ellos, limita el registro de medidas o datos en la plataforma a sensores o productores de confianza, del mismo modo que restringe el acceso a la información a clientes debidamente registrados y validados. El registro de estos usuarios, tanto productores como consumidores, se hace mediante un procedimiento de gestión de usuarios cuyas credenciales, vinculadas a sus cuentas Ethereum y/o certificados digitales, se integran con la base de datos de usuarios a la que accede el contrato de control de acceso.

El contrato vinculado al almacenamiento de datos gestiona cómo se guarda la información en la cadena de bloques. El modelo de datos empleado incluye, además del hash de la medida, como parámetro de indexación y garantía de integridad, una referencia absoluta a su localización en el subsistema de persistencia de datos, de forma que se pueda recuperar de forma total o parcial según lo acordado en la transacción de compra. Además, se incorporan una serie de metadatos descriptivos de la medida, que ayudarán a publicitarla en el propio mercado. En la implementación que se ha realizado, la información contenida en estos metadatos se refiere al fenómeno físico medido en la observación, al sensor del que proviene y al precio asignado a la medida, pero desde el punto de vista de diseño, se podría extender para incluir características de calidad de la medida, reputación del productor, etc. Por último, el contrato de pagos gestiona la transacción de adquisición de una medida, evitando pagos duplicados y garantizando la recepción de la misma según las condiciones de compra.

A continuación, se detalla la interacción entre ellos para dar respuesta a las necesidades de autenticación y acceso a la información.

Para garantizar el origen de la información almacenada, únicamente sensores o proveedores de confianza previamente autorizados pueden interactuar con la plataforma. El proceso de autorización consiste en asociar un identificador único a estas fuentes de información. El proceso de asociación puede realizarse de múltiples formas, entre ellas delegando la confianza en el propio mercado de datos. En el caso que se describe en este artículo, se ha optado por generar las credenciales fuera de línea y grabarlas de forma segura en los dispositivos, es decir, el gestor particular del BIDM genera un identificador y una contraseña única para cada dispositivo. Adicionalmente se provee la clave pública o el certificado digital del BIDM.

Las solicitudes de registro de medidas enviadas por los proveedores deben, por tanto, incluir, además de la propia medida en formato NGSIv2 [21], las credenciales que

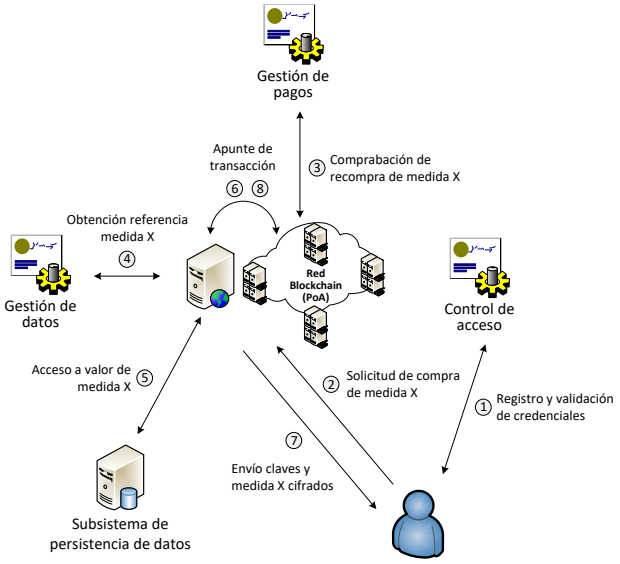

Fig. 2. Proceso de acceso a medidas

permitan validar la identidad del proveedor. Para evitar comprometer la confidencialidad de las mismas, tanto el identificador como la contraseña se cifran con la clave pública del BIDM.

A la recepción de la medida, y una vez comprobado que proviene de un productor autorizado, se comprueba la integridad y validez de la información recibida y se adapta el documento eliminando información no relevante o redundante. Posteriormente, se calcula el hash del documento final y redirige para su almacenamiento.

Una vez confirmado el almacenamiento de la medida por parte del subsistema de persistencia de datos, que incluye un enlace único y permanente al documento almacenado, se procede a inyectar el hash, la referencia y el conjunto de metadatos (descripción, etc.) en la cadena de bloques.

La información residente en la cadena de bloques permite facilitar la búsqueda de datos apoyándose únicamente en los datos disponibles en ella, al tiempo que se reduce el tamaño de la mismo al externalizar el almacenamiento de los datos de la medida. No obstante, se mantienen las garantías de integridad al incorporar de forma disjunta la referencia a la medida y el resumen de la misma. La confianza en el conjunto de datos que conforman el documento la otorga la propia plataforma y operativa Blockchain.

El proceso de búsqueda se lleva a cabo por parte de los potenciales clientes. Los clientes son entidades también registradas y validadas en la red Blockchain, pero a diferencia de los proveedores IoT, éstos tienen permisos restringidos a operaciones de lectura. La búsqueda se realiza directamente sobre la propia cadena de bloques, si bien, como alternativa, se puede considerar la búsqueda directa en el entorno de persistencia a través de un API generada para tal efecto. El resultado de ambas búsquedas será el hash del documento que permita referenciar a la cadena de bloques.

Identificada la medida o conjunto de medidas que se quieren adquirir, se procede a continuación a la compra, la cual otorga el derecho de acceso a los valores de las

mismas. La Fig. 2 muestra el desarrollo del proceso que deben seguir los consumidores, en el que están involucrados todos los contratos inteligentes.

El cliente comienza el proceso de compra iniciando una transacción de compra con el contrato inteligente de pagos (paso 2 en la Fig. 2), quien apoyado en el contrato de control de acceso garantiza que se trata de un cliente autorizado. Entre los datos incluidos en la transacción de compra se encuentra además de los identificadores de cliente, el identificador único o hash de las medidas que se desean adquirir. A partir de éste, puesto que está almacenado también en la cadena de bloques, el contrato obtiene la referencia única (i.e. URL) a la medida. Teniendo en cuenta que el agente del subsistema de persistencia ofrece una interfaz para acceso a la información basada en servicios RESTful, tras la correspondiente petición HTTP se obtiene el valor de la medida.

La última fase del proceso garantiza que el proceso de pago finaliza únicamente cuando el comprador accede a los datos. Para ello, antes de proceder a su entrega se acondicionan los datos para garantizar que únicamente el adquiriente puede acceder a ellos.

De este modo, la medida se cifra empleando un algoritmo de cifrado simétrico (i.e. AES) utilizando una clave suficientemente robusta generada de manera aleatoria. Esta clave se facilita al cliente cifrándola con la clave pública incluida en su propio certificado. De esta forma se garantiza que únicamente dicho cliente es capaz de descifrar la clave y, por tanto, la medida.

Adicionalmente, con objeto de que el administrador del BIDM pueda acceder a la medida en caso de disputa, también se cifra la clave con la clave pública vinculada al BIDM. De esta forma, si el cliente reporta que la medida no se ajusta a lo adquirido, el administrador podrá comprobar qué valores se le remitieron.

Toda esta información, claves y medida cifrada, se incluye en una transacción entre el BIDM y el cliente, que se anota en la red Blockchain. Dada la naturaleza pública de la información incluida en los bloques de la Blockchain, cualquier usuario con credenciales autorizadas tiene acceso a esta información vinculada a la compra. Sin embargo, únicamente el cliente que ha realizado la compra podrá acceder a la medida en sí ya que esta se almacena en el subsistema de persistencia de la información protegida según el procedimiento anterior.

En este momento, se da por concluida la transacción de pago reflejándolo con el apunte correspondiente en la cadena de bloques.

El proceso descrito implica el almacenaje de la medida en la cadena de bloques de forma cifrada. Inicialmente puede resultar incongruente con la premisa inicial que imponía almacenar las medidas fuera de la cadena de bloques en el componente de persistencia de datos. Sin embargo, el volumen de datos generados por los proveedores excede con mucho las compras que se realicen. Es por ello que se ha optado por esta metodología pues se considera que los beneficios en cuanto a garantía de disponibilidad compensan las necesidades adicionales de espacio de almacenaje.

Como proceso adicional, el cliente puede comprobar que la medida obtenida coincide con la solicitada gracias al resumen que se incluye de ésta en la Blockchain en el momento de publicar la medida.

Para concluir, señalar que los procesos descritos permiten la trazabilidad completa del ciclo de vida de un dato generado por cualquier proveedor IoT, tanto en el propio proceso de generación como en tantos procesos de adquisición como consumidores haya interesados en dicha observación.

IV. Prueba de concepto

A. *Entorno de desarrollo y despliegue*

Para la validación de la solución descrita en este artículo, se han desarrollado e integrado todos los componentes funcionales del BIDM en una implementación de prueba de concepto. El despliegue se ha realizado en un entorno virtual empleando contenedores Docker para facilitar la replicabilidad del sistema.

Se ha tomado la decisión de emplear una red Blockchain privada basada en Ethereum Clique [22], configurada para usar el protocolo de consenso PoA disponible. La red desplegada para la validación consta de cuatro nodos, dos de ellos actuando como validadores y los otros dos como puntos de entrada a la red (sin permisos de validación) para un proveedor, y una cartera de consumidor de información de contexto respectivamente. Adicionalmente se despliega un quinto nodo como nodo inicializador de apoyo al descubrimiento de la configuración de la red distribuida. Si bien puede no considerarse indispensable, la presencia de este nodo reduce y facilita significativamente el proceso de descubrimiento de nodos en redes de gran tamaño, motivo por el cual se incluye como apoyo al soporte a la escalabilidad.

Los contratos inteligentes se han desarrollado en Solidity y desplegado directamente en la red Blockchain, estando por tanto disponibles desde el inicio de la misma.

Finalmente, para el almacenamiento persistente de la información de contexto recolectada de las infraestructuras IoT se han empleado los habilitadores de FIWARE Orion Context Broker y Cygnus, ambos desplegados mediante sendos contenedores Docker.

La interfaz del mostrador o escaparate y la cartera de los clientes se ha realizado empleando tecnologías web, la lógica del servicio web en Nodejs y el interfaz de usuario en HTML y Javascript.

B. *Integración y validación en infraestructura IoT real*

La validación de la implementación realizada se enmarca dentro de la infraestructura IoT disponible en la ciudad de Santander (España), gestionada en el ámbito del proyecto SmartSantander.

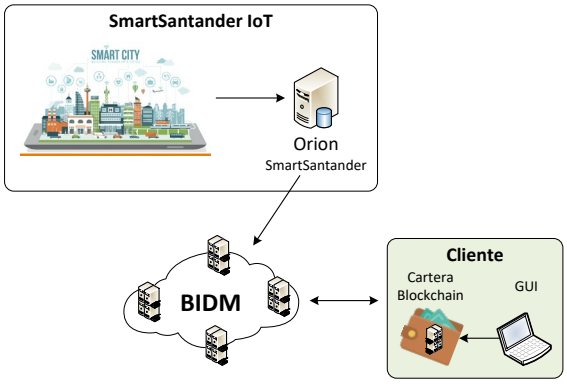

Fig. 3. Integración del BIDM en la infraestructura de SmartSantander

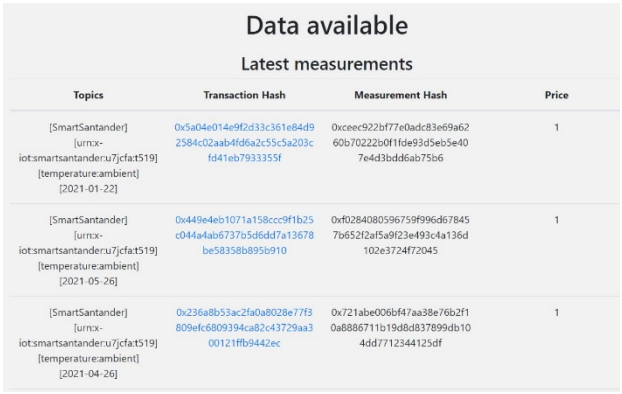

Fig. 4. Datos disponibles en la cadena de bloques

Tal como se muestra en la Fig. 3, el BIDM, para el que únicamente se ha desplegado una instancia del escaparate de datos, se suscribe a las medidas generadas por los sensores disponibles en la ciudad de Santander y exportadas a través de un Orion Context Broker dispuesto a tal efecto. Por tanto, la infraestructura de SmartSantander actúa como proveedor de confianza autorizado en el BIDM. La información recolectada por el BIDM, en formato NGSIv2, es tratada y almacenada tanto en la cadena de bloques asociada al BIDM como en el entorno de persistencia según se ha descrito, para que cualquier cliente pueda solicitar su adquisición. En la Fig. 4, se muestra un ejemplo de cómo se almacenan las medidas en la cadena de bloques. A través de la lectura de la cadena de bloques, el consumidor de información de contexto, además de al hash, tiene acceso a la información descriptiva de dicha medida (en el caso de la implementación realizada, esta información era el identificador del sensor que generó la medida, una marca temporal y el precio fijado para su adquisición.
Un cliente interesado y autorizado puede realizar la compra a través de su cartera virtual.

La Fig. 5 muestra el interfaz de una sencilla cartera, implementada como una página web desde la cual se puede explorar la Blockchain y ver la información incluida en el Mostrador/Escaparate (i.e. la información incluida en los bloques de publicación de medidas). A través de ella, era posible obtener el resumen de la medida deseada y, con él, lanzar una petición de compra, resultado de la cual obtendrá la medida cifrada y la correspondiente clave para descifrarla. Lo que en esta prueba de concepto se implementa como una web desde la cual se seleccionan medidas y se ejecutan compras, en un caso de uso característico podría ser una aplicación móvil que ofrezca un servicio de guía turística en la ciudad y entre sus servicios esté el de recomendación de rutas para ir de un lugar a otro de la misma. La aplicación actuará como cliente y dispondrá de su propia cartera virtual. Cuando el usuario solicite una recomendación para un desplazamiento, la aplicación comprará en el BIDM la información relativa a los tiempos de llegada de los autobuses urbanos a la parada más próxima, las bicicletas disponibles en las estaciones del servicio público de alquiler más cercanas al origen y destino, y el número de plazas de aparcamiento en las inmediaciones del destino, para con ello ofrecer diferentes alternativas de viaje al usuario. De otra parte, el BIDM publica y permite el acceso a la información toda vez se ha cumplimentado el pago por la misma y se satisfacen las condiciones de uso impuestas. El BIDM garantiza, en cierto modo, la calidad de la información y su procedencia. En esta situación, todos los participantes en la cadena del servicio obtienen un beneficio dentro de un ecosistema de confianza mutua. La remuneración obtenida por la venta de los datos permitirá al proveedor mejorar y/o ampliar su infraestructura, lo que redunda en el beneficio del desarrollador de la aplicación que podrá ofrecerla en mejores condiciones a un mayor número de usuarios.

La Fig. 6 muestra una captura de la aplicación de cartera desarrollada en la que se muestra la información disponible a la finalización de una compra en la que se incluye el hash de la transacción que incorpora la clave simétrica de cifrado a la cadena de bloques (KeyTxHash) y el hash de la transacción vinculada a la transferencia de la medida solicitada cifrada (DataTxHash), además del propio hash del evento informativo del final de la compra (EventTxHash). Si bien mediante estas referencias el usuario podría acceder al valor de la medida, la aplicación, con el objetivo de facilitar la operativa al cliente, muestra directamente la medida en claro. En el ejemplo, se proporciona una medida de un sensor que monitoriza el flujo de tráfico en una posición específica.

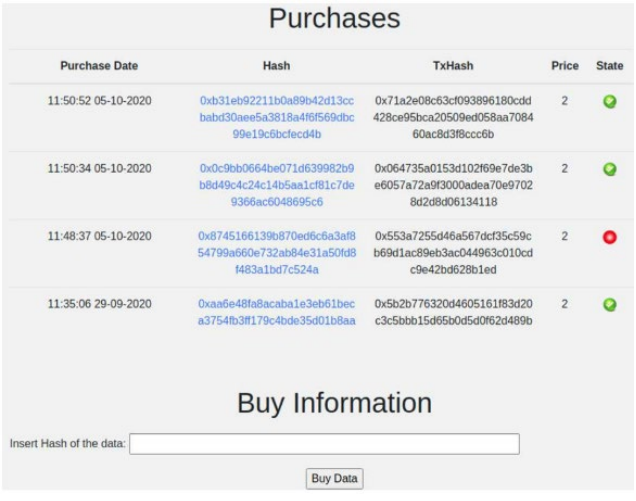

Fig. 5. Interfaz de usuario de la cartera de usuario

Fig. 6. Ejemplo de medida adquirida por un cliente

V. Conclusiones

Este articulo presenta una plataforma que habilita un mercado de datos IoT descentralizado mediante el uso de tecnología Blockchain. A través del BIDM las infraestructuras IoT y las aplicaciones consumidoras de datos de contexto pueden intercambiar información de forma confiable y transparente.

La solución propuesta y descrita en el artículo combina ecosistemas IoT basados en los bloques definidos en el ámbito de Conecting Europe's Facilities (CEF), como es el Orion Context Broker, con la tecnología Blockchain para crear un novedoso entorno que permita la monetización de los flujos de datos con garantías de trazabilidad en todo el ciclo de vida del dato. Gracias a los mecanismos de autenticación y autorización, como a las inherentes propiedades de la tecnología Blockchain se puede garantizar la veracidad, fiabilidad y calidad de los datos.

La solución aborda los potenciales problemas de escalabilidad que podrían resultar del elevado e insostenible crecimiento del tamaño de la cadena bloques. Para ello, se aplica una estrategia de almacenamiento de datos denominada off-chain. En lugar de almacenar todos los datos IoT en la propia Blockchain, estos se almacenan en un entorno especializado e integrado en las infraestructuras IoT, manteniendo en la cadena de bloques únicamente una referencia inmutable a las transacciones realizadas con dichos datos (i.e. registro y compra-venta).

Adicionalmente la solución diseñada da soporte al acceso seguro y garantizado a la información únicamente a aquellos usuarios que, previo pago de la misma, la han adquirido. La combinación de la cadena de bloques, la ejecución de contratos inteligentes en ella y mecanismos de cifrado adicionales lo hacen posible.

Si bien la solución desplegada ha demostrado la viabilidad de un mercado de datos confiable y trazable que combina soluciones estándar de plataformas IoT (i.e. habilitadores funcionales abiertos del ecosistema FIWARE) y las redes Blockchain, capaz de integrarse en un entorno real como es el ecosistema de la ciudad de Santander, aún existen diversas mejoras que aplicar. En este sentido, como trabajo futuro se plantea un exhaustivo análisis de rendimiento y estudio de la escalabilidad del sistema, haciendo hincapié no solo en aspectos vinculados a la seguridad y capacidad de almacenaje de datos, sino también a calidad de servicio y de experiencia de usuario a medida que el volumen de datos aumenta. Además, se plantea la búsqueda de nuevos mecanismos más robustos y amigables de gestionar el ciclo de vida de la información almacenada desde su generación hasta su adquisición y uso por parte del cliente final. Por último, se plantea la extensión del BIDM para dar soporte a consumidores de información con necesidades de tiempo real para lo cual es necesario habilitar un acceso asíncrono (i.e. basado en subscripciones) a las medidas.

Agradecimientos

Este trabajo ha sido realizado en el marco del proyecto FIERCE "Future Internet Enabled Resilient CitiEs" perteneciente al Programa Estatal de I+D+i Orientada a los Retos de la Sociedad (RTI2018-093475-A-I00).

Referencias

[1] H. Hejazi, H. Rajab, T. Cinkler, and L. Lengyel, "Survey of platforms for massive IoT", *2018 IEEE International Conference on Future IoT Technologies, Future IoT 2018*, Mar. 2018, vol. 2018-January, pp. 1–8, doi: 10.1109/FIOT.2018.8325598.

[2] K. J. Singh and D. S. Kapoor, "Create Your Own Internet of Things: A survey of IoT platforms", *IEEE Consumer Electronics Magazine*, vol. 6, no. 2. Institute of Electrical and Electronics Engineers Inc., pp. 57–68, Apr. 01, 2017, doi: 10.1109/MCE.2016.2640718.

[3] J. Kim et al., "Standard-based IoT platforms interworking: Implementation, experiences, and lessons learned," *IEEE Communications Magazine*, vol. 54, no. 7, pp. 48–54, Jul. 2016, doi: 10.1109/MCOM.2016.7514163.

[4] L. Sanchez et al., "SmartSantander: IoT experimentation over a smart city testbed," *Computer Networks*, vol. 61, pp. 217–238, 2014.

[5] P. Banerjee et al., "Everything as a service: Powering the new information economy," *Computer*, vol. 44, no. 3, pp. 36–43, Mar. 2011, doi: 10.1109/MC.2011.67.

[6] R. Díaz-Díaz, L. Muñoz, and D. Pérez-González, "Business model analysis of public services operating in the smart city ecosystem: The case of SmartSantander," *Future Generation Computer Systems*, vol. 76, pp. 198–214, Nov. 2017, doi: 10.1016/j.future.2017.01.032.

[7] Z. Huang, X. Su, Y. Zhang, C. Shi, H. Zhang, and L. Xie, "A decentralized solution for IoT data trusted exchange based-on blockchain," in 2017 3rd IEEE International Conference on Computer and Communications, ICCC 2017, Mar. 2018, vol. 2018-January, pp. 1180–1184, doi: 10.1109/CompComm.2017.8322729.

[8] Z. Yan, P. Zhang, and A. Vasilakos, "A survey on trust management for Internet of Things," *Journal of Network and Computer Applications*, vol. 42, pp. 120–134, Jun. 2014, doi: 10.1016/j.jnca.2014.01.014.

[9] C. Perera et al., "Context-aware sensor search, selection and ranking model for internet of things middleware," *2013 IEEE 14th international conference on mobile data management*, vol. 1, pp. 314-322.

[10] S. K. Lo et al., "Analysis of Blockchain Solutions for IoT: A Systematic Literature Review," *IEEE Access*, vol. 7, pp. 58822–58835, 2019, doi: 10.1109/ACCESS.2019.2914675.

[11] A. Panarello, N. Tapas, G. Merlino, F. Longo, and A. Puliafito, "Blockchain and IoT Integration: A Systematic Survey," *Sensors*, vol. 18, no. 8, p. 2575, Aug. 2018, doi: 10.3390/s18082575.

[12] A. Dwivedi, G. Srivastava, S. Dhar, and R. Singh, "A Decentralized Privacy-Preserving Healthcare Blockchain for IoT," *Sensors*, vol. 19, no. 2, p. 326, Jan. 2019, doi: 475 10.3390/s19020326.

[13] Rathee, Sharma, Iqbal, Aloqaily, Jaglan, and Kumar, "A Blockchain Framework for Securing Connected and Autonomous Vehicles," *Sensors*, vol. 19, no. 14, p. 3165, Jul. 2019, doi: 10.3390/s19143165.

[14] L. Bai, M. Hu, M. Liu, and J. Wang, "BPIIoT: A Light-Weighted Blockchain-Based Platform for Industrial IoT," *IEEE Access*, vol. 7, pp. 58381–58393, 2019, doi: 10.1109/ACCESS.2019.2914223.

[15] Y. P. Tsang, K. L. Choy, C. H. Wu, G. T. S. Ho, and H. Y. Lam, "Blockchain-Driven IoT for Food Traceability with an Integrated Consensus Mechanism," *IEEE Access*, vol. 7, pp. 129000–129017, 2019, doi: 10.1109/ACCESS.2019.2940227.

[16] T. D. Cao, T. V. Pham, Q. H. Vu, H. L. Truong, D. H. Le, and S. Dustdar, "MARSA: A marketplace for real-time human sensing data," *ACM Transactions on Internet Technology*, vol. 16, no. 3, pp. 1–21, May 2016, doi: 10.1145/2883611.

[17] K. Mišura and M. Žagar, "Data marketplace for Internet of Things," *Proceedings of 2016 International Conference on Smart Systems and Technologies*, SST 2016, Dec. 2016, pp. 255–260, doi: 10.1109/SST.2016.7765669.

[18] K. R. Ozyilmaz, M. Dogan, and A. Yurdakul, "IDMoB: IoT data marketplace on blockchain," *Proceedings - 2018 Crypto Valley Conference on Blockchain Technology, CVCBT 2018*, Nov. 2018, pp. 11–19, doi: 10.1109/CVCBT.2018.00007.

[19] V. Tron, "Swarm alpha public pilot and the basics of Swarm," *Ethereum Blog*, 2016. https://blog.ethereum.org/2016/12/15/swarm-alpha-public-pilot-basics-swarm/ (accessed Sep. 21, 2020).

[20] F. Cirillo, G. Solmaz, E. L. Berz, M. Bauer, B. Cheng, and E. Kovacs, "A Standard-Based Open Source IoT Platform: FIWARE," *IEEE Internet of Things Magazine*, vol. 2, no. 3, pp. 12–18, Jan. 2020, doi: 10.1109/iotm.0001.1800022.

[21] FIWARE Data Models, https://www.fiware.org/developers/data-models/

[22] Péter Szilágyi, "Clique proof-of-authority consensus protocol", *Ethereum Improvement Proposal – 225*, March 2017 https://eips.ethereum.org/EIPS/eip-225