RESULTADOS DOPCHAIN

SOLUCIÓN BASADA EN TECNOLOGÍAS BLOCKCHAIN PARA LA TRAZABILIDAD DE PRODUCTOS DE CALIDAD PROTEGIDA

En	Gijón	, a	29	de	Diciembre	de	2023

1. MEMORIA TÉCNICA

Introducción

El proyecto DOPCHAIN es ejecutado por Fundación CTIC – Centro Tecnológico entre el 1 de enero de 2021 y el 31 de diciembre de 2023. **Esta memoria recoge la descripción de los trabajos realizados durante todo el proyecto, por tanto, incluye las tres anualidades: 2021, 2022 y 2023.**

El proyecto DOPCHAIN se plantea con el objetivo general de desarrollar una solución de trazabilidad basada en tecnologías Blockchain para mejorar la confianza de los consumidores en los productos agroalimentarios de calidad protegida.

Este planteamiento se resume, de forma gráfica, en la siguiente figura.

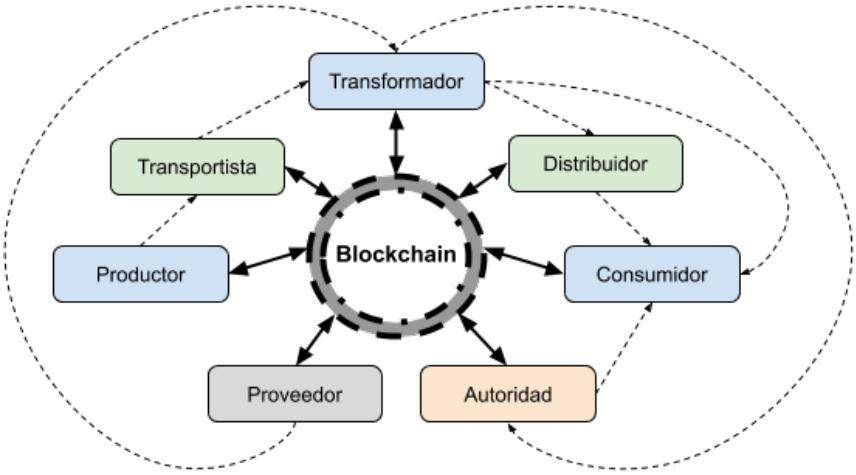

Figura 1: Esquema conceptual de DOPCHAIN

A su vez, la ejecución técnica del proyecto se ha dividido en varios paquetes de trabajo relacionados entre sí:

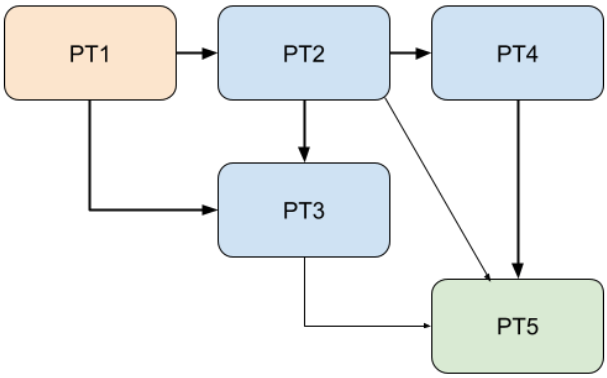

Figura 2: Esquema de relación entre paquetes de trabajo en DOPCHAIN

Justificación 2021

A continuación, se describen las tareas realizadas en este hito de trabajo y los resultados conseguidos.

Paquete de Trabajo 1: Escenario, casos uso y requisitos

El objetivo de este paquete es doble: por un lado la identificación y análisis de sistemas de trazabilidad alimentaria, estándares y casos de uso (basados o no en tecnologías blockchain), para conocer la tipología de actores, sus relaciones más habituales, y mecanismos tecnológicos empleados para orquestar dicha relación, y por otro lado tenemos el objetivo de seleccionar dos casos de uso que servirán de modelo y de prueba para la solución de trazabilidad basada en blockchain a desarrollar en el proyecto DOPCHAIN.

Este paquete se organiza en torno a cuatro tareas, tres de ellas iniciadas y finalizadas en su totalidad en la anualidad 2021, y la restante (T1.3) ha sido iniciada para finalizar en la siguiente anualidad:

- T1.1: Estado del arte: Blockchain y trazabilidad [Finalizada]
- T1.2: Catálogo de requisitos (tecnológicos, usabilidad) y caso de uso [Finalizada]
- T1.3: Seguridad física de las etiquetas [Iniciada]
- T1.4: Diseño conceptual [Finalizada]

A continuación se describen las acciones desarrolladas en cada una de las tareas y los principales resultados alcanzados en cada una de ellas.

T1.1: Estado del arte: Blockchain y trazabilidad.

En esta tarea se ha realizado una consulta a diversas fuentes públicas accesibles desde Internet, como páginas de organismos públicos y empresas, organismos de estandarización y revistas especializadas en cadena de suministro, logística y agroalimentación.

Estándares y buenas prácticas

Entre los principales estándares observados, se han analizado los siguientes:

- EDI, el intercambio electrónico de datos puede considerarse la primera gran tecnología digital innovadora usada de la cadena de suministro. El protocolo de intercambio EDI se basa en estándares reconocidos (como X12, EDIFACT, JSON, XML, etc.) que rigen los formatos de los mensajes transmitidos entre los actores de la cadena.
- El GS1 Global Traceability Compliance Criteria Standard, que describe unos criterios de evaluación para la trazabilidad de toda la cadena. https://www.gs1.org/standards/global-trace-check-list/current-standard
- AESAN, la Agencia Española de Seguridad Alimentaria y Nutrición, publicó una Guía para la aplicación del sistema de Trazabilidad en la empresa agroalimentaria. https://www.aesan.gob.es/AECOSAN/docs/documentos/publicaciones/seguridad_alimentaria/guia_trazabilidad.pdf Esta Guía pretende facilitar la aplicación de las obligaciones recogidas en el artículo 18 del Reglamento 178/2002 por el que se fijan procedimientos relativos a la seguridad alimentaria, debiendo asegurarse la trazabilidad de los alimentos y los piensos en todas las etapas de producción, transformación y distribución.

Sistemas basados en software tradicional

En general, el sistema que gestiona transacciones relacionadas con la trazabilidad basa su lógica de funcionamiento en el empleo de un dato único (por ejemplo, la fecha/hora del pedido o un número de secuencia serializado) que pueda ser rastreado a través de todo el flujo de información en todas las aplicaciones de software relacionadas. Así, se pueden auditar los mensajes y archivos en cualquier punto del sistema para comprobar que son correctos y completos, utilizando la clave de trazabilidad para encontrar la transacción concreta.

En este sentido, hemos observado que hay sistemas y aplicaciones más o menos enfocados a gestionar un tipo de trazabilidad, distinguiendo entre trazabilidad hacia atrás, trazabilidad interna y trazabilidad hacia adelante.

Por otro lado, en cuanto a la arquitectura tecnológica de estos sistemas, se basan en la típica arquitectura cliente-servidor, ya sea implantada en un entorno local dentro del ámbito empresarial, habitualmente en el actor de mayor tamaño de la cadena, o que concentra más información y procesos, como suele ser el elaborador del producto, o ya sea en modo software como servicio (SaaS) empleando un sistema en la nube (cloud) ofrecido por un proveedor de tecnología.

Sistemas basados en blockchain

El empleo del "dato único" o "huella de traza" en los sistemas de trazabilidad tradicionales, casa muy bien con la filosofía de registro distribuido pero único, y otros aspectos de la tecnología blockchain como la transparencia en forma de auditabilidad del registro de transacciones. No es de extrañar pues que desde su aparición, su aplicación a los sistemas de trazabilidad ha sido debatida y experimentada por algunos actores importantes, como cadenas de alimentación, con la ayuda de conocidos proveedores de tecnología, como IBM y otros. En esta subsección se analizarán diferentes iniciativas del ámbito nacional e internacional para establecer qué iniciativas existen, en qué ámbitos se aplican y cuál es su estado de desarrollo.

El modelo tecnológico más habitual observado es la replicación de un sistema de trazabilidad en la nube, pero con el empleo de tecnologías blockchain. Quizás el ejemplo de solución más notorio en este ámbito es el caso de la IBM Food Trust. IBM apostó fuertemente por el sector de la trazabilidad alimentaria en los inicios del desarrollo blockchain. Su plataforma Food Trust utiliza su propia tecnología Hyperledger Fabric.

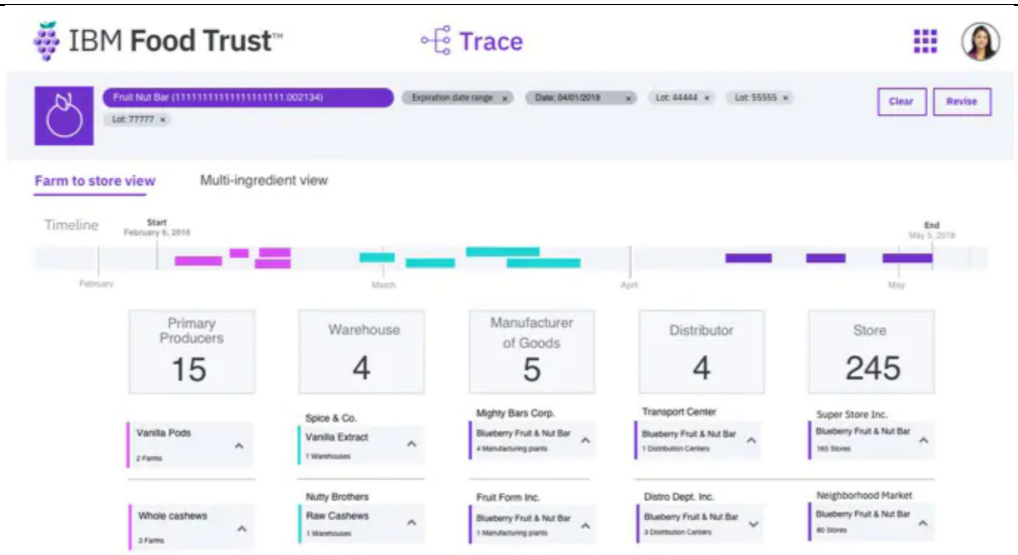

Figura 5. ejemplo del interfaz web de IBM Food Trust

Actualmente es una de las iniciativas de trazabilidad que utiliza tecnología blockchain más extendidas, alcanzado un nivel de implantación comercial. Un ejemplo es su uso por parte de Carrefour, cuyo histórico se puede consultar en este artículo. Como se puede observar, Carrefour fue de las primeras cadenas de supermercados que apostó por esta tecnología, y Walmart puede ser considerada otra de las pioneras en este ámbito. Inicialmente Carrefour introdujo la implantación de esta tecnología para los datos de la producción de cierta carne de pollo, para luego extenderse a otros productos como paso hacia una estrategia generalizada de trazabilidad.

Cabe destacar que la iniciativa de IBM en la trazabilidad alimentaria consiste en una plataforma propietaria, con lo que pese a estar hablando de tecnología blockchain, el uso de esta plataforma estaría sujeto al pago y condiciones impuestas por IBM. Estando por lo general pensada e implementada en grandes empresas. Alejándose del paradigma de desarrollo presente en el desarrollo de la tecnología blockchain de libre uso de una infraestructura común, que muchas veces es beneficioso para que pequeños productores o comercializadores puedan cooperar y competir con la tecnología implementada por estos gigantes de la alimentación.

Otro de los grandes actores dentro del panorama actual Blockchain, es la empresa ConsenSys, desarrolladora del protocolo Quorum que es una versión del protocolo de Ethereum adaptado para trabajar "permisionadamente" en un entorno empresarial. Como ocurre con IBM la trazabilidad alimentaria es un gran escaparate que desde ConsenSys han aprovechado para mostrar las capacidades de su tecnología. Un ejemplo de este tipo de proyectos es el de la trazabilidad del atún en colaboración con la WWF. Este proyecto está desarrollado por Treum, una empresa de ConsenSys, y pone énfasis en la sostenibilidad medioambiental de la actividad. Este parece ser otro de los grandes énfasis que encontramos a lo largo de diferentes soluciones, que buscan atraer al consumidor mediante esta sostenibilidad.

Otra característica de muchas de las soluciones ofrecidas es el empleo de una red blockchain privada o consorciada, es decir, de acceso limitado a un determinado tipo de actores, previamente identificados y autorizados por uno o un conjunto de ellos que actúa como "gobernantes" de la red. Este tipo de redes se basa en la confianza entre actores, no precisamente en la desconfianza como característica de las redes

blochain públicas, donde la participación y auditoría de su registro de transacciones es transparente, no selectiva y fundamentalmente anónima.

En España ha habido diferentes iniciativas que utilizan este modelo de red permisionada para generar un marco de desarrollo adaptado al ecosistema empresarial español. Uno de estos ejemplos es Alastria que utilizan dos redes permisionadas (basadas en Quorum e Hyperledger) para trabajar con diferentes empresas de ámbito nacional en un espacio de trabajo controlado por el consorcio. Dentro de estas redes se han desarrollado a lo largo de los últimos años diferentes pruebas de concepto sobre sistemas de trazabilidad alimentaria, como el vino o la ginebra. Y actualmente están trabajando para implementar la trazabilidad del jamón Navidul Ibérico a través de su sistema a una escala comercial.

Existen otras iniciativas a nivel Nacional que también pretenden acercar la tecnología blockchain al ecosistema empresarial nacional sin ceñirse al uso exclusivo de plataformas permisionadas. Por ejemplo Vottum tiene como objetivo ofrecer el "wordpress para blockchain". Esto se traduce en una suite de desarrollo que facilite a las empresas adoptar o desarrollar aplicaciones blockchain de forma sencilla. Se podría considerar esta estrategia de negocio como Blockchain-as-a-service. En este caso Vottum ofrece a las empresas un stack tecnológico más amigable a desarrolladores blockchain sin imponer el uso de redes permisionadas, dejando libertad al desarrollador para escoger el uso de la red blockchain que más se ajuste a sus necesidades. La trazabilidad agroalimentaria parece ser uno de los focos de Vottum, dentro de este ámbito han lanzado Fish World Track, una ambiciosa iniciativa que pretende implantar la trazabilidad de las empresas pesqueras empezando desde Galicia.

Sistemas de Comercio Justo (basados en blockchain)

Dentro de los sistemas de trazabilidad alimentaria, existe una categoría de soluciones centrada en dar visibilidad no solo al origen de las materias primas, sino especialmente al precio que reciben por ellas sus productores. Algunas de estas soluciones apuestan por la tecnología blockchain, aprovechando su aspecto de transparencia, sin embargo su forma de aplicación varía según los actores involucrados, especialmente los actores tecnológicos, que pueden proveer tanto un protocolo de red privado, de tipo BaaS (blockchain as a service), como público.

Un ejemplo lo observamos en la empresa suiza Koa Switzerland AG (https://koa-impact.com/), que es una importadora de cacao africano procedente de Ghana, con clientes tan importantes como la empresa chocolatera Lindt.

Koa aprovecha la tecnología blockchain, en modalidad BaaS (https://wiki.topl.co/) y mantenida por Topl (https://www.topl.co/), para ofrecer al consumidor y agricultores un medio de seguimiento público de las transacciones correspondientes a los pagos efectuados a los productores.

Los datos se muestran a través de un interfaz web https://products.seedtrace.org/koa que también enlaza con un explorador de transacciones para acceder a los datos "en crudo" registrados en la blockchain de Topl.

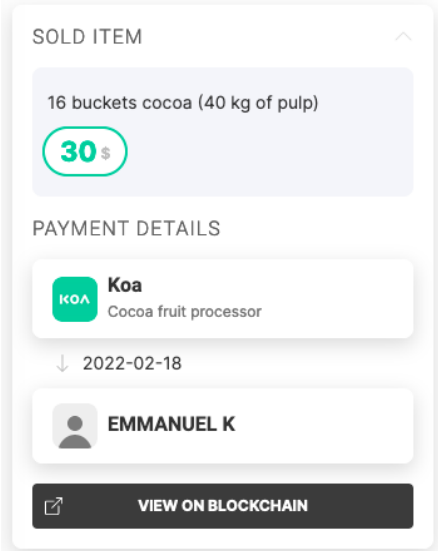

Figura 6. Ejemplo del interfaz webapp de Koa

Aunque el seguimiento del precio a lo largo de la cadena alimentaria es un dato considerado "sensible" por muchos actores de la misma, especialmente para los que están entre los extremos (todos menos productores primarios y consumidores), y es el motivo principal por el que los sistemas de trazabilidad no suelen incluir el mismo entre la información pública que ofrecen, hay estudios (https://www.mdpi.com/2304-8158/10/1/72) que indican que más del 60% de los consumidores están interesados en conocer dos tipos de información que no se les proporciona actualmente: la fecha de cosecha y el porcentaje de precio percibido por los agricultores.

Table 1. Information gaps. Percentage of consumers who declared receiving different packaging labels when purchasing fruit vs. the percentage of those interested in each one. A 20% difference was established as the threshold to identify gaps, which are indicated with **.

Labels	% of Consumers	
	Receive	Wish to Receive
Production area	75.3	84.4
Country of origin *	84.8	82.7
Production method	41.7	79.1 **
Name of fruit *	91.5	74.2
Variety *	64.7	66.8
Packing date	68.9	66.8
Harvest date	0.3	62.9 **
% of the price received by the farmer	0	61.5 **
Quality Seals	42.0	61.1
Best before date	52.3	60.8
Net weight *	70.3	60.4
$ Application of treatments	4.9	54.1 **
Taste, aroma, and texturecharacteristics	4.6	52.3 **
Environmental information	13.1	51.6 **
Nutritional facts	23.7	51.2 **
Category/Class *	46.6	48.1
Preservation method	19.4	47.0 **
Company (Brand) *	73.1	42.8
Beneficial properties	11.7	40.3 **
If it is "Ready-to-eat"	13.1	37.1 **
Preparation recommendations	12.4	36.4 **
$ With seeds or seedless	22.3	33.6
Recommended use	15.9	32.9
Number of pieces *	27.2	30.7
Size (caliber) *	41.7	30.0
Batch number *	57.2	26.9
None	0.7	-

* Indicates that this information is mandatory to be provided irrespectively of fruit. $ indicates information that must be provided only for citrus fruit.

Tabla 1. Lagunas de información en el etiquetado (según el estudio referenciado)

Esta preocupación por el elemento precio se acompasa con cambios legistativos que se están produciendo, como la Ley 16/2021 (https://www.boe.es/diario_boe/txt.php?id=BOE-A-2021-20630), por la que se modifica la Ley 12/2013, de medidas para mejorar el funcionamiento de la cadena alimentaria (Ley de la Cadena Alimentaria o LCA). Esta Ley 16/2021 tiene por propósito transponer a la regulación española de la cadena alimentaria las exigencias de la Directiva (UE) 2019/633 del Parlamento Europeo y del Consejo, de 17 de abril de 2019.

Retos y oportunidades

Los principales retos observados en los sistemas de trazabilidad, tanto aquellos basados en tecnología blockchain como los tradicionales, giran en torno a la confianza en la gestión del flujo de información, con

dos retos muy relacionados entre sí, como son poder garantizar la veracidad de la información y la honestidad de los actores que la suministran.

Reto 1. Aumentar la confiabilidad de la información registrada

El aspecto de veracidad de la información no es algo que se solucione por el simple hecho de que las información haya sido registrada mediante una plataforma blockchain. En realidad depende de otros mecanismos y estrategias, que pueden implementarse con o sin tecnología blockchain. Por ejemplo, un aumento de automatización e integración entre sistemas de la cadena evita errores o manipulaciones más fácilmente introducibles desde sistemas manuales.

También el empleo de sistemas físicos de protección de la "huella de traza" para evitar su reutilización o falsificación, pueden contribuir a la confiabilidad en la información manejada por el sistema, especialmente dando seguridad al consumidor final.

Reto 2. Aumentar la confiabilidad de los actores de la cadena

El hecho de adoptar entre los actores un sistema de registro distribuido, donde cada uno es responsable de la información suministrada, y a la vez participa del control del sistema de forma "mancomunada", introduce por sí un elemento de "vigilancia mutua" que evita normalmente que uno de los actores tenga demasiado control y pueda imponer sus intereses. Sin embargo, aunque esta forma de operativa B2B sea la más ampliamente adoptada por las soluciones blockchain basadas en trazabilidad observadas, hay una actor importante de la cadena que queda al margen: el cliente o consumidor final. Éste suele verse obligado a confiar en el resto de actores, sin posibilidad real de auditar el proceso de registro seguido, ya que la plataforma blockchain empleada suele ser privada y accesible únicamente para B2B, no para B2C.

T1.2: Catálogo de requisitos (tecnológicos, usabilidad) y caso de uso

Siendo el objetivo principal del proyecto DOPCHAIN desarrollar un sistema de trazabilidad basado en tecnologías blockchain, hemos determinado que dicho sistema conlleva una infraestructura tecnológica de registro distribuido, basada en una plataforma blockchain conocida, y además una o varias aplicaciones de usuario (software) que permitan tanto el registro como consulta de información relativa a la traza de productos agroalimentarios de calidad protegida.

Basándonos en el análisis previo realizado, se analizaron y seleccionaron aquellos requisitos que hemos considerado mínimos para los diferentes componentes y fases del proyecto, y que debe satisfacer el sistema para que esté dentro de los cánones esperados. Así, hemos detallado dichos requisitos agrupándolos en tres apartados:

- Requisitos generales.
- Requisitos de los sellos de calidad.
- Requisitos de codificación y etiquetado.

En cuanto a los **requisitos generales**, se han tenido en cuenta las características funcionales que debe tener un sistema de trazabilidad hacia atrás, considerando la tipología de actores y productos a tratar más comunes. En el siguiente cuadro pueden verse los requisitos de medios de acceso y uso esperado de la plataforma blockchain del proyecto por cada tipo de actor.

Actores	Medios Acceso	Uso Blockchain

		
Agricultor Transformador Organismo Control Distribuidor y POV	Aplicación Web API (para sist. externos)	Registro de los datos más importantes de su actividad diaria (eventos/procesos, etc.)
Consumidores	Aplicación Web multilingüe	Consulta de origen, fechas de eventos e info adicional (p.ej. notas de cata) Registro de valoraciones

Tabla 2. Tabla relacionando actores, medios de acceso y uso del registro blockchain

En cuanto a los requisitos de los **sellos de calidad**, se han tenido en cuenta tanto las etiquetas que conllevan la atestación por terceros como las que simplemente se gestionan como autodeclaración por alguno de los actores. En el siguiente cuadro pueden verse algunos ejemplos de sellos que se considera lógico que tengas atestación por terceros, y otros que probablemente se basen en autodeclaración.

Sellos con atestación por 3os	Sellos con autodeclaración
	
DOP; IGP	World Cheese Award; Premios Alimentos de España; International Cider Challenge

Tabla 3. Ejemplos de sellos con atestación por terceros y sin ella (autodeclaración)

En cuanto a los requisitos de **codificación y etiquetado**, se avanzan unos mínimos que en realidad serán ampliados y analizados en detalle en la siguiente tarea. La principal cuestión es poder incluir la codificación interna que emplean para sus lotes las empresas participantes, ya que las empresas suelen registrar el número de lote y/o número de identificación de las agrupaciones de productos que entran en la empresa y también crean una identificación del producto final que entregan al cliente, mediante un código que corresponde al lote u otra forma de agrupación y acompaña al producto en el momento de la entrega.
El código de lote interno de cada producto y empresa suele ser una combinación de números y letras, con una longitud diferente y significado propio según cada empresa, pues está ligado a sus sistemas de gestión y producción internos. Cada código de lote está compuesto por una combinación de distintos códigos de identificación, relativos al producto, la línea de producción, la fecha de producción, la hora de producción, etc. P.ej. un lote de código 202109301030P02M02 podría indicar, de izda. a dcha., que 2021 es el año de

producción, 09 y 30 que se ha producido el 30 de septiembre, 1030 que tuvo lugar a las 10:30h., P02 se ha producido en la planta 2 y M02 sería la máquina 2.
Este código interno de lote normalmente ya viene impreso en el propio envase (botella, bolsa, etc.) o en algún etiquetado que los productores adhieren al producto. Sin embargo, el "código" o número de serie adicional otorgado por organismos de control, y también el vínculo a la información registrada en blockchain, deberán o bien añadirse al etiquetado existente o bien formar parte de uno nuevo. De ahí que sea preciso analizar su seguridad en la tarea específica T1.3.

T1.3: Seguridad física de las etiquetas

Se ha desarrollado aproximadamente un 35% del trabajo asociado a esta tarea. En concreto, se ha analizado la aplicabilidad de tecnologías bidimensionales, tipo QR, y se han empezado a analizar tecnologías inalámbricas como RFID y NFC.

Los códigos bidimensionales (2D) combinan el marcaje industrial y los lectores móviles para proporcionar información de lectura rápida. El código QR, también conocido como Quick Response, es un método de guardar información en una matriz cuadrada de puntos. Dicho código puede ser leído a través de cámaras industriales y aplicaciones incorporadas en la mayoría de smartphones del mercado. La información codificada en una etiqueta QR contiene caracteres alfanuméricos que pueden contener texto simple, direcciones web y tarjetas de presentación en formato Vcard, entre otros formatos.

Figura 7. Captura de un código QR mediante un teléfono móvil

A pesar de las ventajas que el empleo de códigos QR tiene, como su bajo coste de generación y versatilidad para representar un diverso rango de información, presentan algunos inconvenientes motivados por ejemplo por el desgaste y pérdida de color, lo que puede dificultar la lectura de los mismos. Podemos ver en la siguiente tabla las diferencias que se observan respecto a etiquetas de tipo RFID y NFC.

QR	RFID/NFC
Lectura a corta distancia	Diferentes distancias, según estándar
Lectura lenta, requiere visión directa con el código y precisa de enfoque	Lectura rápida, no le afecta la visibilidad e iluminación
Sin seguridad: la información se puede alterar	Seguridad integrada: difícil de alterar (si no se

y dañar	desea) y dañable
Solo se permite la lectura simultánea de una etiqueta	Identificación simultánea de varias etiquetas según estándar

Tabla 4. Comparativa de aspectos destacables entre tecnologías QR y RFID/NFC

En cuanto a los aspectos de seguridad se ha establecido una base para diferenciar aspectos dependientes del propio uso de las etiquetas, su soporte y las características del almacenaje y transporte del producto, y aspectos dependientes de replicación o manipulación indeseada por actores maliciosos de la cadena, competidores, etc.
Entre los riesgos que pueden sufrir los clientes debido al uso de estos códigos maliciosos, entre los analizados hasta el momento destacan los siguientes:

- Ataques de tipo **phishing**, cuando el usuario al escanear el QR es redirigido a una página web que suplanta a la de la empresa, habitualmente para solicitarle información confidencial.
- Descarga de **malware** o inyección de código malicioso, que se caracteriza por la descarga de manera forzada de software malicioso cuando el usuario visita el sitio web al que le dirige el QR.
- **Qrljacking** o secuestro de sesión, que se caracteriza por hacer uso de la ingeniería social para secuestrar la cuenta de un servicio que acepte la función “Inicio de sesión con código QR”.

T1.4: Diseño conceptual

Tras determinar los diferentes requisitos en la tarea previa T1.2, se procede con el diseño conceptual de la propia solución a llevar a cabo a lo largo de este proyecto. Dentro de ésta, se pueden distinguir diferentes módulos, estrechamente ligados con los propios paquetes de trabajo del proyecto.

Sistema de administración de la solución

En este módulo, se identifican todas las fuentes de datos seleccionadas, llevando a cabo todos los pasos correspondientes para tanto su recogida, tratamiento, pre-procesado, preparación para fases posteriores, y almacenamiento final con la estructuración adecuada.
Se trata de un módulo altamente relevante y de gran importancia para el correcto funcionamiento del sistema completo, dado que la configuración de la red y los contratos es indispensable para que los sistemas de los módulos posteriores tengan un funcionamiento adecuado.

Sistema de registro de datos

En este módulo se lleva a cabo el registro de los datos relevantes procedentes de las fuentes de datos manejadas por los actores de la cadena agroalimentaria.
Dependiendo del ámbito concreto de cada caso de uso, puede ser que varíen las fuentes y la variedad y tipología de la información que es necesario registrar. Ello dependerá de los procesos relevantes para la trazabilidad de los productos que se consideren en cada caso de uso específico.
Respecto al mecanismo de registro, tal como se estableció en la tarea T1.2 donde definimos los requisitos, además de la posibilidad de conectar sistemas de terceros vía API, el sistema de trazabilidad DOPCHAIN ofrecerá un interfaz web para la introducción manual de la información. Un ejemplo del diseño de dicho interfaz puede verse a continuación:

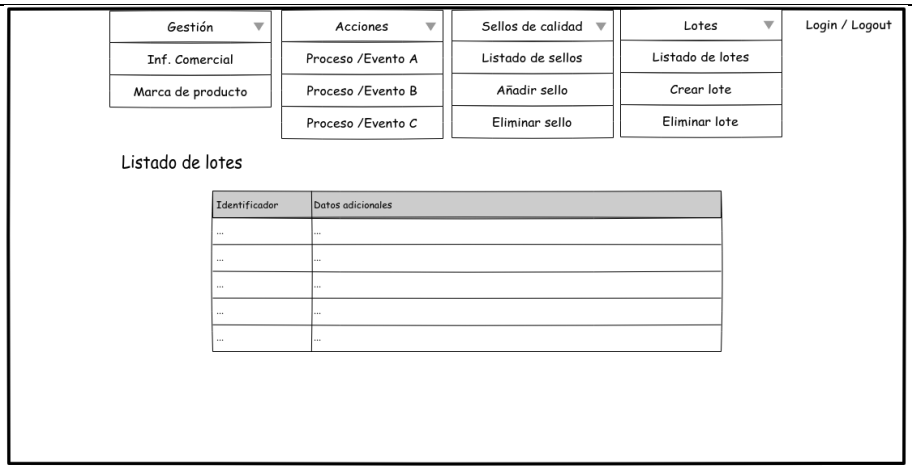

Figura 8. Diseño propuesto para la interfaz de la aplicación de registro (menú principal)

Interfaz de consulta y visualización de datos

Este módulo incluye todo lo relativo a la visualización de las diferentes componentes previas del proyecto. Esto comprende tanto la propia aplicación de consulta para consumidores finales, como resultados asociados al sistema externo de mapas y otros que puedan considerarse útiles. Dicho interfaz de visualización será interpretable para el usuario, siendo validado a través de los datos recogidos en el proyecto con diferentes tipos de representaciones gráficas. Un ejemplo del diseño de dicho interfaz, basado en una línea temporal de eventos a lo largo de la cadena, puede verse a continuación:

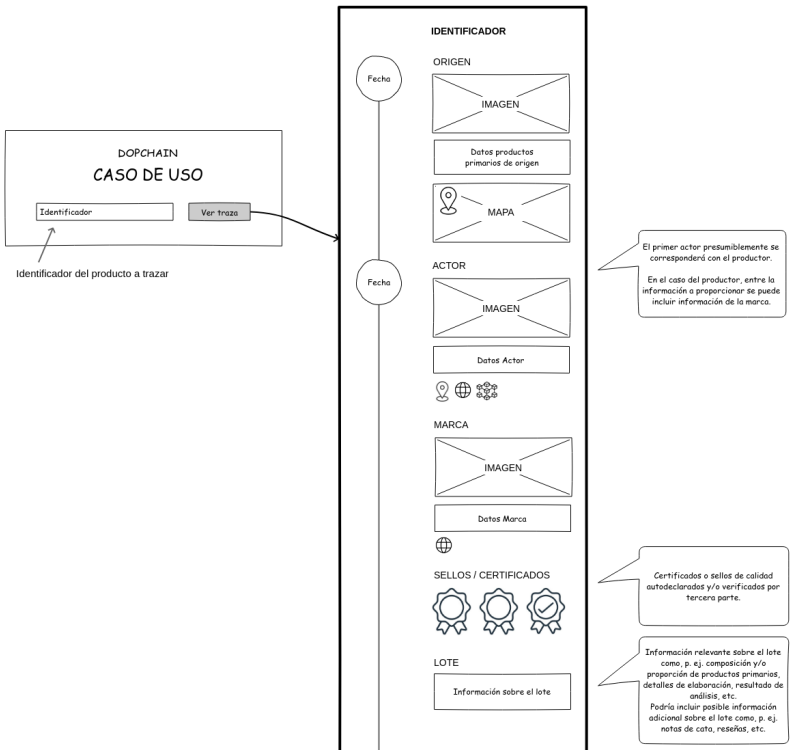

Figura 9. Diseño propuesto para la interfaz de la aplicación de consulta

A modo ilustrativo, en la siguiente figura se presenta la organización y conexión de los tres módulos anteriormente mencionados.

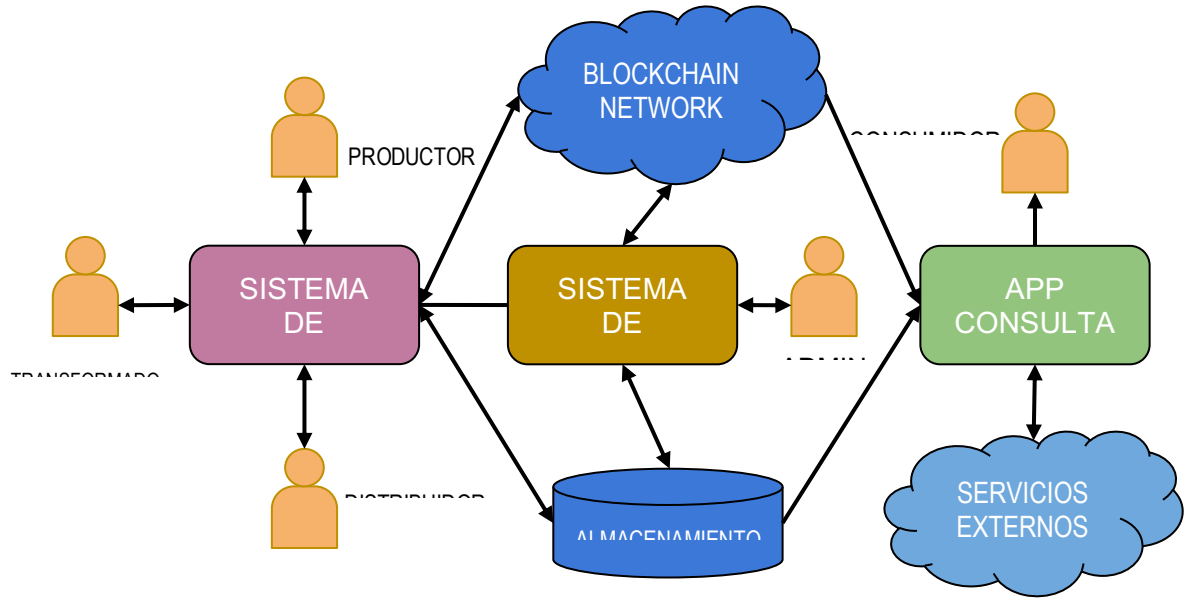

Figura 10. Diagrama de interrelación entre módulos, componentes y actores del sistema de trazabilidad

Dicha estructura propuesta, tal y como se puede apreciar, presenta las interconexiones presentes entre los diferentes módulos y que, resumidamente, son las siguientes:

- El **sistema de gestión de la solución** requerirá de toda la información procesada de las fuentes de datos seleccionadas inicialmente para su generación en el **módulo de selección y tratamiento de fuentes de datos**.
- El **sistema de registro de datos** hará uso de los contratos inteligentes desarrollados y desplegados en la red blockchain correspondiente, de forma acorde a los parámetros operacionales del sistema establecidos con el módulo anterior, es decir, el sistema de gestión de la solución.
- La **interfaz de consulta y visualización de datos** presentará mediante una aplicación web la información asociada al módulo previo, es decir, la información y datos existentes en el registro blockchain introducidos mediante el sistema de registro.

Paquete de Trabajo 2: Componentes principales del sistema Blockchain

En esta fase se llevará a cabo el grueso del desarrollo tecnológico del proyecto, implicando un total de 4 tareas dentro del paquete de trabajo, las cuales aluden al protocolo blockchain a utilizar, al tipo de datos de trazabilidad a gestionar, al sistema de acceso e identificación de los actores en el sistema y a la lógica de negocio de la cadena de suministro a implementar en el protocolo de la red blockchain.

En el período perteneciente a 2021 se han iniciado las siguientes tareas:

- T2.1: Comparativa de redes Blockchain, habiendo desarrollado aproximadamente un 85% del trabajo asociado a dicha tarea.

En la misma, se realizó una evaluación de las principales redes blockchain, con especial énfasis en las tendencias emergentes y los retos tecnológicos que implican en cuanto a su aplicación a los sistemas de trazabilidad.

En particular, se ha realizado un análisis basado en distintas generaciones de protocolos, desde la primera hasta la tercera vigente, comprendiendo 4 redes ampliamente conocidas y utilizadas: **Bitcoin** (1ª generación), **Ethereum** (2ª generación), **Hyperledger Fabric** (2ª generación) y **EOSIO/Telos** (3ª generación). En todas ellas se ha analizado tanto las características del protocolo, tales como el **algoritmo de consenso** empleado y la **velocidad de proceso** de la red (medida en transacciones por segundo), como los aspectos relativos a la comunidad y **herramientas de desarrollo**.

- Redes blockchain de 1ª generación: **Bitcoin** usa un algoritmo de consenso basado en el Hashcash Proof-of-Work (**PoW**) que, a día de hoy, es uno de los más seguros. Pero lo es a costa de un gran consumo energético y una baja capacidad de proceso en cuanto al número de transacciones (Tx) por segundo (TPS), con un máximo de cerca de 5 y una media de 3 TPS. El protocolo Bitcoin carece de la posibilidad de programar contratos inteligentes, aunque facilita una versión débil de dicho concepto al contar con cierta capacidad programación. La UTXO en Bitcoin puede ser propiedad no solo de una clave pública, sino también de un script más complicado expresado en un lenguaje simple de programación basado en pila, el Bitcoin Script. Sin embargo, el lenguaje de scripting implementado en Bitcoin tiene varias limitaciones importantes: falta de completitud Turing, indiferencia al valor, falta de estado y "ceguera" a los datos de la blockchain.
- Redes blockchain de 2ª generación:
  - **Ethereum** utiliza un algoritmo de consenso **PoW** similar al de Bitcoin, aunque con más capacidad para procesar transacciones (~20 TPS) y con una menor latencia (~13 segundos). La blockchain de Ethereum es en muchas maneras similar a la blockchain de Bitcoin, aunque tiene algunas diferencias. La principal tiene relación con la arquitectura blockchain pues, a diferencia de Bitcoin (que solo contiene una copia de la lista de la transacciones), los bloques de Ethereum contienen una copia tanto de la lista de transacciones como del estado más reciente. Por otro lado, el alto consumo energético que Ethereum comparte con Bitcoin, tendrá solución pronto, pues la red cambiará a lo largo de 2022 al algoritmo de consenso Proof-of-Stake (PoS) que se usa habitualmente en las redes de 3ª generación. A diferencia de Bitcoin, la plataforma de contratos inteligentes de Ethereum sí es Turing completa, permitiendo crear código de propósito general que puede ser utilizado para cualquier tarea.
  - **Hyperledger Fabric** emplea habitualmente el algoritmo de consenso Proof-of-Authority (**PoA**), que solo se recomienda cuando los participantes se conocen entre sí y existe un alto nivel de confianza entre ellos. Por ello esta red se suele emplear para conformar redes privadas o permisionadas. La red soporta el desarrollo de smart contracts y chaincodes, siendo éste un concepto propio de la red asociado a su carácter privado/permisionado.
- Redes blockchain de 3ª generación: **EOSIO** emplea el algoritmo de consenso Delegated Proof-of-Stake (**DPoS**), una variante de PoS, con menor consumo energético y un

compromiso aceptable entre escalabilidad y seguridad. El Proof-of-Work o prueba de participación es un enfoque alternativo al del PoW, ya que calcula el peso de un nodo como la parte proporcional de sus (cripto)monedas en propiedad, y no sus recursos computacionales. En la siguiente infografía se aprecian las ventajas del PoS sobre PoW.

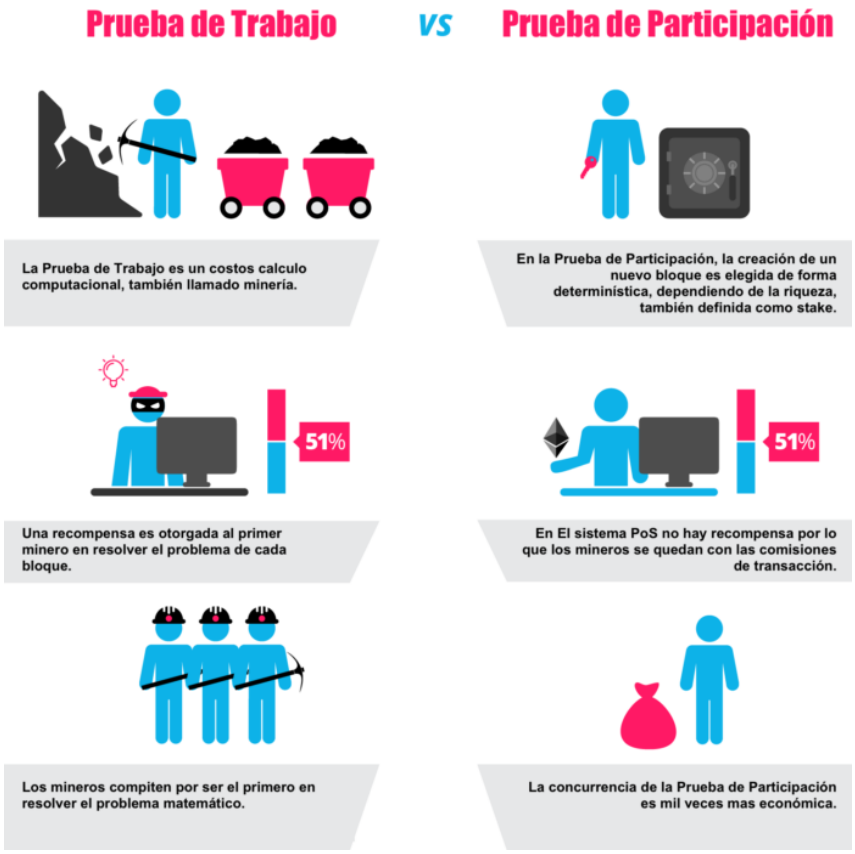

Figura 12. Diferencias entre PoW vs PoS

Telos, una de las redes blockchain que usan el software EOSIO, integra además un gobierno de la red en la propia cadena. Además es capaz de procesar hasta 10.000 TPS y registrar un bloque cada medio segundo. En cuanto a las herramientas de desarrollo, el ecosistema EOSIO ofrece un buen número de ellas y documentación de referencia para desarrolladores, que pueden crear contratos inteligentes, más avanzados incluso que los de Ethereum, para la creación de aplicaciones de cualquier propósito.

También hemos determinado el estado de cada red respecto al conocido como "trilema Blockchain", que consiste en representar la situación de la red en cuanto a las 3 características más importantes: **escalabilidad, seguridad y descentralización** efectiva.

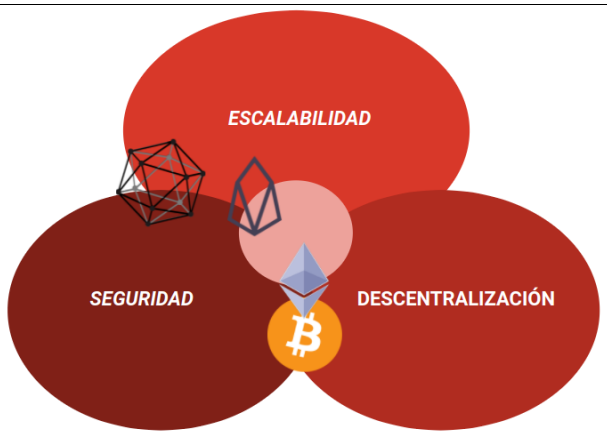

Figura 13. EOSIO vs. Hyperledger, Ethereum y Bitcoin en el "trilema Blockchain"

Al respecto podemos concluir que Bitcoin adolece de alta escalabilidad, pero por contra ofrece muy buena seguridad y descentralización. Por su parte y en su actual encarnación del algoritmo de consenso PoW, Ethereum mejora ligeramente la escalabilidad frente a Bitcoin. Consideramos que dado su enfoque a las redes privadas/permisionadas, Hyperledger ha dejado prácticamente de lado la descentralización, mientras que EOSIO tiene una escalabilidad notablemente superior a las redes precedentes, aunque lo consigue a costa de sacrificar cierta descentralización.
Finalmente, se ha iniciado la selección razonada, entre las redes analizadas, de la que formará la base de la infraestructura tecnológica del proyecto. Para ello, hemos realizado una comparativa de herramientas, como puede verse en el siguiente cuadro:

	Smart Contracts	Línea comandos	API	IDE	SDKs	Wallet (app auth)
Bitcoin	Script	bitcoind	JSON-RPC			
Ethereum	Solidity/ Vyper	solc	RPC	Remix Ganache		MetaMask / Trust Wallet
Hyperledger	Go / JS / Java	peer	gRPC	Chaincoder		Ad-Hoc
EOSIO/Telos	C++	cleos	RPC	EOS/Telos Studio	iOS Android	Anchor

El resto de aspectos a considerar y las conclusiones para tomar la decisión final se completará durante el primer mes de 2022.

- T2.2: Diseño del modelo de datos, habiendo desarrollado aproximadamente un 40% del trabajo asociado a dicha tarea.

En la misma, se ha realizado una propuesta de modelo de datos para el primer caso de uso (Vino DOP Cangas), considerando la diversidad de procesos, actores involucrados y la información que manejan.

Así hemos analizado en detalle qué **tipos y aspectos de la trazabilidad se ven involucrados**, entendiendo por trazabilidad la capacidad de seguir una unidad o lote de productos a lo largo de cada una de las fases del proceso de suministros, de modo que se pueda conocer su historia, ubicación y trayectoria a lo largo de la cadena de suministros.

- Trazabilidad ascendente: trata de conocer con detalle el origen de la materia prima, es decir:
  - La uva se ha recolectado en un lugar, es decir, en una finca.
  - La uva la ha recolectado un determinado productor.
  - La fecha de la recolección y/o de entrega a la bodega, con el lote de producto
- Trazabilidad de procesos: trata de conocer el proceso de transformación de la materia prima en la industria, es decir, de la uva en la bodega.
  - La uva la ha procesado una determinada bodega.
  - Los ingredientes y sus cantidades, es decir, variedades de uva y proporción de mezcla en el lote.
  - Los procesos a los que han sido sometidos (temperatura, tiempo, etc.).
  - El producto final, que será vino tinto o blanco embotellado.
- Trazabilidad descendente: trata de conocer el detalle logístico que se refiere a la distribución del producto final al cliente y consumidor del mismo.
  - Las botellas de vino las ha repartido un determinado distribuidor.
  - Las botellas de vino se han vendido, o servido, en un determinado punto de venta.

En cuanto a la trazabilidad de procesos, solo se considerarán los procesos de inicio y final, es decir el estrujado y el corchado o embotellado del vino, ya que el resto de procesos internos no aportan gran valor al consumidor final del producto.

Según los actores y procesos involucrados, se ha establecido un modelo de datos que podemos ver resumido en la siguiente tabla:

ACTOR	**DATOS A REGISTRAR**
Productor de uva	ID Viticultor, variedad de uva, finca origen
Bodega (productor de vino)	ID Bodega, lote, mezcla de variedades uva, proceso y fecha del mismo, marca del producto final, notas de cata
Consejo Regulador	ID Organismo Control, lote , ID bodega del lote, rango precintas
Distribuidor	ID Distribuidor, lote y fecha de expedición

Punto de Venta	ID Punto de venta, lote y fecha de venta
Consumidor	ID Consumidor, lote y fecha de consumo, valoración

El modelo de datos así definido cubre en principio todos los actores que pueden verse involucrados. Sin embargo, su aplicación concreta dependerá de factores diversos que modulan la cadena de suministro formada. Por ejemplo, si la botella de vino se consume en un bar, el registro del lote y fecha de consumo puede hacerlo el bar como punto de venta. Es por ello que durante el desarrollo del sistema se probarán mecanismos o estrategias que hagan posible estas variaciones, eligiendo la más oportuna.

- T2.3: Gestión de la identidad y acceso a recursos, habiendo desarrollado aproximadamente un 50% del trabajo asociado a dicha tarea.
  Considerando el modelo de datos propuesto en la tarea T2.2 y el tipo de actores involucrados, hemos diseñado la base para una adecuada gestión de la identidad.
  En concreto, se han evaluado diferentes alternativas de gestión de la identidad directamente compatibles con blockchain, como:
  - identidades nativas, basadas en las clave pública/privada de cada blockchain (comúnmente conocidas como wallets)
  - aplicaciones descentralizadas de gestión de identidad blockchain, basadas en smart contracts (implementaciones ad-hoc de esquemas de identidad, generalmente propietarios, y que están ligados directamente a una red blockchain concreta)
  - identificadores descentralizados basados en estándares internacionales (comúnmente conocidos como DID), y que consisten en unos protocolos que permiten implementar identificadores únicos sin necesidad de una entidad central de gestión y técnicamente basados en una abanico de plataformas tecnológicas, entre otras blockchain.

  En una arquitectura abierta y flexible como la que aspira a construir DOPChain, hemos identificados los DID de W3C (**https://www.w3.org/TR/did-core/**) como la opción más prometedora, y hemos comenzado los trabajos para integrar este tipo de identificadores de una forma que permita a los usuarios abstraerse de las complejidades de la gestión de claves en blockchain, que suele ser la principal barrera de acceso para el usuario medio.

  En este caso, la integración se ha comenzado con una primera prueba de concepto de adaptación en la red blockchain EOSIO. Es importante destacar que el enfoque a seguir consistirá en una implementación con middleware open source, sin dependencias de productos comerciales propietarios, ya que esto podría suponer un escollo en posibles evoluciones futuras.
  Así, hemos partido del análisis del trabajo que Gimly está realizado para la aplicación de DIDs en la plataforma blockchain EOSIO, con su propuesta de implementación de DIDs (https://github.com/Gimly-Blockchain/eosio-did-spec), para adaptarlo a las necesidades del proyecto DOPCHAIN. En ejemplo puede verse en este código:

```
{
    "@context": "https://www.w3.org/ns/did/v1",
    "id": "did:example:123",
    "verificationMethod": [{
            "id": "did:example:123#owner",
            "type": "Ed25519VerificationKey2018",
            "controller": "did:example:123",
            "publicKeyBase58": "7NFuBesBKK5XHHLtzFxm7S57Eq11gUtndrsvq3Mt3XZNMTHfqc"
        },
        {
            "id": "did:example:123#active",
            "type": "Ed25519VerificationKey2018",
            "controller": "did:example:123#owner",
            "publicKeyBase58": "7idX86zQ6M3mrzkGQ9MGHf4btSECmcTj4i8Le59ga7CpSpZYy5"
        }
    ]
}
```

El resultado de dichas tareas será entregado en 2022, período en que se iniciará igualmente la tarea T2.4: Reglas de negocio (contratos inteligentes) de este paquete de trabajo.

Justificación 2022

A continuación, se describen las tareas realizadas en este hito de trabajo y los resultados conseguidos.

Paquete de Trabajo 1: Escenario, casos uso y requisitos

El objetivo de este paquete es doble: por un lado la identificación y análisis de sistemas de trazabilidad alimentaria, estándares y casos de uso (basados o no en tecnologías blockchain), para conocer la tipología de actores, sus relaciones más habituales, y mecanismos tecnológicos empleados para orquestar dicha relación, y por otro lado tenemos el objetivo de seleccionar dos casos de uso que servirán de modelo y de prueba para la solución de trazabilidad basada en blockchain a desarrollar en el proyecto DOPCHAIN.

Este paquete se organiza en torno a cuatro tareas, tres de ellas (T1.1, T1.2, T1.4) finalizadas en la anualidad 2021, y la restante (T1.3) iniciada y finalizada en la anualidad 2022:

- T1.3: Seguridad física de las etiquetas [Finalizada]

A continuación se describen las acciones desarrolladas en la tarea y los principales resultados alcanzados.

T1.3: Seguridad física de las etiquetas

Se ha desarrollado el 100% del trabajo asociado a esta tarea. En concreto, se ha analizado la aplicabilidad de tecnologías bidimensionales, tipo QR, y se han analizado tecnologías inalámbricas como RFID y NFC, con una comparativa entre ellas y también considerado aspectos de seguridad de las mismas.

Respecto a los códigos QR analizamos las diferencias y posibilidades de los QR estáticos vs. dinámicos. Estos últimos permiten cambiar a posteriori (tras su creación) el destino o el contenido del código QR, evitando volver a imprimirlos y además permitiendo un seguimiento de los escaneos del código por los

usuarios. Esta última opción puede ser interesante para algunos de los actores de la cadena, que podrían estar interesados en conocer por ejemplo las horas del día con más consultas (escaneos), la ubicación o incluso el tipo de dispositivo, de cara a realizar actividades específicas de promoción.

También analizamos las posibilidades de los sistemas de marcaje, como los más habituales basados en impresión con tinta y térmico, pero también otros más innovadores como el marcaje por láser, cuya aplicabilidad al caso de uso del vino, al marcar QR en corchos se consideró a priori una opción a tener en cuenta.

Figura 15. Ejemplos de tapones de corcho marcados con un código QR

Los requisitos mínimos de **codificación y etiquetado** se ampliaron y analizaron en detalle en esta tarea. La codificación interna que usan las empresas con sus lotes (una combinación de números y letras, con una longitud diferente y significado propio según cada empresa) normalmente viene impresa en el propio envase (botella, bolsa, etc.) o en algún etiquetado adherido al producto.

Sin embargo, el "código" o número de serie adicional otorgado por organismos de control, y también el vínculo a la información registrada en blockchain, debe o bien añadirse al etiquetado existente o bien formar parte de uno nuevo. Es la habitualmente denominada precinta, o contraetiqueta en los casos del Vino de Cangas y el Queso Manchego.

Figura 16. Ejemplos de contraetiquetas de las D.O.P. Cangas (izda.) y Queso Manchego (dcha.)

Tras analizar la cadena de producción de ambos casos de uso y conocer mejor la tipología del lote del productor en cada uno de ellos, concluimos que el etiquetado en DOPCHain para el caso del vino no era factible manejarlo a nivel de botella para el productor. Es decir, imprimir un QR por cada botella no era viable (ni económicamente ni técnicamente sin importantes cambios) para la bodega. Y en el caso del queso manchego sí podía ser más factible económicamente (por el mayor valor de cada unidad del producto), pero tampoco tanto técnicamente cuando entraba en juego el formato de cuñas.

En ambos casos la inclusión de un QR en el etiquetado serviría para dar acceso a la aplicación de consulta de la traza, pero después el usuario necesitará introducir el código de la contraetiqueta del producto (botella de vino o pieza de queso). Esta introducción manual "rompe" en cierto sentido el flujo de usuario

iniciado con la acción de capturar un código QR, además de ser propenso a errores en la introducción mediante el teclado.

Por ello estudiamos también las posibilidades de utilizar e integrar en las aplicaciones de consulta de DOPChain algún sistema de reconocimiento óptico de caracteres, OCR por sus siglas en inglés, que mejore la experiencia de usuario y le evite fijarse en el código y teclearlo luego. Así probamos algunas herramientas y librerías disponibles e hicimos pruebas con las etiquetas de las D.O.P. Cangas y Queso Manchego, mandándonos incluso el Consejo Regulador de esta última una serie de ellas en sus diferentes formatos (quesos y cuñas/porciones).

Las pruebas han sido exitosas y concluimos que el servicio Google Lens, y su Cloud Vision API, podría ser usado en DOPChain, por su precisión, posibilidades de configuración y coste asequible por número de lecturas (entre 0,60 y 1,5 dólares USA cada paquete de 1000 lecturas).

Figura 17. Google Lens y su OCR para convertir imágenes en texto

Paquete de Trabajo 2: Componentes principales del sistema Blockchain

En esta fase se lleva a cabo el grueso del desarrollo tecnológico del proyecto, implicando un total de 4 tareas dentro del paquete de trabajo, las cuales aluden al protocolo blockchain a utilizar, al tipo de datos de trazabilidad a gestionar, al sistema de acceso e identificación de los actores en el sistema y a la lógica de negocio de la cadena de suministro a implementar en el protocolo de la red blockchain.

En el período correspondiente a 2022 se han finalizado todas las tareas del paquete y a continuación se describen las acciones desarrolladas en las mismas y los principales resultados alcanzados.

T2.1: Comparativa de redes Blockchain

Partiendo de nuestra evaluación realizada en 2021 sobre las principales redes blockchain, en particular considerando distintas generaciones de protocolos, como: **Bitcoin** (1ª generación), **Ethereum** (2ª generación), **Hyperledger Fabric** (2ª generación) y **EOSIO/Telos** (3ª generación), cuyo detalle amplio del análisis se puede consultar en el informe correspondiente, procedimos a la selección razonada de las redes que formarán la base de la infraestructura tecnológica del proyecto.

Para ello, también nos basamos en una comparativa de herramientas incluida en un cuadro del citado informe, y así durante el primer mes de 2022 concluimos que íbamos a trabajar sobre dos redes: Telos (EOSIO) y Ethereum.

Aunque inicialmente la única red de 3ª generación y más prometedora para las necesidades del proyecto parecía Telos, valoramos muy positivamente el avance de la red Ethereum para pasar de ser una red

basada en algoritmo de consenso PoW al algoritmo PoS, convirtiéndose así en una red moderna de 3ª generación y solventando algunas de sus desventajas como la escalabilidad y velocidad de Tx.

Además en Ethereum ha ganado fuerza y adopción la denominada "capa 2", que es cualquier cadena de bloques independiente que amplía Ethereum y hereda sus garantías de seguridad. Cuando la demanda para utilizar Ethereum es alta, la red se congestiona, lo que genera un aumento en las comisiones de transacción y hace que muchas transacciones sean inviables por su alto coste para los usuarios. Y aquí es donde entran las soluciones de capa 2. El mismo Vitalik Buterin, cofundador de Ethereum, incluyó este paradigma en su presentación de apertura de la conferencia DEVCON Bogotá 2022 en la que estuvimos (véase el apartado 7. INFORMACIÓN ADICIONAL en este documento para más información sobre nuestra asistencia).

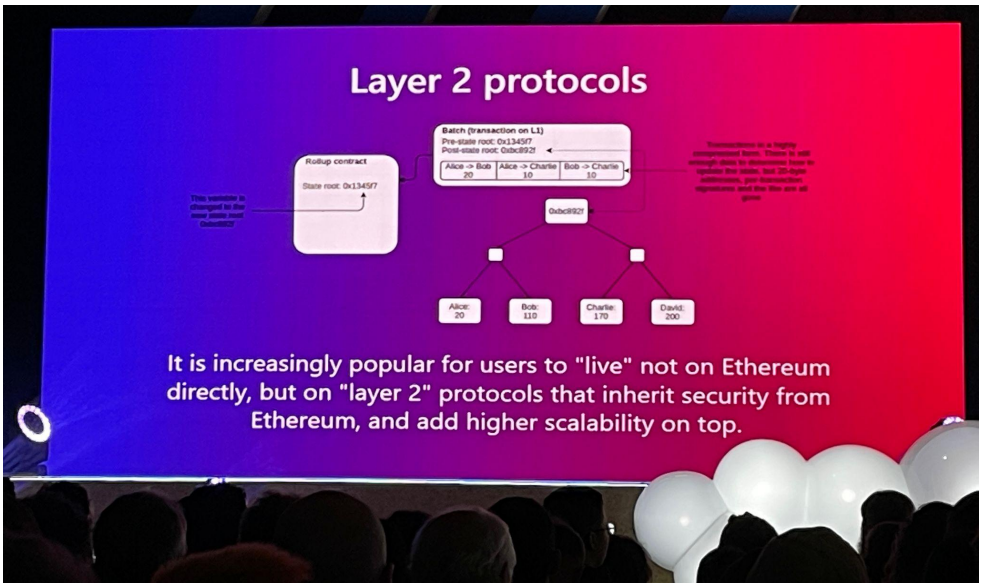

Figura 19. Diapositiva mencionando la Capa 2 de Ethereum en la DEVCON Bogotá 2023

Además, el reto de adoptar para DOPChain dos infraestructuras de red blockchain diferentes nos permite basar nuestras decisiones de diseño, en cuanto a la arquitectura de contratos inteligentes, de una forma más simple y "agnóstica" a la tecnología blockchain de base. Lo cual supone una ventaja a la hora de evolucionar DOPChain a otro tipo de redes o los cambios futuros.

T2.2: Diseño del modelo de datos

Siguiendo la propuesta de modelo de datos realizada para el primer caso de uso (Vino DOP Cangas), hemos hecho lo mismo para el segundo caso (Queso Manchego), considerando igualmente la diversidad de procesos, actores involucrados y la información que manejan.

Así hemos analizado en detalle qué **tipos y aspectos de la trazabilidad se ven involucrados**, entendiendo por trazabilidad la capacidad de seguir una unidad o lote de productos a lo largo de cada una de las fases del proceso de suministros, de modo que se pueda conocer su historia, ubicación y trayectoria a lo largo de la cadena de suministros.

- Trazabilidad ascendente: trata de conocer con detalle el origen de la materia prima, es decir:
  - La leche se ha ordeñado en un lugar, es decir, en una granja.

- La leche la ha recolectado un determinado productor.
- La fecha de ordeño y/o de entrega a la quesería, con el lote de producto

- Trazabilidad de procesos: trata de conocer el proceso de transformación de la materia prima en la industria, es decir, de la leche en la quesería.
  - La leche la ha procesado una determinada quesería.
  - La medición de las propiedades de la leche, como grasa, proteína y lactosa.
  - Los procesos a los que han sido sometidos (temperatura, tiempo, etc.).
  - El producto final, que será queso entero y en porciones (cuñas).
- Trazabilidad descendente: trata de conocer el detalle logístico que se refiere a la distribución del producto final al cliente y consumidor del mismo.
  - Los quesos y cuñas las ha repartido un determinado distribuidor.
  - Los quesos y cuñas se han vendido, o servido, en un determinado punto de venta.

En cuanto a la trazabilidad de procesos, se han considerado los de ordeño de leche, análisis de leche, fabricación del queso, maduración y el empaquetado y etiquetado del queso y las cuñas.

Según los actores y procesos involucrados, se ha establecido un modelo de datos que podemos ver resumido en la siguiente tabla:

ACTOR	**DATOS A REGISTRAR**
Productor de leche	ID productor, variedad de animal*/leche, granja origen
Quesería (productor de queso)	ID quesería, lote, mezcla de variedades leche*, proceso y fecha del mismo, marca del producto final, notas de cata
Consejo Regulador	ID Organismo Control, lote , ID granja del lote, rango precintas
Distribuidor	ID Distribuidor, lote y fecha de expedición
Punto de Venta	ID Punto de venta, lote y fecha de venta
Consumidor	ID Consumidor, lote y fecha de consumo, valoración

* aunque el queso manchego es aquel elaborado solo con leche de oveja de la raza manchega, a nivel de estructura de datos conviene disponer de este campo para poder adaptarlo a otro tipo de quesos que pueden llevar mezcla de leches procedentes de diferentes animales (oveja, vaca, cabra).

El modelo de datos así definido cubre en principio todos los actores que pueden verse involucrados.

T2.3: Gestión de la identidad y acceso a recursos

Se ha realizado el diseño base para una adecuada gestión de la identidad teniendo en cuenta el modelo de datos definido en la tarea T2.2 y el tipo de actores involucrados.

Tras evaluar diferentes alternativas de gestión de la identidad directamente compatibles con blockchain, como identidades nativas, aplicaciones descentralizadas de gestión de identidad blockchain, y después identificadores descentralizados basados en estándares internacionales (comúnmente conocidos como DID), habíamos optado por comenzar con una primera prueba de concepto de adaptación en la red blockchain EOSIO, partiendo del trabajo previo de Gimly para la aplicación de DIDs en la plataforma blockchain EOSIO.

Sin embargo, pronto vimos que el empleo DIDs para identificar personas u organizaciones (entidades) no tenía visos de aportar mucho al proyecto si no iba acompañado de otro elemento como son las Credenciales Verificables, o VC por sus siglas en inglés.

Y usar la tecnología blockchain para la gestión de la identidad con DID y VC, implica que los actores que entran en juego tienen alguno (o varios) de estos tres roles: propietarios, emisores y verificadores de la identidad). Pero todos ellos deben gestionar su identidad, credenciales y acciones relacionadas habitualmente mediante un monedero de identidad digital (identity wallet), un software que permite almacenar las credenciales verificables y documentos digitales para compartirlos con otras personas/entidades a voluntad.

Algo que parece bueno, por la seguridad y el entorno digital que conlleva (interoperabilidad), no evita que el manejo de estas wallets pueda suponer una barrera para “no iniciados”, ya que deberán instalar un software en su móvil u ordenador y completar un proceso de registro. Con lo que no hay mucho avance en este sentido respecto a otros métodos de gestión de la identidad existentes y más probados.

Por ello, y con el nuevo conocimiento adquirido, dejamos por el momento la opción del empleo de DIDs y VCs para el proyecto DOPChain y nos enfocamos en otras soluciones que nos aporten la robustez y confianza que necesitamos.

Así planteamos un **módulo de control de usuarios** que identifique de forma unívoca a los usuarios de la aplicación (de registro y consulta de datos en blockchain). Mediante **passkeys** y **contraseñas de doble factor** nos aseguramos la autenticación de los usuarios, así como su asignación a un determinado rol acorde con el modelo de datos definido, como productor, transformador, certificador, distribuidor y punto de venta.

Para el **sistema de gestión de claves**, optamos por integrar un módulo que es el encargado de almacenar las claves privadas de cada usuario, necesarias para la firma de transacciones en la red Blockchain oportuna. Valoramos diferentes sistemas de custodia, tanto software como hardware e híbridos, eligiendo finalmente la aproximación software basada en la solución Vault (https://www.vaultproject.io/) de Hashicorp. Se trata de un middleware open source con soporte para distintos mecanismos de autenticación y de almacenamiento físico.

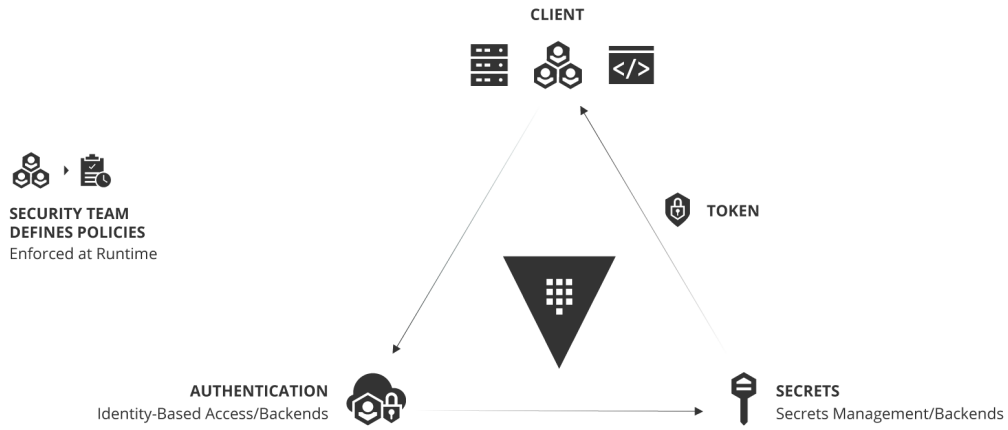

Figura 20. Diagrama de alto nivel del flujo de identificación en Vault

Adaptamos el esquema genérico y posibilidades de Vault ejemplificado en el esquema anterior a las necesidades del proyecto DOPChain, con nuestra API implementando la lógica necesaria para gestionar las claves privadas de forma transparente, obteniéndose del keystore del Vault.

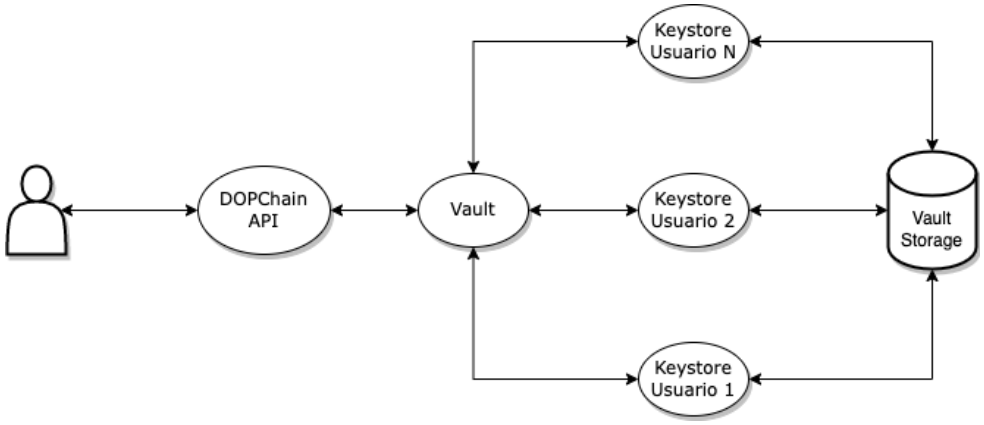

Figura 21. Diagrama de alto nivel de la aplicación de Vault en DOPChain

Las primeras pruebas manuales ejecutadas apuntan a la solución más factible y comprobaremos su eficacia en las pruebas del sistema cuando todas las piezas encajen (contratos, API, apps, etc.), para ajustar y hacer luego las adaptaciones más detalladas que se necesiten.

T2.4: Reglas de negocio (contratos inteligentes)

Respecto a los contratos inteligentes (smart contracts o SC abreviadamente), comenzamos definiendo el objetivo u objetivos de los mismos, que es gestionar la información que será almacenada en el registro blockchain según la lógica deseada e implementada mediante el código de programación correspondiente. En este sentido, establecimos que la información a guardar en blockchain será la mínima necesaria para garantizar la traza del producto, mientras que el resto de información "accesoria", incluyendo cualquier archivo a mostrar en una consulta de la traza, se guardará en un almacenamiento secundario, no blockchain pero distribuido.

Partiendo de lo anterior, pasamos a definir y codificar las principales funcionalidades de los contratos inteligentes junto con las del almacenamiento secundario, pues ambos van a estar íntimamente ligados desde el punto de vista funcional en las aplicaciones de registro y consulta de la traza.

Así, nos hemos centrado en desarrollar una implementación de SC para dos alternativas de entre las redes blockchain exploradas (anteriormente en la tarea T2.1): TELOS, una red basada en EOS.IO y Ethereum.

Para abordar el desarrollo para la red TELOS optamos por emplear dos herramientas ampliamente usadas por la comunidad como son el entorno de desarrollo integrado (IDE) EOS Studio, y el explorador de bloques EOS Authority Explorer. Y como herramienta de desarrollo para la red Ethereum optamos por emplear el entorno Remix IDE. Dichas herramientas se instalaron y configuraron en ordenadores de sobremesa con sistemas operativos Linux (Ubuntu) junto con software basado en tecnología de contenedores (Docker) de forma que facilitasen el despliegue y la replicabilidad de los mismos.

A la hora de abordar el diseño de la arquitectura de contratos específica para cada red blockchain, así como la funcionalidad de dichos contratos, establecimos la premisa de que fuese lo más simple e interoperable posible, buscando "aligerar" la carga de almacenamiento en blockchain y la interoperabilidad con soluciones en otras redes/protocolos para que, por decirlo de alguna manera, "el protocolo de blockchain fuese intercambiable". Sabemos que algo así no es posible de forma directa, pero un adecuado diseño de los SCs puede facilitar esa "extensibilidad" con un esfuerzo abordable.

Abordamos el esquema de permisos de los SC en tres niveles, correspondientes a la cuenta autorizada al despliegue del contrato inteligente, a las cuentas autorizadas a utilizar las funcionalidades del sistema de trazabilidad, y finalmente el tercer nivel correspondiente al "dueño" de la operación trazable. Con estos niveles se cubre la variedad de actores, roles y funcionalidades permitidas en todo el espectro de operaciones.

Y acorde al modelo de datos establecido definimos la estructura de las operaciones trazables, que son la base de estos contratos inteligentes y representan cualquier paso que un actor de la cadena realiza sobre cada producto. También definimos la estructura para los sellos de calidad con sus campos para almacenamiento en blockchain y la información a persistir en el almacenamiento secundario (logos, documentos externos, etc.).

Finalmente se codificaron y probaron (tests) los contratos inteligentes mediante las herramientas de desarrollo anteriormente mencionadas, habiéndose desplegado en redes de desarrollo locales (no públicas) para tal finalidad (desarrollo y pruebas). El código fuente de los contratos para la red TELOS se compone de dos archivos denominados dopcontract.hpp y dopcontract.cpp, mientras que el contrato para la red Ethereum se denomina dopcontract.sol

En el caso de la red Ethereum contemplamos una estrategia o mecanismo para permitir la actualización de los contratos inteligentes, algo fundamental que es más sencillo en las redes TELOS, pero no es trivial en Ethereum. Para ello empleamos la estrategia de Proxy Transparente, consistente en un SC "extra" (proxy) que actúa de intermediario entre el SC de la aplicación de DOPChain y el usuario.

Desarrollados los SC en sus variantes para las redes TELOS y Ethereum, analizamos las diferencias e implicaciones de los mismos, en función de costes de red y otros aspectos, para obtener unas conclusiones que nos ayudan a optimizar en un futuro los mismos y su encaje con el almacenamiento secundario y el planteamiento general de la arquitectura completa de DOPChain. Así vimos que era necesario conocer en más detalle las soluciones para Ethereum denominadas Redes de Capa 2 (Layer 2), contemplando las características y diferencias tanto de Redes L2 de tipo Optimistic rollup como Redes L2 de tipo ZK rollup.

El estado de estas tecnologías es algo que pudimos comprobar mediante la asistencia a diferentes charlas y talleres técnicos en la conferencia de desarrolladores DEVCON VI Bogotá 2023, junto con el Taller SWARM relativo a una solución específica de almacenamiento distribuido.

En cuanto a dicho sistema de almacenamiento secundario, muy ligado a los propios contratos inteligentes, analizamos la solución denominada IPFS (siglas de Inter Planetary File System) y planteamos una arquitectura adecuada a la información a tratar en DOPCHAIN.

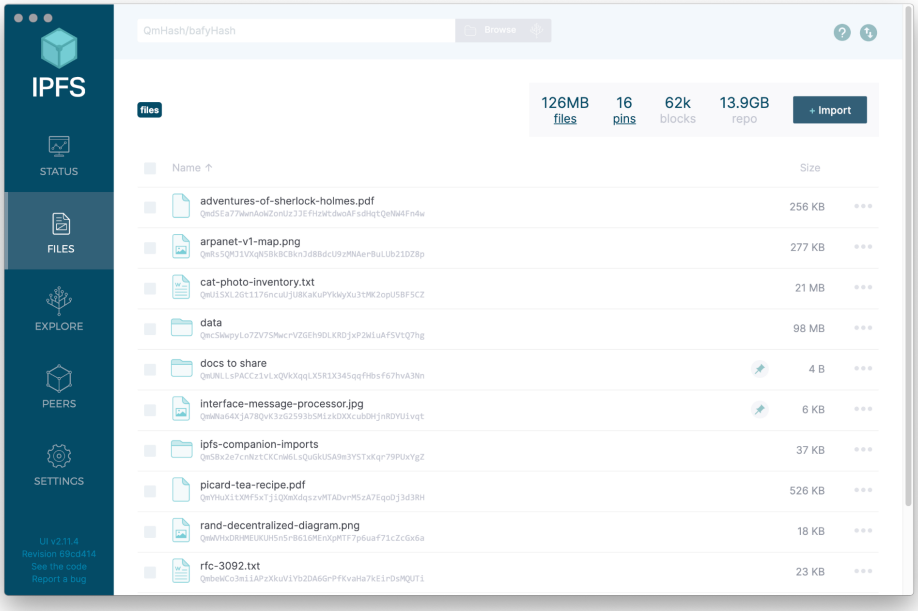

Figura 22. Ejemplo de la pantalla de ficheros de la aplicación cliente oficial de IPFS

Igualmente hicimos con la solución denominada SWARM, aunque en este caso ésta sólo va ligada a redes Ethereum.

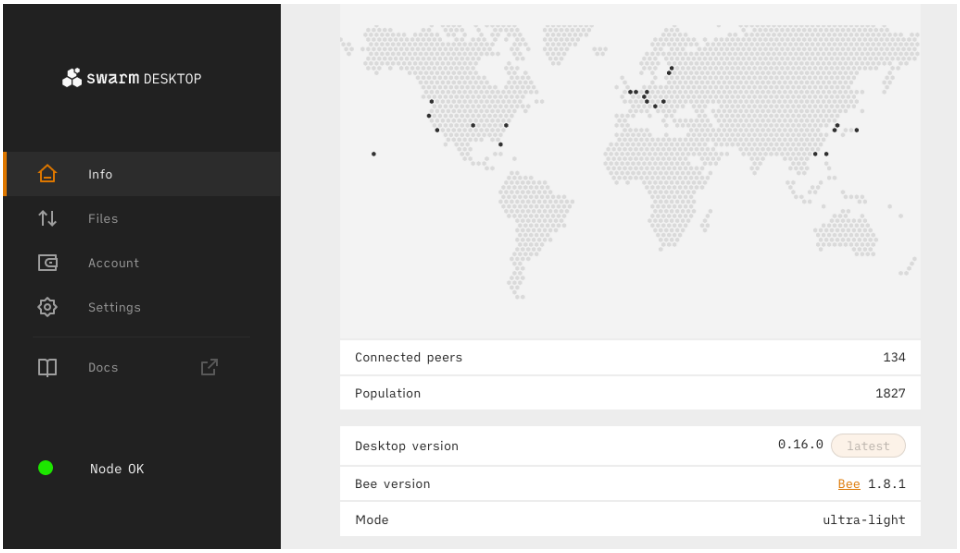

Figura 23. Captura de ejemplo de información de la red Swarm en Swarm Desktop.

Estas dos soluciones fueron las consideradas más prometedoras y adecuadas para este proyecto, habiendo recorrido previamente otras numerosas soluciones disponibles como Hypercore, Filecoin, Arweave, Storj.io, Web3.storage, Lighthouse y NFT.Storage.

Paquete de Trabajo 3: Integración de diferentes fuentes de datos en el sistema Blockchain

En esta fase se lleva a cabo el planteamiento del sistema de integración que permite a las aplicaciones de terceros interactuar con el sistema de trazabilidad basado en blockchain diseñado en DOPChain.

Este paquete se organiza en torno a tres tareas, una de ellas (T3.1) iniciada y finalizada en su totalidad en la anualidad 2022 y otra (T3.2) que ha sido iniciada en esta anualidad para finalizar en 2023.

A continuación se describen las acciones desarrolladas en cada una de dichas tareas y los principales resultados alcanzados en cada una de ellas.

T3.1: Definición de formato de intercambio

Se ha realizado un análisis de los posibles modelos de trazabilidad aplicables a los productos con denominación de origen o identificación geográfica protegida, con el fin de seleccionar el que puede dar cabida a un más amplio conjunto de sectores y productos de empresas agroalimentarias, aparte de los casos de uso inicialmente planteados (vino y queso).

Así se han analizado y comparado lo siguiente posibles modelos aplicables:

1. Modelo **lineal,** donde la unidad trazable es constante y sobre la que se realizan diversos procesos secuencialmente en una línea temporal.
2. Modelo **desagregado**, donde el objeto o unidad trazable sufre una desagregación que se pretende reflejar en la cadena.
3. Modelo de **árbol inverso**, donde la cadena de trazabilidad refleja la composición, desde diferentes orígenes, del objeto o unidad a trazar.
4. Modelo de **grafo**, siendo un modelo mixto que da cabida tanto a un proceso de trazabilidad lineal (1) como a un proceso de composición (3) o de desagregación (2).

De dicho análisis y comparación, teniendo en cuenta la tipología de productos, requisitos y objetivos del proyecto, **se concluyó que el modelo de grafo es el más adecuado** para DOPChain.

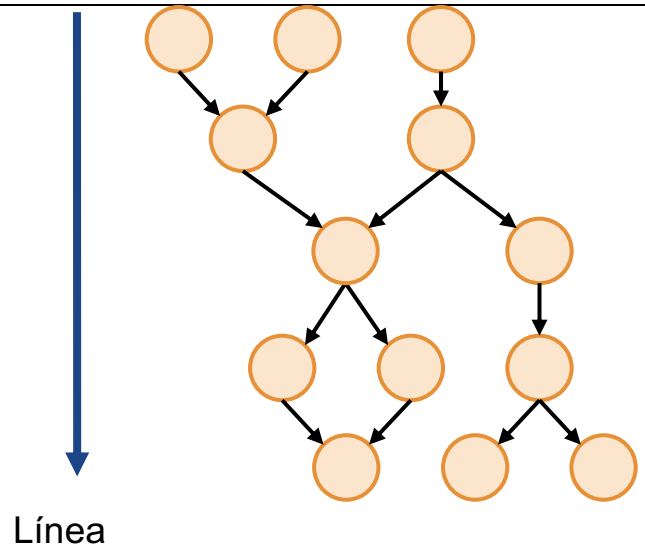

Figura 25. Esquema del modelo de grafo adoptado para DOPChain

La estructura de datos que representaría la cadena de suministro corresponde a un grafo (acíclico dirigido o DAG, de sus siglas en inglés) donde las aristas entre los nodos o vértices tienen una determinada dirección, de modo que al seguir estas direcciones nunca se forma un bucle cerrado.

Así se diseñó un modelo de datos para los contratos inteligentes adecuado para acomodar el modelo DAG seleccionado. En este modelo de datos, determinamos como elemento principal el concepto de **operación trazable**, que se corresponde con un nodo del grafo y representa cualquier paso (proceso, actividad, etc.) que un actor (productor, transformador, distribuidor, etc.) realiza en la cadena de elaboración de un producto. También consideramos un tipo especial de operación trazable calificada como "final", para representar el último paso de la cadena de trazabilidad.

Por otro lado, consideramos otras entidades del modelo de datos que no formando parte de la estructura de grafo, los actores involucrados en la cadena van a necesitar gestionarlas, como es el caso de los posibles **tipos de operaciones trazables**, que pueden formar parte de la cadena de un producto, y de los **sellos de calidad** diferenciada otorgados al producto trazado por las entidades emisoras responsables de su gestión.

Para todas estas entidades definidas en el modelo de datos se ha adoptado una estrategia complementaria de disponer una serie de campos fundamentales, como identificadores, nombres, fechas, y algún otro campo específico de la entidad correspondiente, los cuales están destinados a persistir en el registro de una Blockchain la información mínima imprescindible para observar una trazabilidad completa del producto. Mientras que además se incluye para cada entidad un campo de "información ampliada" destinado a persistir en el registro Blockchain un identificador, hash o apuntador a información

suplementaria (opcional) disponible en un formato JSON, PDF y que no precisa almacenamiento on-chain, pudiendo persistir en un almacenamiento distribuido como IPFS.

T3.2: Diseño e implementación de la API

Se ha desarrollado aproximadamente un 60% del trabajo asociado a esta tarea. En concreto, se ha efectuado la selección de las tecnologías consideradas más apropiadas, y comenzado con la identificación de los endpoints de la API HTML del servidor.

Hemos efectuado una búsqueda de lenguajes de programación y frameworks web disponibles que a priori podríamos considerar viables para la implementación de la API. Tras esta identificación inicial hemos valorado diversos aspectos de los mismos, entre ellos su seguridad y capacidad de interacción con el sistema Blockchain escogido, para finalmente realizar la selección más adecuada para el proyecto.

Así hemos optado por un lenguaje de programación moderno como **Golang** (o simplemente Go), eficiente y seguro que ofrece una gran cantidad de herramientas y recursos para el desarrollo de aplicaciones. Por otro lado, hemos elegido un framework web rápido y ligero como **Fiber**, desarrollado en Go y enfocado a la eficiencia.

Respecto a los **endpoints**, que estarán disponibles vía protocolo HTTP para las aplicaciones de registro y consulta de datos, distinguimos entre aquellos dedicados a responder a las peticiones de información disponible en el registro compartido en Blockchain, y los endpoints dedicados a enviar la información relativa a las actuaciones o procesos a trazar, y por ello a almacenar en el registro Blockchain.

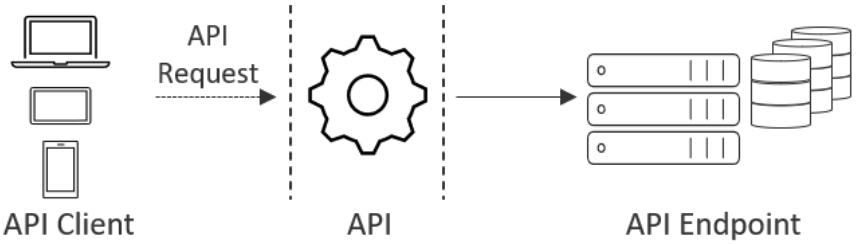

Figura 26. Esquema de alto nivel de los elementos que intervienen en la conexión a la API

Hemos comenzado por definir los endpoints de consulta (de tipo *get*) necesarios para obtener desde el tipo de operación por el que se realizará la búsqueda, hasta la información de un usuario según se recoge en una lista autorizada de los mismos (*whitelist*).

En concreto los endpoints hasta ahora definidos son: *get-operation-name, get-trace-operation, get-final-trace-operation, get-final-trace-operation-by-external-id, get-trace-by-external-id, get-stamp* y *get-whitelist-user*.

Paquete de Trabajo 4: Plataformas de inserción y consulta de datos

En esta fase se lleva a cabo el planteamiento tecnológico, el diseño y el desarrollo de una aplicación adecuada para la inserción de datos en el sistema de trazabilidad basado en blockchain de DOPChain, así como para la consulta de la traza de los productos registrados.

Este paquete se organiza en torno a dos tareas, de las cuales una de ellas (T4.1) ha sido iniciada en esta anualidad para finalizar en 2023, mientras que la otra (T4.2) comenzará con la siguiente anualidad. A continuación se describen las acciones desarrolladas en cada una de dichas tareas y los principales resultados alcanzados en cada una de ellas.

T4.1: Diseño y desarrollo de aplicación inserción

Se ha desarrollado aproximadamente un 65% del trabajo asociado a esta tarea. En concreto, se ha realizado una exploración de las tecnologías existentes que pueden adaptarse a trabajar en conjunto con las plataformas blockchain seleccionadas (TELOS y Ethereum), con los contratos inteligentes creados y la API diseñada. Finalmente valoramos como mejores opciones dos frameworks como son Angular y React.

Angular es un framework front-end para construir aplicaciones web. Es básicamente un conjunto de componentes y una forma muy dirigida de estructurar una aplicación. Tiene un montón de funcionalidades ya listas para usar, como enrutamiento, módulos, etc. pero implica limitarse a la estructura que te ofrecen y usar sus características. Para poder añadir funcionalidades personalizadas, entonces habría que reescribir alguno de sus componentes.

React es una librería de vistas que sigue un enfoque de aplicación de una sola página. La capa de vista de una aplicación web es el foco de React. React se suele utilizar con otras bibliotecas como GraphQL y Redux para construir aplicaciones de una sola página. React es muy modular y se centra en la “componibilidad”. Para añadir alguna funcionalidad personalizada no hay que reescribir el código existente. Se codifica como una pieza separada de código y se compone con los componentes ya existentes. Esta flexibilidad nos ha hecho decantarnos inicialmente por emplear React para el desarrollo de las aplicaciones de registro y consulta en DOPChain.

Asimismo, hemos iniciado la definición completa de los requisitos funcionales para la diversidad de actores involucrados en la cadena que necesitan consultar y registrar datos, según el modelo de datos diseñado y adaptándonos a una múltiple tipología de productos, si bien inicialmente nos hemos centrado en cubrir las necesidades de los casos de uso D.O.P Cangas (vino) y Queso Manchego).

Tras completar los requisitos funcionales, comenzaremos la codificación de los mismos en el framework elegido, algo que se completará ya en 2023.

Justificación 2023

A continuación, se describen las tareas realizadas en este hito de trabajo y los resultados conseguidos.

Paquete de Trabajo 3: Integración de diferentes fuentes de datos en el sistema Blockchain

En esta fase se lleva a cabo el planteamiento del sistema de integración que permite a las aplicaciones de terceros interactuar con el sistema de trazabilidad basado en blockchain diseñado en DOPChain.

Este paquete se organiza en torno a tres tareas, una de ellas (T3.1) iniciada y finalizada en su totalidad en la anualidad 2022, otra (T3.2) iniciada en 2022 y finalizada en 2023 y la tercera (T3.3) también completada en 2023.

A continuación se describen las acciones desarrolladas en cada una de dichas tareas y los principales resultados alcanzados en cada una de ellas.

T3.2: Diseño e implementación de la API

Se ha desarrollado el 100% del trabajo asociado a esta tarea. En concreto, se ha efectuado la selección de las tecnologías consideradas más apropiadas y la identificación de los endpoints de la API HTML del servidor.

Si en la anualidad 2022 efectuamos una búsqueda de lenguajes de programación y frameworks web para la implementación de la API, optando inicialmente por el lenguaje de programación Golang y el framework web Fiber, durante 2023 cambiamos la elección para finalmente completar el finalmente completar el desarrollo del servidor en el lenguaje **Javascript**, y utilizando el framework **Node.js**. La necesidad de realizar este cambio sobre la opción inicialmente investigada fue debido a una mejor compatibilidad de diferentes librerías de integración con las redes Blockchain.

Respecto a los **endpoints de la API,** si en la anualidad 2022 comenzamos a definir los endpoints de consulta (de tipo *get*), durante 2023 éstos se han mantenido con mínimos cambios, así mismo, se han añadido nuevos endpoints, como aquellos relacionados con los recursos.

A los endpoints de creación, se les ha añadido una versión que añade los datos extra a IPFS. IPFS o "InterPlanetary File System", es un protocolo de red p2p para el almacenamiento de archivos en una red distribuida que ya analizamos durante la ejecución de la tarea T2.4 (Reglas de negocio - contratos inteligentes) y fue finalmente la tecnología seleccionada para el almacenamiento secundario en nuestra solución de trazabilidad.

El uso de esta tecnología IPFS nos permite almacenar toda aquella información (y documentos) que no consideramos viable almacenar el Blockchain, principalmente debido al coste de red asociado en que incurrirían las empresas usuarias del sistema de traza. La solución óptima usada en DOPChain consiste en tratar este tipo de información mediante un archivo que se introduce en el almacenamiento secundario que nos brinda IPFS, archivo que es identificado mediante un hash único, el cual almacenamos en blockchain junto al resto de datos de la traza que se registran "on-chain".

T3.3: Implementación de integración de referencia

Se ha desarrollado el 100% del trabajo asociado a esta tarea. En concreto, para la implementación de integración de referencia se han considerado dos, a partir de lo descrito en previos PTs, concretamente para la DOP del Vino de Cangas, y para la DOP del queso Manchego. Con ello se buscó validar nuestro modelo de datos y la API creada en casos que presentan diferencias y particularidades. O visto de otra forma, es una implementación que da servicio a dos casos de uso.

Y dado que tanto la aplicación de inserción (T4.1) como la de consulta (T4.2) basan su ejecución en la API desarrollada, y en el posible grado de integración de ésta con los sistemas de las empresas usuarias del

sistema de traza, se hizo necesario ya desde esta tarea realizar un profundo análisis para las dos DOP mencionadas.

Para la **implementación de referencia del Vino de Cangas**, obtuvimos diferentes documentos del organismo encargado de su denominación de origen, el Consejo Regulador de la Denominación Vino de Cangas[1]. Asimismo, se comprobó que hay ocho bodegas que elaboran Vino de Cangas y que serían las principales empresas que registren datos en el sistema de traza como potenciales usuarios tanto de la API como de la aplicación de registro.

El objetivo fue obtener toda la información posible sobre el proceso de producción de dicho producto, y en la medida de lo posible conocer el estado tecnológico de los principales actores de la cadena del vino, con especial atención al posible grado de integración de sus sistemas de información con la API ofrecida por el sistema DOPchain para registrar y consultar los eventos a trazar.

Con el fin de determinar qué eventos ocurren en la producción del Vino de Cangas, y qué actores se ven involucrados, se realizó un estudio de la cadena de producción. Para ello, se realizaron consultas a la DOP del producto para poder conocer en detalle qué características específicas tienen los procesos asociados a la elaboración del Vino de Cangas.

De ello concluimos que ciertos requisitos establecidos en la DOP[2], como el análisis químico del vino, los requisitos de cómo se realiza el cultivo de la uva o las características organolépticas, no resultan relevantes para un consumidor final y por tanto carecen de peso al trazar (inversamente) el producto.

Sin embargo, otra información como las diferentes **variedades de uva** usadas para la elaboración del vino tinto y blanco, así como el **origen geográfico de la uva**, sí es información que el usuario consumidor aprecia. Así, el vino tinto de Cangas sólo puede usar uva de entre 7 variedades concretas y procedentes de zonas geográficas enmarcadas en los términos municipales de Allande, Cangas de Narcea, Degaña, Grandas de Salime, Ibias, Pesoz, y algunas zonas de Tineo.

Figura 29. Mapa de los términos municipales aceptados para la plantación de uva de Vino de Cangas

Teniendo en cuenta estas características, se determinó que el Vino de Cangas pasa por los siguientes procesos para su producción: **recogida** de la uva (donde se indica donde se realizó dicha vendimia), el **prensado**, **certificación** (donde se indica la fecha de obtención del sello de calidad) y el **embotellado**. A esta serie de eventos, que comprenden hasta obtener el producto en su forma final (botellas de vino),

[1] Consejo Regulador de la Denominación Vino de Cangas https://docangas.es/consejo-regulador-y-legislacion/

[2] Pliego de Condiciones de la DOP Vino de Cangas https://www.mapa.gob.es/es/alimentacion/temas/calidad-diferenciada/cangas_2019_01_01_tcm30-210490.pdf

para completar el sistema de trazabilidad debemos al menos añadir un evento correspondiente a la **distribución** del producto.

Durante la modelación de procesos del Vino de Cangas, se ha detectado que, aunque la trazabilidad sea 'lineal', p.ej. Agricultor → transformador/productor → distribuidor → consumidor, se debería contemplar la posibilidad de que haya para un mismo tipo de evento, más de una empresa implicada. Por ejemplo, podría haber dos transformadores y tres distribuidores, tanto en línea como en paralelo. Un ejemplo de esto sería que haya un transformador que recoja la uva, la procese, y después, en lugar en meterlo en barrica para su fermentación, se embotella y vende (lo que se conoce como mosto), y que sea otra empresa la que recibe ese zumo de uva y continúe con el proceso hasta crear vino. En dicho ejemplo, tendrían que considerarse dos transformadores.

Otro aspecto detectado es que una misma empresa productora podría tener distintas marcas del producto (incluso bajo una misma DOP). Por ello, también debe poder permitirse que una misma empresa cuente con distintas marcas en el sistema.

Respecto a la integración de los procesos con el sistema DOPChain, se detectó un inconveniente relativo a la inclusión de un QR en las contra etiquetas en las botellas: la adición de nuevos elementos al diseño actual de la contraetiqueta conlleva el desafío de integrarlo en el mismo, pues o bien implica usar un QR demasiado pequeño, o bien optar por ubicarlo a la derecha produciendo una etiqueta demasiado larga.

Figura 30. Ejemplo de contraetiqueta de Vino de Cangas con código QR

Además, cualquier cambio puede conllevar un sobrecoste relacionado con la impresión de nuevas etiquetas, e incluso la necesidad de adaptar o renovar algunos dispositivos de impresión, algo que algunas bodegas consideran no deseable por el momento, o incluso no asumible en algunos casos.

Por ello, una propuesta más realista es utilizar el código QR en materiales promocionales, para medios de comunicación, hostelería y comercios, entre otros, como puede verse en la siguiente propuesta:

Figura 31. Ejemplo de etiqueta con el QR para una botella de Vino de Cangas

Este código QR promocional funcionaría como punto de acceso rápido de los consumidores a la aplicación de consulta, donde podrían introducir el código identificador que aparece en la contraetiqueta de la botella. De esta forma el usuario accedería de manera sencilla a la traza del producto (lote de vino).

Sobre la **implementación de referencia del Queso Manchego,** también se obtuvo información de diversos documentos del Consejo Regulador de la Denominación Queso Manchego. Asimismo, se comprobó que hay unos 70 elaboradores inscritos en la DOP (35 de leche pasteurizada y 29 de leche cruda) más 6 cámaras de maduración, y que serían las principales empresas que registren datos en el sistema de traza como potenciales usuarios tanto de la API como de la aplicación de registro.

Nuestro objetivo consistió en recopilar toda la información disponible acerca del proceso de producción de este producto específico. Al igual que con el Vino de Cangas, también buscamos conocer el nivel tecnológico de los principales participantes en la cadena de producción del queso.

También se estudió la propia cadena de producción del Queso Manchego, para así conocer los eventos y actores involucrados en la misma. Para ello, se consultó a la DOP del producto para poder conocer en detalle qué características específicas tienen los procesos asociados a la elaboración del Queso Manchego.

Gracias a este estudio, pudimos determinar que ciertos aspectos mencionados en el pliego de condiciones de DOP Queso Manchego[3], como las características analíticas de la leche, las características físicas del queso en maduración, así como las características físico-químicas y organolépticas, no son de especial interés para la traza del producto desde el punto de vista del consumidor final.

Tampoco lo son varios procesos internos de las queserías inherentes a la elaboración del queso, como el cuajado, salado, desuerado, moldeado y prensado, y por ello no han sido considerados para la implementación de referencia del sistema de trazabilidad.

Sin embargo, las características ligadas a la geografía, y ciertos procesos que diferencian comercialmente el producto final, como la maduración, sí son de interés para un consumidor final, y por ello a tener en cuenta en el sistema de trazabilidad.

[3] Pliego de condiciones de la DOP Queso Manchego
https://www.mapa.gob.es/images/es/queso_manchego_2022_11_03_rev_tcm30-209998.pdf

Se ha determinado que la **producción, elaboración y maduración** del Queso Manchego deben llevarse a cabo exclusivamente en la comarca de La Mancha, específicamente en los términos municipales de las provincias de Albacete, Ciudad Real, Cuenca, y Toledo. Esta información es importante para que el consumidor pueda constatar el origen del Queso Manchego.

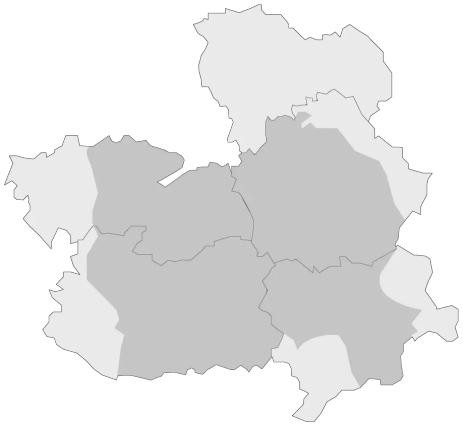

Figura 32. Mapa de las zonas geográficas permitidas para la elaboración del Queso Manchego en la comunidad de Castilla la Mancha.

Sobre el proceso de maduración, también se ha observado que **el tiempo que el queso ha estado madurando es importante**, pues es común distinguir comercialmente entre **quesos semicurados, curados y añejos**, algo que suele llevar aparejada también una **diferenciación en su precio** de venta (alrededor de un 10% por nivel de maduración).

Figura 33. Ejemplo de quesos: semicurado (izda.), curado (centro) y añejo (dcha.). Fuente: Artequeso.

Con toda esta información, se determinó que la traza que se va a utilizar para la DOP Queso Manchego estará compuesta por, primero el **ordeño de la oveja** (indicando la ganadería de origen del animal), el **análisis de la leche** (sin hacer especial referencia a sus características), la **elaboración del queso**, indicando el lugar donde este se está llevando a cabo, pero sin entrar en los procesos internos del mismo. Además, debido a que un mismo queso puede tener tiempos de curación diferentes, esto también formará parte de la traza como **maduración**. Finalmente, una vez el queso ha completado su proceso de producción, puede venderse en diversos formatos (queso entero, medio queso, queso pequeño de kilo, cuñas, etc.), información que formará parte también de la traza dentro del proceso de **empaquetado**.

Figura 34. Ejemplos de empaquetado: medio queso (izda.), cuña (centro) y queso de kilo (dcha.). Fuente: Artequeso.

Para el estudio de integración del código QR en el Queso Manchego, CTIC recibió de su Consejo Regulador de la DOP un conjunto representativo de las contraetiquetas numeradas en sus diferentes formas, incluyendo la variante de queso artesano (elaborado con leche cruda) y diversos formatos de empaquetado (cuñas 1/12, 1/16). Se observó también que en dichas etiquetas no existe una distinción entre quesos curados y semicurados.

Figura 35. Contraetiquetas identificativas del Queso Manchego.

Gracias a esto, pudimos concluir que la inclusión del código en la mismas es inviable, debido al pequeño tamaño de las mismas, lo que lo haría ilegible. La inclusión del código QR requeriría cambiar el formato de las propias etiquetas, solución que fue descartada por los problemas que esto causaría a la propia DOP y sus miembros.

Otro aspecto observado es el **pequeño tamaño del número identificativo en la contraetiqueta**, lo que dificulta una rápida y clara lectura para usuarios con problemas de visión o en condiciones de luz escasa y propicia que llegue con errores dicho número a la aplicación de consulta de la traza. Esto impacta negativamente en la experiencia de usuario, ya que solo recibirá un mensaje sobre la inexistencia en el sistema del producto.

Como posible solución, se investigó la inclusión de un sistema óptico de reconocimiento de caracteres (u OCR), con la idea de que el usuario pudiese simplemente fotografiar con su dispositivo móvil la contraetiqueta para buscar directamente la traza. Para ello, nos enfocamos en las posibilidades de una solución de Google Cloud[4], la cual requiere de un pago por cada cierto número de peticiones realizadas.

[4] Google cloud OCR https://cloud.google.com/use-cases/ocr?hl=es

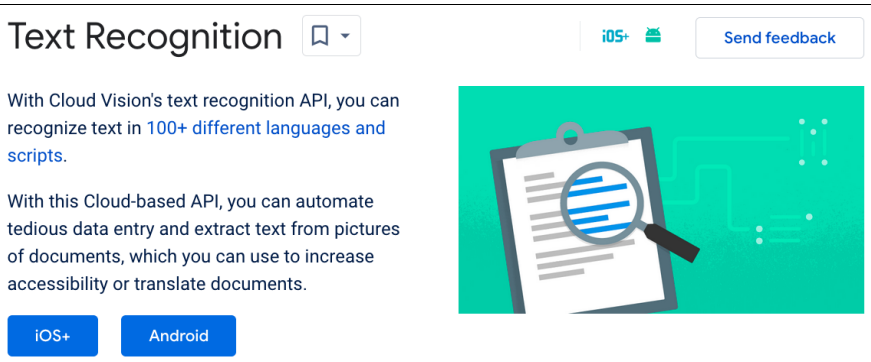

Figura 36. Servicio de Google para dotar de funcionalidad OCR a aplicaciones móviles iOS y Android.

Las pruebas realizadas arrojaron unos buenos resultados, pero consideramos que la integración de este tipo de sistema requiere, aparte del pago por uso, de una complejidad de desarrollo que a nuestro juicio excede la de una implementación de referencia como la prevista en este proyecto. Sin embargo, concluimos que es una vía de futuro prometedora que a alguna DOP le puede interesar explorar.

Otra cuestión particular del Queso Manchego es la existencia de **problemas relacionados con su falsificación o imitación/evocación**[5] de la DOP Queso Manchego, algo que un simple código QR tampoco puede evitar, ya que pueden replicarse o falsificarse fácilmente, pues son de código abierto y cualquiera puede crearlos en cuestión de segundos.

Teniendo en cuenta que otro elemento de identificación que emplea la DOP es una placa de caseína con forma de corona circular incrustada en la corteza del queso (con el texto "D.O.P. QUESO MANCHEGO" y una serie de dígitos y letras), analizamos la posibilidad de incluir en la misma un elemento físico basado en tecnología RFID o bien en un micro-transpondedor (similar a los usados para la identificación animal) que alguna otra DOP de queso en Europa parece haber comenzado[6] a explorar.

Finalmente, aunque se considera como una vía de futuro a explorar, se descarta abordar la consideración de este tipo de elemento de seguridad en la actual implementación de referencia, por introducir una mayor complejidad en su gestión, costes asociados al equipamiento específico con el que deberían dotarse los productores de queso, y no ser algo destinado al consumidor final (que carece del dispositivo lector del transpondedor).

Paquete de Trabajo 4: Plataformas de inserción y consulta de datos

En esta fase se lleva a cabo el planteamiento tecnológico, el diseño y el desarrollo de una aplicación adecuada para la inserción de datos en el sistema de trazabilidad basado en blockchain de DOPChain, así como para la consulta de la traza de los productos registrados.

[5] Sentencia del Tribunal Supremo de 18 de julio de 2019 sobre evocación de la Denominación de Origen "Queso Manchego" https://berenguer-pomares.com/asuntos-del-despacho/supremo-manchego/

[6] How a Breakthrough Partnership Changed the Game for Parmigiano Reggiano https://p-chip.com/how-a-breakthrough-partnership-changed-the-game-for-parmigiano-reggiano/

Este paquete se organiza en torno a dos tareas, de las cuales una de ellas (T4.1) se inició en 2022 y completó en 2023, mientras que la otra (T4.2) se inició y terminó en la anualidad 2023. A continuación se describen las acciones desarrolladas en cada una de dichas tareas y los principales resultados alcanzados.

T4.1: Diseño y desarrollo de aplicación inserción

Se ha desarrollado el 100% del trabajo asociado a esta tarea. En concreto, si en la anualidad 2022 exploramos tecnologías adecuadas para trabajar con las plataformas blockchain TELOS y Ethereum, y nuestros contratos inteligentes y API, valorando como mejores opciones los frameworks Angular y React, durante 2023 optamos por desarrollar la aplicación de inserción utilizando el framework **React**.

Basándonos en una definición completa de los requisitos funcionales para la diversidad de actores involucrados en la cadena, según el modelo de datos diseñado, adaptándonos a una múltiple tipología de productos, y considerando las especificidades y definición de alcance para implementaciones de referencia asociadas a los casos de uso considerados (vino D.O.P Cangas y Queso Manchego), como se analizó en la tarea correspondiente (T3.3: Implementación de integración de referencia), desarrollamos una aplicación web que, a base de formularios, permite crear los distintos elementos necesarios para la construcción de la traza del producto.

Dicha aplicación web cuenta con una pantalla de login donde los usuarios inician sesión, usando su usuario, contraseña y código TOTP. TOTP (time-based one time password) o contraseña de un solo uso basada en tiempo, es un método que obliga al usuario a introducir un código de 6 dígitos al iniciar sesión, el cual expira cada poco tiempo. Esto nos ha permitido añadir una capa extra de seguridad a la aplicación.

En la construcción del frontend, la interfaz de usuario, utilizamos varios componentes pertenecientes a la librería React Bootstrap[7], como por ejemplo la barra superior de tareas. Y para los formularios nos hemos apoyado en la librería React Hook Form, la cual simplifica la creación de formularios, incluyendo ayudas a la creación de campos en forma de array por ejemplo.

T4.2: Diseño y desarrollo de aplicación de consulta

Se ha desarrollado el 100% del trabajo asociado a esta tarea. De la misma forma que para la aplicación de consulta, la interfaz de la aplicación fue desarrollada en React.

Esta aplicación de consulta consta de dos pantallas, la principal, donde el usuario puede introducir un identificador de un producto para buscar su traza, y otra donde dicha traza es mostrada.

Para mostrar dicha traza, se ha desarrollado un módulo basado en React-flow llamado dango-graph, el cual nos permite mostrar de forma flexible cualquier tipo de traza que cumpla con el modelo de datos.

El formato de presentación de la información al usuario se realiza mediante lo que llamamos tarjetas interconectadas, derivado de una tendencia de diseño denominada en inglés Card UI (muy popular en aplicaciones móviles y redes sociales), que hemos construido sobre un módulo que toma como base React Flow[8]. En esta interfaz de consulta, cada una de las tarjetas o cards corresponde en el sistema a un evento en la traza del producto.

[7] Página web de React Bootstrap https://react-bootstrap.netlify.app/

[8] Página web de React flow https://reactflow.dev/

Conceptualmente, estas tarjetas asemejan tarjetas o cartas físicas (como en una baraja), algo familiar que puede ayudar a que los usuarios comprendan rápidamente el propósito de cada tarjeta en la aplicación. Proporcionan una jerarquía visual clara, organizando la información en pequeños bloques autónomos, y se adaptan bien al diseño responsivo, lo que permite adaptarlas a distintos tamaños de pantalla, orientaciones y tipos de dispositivo, como teléfonos o tabletas.

Pero no se ha optado por diseñar una interfaz optimizada para dispositivos móviles solo por su aspecto visual, sino también porque constatamos que el número de visitas recibidas por este tipo de dispositivos en las páginas web es superior[9], una tendencia a seguir creciendo en los próximos años.

Otra razón que apoya esta decisión tiene relación con el contexto de uso, pues entendemos que un usuario que quiera conocer la traza de un producto de estas características (vino, queso) es muy probable que lo haga en un entorno donde llevar otro tipo de dispositivos no es habitual (por ejemplo, en una tienda o un restaurante).

Durante el desarrollo de esta interfaz, debimos solventar una problemática asociada al espacio disponible, pues un teléfono móvil, aun teniendo una pantalla relativamente grande, no permite incluir una gran cantidad de datos. De hecho, una de las recomendaciones para este tipo de interfaz es limitar el contenido del grueso del texto a menos de 100 caracteres o a no más de un par de frases cortas.

Si bien utilizamos casi la totalidad de la pantalla para mostrar la información, observamos situaciones en las que el evento que se está mostrando requiera mostrar una cantidad de información que excede lo recomendable, o incluso el máximo espacio visualizable en la interfaz.

Es por esto que planteamos distintos diseños del interior de la tarjeta, buscando aprovechar al máximo el espacio según la información. Por ejemplo, para información relativa a actores o sellos de calidad, se implementó un *slider* (control deslizante) que mediante unas flechas permite cambiar la información mostrada en una sección de la tarjeta.

Concluimos también que una posible mejora para esta interfaz sería dotarla de un sistema de navegación por la misma mediante gestos, ya que los usuarios están ya acostumbrados a usarlos en otras aplicaciones móviles, siendo algo que se podría investigar en un futuro.

Paquete de Trabajo 5: Plan de pruebas, validación y transferencia

En esta fase se diseñó el plan y entorno de pruebas, para constatar el correcto funcionamiento del sistema, así como el despliegue de una versión piloto. En base a los resultados obtenidos, se realizó una evaluación del sistema. Finalmente, una vez probado y validado el piloto, se ha creado el material necesario para una transferencia del conocimiento del sistema.

Este paquete de trabajo consta de un total de 4 tareas, las cuales comenzaron y concluyeron todas en la anualidad 2023. A continuación se describen las acciones desarrolladas y los principales resultados alcanzados en cada una de dichas tareas.

T5.1: Definición de los criterios de evaluación y del entorno de pruebas

Se ha desarrollado el 100% del trabajo asociado a esta tarea. Se ha diseñado un plan de pruebas que nos permita comprobar el correcto funcionamiento del sistema. Para testear el componente del servidor, se

[9] Internet Traffic from Mobile Devices https://explodingtopics.com/blog/mobile-internet-traffic

diseñó un plan de test unitarios con el fin de ejecutarlos usando el framework de test Jest. Una prueba unitaria de software es un tipo de prueba que evalúa de manera aislada y exhaustiva el comportamiento de un componente individual del código. Se centra en verificar que cada función o método produzca los resultados esperados bajo diferentes condiciones, ayudando a garantizar la calidad y robustez del sistema.

También se realizaron pruebas de integración para probar las comunicaciones entre los distintos componentes del sistema. Las pruebas de integración evalúan la interacción entre distintos módulos del sistema para garantizar su correcta combinación y funcionamiento. Por ejemplo para testear los diferentes endpoints del servidor, se utilizó peticiones Postman. Así mismo, se ha probado como las diferentes funcionalidades implementadas en dichos endpoints interactúan con otros componentes, como las redes blockchain.

Finalmente, se realizaron pruebas funcionales. Esto nos permite comprobar el correcto funcionamiento de las funcionalidades del sistema (las mismas que utiliza el usuario final).

T5.2: Despliegue piloto del sistema en entorno de pruebas

Se ha desarrollado el 100% del trabajo asociado a esta tarea. Se ha desplegado un piloto del sistema utilizando la implementación de referencia de la DOP del Vino de Cangas, principalmente por su menor tamaño (8 productores) y cercanía geográfica, lo cual facilita resolver in-situ cuestiones de integración y pruebas que puedan necesita una visita presencial, ya sea de alguna de las empresas usuarias en nuestro entorno de pruebas en CTIC, o de personal de CTIC a las instalaciones de la empresa en casos concretos.

Con esto logramos tener un sistema de demostración robusto con el que todo tipo de usuarios (empresas y consumidores finales) pueden interactuar, y así comprobamos que el sistema no solo funciona como técnicamente estaba previsto (las funcionalidades fueron implementadas), sino que además es usable por la diversidad de actores involucrados en la cadena del producto.

A partir del despliegue de dicho piloto, dispusimos de toda la información necesaria para crear el manual de usuario, que es el documento de guía en el uso de las aplicaciones de consulta y registro.

T5.3: Evaluación y análisis de resultados

Se ha desarrollado el 100% del trabajo asociado a esta tarea. Se ha desarrollado una evaluación exhaustiva y un análisis detallado de los resultados para asegurar que **ambas aplicaciones, la de registro y la de consulta**, cumplen con los objetivos y requisitos establecidos.

A través de dicho análisis, **hemos validado su eficacia y rendimiento**, garantizando así su alineación con los criterios previamente definidos. Toda la arquitectura validada comprende los elementos indicados en la imágen mostrada a continuación.

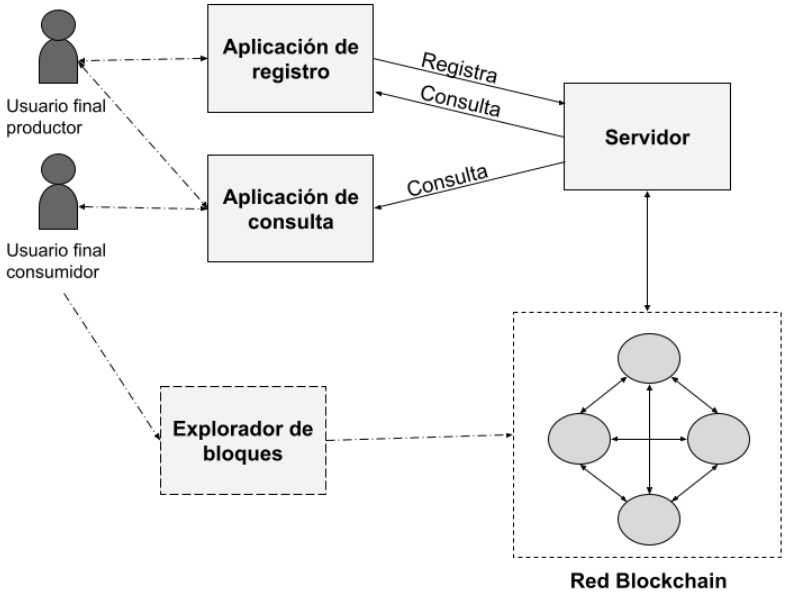

Figura 39. Arquitectura DOPChain de alta capa con aplicaciones de registro y consulta

Un aspecto destacable, alineado con la tecnología Blockchain, es que independiente del sistema de registro y consulta que hemos implementado mediante sendas aplicaciones, **un usuario siempre podrá acceder de forma independiente desde un explorador de bloques a toda la información almacenada por DOPChain** en el registro de la plataforma Blockchain correspondiente.

Por ejemplo, en Ethereum podría usar Etherscan[10], tanto para la red principal o *mainnet* como para redes de test como Sepolia[11], mientras que en la plataforma Blockchain Telos podría usar EOS Authority, tanto para su red principal[12] como para la red de test[13].

Figura 40. Ejemplo de transacciones DOPChain mostradas desde el explorador de EOS Authority

T5.4: Generación de material para transferencia

[10] Etherscan Ethereum Blockchain Explorer https://etherscan.io/
[11] Etherscan Sepolia Testnet Explorer https://sepolia.etherscan.io/
[12] EOS Authority Telos Explorer https://eosauthority.com/?network=telos
[13] EOS Authority Telos Testnet Explorer https://eosauthority.com/?network=telostest

Se ha desarrollado el 100% del trabajo asociado a esta tarea. Se ha creado el material necesario para ejecutar el sistema en nuevos entornos y para el manejo del mismo por los usuarios.

Por un lado, como ya se mencionó con anterioridad (en T5.2), se ha elaborado un manual (E5.2 - Manual de usuario) para referencia funcional del sistema y consulta por Consejos Reguladores, empresas productoras y usuarios finales interesados.

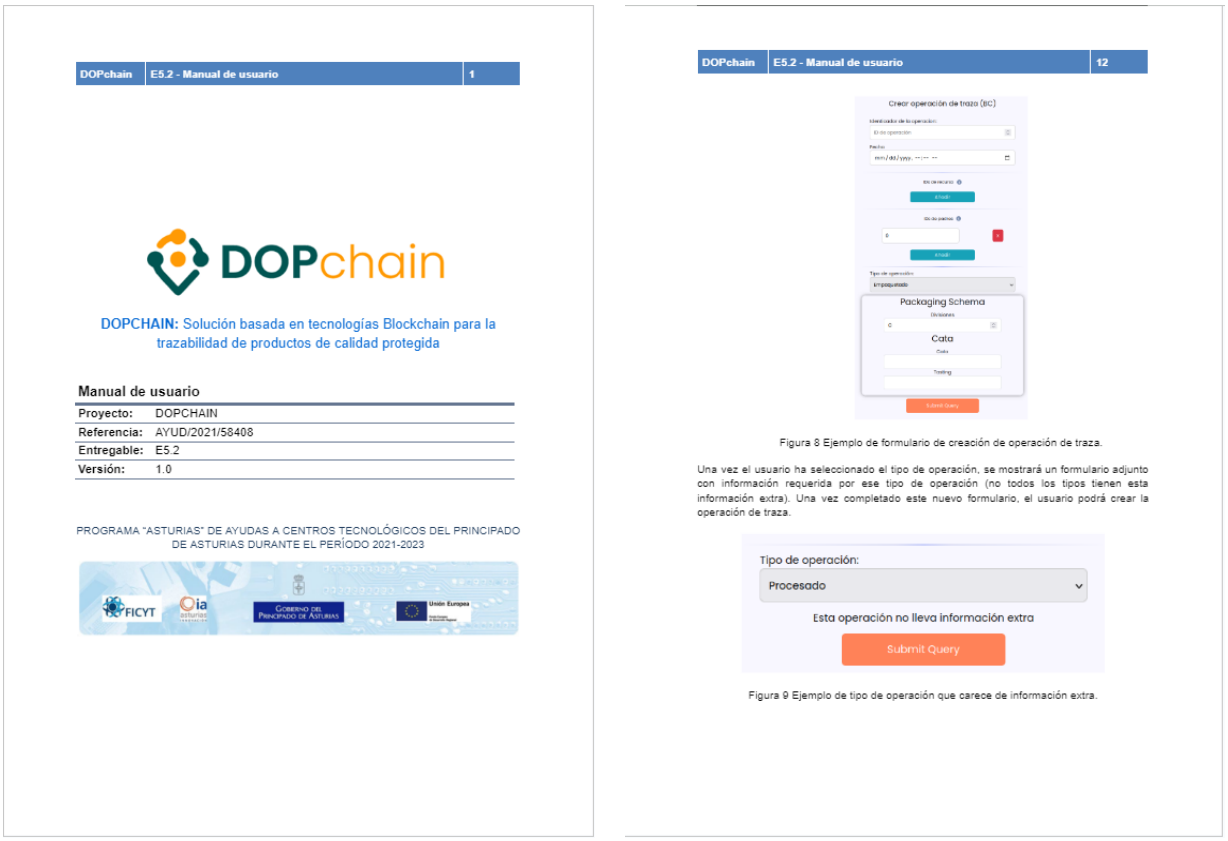

Figura 41. Portada (izda.) y página de ejemplo (dcha.) del manual de usuario (E5.2)

Pero además, se ha elaborado otro manual para referencia técnica del sistema y consulta por empresas implantadoras (del sector TI principalmente), o incluso por empresas productoras que cuentan con personal experto. Dicho manual incluye guías sobre cómo descargar, configurar y desplegar el sistema en cualquier nuevo equipo/entorno de infraestructuras de datos.

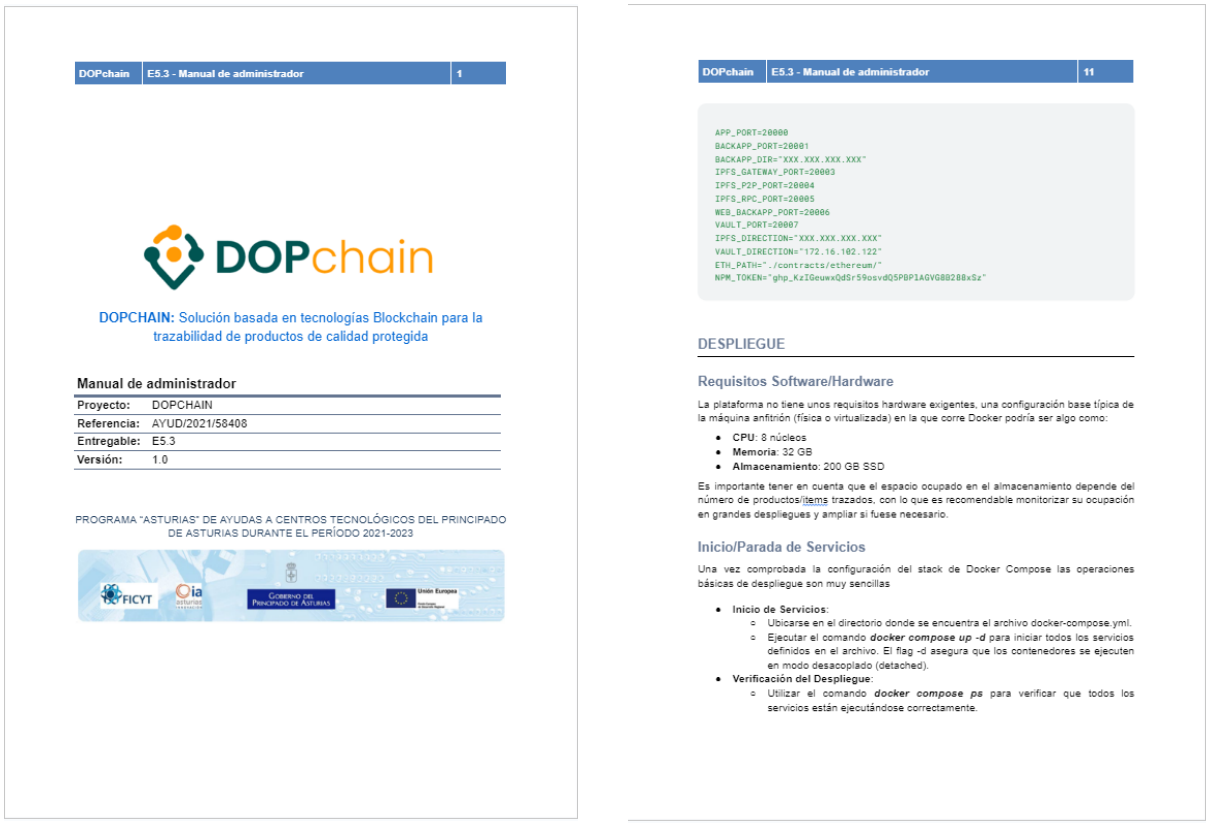

Figura 42. Portada (izda.) y página de ejemplo (dcha.) del manual de administrador (E5.3)

2. RESULTADOS CONSEGUIDOS

Justificación 2021

Se han conseguido todos los resultados planificados para esta primera anualidad, tal y como se había planteado en la memoria inicial. Dichos resultados se relacionan principalmente con el OE1 y OE4, como se muestra a continuación:

- OE1 – Facilitar y mejorar el acceso a información sobre la trazabilidad de los productos agroalimentarios.
- OE3 - Favorecer la digitalización de los procesos productivos a lo largo de la cadena de valor mediante una solución de trazabilidad que refleje esta digitalización al consumidor.
- OE4 – Habilitación de un gran espacio de datos abiertos en blockchain sobre los productos protegidos.

Por otro lado, la T1.3 iniciada en 2021 y con fecha de finalización prevista en 2022 se encuentra ligada fundamentalmente al OE5 - Mejorar la seguridad de los productos con elementos físicos y certificados digitales.

Así, **se cumple la planificación planteada hasta el momento para alcanzar cada uno de estos objetivos**, siendo satisfechos de forma parcial hasta el momento y alcanzándose las metas de avance establecidas hacia su completa consecución. Los resultados que se espera obtener se entiende que contribuirán a incrementar el corpus de conocimiento en torno a las tecnologías de registro distribuido y blockchain, especialmente en su aplicación a retos de la industria agroalimentaria y su problemática habitual explicitada mediante casos de uso reales, complementando proyectos de investigación recientes, en los que CTIC ha tomado parte activa.

A nivel interno, DOPCHAIN está alineado totalmente con la Estrategia del Centro, tanto a nivel tecnológico como a nivel de contribución a la Misión/Visión del Centro (localización, generación de valor en empresas y Sociedad, desarrollar actividad en el estado de la técnica).

En base a ello, DOPCHAIN es uno de los proyectos estratégicos que CTIC-Centro Tecnológico ha lanzado en el año 2021 para vertebrar el I+D asociado al despliegue de su Roadmap Tecnológico.

Justificación 2022

Se han conseguido todos los resultados planificados para esta segunda anualidad, tal y como se había planteado en la memoria inicial, tal como se muestra a continuación:

- OE1 – Facilitar y mejorar el acceso a información sobre la trazabilidad de los productos agroalimentarios.
- OE3 - Favorecer la digitalización de los procesos productivos a lo largo de la cadena de valor mediante una solución de trazabilidad que refleje esta digitalización al consumidor.
- OE4 – Habilitación de un gran espacio de datos abiertos en blockchain sobre los productos protegidos.
- OE5 – Mejorar la seguridad de los productos con elementos físicos y certificados digitales.

Los resultados que se espera obtener se entiende que contribuirán a incrementar el corpus de conocimiento en torno a las tecnologías de registro distribuido y blockchain, especialmente en su aplicación a retos de la industria agroalimentaria y su problemática habitual explicitada mediante casos de uso reales, complementando proyectos de investigación recientes, en los que CTIC ha tomado parte activa.
A nivel interno, DOPCHAIN está alineado totalmente con la Estrategia del Centro, tanto a nivel tecnológico como a nivel de contribución a la Misión/Visión del Centro (localización, generación de valor en empresas y Sociedad, desarrollar actividad en el estado de la técnica).

En base a ello, DOPCHAIN es uno de los proyectos estratégicos que CTIC-Centro Tecnológico ha lanzado en el año 2021 para vertebrar el I+D asociado al despliegue de su Roadmap Tecnológico.

Justificación 2023

Se han conseguido todos los resultados planificados para esta tercera y última anualidad, tal como se muestra a continuación:

- OE1 – Facilitar y mejorar el acceso a información sobre la trazabilidad de los productos agroalimentarios.
- OE2 - Visibilizar la calidad de los productos y los procedimientos que rigen una entidad.
- OE3 - Favorecer la digitalización de los procesos productivos a lo largo de la cadena de valor mediante una solución de trazabilidad que refleje esta digitalización al consumidor.
- OE4 – Habilitación de un gran espacio de datos abiertos en blockchain sobre los productos protegidos.
- OE5 – Mejorar la seguridad de los productos con elementos físicos y certificados digitales.

Los resultados obtenidos contribuyen a incrementar el corpus de conocimiento en torno a las tecnologías de registro distribuido y blockchain, especialmente en su aplicación a retos de la industria agroalimentaria y su problemática explicitada mediante casos de uso reales, complementando proyectos de investigación recientes, en los que CTIC ha tomado parte activa.

A nivel interno, DOPCHAIN está alineado totalmente con la Estrategia del Centro, tanto a nivel tecnológico como a nivel de contribución a la Misión/Visión del Centro (localización, generación de valor en empresas y Sociedad, desarrollar actividad en el estado de la técnica).

En base a ello, DOPCHAIN es uno de los proyectos estratégicos que CTIC-Centro Tecnológico lanzó en el año 2021 para vertebrar el I+D asociado al despliegue de su Roadmap Tecnológico.