Programa Superior en Blockchain Tenerife 2019

Proyecto

Back Office Tarjeta Ciudadana

Alumnos:

- Francisco Jesús Gómez Mesa
- Ginés León Rodríguez
- David Pérez Rodríguez
- Miguel Pintor Sepúlveda
- Zulay Rodríguez Castilla
- Tomás de Villanueva Romero Clavijo

Julio de 2019

1.- RESUMEN EJECUTIVO

El objetivo del proyecto es desarrollar la infraestructura tecnológica que ofrezca soporte a la tarjeta ciudadana respaldada con tecnología blockchain.

El producto final es un back office de servicios sobre blockchain que ofrezca un sistema de administración de servicios más flexible y transparente tanto para los ciudadanos como para los prestadores de servicios.
Aunque este documento se centrará en la Tarjeta Ciudadana de la isla de Tenerife, con el fin de darle mayor alcance al proyecto, se recoge la metodología y tecnología blockchain que puede ser aplicado a este tipo de tarjetas en general, por lo que atiende a las características y alcance que cada gobierno o administración le quiera dar a este tipo de tarjetas

En este proyecto inicialmente la tarjeta permite el uso del transporte público (bus, tranvía, metro, etc.) a modo de abono de transporte en cualquiera de sus modalidades (abono monedero, abono tiempo, etc.). La arquitectura planteada permite la incorporación posterior de otros servicios a la tarjeta, bien prestados por la Administración, bien desde el ámbito privado (culturales, deportivos, ocio, etc.).

La lógica del sistema incluye las oportunas liquidaciones entre las partes.

La implantación debe ser liderada por una administración pública y permitirá la adquisición de todo tipo de títulos de transporte incorporando aquellos que incluyen subvenciones provenientes de las políticas de transporte existentes (abono joven, abono tercera edad, etc.). Igualmente permitirá la adquisición de abonos para el uso de instalaciones deportivas y asistencia a eventos culturales entre otros, permitiendo descuentos en el uso de estos servicios, acumulación de puntos de descuentos etc.

La incorporación de agentes privados al ecosistema primará conductas sostenibles. Por ejemplo, descuentos por utilizar transporte colectivo en un desplazamiento, o incentivos al uso de vehículos de alta ocupación.

El sistema en funcionamiento actualmente incluye compensaciones entre los principales actores (en el caso de la isla de Tenerife se encuentra el Cabildo, TITSA, Metropolitano de Tenerife, etc.). Estas compensaciones suponen un gasto de dinero público y, por tanto, están sujetas a fiscalización por parte de las administraciones. Uno de los problemas que se resuelve con este proyecto es precisamente reducir el coste asociado a las compensaciones al mismo tiempo que se dota de transparencia al nuevo sistema, facilitando que cualquier administración/empresa participante pueda acceder a los datos que les afecten.

Desarrollos posteriores ampliarán la oferta de transporte a otros modos como el aéreo, o el marítimo. De esta forma pueden emitirse billetes combinados y realizar un sistema de liquidación para cada uno de los operadores.

2.- PROPUESTA DE VALOR Y ANÁLISIS DE LA COMPETENCIA

2.1 Definición del problema a resolver

Supongamos que somos propietarios de una tarjeta ciudadana y que la usamos para disfrutar de una serie de servicios que ofrecen ventajas como descuentos en el transporte público, descuentos en el acceso a la piscina municipal, uso de la biblioteca pública de forma gratuita, y acumulación de puntos que repercute en nuevos descuentos sobre el ecosistema de servicios.

La Administración es el agente que suministra las tarjetas ciudadanas, fija los descuentos que tiene cada usuario y compensa a cada prestador de servicios la cantidad subvencionada que tiene ese ciudadano en ese servicio en concreto por cada uso que ha realizado.

Cada mes debe se tiene que realizar una compensación a cada agente por parte de la Administración, debe de poder realizarse una trazabilidad de los usos que cada usuario le ha dado a su tarjeta y una comunicación a las entidades financieras que realizarán el ingreso en cada cuenta del dinero que le corresponde a cada agente.

2.2 Producto y propuesta de valor

El producto a desarrollar y comercializar es una infraestructura tecnológica basada en blockchain en la que se registran todas las operaciones relevantes efectuadas por cada una de las tarjetas que son de interés para todos los agentes del ecosistema al ser necesarias de alguna forma para algunos de ellos y que debe ser accesible de forma clara, concisa, transparente y confiable.

Cada agente del sistema utilizará sus sistemas para interactuar con cada una de las tarjetas. Se crearán una serie de canales privados que enviarán a la cadena blockchain sólo aquellos datos que son de interés para algunos de los agentes, garantizando que la información jamás se podrá perder, modificar o eliminar.

Por tanto, cualquier información necesaria para los agentes que necesite ser preservada y disponible puede ser almacenada en esta infraestructura tecnológica basada en blockchain de manera segura, descentralizada y más económica que utilizando intermediarios. Además, al almacenar esta información de forma cifrada se garantiza su confidencialidad ya que solo quien cuente con la llave de cifrado puede acceder a ella.

Todos los agentes registran información de cada uso de cada tarjeta a la blockchain de forma que se tiene un sistema centralizado, robusto y seguro de toda la información que es relevante para cada uno de los agentes y se agilizan todas las operaciones que precisan de esta información, con transparencia para todos los agentes intervinientes y eliminando los intermediarios que existen en un modelo tradicional.

La Administración jugará un papel decisivo como la entidad certificadora de más peso, por no considerarse la única, ya que la que al final pone el dinero a través de las subvenciones.

El producto final consiste en:

- **La infraestructura tecnológica basada en blockchain que registra cada uno de los usos que le da el usuario a la tarjeta ciudadana con capacidad de realizar todas las compensaciones de forma automática siendo transparente para todos los implicados.**

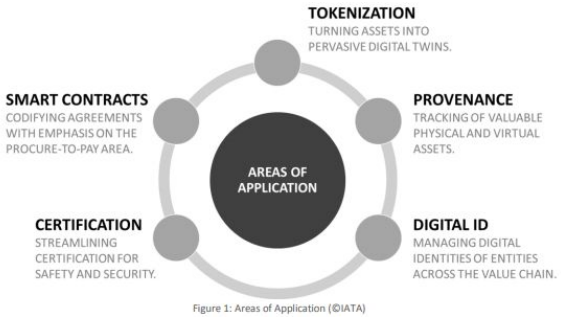


Figure 1: Areas of Application (©IATA)

La propuesta de valor del producto es:

- Disponer de toda la información de todos los operadores de forma inmediata.
- Controlar los movimientos de cada tarjeta de forma sencilla y transparente.
- Transparencia entre los agentes.
- Automatizar la gestión de las compensaciones.
- Almacenar la información de forma segura e inmutable.
- Estructurar la lógica de las compensaciones.
- Crear una capa de contabilidad triple que no afecte al core del funcionamiento del sistema actual.
- Facilitar la interoperabilidad de los distintos servicios que prestan distintos actores.

Problemas que resuelve la tecnología blockchain:

- Falta de confianza en el cálculo de compensaciones.
- Falta de transparencia e inmutabilidad de las transacciones.
- Complejidad en el cálculo de compensaciones tanto por el alto número de transacciones (150k diarias) como por la participación de múltiples actores.
- Retraso en el pago de las respectivas compensaciones.
- Dificultad para incluir nuevos operadores de servicios y administraciones públicas.

2.3 Mercado objetivo

Por un lado, este proyecto cubre una necesidad que es común a todas las tarjetas ciudadanas que se han implantado en España: el sistema de compensación entre los agentes, la confianza, la trazabilidad y el acceso a nuevos actores en el sistema de uso y compensación de dicho medio.

No todos los ayuntamientos la han implantado, quizás por no resolver o no dar seguridad en estos aspectos, por lo que además de los lugares dónde ha sido implementada, se tiene como objetivo aquellos que no la hayan incorporado. No obstante, todos ellos, de alguna u otra forma, poseen algún medio con el que el ciudadano se identifica para obtener servicios subvencionados por lo que en este caso, el objetivo es consolidar todos ellos en uno solo.

El objetivo principal es la mejora o implantación de la tarjeta a aquellas Administraciones Públicas (AAPP) prestatarias de servicios. Por tanto, el mercado objetivo en España incluiría a ayuntamientos, en concreto a aquellos de más de 50.000 habitantes, cabildos y diputaciones, consejos insulares, comunidades autónomas y el propio Estado.

El potencial de este producto extiende su mercado más allá de la tarjeta ciudadana. Existen otros como el uso de tarjetas de transporte en servicios públicos, o de fidelización, como pueden ser las aerolíneas, gasolineras,o el retail. Este producto crea una infraestructura de compensación entre los agentes con total transparencia entre los participantes. Es decir, esta infraestructura tecnológica es útil para todos los sistemas de compensación en los que intervienen diferentes agentes, sea necesario registrar de forma sencilla, transparente, fiable e inmutable las transacciones realizadas por cada usuario, y se realice una compensación entre agentes por el uso de los servicios por parte del usuario de la tarjeta.

El desarrollo de los sistemas de compensación automatizados se puede realizar sobre Smart Contracts, contratos inteligentes sobre blockchain, ofreciendo una ventaja competitiva respecto a otras soluciones. Los Smart Contracts incorporan una diferencia tecnológica categórica respecto a los actuales sistemas ya que, embebida en la blockchain, ofrece una forma efectiva de implementar las compensaciones al poder ejecutarse y hacerse cumplir por sí mismos, de manera autónoma y automática, sin intermediarios ni mediadores, y evitando los problemas de interpretación que se generan en el lenguaje común. Además, los Smarts Contracts, al ser visibles para todos y no poder modificarse, ofrecen un carácter descentralizado, inmutable y transparente.

2.4 Variables de mercado

Solo centrándose en los municipios de España, hay 145 localidades con más de 50.000 habitantes. En el ámbito de las grandes empresas, todas poseen de alguna forma tarjetas de fidelización. En algunos casos son propias y en otros permiten operar en varios establecimientos. Estas últimas son nuestro objetivo. En el Anexo 1 se encuentra la lista de municipios con más de 50.000 habitantes.

En cuanto a la posibilidad de pivotar el producto hacia las tarjetas de fidelización, un estudio de American Express España señala que “más del 80% de los consumidores nacionales utiliza alguna tarjeta de fidelización”, siendo el valor medio de los regalos recibidos al año superior a los 200 euros. Adicionalmente en algunos comercios, como las estaciones de servicio Carrefour, o la Cadena Meliá, obtienen respectivamente el 60% y 40% de las ventas gracias a estos programas de fidelización. Con estos valores se constata la importancia de las aplicaciones de esta tecnología en un entorno cada vez más competitivo, en el que los sectores comercial están evolucionando para lograr una experiencia de usuario más personalizada y que aporte mayor valor añadido.

No obstante, en un informe de Maritz (http://www.maritzmotivation.com/customer-loyalty) se concluye que el 70% de los usuarios terminaban por abandonar estos programas de fidelización ante la imposibilidad de alcanzar las recompensas. Esta pérdida de atractivo, la saturación del mercado ante la aparición de múltiples

programas de varios sectores (incluso repetidos), la falta de digitalización y la caducidad de los puntos conseguidos, terminan por saturar al cliente y generan el efecto contrario al deseado.

Por lo tanto, una aplicación que permita tener estos programas de fidelización unificados en una única plataforma transparente para las partes, supone una solución disruptivo en el sistema actual. Por este motivo la tecnología blockchain agrega valor a un sistema en el que son las entidades certificadoras las que asignan los puntos de recompensa. Los vales, o puntos, tendría un protocolo de 'tokenizar' que generaría un 'token' en el Smart Contract. Estos tokens tendrían un valor en correspondencia con el activo real y se podrían eventualmente comercializar en la plataforma blockchain. En el Anexo 2 se incluye un estudio de algunas tarjetas de fidelización que existen en el mercado español.

2.5 Competidores

Las plataformas de fidelización se gestionan actualmente utilizando bases de datos tradicionales (relacionales) y software específico (ad-hoc) para el cálculo de las compensaciones entre agentes.

En el mercado existen varias empresas que han implantado en el territorio español la tarjeta ciudadana, aunque ninguna ha utilizado tecnología blockchain.

Algunas de las que han implantado este tipo de soluciones son:

- Hiberus https://www.hiberus.com
- Wdreams https://www.wdreams.com/
- Deloitte https://www2.deloitte.com/es/es.html

El producto que se presenta en este documento va más allá de la tarjeta ciudadana, pues gestiona todas las transacciones que se realizan a través de los sistemas implementados en estos sistemas y que son de interés para todos los agentes del ecosistema utilizando infraestructura blockchain y con un sistema de compensaciones ya implementado.

No se descartan alianzas estratégicas con algunas de las empresas que tengan una propuesta de solución con blockchain a las tarjetas de fidelización. Esto implica tener un punto de partida en el sistema de compensaciones en blockchain de la tarjeta ciudadana, por lo que se realizaría una integración vertical hacia atrás.

La solución propuesta tiene que otorgar flexibilidad a la incorporación de nuevos agentes, la posibilidad de aplicarse a otro tipo de tarjetas que no necesariamente tienen que ser tarjetas ciudadanas (como las tarjetas de fidelización, o las tarjetas de transporte). En este sentido, la infraestructura planteada es válida para sistemas donde intervengan varios agentes, interese tener registrado de forma sencilla, transparente, fiable e inmutable las transacciones realizadas por cada usuario, y exista un sistema de compensación entre los agentes por el uso de los servicios por parte del usuario de la tarjeta.

Otros competidores a tener en cuenta son: la startup Benebit y la compañía Loyyal.

Benebit ha lanzado una plataforma que ofrece a los consumidores la posibilidad de convertir los puntos de fidelización en tokens (criptomonedas), que posteriormente se podrán utilizar para comprar productos en línea de manera similar a la moneda fiat. Aunque no es realmente el sistema que se persigue. El objetivo de Benebit es introducirse en el mercado de retail online al eliminar el sistema tradicional que implica tener numerosas

tarjetas de fidelización, algutinándolas en una única tarjeta y aplicación que puede dar soporte a miles de negocios en todo el mundo.

- https://tarjetabenebit.com/
- https://www.aecoc.es/innovation-hub-noticias/una-plataforma-basada-en-blockchain-convierte-los-puntos-de-fidelizacion-en-tokens-criptomonedas/

La misma filosofía de este proyecto es el que está trabajando Loyyal con el gobierno de Dubai. Está desarrollando un sistema bajo blockchain que proporcione transferencia de valores entre los participantes en programas de fidelización. Este proyecto persigue unificar los sistemas de fidelización en uno solo, para intentar lograr el concepto de red conocido como "Internet de la fidelización".

3.- ANÁLISIS INTERNO

3.1 Desarrollo del Trabajo

Se trata de un desarrollo ex profeso para la Administración, siendo esta la principal impulsora de la acción debido a los enormes beneficios que le reportará la solución.

Se prevé que la contratación se realice mediante licitación pública mediante el correspondiente proceso de contratación. Para tal efecto se diseñarán los respectivos pliegos de prescripciones técnicas y administrativas que definan las condiciones bajo las que la empresa adjudicataria habrá de desarrollar el producto. Estas condiciones técnicas se basarán en el Plan Tecnológico del producto descrito en la sección 5 del presente documento, documentación que habrá que desarrollar en detalle para la confección de los pliegos.

3.2 Equipo de desarrollo y puesta en marcha

Se contará con personal técnico cualificado existente por parte de la administración. Por parte de la empresa adjudicataria, las labores y responsabilidades de cada equipo son las siguientes:

Equipo técnico de la administración:

En el equipo técnico designado por la administración para la coordinación y ejecución del contrato, se identifican los siguientes roles:

- La figura del Responsable del Contrato, encargado de velar por el cumplimiento del contrato y el nivel de calidad de los trabajos realizados, supervisando el desarrollo de los mismos.
- Uno o varios Responsables de Servicio realizarán el seguimiento de los servicios concretos demandados. Son los encargados de asegurar el envío de los datos a la blockchain, así como el seguimiento de los hitos del proyecto, las pruebas de concepto del producto, pruebas pilotos, etc.

Equipo técnico de la empresa adjudicataria:

La empresa adjudicataria que desarrollará el producto facilitará el equipo técnico necesario para cumplir los plazos estipulados, identificándose los siguientes roles:

- El Responsable del Proyecto, por parte del adjudicatario, es la figura encargada de la comunicación con el responsable del Contrato y la supervisión global de los acuerdos incluidos en éste.
- Un Jefe de Proyecto, encargado de la implantación y operativa, apoyado por el Equipo de Proyecto.
- El Equipo de Proyecto, con los recursos suficientes encargados de la ejecución de los trabajos demandados.

3.3 Labores Comerciales

Con el objeto de dar a conocer este novedoso producto entre posibles actores interesados como las administraciones públicas, operadores de transporte, ..., se prevé la asistencia a congresos donde se expondrá la solución desarrollada haciendo especial hincapié en la innovación que aporta y en sus beneficios para todos los actores.

Cada vez es más patente la necesidad de innovar en la administración pública, un mensaje que está calando en los responsables públicos y políticos. Debemos aprovechar la existencia de soluciones novedosas e innovadoras como la presente y los enormes beneficios que aporta a todas las partes con el fin de concienciar a todos, tanto al sector público como a la ciudadanía, en impulsar la innovación en el Sector Público; este ha de ser nuestro mensaje, y nuestro principal valor.

No solo se pretende asistir a congresos a nivel nacional, sino que también se busca el alcance en congresos de ámbito internacional con temáticas de innovación y la transformación digital.

En paralelo se realizará una labor de presencia en los medios con la publicación de notas de prensa desde el gabinete de la institución, así como la publicación de artículos en revistas especializadas. En este punto se ejecutará un plan de presencia en medios adaptados a la solución con el principal objetivo de dar a conocer la solución a ciudadanía y empresas, así como concienciar de las bondades de su uso.

3.4 Financiación

El proyecto se financiará con fondos públicos, o bien directos de las propias administraciones implicadas, o a través de mecanismos de financiación externos como pueden ser los programas nacionales y/o europeos de fomento de la innovación.

En el caso concreto de la Unión Europea (UE) ya existen líneas específicas para proyectos basados en tecnología blockchain. La UE ya ha dado un paso de gigantes en febrero de 2018 al lanzar el Observatorio y Foro de Blockchain junto con una inversión de 300 millones de euros para proyectos que respalden esta tecnología de cadena de bloques. El reto europeo es abordar en las mejores condiciones el mercado digital único, en el que la “naturaleza descentralizada y colaborativa del blockchain” deberá jugar un papel clave, siempre que exista una estrecha colaboración entre los países miembros, generando un mercado único que evite enfoques fragmentados y garantizando la interoperabilidad y un despliegue amplio de los servicios.

Entendemos que nuestro proyecto encaja de forma directa con estos objetivos de la agenda de la UE y concretamente dentro de su nuevo programa marco para la investigación y la innovación europeas, ‘Horizonte Europa’, que sucede al exitoso Horizonte 2020.

4.- DAFO

El análisis DAFO es una herramienta analítica que establece el punto de partida del pensamiento estratégico. Permite desarrollar un esquema mental con el que realizar un análisis correcto de la situación competitiva de una empresa. Analiza el contexto competitivo desde dos vertientes:

- Desde una vertiente externa identifica las amenazas y oportunidades que se dan en el sector o industria de la empresa, siendo necesario superarlas o aprovecharlas pero siempre anticipándose a las mismas.
- Desde una vertiente interna identifica las fortalezas y debilidades de la empresa, siendo necesario analizar sus recursos y capacidades (producción, marketing, financiación, organización, ...).

¿Cuáles son los puntos negativos? Las amenazas y las debilidades. ¿Cuáles son los puntos positivos? Las oportunidades y las fortalezas. ¿Qué se consigue? Ser capaces de responder a las siguientes preguntas: ¿Cómo se puede explotar cada fortaleza? ¿Cómo se puede aprovechar cada oportunidad? ¿Cómo se puede minimizar cada debilidad? ¿Cómo se puede defender de cada amenaza?

- Debilidades: son aspectos que limitan o reducen la capacidad de desarrollo efectivo de la estrategia de la empresa y constituyen una amenaza para la organización y deben, por tanto, ser controladas y minimizadas.
- Fortalezas: son capacidades, recursos y posiciones alcanzadas y, consecuentemente, ventajas competitivas que deben y pueden servir para explotar oportunidades.
- Amenazas: son toda fuerza del entorno que pueda bien impedir la implantación de una estrategia o bien reducir su efectividad, incrementar sus riesgos o los recursos necesarios para su implantación o reducir sus ingresos esperados o rentabilidad.
- Oportunidades: es todo aquello que pueda suponer una ventaja competitiva para la empresa o representar una posibilidad para mejorar la rentabilidad de la misma o aumentar la cifra de sus negocios.

En cada categoría conviene hacerse una serie de preguntas:

- Oportunidades: ¿A qué buenas oportunidades se enfrenta la empresa? ¿De qué tendencias del mercado se tiene información? ¿Existe una coyuntura en la economía del país? ¿Qué cambios de tecnología se están presentando en el mercado? ¿Qué cambios en la normatividad legal o política se están presentando? ¿Qué cambios en los patrones sociales o estilos de vida se están presentando?
- Amenazas: ¿A qué obstáculos se enfrenta la empresa? ¿Qué están haciendo los competidores? ¿Se tienen problemas de recursos de capital? ¿Puede algunas de las amenazas impedir totalmente la actividad de la empresa?
- Fortalezas: ¿Qué ventajas tiene la empresa? ¿Qué hace la empresa mejor que cualquier otra? ¿A qué recursos de bajo costo o de manera única se tiene acceso? ¿Qué percibe el mercado como una fortaleza? ¿Qué elementos facilitan obtener una venta?
- Debilidades: ¿Qué se puede mejorar? ¿Qué se debería evitar? ¿Qué percibe el mercado como una debilidad? ¿Qué factores reducen las ventas o el éxito del proyecto?

Con el fin de responder a todas estas consideraciones se establece el análisis presentado en la tabla mostrada a continuación.

DAFO	
Debilidades	
a	Tener que poner de acuerdo a múltiples y diversas organizaciones participantes.
b	La escalabilidad del sistema, especialmente con vistas a la inclusión de nuevos actores y aplicaciones, pudiendo incrementar notablemente el número de transacciones por segundo.
c	Falta de madurez de la tecnología (no está suficientemente probada).
d	Falta de estándares.
e	Desconocimiento sobre la tecnología blockchain o equiparación con criptomonedas, pudiendo limitar el apoyo por parte de las organizaciones participantes al proyecto.
f	Ausencia de conectividad en el momento de las transacciones si se requiere operativa en tiempo real.
Amenazas	
a	Normativa legal (o ausencia de la misma) en el ámbito de la tecnología blockchain.
b	Percepción y adopción de la tecnología por los reguladores nacionales e internacionales.
c	Resistencia al cambio por parte de las organizaciones participantes.
d	La seguridad de la infraestructura, especialmente los “endorsing peers” que son los responsables de validar las transacciones, así como los nodos del servicio del Orderer que son los responsables de ordenar las transacciones, generar los bloques y difundirlos a los respectivos peers.
Fortalezas	
a	Proporciona simultáneamente transparencia, inmutabilidad y automatización en el cálculo de las compensaciones debidas a los Operadores de Servicio (OS) por parte de las Administraciones Públicas.
b	No requiere modificar la arquitectura de la solución actual sino añadir una nueva capa (contabilidad triple).
c	Innovación en el sector de la movilidad.
d	Relativo bajo coste de desarrollo y despliegue de la infraestructura de Blockchain.
Oportunidades	
a	Ciclo de vida de la tecnología blockchain (Gartner Hype Cycle) todavía no ha alcanzado la meseta de productividad.
b	Incentivos y ayudas de las instituciones políticas para proyectos desarrollados con tecnología blockchain.
c	Las políticas e iniciativas tanto a nivel público, transparencia, como a nivel privado, de reducción de la economía sumergida.
d	La infraestructura blockchain permitirá desarrollar un ecosistema sobre el que desplegar nuevas aplicaciones y servicios y a la que sumar nuevas organizaciones participantes.
e	Poder trasladar fácilmente esta solución basada en blockchain a otros entornos con problemáticas similares.

5.- PLAN TECNOLÓGICO

5.1 Introducción

El back-office para la tarjeta ciudadana sobre blockchain dará soporte a todo tipo de servicios prestados por la administración -directamente o mediante empresas públicas- y empresas privadas a usuarios anónimos o registrados. Se pretende, mediante la puesta en marcha del sistema, dar respuesta a la necesidad de control económico de los servicios prestados a través de esta tarjeta de forma fiable y automatizada.

La efectiva compensación económica entre los agentes la blockchain implica establecer una **stable coin** cuyo cambio sea fijo con la moneda nacional, de tal forma que las relaciones entre el rol Banco y el resto de los agentes se limite al intercambio de la stable coin por fiat y viceversa. Se define una segunda stable coin en el sistema a modo de puntos, que podrán suponer descuentos en determinados servicios (puntos que tendrán un tipo de cambio en la stable coin paritaria fiat diferente para cada servicio)

5.5.1 Participantes

Los roles incluidos en el sistema son los siguientes:

- AP Administración Pública
- OP Operadores de Servicios
- US Usuarios de Servicios
- DR Distribución y Recarga de Tarjeta
- BC Bancos

AP Administración pública

El despliegue del sistema lo liderará una de las administraciones públicas participantes, aunque la relación ideal entre ellas es la de federación.

Las administraciones públicas implicadas serán las responsables de dar acceso al sistema al resto de agentes implicados de tal forma que:

- Únicamente se incluyan los prestadores de servicios que la administración considere elegibles. En concreto, todos los servicios públicos que desde un punto de vista técnico puedan ser incluídos.
- La inclusión de usuarios del servicio en el sistema será un derecho de todos aquellos ciudadanos susceptibles de recibir servicios por parte de las administraciones públicas presentes en el sistema.
- La inclusión en el sistema de DR de tarjetas y BC bancos seguirán criterios económicos, de eficacia y eficiencia, realizándose siempre bajo procedimientos transparentes.
-

Las administraciones públicas serán las responsables de dar entrada en el sistema al resto de participantes, siendo la responsable de emitir los respectivos certificados.

OP Operadores de servicios

Este rol puede ser jugado por empresas públicas prestadoras de servicios (servicios de transporte, sanitarios, deporte, ocio, etc.), o por empresas privadas cuyos servicios estén alineados con las políticas de la Administración. El mayor volumen de las transacciones registradas consistirán en cancelaciones de la tarjeta por uso de los servicios que los operadores prestan.

US Usuarios

El registro del usuario es obligatorio para aquellos servicios que incluyan algún tipo de bonificación a colectivos determinados y debe de promoverse el registro entre aquellos que no reciban subvenciones con el fin de enriquecer los datos recogidos.

Esto implica el mantenimiento de una base de datos de usuarios fuera de la infraestructura blockchain que utiliza un identificador que anonimiza la información del usuario, el cual es el que se escribe en la blockchain. Esta base de datos incluirá todos los datos personales que justifiquen la recepción por parte del usuario de bonificaciones en los servicios.

A modo de ejemplo, la tarjeta *TEN+* debe incluir nombre, apellidos, número de DNI, municipio de empadronamiento y fecha de nacimiento para la obtención de tarjetas de transporte que incluya descuentos para menores de 30 años o mayores de 65. El registro de estos colectivos implica la obligatoriedad de personarse físicamente en las oficinas de las administraciones que financian las subvenciones a las que se pretenda acceder (u otras entidades en las que éstas deleguen).

Fuente: www.titsa.com

DR Distribución y recarga de tarjetas

Una parte importante del producto es la que da acceso a los usuarios a su registro en el sistema y permite la recarga de la tarjeta ciudadana.

Este rol podrá ser adoptado por las propias administraciones públicas, por los prestadores de servicios, por los bancos o de forma independiente. Esto significa que todos los participantes a excepto de los usuarios podrán ser además distribuidores-recargadores de la tarjeta o podrán existir agentes en el sistema cuyo único rol sea el de distribuir y recargar la tarjeta ciudadana.

La AP, administración pública, puede ceder la gestión de este servicio a terceros, que serán compensados económicamente por prestarlo (p.e. estancos) en un porcentaje de la recarga que se realice. Entre las fuciones de estos participantes se encuentra:

- Distribución de tarjetas que no incluyan subvenciones ya sean anonimizadas o no.
- Distribución de tarjetas que supongan derecho a subvenciones.
- Recarga de la tarjeta con bonos tiempo.
- Recarga de las tarjetas monedero.
- Retirada de tarjetas.

BC Bancos

El papel de los bancos en el sistema consiste en el cambio entre dinero fiat y la stable coin del sistema de forma que una vez realizadas las compensaciones, los operadores cambien la stable coin recibida como contraprestación a sus servicios por moneda fiat.

5.5.2 Assets

Los assets del sistema son:

- DN Dinero
- SC Stable Coin
- PT Puntos
- IF Información
- BT Bono tiempo

DN Dinero

Los US usuarios deberán recargar su tarjeta mediante pagos a los DR distribuidores recargadores de tarjetas, a cambio recibirán SC stable coin que podrán intercambiar por servicios o BT bonos tiempo.

SC Stable Coin

Con la que se recargan las tarjetas de los US usuarios y se realizarán las compensaciones por parte de las AP administraciones públicas a los OP operadores de servicios.

PT Puntos

Las AP administraciones públicas y los OP operadores de servicios podrán poner en marcha políticas de fidelización de los US usuarios que obtendrían puntos por determinados usos de los servicios incluidos en la tarjeta que serán canjeables por descuentos en otros servicios. Esto permite a los operadores privados ofrecer descuentos en servicios públicos al hacer uso de sus servicios siempre que estén alineados con políticas de la Administración (p.e. descuento en el transporte público para acceder a un centro comercial).

BT Bono Tiempo

Determinados servicios incluidos en la tarjeta pueden ser susceptibles de ser prestados mediante derechos adquiridos de forma temporal. Se trata por tanto de una “tarifa plana” que da acceso a determinados servicios. Por ejemplo, los abonos mensuales o semanales en el transporte público, o los que dan acceso a instalaciones deportivas municipales.

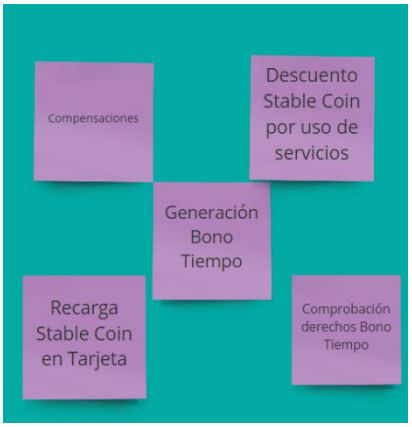
IF Información

Esta debe ser relativa a la utilización de los servicios ofertados por los OP operadores. Con el fin de realizar la compensación de los servicios prestados, la AP administración debe contar con esta información que da derecho a contraprestaciones económicas y por tanto debe ser considerada como un activo.

5.5.3.- Smart Contracts

El sistema debe incluir al menos los siguientes smart contracts:

- Compensaciones
- Descuento de SC en tarjeta del usuario por uso de servicios
- Comprobación de derechos de uso de servicios en bono tiempo
- Recarga de SC en tarjeta
- Generación de bono tiempo



Compensaciones

Es el servicio de compensación económica a los OP operadores de servicios por el uso de servicios.

Estas compensaciones se calculan de diferentes maneras:

- En los servicios subvencionados en los que el usuario abona parte del coste del servicio, la Administración debe compensar al operador por un valor igual al coste del servicio restando la parte abonada por el usuario.
- En los servicios que se prestan contra derechos incluidos en bonos tiempo, la Administración compensará al operador por la totalidad del valor del servicio prestado.

Descuento de SC en tarjeta del usuario por uso de servicios

Se produce cuando un usuario tiene que abonar total, o parcialmente, el coste de un servicio que vaya a recibir. La tarjeta ciudadana mantendrá un saldo en SC Stable Coin del que se descontará esta compensación.

Comprobación de derechos de uso de servicios en bono tiempo

Cuando un usuario haga uso de un servicio mediante un bono tiempo, el sistema validará el uso comprobando que el usuario ha adquirido y está en vigor el mismo.

Recarga de SC en tarjeta ciudadana

Los DR distribución recarga de la tarjeta incrementa el saldo en SC stable coin de la tarjeta ciudadana cuando un usuario de la misma la recargue y cederá el saldo a la Administración tras descontar el pago por el servicio de recarga en caso de que sea aplicable.

Generación de bono tiempo

Los DR distribución recarga de la tarjeta generará el bono tiempo en el sistema cuando un usuario lo adquiera. En caso de que este bono tiempo cuente con subvenciones de algún tipo, se comprobará el derecho a la misma en el sistema. El DR abonará a la AP administración pública el coste del BT bono tiempo tras descontar el coste del servicio de recarga en caso de que la recarga no la realice directamente la propia AP administración pública.

5.2 Arquitectura del sistema

La primera pregunta que debe responderse al diseñar un backoffice para tarjeta ciudadana sobre tecnología blockchain, es si realmente esta tecnología es la más adecuada y qué plataforma de entre las existentes es la que ofrece la mejor respuesta a los requerimientos exigidos.

5.2.1 ¿Necesitamos una Decentralized Ledger (DL) / Blockchain (BC)?

Antes de nada, se definen una serie de conceptos análogos que pueden ser utilizados para resolver el problema y que habitualmente se prestan a confusión por su similitud funcional.

Una DL es un sistema formado por un conjunto de nodos. Cada nodo es un recurso que puede almacenar datos, ejecutar software y comunicarse con el resto de nodos. No existe un intermediario que controle los intercambios de información que son las transacciones que se producen en el sistema. Cada nodo guarda un registro de todas las transacciones que se realiza en el sistema. Un algoritmo de consenso se encarga de mantener estos registros mutuamente consistentes. En algunos sistemas todos los nodos contienen exactamente la misma réplica del registro completo de transacciones, en otros diferentes nodos pueden almacenar diferentes partes superpuestas de dicho registro que son mutuamente consistentes. Cabe destacar que la esencia de una DL no es solo el registro distribuido de las transacciones entre los distintos nodos, sino la existencia de un control central que regule las transacciones que se producen.

Una Blockchain (BC) es un caso particular de DL que realiza el registro de transacciones en una cadena de bloques. Cada bloque contiene un conjunto de transacciones coincidentes en el tiempo y un hash del bloque anterior, de modo que si se modifica su contenido, su hash cambiaría y, por ende, el de todos los bloques posteriores. Por lo tanto, a partir del hash del bloque más reciente se puede comprobar fácilmente si se ha modificado algún bloque de la cadena.

Una base de datos (DB) es un sistema de información que almacena los datos en un único nodo, o distribuidos en varios con un único propietario responsable de su administración. Es decir, desde el punto de vista del almacenamiento, puede ser distribuido, pero desde el punto de vista del control, está centralizado.

A continuación se muestra un formulario a modo de diagrama de flujo que, a través de varias preguntas, guía la necesidad de una DL o una BC en el proyecto:

Pregunta	Respuesta	Sí	No
¿Existen actores independientes que necesiten tener un almacenamiento compartido de datos? Los actores son personas u organizaciones que necesitan compartir datos para coordinar las acciones que realizan.	La respuesta es sí porque tanto las Administraciones Públicas (AP) como los Prestadores de Servicios (PS) necesitan compartir los datos de las cancelaciones de los Usuarios de los Servicios (US) para poder realizar el cálculo de las compensaciones debidas por dichos servicios.	Vete a la siguiente pregunta.	No es necesario una DL y, por lo tanto, tampoco una BC porque se requiere compartir datos. Omite las siguientes preguntas.

¿Existen actores independientes que necesiten escribir sobre la DL?	La respuesta es sí porque los distintos Prestadores de Servicios (PS) necesitarán escribir sobre la DL las cancelaciones de los Usuarios de sus Servicios (US).	Vete a la siguiente pregunta.	No es necesario una DL y, por lo tanto, tampoco una BC porque solo existe un único actor responsable del contenido del almacenamiento compartido de datos. Omite las siguientes preguntas.
¿Existe un intermediario de confianza? ¿A los actores les cuesta decidir quién debe estar en control del almacenamiento compartido de datos?	La respuesta es no porque no existe un intermediario de confianza. Tanto las Administraciones Públicas (AP) como los Prestadores de Servicios (PS) son parte interesada en el cálculo de las compensaciones debidas a los Operadores de Servicios (OS) por las Administraciones Públicas (AP).	No es necesario una DL y, por lo tanto, tampoco una BC porque resulta más simple una tecnología de DB. Omite las siguientes preguntas.	Vete a la siguiente pregunta.
¿El registro de transacciones debe ser inmutable?	La respuesta es sí porque no existe un intermediario de confianza. Para garantizar dicha inmutabilidad, las tecnologías de DB necesitan un intermediario de confianza mientras que las de DL utilizan un algoritmo de consenso, siendo prescindible dicho intermediario.	Es necesario una BC porque, al no haber un intermediario de confianza, la inmutabilidad se garantiza mediante un algoritmo de consenso.	¿?

5.2.2. ¿Qué tipo de BC se necesita?

A continuación se responde a tres de preguntas que permite definir qué tipo de BC se necesita para el proyecto.

1. ¿Todas las transacciones son públicas?

Las transacciones en sistemas no permisionados, como Bitcoin, son visibles para todos sus usuarios, mientras que aquellas en sistemas permisionados, como Corda, son únicamente visibles para un número reducido de participantes según se haya configurado.

En el caso propuesto, todas las transacciones no tienen (ni se prevé que tengan) que ser públicas. Resulta muy conveniente que determinadas transacciones sean únicamente visibles para un número reducido de participantes en función de sus características o acuerdos con otros participantes, pudiendo ser además configurable. Por todo ello, se opta por un tipo de BC privada.

2. ¿Todos los actores son conocidos?

Los sistemas de criptomonedas pueden ser utilizados por usuarios anónimos, mientras que los utilizados por las instituciones financieras deben implementar regulaciones de Know Your Customer (KYC), requiriendo una gestión de la identidad de sus usuarios.

Por un lado, los tipos de BC no permisionadas (por ejemplo, sistemas de criptomoneda) no tienen barreras de participación, utilizando claves públicas (direcciones) como pseudónimo. Por otro lado, los permisionados (por ejemplo, aquellos utilizados por instituciones financieras) utilizan sistemas de gestión de identidad para identificar y admitir participantes, pudiendo estos sistemas ser centralizados o descentralizados.

En nuestro caso, todos los actores deben ser conocidos para garantizar la transparencia del sistema, siendo necesario un subsistema de gestión de identidad para identificar, admitir, gestionar y rechazar participantes. Este subsistema es responsabilidad de las Administraciones Públicas (AP). Por lo tanto requiere estar centralizado. Por todo ello, se opta por un tipo de BC permisionada.

3. ¿Qué requisitos necesita el algoritmo de consenso?

Los datos almacenados en la cadena de bloques deben estar sincronizados en los distintos nodos mediante un algoritmo. En algunos tipos de BC todos los nodos replican el contenido de la cadena de bloques y en otros diferentes nodos pueden contener datos superpuestos. En cualquier caso, los datos deben mantenerse mutuamente consistentes en en los distintos nodos mediante un algoritmo de consenso.

Los requisitos de un algoritmo de consenso incluyen la escalabilidad en el número de nodos, el número de transacciones por segundo, el uso de energía para su ejecución, la finalidad de las transacciones (período durante el cual una transacción aún no es definitiva) y la vulnerabilidad ante el fraude.

Si se requiere un número alto de transacciones por segundo, del orden de millares, la mayor parte de las opciones se limita a BC permisionadas.

En el caso de estudio, en cuanto al número de nodos, no se necesita (ni se prevé necesitar) un gran número. En cuanto al número de transacciones por segundo, éste será del orden de las centenas de miles de transacciones por día. En cuanto al uso de la energía, éste debe ser mínimo para reducir los costes asociados a la ejecución del algoritmo de consenso. En cuanto a la finalidad de las transacciones, éste debe ser tal de modo que exista un cierto margen durante el cual una transacción aún no sea definitiva ya que las cancelaciones en muchos casos se registran a posteriori de producirse debido a la ausencia de conectividad. Finalmente, en cuanto a la vulnerabilidad ante el fraude, ésta debe ser tal que garantice tanto la inmutabilidad del registro como la consistencia de las copias almacenadas en los distintos nodos.

5.2.3 ¿Por qué Hyperledger Fabric?

A continuación se describen los motivos principales por los que se ha optado por este tipo de BC para resolver nuestro problema:

- Porque es un tipo de BC privada en la que se pueden añadir participantes con un permiso de acceso.
- Es un tipo de BC permisionada que dispone de un sistema de gestión de identidad que permite identificar y admitir participantes, pudiendo de este modo elegir tanto quién podrá acceder, como el nivel de acceso del mismo.
- Es un tipo de BC que permite elegir el algoritmo de consenso que mejor se ajuste a las necesidades del problema.

Arquitectura de Hyperledger Fabric

La arquitectura básica de Hyperledger Fabric de un único canal se muestra en la siguiente figura:

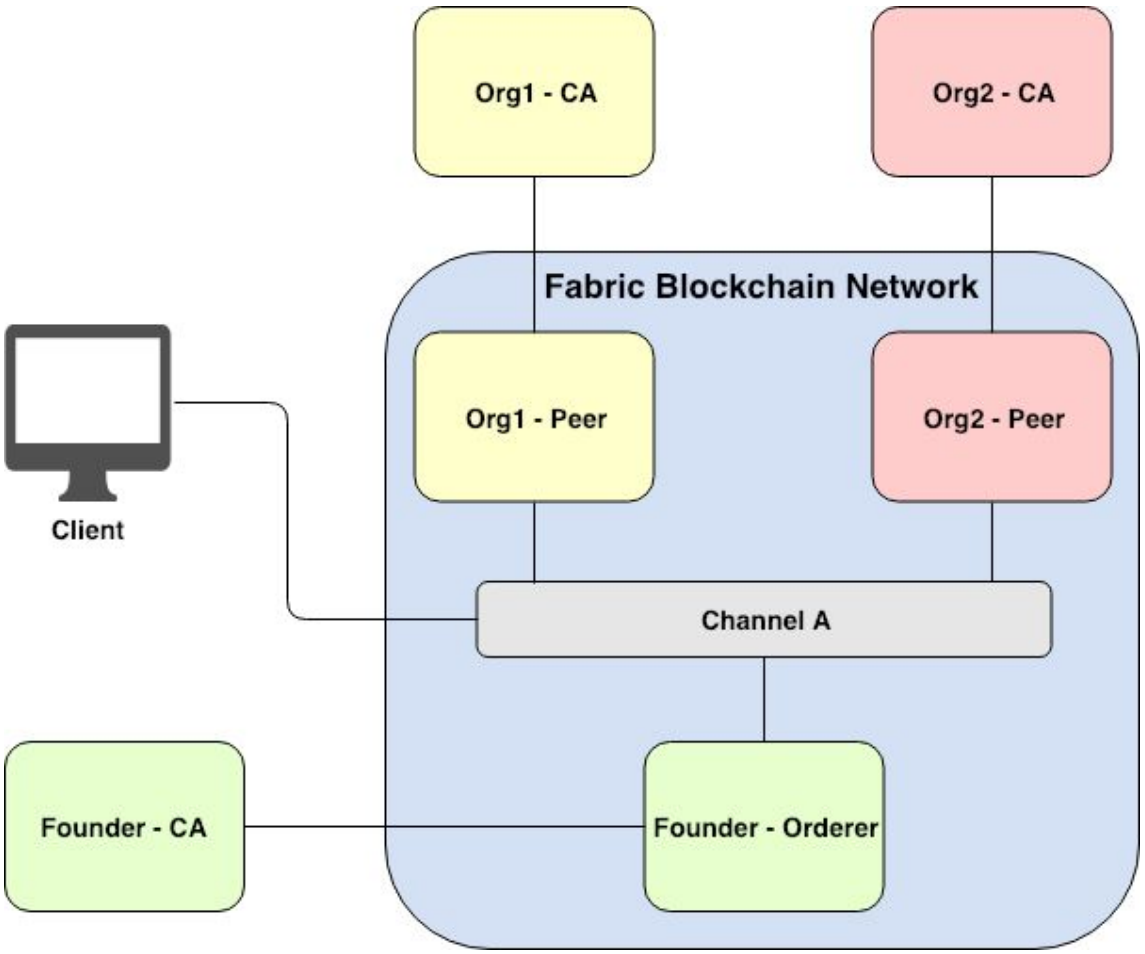


Figura: Arquitectura básica de Hyperledger Fabric con un único canal.

A continuación se describen brevemente sus componentes principales:

Canales

Los canales permiten a las organizaciones participantes unirse y comunicarse entre sí. Pueden considerarse como un túnel que permite a una organización comunicarse en secreto con otras organizaciones participantes del mismo canal. Cualquier otro miembro que no participe en dicho canal no tendrá acceso a ninguna transacción e información asociada a ese canal. Una organización puede participar en múltiples canales al mismo tiempo. En este proyecto las organizaciones participantes son las Administraciones Públicas (AP) y los Operadores de Servicios (OP). Los canales permiten que determinadas transacciones sean únicamente visibles para un número reducido de participantes en función de sus características o acuerdos con otros participantes. Por ejemplo, acuerdos a los que hubieran llegado determinadas Administraciones Públicas (AP) con determinados Operadores de Servicios (OP) sujetos a cláusulas de privacidad con respecto de terceros participantes.

Peers

Los peers son los nodos de la BC que almacenan todas las transacciones de un determinado canal. Cada peer puede unirse a uno o más canales según sea necesario. Sin embargo, el almacenamiento para diferentes canales en el mismo peer está separado. De esta forma se garantiza que la información confidencial se comparte solo con los participantes permitidos en dicho canal. En nuestro caso, el número de peers se distribuirá entre los participantes en función de su entidad e interés en la solución adoptada, principalmente las Administraciones Públicas (AP) y los Operadores de Servicios (OS). De este modo se eliminan los costes de operación de la infraestructura para los participantes de menor entidad.

Orderer

El Orderer es uno de los componentes más importantes. Se utiliza en el mecanismo de consenso. Es responsable de ordenar las transacciones, crear un nuevo bloque de transacciones ordenadas y distribuirlo a todos los peers del respectivo canal. Apache Kakfa proporciona actualmente un mecanismo de consenso con tolerancia a fallos, óptimo en términos de rendimiento (del orden de mil transacciones por segundo). El gran inconveniente de esta solución es que se debe de confiar en los nodos del servicio del Orderer. Este servicio sólo puede ser controlado actualmente por una única organización participante. En desarrollo, aún no disponible para un sistema en producción, se está desarrollando un mecanismo de consenso tipo BFT que permite a distintas organizaciones participantes controlar conjuntamente este servicio, contribuyendo a éste con nodos propios. En este proyecto el Orderer es una responsabilidad de las Administraciones Públicas (AP).

Autoridades de Certificación (CA)

Las Autoridades de Certificación (CA) son responsables de administrar los certificados de usuario. Más específicamente, Hyperledger Fabric utiliza un certificado estándar X.509 para representar permisos, roles y atributos para cada usuario, pudiendo consultar o invocar cualquier transacción en cualquier canal en función de los permisos, roles y atributos que le haya sido concedidos. Hay dos formas de implementar Fabric CA. En primer lugar, configurar Fabric CA sin extender el servidor LDAP. Con esta configuración, Fabric CA se usaría para registrar, autenticar y revocar usuarios así como emitir certificados de usuario. En segundo lugar, configurar Fabric CA con la extensión del servidor LDAP. Con esta configuración, Fabric CA se usaría sólo para emitir certificados de usuario, delegando al servidor LDAP el resto de tareas administrativas. En nuestro caso, el sistema de gestión de identidad (Founder - CA) será responsabilidad de las Administraciones Públicas (AP) mientras que cada uno de los restantes participantes será responsable de la concesión o revocación de permisos, roles y atributos para cada usuario de su organización (Org - CA).

Clientes

Los clientes son aplicaciones que interactúan con la BC de acuerdo con sus permisos, roles y atributos, tal como se especifica en su certificado derivado de la CA de su respectiva organización. Las aplicaciones cliente pueden interactuar con la BC de Fabric de dos formas: SDK o CLI. Fabric SDK proporciona un conjunto de funciones enriquecidas que son apropiadas para su uso en producción. Normalmente, la aplicación cliente se conecta a través de un servidor API RESTful utilizando el SDK de Fabric como una biblioteca para comunicarse con la BC. Actualmente admite Node.js y lenguajes Java aunque versiones de Python, Golang y REST SDK están en desarrollo. Fabric CLI es apropiado para su uso en desarrollo o mantenimiento. En nuestro caso, las aplicaciones registran las cancelaciones de los servicios prestados por los Operadores de Servicio (OS) en representación de las Administraciones Públicas (AP). Cabe destacar que este registro se efectúa a posteriori de producirse debido a la ausencia de conectividad.

Smart Contracts

En Hyperledger Fabric, por un lado, los Smart Contracts gestionan la lógica de las transacciones, es decir, la lógica de negocio. En el proyecto automatizan el cálculo de las compensaciones debidas a los Operadores de Servicios (OP) por las Administraciones Públicas (AP).

Chaincode

Los Chaincode gestionan la lógica de los Smart Contracts definidos en ellos. Para desplegar un Chaincode se debe instalar en todos los peers asociados a un canal determinado y posteriormente, a través del Orderer, crear una instancia del mismo en dicho canal. Al crear esta instancia se puede definir una endorsement policy que especifica qué peers necesitan generar el mismo resultado de una transacción antes de que la transacción pueda registrarse en la cadena de bloques de todos los peers de dicho canal.

Endorsement peer

Un peer especificado en la endorsement policy se denomina endorsement peer. Tiene una cadena de bloques local así como un Chaincode instalado. Aquellos peers no especificados se denominan committing peers, y tienen únicamente una cadena de bloques local. En nuestro caso, el número de endorsing peers se distribuirá entre los participantes que sean parte interesada en el cálculo de las compensaciones, principalmente las Administraciones Públicas (AP) y los Operadores de Servicios (OS) mientras que el número de committing peers dependerá de cuestiones tales como el rendimiento, la escalabilidad, la redundancia, el coste, ...

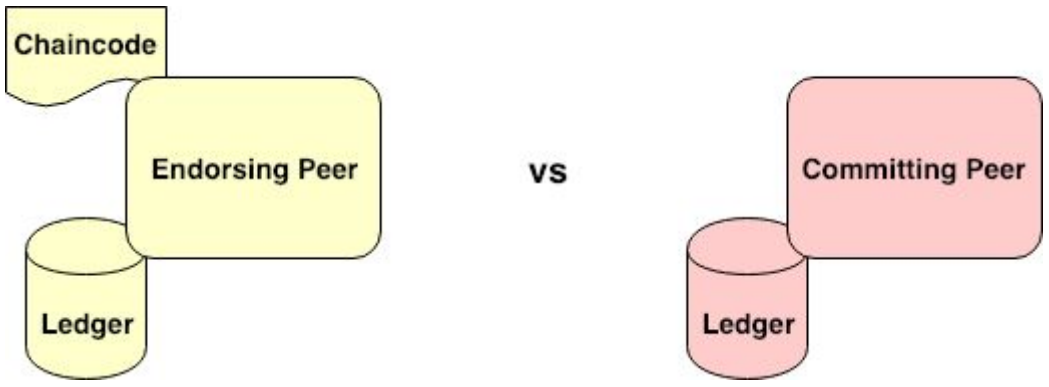


Figura . Endorsing vs Commiting Peer.

World State

El ledger de cada peer está formado por una cadena de bloques y un World State. La cadena de bloques contiene el historial de todas las transacciones para cada chaincode de un canal determinado mientras que el World State mantiene el estado actual de las variables para cada chaincode en particular. En Fabric existen actualmente dos opciones de base de datos para el World State: LevelDB y CouchDB. LevelDB es una base de datos clave-valor mientras que CouchDB es una basada documentos. En nuestro caso, hemos optado por CouchDB porque soporta funciones avanzadas como operaciones de consulta basadas en objetos JSON, indexación o replicación mientras que LevelDB solo soporta funciones limitadas.

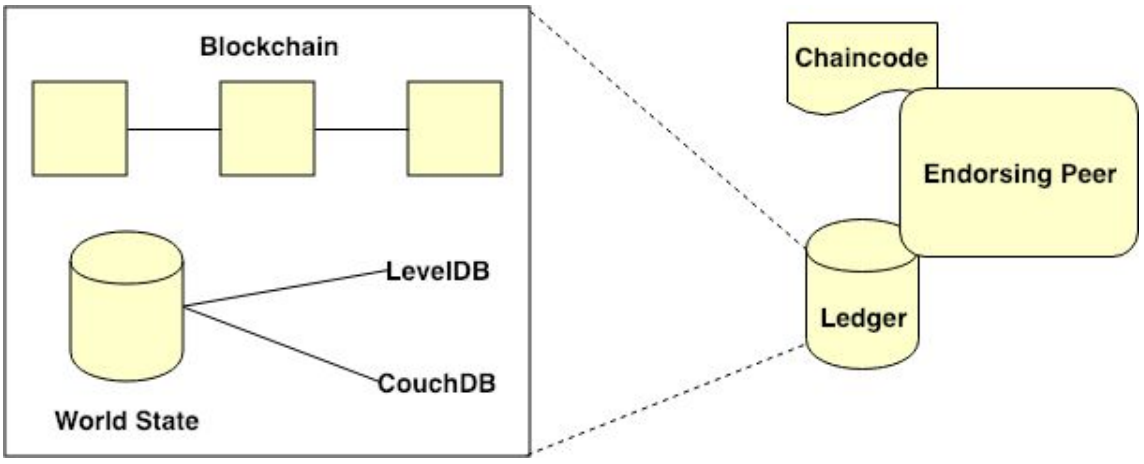


Figura . Blockchain y World State.

System Chaincode

Cabe destacar que en el Orderer se instalan un tipo especial de Chaincode denominado System Chaincode cuyo objetivo es recopilar información de configuración relativa a la red, los canales y el sistema subyacente para garantizar el correcto funcionamiento de la máquina virtual de Fabric. De hecho, también se instalan en todos los peers aunque por simplicidad no se muestran en la siguiente figura.

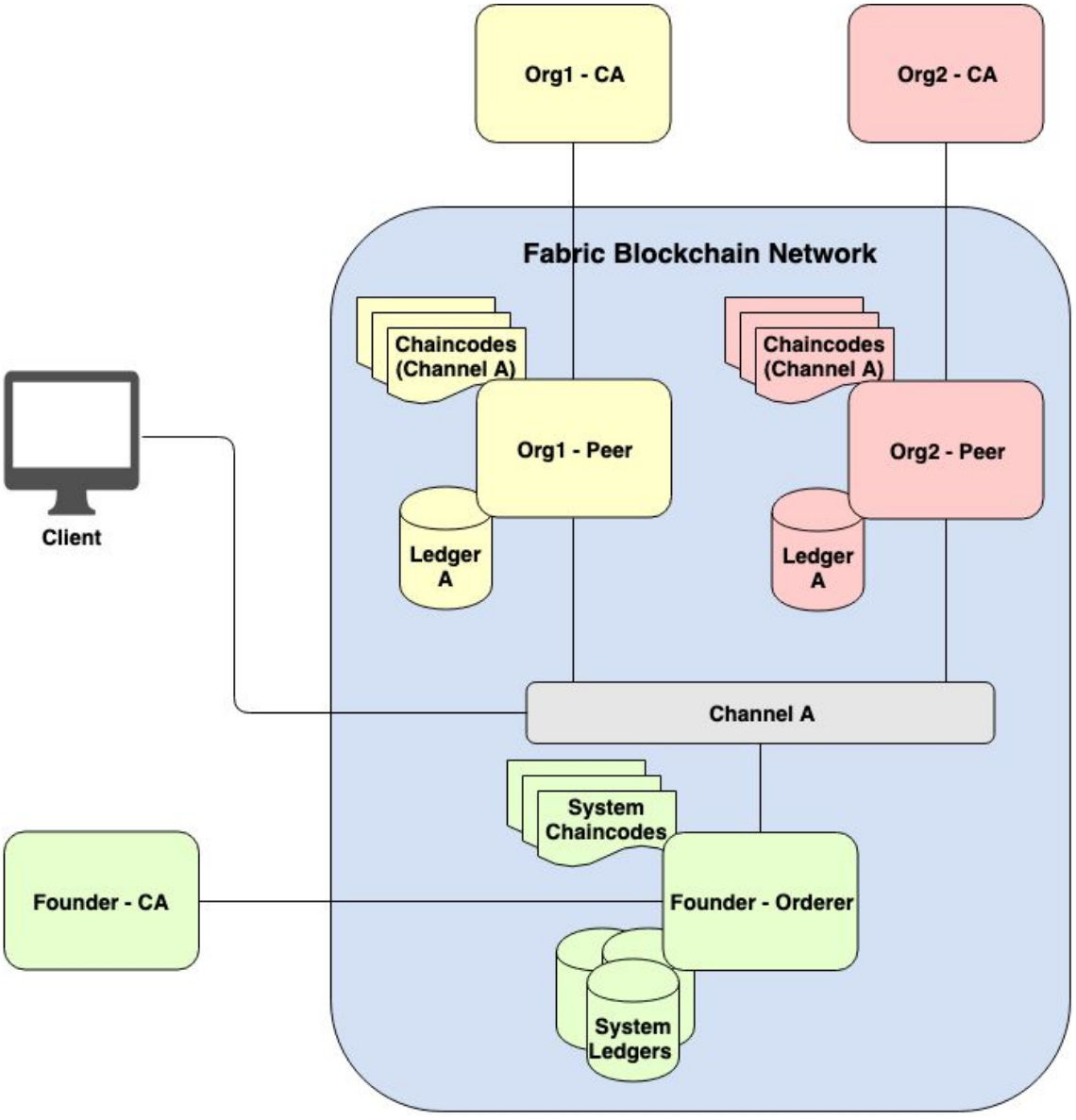


Figura . Arquitectura de Hyperledger Fabric con un único canal.

La siguiente figura muestra la arquitectura de Hyperledger Fabric con varios canales. Las organizaciones que se unen a un canal pueden compartir información (transacciones) sin que sea visible para el resto de organizaciones que no formen parte de ese canal. En este proyecto las organizaciones participantes son las Administraciones Públicas (AP) y los Operadores de Servicios (OS). Los canales permiten que determinadas transacciones sean únicamente visibles para un número reducido de participantes en función de sus características, o acuerdos con otros participantes. Por ejemplo, acuerdos a los que hubieran llegado determinadas Administraciones Públicas (AP) con determinados Operadores de Servicios (OS) sujetos a cláusulas de privacidad con respecto de terceros participantes.

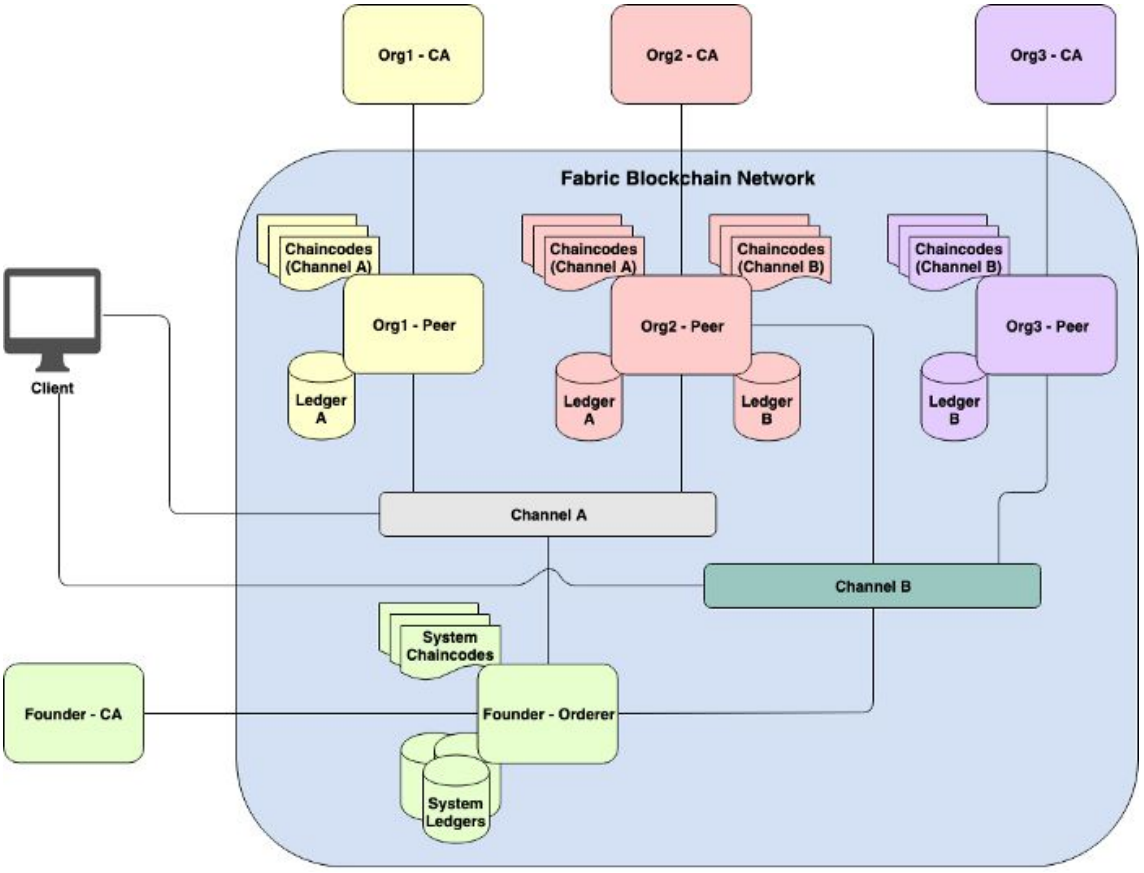


Figura . Arquitectura de Hyperledger Fabric con varios canales.

A continuación se muestra la arquitectura de Hyperledger Fabric con varios canales en un entorno de producción:

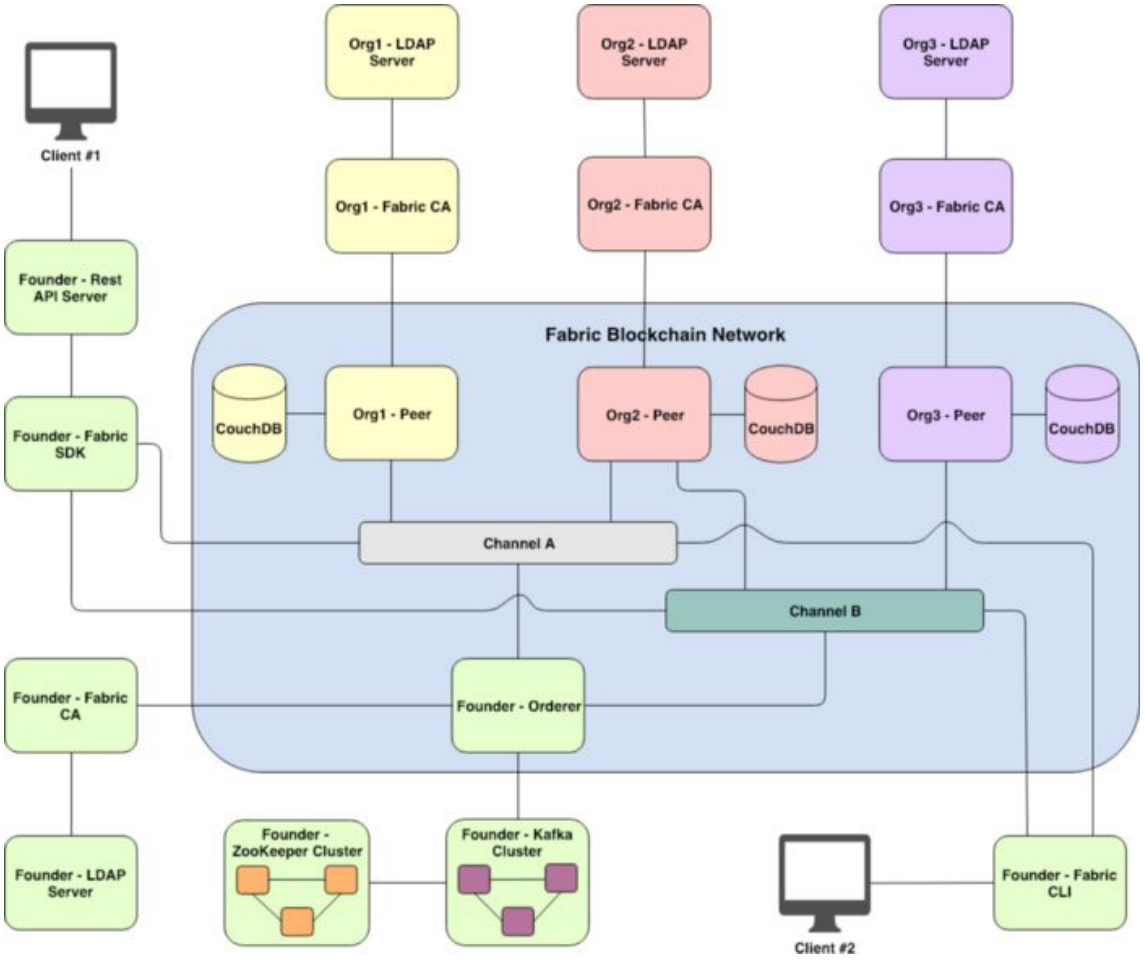


Figura . Arquitectura de Hyperledger Fabric con varios canales en un entorno de producción.

En Hyperledger Fabric, el consenso se alcanza a través de una serie de comprobaciones de endorsement, validación y versionado que se llevan a cabo en múltiples etapas y niveles. Múltiples fases garantizan la autorización, la aprobación, la sincronización de los datos entre participantes, el orden de las transacciones y la corrección de los cambios antes de escribir cualquier bloque de transacciones en la cadena de bloques.

Fabric utiliza un mecanismo de consenso permisionado basado en votos que asume que todos los participantes son parcialmente confiables, pudiendo dividirse en tres fases:

- Endorsement (pasos 1-3 de la siguiente figura)
- Ordenamiento (pasos 4-5 de la siguiente figura)
- Validación y Commitment (paso 6 de la siguiente figura)

El flujo de trabajo sobre el consenso de una transacción se muestra en la siguiente figura:

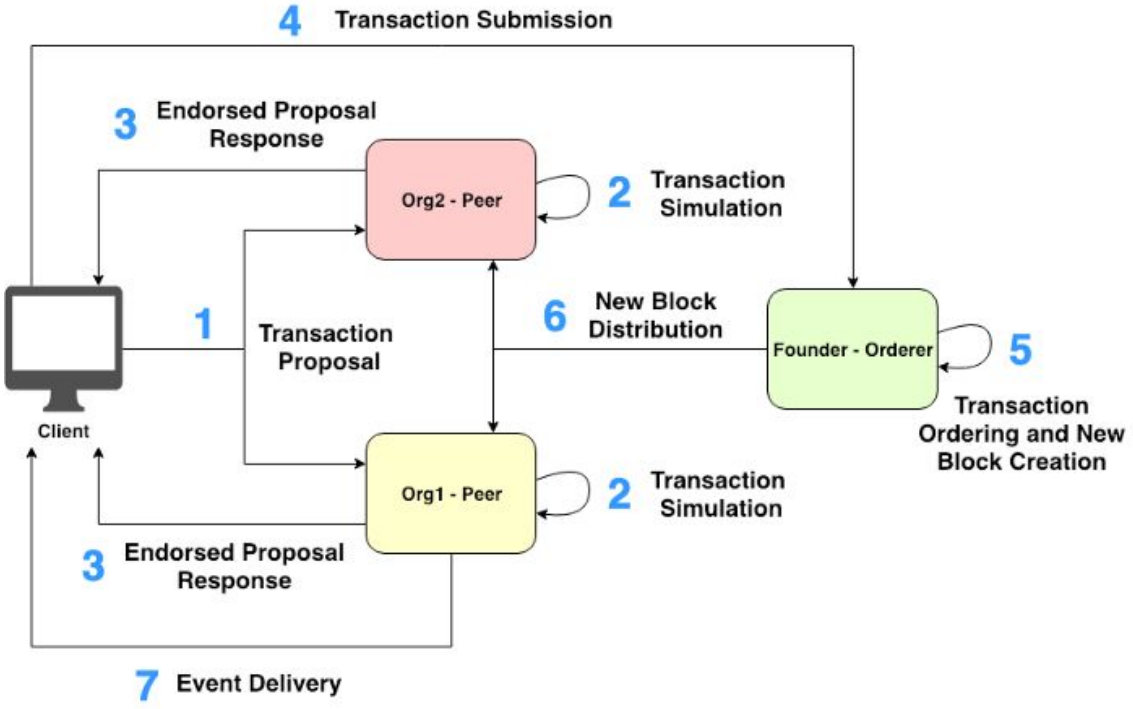


Figura . Flujo de trabajo sobre el consenso de una transacción.

A continuación se describen brevemente sus pasos principales:

1. El cliente realiza una propuesta de transacción, la firma con el certificado del usuario y la envía a un conjunto predeterminado de endorsing peers del canal en cuestión.
2. Cada uno de los endorsing peers verifican la identidad del usuario y su autorización a partir de la propuesta de transacción. Si la verificación es satisfactoria, los endorsing peers ejecutan la transacción y se genera una propuesta de respuesta que posteriormente respaldan mediante con su certificado.
3. El cliente recopila y verifica las propuestas de respuesta respaldadas por los endorsing peers.
4. El cliente envía la transacción junto con las propuestas de respuesta respaldadas al Orderer.
5. El Orderer ordena las transacciones recibidas, genera un nuevo bloque de transacciones ordenadas y firma el bloque generado con su certificado.
6. El Orderer difunde el bloque generado a todos los peers (tanto a los endorsing como a los committing) del canal en cuestión. Cada peer se asegura de que cada transacción del bloque recibido haya sido firmada por los respectivos endorsing peers. Posteriormente cada uno de ellos realiza una verificación del versionado que valide la corrección de cada transacción de dicho bloque, comparando los parámetros de entrada de cada transacción con su propio World State. Si la verificación es satisfactoria, dicha transacción se marca como válida y se actualiza el estado de su respectivo World State. En caso contrario, se marca como no válida y no se actualiza su respectivo World State. Finalmente, el bloque recibido se añade a la cadena de bloques local de cada peer, independientemente de si el bloque contiene o no transacciones no válidas.
7. El cliente recibe información sobre su propuesta de transacción a través de un servicio de subscripción orientado a eventos.

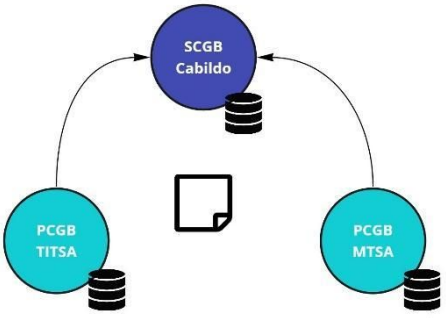
5.3 Implantación del sistema

Actualmente está en funcionamiento la tarjeta de transportes de Tenerife *TEN+* (https://tenmas.es/) gestionada por el Cabildo insular de Tenerife. Es una tarjeta contactless, de pago sin contacto, que puede usarse tanto como tarjeta monedero, como con bonos tiempo. También se puede utilizar el transporte público haciendo uso de la aplicación para teléfonos móviles *Ten+móvil* (https://tenmasmovil.es/) y realizando el pago en metálico.

Esta tarjeta nació con la vocación de convertirse en una tarjeta ciudadana y se pretende que en el futuro pueda ser utilizada con nuevos operadores de servicio. El sistema actualmente en funcionamiento (registro de transacciones sobre una base de datos relacional y software desarrollado de forma específica para el cálculo de las compensaciones) ya está demostrando dificultades a la hora de incluir nuevos actores.

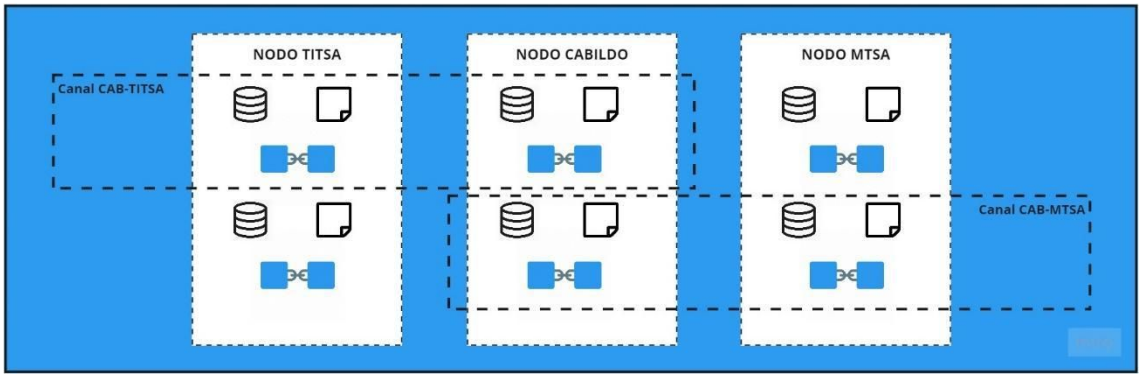
Con el fin de no interferir en el sistema en producción se pondrá en marcha el back office sin entorpecer sus funcionalidades extrayendo aquellos datos necesarios desde diferentes fuentes haciendo uso de automatización robótica de procesos RPA o extracción-transformación-carga de datos ETL.

El sistema cuenta con tres subsistemas, uno para la administración pública -Sistema Central de Gestión del Billetaje o SCGB- y otros dos para cada uno de los operadores importantes -Punto Central de Gestión del Billetaje o PCGB. En cada uno de los subsistemas se registran los datos que son de interés para cada una de las partes, compartiendo gran cantidad de datos entre los diferentes subsistemas.

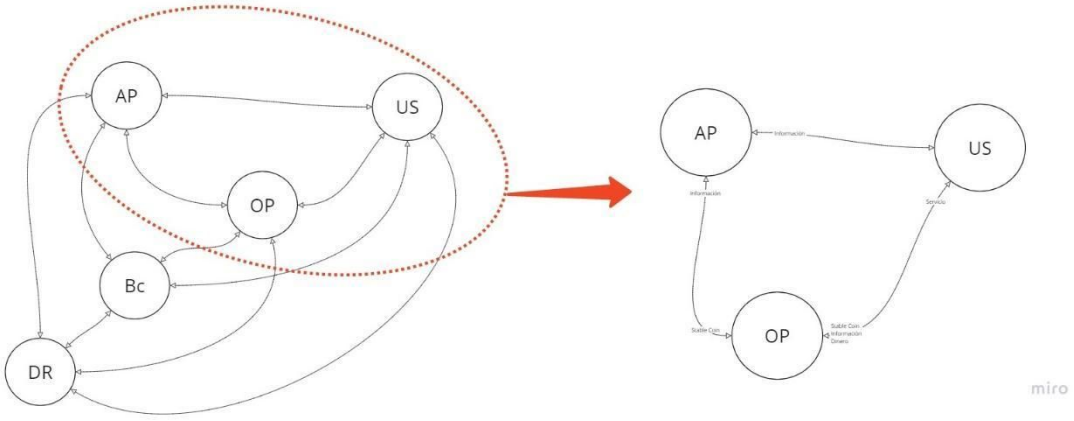


No se pretende migrar de forma completa de un sistema a otro. Una vez que esté en funcionamiento y haya demostrado el back office su estabilidad sobre blockchain, se dejará de registrar los datos sobre transacciones en el sistema actual que seguirá manteniendo otras funciones relativas a la gestión de canceladoras, puntos de venta, etc.

Para aprovechar el sistema de billetaje se iniciará la implantación sobre el sistema actual, migrando de los tres subsistemas a una blockchain con tres agentes y dos canales a modo de cadena mínima viable.



En esta cadena mínima viable únicamente aparecen tres de los cinco participantes y permite poner en marcha una prueba de concepto que añade valor al sistema.



6.- OTROS PLANES OPERATIVOS

6.1 Plan de Marketing

6.1.1 Descripción del Producto / Servicio

Planteamos una nueva tarjeta ciudadana basada en una administración de servicios más flexible y transparente para ciudadanos y empresas colaboradoras.

Inicialmente, la tarjeta irá destinada al uso de transporte público (bus, tranvía, metro,...) a modo de abono de transporte en cualquiera de sus modalidades (abono monedero, abono tiempo, ...), pudiendo ampliarse más adelante a otros servicios prestados por la Administración o por colaboradores privados del ámbito cultural, deportivo, ocio etc.

Esta nueva tarjeta persigue un doble objetivo. Por una parte permite a los usuarios disfrutar de ventajas tales como descuentos y acumulación de puntos canjeables en el ecosistema de servicios. Por otra, pone a disposición de las empresas colaboradoras una serie de canales a través de los cuales se comparten únicamente los datos relevantes para cada perfil, garantizando que la información jamás se podrá perder, modificar o eliminar.

Estas características son posibles porque la nueva tarjeta ciudadana se basa en una infraestructura respaldada por tecnología blockchain que permite reconocer de forma automática, transparente e inmutable a los usuarios de políticas de transporte existentes (abono joven, abono tercera edad, etc.) y a los beneficiarios de descuentos en el uso de estos servicios como consecuencia de la acumulación de puntos, o como premio a conductas sostenibles (por ejemplo, descuentos en caso de haberse trasladado en transporte colectivo o incentivos al usar vehículos de alta ocupación).

Se cubre así una necesidad común a todas las tarjetas ciudadanas que se han implantado en España en referencia al sistema de compensación entre los agentes, la confianza, la trazabilidad y el acceso a nuevos actores en el sistema de uso y compensación de dicho medio, maximizando el control de los movimientos de

cada tarjeta, reduciendo la complejidad y el tiempo de pago en el cálculo y pago de las compensaciones, respectivamente y por tanto, agilizando las compensaciones en su totalidad.

6.1.2 Política de Precios

El objetivo de este servicio es su puesta en marcha y progresiva incorporación de nuevos agentes. Por este motivo durante el primer año de este proyecto liderado por la Administración, no existe una política de precios como tal. A partir del primer año el sistema se debe mantener mediante el pago de un porcentaje sobre el coste de las transacciones. Es decir, por las operaciones realizadas en el ámbito de todas las AAPP participantes que, de forma ideal deberían de constituir una federación/consorcio.

6.1.3 Política de Distribución

El producto no es distribuible. Esta política se enmarca en las labores comerciales desarrolladas en el punto 3.3 de este documento que facilitará el conocimiento de esta novedosa plataforma tecnológica.

6.1.4 Política de Promoción y Comunicación

Como objetivo principal se tiene la mejora o implantación de la tarjeta a aquellas Administraciones Públicas (AAPP) prestatarias de servicios. Por tanto, el mercado objetivo en España incluiría a los Ayuntamientos, en concreto los 145 municipios que hay en España de más de 50.000 habitantes, además de, Cabildos, Consejos Insulares, Diputaciones, Comunidades Autónomas y el propio Estado.

Desde el punto de vista de las grandes empresas, dado que todas ellas poseen de alguna forma tarjetas de fidelización, algunas propias y otras con las que se pueden operar en varios establecimientos, éstas también serían nuestro objetivo.

6.2 Plan de Operaciones (N.A.)

No aplica porque se plantea una solución para sector público

6.3 Plan Jurídico - Fiscal - Laboral (N.A.)

No aplica porque se plantea una solución para sector público pero en el caso de crear una estructura legal, se optaría crear una Sociedad Limitada con un capital inicial estimado de 3.000. Su objeto social es la prestación de soluciones tecnológicas de back office basadas en blockchain para la administración de servicios. La sociedad tendrá un administrador único,o un conjunto de administradores mancomunados en el caso de contar con una federación de administraciones participantes. Contará con seis socios con mismo porcentaje del capital social.

6.4 Plan Financiero

Cadena Mínima Viable con 3 nodos: uno desarrollado por la Administración, el segundo por el adjudicatario y el tercero, la empresa de software.

Ante la dificultad de cuantificar el coste de la Cadena Mínima Viable de tres nodos debido a la estrategia comercial de los proveedores de soluciones con tecnología blockchain, se ha utilizado como referencia un

proyecto liderado por una Administración que tiene similitudes. Es el sistema de "Registro Distribuido de Ofertas y Evaluación Automatizada de las Mismas" desarrollado desde el Gobierno de Aragón cuyo presupuesto de licitación ascendió a 56.725,13€, correspondiendo aproximadamente el 55% del presupuesto a el coste de profesionales y el resto a infraestructura y operación. Estos proyectos son subvencionables hasta en un 85% con fondos europeos al estar alineado con los objetivos de la agenda de la UE, en concreto con el nuevo programa marco para la investigación y la innovación europeas, 'Horizonte Europa'.

En el caso de pivotar al ámbito privado de las tarjetas de fidelización en grandes empresas, el coste será soportado por los participantes que establecerán una federación de servicios.

No se descarta la obtención de ingresos adaptando la infraestructura core a operadores privados aprovechando el know-how adquirido durante el desarrollo de la cadena mínima viable de lanzamiento del proyecto.

7.- CALENDARIO DE EJECUCIÓN

El proyecto se ejecutará en dos plazos diferenciados:

- El producto mínimo viable planteado (una administración público y dos operadores) en el documento se desarrollará en un plazo máximo de seis meses
- En los siguientes seis meses se realizará el mantenimiento inicial del sistema.

Anexo 1: Ayuntamientos con más de 50.000 habitantes

La siguiente tabla presenta los datos recogidos en la encuesta INE 2018.

Posición	Nombre	Población	Provincia
1	Madrid	3 223 334	Madrid
2	Barcelona	1 620 343	Barcelona
3	Valencia	791 413	Valencia
4	Sevilla	688 711	Sevilla
5	Zaragoza	666 880	Zaragoza
6	Málaga	571 026	Málaga
7	Murcia	447 182	Murcia
8	Palma de Mallorca	409 661	Islas Baleares
9	Las Palmas de Gran Canaria	378 517	Las Palmas
10	Bilbao	345 821	Vizcaya

11	Alicante	331 577	Alicante
12	Córdoba	325 708	Córdoba
13	Valladolid	298 866	Valladolid
14	Vigo	293 642	Pontevedra
15	Gijón	271 843	Asturias
16	Hospitalet de Llobregat	261 068	Barcelona
17	Vitoria-Gasteiz	249 176	Álava
18	La Coruña	244 850	La Coruña
19	Granada	232 208	Granada
20	Elche	230 625	Alicante
21	Oviedo	220 020	Asturias
22	Tarrasa	218 535	Barcelona
23	Badalona	217 741	Barcelona
24	Cartagena	213 943	Murcia
25	Jerez de la Frontera	212 879	Cádiz
26	Sabadell	211 734	Barcelona
27	Móstoles	207 095	Madrid
28	Santa Cruz de Tenerife	204 856	Santa Cruz de Tenerife
29	Pamplona	199 066	Navarra
30	Almería	196 851	Almería
31	Alcalá de Henares	193 751	Madrid
32	Fuenlabrada	193 586	Madrid
33	Leganés	188 425	Madrid
34	Donostia-San Sebastián	186 665	Guipúzcoa
35	Getafe	180 747	Madrid
36	Burgos	175 921	Burgos
37	Albacete	173 050	Albacete
38	Santander	172 044	Cantabria
39	Castellón de la Plana	170 888	Castellón
40	Alcorcón	169 502	Madrid
41	San Cristóbal de La Laguna	155 549	Santa Cruz de Tenerife
42	Logroño	151 113	La Rioja
43	Badajoz	150 530	Badajoz
44	Huelva	144 258	Huelva

45	Salamanca	143 978	Salamanca
46	Marbella	141 463	Málaga
47	Lérida	137 856	Lérida
48	Dos Hermanas	133 168	Sevilla
49	Tarragona	132 299	Tarragona
50	Torrejón de Ardoz	129 729	Madrid
51	Parla	128 256	Madrid
52	Mataró	126 988	Barcelona
53	León	124 772	León
54	Algeciras	121 414	Cádiz
55	Santa Coloma de Gramanet	118 821	Barcelona
56	Cádiz	116 979	Cádiz
57	Alcobendas	116 037	Madrid
58	Jaén	113 457	Jaén
59	Orense	105 505	Orense
60	Reus	103 477	Tarragona
61	Telde	102 424	Las Palmas
62	Orihuela	101 321	Alicante
63	Baracaldo	100 435	Vizcaya
64	Gerona	100 266	Gerona
65	Lugo	98 025	Lugo
66	Santiago de Compostela	96 405	La Coruña
67	Cáceres	96 068	Cáceres
68	Las Rozas de Madrid	95 550	Madrid
69	San Fernando	95 174	Cádiz
70	Roquetas de Mar	94 925	Almería
71	Lorca	93 079	Murcia
72	San Cugat del Vallés	90 664	Barcelona
73	El Puerto de Santa María	88 364	Cádiz
74	San Sebastián de los Reyes	87 724	Madrid
75	Cornellá de Llobregat	87 173	Barcelona
76	Melilla	86 384	Melilla
77	Pozuelo de Alarcón	86 172	Madrid
78	Rivas-Vaciamadrid	85 893	Madrid
79	Ceuta	85 144	Ceuta

80	Guadalajara	84 910	Guadalajara
81	El Ejido	84 710	Almería
82	Toledo	84 282	Toledo
83	Chiclana de la Frontera	83 831	Cádiz
84	Talavera de la Reina	83 009	Toledo
85	San Baudilio de Llobregat	82 904	Barcelona
86	Pontevedra	82 802	Pontevedra
87	Torrevieja	82 599	Alicante
88	Coslada	81 860	Madrid
89	Torrente	81 245	Valencia
90	Vélez-Málaga	80 817	Málaga
91	Mijas	80 630	Málaga
92	Arona	79 448	Santa Cruz de Tenerife
93	Avilés	78 715	Asturias
94	Palencia	78 629	Palencia
95	Guecho	78 276	Vizcaya
96	Rubí	76 423	Barcelona
97	Manresa	76 250	Barcelona
98	Fuengirola	75 396	Málaga
99	Alcalá de Guadaíra	75 256	Sevilla
100	Valdemoro	74 745	Comunidad de Madrid
101	Ciudad Real	74 743	Ciudad Real
102	Gandía	73 829	Valencia
103	Santa Lucía de Tirajana	71 863	Las Palmas
104	Majadahonda	71 785	Madrid
105	Molina de Segura	70 964	Murcia
106	Paterna	69 156	Valencia
107	Torremolinos	68 262	Málaga
108	Sanlúcar de Barrameda	68 037	Cádiz
109	Benalmádena	67 746	Málaga
110	Benidorm	67 558	Alicante
111	Estepona	67 012	Málaga
112	Ferrol	66 799	La Coruña
113	Casteldefels	66 375	Barcelona
114	Villanueva y Geltrú	66 274	Barcelona

115	Viladecans	66 168	Barcelona
116	Sagunto	65 669	Valencia
117	Ponferrada	65 239	León
118	El Prat de Llobregat	64 132	Barcelona
119	Collado Villalba	63 074	Madrid
120	La Línea de la Concepción	62 940	Cádiz
121	Irún	61 983	Guipúzcoa
122	Zamora	61 827	Zamora
123	Arrecife	61 351	Las Palmas
124	Granollers	60 981	Barcelona
125	Motril	60 592	Granada
126	Mérida	59 352	Badajoz
127	Aranjuez	59 037	Madrid
128	Alcoy	58 977	Alicante
129	Linares	57 811	Jaén
130	San Vicente del Raspeig	57 785	Alicante
131	Sardañola del Vallés	57 740	Barcelona
132	Ávila	57 657	Ávila
133	Cuenca	54 898	Cuenca
134	Arganda del Rey	54 554	Comunidad de Madrid
135	San Bartolomé de Tirajana	53 588	Las Palmas
136	Boadilla del Monte	52 626	Comunidad de Madrid
137	Utrera	52 617	Sevilla
138	Huesca	52 463	Huesca
139	Elda	52 404	Alicante
140	Torrelavega	51 687	Cantabria
141	Segovia	51 683	Segovia
142	Siero	51 662	Asturias
143	Pinto	51 541	Comunidad de Madrid
144	Mollet del Vallés	51 133	Barcelona
145	Villarreal	50 577	Castellón

Anexo 2: tarjetas de fidelización

Mejores tarjetas de fidelización para ahorrar en facturas

- Tarjeta Visa Vodafone
    - Descuento principal: descuento del 4% en compras aplazadas el primer año y del 2% en el segundo año y sucesivos; y del 0'5% en "forma de pago a fin de mes" que se descuentan de la factura del móvil.
    - Promociones adicional: promoción bienvenida de 30€ de descuento en factura una vez realizada la tercera compra con la tarjeta.
    - Posibilidades de pago: TAE del 26.82% por pago aplazado.

- Tarjeta Global Oficinadirecta
    - Descuento principal: 2% de devolución de recibos de luz, gas, teléfono fijo y móvil e internet, siempre que se mantengan domiciliados unos ingresos mínimos de 1000€ mensuales.
    - Promociones adicionales: con la tarjeta American Express Gold 1% de devolución en compras realizadas con esta y un 5% de bonificación en supermercados durante el primer mes con la tarjeta.

Mejores tarjetas de fidelización para ahorrar en gasolina

- Tarjeta Repsol Máxima
    - Descuento principal: 2% en carburante y 5% en productos de tiendas asociadas a Repsol, Campsa y Petronor.
    - Promociones adicionales: hasta el 30 de junio de 2015 un 3% en Diesel e+10 y Efitec 98, además de descuentos en hoteles, agencias de viajes y alquiler de coches entre otros.

- Tarjeta Repsol Más
    - Descuento principal: descuento directo de 3 céntimos por litro en estaciones Repsol.

- Tarjeta Visa BP
    - Descuento principal:
        - Ahorro en combustible: 6% si se paga de forma aplazada y 3% si se paga a fin de mes.
        - Ahorro en compras: 3% en compras aplazadas y 0'30% si se paga a fin de mes.
    - Promociones adicionales:
        - Ahorro del 10% del importe de las compras en el seguro contratado con Verti.
        - Programa de puntos BP Premier Plus: se acumula un punto por cada litro de gasolina y son canjeables por regalos.
    - Posibilidades de pago: bien pago aplazado bien a final de mes (TAE: 21'84%).

- Tarjeta Visa Cepsa
    - Descuento principal: 3% de descuento directo en estaciones Cepsa y 3% de descuento extra si gastas más de 300€ al mes en establecimientos distintos
    - Promociones adicionales: 1% de descuento en alimentación y agencias de viajes en determinados establecimiento adheridos. El descuento se carga a la cuenta.

- Posibilidades de pago: TAE del 27'24% por pago aplazado. Esta tarjeta también incluye seguro de accidente en circulación, seguro de accidente y asistencia en viaje 24 horas y seguro de protección de compras contra robo o daño de la tarjeta.

- Tarjeta Visa Repsol
  - Descuento principal: 2% de descuento en todas las compras realizadas en estaciones de servicio Repsol, Campsa y Petronor, abonado mensualmente.
  - Promociones adicionales: Si facturas más de 400€ al mes en cualquier establecimiento adherido a Visa, el descuento anterior será de un 3%. Además, hay descuentos en algunos hoteles como NH y Zenit.
  - Posibilidades de pago: El TAE es de un 26'82%.

Mejores tarjetas de fidelización para ahorrar en supermercados y grandes superficies

- Tarjeta El Corte Inglés
  - Descuento principal: 4% del importe de los repostajes de gasolina en Repsol, Campsa y Petronor, que podrán ser canjeados por compras en el Corte Inglés, Hipercor, Supercor, Supercor Express y Opencor en la sección de alimentación, droguería y perfumería.
  - Posibilidades de pago: puedes pagar o bien al mes siguiente, aplazando hasta 3 meses (con gastos de gestión de entre 3 y 12€ dependiendo del importe) o hasta 36 meses (TAE: 19'56%).

- Tarjeta Pass de Carrefour
  - Descuento principal: 1% de todas las compras en alimentación, droguería y perfumería y limpieza y comida de animales.
  - Promociones adicionales: promociones especiales en establecimiento y descuento de un 5% en el recibo de la luz con la compañía EDP, descuento del 8% de carburante en Estaciones de Servicio Carrefour y del 4% en Estaciones de Servicio CEPSA, descuento del 1% en Viajes Carrefour, descuento del 1% de las compras realizadas con la tarjeta fuera de carrefour (siempre que superen los 300€ trimestrales) y descuento del 10% en la tarifa de contrato de Carrefour Móvil.

  - Posibilidades de pago: la tarjeta se puede utilizar como tarjeta de débito o crédito, pudiendo elegir entre pagar al contado o a fin de mes o pagando una mensualidad (TAE: 21'99%).

- Tarjeta Consum
  - Descuento principal:
    - Si tus compras superan los 50€ al mes, descuento del 0'75%
    - Si tus compras superan los 250€ al mes, descuento del 1'25%
  - Promociones adicionales: descuento del 2% en carburante en las gasolineras Repsol, Campsa y Petronor y todos los gastos en estas gasolineras se liquidan en un cargo conjunto al principio del mes siguiente.
  - Posibilidades de pago: puedes pagar al contado o al mes siguiente.

Compañías Aéreas:

- Iberia
    - Es la aerolínea española con el FFP (Iberia Plus) más desarrollado, entendiendo como tal el de mayor número de titulares de su tarjeta y el de mayor número de asociados en su red. Segmenta a sus clientes mediante tarjetas de fidelización, diferenciadas en cuatro categorías según su consumo: clásica, plata, oro y, platino. Algunas de las ventajas destacadas en su programa son: la prioridad en la lista de espera del aeropuerto, un seguro de asistencia en el extranjero, facturación en Business Class, acceso a salas vip o limusinas a disposición del cliente.

- Vueling
    - Si bien el Programa Punto de Vueling llama la atención por su simplicidad – limitándose a los hoteles y los rent-a-car – su ventaja estriba en que, al pertenecer a Iberia, puede igualmente beneficiarse del programa Iberia Plus. Además trata de promover estas reservas de forma online para que el cliente lo gestione todo de forma "paquetizada" ganando de esa manera más puntos en el programa.

- Air Europa
    - Air Europa ha optado por adherirse al programa Flying Blue de Air France y KLM, cuya principal característica es que no otorga puntos sino millas. Aspectos como el precio del billete o la clase del asiento se traducen también en millas para que cuenten en la forma de premiar al cliente. Los pasajeros más destacados pertenecen al Flying Blue Elite, que al igual que otras divide a sus clientes en tres categorías similares.

- BinterMás
    - La Tarjeta BinterMás da una serie de beneficios en relación con el consumo de los productos y/o servicios prestados por las entidades asociadas al Programa.

    - Actualmente las entidades asociadas superan la veintena de empresas.
    - El Nivel BinterMás se obtiene sólo volando con Binter. Se asciende a Nivel Plata con 2.500 puntos y a Oro con 8.000. Mejorando su Nivel de BinterMás aumentarán sus ventajas como prioridad en lista de espera, facilidades de facturación y de atención.