Escuela Superior
de Ingeniería y Tecnología
Universidad de La Laguna

Trabajo de Fin de Grado

Grado en Ingeniería Informática

Servicios de participación ciudadana soportados en Blockchain

Citizen participation services supported on Blockchain

Javier Gómez de Vera

La Laguna, a 13 de junio de 2022

D. Julio Antonio Brito Santana, con N.I.F. 42.812.143-Q Profesor Titular de Universidad adscrito al Departamento de Ingeniería Informática y de Sistemas de la Universidad de La Laguna, como tutor

D. Benito Cuesta Viera, con N.I.F. 43.818.241-K, Técnico del Subárea de Gestión - Área de Servicios TIC del Servicio de Tecnologías de la Información y la Comunicación de la Universidad de La Laguna, como cotutor

C E R T I F I C A (N)

Que la presente memoria titulada:

"Servicios de participación ciudadana soportados en Blockchain"

ha sido realizada bajo su dirección por D. Javier Gómez de Vera,

con N.I.F. 79099981-Z.

Y para que así conste, en cumplimiento de la legislación vigente y a los efectos oportunos firman la presente en La Laguna a **13 de junio de 2022**

Agradecimientos

A mi familia por acompañarme durante toda la carrera
A mis amigos que han sido el gran apoyo
A mi tutor y cotutor

Licencia

Resumen

Las Administraciones Públicas se encuentran ante un nuevo escenario donde los ciudadanos demandan una mayor participación en la gobernanza de las ciudades. La participación ciudadana consiste en crear espacios adecuados de colaboración para permitir y facilitar la intervención en las decisiones públicas, en la definición y desarrollo de acciones, y en el uso de los recursos públicos. Así, participar es conocer, opinar, debatir, colaborar, co-crear y tomar decisiones. Las ciudades tienen que dar respuesta al reto de prestar mejores y nuevos servicios, más eficientemente, junto al aumento de la transparencia y la participación ciudadana. Esto es, impulsar una gobernanza inteligente, uno de los pilares y ejes de actuación de la estrategia de Ciudades Inteligentes. Las Tecnologías de la Información y la Comunicación (TIC) juegan un papel catalizador y dinamizador de esta estrategia, facilitando el desarrollo de proyectos, aplicaciones y servicios. Este proyecto trata de identificar y analizar el conjunto de servicios que tienen que ser implementados para aumentar y facilitar la participación ciudadana. También incluye el diseño de una plataforma que proporcione a los ciudadanos, a los diferentes colectivos vecinales y al tejido asociativo herramientas para el traslado de conocimiento, opiniones y sugerencias, la elaboración y creación colectiva de proyectos y propuestas, y facilite la toma de decisiones colectiva. Estos servicios necesitan procedimientos de identificación y autentificación y entornos con garantías de seguridad, inmutabilidad, transparencia y mantenimiento del anonimato. Para todo ello el uso de tecnologías descentralizadas y blockchain pueden ser adecuadas para su desarrollo e implementación.

Palabras clave: Gobernanza Inteligente, Participación Ciudadana, Identidad Digital, Blockchain

Abstract

Public Administrations are facing a new scenario where citizens demand greater participation in the governance of cities. Citizen participation consists of creating adequate spaces for collaboration to allow and facilitate intervention in public decisions, in the definition and development of actions, and in the use of public resources. Thus, participating is knowing, giving opinions, debating, collaborating, co-creating and making decisions. Cities have to respond to the challenge of providing better and new services, more efficiently, together with increased transparency and citizen participation. That is, promoting smart governance, one of the pillars and lines of action of the Smart Cities strategy. Information and Communication Technologies (ICT) play a catalytic and dynamic role in this strategy, facilitating the development of projects, applications and services. This project tries to identify and analyze the set of services that have to be implemented to increase and facilitate citizen participation. It also includes the design of a platform that provides citizens, different neighborhood groups and the associative fabric, tools for the transfer of knowledge, opinions and suggestions, supports the collective elaboration and creation of projects and proposals, and allows the taking of collective decisions. These services require identification and authentication procedures and environments with guarantees of security, immutability, transparency and maintenance of anonymity. For all this, the use of decentralized technologies and blockchain can be suitable for its development and implementation.

Keywords: Smart Governance, Citizen Participation, Digital Identity, Blockchain

Índice General

Índice Figuras

Índice Tablas

Capítulo 1: Introducción

1.1 Motivación

El propósito de este proyecto es por un lado adquirir conocimientos de una nueva tecnología en auge como es Blockchain y por otro lado, analizar el contexto de las ciudades inteligentes donde se puede aplicar para mejorar los servicios de participación ciudadana. El propósito de conseguir una ciudad inteligente forma parte de las estrategias de muchos ayuntamientos. Estos consideran que es el nuevo paradigma de modernización y progreso económico para sus municipios. Además en el momento actual las Administraciones Públicas se encuentran ante un nuevo escenario donde los ciudadanos demandan una mayor participación. Muchos de estos procedimientos de participación en los que interviene un sistema de votación o la generación de incidencias, necesitan de procesos de identificación que verifiquen la identidad del ciudadano y a su vez protejan sus datos personales de forma anónima. La gobernanza inteligente es uno de los pilares de las ciudades inteligentes y está relacionada directamente con la gobernanza abierta y la participación ciudadana.

Existe una amplia gama de aplicaciones que tiene la tecnología Blockchain en muchos campos y también en el ámbito de la gobernanza. Resulta altamente atrayente el poder ampliar ciertos conocimientos sobre aplicaciones de la Blockchain en este ámbito. Las criptomonedas como ethereum, las NFTs y otras aplicaciones de las tecnologías Blockchain han aumentado su popularidad. En los últimos años ha habido un incremento en la investigación y en el interés de la comunidad de desarrolladores en estas tecnologías. Este proyecto trata de acercarse a la implementación de aplicaciones de participación ciudadana con el uso de la tecnología Blockchain.

1.2 Objetivos

El trabajo tiene dos objetivos fundamentales. El primer objetivo es comprender la tecnología y el funcionamiento de Blockchain, en especial las características específicas de la plataforma Hyperledger. Dentro de este ámbito se tendrá en cuenta el funcionamiento básico de una cadena de bloques y los contratos inteligentes. El segundo objetivo es estudiar el estado actual de la participación ciudadana, y las aplicaciones de Blockchain en este ámbito, así como la seguridad y anonimato que puede proporcionar esta tecnología.. Para alcanzar ambos objetivos se ha propuesto el desarrollo de un prototipo de aplicación móvil, junto con una demo en Hyperledger de su funcionamiento, además de una arquitectura de referencia que enlace la plataforma de servicios de cualquier ayuntamiento (en nuestro caso hemos usado de referencia el Ayuntamiento de Santa Cruz de Tenerife y su plataforma de participación ciudadana). Con ello se espera el aumento en la seguridad, integridad y transparencia en los procesos de participación, características que aporta la Blockchain.

1.3 Proceso de desarrollo

Se ha realizado en dos grandes fases, la fase de estudio y la fase práctica, avanzando en ambas de forma simultánea. La primera fase trata el estudio y análisis de los conceptos fundamentales sobre la participación ciudadana y Blockchain, donde se han aprendido conceptos para el proyecto como gobierno abierto, gobernanza inteligente y mecanismos de participación, así

como el uso y ventajas de las tecnologías Blockchain. En la fase práctica se han probado y seleccionado las tecnologías y herramientas, y se ha analizado la viabilidad de la solución final. Finalmente se ha realizado una propuesta de diseño de la aplicación: la arquitectura que llevaría una plataforma municipal de participación con la integración de Blockchain y el prototipado de la aplicación móvil.

1.4 Estructura de la memoria

La estructura de esta memoria se ha dividido en 7 capítulos donde se ha descrito y se deja constancia del trabajo realizado

El primer capítulo expone una introducción al proyecto donde se especifica la motivación, los objetivos, el proceso que se ha seguido y el punto actual donde se explica la estructura de este documento.

El segundo capítulo consiste en un análisis de la participación ciudadana y cada uno de los conceptos claves para su comprensión. También en este capítulo se ha estudiado y descrito la noción de gobierno abierto, así como diferentes aplicaciones y tecnologías utilizadas.

El tercer capítulo analiza la tecnología Blockchain y cada uno de los aspectos y características de interés. En este capítulo se dan detalles de la plataforma Hyperledger.

El cuarto capítulo presenta el diseño prototipado de la propuesta de integración.

En el quinto y sexto capítulo, presentan las conclusiones obtenidas a raíz de la realización de este trabajo y se proponen líneas de trabajo futuro tanto para la mejora de la aplicación como para la mejora del uso de blockchain para la participación ciudadana.

Finalmente, en el séptimo punto se describe y se propone un presupuesto en base al costo personal y los componentes necesarios para hacer un despliegue de la solución propuesta.

Capítulo 2: Participación ciudadana, en el contexto de la gobernanza abierta e inteligente

2.1 Participación ciudadana

La participación ciudadana en el ámbito de las Administraciones Públicas es un derecho reconocido por el art. 23 de la Constitución Española [1] que permite a los ciudadanos participar en los asuntos públicos, directamente o por medio de representantes.

En correspondencia con la madurez democrática de la sociedad, en la última década hay una mayor demanda por parte de los ciudadanos de aumentar la participación y transparencia en todas las instituciones públicas. Con esta tendencia las Administracione Públicas han tomado la iniciativa para dar los pasos necesarios en este sentido. Una nueva gobernanza caracterizada por una

participación real y activa de los ciudadanos en los asuntos políticos, económicos, culturales y sociales. A este nuevo estilo de gobierno se le ha denominado gobernanza inteligente o gobernanza abierta, donde la participación ciudadana constituye uno de sus pilares básicos.

2.1.1 Gobierno Abierto

Gobierno abierto es una forma de gobernanza de las Administraciones Públicas que tiene como objetivo que los ciudadanos colaboren en la mejora de los servicios públicos, sustentandose en tres principios: la transparencia, la colaboración y la participación.

La Constitución española [2] garantiza a la ciudadanía el derecho a participar en los asuntos públicos, directamente o a través de sus representantes. Cada Administración Pública tiene competencia exclusiva en materia de gobierno abierto, excepto en lo relativo a la transparencia, cuya regulación viene dada por una norma estatal, la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno [3].

El Estado, las Comunidades Autónomas y las Entidades Locales desarrollan sus propias políticas y cuentan con sus propios órganos competentes en esta materia.

El concepto de **gobierno abierto** [4] está relacionado con el de **buen gobierno,** que no es más que aquel que promueve los siguientes aspectos recogidos en el Libro Blanco de la Gobernanza Europea [5]:

- Transparencia
- Participación
- Responsabilidad
- Eficacia
- Coherencia

En la actualidad estos aspectos se han unido al desarrollo tecnológico y de ahí el concepto de gobernanza inteligente, donde las tecnologías son un factor dinamizador y catalizador de este nuevo modelo de gobernanza. Los aspectos tecnológicos son fundamentales para la implementación de estos principios, sin embargo, la transformación hacia un **gobierno abierto** no es una simple cuestión tecnológica, sino que precisa de cambios en la concepción de los servicios públicos, los enfoques y modelos organizativos, además de requerir el compromiso ético y la implicación de los funcionarios públicos en un nuevo modelo de gestión pública.

2.1.2 Gobernanza Inteligente

Gobernanza inteligente [6] es el modelo de gobernanza aplicado a un territorio y sociedad específicos, caracterizado por el uso intensivo e inteligente de las Tecnologías de la Información y Comunicaciones (en adelante TIC), que busca maximizar los resultados positivos asociados a la búsqueda del gobierno abierto. Persigue dar respuesta a las Administraciones Públicas en el desarrollo de su actividad y en la prestación de los servicios públicos, entre otras, facilitando una mayor participación ciudadana en la toma de decisiones públicas a través del uso de las TIC para obtener mejores resultados.

Para ello, las Administraciones públicas y la ciudadanía deben poder utilizar, compartir y analizar la información que se deriva de la actuación de las Administraciones Públicas y de las interacciones de la ciudadanía con ella. En el marco de la **gobernanza inteligente** este uso,

compartición y análisis no se realiza únicamente por las Administraciones Públicas, sino que la ciudadanía participa activamente aportando su visión y su capacidad de análisis y de reutilización de la información. Esto no sólo le permite conocer mejor la actuación de las Administraciones Públicas sino también evaluarla.

2.1.3 Transparencia

La transparencia [7] se refiere al deber de los poderes públicos de exponer y someter al análisis de la ciudadanía la información relativa a su gestión, al manejo de los recursos que la sociedad les confía, a los criterios que sustentan sus decisiones, y a la conducta de sus funcionarios.

Los fundamentos de la transparencia se enmarcan en:

- ☐ **Derecho de acceso a la información por parte de la ciudadanía.** El Gobierno debe reconocer el derecho básico de los ciudadanos a obtener toda la información (con excepciones limitadas) y proporcionar información de manera proactiva cuando se le solicite. Solo cuando la divulgación de información pueda causar un daño evidente a los intereses legítimos, puede negarse a proporcionar información. Estos intereses deben estar claramente protegidos por la legislación.

- ☐ **Publicidad activa.** El Gobierno debe publicar activamente información de interés público y hacer los esfuerzos necesarios para asegurar un acceso fácil, rápido, efectivo y práctico a dicha información.

- ☐ **Buen gobierno.** Los principios generales y de actuación a cumplir por los miembros del Gobierno, los Secretarios de Estado y el resto de los altos cargos de la Administración General del Estado y de las entidades de derecho público o privado.

2.2 Mecanismos para la participación ciudadana

Los mecanismos de participación ciudadana son los medios a través de los cuales se materializa el derecho fundamental a la participación democrática, y permiten la intervención de los ciudadanos en la conformación, ejercicio y control del poder político.

En el ámbito de la Comunidad Autónoma de Canarias la participación ciudadana viene regulada por la ley 5/2010, de 21 de junio, Canaria de Fomento a la Participación ciudadana [8].

La citada norma establece como mecanismos de participación ciudadana los siguientes:

- **Consultas a la ciudadanía.** El Gobierno podrá, a instancias del presidente, recabar la opinión de la ciudadanía sobre asuntos de interés general de competencia autonómica, mediante sondeos, encuestas o cualquier otro instrumento de participación ciudadana.

- **Foros de consulta.** Espacios de debate y análisis de las políticas públicas, de carácter orgánico, que se establezcan por la administración con el objetivo de obtener de forma dinámica y actualizada opiniones, propuestas o críticas a las diferentes iniciativas de actuación pública, tanto en la fase de elaboración como con posterioridad a su implementación en procesos de carácter evaluativo.

- **Paneles ciudadanos.** Espacios de información constante e inmediata que se crean con carácter temporal, sobre cuestiones de interés para la ciudadanía, en temas de gestión pública, mediante los que la Administración informa o realiza consultas relacionadas con cualquier asunto de interés público.

- **Jurados ciudadanos.** Su función es valorar la eficacia y el resultado de una iniciativa concreta o un programa de actuación llevada a cabo por la Administración Pública.

- **Otros órganos de participación ciudadana.** Desempeñan funciones de información y asesoramiento de los organismos e instituciones de los diferentes poderes públicos y de la propia ciudadanía. En ningún caso tendrán competencias decisorias.

2.3 Aplicaciones y tecnologías para la participación

La implementación de nuevas tecnologías en la gestión pública puede incrementar la participación y colaboración ciudadana en la gestión de los servicios públicos.

En el ámbito nacional podemos encontrar diferentes aplicaciones diseñadas como herramientas para fomentar la participación ciudadana. A continuación describimos algunas de ellas, las cuales se han puesto en marcha en algunas Comunidades Autónomas y Ayuntamientos y también algunas iniciativas privadas que han desarrollado aplicaciones para prestar servicios en este ámbito.

2.3.1 Herramientas tecnológicas

La implementación de nuevas tecnologías en la gestión pública puede incrementar la participación y colaboración ciudadana en la gestión de los servicios públicos.

Algunas herramientas que pueden allanar el camino para el Gobierno Abierto [9]:

- **Escucha activa.** Herramienta en la que los ciudadanos vierten su opinión o soluciones a cualquier situación pública. Se trata de recursos como blogs, redes sociales y aparición en medios de comunicación.

- **Distribución de eventos.** Facilitar la presencia virtual en acontecimientos o debates públicos (plenos, presentaciones de proyectos, etc.) Una de las soluciones más utilizadas es el streaming.

- **Colaboración.** A través de apps donde los ciudadanos puedan comunicar una incidencia, como por ejemplo, las malas condiciones del mobiliario público.

- **Voto electrónico.** Sistemas formales de voto o con herramientas que permitan pulsar la opinión pública

- **CRM y ticketing.** Se busca atender y gestionar las opiniones de los ciudadanos. Estos incluyen:

    - **CRM.** Basado en el modelo de gestión orientado al cliente de toda la organización, en este caso el ciudadano.

    - **Ticketing.** Herramienta de gestión de incidencias para facilitar el manejo de solicitudes o incidencias.

- **Portales de participación.** Son el principal canal de comunicación. La mayoría de estos se realizan a través de los sitios web de las Administraciones públicas, que incluyen mecanismos de apoyo para la comunicación sencilla con el público.

2.3.2 Aplicaciones

En este apartado se describen algunas aplicaciones móviles actuales que fomentan la participación ciudadana, de las cuales se han llevado a cabo un estudio e investigación como referencia para este proyecto algunas de las más importantes son [10] :

Arrels Localizador (España). Su objetivo es facilitar el trabajo a los equipos de asistencia a personas sin hogar, gracias a la participación ciudadana. Desde la app, cualquier usuario puede informar de la localización de personas que pasan la noche a la intemperie para que los equipos de la Fundación puedan asistirlas.

Agenda de Comunicación (España). Informa acerca de los contactos y eventos de instituciones públicas como los ministerios, las entidades de las comunidades autónomas y la administración local, hasta los contactos de la prensa nacional y extranjera, partidos políticos y embajadas, entre otras entidades relevantes.

Ojo con el voto (Argentina). Esta herramienta móvil es una iniciativa para incentivar a la ciudadanía a ejercer el papel de observador electoral durante las elecciones en Argentina. Esta app pretende evitar el fraude electoral e implicar al ciudadano a través de la realización de reportes sobre incidencias en el proceso electoral, como la falta de papeletas o problemas con las autoridades de las mesas. Garantizando la calidad del proceso electoral y el cumplimiento de las leyes.

Mapee (Colombia). El objetivo de esta app es convertir al ciudadano en un actor activo del proceso electoral. Su uso es bastante sencillo: el usuario solo necesita fotografiar y geolocalizar la propaganda difundida por los partidos y candidatos políticos para generar un mapa colaborativo en el que se visualiza la cantidad y tipo de publicidad política usada en cada espacio. Funciona como mecanismo de control para comprobar que las campañas cumplen con los topes máximos impuestos, comparando los gastos de publicidad registrados por los candidatos

Cityzn. Permite que los habitantes de las ciudades aporten ideas para fomentar el bienestar común y facilitar el consenso entre vecinos y comunidades. La app permite realizar presupuestos participativos, propuestas ciudadanas, declaración de incidencias y aportar soluciones basadas en las dinámicas de cocreación vecinal.

YoVeoVeo (Ecuador). Con el objetivo de reducir el exceso de burocracia e incentivar al

ciudadano a denunciar incidencias a la administración nació esta app en Ecuador, que sirve de canal directo de comunicación entre el gobierno y los ciudadanos comprometidos con la gestión pública.

Hackity App. Esta herramienta digital sirve de plataforma para que los ciudadanos puedan gestionar el espacio público informando de incidencias de su entorno y aportando propuestas e ideas para solventarlo. Un usuario puede subir una foto desde el móvil acompañada de una breve descripción del problema y, posteriormente, desde la plataforma se facilita que el resto de usuarios aporten ideas y comentarios para encontrar la solución más adecuada. Las propuestas que más apoyos reciban desde la app será comunicada a la administración pública correspondiente, para que se lleven a cabo las medidas propuestas por los usuarios.

Civic Triage. Nació con el objetivo de optimizar las relaciones y la comunicación entre los ciudadanos y el gobierno. La app sirve para mejorar la calidad y el tiempo de respuesta a las peticiones y solicitudes de los ciudadanos. Gracias al uso de metadatos, la respuesta de la administración se adapta a las necesidades de los usuarios, mejorando la responsabilidad de las entidades y humanizando los procesos burocráticos.

El empleo de la inteligencia artificial a través de esta app permite tratar los temas relevantes para la ciudadanía de manera más personalizada, de modo que el sector público puede ser más eficiente y ganar calidad en la atención al público.

SC Mejora(España) [11]**.** Esta app del Ayuntamiento de Santa Cruz de Tenerife permite enviar avisos, directamente al personal responsable encargado del mantenimiento de los espacios públicos municipales, de cualquier incidencia relacionada con alumbrado, calles, jardines, limpieza, mobiliario, señales u otros. De forma rápida e intuitiva, permite a los ciudadanos en pocos pasos dar de alta y enviar los avisos. Incluye geolocalización, descripción de la incidencia y la posibilidad de aportar imágenes.

Una vez analizadas y estudiadas estas aplicaciones móviles de participación ciudadana, destacan elementos comunes como el hecho de enviar incidencias de diferentes tipos, como son aquellas para comprobar que los partidos políticos llevan a cabo el uso del presupuesto permitido correctamente en sus campañas, hasta incidencias de servicio municipal para mejorar el bienestar de los ciudadanos, así como la aportación de ideas, todas estas acompañadas con una breve descripción y una geolocalización para comprobar de donde es la incidencia que les corresponde.Todo ello con la finalidad de mantener informado a la ciudadanía.

2.4 Propuesta de trabajo

La participación ciudadana no alcanza el protagonismo requerido, concretamente, en períodos en los que se excava la confianza de los ciudadanos en las instituciones y cuando se derrumba el crédito público de los partidos políticos (y por ende de los representantes del sistema), especialmente, en esos períodos [12].

Nos encontramos con una gran capacidad de conectar la Blockchain como herramienta a utilizar en la participación ciudadana.

Este proyecto pretende adentrarse en el uso de blockchain en los mecanismos de participación. Podemos aprovechar esta tecnología para la gestión de incidencias que pueden

comunicar los ciudadanos a través de una aplicación móvil conectada a la Blockchain. Hechos como, garantizar la transparencia, la seguridad de los datos y procesos de la participación ciudadana son algunos de los aspectos a tener en cuenta..

La ciudadanía requiere una nueva forma de participación. De esta forma, ya sea individual o colectiva, estos tienen más importancia en la toma de decisiones de políticas públicas y servicios. Las ciudades inteligentes representan un estímulo que pueden generar una nueva ciudadanía. Aquí es donde entra Blockchain ya que posee características de interés para su utilización, entre ellas están la transparencia, la seguridad y consenso.

De todo esto se deduce, las siguientes cuestiones a tener en cuenta en el desarrollo de herramientas para la participación y en particular en este proyecto :

- La confidencialidad y veracidad de la información, vinculado a la autoría de la transacción.
- Los mecanismos de identificación que permitan controlar y autentificar a los ciudadanos por medio de la Blockchain (Identidad Digital).
- El desarrollo de contratos inteligentes para resolver y automatizar determinados procedimientos de la administración.
- El tipo de Blockchain necesaria a utilizar (pública o privada) en la Administración Pública.
- El tipo de algoritmos de consenso ha de utilizarse y para qué ámbitos.
- La información que se tokeniza en diferentes proyectos.
- Asegurar los principios de participación ciudadana a través de esta tecnología.
- El papel desempeñan las Administraciones Públicas en la Blockchain para fomentar la participación ciudadana.

Capítulo 3 Tecnologías Blockchain, características, componentes

Una Blockchain [13] es un registro de información distribuida, de forma que todas las entidades de negocio comparten el mismo registro. La propia tecnología es en sí misma un protocolo que garantiza el funcionamiento del sistema. Es decir, la información se comparte siguiendo todos las mismas reglas, y garantizando que si alguien no las cumple, es fácilmente identificable por el resto de intervinientes del sistema.

3.1 Historia

La tecnología Blockchain surgió buscando soluciones de comercio electrónico sin la necesidad de un tercero confiable.

Nació de la propuesta de implementar Bitcoin en octubre de 2008 y se implementó utilizando la criptomoneda por primera vez el 9 de enero de 2009. Sin embargo, la tecnología en sí, se basa en un conjunto de algoritmos y otras tecnologías existentes.

Se basa en el protocolo de telecomunicaciones utilizado en Internet, que se ha desarrollado desde principios de la década de 1970. En cuanto al algoritmo de consenso, el utilizado por Bitcoin para la prueba de trabajo se llama HashCash, que se discutirá más adelante, era una fórmula y se utilizó durante 1997 para combatir el spam. La criptografía asimétrica es la base de los mecanismos de cifrado y firma electrónica utilizados en todas las cadenas de bloques y se inventó en 1976. Estos

son solo algunos ejemplos, que muestran que el nacimiento de la tecnología Blockchain fue una verdadera innovación en ese momento.

Aunque su creador lo contextualiza en el desarrollo del sistema de moneda electrónica (según el artículo original de Bitcoin [14]), todo se descubrió rápidamente. Con la capacidad de aplicarla a múltiples casos de uso mediante la ejecución de código integrado (llamados contratos inteligentes) en la propia plataforma.

La primera plataforma que proporcionó esta utilidad fue Ethereum en 2013. Hoy en día, el ecosistema tecnológico que rodea a la cadena de bloques es muy grande y crece exponencialmente.

3.2 Características

La característica principal de la Blockchain se basa en la unidad de datos principal, los bloques. Los nodos se enfocan en construir y verificar estos bloques usando algoritmos de consenso.

A continuación en los siguientes apartados se explicarán los elementos de la Blockchain con el fin de detallar el funcionamiento de esta tecnología.

3.2.1 Tipos de Blockchain.

Existen dos grandes clasificaciones:

- Públicas y privadas
- Permisionadas y no permisionadas

Las redes públicas de blockchain son aquellas en las que cualquier persona o entidad puede hacer uso o formar parte de ella, es decir, podría implantar un nodo y colaborar en la consecución de los objetivos de la red. Por ende, los participantes de dichas redes no tienen porqué conocerse entre ellos y mucho menos confiar los unos en los otros. Por ejemplo Bitcoin o Ethereum.

Las redes privadas de blockchain son aquellas en la que para participar de ellas se debe tener autorización expresa por parte de los “propietarios”. Por lo tanto, no todo el mundo puede formar parte de la red.

La segunda gran clasificación está relacionada con la privacidad de la información. Una Blockchain se considera no permisionada, cuando cualquier participante puede leer o escribir en la red, es decir que, pueda ejecutar transacciones en la red, sin perjuicio de los controles que puedan existir durante la ejecución de los contratos inteligentes.

Por contra, en las redes permisionadas, la propia plataforma establece las condiciones bajo las que un participante puede realizar una determinada operación.

Algunas blockchain pueden ser consideradas públicas-permisionadas, combinando los permisos asociados a consorcios privados, con un modelo de gobierno descentralizado, intentando alcanzar las mejores características de ambos modelos.

También es posible la implantación de una blockchain privada-no permisionada, es decir, una versión de una plataforma en la que cualquiera pudiera operar (leer o escribir), pero que no todo el mundo tuviera acceso a ella.

3.2.2 Algoritmo de consenso.

El consenso en una red blockchain se refiere al proceso de lograr un acuerdo entre los participantes de la red en lo que respecta al estado de los datos del sistema. El consenso lleva a que todos los nodos compartan exactamente los mismos datos.

El algoritmo de consenso da respuesta al problema de encontrar un plan de acción común, a partir de una estructura jerárquica, donde uno de los sistemas que tiene mayor rango proporciona una orden a partir de la cual el resto de sistemas tiene que operar.

Por lo tanto, hace dos cosas: asegura que los datos del registro distribuido sean los mismos para todos los nodos en la red y, a su vez, evita que los actores maliciosos manipulen los datos.

El algoritmo de consenso varía con diferentes implementaciones de blockchain. Mientras que Bitcoin usa Prueba de Trabajo (en inglés Proof of Work o PoW), otras blockchain usan Prueba de Participación (Proof of Stake o PoS), Prueba de paso de Tiempo (Proof of Elapsed Time o PoET), Practical Bizantine Fault Tolerance (PBFT), o muchos otros dependiendo de los requisitos específicos de la red.

Los mencionados algoritmos de consenso cobran sentido cuando los participantes de la red blockchain no se conocen o no confían entre ellos. En las plataformas privadas de blockchain lo más habitual es que haya confianza entre los participantes (bien porque todos los nodos pertenecen a la misma compañía), o porque existen acuerdos de colaboración entre las diferentes organizaciones.

3.2.3 Hashing

El **hash** se refiere al proceso de generar una salida de longitud fija a partir de una entrada de longitud variable. Esto se puede lograr utilizando una fórmula matemática llamada función hash (implementada como un algoritmo hash).

Las funciones hash tienen propiedades matemáticas importantes, una de ellas es que son unidireccionales, es decir, la misma entrada siempre resultará en la misma salida. Aunque se proporciona la salida, no se puede determinar la entrada correspondiente. El hecho de que dos o más entradas produzcan el mismo valor de salida se denomina conflicto, que es un problema muy grave para los sistemas que utilizan este algoritmo.

Sin embargo, existen muchos algoritmos hash, como MD5 [15] (que se ha considerado inseguro durante mucho tiempo) o diferentes versiones del algoritmo SHA, como SHA-256, SHA-384 y SHA-512 (todo ellos dependiendo de la longitud del salida generada), actualmente, este último se considera el algoritmo hash más utilizado.

3.2.4 Transacciones

Las operaciones que se realizan para agregar información a una Blockchain son denominadas transacciones. Una transacción puede ser simplemente una línea de texto, o un hash de un documento almacenado fuera de la cadena de bloques. Las transacciones contienen los siguientes elementos:

- **Hash:** el resultado de aplicar el algoritmo hash al resto de los datos de la transacción.
- **Inputs:** datos de entrada de la transacción. Puede incluir el método de contrato inteligente que se llamará, los datos de entrada proporcionados, la cuenta utilizada,

etc.

- **Outputs:** para transacciones de divisas (criptomonedas), pueden incluir la distribución de importes en diferentes cuentas objetivo.
- **Timestamp:** Momento en el que se creó la transacción.
- **Memo:** otra información de interés, como firmas digitales asociadas a operaciones.

Por lo tanto, cualquier persona que desee ejecutar una transacción en la cadena de bloques debe construir una estructura de datos similar, firmar electrónicamente la transacción (para asegurarse de que se haya creado) y luego enviarla a cualquier parte del nodo de la red de cadena de bloques blockchain (en el caso de redes privadas, a un nodo en la que tengan permisos).

Una vez realizada las transacciones se empiezan a construir los bloques.

3.2.5 Bloques

Un bloque es una estructura de datos que incluye un conjunto de transacciones (pueden ser más de una o ni siquiera una).

La raíz del árbol de Merkel [16] (nombre que se le atribuye a la estructura construida a partir del cálculo de los hash de un conjunto de datos o transacciones),indica otro timestamp (indicando el momento de construcción del bloque), un nonce, es el hash de todo el bloque, y lo más importante el hash del bloque anterior (porque esto es lo que le da a la estructura de datos forma de cadena y le asigna su nombre a la tecnología Blockchain).

El nonce (asumiendo que la red usa PoW) es el resultado del proceso de minería del bloque, es decir, es el valor obtenido después de que se ejecuta el algoritmo de prueba de trabajo en todas las transacciones del bloque. Solo sabemos que es una prueba fehaciente de que el nodo ha realizado la prueba de trabajo (minado), por lo que tiene derecho a publicar el bloque en la red. Los bloques construidos (extraídos) de esta manera no se escribirán directamente en la cadena de bloques, sino que se enviarán a todos los nodos para su verificación. En el momento de que un nodo reciba un bloque minado de otro nodo, lo verifica utilizando el nonce previsto (para saber que el nodo ejecutó la prueba de trabajo) y calculando el árbol de Merkle de las transacciones para comprobar que coincide con el informado. En caso de superar la verificación, el nodo detiene cualquier proceso de minado que pudiera estar ejecutando, procede a escribir el bloque en su copia de la blockchain, y comienza un nuevo proceso de minado con nuevas transacciones.

De esta forma, se realiza un proceso cíclico en el que las transacciones se restauran continuamente para ser incluidas en los bloques potenciales que deben ser extraídos y verificados por todos los nodos de la red.

3.3 Componentes

Entre los principales componentes comunes de una Blockchain destacan los siguientes:

- **Consenso**. Todos los nodos de la red deben llegar a un consenso sobre cómo verificar la transacción, ya sea por mayoría o por otros algoritmos seleccionados entre posibles transacciones
- **Nodos**. No hay red sin un conjunto de servidores interconectados. Los nodos pueden desempeñar diferentes roles según la topología y la plataforma Blockchain utilizada, fundamentalmente verifican y ejecutan transacciones.

- **Cadena de bloques**. Es lo que le da nombre a la Blockchain. El sistema de registro de todas las transacciones es inmutable, compartido por toda la red (o por personas con derechos de acceso en una red privada) y cada nodo mantiene su propia copia.
- **Seguridad**. La Blockchain utiliza una gran cantidad de tecnologías de encriptación para mantener las características de inmutabilidad, permitir la autenticación, autorización del usuario (en una red privada), la aplicación de políticas, listas de control de acceso (ACL) y muchas más. Son estas medidas de seguridad las que generan la confianza necesaria entre los participantes de la red para que puedan participar en cada caso donde se garantice la transparencia y la privacidad.
- **Contratos inteligentes.** En estos reside la lógica de negocio que manipula el estado de la cadena de bloques.. Son códigos asociados a programas desplegados en la red Blockchain utilizando transacciones de despliegue. Por lo tanto, son tan seguros como lo sea él código del programa. En general, siempre es necesario producir código de alta calidad, y haber pasado todos los niveles de prueba recomendados en el desarrollo de software.
- **Tokens.** Son los activos digitales o criptográficos que pueden ser el reflejo de un activo real subyacente.

3.4 Hyperledger

Hyperledger [17] es un proyecto open source creado por la Fundación Linux con la idea de permitir la utilización de la Blockchain más allá de las criptomonedas. Desarrollando estándares, herramientas y comunidades. Este proyecto ya cuenta con empresas participantes tanto como empresas financieras y empresas de tecnología de cadena de suministros.

Hyperledger crea blockchain para ser usadas en un entorno privado y que estén comunicados entre empresas con todo el poder que da una base de datos distribuida, inmutable y cifrada. Dentro de esta gran iniciativa se encuentran separados dos grandes bloques de proyectos: los frameworks y las herramientas dentro de los frameworks.

3.4.1 Características

- **Frameworks.** Se tratan de enfoques significativamente diferenciados para los marcos de negocios de blockchain desarrollados por una creciente comunidad. Dentro de los frameworks tenemos los siguientes:

  - ☐ **Hyperledger Fabric**. Plataforma de libro mayor abierta y probada a nivel empresarial y distribuida. Tiene controles de privacidad avanzados, por lo que solo los datos que quiere compartir se comparten entre los participantes de la red "autorizados" (conocidos). En el siguiente apartado hablaremos más sobre este Framework.
  - ☐ **Hyperledger Indy.** Ha sido diseñado para llevar lo que es la entidad descentralizada, es decir descentralizar tu información personal y decidir a quiénes se las puede dejar y a quienes no y hasta ganar dinero por ello.
  - ☐ **Hyperledger Iroha.** Su idea principal es poder crear rápidamente cadenas de bloques y operar en ellas desde dispositivos móviles, tiene disponible bibliotecas para Android y también para IOS.
  - ☐ **Hyperledger Sawtooth.** Su característica principal es que su consenso es el de "Proof of Elapsed Time", esto es una prueba de tiempo,que evita el consumo de cpu como va a ser la blockchain de Bitcoin que tiene otro consenso. Destaca por como se separa la

capa de la aplicación con la capa de lógica de negocio, permitiendo programar en muchos más lenguajes y tiene características muy interesantes como soportar transacciones paralelas.

- ☐ **Hyperledger Burrow.** Utiliza la máquina virtual de Ethereum y su forma de comunicarse con las aplicaciones mediante el RPC se programa mediante Solidity y utiliza toda la tecnología de Ethereum que tenemos actualmente .

Estos cinco frameworks lo que te permiten es crear las Blockchain dependiendo de la necesidad del negocio o de la red de negocio que vayas a crear.

● **Herramientas.** Normalmente construido para un framework, y a través del enfoque de licencias comunes, adaptado a otros frameworks. Dentro de las herramientas podemos encontrar:

- ☐ **Hyperledger Composer (descontinuada desde 2019).** Se trata de la herramienta principal que nos permite crear los contratos inteligentes mediante Javascript y brinda una API con las tareas más comunes que se realizan para tener una programación más rápida. Cabe señalar que los contratos inteligentes en Hyperledger Fabric se llaman chaincode y se programan en lenguaje Go, como no muchos lo conocen pues, Hyperledger Composer facilita pudiendo programar directamente en un lenguaje como Javascript.
- ☐ **Hyperledger Cello.** Permite crear una Blockchain bajo demanda, la idea es que se despliegue en la nube y sea como un servicio. Por ejemplo un entorno SAS que es un "Software as a Service" pues en este caso sería un BAR que es un "Blockchain as a Service".
- ☐ **Hyperledger Explorer.** Permite visualizar las operaciones de la Blockchain, es una aplicación web para monitorear cada movimiento es muy bueno para hacer una auditoría y para tener un dashboard de todo el movimiento de tu red.

3.4.2 Hyperledger Fabric

Una de las características principales que se encuentran en Hyperledger Fabric es que su Blockchain es permisionada, esto quiere decir que los nodos que pertenecen a esa red no necesariamente tienen acceso a toda la Blockchain. La idea de tener una Blockchain privada es justamente que prevalezca una confianza entre los nodos, porque ellos se conocen, entonces esta red no es anónima.

Se manejan diferentes tipos de consenso, esto depende del administrador que escoja. Tiene canales, eso quiere decir que permite tener más cadenas de bloques independientes dentro de una Blockchain, es decir, dentro de una Blockchain principal se pueden tener otros canales de comunicación para que no todos los nodos se comunicarán entre ellos.

Maneja tres tipos de nodos: el commit, cambia el bloque situándose dentro de la Blockchain, los que validan la información antes de que pertenezca al bloque y los que ordenan los bloques.

No existe la minería como en el Bitcoin, aquí directamente cada nodo tiene una función y la ejecuta, no hay recompensa por ejecutar las transacciones. Las transacciones son ejecutadas sin necesidad de tener asociadas una criptomoneda.

Tiene una base de datos adicional llamada World State que guarda el estado actual de la Blockchain y se utiliza para realizar consultas mucho más rápidas, que recorrer cada uno de los bloques. La Blockchain es la entrada y el World State es la salida.

Maneja criptografía y certificados digitales, las políticas son configurables, es posible definir qué se tiene que cumplir y por qué validaciones tiene que pasar una transacción. Para agregar un bloque posee un SDK (Software Development Kit) [18].

Hyperledger Fabric es de código abierto, así que muchas empresas que están involucradas en el proyecto general del Hyperledger hacen que sea sólido, que tenga una forma de estandarización y todas las transacciones son encriptadas, con lo cual se asegura que todos los nodos les llegue la información correcta.

3.4.3 Hyperledger Composer

Es una herramienta de código abierto que permite el desarrollo de aplicaciones Blockchain sobre Hyperledger Fabric de una manera rápida y simple, sin la necesidad de conocer mucho del mundo de Blockchain. Esta herramienta dejo de desarrollarse desde 2019, pero sirve para el desarrollo de prototipos

El valor de esta herramienta es el de acelerar el desarrollo brindando un API, para no acceder directamente al Hyperledger Fabric, ahorrando tiempo y esfuerzo de hacer una demo con Blockchain creando todos los componentes y conociendo cada término o concepto, pues el Hyperledger Composer te permite realizar demos en unas pocas horas e ir cambiándolo hasta llegar al punto deseado.

El Hyperledger Composer se trata de el framework de desarrollo, Hyperledger Fabric utiliza lenguaje de programación Go ,el cual no es muy conocido, por lo cual el Hyperledger Composer no brinda Javascript.

Dentro de las características principales del Hyperledger Composer tenemos que es un entorno que permite la creación de redes de negocios en alto nivel, permite el modelado pruebas y despliegue del modelo de negocio.

Dentro del modelado se define quiénes son los los activos o assets y las transacciones que se realizan con esos activos, permite a sistemas externos operar con la Blockchain y permite crear los contratos inteligentes mediante Javascript. Destacar que los contratos inteligentes en Hyperledger Fabric se denominan Chaincode.

Algunas características adicionales del Hyperledger Composer son el modelar los datos que se proveerán en la aplicación, un entorno de prueba en línea, paquetes de librerías para los clientes, programas de edición como el Atom o el Visual Studio Code que dispone de un plugin para Hyperledger Composer, con lo cual se hace más sencillo el escribir el código, pues se compila al momento de la digitación y se colorea para una mejor visualización. También posee utilidades de línea de código, generador del código Yeoman [19] con el que se puede crear una maqueta del proyecto web en Angular obteniendo el modelo desde la configuración.

Tiene los componentes a utilizar para empezar con la codificación. El playground se puede utilizar como plantilla, contenedores del Docker [20] para hacer el deploy directamente en nuestras máquinas, la librería Javascript y los entornos de programación con sus respectivos plugins.

En resumen el Hyperledger Composer es un conjunto de librerías o APIs que nos permitirán conectar nuestras aplicaciones con la Blockchain de Hyperledger Fabric entendiendo que la Blockchain es una base de datos distribuida que tiene permisos y transacciones.

3.5 Estado del arte de aplicaciones de la blockchain para la participación

Hoy en día, con la ayuda de Blockchain, se puede construir un sistema descentralizado eliminando la dependencia de agencias intermediarias y agencias centrales. Por ello, se asume que es una tecnología habilitadora que cambiará por completo los métodos y mecanismos de participación existentes [21].

En un proceso participativo deliberativo, como por ejemplo la votación para la elección de un candidato, la votación de un presupuesto participativo, la decisión de un proyecto. En este tipo de escenarios se crean una inmensa cantidad de datos. Estos datos en el contexto actual pueden verse afectados por hackers, caídas de sistemas de almacenamiento y validaciones de un solo sistema. Lo que también repercute en los datos personales de cada ciudadano, como pueden ser su DNI o el domicilio donde residen, a este problema se le puede encontrar una solución en la identidad soberana.

Blockchain, actúa desde el bloque principal hasta la creación de una cadena de bloques para mantener la seguridad y validación del dato. Esto favorece a que no se pueda modificar o alterar los datos obtenidos en el proceso de votación, puesto que automáticamente se podría identificar a través de su Hash.

Pero no todo es seguridad que proporciona esta tecnología. Otras ventajas que han demostrado las aplicaciones actuales de Blockchain en diversas ciudades son el hecho de mayor transparencia e interconectividad. Las ciudades pueden interconectar con la blockchain servicios verticales como la movilidad, la energía o la seguridad a través de un sistema único, abierto, accesible, transversal y capaz de intercambiar datos con sus habitantes en tiempo real.

Por otro lado, una comunicación directa, ya que posibilita que las administraciones públicas y los ciudadanos puedan interactuar de forma digital y sin necesidad de intermediarios permite conocer el origen y destino de cada recurso tanto a ciudadanos como a gobernantes. Además, estos últimos pueden conocer cómo se utilizan los servicios urbanos sin comprometer la privacidad de las personas.

Estas características mencionadas pueden llegar a favorecer la participación ciudadana, debido a la comunicación que se crea entre administración y ciudadano, a través de plataformas digitales, por otro lado asegura una inmutabilidad de los datos (mejor que ninguna otra plataforma tecnológica) y a la vez una transparencia de los mismos, como se menciona anteriormente. Finalmente puede asegurar que todos los procesos participativos que se deseen realizar sean almacenados de forma distribuida o privada y al alcance de todos.

3.5.1 Identidad soberana a través de Blockchain

En este apartado introducimos la identidad soberana. Ya que es uno de los aspectos fundamentales que se relacionan con la confidencialidad,

las preocupaciones actuales de las entidades locales en el uso de las herramientas de participación.

La verificación de la identidad de un ciudadano, la necesitamos en casos como la gestión de incidencias o en procesos de votación, de ahí nace la importancia de la identidad digital, esta

identidad digital se puede implementar de manera certera con tecnología Blockchain.

A día de hoy, nuestros datos personales, al darnos de alta en diferentes servicios y proveedores digitales, no sabemos ni donde se encuentran almacenados. Aceptamos que nuestros datos personales han sido cedidos con nuestro consentimiento a diferentes empresas en situaciones que ni recordamos, y estás se ven legitimadas para tratar nuestra información y en ocasiones compartirla con otros proveedores.

La identidad soberana es una forma de identidad digital en la que los usuarios tienen control total sobre sus datos. Además de poder controlar quién tiene acceso a ellos y en qué condiciones. los ciudadanos se preocupan por su privacidad y el acceso a sus datos en el mundo conectado en el que vivimos.

Blockchain destaca como la mejor base para esta tecnología. Gracias a las propiedades criptográficas, descentralizadas y seguras que posee.

En este sistema, la identidad se almacena en un formato criptográfico protegido por criptografía asimétrica. De esta forma, los usuarios pueden intercambiar datos con terceros de forma segura y sin fugas de datos no deseadas.

Además, el usuario tiene control sobre cada transacción proporcionando información. En esta etapa, cada intercambio de datos se lleva a cabo bajo condiciones especificadas por el usuario. Los usuarios deciden por sí mismos qué información compartir, cuánta y con quién.

Cada participante puede estar de acuerdo o en desacuerdo por consenso si la identidad proporcionada es verdadera o falsa. No hay una autoridad central y no hay nadie que dicte las reglas o acciones de los censores.

Las empresas que gestionan la identidad de sus usuarios saben mejor que nadie que esos datos son su mercancía. Y una solución a esto es: crear sistemas descentralizados para evitar esto. Blockchain es actualmente un sistema que se adapta bien a esta tarea. En este punto, es importante destacar algunos de los proyectos de identificación de soberanía actualmente en desarrollo.

- **NameID**. Es uno de los primeros sistemas de identidad soberana que utiliza Blockchain. Es una cadena de bloques que tiene como objetivo crear un sistema de nombres de dominio descentralizado. O, de manera equivalente, un sistema de identidad de Internet basado en blockchain descentralizado y sin censura.

- **Sovrin.** La red Sovrin busca desarrollar un nuevo estándar para la identidad soberana. Su objetivo es diseñar una identidad soberana fácil de usar como una licencia de conducir o documento de identidad.

- **EBSI(European Blockchain Services Infrastructure)**. La European Blockchain Partnership (EBP) es una iniciativa para desarrollar la estrategia Blockchain de la UE y construir una infraestructura Blockchain para los servicios públicos. Ayuda a evitar la fragmentación del panorama Blockchain al promover una estrecha cooperación entre los países de la UE. La asociación apoya la interoperabilidad y el despliegue generalizado de servicios basados en Blockchain. Proporciona un entorno compatible que cumple totalmente con las regulaciones de la Unión Europea y con estructuras y modelos de gobierno claros para ayudar a Blockchain a prosperar en toda Europa.

Entre los diferentes casos de uso que han desarrollado tienen en sus manos uno sobre identificación auto-soberana. El propósito de este caso de uso es implementar una estructura de Identidad Auto-Soberana (SSI) rica en funciones, definir las especificaciones requeridas y crear servicios y capacidades de soporte que permitan a los ciudadanos crear, administrar y usar sus propias identidades digitales (incluidas las identificación , autenticación y muchos otros tipos de información relacionadas con la identidad) sin tener que depender de una única autoridad central. ESSIF (European Self-Sovereign Identity Framework) es parte de un ecosistema de identidad descentralizado más amplio e interactúa con otros sistemas y plataformas de organizaciones públicas y privadas. Por lo tanto, este caso de uso no solo facilita todo tipo de interacciones digitales entre diferentes partes de los sectores público y privado, sino también procesos entre ciudadanos y administraciones públicas u organizaciones privadas en todos los Estados miembros de la UE.

- **Alastria_ID**. Alastria es una asociación sin ánimo de lucro que promueve la tecnología digital economía a través del desarrollo de tecnología Blockchain. Alastria_ID es un modelo de identidad digital propuesto por el Consorcio para su uso en servicios digitales, inspirado en el concepto Self Sovereign Identity (SSI). El proyecto Alastria_ID está desplegado como una de las aplicaciones básicas de la infraestructura Blockchain promovida por el Consorcio dentro de su plataforma. El protocolo implementa contratos y componentes de software que permiten su integración con backends de diferentes servicios. Todo ello en una app básica, que evoluciona y se adapta con los requerimientos de los usuarios y proveedores. Mediante esta app, y bajo un modelo SSI, los usuarios tienen control sobre las transacciones asociadas a su identidad y pueden acceder a diferentes servicios.

3.5.2 Ejemplos de uso de blockchain en participación ciudadana

A día de hoy, la tecnología Blockchain es utilizada en diferentes países para la participación ciudadana. Destacan [22]:

Canadá. El Consejo Nacional de Investigación de Canadá, a través de su Programa de Asistencia de Investigación Industrial (NRC-IRAP), anunció que ha implementado con éxito su explorador de la blockchain de Ethereum para la administración transparente de subsidios y otras contribuciones del gobierno.

La meta del Consejo es que los usuarios utilicen la plataforma para tener acceso a la información de los subsidios y probar el uso de la tecnología de contabilidad distribuida (DLT) para buscar de forma instantánea las subvenciones en la blockchain de Ethereum.

Estonia. Es el primer país en replantearse cómo sería un gobierno digital en la nube, lanzando la iniciativa de e-residency, que es un modelo de identidad digital transnacional que permite, con independencia del país europeo en el que residas, acceder a un amplio espectro de servicios legales, de registro, de voto y firma. Los servicios son gestionados por la propia plataforma de Estonia.

Igualmente se ha desarrollado un servicio de gestión de registros médicos electrónicos, que cuenta con la capacidad de unificar en un registro de salud único la información disipada a lo largo de los diferentes proveedores de servicios de salud, así como un modelo de votación online en juntas de accionistas que no requiere de presencia física.

Suecia, Honduras y Georgia. Están haciendo uso de la Blockchain para registros públicos,

partiendo del registro de la propiedad de tierras.

Tomando un enfoque más amplio, el gobierno de Dubái lanzó una iniciativa llamada “ Smart Dubai ”, que aboga por transferir toda la información existente a blockchain antes del año 2020, con objeto de facilitar el acceso y gestión de la misma. Su objetivo es proponer un modelo de gobierno más eficiente, que reemplace los procesos basados en papel o comunicación por fax o teléfono por documentos digitales y contratos inteligentes, que permitan facilitar la trazabilidad y la gestión del envío de bienes y mercancías.

En definitiva, blockchain permitirá a los ciudadanos disponer del pleno control sobre su información y voluntad de acción, con modelos de gobierno representativos y personalizados en el que los ciudadanos pueden escoger aquellos servicios en un contexto global, que mejor se adapten a sus necesidades y mejoren su calidad de vida.

También podemos encontrar diferentes ejemplos relacionados con la participación ciudadana y Blockchain en nuestro país como:

- **Alcobendas.** El Ayuntamiento de Alcobendas, en España, suscribió un convenio con la asociación sin ánimo de lucro Alastria (mencionado en el apartado anterior), por el que ambas entidades fomentarán el desarrollo a través de la tecnología Blockchain. El acuerdo incluía acciones para dar a conocer la tecnología Blockchain en el ecosistema digital de la región. Con esta iniciativa, se prevé que la Administración autonómica pudiera crear su propio nodo de blockchain en la red de Alastria. El objetivo es que, desde Galicia, se puedan generar pilotos con esta tecnología al servicio de la investigación, la formación y la experimentación.

- **Gobierno Vasco.** Tiene como objetivo la realización de los servicios de análisis, desarrollo e implantación de una solución Blockchain para cubrir escenarios ligados al registro de contratistas del Gobierno Vasco. Desde un punto de vista funcional el plan consiste en:

  - Los proveedores aportan documentos al registro relativos a su actividad profesional y económica.

  - Los proveedores presentan ofertas a ofertas públicas sin aportar documentos relativos a certificaciones.

  - Las diferentes entidades públicas consultan el registro para comprobar que los proveedores disponen de las certificaciones requeridas.

- **Cabildo de Tenerife.** Ha implantado en la biblioteca TEA (Tenerife Espacio de las Artes) y de forma experimental un sistema de autenticación basado en la tecnología Blockchain que permite el acceso a cualquier aplicación haciendo uso único de un dispositivo móvil. También es un facilitador para la prestación de servicios complementarios, como por ejemplo servicios de pago o recompensa.

- **Gobierno de Aragón.** Se trata de un sistema para la presentación de documentos asociados a procesos de contratación pública en el que lo que se presenta es la huella electrónica de los documentos (no los documentos en sí). Se utiliza blockchain como plataforma distribuida que garantiza la inmutabilidad y auditoría de la información. El sistema además permite que la Administración, una vez finalizado el plazo de presentación de documentos, pueda verificar

los documentos originales con las huellas electrónicas presentadas.

Capítulo 4 Diseño conceptual y prototipado

Este capítulo contiene el diseño conceptual y prototipado. Se describe un diseño conceptual de una aplicación móvil que recoja incidencias ciudadanas con el uso de la Blockchain, incluyendo en el proyecto una demo a través de Hyperledger Composer. Junto con una propuesta para conseguir conectar la aplicación móvil de incidencias con la red de Blockchain que se encuentre desplegada en las infraestructuras informáticas de un ayuntamiento (como ya nombrados en el capítulo uno tomamos de referencia el ayuntamiento de Santa Cruz de Tenerife) y llevar el proyecto a una mayor escala, en la cual a través de la aplicación los usuarios no solo podrán mandar incidencias, sino que podrán conectarse a la sede electrónica del portal de participación ciudadana que disponga un ayuntamiento y podrán realizar diferentes trámites que ofrece este mismo a través de la aplicación y queden almacenados en la Blockchain, además de tener la posibilidad de llevar a cabo un proceso de autentificación de los ciudadanos a través de EBSI.

4.1 Descripción de la aplicación

Se trata de un prototipado de aplicación móvil, ya que es una tecnología accesible para cualquier ciudadano con la cual poder fomentar la participación ciudadana junto con la gobernanza inteligente y con ello poder llevar a cabo el desarrollo de una ciudad inteligente capaz de gestionar el conocimiento que diferentes usuarios quieran compartir en la red sobre la ciudad en la que viven, además de sentirse partícipes del desarrollo, lo cual permitirá que otros usuarios puedan beneficiarse de ese servicio.

Con la aplicación se podrá ofrecer diferentes tipos de incidencias en la vía pública, de forma rápida, fácil y cómoda, localizar tu ubicación y avisar el lugar exacto donde se produce un incidente, comprobar los avisos que hayas enviado y ver en cualquier momento el estado de la resolución.Todo ello apoyado en Blockchain.

4.1.1 Características de la aplicación

La principal característica que tendrá la aplicación, tratará de que de momento las incidencias que se realicen a través de ella pasarán y serán almacenados en una Blockchain privada que en este caso la maneja el correspondiente ayuntamiento. Del prototipo se destacan las siguientes características:

1. **Autenticación del usuario.** la información confidencial que rellene el usuario, será inmutable, replicada y cifrada en un nodo que tendrá el ayuntamiento. Este proceso se realiza con una plataforma que facilita la identidad soberana.
2. **Reporte de Incidencias:** deberá especificar el tipo de incidencia, una breve descripción (de manera opcional) e incorporar una fotografía.
3. **Almacenaje de Incidencias:** el usuario podrá consultar todas las incidencias que ha remitido y podrá comprobar también no solo la suya, sino también las que han sido reportadas por el resto de la ciudadanía
4. **Geolocalización:** la aplicación ubicará automáticamente el mapa sobre su posición actual para que pueda remitir una incidencia desde el lugar en el que se encuentra. También puede realizar una fotografía y, con posterioridad, remitir señalando manualmente su ubicación en

el mapa.

5. **Seguridad:** la criptografía que ofrece Blockchain es un pilar fundamental en el funcionamiento de la cadena de bloques,aporta seguridad sobre las incidencias que se almacenarán**.**
6. **Transparencia:** la aplicación ofrece la situación en la que se encuentran todas las incidencias tanto las propias como las reportadas por otros ciudadanos así como su estado de resolución. Seleccionando cada una de ellas se podrá ver el detalle de las mismas y los comentarios específicos de los técnicos de mantenimiento del Ayuntamiento en el caso de que los hubiesen introducido

4.2 Tecnologías

En el diseño tanto del prototipo de la aplicación como el diseño de la arquitectura, junto con la demo en Blockchain se han utilizado las siguientes tecnologías:

- **Hyperledger Fabric:** plataforma de tecnología de libro mayor distribuido (DLT) de código abierto y de grado empresarial, diseñada para su uso en contextos empresariales, que ofrece algunas capacidades de diferenciación clave sobre otras plataformas populares de contabilidad distribuida o blockchain.
- **Hyperledger Composer:** conjunto de herramientas de Hyperledger que utilizan JavaScript para facilitar la creación de aplicaciones de blockchain de Hyperledger Fabric.
- **Javascript**: lenguaje de programación interpretado, dialecto del estándar ECMAScript. Se define como orientado a objetos, basado en prototipos, imperativo, débilmente tipado y dinámico.
- **Archimate**: Lenguaje de modelado de arquitectura de software empresarial abierto e independiente para soportar la descripción, análisis y visualización de la arquitectura dentro y entre dominios comercialesde una manera inequívoca. Es un tipo de lenguaje descriptor de arquitectura.
- **Visual Studio Code (Plugin Hyperledger Composer)**: Esta extensión VSCode analiza archivos '.cto' utilizando el analizador Hyperledger Composer e informa cualquier error de validación. También analizará y validará los archivos 'permissions.acl' de Hyperledger Composer y los archivos de consulta ('.qry'). Para trabajar con modelos que utilizan importaciones y abarcan varios archivos, debe abrir todos los archivos relacionados. Para validar el archivo ACL y los archivos de consulta, también se deben abrir los archivos de modelo correspondientes.
- **Justinmind**: Herramienta de creación de prototipos y wireframing para la creación de prototipos de alta fidelidad de aplicaciones web y móviles. Es conocido por su capacidad para generar versiones realistas de un producto terminado, además de ofrecer funciones de colaboración, interacción y diseño.

4.3 Diseño y desarrollo

Antes de adentrarnos y explicar la arquitectura propuesta, debemos mencionar uno de los procesos o componentes necesarios para dar garantías autentificación de los usuarios de la aplicación. En este proceso el usuario normalmente se registraría en el portal de participación de un ayuntamiento, en nuestro caso al tomar de referencia el Ayuntamiento de Santa Cruz de Tenerife. En este caso los usuarios se registran en la página web oficial del Ayuntamiento, este registro puede ser a través de Facebook, Twitter o creando un nuevo usuario a través de un correo electrónico y una contraseña. Esto genera problemas de veracidad de los datos y la autenticación del ciudadano, es decir si pertenece realmente a Santa Cruz de Tenerife junto con la posibilidad de crear una cantidad ilimitada de cuentas. Por otro lado, con este proceso, los usuarios no mantienen su privacidad y

anonimato. Por ello se plantea el uso de la identidad soberana como solución a este problema. A través de EBSI (mencionado anteriormente en el documento) se verifica a los ciudadanos como personas reales, pertenecientes al Ayuntamiento de Santa Cruz de Tenerife, manteniendo su anonimato.

Para usar el sistema de identidad digital de EBSI los ciudadanos deben tener en cuenta el uso de una nueva billetera digital. Deben configurar su billetera y solicitar una identificación verificable de la Autoridad de registro de confianza (TAR), en este caso la Unión Europea.

Descargan la billetera y la configuran. Crean su DID (identificador descentralizado) protegido por una clave privada. Solo el propietario de la clave privada puede demostrar que posee o controla su identidad y lo guarda de forma segura en su billetera junto con sus claves públicas/privadas asociadas. Finalmente solicita el registro del DID en el libro mayor de EBSI.

La Autoridad de Registro de Confianza ayuda en el registro del DID incluyendo la clave pública en el Libro mayor de EBSI, emite una identificación verificable y se la envía al ciudadano. El ciudadano obtiene la identificación verificable y la almacena en su cartera digital

El ayuntamiento también deberá incorporarse a EBSI. El proceso es el mismo que para los ciudadanos. Una vez que se produce la incorporación, una entidad jurídica puede comenzar a emitir y verificar/consumir datos (personales), en forma de Credenciales verificables (VC), para facilitar las interacciones (digitales) con otras partes, en particular la prestación de servicios.

Como resultado final se ha configurado una Entrise Wallet, la entidad jurídica crea y almacena de forma segura los DID y la claves pública/privada asociada, esos DID quedan registrados en el libro mayor de EBSI. Ahora al acceder al portal del ayuntamiento accederán a través de este DID.

4.3.1 Arquitectura

La arquitectura elaborada en este proyecto, se ha planteado como una propuesta para conseguir conectar la aplicación móvil de incidencias con la red de Blockchain que se encuentre desplegada en las infraestructuras informáticas de un ayuntamiento.

Se trata de un arquitectura más general, que pretende no sólo conectar con la aplicación actual de incidencias, sino que en un futuro esta aplicación pueda conectarse a la sede electrónica del portal de participación de un ayuntamiento y a través de esta poder rellenar diferentes trámites, así como futuros avances que se puedan realizar. Con ello se plantea una arquitectura en la que se recogen una prestación de solicitudes, estas mismas se tratan de servicios que ofrece el ayuntamiento y son accesibles a los ciudadanos a través del portal de participación ciudadana de ese mismo ayuntamiento y se guardan los tokens en la Blockchain con respecto a este tema.

El diseño de la arquitectura se ha llevado a cabo con el kit de herramientas de modelado Archi [22]. El lenguaje de modelado utilizado ha sido Archimate, estándar de arquitectura empresarial abierto e independiente que admite la descripción, el análisis y la visualización de la arquitectura dentro y entre los dominios comerciales.

Para obtener una descripción general del impacto de la implementación de Blockchain. Se necesita una visión de sus procesos de negocio, sistemas de información y capa tecnológica.

El marco completo se presenta en 6 capas: estrategia, negocios, aplicación, tecnología, física e implementación y migración. El marco principal de Archimate consta de la capa de negocios, aplicaciones y tecnología. La siguiente imagen [Figura 4.1] muestra una descripción general de los conceptos utilizados en Archimate. Es un modelo orientado a servicios, las capas superiores utilizan los servicios proporcionados por las capas inferiores.

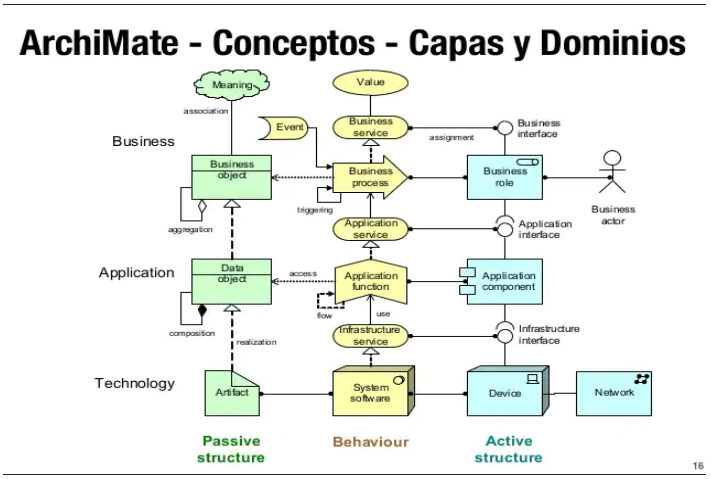

Figura 4.1: Conceptos de Archimate.

En base a estos conceptos [23] de Archimate se ha llevado a cabo un estudio y análisis del lenguaje para llegar a formalizar una arquitectura sencilla y comprensible en base a los estándares con los que se maneja Archi.

Se pretende que la arquitectura incluya todo lo necesario para poder gestionar y desarrollar el proyecto. Mediante un método estructurado. Realizando una evaluación basada en los atributos de calidad de la arquitectura.

Implica que la arquitectura sea clara y concisa, es decir debe proporcionar una visión general y clara, con lo cual solo debe usarse los elementos del modelo necesarios para evitar confusiones y usar un orden lógico de elementos de arriba a abajo, uniforme y cohesionada con exactitud, por lo cual debe el resultado esperado y debe ser útil ya que debe tener propósito claro en el contexto en que se desarrolla para el objetivo descrito anteriormente.

Finalmente esta arquitectura debe transmitir información básica y proporcionar un nivel de detalle al mismo tiempo.

A continuación se puede observar la arquitectura que se ha modelado [Figura 4.2]

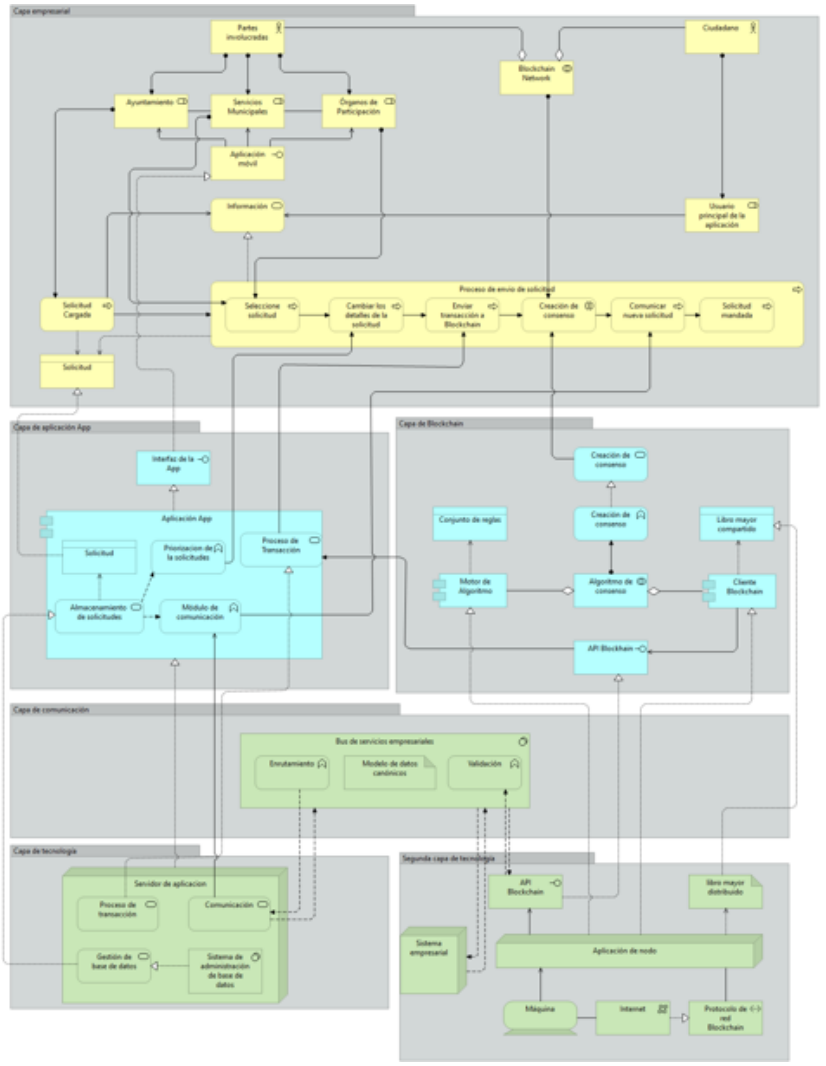

Figura 4.2: Arquitectura final.

Capa empresarial. La capa empresarial es la capa superior de la arquitectura, indicada por los bloques amarillos.

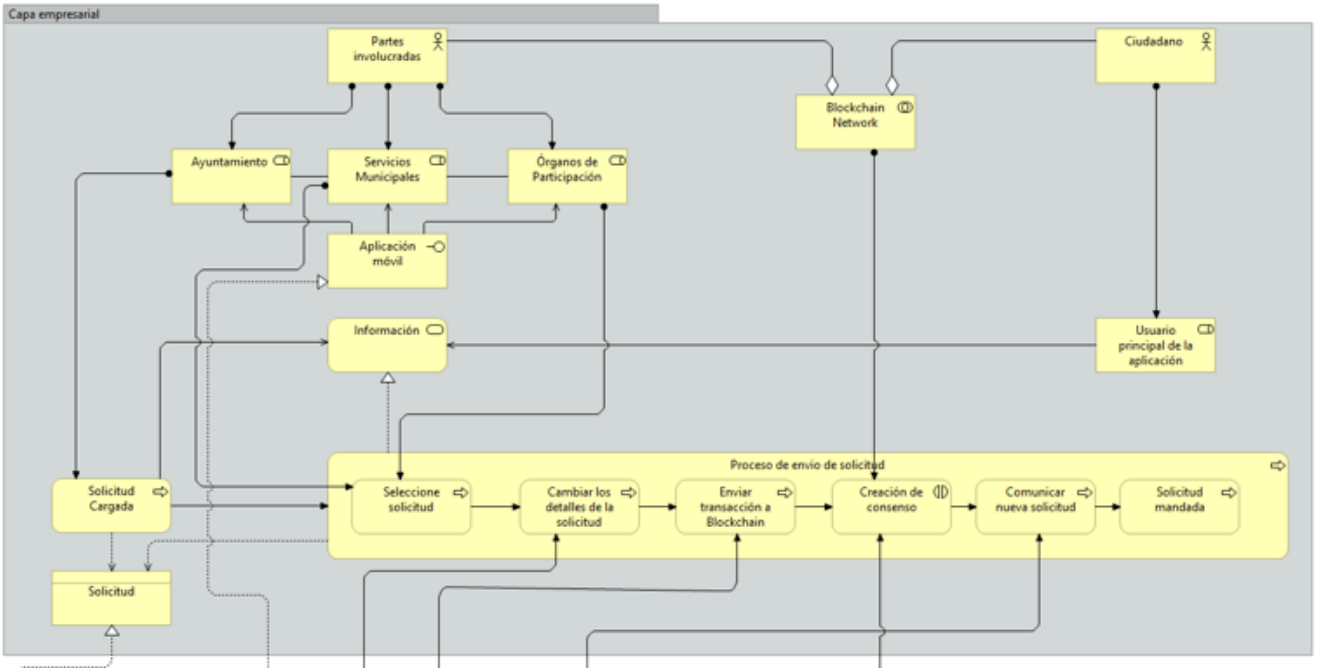

Figura 4.3: Capa empresarial.

En la parte superior, se describen tres actores: el ayuntamiento, los servicios municipales y los órganos de participación. Estos tres actores serán los involucrados, ya que todo el proceso pasará y será manejado por el ayuntamiento, el cual cuenta con los servicios municipales, que serán los encargados en solucionar las incidencias viales correspondientes y los órganos de participación que serán los encargados en atender las solicitudes que sean destinadas desde la sede electrónica de participación ciudadana, a través de la aplicación móvil. Para la aplicación, son usuarios del sistema. Los trabajadores del ayuntamiento tendrán diferentes tipos de cuentas de usuarios a la de los ciudadanos para entrar en la aplicación. El principal servicio que brinda es la información de los trámites o solicitudes a través del registro de nuevas solicitudes. Los diferentes usuarios utilizan una interfaz de móvil para comunicarse con la aplicación y, al hacerlo, reciben los servicios que brinda el ayuntamiento. El servicio se implementa mediante el proceso de envío de solicitudes. Este es el proceso central de la aplicación. La principal responsabilidad del ciudadano es mandar las solicitudes que tenga realizadas a la plataforma. Sin la carga de la solicitud, el proceso de su envío no puede comenzar. Esto se debe a que la responsabilidad de los órganos de participación es seleccionar y comprobar las solicitudes para su envío. Los detalles de la solicitud pueden ser cambiados si han localizado algún error. Esto luego se comunica al ciudadano a través de la aplicación, con ello tiene la posibilidad de cambiar los errores. Por último comienza el proceso de envío, donde los órganos de participación recibirán y atenderán las solicitudes. Respecto a las incidencias como es un proceso más sencillo, en el cual se describe la incidencia, mandando una foto y la localización, directamente se envía con esos datos y los servicios municipales serán los encargados de decidir atenderlas o no e informar del estado en que se encuentre esas incidencias a través de la aplicación para todos los ciudadanos. Con ello todos los actores del sistema participarán en la colaboración de la red Blockchain.

Capa de aplicación. Capa intermedia de la arquitectura, indicada por los bloques azules[Figura 4.4]

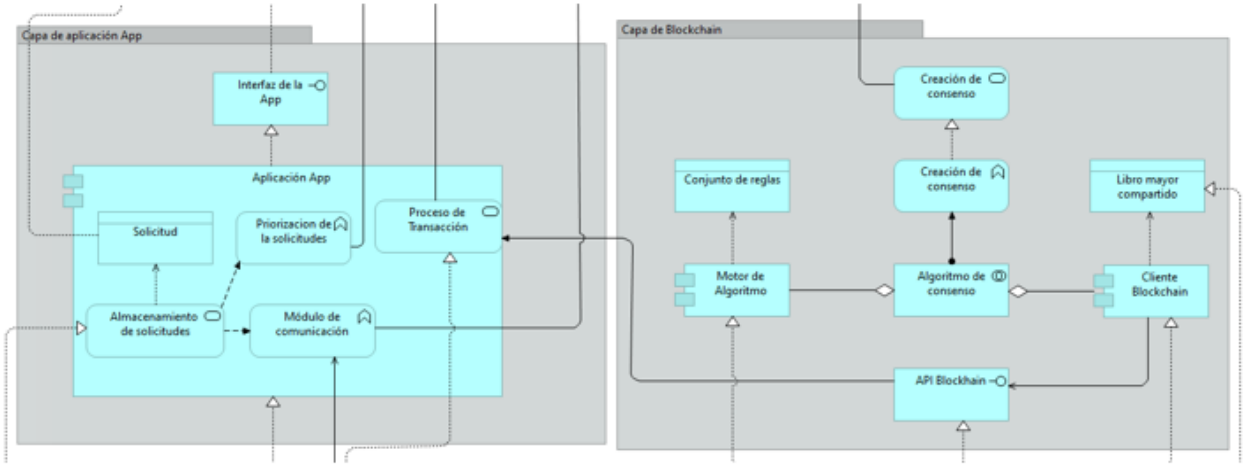

Figura 4.4: Capa de aplicación.

Para que los diferentes roles utilicen el sistema, utilizan una interfaz de móvil. Esta es una interfaz de aplicación. La aplicación está compuesta por múltiples funciones y servicios. Una función que no se ha mencionado es la *Priorización de solicitudes*, sirve para cambiar la prioridad de las solicitudes que has mandado desde la capa empresarial, si has mandado una, pues no se utiliza esta función. La función del *Módulo de Comunicación* da servicio a la comunicación de los nuevos detalles de la solicitud. Esto se hace a través de la aplicación. Por último, la aplicación accede a la base de datos del *Servidor Aplicación* donde se almacenan las solicitudes, en la arquitectura faltaría añadir el detalle de que la aplicación cuenta con un front end y un back end que se encarga de procesar las peticiones enviadas y aquí es donde se almacenan, no en la propia aplicación, teniendo Hyperledger se pueden almacenar en la misma Blockchain. Este servicio se encarga de gestionar todas las solicitudes en la aplicación y ponerlas a disposición del resto de funciones y servicios que necesiten. Además de la capa Blockchain, para utilizar esta misma y el servicio *Enviar transacción a Blockchain* y un nuevo servicio a la aplicación móvil: *Proceso de transacción*.

El grupo de las capas de aplicación es donde se implementa la aplicación real del servicio. Esta interfaz expone el componente de software al entorno. Implementa la interfaz empresarial desde la capa empresarial. El componente de software debe tener al menos dos elementos: el servicio de la aplicación *Proceso de transacción* y la función de aplicación *Módulo de comunicación*. El *Proceso de Transacción* es necesario para enviar la transacción a la Blockchain. Sirve al proceso empresarial *Enviar transacción a Blockchain* para hacer posible este proceso. El *Módulo de comunicación* es necesario para enviar la transacción a la Blockchain y brindar las posibles integraciones con otros sistemas. El grupo *Capa Blockchain* son los elementos de aplicación de Blockchain. Se ejecutan en la *Aplicación de nodo* de la capa tecnología. Este nodo tiene todos los elementos de la aplicación Blockchain. El *Cliente Blockchain* es un componente de software que es responsable de la comunicación con el mundo exterior, sirve a una API Blockchain para exponer el *Libro mayor compartido* al procesamiento de transacciones de la aplicación móvil. Este es el objeto de datos de la aplicación que representa todas las transacciones que se guardan en la cadena de bloques. El *Cliente Blockchain* puede acceder a este libro mayor para recuperar datos o enviar una nueva transacción cuando el algoritmo de consenso tenga éxito. El *Cliente Blockchain* se modela como un componente de software diferente al motor de algoritmo. Aunque ambos se ejecutan en el mismo entorno, tienen diferentes funciones. El *Motor de algoritmo* es responsable del

trabajo que se debe realizar para construir un consenso. Estos son principalmente los cálculos de los hash para la cadena de bloques. La forma en que se construye el consenso en el nodo se registra en el *Conjunto de reglas*. El *Motor de algoritmo* y el *Cliente Blockchain* tienen que trabajar juntos para hacer su parte en la construcción del consenso, el *Motor de algoritmo* hará los cálculos y el *Cliente Blockchain* proporcionará los datos y se encargará de la comunicación. Esta colaboración de creación de consenso es responsable de la función de *Creación de consenso*, que implementa este mismo servicio. Este servicio de *Creación de consenso* sirve para la interacción empresarial.

Capa tecnológica. Capa inferior de la arquitectura, indicadas por los bloques verdes[Figura 4.5].

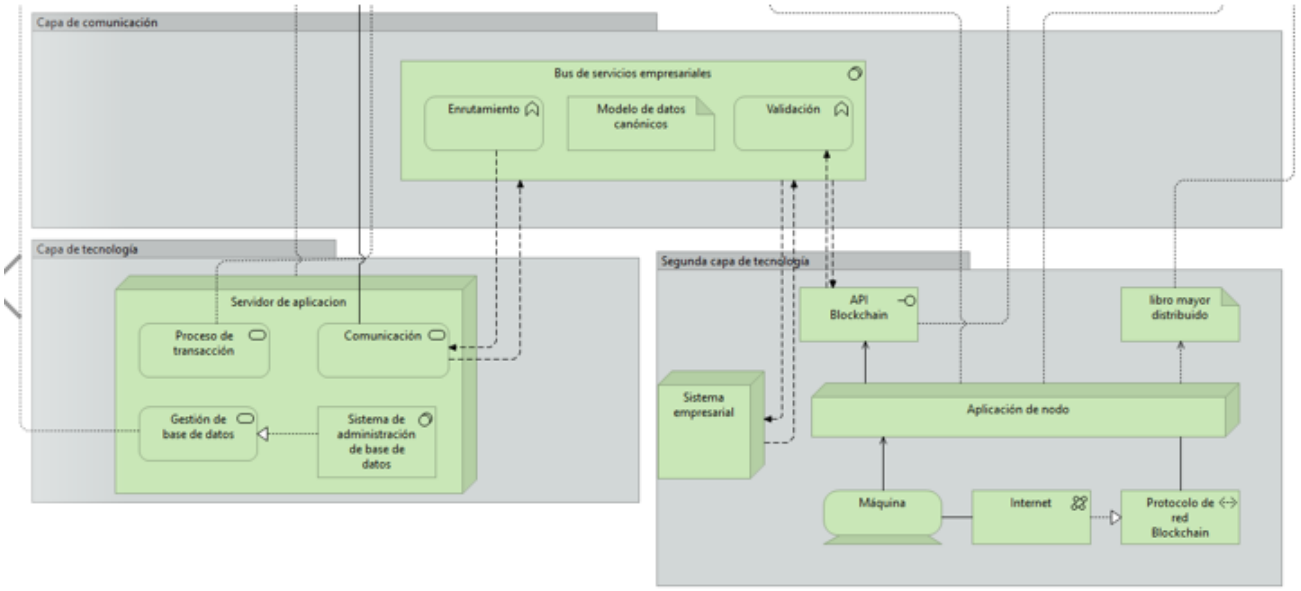

Figura 4.5: Capa de comunicación y tecnológica.

El Ayuntamiento tiene su propio servidor para alojar la aplicación. Para crear una descripción clara de la arquitectura, se modela el servidor como un nodo. En realidad, el alojamiento de la aplicación está hecho por tres servidores distintos. Comparten la carga y sirven de respaldo entre sí. Por ahora, se asume que es un servidor. En este servidor se ejecutan todas las tecnologías para hacer posible la aplicación. Los servicios más importantes son la *Comunicación* y la *Gestión de bases de datos*. Son responsables del servicio e implementación y función de la aplicación correspondiente.

En este caso la capa tecnológica está dividida en tres grupos diferentes. Una capa de comunicación, una capa de tecnología y una denominada segunda capa de tecnología.

El servidor está modelado como un nodo. El *Servidor de aplicación* implementa la aplicación móvil del componente de software. El *Servidor de aplicación* debe tener al menos dos servicios tecnológicos: *Comunicación* y *Proceso de transacción*. El servicio de *Proceso de transacciones es la* implementación del servicio de procesamiento de transacciones de la aplicación. El servicio de *Comunicación* es responsable de la comunicación con el bus de servicio empresarial, que nos lleva a la capa de comunicación.

Para crear integraciones rápidas, se utiliza un bus de servicio empresarial para manejar la comunicación entre los diferentes nodos de tecnología. Este bus de servicio empresarial se modela

como un componente de software del sistema. El bus de servicios empresarial se puede alojar en cualquier lugar. Tiene algunos elementos generales como funciones de *Enrutamiento* y *Validación* y utiliza un *Modelo de datos canónico* para mapear los mensajes entrantes a la salida deseada para cada sistema. El bus de servicio, se trata de un medio de comunicación entre la aplicación y la Blockchain.

La denominada segunda capa de tecnología representa la capa de tecnología de cada uno de los actores participantes dentro del sistema. Tiene un nodo llamado *Sistema empresarial*. No podemos conocer el entorno tecnológico exacto de cada actor, pero se indica que con esta configuración, es fácil integrar los sistemas empresariales a través del bus de servicios empresariales. Lo que cada actor debe tener es la configuración de la Blockchain.

Cada usuario debe estar activo para participar en la red Blockchain. Por lo tanto, cada usuario debe ejecutar una *Aplicación de nodo* en una máquina. Esta podría ser una máquina virtual o alojada en un servidor local, pero debería estar activa. Los nodos se comunican entre sí cuando se envía una nueva transacción y crean un consenso. Esto se hace directamente entre los nodos, a través de Internet utilizando el protocolo de la red blockchain específico. La aplicación de nodo implementa tanto el cliente Blockchain como el *Motor de algoritmo*. Se separan para indicar la diferencia, pero se ejecutan en el mismo nodo. Los nodos se comunicarán entre sí a través de su propio protocolo, pero la comunicación con la aplicación se realiza a través de la interfaz Blockchain y el bus de servicio empresarial.

Otra ventaja es que, debería ser más rápido. Debido a que el bus de servicio empresarial recibe todos los mensajes y respuestas, es el primer nodo al que se le notifica cuando se alcanza un consenso y se envía una transacción correctamente. El bus de servicio empresarial puede entonces notificar a todos los sistemas integrados.

El bus es responsable de la comunicación entre blockchain y la aplicación. Por ahora, el bus conecta dos sistemas, la aplicación y la API blockchain. Todas las solicitudes son iniciadas por la aplicación. La solicitud es una llamada síncrona que solicita todos los bloques que están en la Blockchain. Recibirá una respuesta de la Blockchain. Lo mismo ocurre con *Seleccione solicitud*, que recupera todas las solicitudes, son solicitudes asincrónicas, solicitudes que no reciben una respuesta a menos que algo salga mal y envían una nueva transacción, a la cadena de bloques.

4.3.2 Implementación en Hyperledger Composer

En esta sección se describe la implementación a través de Hyperledger Composer de componentes que tenemos que definir en este proyecto Blockchain. Se define los participantes de la red, los roles que éstos desempeñarán, los activos que podrán maniobrar, las transacciones que podrán ejecutar y cómo los usuarios finales interactúan con la Blockchain.

Una de las funciones más importantes del Hyperledger Composer es la de modelar la red de negocios para lo cual se debe definir quiénes son los participantes, cuáles son los activos o assets.

Se pueden crear diferentes tipos de archivos ,el modelo que tiene la extensión CTO donde se pueden definir los participantes los activos y las transacciones usando el lenguaje del composer, el archivo script que tiene extensión JS donde se define la lógica de ejecución de las transacciones o mejor dicho los contratos inteligentes en Javascript, el archivo de control de acceso que tiene extensión ACL donde definen todos los accesos de los participantes y de los nodos hacia las transacciones y los datos el archivo de consultas con extensión QR y donde se definen todas las consultas que van a acceder a la bloque. Por último el archivo de negocio con extensión BNA que

empaqueta a todos los demás.

En este caso me he limitado a la creación en el archivo CTO la definición de los participantes que serían los ciudadanos y los trabajadores del servicio municipal y como activo las incidencias. En las siguientes imágenes se puede observar que compone a cada uno de estos elementos.

En primer lugar se crea a los participantes involucrados en el uso de la aplicación. En la siguiente imagen [Figura 4.6] se define el trabajador del servicio municipal, el cual tendrá un código asociado, nombre y apellidos, más la fecha en la que se registró y finalmente el DNI y su correo electrónico, que en este caso será común para todos los trabajadores del servicio municipal, ya que tendrá el correo correspondiente a este servicio.

```
participant serviciomunicipal identified by codigo{
  o String codigo
  o String nombre
  o String apellidos
  o DateTime fecha
  o String email
  o String DNI
}
```

Figura 4.6: Definición del participante del servicio municipal.

En la siguiente imagen [Figura 4.7] se define al ciudadano y sus correspondientes características, al igual que los trabajadores del servicio municipal tendrán un código asociado, junto a su dirección y código postal, más el nombre y los apellidos, la fecha en que se registra, su correo electrónico y finalmente su DNI.

```
participant Ciudadano identified by codigo {
  o String codigo
  o String nombre
  o String apellidos
  o Integer cod_postal
  o String localización
  o DateTime fecha
  o String email
  o String DNI
}
```

Figura 4.7: Definición del participante ciudadano.

A continuación se crea las el asset o activo, en este caso se trata de las incidencias. En la siguientes imágenes [Figura 4.8 , Figura 4.9, Figura 4.10] se observa las características que tendrá las incidencias. En primer lugar tendrán un código asociado al igual que los participantes, una breve descripción, la fecha en que se publica, la localización donde sucede la incidencia, el estado en el que se encuentra la incidencia, este estado se divide en tres estados, lo cuales serán: resuelta, pendiente, denegada. Este tipo de estado los determinarán los trabajadores de los servicios municipales. Finalmente cuenta con diferentes categorías, estas se dividen en: alumbrado, calles, jardines, limpieza, mobiliario, señales, playas y abastecimiento y saneamiento.

```
asset incidencia identified by codIncidencia {
  o String codIncidencia
  o String descricipción
  o DateTime publicacion
  o String localización
  o Estado estado
  o Categoria categoria
  --> Ciudadano ciudadano
}
```

Figura 4.8: Definición del asset incidencia.

```
enum Estado {
  o Resuelta
  o Pendiente
  o Denegada
}
```

Figura 4.9: Definición del estado de las incidencias.

```
enum Categoria {
o Alumbrado
o Calles
o Jardines
o Limpieza
o Mobiliario
o Señales
o Playas
o Abastecimiento_Saneamiento
}
```

Figura 4.10: Definición de las categorías de las incidencias.

Una vez realizada la creación de los participantes y el activo he podido llevar a cabo un test de prueba rellenando los datos correspondientes de cada uno para comprobar cómo se guardan en la Blockchain. En la siguiente imagen [Figura 4.11] se observan los datos de un ciudadano.

En las siguientes imágenes se muestra el resultado final de como ha quedado guardado en la Blockchain.

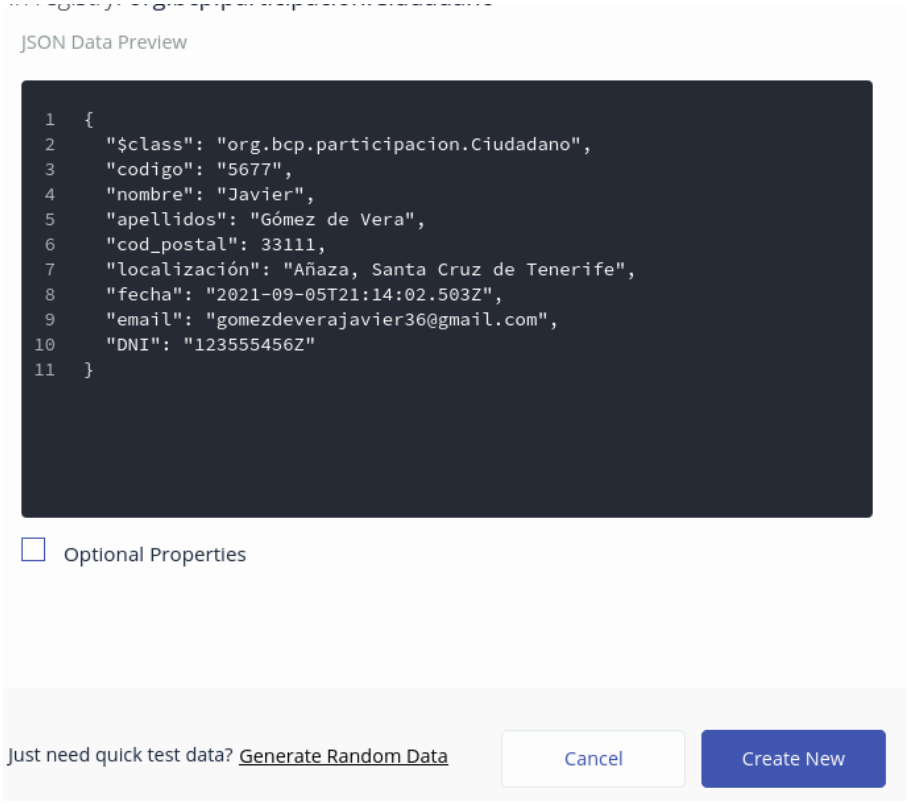

Figura 4.11: Datos rellenos del ciudadano.

A continuación, en la siguiente imagen [Figura 4.12] se tienen los datos de un trabajador municipal.

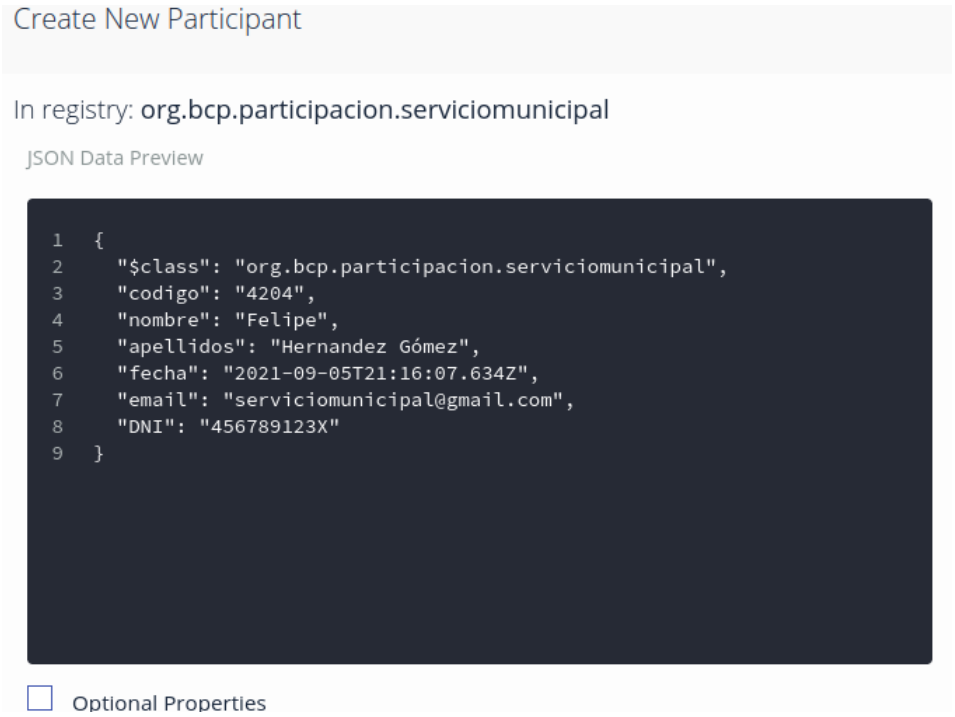

Figura 4.12: Datos rellenos del trabajador del servicio municipal.

Finalmente, en la siguiente imagen [Figura 4.13] se tiene los datos rellenos de una incidencia, la cual se observa que tiene su propio código, a su vez tiene el código del ciudadano asociado para distinguir quien la ha mandado.

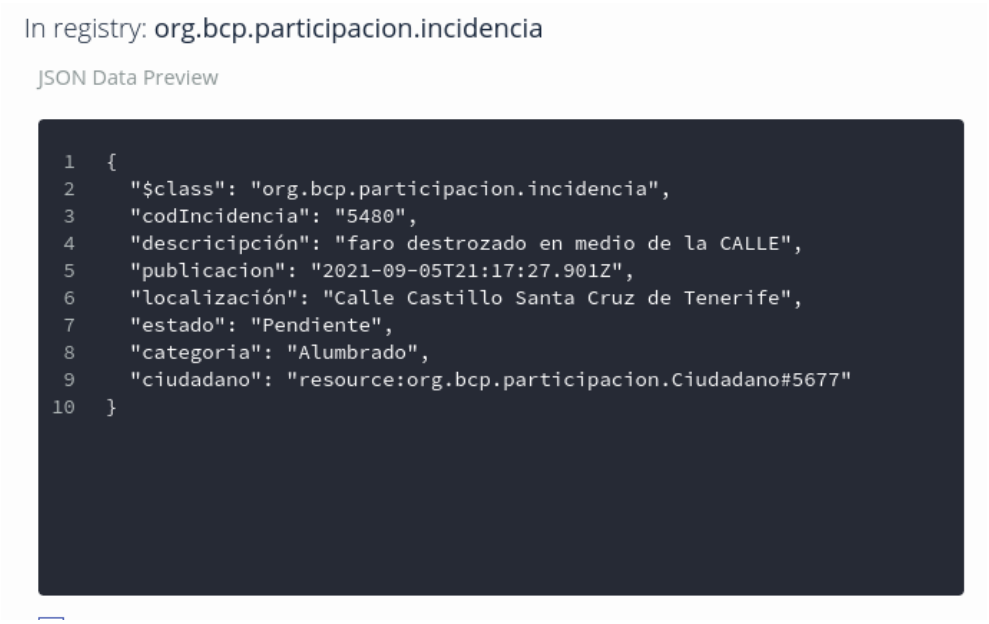

Figura 4.13: Datos rellenos de una incidencia.

En las siguientes imágenes [Figura 4.14, Figura 4.15, Figura 4.16 y Figura 4.17] se muestra el resultado final de como ha quedado guardado en la Blockchain, tanto los datos como las transacciones.

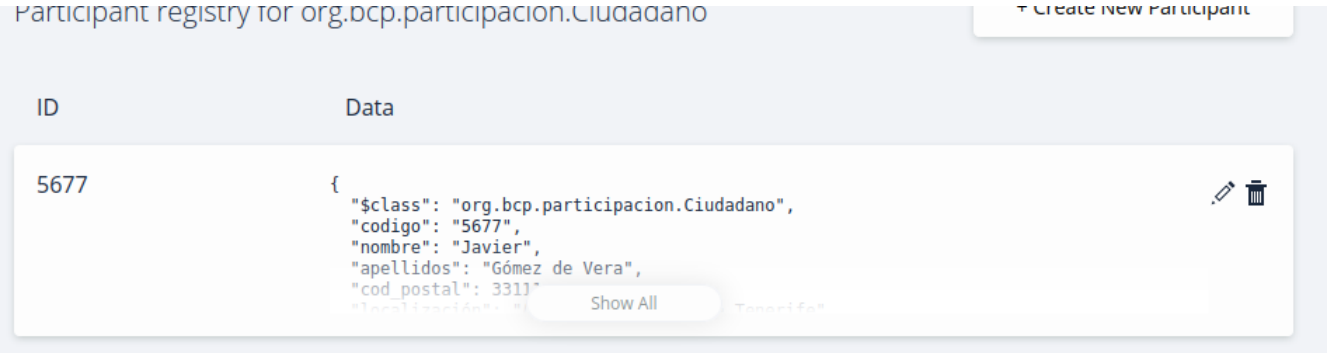

Figura 4.14: Datos almacenados en la Blockchain del ciudadano.

Figura 4.15: Datos almacenados en la Blockchain del trabajador del servicio municipal.

Figura 4.16: Datos almacenados de la incidencia.

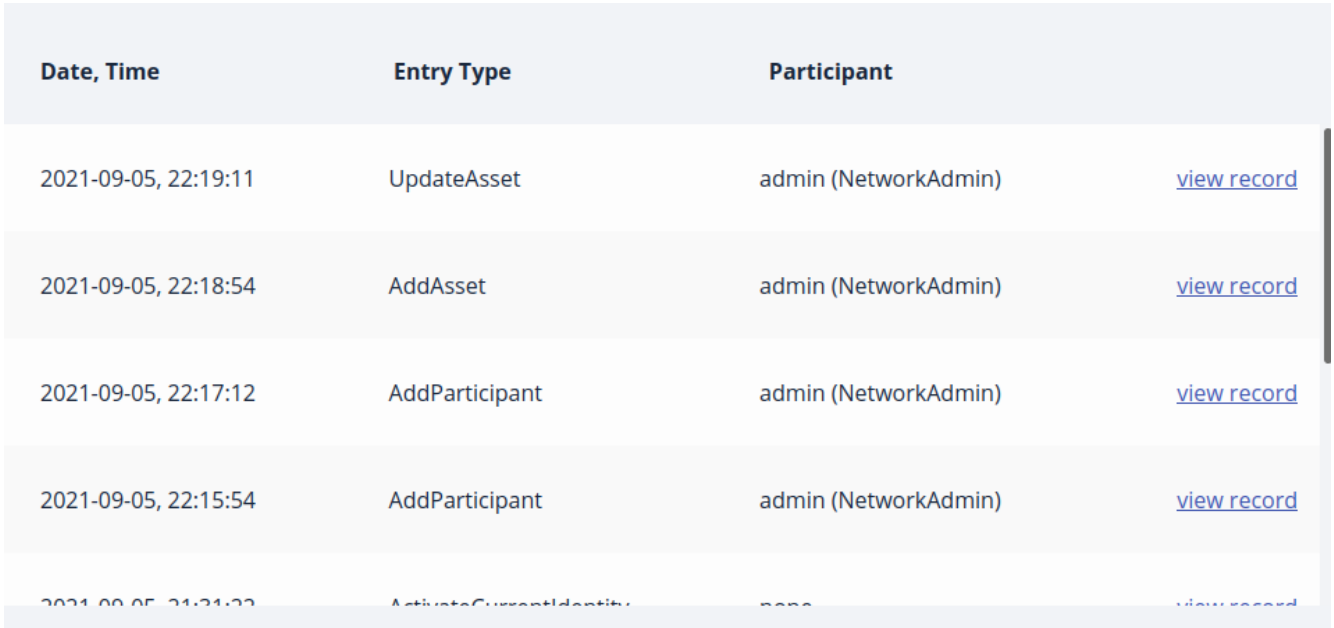

Figura 4.17: Transacciones almacenadas en la Blockchain.

4.3.3 Prototipado

En este apartado se muestra el prototipo de la aplicación móvil realizada haciendo uso de Justinmind [24]. En el prototipo podemos encontrar lo siguiente:

1.Menú de Inicio: Desde aquí accedemos al portal del ayuntamiento [Figura 4.18]

Figura 4.18: Pantalla de menú de inicio.

2.Incidencias: Interfaz de cómo un usuario podría mandar una incidencia [Figura 4.19, Figura 4.20 y Figura 4.21]

Figura 4.19: Pantalla para introducir incidencias.

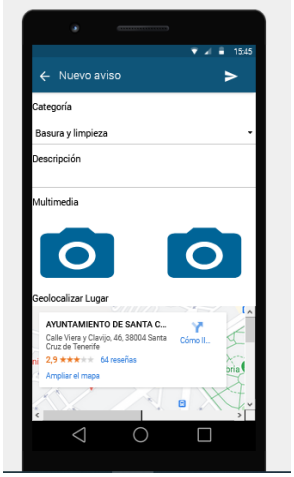

Figura 4.20: Pantalla para rellenar las incidencias.

Figura 4.21: Pantalla donde se almacenan las incidencias.

3.Mapa Global: Para poder establecer la localización del usuario [Figura 4.22].

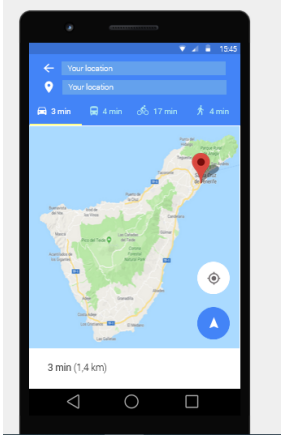

Figura 4.22: Pantalla para colocar tu localización.

4.Formulario de quejas: Si los usuarios tienen alguna queja respecto a la aplicación o a las medidas tomadas por el ayuntamiento lo rellenan por aquí [Figura 4.23 y Figura 4.24].

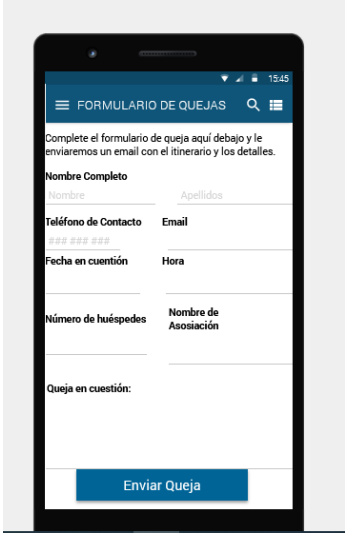

Figura 4.23: Pantalla de formulario de quejas.

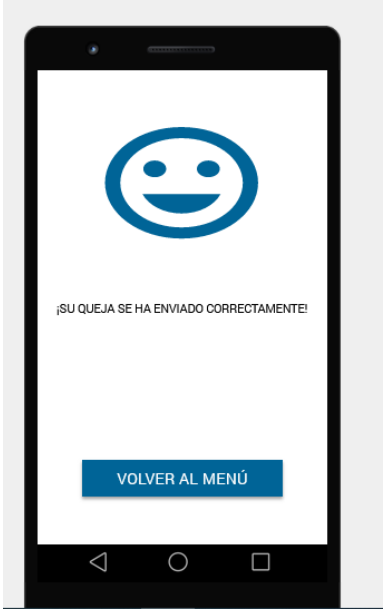

Figura 4.24: Pantalla de Queja aceptada

5.Información: Explicación a los usuarios de cómo funciona la aplicación [Figura 4.25].

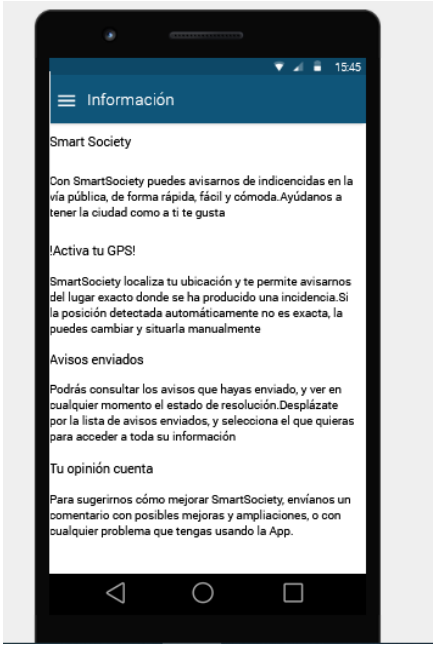

Figura 4.25: Pantalla de información de la aplicación.

Capítulo 5 Conclusiones y líneas futuras

En este capítulo se describen las conclusiones obtenidas del desarrollo de este trabajo. Así como las líneas futuras de trabajo para el desarrollo de las herramientas de participación e implementación con la tecnología Blockchain.

5.1 Conclusiones

Blockchain es una tecnología en auge que se ha implantado en diversos campos. Esta tecnología ha destacado sobre todo por su uso en la minería de criptomonedas. Pero a lo largo de este trabajo se ha observado el uso que puede tener a nivel de gobernanza inteligente y en diferentes herramientas para la participación ciudadana. En la gobernanza se valora la transparencia, seguridad y confianza que deben tener las Administraciones Públicas. Estos dos aspectos con la Blockchain se refuerzan debido a la seguridad que la criptografía aporta a los datos de los usuarios, así como a su anonimato. Así los usuarios pueden estar seguros cuando realicen transacciones, ya que se detectará cualquier manipulación. Un aspecto importante de esto puede ser en el uso de votaciones electorales, junto con la identidad soberana. Esto lleva a valorar la importancia que tendrá en un futuro no solo en el ámbito tratado en este trabajo, sino que podría cambiar modelos y procesos en el sistema político y administrativo de hoy en día.

Con este proyecto he logrado hacer una propuesta que permite integrar la tecnologías Blockchain en las herramientas de participación ciudadana. Específicamente Blockchain e identidad soberana en un sistema de incidencias municipales, logrando así una mayor transparencia en los trámites o quejas protegiendo y anonimizando la identidad de quien las realiza.

Si se utilizaran contratos inteligentes asociados, estas aplicaciones facilitarían la resolución

automática de incidencias. Así, se podría programar automáticamente los requisitos que tienen que cumplir esa incidencia para que sea resuelta.

De los aspectos estudiados, no todos son positivos en el uso de Blockchain. Existen aspectos negativos que hay que considerar, entre ellos el hecho de que en la arquitectura Blockchain las transacciones tardan más tiempo en llevarse a cabo porque tiene que pasar por un proceso de validación. El espacio de memoria puede ser limitante, aunque si se trata de una red privada están delimitadas a un ámbito concreto al cual se dirigen.

Cabe destacar que, en la fase inicial del trabajo donde se estudiaron y analizaron los diferentes procesos por los que tiene que pasar la queja o incidencia en un ayuntamiento. Se observa que se trata de procesos complejos, la mayoría de las veces complicados de seguir. Con la tecnología Blockchain y específicamente con los contratos inteligentes se puede automatizar algunas tareas y hacer el seguimiento y trazabilidad de manera más sencilla lo que ofrece a la ciudadanía una seguridad y transparencia. El trabajo aporta una arquitectura en la cual se puedan unir estos mundos que a primera vista no tienen porqué realizarse, junto una implementación sencilla que aporta un ejemplo de cómo puede resultar esta propuesta. Además se presenta un prototipo que aporta un ejemplo visual. Finalmente, se destaca que el potencial de uso de estas tecnologías es amplio y quedan por descubrir muchos beneficios de las mismas en la gobernanza y en otros ámbitos.

5.2 Líneas Futuras

Algunas líneas futuras de trabajo, será la ampliación las funcionalidades y servicios de la aplicación móvil propuesta en el Trabajo de Fin de Grado. La propuesta realizada podría crecer en algunos aspectos, como son: terminar de perfeccionar el proyecto con respecto a la funcionalidad en relación a la Blockchain, evaluar el interés y la viabilidad de esta arquitectura y prototipo en la administración y para la ciudadanía e implementar la propuesta como caso en un caso de uso real. Por último sería la integración de la identidad soberana de la Unión Europea o considerar y valorar otras propuestas.

Capítulo 6 Summary and Conclusions

6.1 Conclusions

Blockchain is a booming technology that has been implemented in various fields. This technology has stood out above all for its use in cryptocurrency mining. But throughout this work, the use that it can have at the level of smart governance and in different tools for citizen participation has been observed. In governance, the transparency, security and trust that Public Administrations must have is valued. These two aspects with the Blockchain are reinforced due to the security that cryptography provides to user data, as well as its anonymity. Thus, users can be sure when making transactions, since any manipulation will be detected. An important aspect of this may be in the use of electoral votes, along with the sovereign identity. This leads to assessing the importance that it will have in the future not only in the area covered in this work, but also that it could change models and processes in today's political and administrative system.

With this project, it was possible to make a proposal that allows integrating Blockchain technologies into citizen participation tools. Specifically, Blockchain and sovereign identity in a system of municipal incidents, thus achieving greater transparency in the procedures or complaints, protecting and anonymizing the identity of the person who carries them out.

If associated smart contracts were used, these applications would facilitate the automatic resolution of incidents. Thus, it would be possible to automatically program the requirements that this incident must meet in order for it to be resolved.

Of the aspects studied, not all are positive in the use of Blockchain. There are negative aspects that must be considered, among them the fact that in the Blockchain architecture, transactions take longer to carry out because they have to go through a validation process. The memory space can be limited, although if it is a private network they are limited to a specific area to which they are addressed.

It should be noted that, in the initial phase of the work, the different processes through which the complaint or incident has to go through in a town hall were studied and analyzed. It is observed that these are complex processes, most of the time complicated to follow. With Blockchain technology and specifically with smart contracts, some tasks can be automated and monitoring and traceability can be done more easily, which offers citizens security and transparency. The work provides an architecture in which these worlds that at first sight do not have to be carried out can be united, together with a simple implementation that provides an example of how this proposal can turn out. In addition, a prototype is presented that provides a visual example. Finally, it is highlighted that the potential use of these technologies is wide and many benefits remain to be discovered in governance and other areas.

6.2 Future works

Some future lines of work will be the expansion of the functionalities and services of the mobile application proposed in the Final Degree Project. The proposal could grow in some aspects, such as: finish perfecting the project with respect to functionality in relation to the Blockchain, evaluate the interest and viability of this architecture and prototype in the administration and for citizens and implement the proposal. as a case in a real use case. Finally, it would be the integration of the sovereign identity of the European Union or considering and assessing other proposals.

Capítulo 7 Presupuesto

En este capítulo se hará una estimación sobre el coste de la aplicación, incluyendo los costes del análisis y gestión del uso de la Blockchain Hyperledger, el prototipo de la aplicación y el modelado de la arquitectura para implementar y desplegar la solución final en un entorno real.

7.1 Costes de Personal

En este apartado se estiman los costes de personal en horas de trabajo y formación que han sido invertidas en el estudio, documentación e implementación de la solución final.

Concepto	Cantidad de Horas	Coste	Total
Estudio de la tecnología Blockchain	40	18€	720€
Estudio de la tecnología Hyperledger	40	18€	720€

Diseño de la aplicación	60	18€	1080€
Diseño de la arquitectura	60	18€	1080€
Implementación Front-End	500	18€	9000€
Comunicación Front-End y Back-End (teniendo Hyperledger)	170	18€	3060€
Implementación Chaincode	300	18€	5400€
Total:	**1100 horas**		**21060€**

Tabla 7.1: Costes de personal.

7.2 Costes de equipamiento

En este apartado se calculan los costes de los distintos componentes necesarios para lanzar la aplicación. En una primera propuesta, se propone la creación de una red Hyperledger privada como solución. Se propone la existencia de al menos un nodo completo que participe activamente de la Blockchain y sirva la aplicación.

Concepto	Cantidad	Coste	Total
Servidor	1	700€	700€
Ordenador	1	600€	600€
Total:			**1300€**

Tabla 7.2: Costes de equipamientos.

7.3 Presupuesto final

El presupuesto final teniendo en cuenta el presupuesto personal y utilizando el presupuesto de componentes que se basa en el control local de la red es el siguiente:

Concepto	Precio
Coste de Personal	21060€
Costes de equipamientos	1300€
Total:	**22360€**

Tabla 7.3: Presupuesto Final.

Bibliografía

[1] *Boletín Oficial del Estado*: Artículo 23 de la Constitución Española, BOE-A-1978-31229, Cortes Generales, España.
[2] *Boletín Oficial del Estado*: Constitución Española, BOE-A-1978-31229, Cortes Generales, España.
[3] *Boletín Oficial del Estado*: ley 19/2013 de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno, BOE-A-2013-12887, Cortes Generales, España.
[4] C. Calderón and A. Lorenzo, Open government: gobierno abierto. Algon, 2010.
[5] *Libro Blanco sobre la gobernanza:* EUR-Lex-l10109-EN-EUR-Lex, Comisión Europea,
[6] A. Cerrillo i Martínez, "La gobernanza inteligente: datos abiertos y datos masivos al servicio de la innovación en las Administraciones públicas," Madrid, España, Sep. 2017.
[7] A.Carmazane Mariscal, "La transparencia en la administración pública," Trabajo Fin de Grado, Dpto. de Economía y Empresas., Univ. del País Vasco, País Vasco, España, 2016.
[8] *Boletín Oficial del Estado*: Constitución Española, Ley 5/2010, de 21 de junio, canaria de fomento a la participación ciudadana, BOE-A-2010-10985, Cortes Generales, España.
[9] La transformación digital y el Gobierno Abierto,Systems Group, Dec. 04, 2019. [En línea] Disponible en: https://systemsgroup.es/transformacion-digital/transformacion-digital-gobierno-abierto/32852/ (Accedido: 20-my-2021).
[10] B.C. Martisi,"Las 10 mejores 'apps' que impulsan la participación ciudadana y la transparencia," *Comp. Empresarial,* Feb, 2018.
[11] E. web-A. de S. C. de Tenerife, "Ayuntamiento de Santa Cruz de Tenerife: App SC Mejora."[En linea] Disponible en: https://www.santacruzdetenerife.es/web/servicios-municipales/servicios-publicos/app-sc-mejora (Accedido: 20-ag-2021)
[12] U. L. Piedra, "¿Podría blockchain fortalecer los sistemas democráticos actuales?," Izertis, Dec. 11, 2018. [En línea] Disponible en: https://www.izertis.com/es/-/blog/podria-blockchain-fortalecer-los-sistemas-democraticos-actuales (Accedido:10-jun-2021).
[13] A. T. Norman, Todo sobre tecnología blockchain: La guía definitiva para principiantes sobre monederos blockchain. Tektime, 2019.
[14] Nakamoto, Satoshi. (2009). Bitcoin: A Peer-to-Peer Electronic Cash System.
[15] L. Salcedo, "Algoritmo de Resumen del Mensaje 5 (MD5) - Criptografía con Python," Mi Diario Python, Jul. 12, 2018.
[16] B. Academy, "¿Qué es un Árbol Merkle?," Bit2Me Academy, Nov. 11, 2019.
[17] N. Gaur, A. O'Dowd, P. Novotny, L. Desrosiers, V. Ramakrishna, and S. A. Baset, Blockchain with Hyperledger Fabric: Build decentralized applications using Hyperledger Fabric 2, 2nd Edition. Packt Publishing Ltd, 2020.
[18] ¿Qué es un SDK? [En línea] Disponible en: https://www.redhat.com/es/topics/cloud-native-apps/what-is-SDK (Accedido: 15j-ul-2021).
[19] The web's scaffolding tool for modern webapps [En línea] Disponible en: https://yeoman.io/ (Accedido: 15-jul-2021).

[20] Empowering App Development for Developers, Docker. https://www.docker.com/ (Accedido: 08-jul-2021).
[21] C. Güemes,"*Blockchain* en procesos de participación ciudadana: innovando desde la práctica en el Ayuntamiento de Alcobendas," *Participación ciudadana experiencias inspiradoras en España,* Editor Centro de Estudios Políticos y Constitucionales. Mº de la Presidencia. Madrid: GIGAPP, 2018, pp. 147-158.
[22] Archi – Open Source ArchiMate Modelling. https://www.archimatetool.com/ (Accedido:1-my-2021).
[23] E.C. Spijkerboer (Christian), "BLOCKCHAIN BASED TRANSACTION PROCESSING SYSTEM A REFERENCE ARCHITECTURE FOR AN INTEGRATED BLOCKCHAIN BASED TRANSACTION PROCESSING SYSTEM," 2018.
[24] Free prototyping tool for web; mobile apps - Justinmind [En línea] Disponible en: https://www.justinmind.com/ (Accedido: 01-ag-2021).